Оставьте отзыв о скачивании PDF-файла.

документация по Exchange Server

Добро пожаловать в Microsoft Exchange Server! Ниже приведены основные сведения о начале работы.

О Exchange Server

СКАЧАТЬ

Приобретение Exchange или скачивание пробной версии

Скачивание полных версий, включая обновления

НОВОЕ

Новые возможности

Настройка Outlook

Планирование и развертывание

ОБЩИЕ СВЕДЕНИЯ

Помощник по развертыванию Exchange Server для быстрого развертывания

Заметки о выпуске для Exchange

РАЗВЕРНУТЬ

Требования к системе Exchange

Предварительные требования для Exchange

Подготовка Active Directory и доменов

Установка и обновление

ПРАКТИЧЕСКОЕ РУКОВОДСТВО

Установка роли почтового ящика Exchange с помощью мастера установки

Установка Exchange в автоматическом режиме

Установка роли пограничного транспорта Exchange с помощью мастера установки

Обновление Exchange до последнего накопительного обновления

Задачи Exchange после установки

Ссылка

ССЫЛКА

форумы Exchange Server

Exchange Server 2010

Exchange Server 2013

Новые возможности Exchange Server

Статья • 04.04.2023

Exchange Server 2019 г. предоставляет новый набор технологий, функций и служб для Exchange Server, платформу обмена сообщениями, которая предоставляет электронную почту, планирование и инструменты для пользовательских приложений службы совместной работы и обмена сообщениями. Ее цель — поддержка пользователей и организаций по мере того, как акцент в их деятельности переходит от связи к совместной работе. В то же время Exchange 2019 помогает снизить общую стоимость владения при развертывании Exchange 2019 в локальной среде или подготовке почтовых ящиков в облаке.

Выберите раздел ниже, соответствующий версии Exchange, с которую выполняется обновление. Если вы хотите узнать о функциях, которые были удалены или заменены в Exchange 2019, см. статью Что прекращено в Exchange Server.

Дополнительные сведения о развертывании Exchange 2019 см. в статье Планирование и развертывание Exchange Server.

Какие новые возможности появятся при обновлении Exchange 2016 до Exchange 2019?

Настройка

- **Сохранение пользовательской конфигурации**. Программа установки Exchange теперь выполняет резервное копирование и восстановление наиболее распространенных файлов конфигурации, чтобы администраторам больше не нужно восстанавливать их вручную или повторно применить их. Дополнительные сведения см. в разделе Exchange Server сохранение настраиваемой конфигурации.

Безопасность

- **Поддержка Windows Server Core**. Работа Exchange при развертывании Windows с меньшей областью взаимодействия помогает уменьшить возможности для атак и сократить количество обслуживаемых компонентов.
- **Блокировка внешнего доступа к Центру администрирования Exchange и командной консоли Exchange**. Правила клиентского доступа позволяют

разрешить администрирование Exchange только из внутренней сети без вовлечения сложных сетей и правил брандмауэра.

- **TLS 1.2 — единственная версия, включенная по умолчанию**. Exchange Server 2019 содержит важные изменения, повышающие безопасность клиентских и серверных подключений. Настройка по умолчанию для шифрования поддерживает только TLS 1.2 и не поддерживает более ранние алгоритмы (а именно, DES, 3DES, RC2, RC4 и MD5). В ней также настроены алгоритмы обмена ключами эллиптических кривых, обладающие приоритетом над алгоритмами неэллиптических кривых. В Exchange Server 2016 и более поздних версиях все параметры шифрования наследуются из настройки, указанной в операционной системе. Дополнительные сведения см. в руководстве по Exchange Server TLS.

- **Поддержка современной проверки подлинности для чистых локальных сред**: Exchange Server 2019 поддерживает OAuth 2.0 (современная проверка подлинности) для чистых локальных сред, использующих ADFS в качестве службы маркеров безопасности (STS). Дополнительные сведения и требования см. в статье Включение современной проверки подлинности в локальной среде Exchange.

Производительность

- **Улучшенная инфраструктура поиска**. Полностью перестроенная инфраструктура поиска для масштабирования и надежности облака в Exchange Online теперь доступна в Exchange 2019. Эта новая инфраструктура поиска позволяет индексировать файлы большего размера, упростить управление и повысить производительность поиска.

- **Более быстрая и надежная отработка отказов.** Изменения архитектуры поиска привели к гораздо более быстрой и надежной отработке отказа между серверами.

- **База данных Metacache**. Улучшения в ядре СУБД Exchange позволили повысить общую производительность и использовать новейшее оборудование для хранения, в том числе SSD и другие диски большего размера.

- **Поддержка современного оборудования**. Exchange теперь поддерживает до 256 ГБ памяти и до 48 ядер ЦП.

- **Динамический кэш базы данных**. Для процесса хранения информации используется выделение кэша динамической памяти, что оптимизирует

использование памяти для активного использования базы данных.

Клиенты

- **Параметр "Не пересылать" для календаря.** Напоминает управление правами на доступ к данным (IRM) для элементов календаря без требований к развертыванию IRM. Посетители не могут пересылать приглашение другим людям, и только организатор может пригласить других пользователей.
- **Календарь— лучшее отсутствие на рабочем месте**: дополнительные параметры, когда вы не будете в офисе. К ключевым параметрам относятся: добавление в календарь события, которое отображает вас как "Вне офиса", а также быстрый вариант отмены или отклонения собраний, которые будут происходить в отсутствие.
- **Календарь — Remove-CalendarEvents командлет**: позволяет администраторам отменять собрания, организованные пользователем, покинующим компанию. Ранее конференц-залы или участники собрания постоянно имели эти несуществующее собрание в своих календарях.
- **Интернационализация адресов электронной почты (EAI)**. Маршрутизация и доставка электронных адресов с символами, отсутствующими в английском алфавите, выполняется теперь нативно.

Какие новые возможности появятся при обновлении Exchange 2013 до Exchange 2019?

Архитектура Exchange 2019

Сегодня ЦП с высокой вычислительной мощностью стоят значительно меньше, поэтому их цена больше не является сдерживающим фактором. Когда это ограничение снято, основной целью проектирования для Exchange 2019 является простота масштабирования, использования оборудования и изоляции сбоев. В Exchange 2019 мы сократили число ролей сервера до двух: почтовый ящик и пограничный транспортный сервер.

Единая система обмена сообщениями (UM) удалена из Exchange 2019. Кроме того, сервер почтовых ящиков в Exchange 2019 включает все серверные компоненты из ролей почтового ящика Exchange 2013 и сервера клиентского доступа:

- Службы клиентского доступа обеспечивают аутентификацию, ограниченное перенаправление и работу служб прокси-сервера. Службы клиентского доступа не выполняют обработку данных и включают все обычные протоколы клиентского доступа: HTTP, POP и IMAP, а также SMTP.
- К службам почтовых ящиков относятся все традиционные серверные компоненты, доступные в роли сервера почтовых ящиков Exchange 2013, кроме единой системы обмена сообщениями: протоколы доступа внутреннего клиента, транспортная служба и базы данных почтовых ящиков. Сервер почтовых ящиков отвечает за все действия с активными почтовыми ящиками на сервере.

Роль пограничного транспортного сервера обычно развертывается в сети периметра (за пределами внутреннего леса Active Directory) и предназначена для снижения уязвимости развертывания Exchange. За счет обработки всего потока почты из Интернета она также добавляет дополнительные уровни защиты от вирусов и спама и позволяет применять правила управления потоком обработки почты (также известные как правила транспорта) для управления потоком обработки сообщений.

Дополнительные сведения об архитектуре Exchange 2019 см. в статье Архитектура Exchange.

Наряду с новой ролью почтовых ящиков Exchange 2019 теперь позволяет прокси-трафик от серверов клиентского доступа Exchange 2013 к почтовым ящикам Exchange 2019. Эта новая гибкость обеспечивает больший контроль при переходе на Exchange 2019, не беспокоясь о развертывании достаточного объема интерфейсной емкости для обслуживания новых серверов Exchange 2019.

Клиенты

Outlook в Интернете (прежнее название — Outlook Web App)

Outlook Web App теперь называется Outlook в Интернете и по-прежнему обеспечивает доступ пользователей к почтовым ящикам Exchange из практически любого веб-браузера.

> ⓘ **Примечание**
>
> Outlook в Интернете в Exchange 2019 поддерживает браузеры Microsoft Edge, Internet Explorer 11 и почти все новейшие версии Mozilla Firefox, Google Chrome и Apple Safari.

Прежний пользовательский интерфейс Outlook Web App для настольных компьютеров и ноутбуков был обновлен и оптимизирован также для планшетов и смартфонов. Новые возможности Exchange 2019:

- **Специальные возможности для телефонов** на платформах iOS и Android.
- **Расширенные возможности для Android** с использованием Chrome на устройствах с Android 4.2 и более поздних версий.
- **Улучшение электронной почты**, в том числе новое однострочное представление папки "Входящие" и оптимизированная область чтения, архивация, смайлики и возможность отменить такие действия с почтовым ящиком, как удаление или перемещение сообщения.
- **Связывание контактов** — пользователи могут добавлять контакты из своих учетных записей LinkedIn.
- **Календарь** с новым дизайном и функциями, в том числе напоминаниями по электронной почте для событий календаря, возможностью предложить новое время в приглашениях на собрания, улучшенным поиском и календарями с днями рождения.
- **Варианты и уточнения поиска**, которые улучшают возможности поиска и позволяют быстрее находить требуемую информацию. Система поиска старается предвидеть, что ищет пользователь, и отображает результаты, которые могут ему подойти. Уточнение поиска помогает быстрее находить нужную информацию с помощью контекстных фильтров. Фильтрование данных может выполняться по диапазонам дат, отправителям и т. д.
- **Новые темы** — тринадцать новых тем с графическим оформлением.
- **Параметры** для отдельных почтовых ящиков были пересмотрены.
- **Предварительный просмотр ссылок** позволяет вставлять ссылки в сообщения, для которых Outlook в Интернете автоматически создает подробный эскиз веб-страниц, чтобы получатели могли взглянуть на их содержимое еще до открытия. Поддерживаются также ссылки на видео.
- **Встроенный видеопроигрыватель** экономит время пользователей, не убирая видео из контекста разговора. После вставки URL-адреса видео автоматически отображается его эскиз.

- **Закрепление и флажки** позволяют хранить важные сообщения в верхней части папки "Входящие" (закрепление) и помечать другие для отслеживания (флажки). Закрепление теперь можно выполнять на уровне папок — отличное решение тех, кто использует папки для упорядочения почты. Быстро находите помеченные элементы и управляйте ими с помощью фильтров в папке "Входящие" или нового модуля "Задачи", который доступен в средстве запуска приложений.

- **Улучшение производительности** большинства функций Outlook в Интернете, в том числе создания событий календаря, создания и загрузки сообщений в области чтения, всплывающих окон, поиска, запуска и переключения папок.

- **Новая область действий Outlook в Интернете** позволяет быстро выбрать наиболее часто используемые действия (например, "Создать", "Ответить всем" и "Удалить"). Кроме того, добавлены новые действия, включая "Архивировать", "Очистить" и "Отменить".

Протокол MAPI/HTTP

MAPI over HTTP — это протокол, используемый по умолчанию службой Outlook для связи с сервером Exchange. Протокол MAPI over HTTP повышает надежность и стабильность подключений Outlook и Exchange путем перемещения транспортного уровня в стандартную модель HTTP. Это обеспечивает большую видимость ошибок транспорта и улучшенные возможности восстановления. Дополнительные возможности включают поддержку явной функции приостановки и возобновления, благодаря чему поддерживаемые клиенты могут менять сети или выходить из режима гибернации, поддерживая тот же контекст сервера.

Примечание. Протокол MAPI/HTTP невозможно включить для организации, если выполняются оба следующих условия:

- Вы устанавливаете Exchange 2019 в организации, в которой уже установлены серверы Exchange 2013.

- Протокол MAPI/HTTP не был включен в Exchange 2013.

Хотя MAPI over HTTP теперь используется как стандартный протокол связи между Outlook и Exchange, клиенты, которые не поддерживают его, переводятся на мобильный Outlook (протокол RPC over HTTP).

Дополнительные сведения см. в статье MAPI/HTTP в Exchange Server.

Совместная работа над документами

В Exchange 2019 и SharePoint Server 2019 пользователи Outlook в Интернете могут связывать документы, хранящиеся в OneDrive для бизнеса на локальном сервере SharePoint, и предоставлять доступ к ним, вместо того чтобы вкладывать файлы в сообщения. Пользователи в локальной среде могут совместно работать над файлами аналогичным образом.

Дополнительные сведения о SharePoint Server 2019 см. в статье Новые и улучшенные функции в SharePoint Server 2019.

Когда пользователь Exchange 2019 получает файл Word, Excel или PowerPoint во вложении электронной почты, а файл хранится в OneDrive для бизнеса или локальной среде SharePoint, пользователь сможет просматривать и редактировать этот файл в Outlook в Интернете вместе с сообщением. Для этого вам потребуется отдельный компьютер в локальной организации, на котором работает Office Online Server. Дополнительные сведения см. в статье Установка Office Online Server в организации Exchange.

Кроме того, в Exchange 2019 также добавлены следующие улучшения для совместной работы с документами:

- Сохранение файлов в OneDrive для бизнеса.
- Отправка файла в OneDrive для бизнеса.
- В списки последних использованных документов вносятся файлы, хранящиеся как локально, так и в Интернете.

Гибридная конфигурация Microsoft 365 или Office 365

Мастер гибридной конфигурации, который использовался в Exchange 2013, становится облачным приложением. При выборе настройки гибридного развертывания в Exchange 2019 вам будет предложено скачать и установить мастер как небольшое приложение. Мастер будет работать так же, как и в предыдущих версиях Exchange, но с некоторыми преимуществами:

- мастер можно быстро обновить для поддержки изменений в службе Microsoft 365 или Office 365;
- мастер может обновляться с учетом обнаруженных проблем при попытке пользователей настроить гибридное развертывание;
- улучшены возможности устранения неполадок и диагностики для решения проблем при запуске мастера;

- все будут использовать один и тот же мастер для настройки гибридного развертывания с Exchange 2013 или более поздних версий.

Помимо улучшений мастера гибридной конфигурации, гибридное развертывание с несколькими лесами упрощается с помощью Azure Active Directory Connect (AADConnect). AADConnect включает агенты управления, которые значительно упрощают синхронизацию нескольких локальных лесов Active Directory с одним клиентом Microsoft 365 или Office 365. Дополнительные сведения о AADConnect см. в статье Что такое гибридное удостоверение в Azure Active Directory?

Клиенты Exchange ActiveSync легко перенаправляются в Microsoft 365 или Office 365 при перемещении почтового ящика пользователя в Exchange Online. Для этого клиенты ActiveSync должны поддерживать перенаправление HTTP 451. При перенаправлении клиента его профиль на устройстве обновляется URL-адресом службы Exchange Online. Это означает, что клиент больше не будет пытаться установить подключение к локальному серверу Exchange при попытке найти почтовый ящик.

Политика обмена сообщениями и соответствие требованиям

В Exchange 2019 существует несколько новых и обновленных функций, связанных с политикой обмена сообщениями и соответствием требованиям.

Защита от потери данных

Чтобы соответствовать стандартам ведения коммерческой деятельности и отраслевым нормативным требованиям, организациям необходимо защищать конфиденциальные данные и предотвращать их случайное раскрытие. Вот примеры конфиденциальных данных, которые не должны попасть за пределы вашей организации: номера кредитных карт, номера социального страхования, медицинские карты, а также другие личные сведения. С помощью политики защиты от потери данных и правил потока обработки почты (также известных как правила транспорта) в Exchange 2019 теперь можно определять, отслеживать и защищать 80 различных типов конфиденциальной информации с помощью новых условий и действий:

- С помощью нового условия **Любое вложение имеет эти свойства, включая любые из этих слов** правила потока обработки почты могут сопоставлять сообщения, для которых указанное свойство вложенного документа Office содержит определенные слова. Это условие упрощает интеграцию правил

потока обработки почты Exchange и политик защиты от потери данных с SharePoint, Windows Server 2012 инфраструктурой классификации файлов R2 (FCI) или сторонней системой классификации.

- С помощью нового действия **Уведомить получателя с помощью сообщения** правило потока обработки почты может отправить получателю уведомление с указанным вами текстом. Например, вы можете уведомить получателя, что сообщение было отклонено правилом потока обработки почты или помечено как нежелательное и будет доставлено в папку нежелательной почты.

- Действие **Создать отчет об инциденте и отправить его** обновлено, чтобы можно было уведомить нескольких получателей, указав групповой адрес в качестве получателя.

Дополнительные сведения о защите от потери данных см. в статье Защита от потери данных в Exchange Server.

Архивация, хранение и обнаружение электронных данных на месте

Exchange 2019 включает следующие улучшения для архивации, хранения и обнаружения электронных данных на месте, которые помогут организациям обеспечить соответствие требованиям:

- **Поддержка общедоступных папок для обнаружения электронных данных In-Place и удержания In-Place**. Exchange 2019 интегрирует общедоступные папки в рабочий процесс In-Place обнаружения электронных данных и удержания. You can use In-Place eDiscovery to search public folders in your organization, and you can put an In-Place Hold on public folders. And similar to placing a mailbox on hold, you can place a query-based and a time-based hold on public folders. Currently, you can only search and place a hold on all public folders. In later releases, you'll be able to choose specific public folders to search and place on hold. Дополнительные сведения см. в статье Поиск и удержание общедоступных папок с помощью In-Place обнаружения электронных данных.

- **Поиск соответствия требованиям**. Поиск по соответствию — это новое средство поиска электронных данных в Exchange 2019 с новыми улучшенными возможностями масштабирования и производительности. Его можно использовать для поиска очень большого количества почтовых ящиков в одном поиске. На самом деле, нет ограничений на количество почтовых ящиков, которые можно включить в один поиск, поэтому вы можете выполнять поиск по всем почтовым ящикам в вашей организации

одновременно. Также нет ограничений на количество поисковых запросов, которые могут выполняться одновременно. Для In-Place обнаружения электронных данных в Exchange 2019 ограничения такие же, как и в Exchange 2013: вы можете выполнять поиск до 10 000 почтовых ящиков в одном поиске, а ваша организация может одновременно выполнять не более двух In-Place поиска eDiscovery.

В Exchange 2019 поиск соответствия доступен только с помощью командной консоли Exchange. Сведения об использовании командлетов поиска соответствий требованиям см. в следующих статьях:

- Get-ComplianceSearch
- New-ComplianceSearch
- Remove-ComplianceSearch
- Set-ComplianceSearch
- Start-ComplianceSearch
- Stop-ComplianceSearch

> ⓘ **Примечание**
>
> Чтобы получить доступ к командлетам поиска соответствий требованиям, администратору или менеджеру по обнаружению электронных данных должна быть назначена роль управления поиском в почтовых ящиках или он должен быть членом группы ролей управления обнаружением.

Дополнительные сведения см. в статье Политика обмена сообщениями и соответствие требованиям в Exchange Server.

Улучшения производительности и масштабируемости

В Exchange 2019 была переработана архитектура поиска. Ранее поиск был синхронной операцией, которая не была очень отказоустойчивой. Новая архитектура является асинхронной и децентрализованной. Он распределяет работу между несколькими серверами и продолжает повторять повторные попытки, если какие-либо серверы слишком заняты. Это означает, что мы можем возвращать результаты более надежно и быстрее.

Еще одним преимуществом новой архитектуры является улучшение масштабируемости поиска. Количество почтовых ящиков, которые можно выполнить одновременно с помощью консоли, увеличилось с 5 до 10 тыс. для почтовых ящиков и архивных почтовых ящиков, что позволяет одновременно выполнять поиск в общей сложности 20 тысяч почтовых ящиков.

Возможности, поддержка которых прекращена в Exchange Server

Статья • 04.04.2023

В этом разделе рассказывается о компонентах, возможностях и функциях, которые были удалены, заменены или более не поддерживаются в Exchange 2019.

Функции Exchange 2016, более не поддерживаемые в Exchange 2019

В этом разделе перечислены функции Exchange 2016, которые больше недоступны в Exchange 2019.

Архитектура

Возможность	Замечания и изменения
Единая система обмена сообщениями	Единая система обмена сообщениями удалена из Exchange 2019. Рекомендуется, чтобы организации Exchange 2019 перешли на облачную голосовую почту Skype для бизнеса.

Функции Exchange 2013, более не поддерживаемые в Exchange 2019

В этом разделе перечислены функции Exchange 2013, которые больше недоступны в Exchange 2019.

Архитектура

Возможность	Замечания и изменения
Единая система обмена сообщениями	Единая система обмена сообщениями удалена из Exchange 2019. Рекомендуется, чтобы организации Exchange 2019 перешли на облачную голосовую почту Skype для бизнеса.

Возможность	Замечания и изменения
Роль сервера клиентского доступа	Роль сервера клиентского доступа заменена службами клиентского доступа, которые работают в роли сервера почтовых ящиков. Роль сервера почтовых ящиков теперь выполняет все функции, которые были ранее включены в роль сервера клиентского доступа. Дополнительные сведения о новой роли сервера почтовых ящиков см. в разделе архитектура Exchange Server.
Библиотека MAPI/CDO	Библиотека MAPI/CDO заменена веб-службами Exchange (EWS), Exchange ActiveSync (EAS) и API REST*. Если приложение использует библиотеку MAPI/CDO, ему необходимо перейти на EWS, EAS или REST API для взаимодействия с Exchange 2019.

* REST API будут включены в будущий выпуск Exchange 2019.

Функции, сокращенные в Exchange 2019

В Exchange 2019 указанные ниже функции сокращаются и могут быть исключены из будущих версий Exchange.

- Сторонние API-интерфейсы репликации.
- Протокол RPC через HTTP.
- Поддержка точек административного доступа к отказоустойчивым кластерам группой обеспечения доступности баз данных.

Обновления для Exchange Server

Статья • 12.02.2024

Накопительные пакеты обновлений для Exchange, устраняющие проблемы, о которых сообщают клиенты, выпускаются ежеквартально. Накопительные пакеты обновлений иногда также добавляют новые функциональные возможности.

Важные обновления продуктов — это пакеты, касающиеся бюллетеней по безопасности (Майкрософт) или содержащие изменения в определениях часовых поясов. При основной поддержке важные обновления продукта выпускаются ежемесячно по мере необходимости для последнего и предшествующего ему выпусков накопительных пакетов обновлений. При расширенной поддержке важные обновления продукта выпускаются ежемесячно по мере необходимости только для последнего выпуска накопительных пакетов обновлений.

Чтобы получить последнюю версию Exchange 2019, скачайте и установите накопительный пакет обновления 14 для Exchange Server 2019. Каждый накопительный пакет обновления содержит полную версию Exchange, а также обновления и изменения из всех предыдущих накопительных пакетов обновлений. При установке последнего пакета обновления для Exchange Server не нужно устанавливать Exchange RTM или выпущенный ранее накопительный пакет обновления.

В таблице ниже представлены ссылки на записи блога команды Exchange (сведения "Что нового"), посвященные текущему и другим накопительным пакетам обновлений Exchange 2019.

Развернуть таблицу

Версия	Запись блога
Exchange 2019 с накопительным пакетом обновления 14 (CU14)	Выпущено: накопительный Обновления H1 2024 для Exchange Server
Exchange 2019 CU13	Выпущено: накопительный Обновления H1 2023 для Exchange Server
Exchange 2019 CU12	Выпущено: накопительный пакет обновления H1 2022 для Exchange Server
Exchange 2019 с накопительным пакетом обновления 11 (CU11)	Ежеквартальные обновления для Exchange за сентябрь 2021 г.

Версия	Запись блога
Exchange 2019 с накопительным пакетом обновления 10 (CU10)	Ежеквартальные обновления для Exchange за июнь 2021 г.
Exchange 2019 с накопительным пакетом обновления 9 (CU9)	Ежеквартальные обновления для Exchange за март 2021 г.
Exchange 2019 с накопительным пакетом обновления 8 (CU8)	Ежеквартальные обновления для Exchange за декабрь 2020 г.
Exchange 2019 с накопительным пакетом обновления 7 (CU7)	Ежеквартальные обновления для Exchange за сентябрь 2020 г.
Exchange 2019 с накопительным пакетом обновления 6 (CU6)	Ежеквартальные обновления для Exchange за июнь 2020 г.
Exchange 2019 с накопительным пакетом обновления 5 (CU5)	Ежеквартальные обновления для Exchange за март 2020 г.
Exchange 2019 с накопительным пакетом обновления 4 (CU4)	Ежеквартальные обновления для Exchange за декабрь 2019 г.
Exchange 2019 с накопительным пакетом обновления 3 (CU3)	Ежеквартальные обновления для Exchange за сентябрь 2019 г.
Exchange 2019 с накопительным пакетом обновления 2 (CU2)	Ежеквартальные обновления для Exchange за июнь 2019 г.
Exchange 2019 с накопительным пакетом обновления 1 (CU1)	Ежеквартальные обновления для Exchange за февраль 2019 г.
Exchange 2019 RTM	Теперь доступен Exchange Server 2019

Дополнительные сведения о новых возможностях, которые станут вам доступны после обновления до Exchange 2019 с предыдущих версий Exchange, см. в статье Новые возможности Exchange Server.

- Сведения об установке последнего накопительного пакета обновления после его скачивания см. в статье Установка последнего накопительного пакета обновления для Exchange.
- Файлы для скачивания и обновления для других версий Exchange вы найдете в статье Обновления для Exchange Server: номера сборок и даты выпуска.

Доступность функций для Exchange Server

Статья • 04.04.2023

В следующей таблице перечислены основные Exchange Server функции, доступные в разных поддерживаемых версиях (применяются некоторые предостережения. Дополнительные сведения см. в сносках. Эта таблица может измениться без уведомления).

Возможность	Описание	Exchange Server 2013	Exchange Server 2016	Exchange Server 2019
Защита от нежелательной почты и вредоносных программ	Встроенная защита от нежелательной почты и вредоносных программ	Да	Да	Да
	Настройка политик защиты от нежелательной почты и вредоносных программ	Да через PowerShell	Да через PowerShell	Да через PowerShell
	Карантин — управление администраторами	Да	Да	Да
	Карантин — самостоятельное управление пользователями	Да	Да	Да
Клиенты и мобильные устройства	Outlook для Windows и Mac[1]	Да	Да	Да
	Outlook в Интернете [1]	Да	Да	Да
	Outlook для iOS и Android[1]	Да	Да	Да
	Надстройки Outlook и Outlook MAPI[3]	Да	Да	Да
	Веб-части	Да	Да	Да
	Exchange ActiveSync	Да	Да	Да
	SMTP, POP и IMAP	Да	Да	Да
	Поддержка приложений EWS	Да	Да	Да

Возможность	Описание	Exchange Server 2013	Exchange Server 2016	Exchange Server 2019
Установка и администрирование Exchange Online	Доступ к Центру администрирования Exchange	Да	Да	Да
	Удаленный доступ к Windows PowerShell	Да	Да	Да
	Политики ActiveSync для мобильных устройств	Да	Да	Да
	Отчеты об использовании	Да	Да	Да
Высокий уровень доступности и непрерывность бизнес-процессов	Группы доступности базы данных	Да	Да	Да
	Удаленный почтовый ящик и восстановление удаленных элементов	Да	Да	Да
	Восстановление отдельных элементов	Да	Да	Да
Взаимодействие, связь и совместимость	Skype для бизнеса присутствия в OWA и Outlook	Да	Да	Да
	Взаимодействие с SharePoint	Да	Да	Да
	Поддержка подключения EWS и ретранслятора SMTP	Да	Да	Да
Поток обработки почты	Гибридная электронная почта и настраиваемая маршрутизация исходящей почты	Да	Да	Да
	Secure messaging with a trusted partner	Да	Да	Да
	Условная маршрутизация почты и добавление в список безопасных для входящего трафика	Да	Да	Да

Возможность	Описание	Exchange Server 2013	Exchange Server 2016	Exchange Server 2019
Политика обработки сообщений и соответствие требованиям	Облачная архивация локальных почтовых ящиков[4]	Да	Да	Да
	Управление записями сообщений (MRM) и ведение журнала	Да	Да	Да
	Политики хранения, метки и теги хранения вручную	Да	Да	Да
	Шифрование неактивных данных (BitLocker)[5]	Да	Да	Да
	IRM с использованием Azure Information Protection	Да	Да	Да
	IRM с помощью Windows Server AD RMS[6]	Да	Да	Да
	S/MIME;	Да	Да	Да
	Хранение на месте и хранение для судебного разбирательства	Да	Да	Да
	Обнаружение электронных данных на месте	Да	Да	Да
	Правила транспорта[8]	Да	Да	Да
	Защита от потери данных[9,10]	Да	Да	Да
Разрешения	Разрешения на основе ролей, группы ролей и политики назначений	Да	Да	Да
Планирование и развертывание	Поддержка гибридного развертыванияIMAP, прямой передачи и поэтапной миграции	Да	Да	Да
Получатели	Оповещения о емкости, правила для папки "Входящие" и подсказки по почте	Да	Да	Да
	Папка "Несрочные"	Нет	Нет	Нет

Возможность	Описание	Exchange Server 2013	Exchange Server 2016	Exchange Server 2019
	Делегированный доступ	Да	Да	Да
	Подключенные учетные записи	Да	Да	Да
	Неактивные почтовые ящики	Нет	Нет	Нет
	Автономная адресная книга и политики	Да	Да	Да
	Иерархическая адресная книга	Да	Да	Да
	Списки адресов и глобальный список адресов	Да	Да	Да
	Универсальная карточка контакта, связывание контактов с социальными сетями и внешними контактами	Да	Да	Да
	Ответы вне офиса, управление конференц-залами и почтовые ящики ресурсов	Да	Да	Да
	Общий доступ к календарю	Да	Да	Да
Функции отчетов и средства устранения неполадок	Трассировка сообщений	Да	Нет	Да
	Отчеты аудита	Да	Да	Да
	Отчеты единой системы обмена сообщениями	Да	Да	Да
Общий доступ и совместная работа	Федеративный общий доступ (включая публикацию календаря)	Да	Да	Да
	Почтовые ящики сайта[11]	Да	Да	Да
	Общедоступные папки	Да	Да	Да
Службы голосовых сообщений	Голосовая почта	Да[12]	Нет	Нет
	Интеграция голосовой почты и стороннего факса	Да[12]	Нет	Нет

Возможность	Описание	Exchange Server 2013	Exchange Server 2016	Exchange Server 2019
	Взаимодействие с голосовой почтой сторонних производителей и интеграция Skype для бизнеса	Да[12]	Нет	Нет

[1] В таблице указано, работает ли клиент с сервером. Это не означает, что клиенты включены в покупку этих серверов.
[3] Некоторые сторонние веб-части и надстройки могут быть недоступны.
[4] Требуется подписка на Exchange Online Archiving для каждого пользователя локального почтового ящика с облачным архивом.
Шифрование диска BitLocker [5] поддерживается для Exchange Server, но администратор должен включить эту функцию.
[6] Windows Server AD RMS — это локальный сервер, который должен приобретаться и управляться отдельно, чтобы включить поддерживаемые функции IRM.
[7] Поддерживается для клиентов, работающих Exchange Server 2013 или более поздних версий локальных клиентов, которые приобретают Azure Information Protection. Шифрование сообщений Microsoft Purview требуется, чтобы локальные клиенты направляли электронную почту через Exchange Online либо с помощью Exchange Online Protection для фильтрации электронной почты, либо путем создания гибридного потока обработки почты.
[8] Правила транспорта состоят из гибких критериев, которые позволяют определять условия и исключения, а также действия, которые необходимо выполнить на основе критериев.
[9] Для Exchange 2013 для защиты от потери данных требуется клиентская лицензия Exchange Enterprise(CAL).
[10] Пользователям, работающим Exchange Server 2013 или более поздней версии, необходимо скачать и установить последнее накопительное обновление (CU) или непосредственно предыдущее накопительное обновление, чтобы получить доступ к подсказкам по отпечаткам документов и политикам в OWA и OWA для устройств.
[11] SharePoint Server необходимо развернуть в локальной организации Exchange.
[12] облачная голосовая почта работает с Exchange Online и Exchange 2019. См. статью Планирование службы облачная голосовая почта для локальных пользователей — гибридный Skype для бизнеса | Документация Майкрософт.

Сведения о Exchange Online см. в разделе Описание службы Exchange Online.

Номера сборок и даты выпуска Exchange Server

Статья • 15.08.2023

Вы можете использовать сведения в этой статье для проверки версии Microsoft Exchange Server в вашей организации.

Эта статья состоит из разделов, соответствующих основным выпускам Exchange. В каждом разделе перечислены номера сборок для каждого пакета обновления (SP), накопительного обновления (CU), обновления для системы безопасности (SU), обновления исправлений (HU) или накопительного пакета обновления (RU) конкретного выпуска Exchange.

Также включены ссылки для доступных скачиваемых файлов.

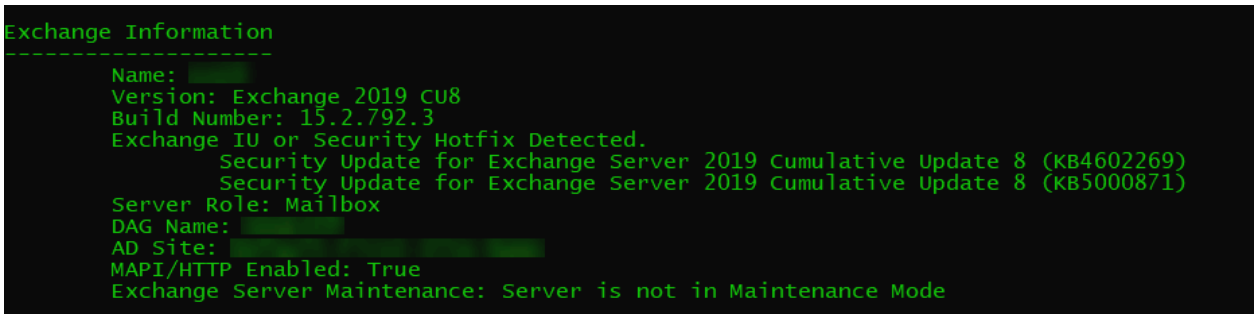
> **Примечание**
>
> Выпуски перечислены в порядке от последнего до самого раннего.
>
> Начиная с обновления безопасности (SU) за март 2021 г., мы также включаем номера сборок для обновлений безопасности.
>
> "RTM" означает "release to manufacturing", то есть окончательную первоначальную версию (первую версию продукта).

Просмотр номера сборки сервера на основе Exchange

В этом разделе описываются различные методы, которые можно использовать для просмотра номера сборки серверов, на которых запущен Exchange Server.

Вариант 1 (рекомендуемый)

Запустите сценарий Exchange HealthChecker и проверка номер сборки.



Вариант 2

Откройте командную консоль Exchange и выполните следующую команду:

PowerShell

```
Get-Command Exsetup.exe | ForEach {$_.FileVersionInfo}
```

Вариант 3

Откройте командную консоль Exchange и выполните следующую команду:

PowerShell

```
Get-ExchangeServer | Format-List Name,Edition,AdminDisplayVersion
```

> ⓘ **Примечание**
>
> Этот параметр указывает только состояние накопительного обновления (CU) и не отражает установленное обновление для системы безопасности (SU) или исправление (HU). Чтобы подтвердить обновления, используйте вариант 1 или 2.

Exchange Server 2019

В таблице этого раздела приведены номера сборок и общие даты выпуска всех версий Microsoft Exchange Server 2019.

⛶ **Развернуть таблицу**

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Exchange Server 2019 cu14 Nov24SUv2	27 ноября 2024 г.	15.2.1544.14	15.02.1544.014
Exchange Server 2019 CU14 Nov24SU	12 ноября 2024 г.	15.2.1544.13	15.02.1544.013
Exchange Server 2019 CU14 Apr24HU	23 апреля 2024 г.	15.2.1544.11	15.02.1544.011
Exchange Server 2019 CU14 Mar24SU	12 марта 2024 г.	15.2.1544.9	15.02.1544.009
Exchange Server 2019 CU14 (2024H1)	13 февраля 2024 г.	15.2.1544.4	15.02.1544.004
Exchange Server 2019 CU13 Nov24SUv2	27 ноября 2024 г.	15.2.1258.39	15.02.1258.039
Exchange Server 2019 cu13 Nov24SU	12 ноября 2024 г.	15.2.1258.38	15.02.1258.038
Exchange Server 2019 cu13 Apr24HU	23 апреля 2024 г.	15.2.1258.34	15.02.1258.034
Exchange Server 2019 CU13 Mar24SU	12 марта 2024 г.	15.2.1258.32	15.02.1258.032
Exchange Server 2019 CU13 Nov23SU	14 ноября 2023 г.	15.2.1258.28	15.02.1258.028
Exchange Server 2019 CU13 oct23SU	10 октября 2023 г.	15.2.1258.27	15.02.1258.027
Exchange Server 2019 cu13 aug23SUv2	15 августа 2023 г.	15.2.1258.25	15.02.1258.025
Exchange Server 2019 CU13 aug23SU	8 августа 2023 г.	15.2.1258.23	15.02.1258.023
Exchange Server 2019 CU13 Jun23SU	13 июня 2023 г.	15.2.1258.16	15.02.1258.016
Exchange Server 2019 CU13 (2023H1)	3 мая 2023 г.	15.2.1258.12	15.02.1258.012
Exchange Server 2019 CU12 Nov23SU	14 ноября 2023 г.	15.2.1118.40	15.02.1118.040

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Exchange Server 2019 CU12 oct23SU	10 октября 2023 г.	15.2.1118.39	15.02.1118.039
Exchange Server 2019 cu12 aug23SUv2	15 августа 2023 г.	15.2.1118.37	15.02.1118.037
Exchange Server 2019 CU12 aug23SU	8 августа 2023 г.	15.2.1118.36	15.02.1118.036
Exchange Server 2019 CU12 Jun23SU	13 июня 2023 г.	15.2.1118.30	15.02.1118.030
Exchange Server 2019 CU12 mar23SU	14 марта 2023 г.	15.2.1118.26	15.02.1118.026
Exchange Server 2019 CU12 Feb23SU	14 февраля 2023 г.	15.2.1118.25	15.02.1118.025
Exchange Server 2019 CU12 Jan23SU	10 января 2023 г.	15.2.1118.21	15.02.1118.021
Exchange Server 2019 CU12 Nov22SU	8 ноября 2022 г.	15.2.1118.20	15.02.1118.020
Exchange Server 2019 CU12 oct22SU	11 октября 2022 г.	15.2.1118.15	15.02.1118.015
Exchange Server 2019 CU12 Aug22SU	9 августа 2022 г.	15.2.1118.12	15.02.1118.012
Exchange Server 2019 CU12 May22SU	10 мая 2022 г.	15.2.1118.9	15.02.1118.009
Сервер Exchange Server 2019 CU12 (2022H1)	20 апреля 2022 г.	15.2.1118.7	15.02.1118.007
Exchange Server 2019 CU11 Mar23SU	14 марта 2023 г.	15.2.986.42	15.02.0986.042
Exchange Server 2019 CU11 Feb23SU	14 февраля 2023 г.	15.2.986.41	15.02.0986.041
Exchange Server 2019 CU11 Jan23SU	10 января 2023 г.	15.2.986.37	15.02.0986.037
Exchange Server 2019 CU11 Nov22SU	8 ноября 2022 г.	15.2.986.36	15.02.0986.036

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Exchange Server 2019 CU11 oct22SU	11 октября 2022 г.	15.2.986.30	15.02.0986.030
Exchange Server 2019 CU11 Aug22SU	9 августа 2022 г.	15.2.986.29	15.02.0986.029
Exchange Server 2019 CU11 May22SU	10 мая 2022 г.	15.2.986.26	15.02.0986.026
Exchange Server 2019 CU11 Mar22SU	8 марта 2022 г.	15.2.986.22	15.02.0986.022
Exchange Server 2019 CU11 Jan22SU	11 января 2022 г.	15.2.986.15	15.02.0986.015
Exchange Server 2019 CU11 Nov21SU	9 ноября 2021 г.	15.2.986.14	15.02.0986.014
Exchange Server 2019 CU11 Oct21SU	12 октября 2021 г.	15.2.986.9	15.02.0986.009
Exchange Server 2019 CU11	28 сентября 2021 г.	15.2.986.5	15.02.0986.005
Exchange Server 2019 CU10 Mar22SU	8 марта 2022 г.	15.2.922.27	15.02.0922.027
Exchange Server 2019 CU10 Jan22SU	11 января 2022 г.	15.2.922.20	15.02.0922.020
Exchange Server 2019 CU10 Nov21SU	9 ноября 2021 г.	15.2.922.19	15.02.0922.019
Exchange Server 2019 CU10 Oct21SU	12 октября 2021 г.	15.2.922.14	15.02.0922.014
Exchange Server 2019 CU10 Jul21SU	13 июля 2021 г.	15.2.922.13	15.02.0922.013
Exchange Server 2019 CU10	29 июня 2021 г.	15.2.922.7	15.02.0922.007
Exchange Server 2019 CU9 Jul21SU	13 июля 2021 г.	15.2.858.15	15.02.0858.015
Exchange Server 2019 CU9 May21SU	11 мая 2021 г.	15.2.858.12	15.02.0858.012
Exchange Server 2019 CU9 Apr21SU	13 апреля 2021 г.	15.2.858.10	15.02.0858.010

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Exchange Server 2019 CU9	16 марта 2021 г.	15.2.858.5	15.02.0858.005
Exchange Server 2019 CU8 May21SU	11 мая 2021 г.	15.2.792.15	15.02.0792.015
Exchange Server 2019 CU8 Apr21SU	13 апреля 2021 г.	15.2.792.13	15.02.0792.013
Exchange Server 2019 CU8 Mar21SU	2 марта 2021 г.	15.2.792.10	15.02.0792.010
Exchange Server 2019 CU8	15 декабря 2020 г.	15.2.792.3	15.02.0792.003
Exchange Server 2019 CU7 Mar21SU	2 марта 2021 г.	15.2.721.13	15.02.0721.013
Exchange Server 2019 CU7	15 сентября 2020 г.	15.2.721.2	15.02.0721.002
Exchange Server 2019 CU6 Mar21SU	2 марта 2021 г.	15.2.659.12	15.02.0659.012
Exchange Server 2019 CU6	16 июня 2020 г.	15.2.659.4	15.02.0659.004
Exchange Server 2019 CU5 Mar21SU	2 марта 2021 г.	15.2.595.8	15.02.0595.008
Exchange Server 2019 CU5	17 марта 2020 г.	15.2.595.3	15.02.0595.003
Exchange Server 2019 CU4 Mar21SU	2 марта 2021 г.	15.2.529.13	15.02.0529.013
Exchange Server 2019 CU4	17 декабря 2019 г.	15.2.529.5	15.02.0529.005
Exchange Server 2019 CU3 Mar21SU	2 марта 2021 г.	15.2.464.15	15.02.0464.015
Exchange Server 2019 CU3	17 сентября 2019 г.	15.2.464.5	15.02.0464.005
Exchange Server 2019 CU2 Mar21SU	2 марта 2021 г.	15.2.397.11	15.02.0397.011
Сервер Exchange Server 2019 CU2	18 июня 2019 г.	15.2.397.3	15.02.0397.003

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Exchange Server 2019 CU1 Mar21SU	2 марта 2021 г.	15.2.330.11	15.02.0330.011
Сервер Exchange Server 2019 CU1	12 февраля 2019 г.	15.2.330.5	15.02.0330.005
Exchange Server 2019 RTM Mar21SU	2 марта 2021 г.	15.2.221.18	15.02.0221.018
Сервер Exchange Server 2019 RTM	22 октября 2018 г.	15.2.221.12	15.02.0221.012
Предварительная версия Exchange Server 2019	24 июля 2018 г.	15.2.196.0	15.02.0196.000

Exchange Server 2016

В таблице этого раздела приведены номера сборок и общие даты выпуска всех версий Microsoft Exchange Server 2016.

Развернуть таблицу

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Exchange Server 2016 cu23 Nov24SUv2	27 ноября 2024 г.	15.1.2507.44	15.01.2507.044
Exchange Server 2016 CU23 Nov24SU	12 ноября 2024 г.	15.1.2507.43	15.01.2507.043
Exchange Server 2016 cu23 Apr24HU	23 апреля 2024 г.	15.1.2507.39	15.01.2507.039
Exchange Server 2016 CU23 Mar24SU	12 марта 2024 г.	15.1.2507.37	15.01.2507.037
Exchange Server 2016 CU23 Nov23SU	14 ноября 2023 г.	15.1.2507.35	15.01.2507.035
Exchange Server 2016 CU23 Oct23SU	10 октября 2023 г.	15.1.2507.34	15.01.2507.034

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Exchange Server 2016 cu23 aug23SUv2	15 августа 2023 г.	15.1.2507.32	15.01.2507.032
Exchange Server 2016 CU23 aug23SU	8 августа 2023 г.	15.1.2507.31	15.01.2507.031
Exchange Server 2016 CU23 Jun23SU	13 июня 2023 г.	15.1.2507.27	15.01.2507.027
Exchange Server 2016 CU23 Mar23SU	14 марта 2023 г.	15.1.2507.23	15.01.2507.023
Exchange Server 2016 CU23 Feb23SU	14 февраля 2023 г.	15.1.2507.21	15.01.2507.021
Exchange Server 2016 CU23 Jan23SU	10 января 2023 г.	15.1.2507.17	15.01.2507.017
Exchange Server 2016 CU23 Nov22SU	8 ноября 2022 г.	15.1.2507.16	15.01.2507.016
Exchange Server 2016 CU23 oct22SU	11 октября 2022 г.	15.1.2507.13	15.01.2507.013
Exchange Server 2016 CU23 Aug22SU	9 августа 2022 г.	15.1.2507.12	15.01.2507.012
Exchange Server 2016 CU23 May22SU	10 мая 2022 г.	15.1.2507.9.	15.01.2507.009.
Сервер Exchange Server 2016 CU23 (2022H1)	20 апреля 2022 г.	15.1.2507.6.	15.01.2507.006.
Exchange Server 2016 CU22 NOV22SU	8 ноября 2022 г.	15.1.2375.37	15.01.2375.037
Exchange Server 2016 CU22 Oct22SU	11 октября 2022 г.	15.1.2375.32	15.01.2375.032
Exchange Server 2016 CU22 Aug22SU	9 августа 2022 г.	15.1.2375.31	15.01.2375.031
Exchange Server 2016 CU22 May22SU	10 мая 2022 г.	15.1.2375.28.	15.01.2375.028.
Exchange Server 2016 CU22 Mar22SU	8 марта 2022 г.	15.1.2375.24	15.01.2375.024

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Exchange Server 2016 CU22 Jan22SU	11 января 2022 г.	15.1.2375.18	15.01.2375.018
Exchange Server 2016 CU22 Nov21SU	9 ноября 2021 г.	15.1.2375.17	15.01.2375.017
Exchange Server 2016 CU22 Oct21SU	12 октября 2021 г.	15.1.2375.12	15.01.2375.012
Exchange Server 2016 CU22	28 сентября 2021 г.	15.1.2375.7	15.01.2375.007
Exchange Server 2016 CU21 Mar22SU	8 марта 2022 г.	15.1.2308.27	15.01.2308.027
Exchange Server 2016 CU21 Jan22SU	11 января 2022 г.	15.1.2308.21	15.01.2308.021
Exchange Server 2016 CU21 Nov21SU	9 ноября 2021 г.	15.1.2308.20	15.01.2308.020
Exchange Server 2016 CU21 Oct21SU	12 октября 2021 г.	15.1.2308.15	15.01.2308.015
Exchange Server 2016 CU21 Jul21SU	13 июля 2021 г.	15.1.2308.14	15.01.2308.014
Exchange Server 2016 CU21	29 июня 2021 г.	15.1.2308.8	15.01.2308.008
Exchange Server 2016 CU20 Jul21SU	13 июля 2021 г.	15.1.2242.12	15.01.2242.012
Exchange Server 2016 CU20 May21SU	11 мая 2021 г.	15.1.2242.10	15.01.2242.010
Exchange Server 2016 CU20 Apr21SU	13 апреля 2021 г.	15.1.2242.8	15.01.2242.008
Exchange Server 2016 CU20	16 марта 2021 г.	15.1.2242.4	15.01.2242.004
Exchange Server 2016 CU19 May21SU	11 мая 2021 г.	15.1.2176.14	15.01.2176.014
Exchange Server 2016 CU19 Apr21SU	13 апреля 2021 г.	15.1.2176.12	15.01.2176.012

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Exchange Server 2016 CU19 Mar21SU	2 марта 2021 г.	15.1.2176.9	15.01.2176.009
Exchange Server 2016 CU19	15 декабря 2020 г.	15.1.2176.2	15.01.2176.002
Exchange Server 2016 CU18 Mar21SU	2 марта 2021 г.	15.1.2106.13	15.01.2106.013
Exchange Server 2016 CU18	15 сентября 2020 г.	15.1.2106.2	15.01.2106.002
Exchange Server 2016 CU17 Mar21SU	2 марта 2021 г.	15.1.2044.13	15.01.2044.013
Exchange Server 2016 CU17	16 июня 2020 г.	15.1.2044.4	15.01.2044.004
Exchange Server 2016 CU16 Mar21SU	2 марта 2021 г.	15.1.1979.8	15.01.1979.008
Exchange Server 2016 CU16	17 марта 2020 г.	15.1.1979.3	15.01.1979.003
Exchange Server 2016 CU15 Mar21SU	2 марта 2021 г.	15.1.1913.12	15.01.1913.012
Exchange Server 2016 CU15	17 декабря 2019 г.	15.1.1913.5	15.01.1913.005
Exchange Server 2016 CU14 Mar21SU	2 марта 2021 г.	15.1.1847.12	15.01.1847.012
Exchange Server 2016 CU14	17 сентября 2019 г.	15.1.1847.3	15.01.1847.003
Exchange Server 2016 CU13 Mar21SU	2 марта 2021 г.	15.1.1779.8	15.01.1779.008
Сервер Exchange Server 2016 CU13	18 июня 2019 г.	15.1.1779.2	15.01.1779.002
Exchange Server 2016 CU12 Mar21SU	2 марта 2021 г.	15.1.1713.10	15.01.1713.010
Сервер Exchange Server 2016 CU12	12 февраля 2019 г.	15.1.1713.5	15.01.1713.005

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Exchange Server 2016 CU11 Mar21SU	2 марта 2021 г.	15.1.1591.18	15.01.1591.018
Сервер Exchange Server 2016 CU11	16 октября 2018 г.	15.1.1591.10	15.01.1591.010
Exchange Server 2016 CU10 Mar21SU	2 марта 2021 г.	15.1.1531.12	15.01.1531.012
Сервер Exchange Server 2016 CU10	19 июня 2018 г.	15.1.1531.3	15.01.1531.003
Exchange Server 2016 CU9 Mar21SU	2 марта 2021 г.	15.1.1466.16	15.01.1466.016
Exchange Server 2016 CU9	20 марта 2018 г.	15.1.1466.3	15.01.1466.003
Exchange Server 2016 CU8 Mar21SU	2 марта 2021 г.	15.1.1415.10	15.01.1415.010
Exchange Server 2016 CU8	19 декабря 2017 г.	15.1.1415.2	15.01.1415.002
Exchange Server 2016 CU7	19 сентября 2017 г.	15.1.1261.35	15.01.1261.035
Exchange Server 2016 CU6	27 июня 2017 г.	15.1.1034.26	15.01.1034.026
Exchange Server 2016 CU5	21 марта 2017 г.	15.1.845.34	15.01.0845.034
Exchange Server 2016 CU4	13 декабря 2016 г.	15.1.669.32	15.01.0669.032
Exchange Server 2016 CU3	20 сентября 2016 г.	15.1.544.27	15.01.0544.027
Exchange Server 2016 CU2	21 июня 2016 г.	15.1.466.34	15.01.0466.034
Exchange Server 2016 CU1	15 марта 2016 г.	15.1.396.30	15.01.0396.030
Exchange Server 2016 RTM	1 октября 2015 г.	15.1.225.42	15.01.0225.042

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Предварительная версия Exchange Server 2016	22 июля 2015 г.	15.1.225.16	15.01.0225.016

Exchange Server 2013

В таблице этого раздела приведены номера сборок и общие даты выпуска всех версий Microsoft Exchange Server 2013.

Развернуть таблицу

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Exchange Server 2013 CU23 Mar23SU	14 марта 2023 г.	15.0.1497.48	15.00.1497.048
Exchange Server 2013 CU23 Feb23SU	14 февраля 2023 г.	15.0.1497.47	15.00.1497.047
Exchange Server 2013 CU23 Jan23SU	10 января 2023 г.	15.0.1497.45	15.00.1497.045
Exchange Server 2013 CU23 Nov22SU	8 ноября 2022 г.	15.0.1497.44	15.00.1497.044
Exchange Server 2013 CU23 oct22SU	11 октября 2022 г.	15.0.1497.42	15.00.1497.042
Exchange Server 2013 CU23 Aug22SU	9 августа 2022 г.	15.0.1497.40	15.00.1497.040
Exchange Server 2013 CU23 May22SU	10 мая 2022 г.	15.0.1497.36.	15.00.1497.036.
Exchange Server 2013 CU23 Mar22SU	8 марта 2022 г.	15.0.1497.33	15.00.1497.033
Exchange Server 2013 CU23 Jan22SU	11 января 2022 г.	15.0.1497.28	15.00.1497.028
Exchange Server 2013 CU23 Nov21SU	9 ноября 2021 г.	15.0.1497.26	15.00.1497.026

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Exchange Server 2013 CU23 Oct21SU	12 октября 2021 г.	15.0.1497.24	15.00.1497.024
Exchange Server 2013 CU23 Jul21SU	13 июля 2021 г.	15.0.1497.23	15.00.1497.023
Exchange Server 2013 CU23 May21SU	11 мая 2021 г.	15.0.1497.18	15.00.1497.018
Exchange Server 2013 CU23 Apr21SU	13 апреля 2021 г.	15.0.1497.15	15.00.1497.015
Exchange Server 2013 CU23 Mar21SU	2 марта 2021 г.	15.0.1497.12	15.00.1497.012
Exchange Server 2013 CU23	18 июня 2019 г.	15.0.1497.2	15.00.1497.002
Exchange Server 2013 CU22 Mar21SU	2 марта 2021 г.	15.0.1473.6	15.00.1473.006
Exchange Server 2013 CU22	12 февраля 2019 г.	15.0.1473.3	15.00.1473.003
Exchange Server 2013 CU21 Mar21SU	2 марта 2021 г.	15.0.1395.12	15.00.1395.012
Exchange Server 2013 CU21	19 июня 2018 г.	15.0.1395.4	15.00.1395.004
Exchange Server 2013 CU20	20 марта 2018 г.	15.0.1367.3	15.00.1367.003
Exchange Server 2013 CU19	19 декабря 2017 г.	15.0.1365.1	15.00.1365.001
Exchange Server 2013 CU18	19 сентября 2017 г.	15.0.1347.2	15.00.1347.002
Exchange Server 2013 CU17	27 июня 2017 г.	15.0.1320.4	15.00.1320.004
Exchange Server 2013 CU16	21 марта 2017 г.	15.0.1293.2	15.00.1293.002
Exchange Server 2013 CU15	13 декабря 2016 г.	15.0.1263.5	15.00.1263.005
Exchange Server 2013 CU14	20 сентября 2016 г.	15.0.1236.3	15.00.1236.003
Exchange Server 2013 CU13	21 июня 2016 г.	15.0.1210.3	15.00.1210.003

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Exchange Server 2013 CU12	15 марта 2016 г.	15.0.1178.4	15.00.1178.004
Exchange Server 2013 CU11	15 декабря 2015 г.	15.0.1156.6	15.00.1156.006
Exchange Server 2013 CU10	15 сентября 2015 г.	15.0.1130.7	15.00.1130.007
Exchange Server 2013 CU9	17 июня 2015 г.	15.0.1104.5	15.00.1104.005
Exchange Server 2013 CU8	17 марта 2015 г.	15.0.1076.9	15.00.1076.009
Exchange Server 2013 CU7	9 декабря 2014 г.	15.0.1044.25	15.00.1044.025
Exchange Server 2013 CU6	26 августа 2014 г.	15.0.995.29	15.00.0995.029
Exchange Server 2013 CU5	27 мая 2014 г.	15.0.913.22	15.00.0913.022
Exchange Server 2013 SP1 Mar21SU	2 марта 2021 г.	15.0.847.64	15.00.0847.064
Exchange Server 2013 SP1	25 февраля 2014 г.	15.0.847.32	15.00.0847.032
Exchange Server 2013 CU3	25 ноября 2013 г.	15.0.775.38	15.00.0775.038
Exchange Server 2013 CU2	9 июля 2013 г.	15.0.712.24	15.00.0712.024
Exchange Server 2013 CU1	2 апреля 2013 г.	15.0.620.29	15.00.0620.029
Exchange Server 2013 RTM	3 декабря 2012 г.	15.0.516.32	15.00.0516.032

Exchange Server 2010

В таблицах этого раздела приведены номера сборок и общие даты выпуска всех версий Microsoft Exchange Server 2010.

Номера сборок Exchange Server 2010 с пакетом обновления 3 (SP3)

Развернуть таблицу

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Накопительный пакет обновления 32 для Exchange Server 2010 SP3	2 марта 2021 г.	14.3.513.0	14.03.0513.000
Накопительный пакет обновления 31 для Exchange Server 2010 SP3	1 декабря 2020 г.	14.3.509.0	14.03.0509.000
Накопительный пакет обновления 30 для Exchange Server 2010 с пакетом обновления 3 (SP3)	11 февраля 2020 г.	14.3.496.0	14.03.0496.000
Накопительный пакет обновления 29 для Exchange Server 2010 SP3	9 июля 2019 г.	14.3.468.0	14.03.0468.000
Накопительный пакет обновления 28 для Exchange Server 2010 SP3	7 июня 2019 г.	14.3.461.1	14.03.0461.001
Накопительный пакет обновления 27 для Exchange Server 2010 SP3	9 апреля 2019 г.	14.3.452.0	14.03.0452.000
Набор исправлений 26 для Exchange Server 2010 с пакетом обновления 3 (SP3)	12 февраля 2019 г.	14.3.442.0	14.03.0442.000
Набор исправлений 25 для Exchange Server 2010 с пакетом обновления 3 (SP3)	8 января 2019 г.	14.3.435.0	14.03.0435.000
Набор исправлений 24 для Exchange Server 2010 с пакетом обновления 3 (SP3)	5 сентября 2018 г.	14.3.419.0	14.03.0419.000
Набор исправлений 23 для Exchange Server 2010 с пакетом обновления 3 (SP3)	13 августа 2018 г.	14.3.417.1	14.03.0417.001
Набор исправлений 22 для Exchange Server 2010 с пакетом обновления 3 (SP3)	19 июня 2018 г.	14.3.411.0	14.03.0411.000
Набор исправлений 21 для Exchange Server 2010 с пакетом обновления 3 (SP3)	7 мая 2018 г.	14.3.399.2	14.03.0399.002
Набор исправлений 20 для Exchange Server 2010 с пакетом обновления 3 (SP3)	5 марта 2018 г.	14.3.389.1	14.03.0389.001
Набор исправлений 19 для Exchange Server 2010 с пакетом обновления 3 (SP3)	19 декабря 2017 г.	14.3.382.0	14.03.0382.000
Набор исправлений 18 для Exchange Server 2010 с пакетом обновления 3 (SP3)	11 июля 2017 г.	14.3.361.1	14.03.0361.001

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Набор исправлений 17 для Exchange Server 2010 с пакетом обновления 3 (SP3)	21 марта 2017 г.	14.3.352.0	14.03.0352.000
Набор исправлений 16 для Exchange Server 2010 с пакетом обновления 3 (SP3)	13 декабря 2016 г.	14.3.336.0	14.03.0336.000
Набор исправлений 15 для Exchange Server 2010 с пакетом обновления 3 (SP3)	20 сентября 2016 г.	14.3.319.2	14.03.0319.002
Набор исправлений 14 для Exchange Server 2010 с пакетом обновления 3 (SP3)	21 июня 2016 г.	14.3.301.0	14.03.0301.000
Набор исправлений 13 для Exchange Server 2010 с пакетом обновления 3 (SP3)	15 марта 2016 г.	14.3.294.0	14.03.0294.000
Набор исправлений 12 для Exchange Server 2010 с пакетом обновления 3 (SP3)	15 декабря 2015 г.	14.3.279.2	14.03.0279.002
Набор исправлений 11 для Exchange Server 2010 с пакетом обновления 3 (SP3)	15 сентября 2015 г.	14.3.266.2	14.03.0266.002
Набор исправлений 10 для Exchange Server 2010 с пакетом обновления 3	17 июня 2015 г.	14.3.248.2	14.03.0248.002
Набор исправлений 9 для Exchange Server 2010 с пакетом обновления 3	17 марта 2015 г.	14.3.235.1	14.03.0235.001
Набор исправлений 8 версии 2 для Exchange Server 2010 с пакетом обновления 3	12 декабря 2014 г.	14.3.224.2	14.03.0224.002
Набор исправлений 8 версии 1 для Exchange Server 2010 с пакетом обновления 3 (заменен)	9 декабря 2014 г.	14.3.224.1	14.03.0224.001
Набор исправлений 7 для Exchange Server 2010 с пакетом обновления 3	26 августа 2014 г.	14.3.210.2	14.03.0210.002
Набор исправлений 6 для Exchange Server 2010 с пакетом обновления 3	27 мая 2014 г.	14.3.195.1	14.03.0195.001
Набор исправлений 5 для Exchange Server 2010 с пакетом обновления 3 (SP3)	24 февраля 2014 г.	14.3.181.6	14.03.0181.006
Набор исправлений 4 для Exchange Server 2010 с пакетом обновления 3	9 декабря 2013 г.	14.3.174.1	14.03.0174.001

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Набор исправлений 3 для Exchange Server 2010 с пакетом обновления 3 (SP3)	25 ноября 2013 г.	14.3.169.1	14.03.0169.001
Набор исправлений 2 для Exchange Server 2010 с пакетом обновления 3 (SP3)	8 августа 2013 г.	14.3.158.1	14.03.0158.001
Набор исправлений 1 для Exchange Server 2010 с пакетом обновления 3 (SP3)	29 мая 2013 г.	14.3.146.0	14.03.0146.000
Exchange Server 2010 SP3	12 февраля 2013 г.	14.3.123.4	14.03.0123.004

Номера сборок предыдущих версий Exchange Server 2010

Развернуть таблицу

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Набор исправлений 8 для Exchange Server 2010 с пакетом обновления 2 (SP2)	9 декабря 2013 г.	14.2.390.3	14.02.0390.003
Набор исправлений 7 для Exchange Server 2010 с пакетом обновления 2 (SP2)	8 августа 2013 г.	14.2.375.0	14.02.0375.000
Набор исправлений 6 для Exchange Server 2010 с пакетом обновления 2 (SP2)	12 февраля 2013 г.	14.2.342.3	14.02.0342.003
Набор исправлений 5 версии 2 для Exchange Server 2010 с пакетом обновления 2 (SP2)	10 декабря 2012 г.	14.2.328.10	14.02.0328.010
Набор исправлений 5 для Exchange Server 2010 с пакетом обновления 2 (SP2)	13 ноября 2012 г.	14.3.328.5	14.03.0328.005
Набор исправлений 4 версии 2 для Exchange Server 2010 с пакетом обновления 2 (SP2)	9 октября 2012 г.	14.2.318.4	14.02.0318.004
Набор исправлений 4 для Exchange Server 2010 с пакетом обновления 2 (SP2)	13 августа 2012 г.	14.2.318.2	14.02.0318.002

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Набор исправлений 3 для Exchange Server 2010 с пакетом обновления 2 (SP2)	29 мая 2012 г.	14.2.309.2	14.02.0309.002
Набор исправлений 2 для Exchange Server 2010 с пакетом обновления 2 (SP2)	16 апреля 2012 г.	14.2.298.4	14.02.0298.004
Набор исправлений 1 для Exchange Server 2010 с пакетом обновления 2 (SP2)	13 февраля 2012 г.	14.2.283.3	14.02.0283.003
Exchange Server 2010 SP2	4 декабря 2011 г.	14.2.247.5	14.02.0247.005
Набор исправлений 8 для Exchange Server 2010 с пакетом обновления 1 (SP1)	10 декабря 2012 г.	14.1.438.0	14.01.0438.000
Набор исправлений 7 версии 3 для Exchange Server 2010 с пакетом обновления 1 (SP1)	13 ноября 2012 г.	14.1.421.3	14.01.0421.003
Набор исправлений 7 версии 2 для Exchange Server 2010 с пакетом обновления 1 (SP1)	10 октября 2012 г.	14.1.421.2	14.01.0421.002
Набор исправлений 7 для Exchange Server 2010 с пакетом обновления 1 (SP1)	8 августа 2012 г.	14.1.421.0	14.01.0421.000
Набор исправлений 6 для Exchange Server 2010 с пакетом обновления 1 (SP1)	27 октября 2011 г.	14.1.355.2	14.01.0355.002
Набор исправлений 5 для Exchange Server 2010 с пакетом обновления 1 (SP1)	23 августа 2011 г.	14.1.339.1	14.01.0339.001
Набор исправлений 4 для Exchange Server 2010 с пакетом обновления 1 (SP1)	27 июля 2011 г.	14.1.323.6	14.01.0323.006
Набор исправлений 3 для Exchange Server 2010 с пакетом обновления 1 (SP1)	6 апреля 2011 г.	14.1.289.7	14.01.0289.007
Набор исправлений 2 для Exchange Server 2010 с пакетом обновления 1 (SP1)	9 декабря 2010 г.	14.1.270.1	14.01.0270.001
Набор исправлений 1 для Exchange Server 2010 с пакетом обновления 1 (SP1)	4 октября 2010 г.	14.1.255.2	14.01.0255.002
Exchange Server 2010 SP1	23 августа 2010 г.	14.1.218.15	14.01.0218.015

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Набор исправлений 5 для Exchange Server 2010	13 декабря 2010 г.	14.0.726.0	14.00.0726.000
Набор исправлений 4 для Exchange Server 2010	10 июня 2010 г.	14.0.702.1	14.00.0702.001
Набор исправлений 3 для Exchange Server 2010	13 апреля 2010 г.	14.0.694.0	14.00.0694.000
Набор исправлений 2 для Exchange Server 2010	4 марта 2010 г.	14.0.689.0	14.00.0689.000
Набор исправлений 1 для Exchange Server 2010	9 декабря 2009 г.	14.0.682.1	14.00.0682.001
Exchange Server 2010 RTM	9 ноября 2009 г.	14.0.639.21	14.00.0639.021

Exchange Server 2007

В таблицах этого раздела приведены номера сборок и общие даты выпуска всех версий Microsoft Exchange Server 2007.

> **Примечание**
>
> Сведения о версии для Exchange Server 2007 SP1 правильно отображаются в консоли управления Exchange, в командной консоли Exchange и в диалоговом окне **справки Exchange Server 2007**. Однако после применения Exchange 2007 с пакетом обновления 1 (SP1) к пограничному транспортному серверу, на котором выполняется RTM-версия Exchange 2007, информация о версии пограничного транспортного сервера не обновляется в консоли управления Exchange, если пограничный транспортный сервер не подписан на сайт Active Directory. Это объясняется тем, что пограничный транспортный сервер напрямую не передает в Active Directory никакие сведения о конфигурации. Вместо этого сведения о версии для пограничных транспортных серверов записываются в Active Directory во время создания пограничной подписки.

Развернуть таблицу

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Набор исправлений 23 для Exchange Server 2007 с пакетом обновления 3 (SP3)	21 марта 2017 г.	8.3.517.0	8.03.0517.000
Набор исправлений 22 для Exchange Server 2007 с пакетом обновления 3 (SP3)	13 декабря 2016 г.	8.3.502.0	8.03.0502.000
Набор исправлений 21 для Exchange Server 2007 с пакетом обновления 3 (SP3)	20 сентября 2016 г.	8.3.485.1	8.03.0485.001
Набор исправлений 20 для Exchange Server 2007 с пакетом обновления 3 (SP3)	21 июня 2016 г.	8.3.468.0	8.03.0468.000
Набор исправлений 19 для Exchange Server 2007 с пакетом обновления 3 (SP3)	15 марта 2016 г.	8.3.459.0	8.03.0459.000
Набор исправлений 18 для Exchange Server 2007 с пакетом обновления 3 (SP3)	декабрь 2015 г.	8.3.445.0	8.03.0445.000
Набор исправлений 17 для Exchange Server 2007 с пакетом обновления 3 (SP3)	17 июня 2015 г.	8.3.417.1	8.03.0417.001
Набор исправлений 16 для Exchange Server 2007 с пакетом обновления 3 (SP3)	17 марта 2015 г.	8.3.406.0	8.03.0406.000
Набор исправлений 15 для Exchange Server 2007 с пакетом обновления 3 (SP3)	9 декабря 2014 г.	8.3.389.2	8.03.0389.002
Набор исправлений 14 для Exchange Server 2007 с пакетом обновления 3 (SP3)	26 августа 2014 г.	8.3.379.2	8.03.0379.002
Набор исправлений 13 для Exchange Server 2007 с пакетом обновления 3 (SP3)	24 февраля 2014 г.	8.3.348.2	8.03.0348.002
Набор исправлений 12 для Exchange Server 2007 с пакетом обновления 3 (SP3)	9 декабря 2013 г.	8.3.342.4	8.03.0342.004
Набор исправлений 11 для Exchange Server 2007 с пакетом обновления 3 (SP3)	13 августа 2013 г.	8.3.327.1	8.03.0327.001
Набор исправлений 10 для Exchange Server 2007 с пакетом обновления 3 (SP3)	11.02.13	8.3.298.3	8.03.0298.003
Набор исправлений 9 для Exchange Server 2007 с пакетом обновления 3 (SP3)	10 декабря 2012 г.	8.3.297.2	8.03.0297.002
Набор исправлений 8 версии 3 для Exchange Server 2007 с пакетом обновления 3 (SP3)	13 ноября 2012 г.	8.3.279.6	8.03.0279.006

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Накопительный пакет обновления 8 версии 2 для Exchange Server 2007 с пакетом обновления 3 (SP3)	9 октября 2012 г.	8.3.279.5	8.03.0279.005
Набор исправлений 8 для Exchange Server 2007 с пакетом обновления 3 (SP3)	13 августа 2012 г.	8.3.279.3	8.03.0279.003
Набор исправлений 7 для Exchange Server 2007 с пакетом обновления 3 (SP3)	16 апреля 2012 г.	8.3.264.0	8.03.0264.000
Набор исправлений 6 для Exchange Server 2007 с пакетом обновления 3 (SP3)	26 января 2012 г.	8.3.245.2	8.03.0245.002
Набор исправлений 5 для Exchange Server 2007 с пакетом обновления 3 (SP3)	21 сентября 2011 г.	8.3.213.1	8.03.0213.001
Набор исправлений 4 для Exchange Server 2007 с пакетом обновления 3 (SP3)	28 мая 2011 г.	8.3.192.1	8.03.0192.001
Набор исправлений 3 версии 2 для Exchange Server 2007 с пакетом обновления 3 (SP3)	30 марта 2011 г.	8.3.159.2	8.03.0159.002
Набор исправлений 2 для Exchange Server 2007 с пакетом обновления 3 (SP3)	10 декабря 2010 г.	8.3.137.3	8.03.0137.003
Набор исправлений 1 для Exchange Server 2007 с пакетом обновления 3 (SP3)	09.09.10	8.3.106.2	8.03.0106.002
Exchange Server 2007 SP3	7 июня 2010 г.	8.3.83.6	8.03.0083.006

Номера сборок предыдущих версий Exchange Server 2007

Развернуть таблицу

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Набор исправлений 5 для Exchange Server 2007 с пакетом обновления 2 (SP2)	7 декабря 2010 г.	8.2.305.3	8.02.0305.003

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Набор исправлений 4 для Exchange Server 2007 с пакетом обновления 2 (SP2)	9 апреля 2010 г.	8.2.254.0	8.02.0254.000
Набор исправлений 3 для Exchange Server 2007 с пакетом обновления 2 (SP2)	17 марта 2010 г.	8.2.247.2	8.02.0247.002
Набор исправлений 2 для Exchange Server 2007 с пакетом обновления 2 (SP2)	22 января 2012 г.	8.2.234.1	8.02.0234.001
Набор исправлений 1 для Exchange Server 2007 с пакетом обновления 2 (SP2)	19 ноября 2009 г.	8.2.217.3	8.02.0217.003
Exchange Server 2007 SP2	24 августа 2009 г.	8.2.176.2	8.02.0176.002
Набор исправлений 10 для Exchange Server 2007 с пакетом обновления 1 (SP1)	13 апреля 2010 г.	8.1.436.0	8.01.0436.000
Набор исправлений 9 для Exchange Server 2007 с пакетом обновления 1 (SP1)	16 июля 2009 г.	8.1.393.1	8.01.0393.001
Набор исправлений 8 для Exchange Server 2007 с пакетом обновления 1 (SP1)	19 мая 2009 г.	8.1.375.2	8.01.0375.002
Набор исправлений 7 для Exchange Server 2007 с пакетом обновления 1 (SP1)	18 марта 2009 г.	8.1.359.2	8.01.0359.002
Набор исправлений 6 для Exchange Server 2007 с пакетом обновления 1 (SP1)	10.02.09	8.1.340.1	8.01.0340.001
Набор исправлений 5 для Exchange Server 2007 с пакетом обновления 1 (SP1)	20 ноября 2008 г.	8.1.336.1	8.01.0336.01
Набор исправлений 4 для Exchange Server 2007 с пакетом обновления 1 (SP1)	7 октября 2008 г.	8.1.311.3	8.01.0311.003
Набор исправлений 3 для Exchange Server 2007 с пакетом обновления 1 (SP1)	8 июля 2008 г.	8.1.291.2	8.01.0291.002
Набор исправлений 2 для Exchange Server 2007 с пакетом обновления 1 (SP1)	9 мая 2008 г.	8.1.278.2	8.01.0278.002
Набор исправлений 1 для Exchange Server 2007 с пакетом обновления 1 (SP1)	28.02.08	8.1.263.1	8.01.0263.001

Название продукта	Дата выпуска	Номер сборки (краткий формат)	Номер сборки (длинный формат)
Сервер Exchange Server 2007 с пакетом обновления 1 (SP1)	29 ноября 2007 г.	8.1.240.6	8.01.0240.006
Набор исправлений 7 для Exchange Server 2007	8 июля 2008 г.	8.0.813.0	8.00.0813.000
Набор исправлений 6 для Exchange Server 2007	21.02.08	8.0.783.2	8.00.0783.002
Набор исправлений 5 для Exchange Server 2007	25 октября 2007 г.	8.0.754.0	8.00.0754.000
Набор исправлений 4 для Exchange Server 2007	23 августа 2007 г.	8.0.744.0	8.00.0744.000
Набор исправлений 3 для Exchange Server 2007	28 июня 2007 г.	8.0.730.1	8.00.0730.001
Набор исправлений 2 для Exchange Server 2007	8 мая 2007 г.	8.0.711.2	8.00.0711.002
Набор исправлений 1 для Exchange Server 2007	17 апреля 2007 г.	8.0.708.3	8.00.0708.003
Exchange Server 2007 RTM	08 марта 2007 г.	8.0.685.25	8.00.0685.025

Exchange Server 2003

В следующей таблице приведены номера сборок и общие даты выпуска всех версий Microsoft Exchange Server 2003. Чтобы узнать номер сборки Exchange Server 2003, откройте диалоговое окно **Свойства** у объекта сервера.

Развернуть таблицу

Название продукта	Дата выпуска	Номер сборки
Exchange Server 2003 после пакета обновления 2 (SP2)	Август 2008 г.	6.5.7654.4
Exchange Server 2003 после пакета обновления 2 (SP2)	Март 2008 г.	6.5.7653.33
Exchange Server 2003 SP2	19 октября 2005 г.	6.5.7683

Название продукта	Дата выпуска	Номер сборки
Exchange Server 2003 SP1	25 мая 2004 г.	6.5.7226
Exchange Server 2003	28.09.03	6.5.6944

Exchange 2000 Server

В следующей таблице приведены номера сборок и общие даты выпуска всех версий Microsoft Exchange 2000 Server. Чтобы узнать номер сборки Exchange 2000 Server, откройте диалоговое окно **Свойства** у объекта сервера.

Развернуть таблицу

Название продукта	Дата выпуска	Номер сборки
Exchange 2000 Server после пакета обновления 3 (SP3)	Август 2008 г.	6.0.6620.7
Exchange 2000 Server после пакета обновления 3 (SP3)	Март 2008 г.	6.0.6620.5
Exchange 2000 Server после пакета обновления 3 (SP3)	Август 2004 г.	6.0.6603
Exchange 2000 Server после пакета обновления 3 (SP3)	Апрель 2004 г.	6.0.6556
Exchange 2000 Server после пакета обновления 3 (SP3)	Сентябрь 2003 г.	6.0.6487
Exchange 2000 Server SP3	18 июля 2002 г.	6.0.6249
Exchange 2000 Server SP2	29.11.01	6.0.5762
Exchange 2000 Server SP1	21 июня 2001 г.	6.0.4712
Exchange 2000 Server	29.11.00	6.0.4417

Exchange Server 5.5

В следующей таблице приведены номера сборок и общие даты выпуска всех версий Microsoft Exchange Server 5.5.

Развернуть таблицу

Название продукта	Дата выпуска	Номер сборки
Exchange Server версии 5.5 SP4	01.11.00	5.5.2653
Exchange Server версии 5.5 SP3	09.09.99	5.5.2650

Название продукта	Дата выпуска	Номер сборки
Exchange Server версии 5.5 SP2	23 декабря 1998 г.	5.5.2448
Exchange Server версии 5.5 SP1	5 августа 1998 г.	5.5.2232
Exchange Server версии 5.5	03.02.98	5.5.1960

Exchange Server 5.0

Развернуть таблицу

Название продукта	Дата выпуска	Номер сборки
Exchange Server 5.0 с пакетом обновления 2 (SP2)	19.02.98	5.0.1460
Exchange Server 5.0 с пакетом обновления 1 (SP1)	18 июня 1997 г.	5.0.1458
Exchange Server 5.0	23 мая 1997 г.	5.0.1457

Exchange Server 4.0

В следующей таблице приведены номера сборок и общие даты выпуска всех версий Microsoft Exchange Server 4.0.

Развернуть таблицу

Название продукта	Дата выпуска	Номер сборки
Exchange Server 4.0 с пакетом обновления 5 (SP5)	5 мая 1998 г.	4.0.996
Exchange Server 4.0 с пакетом обновления 4 (SP4)	28 марта 1997 г.	4.0.995
Exchange Server 4.0 с пакетом обновления 3 (SP3)	29 октября 1996 г.	4.0.994
Exchange Server 4.0 с пакетом обновления 2 (SP2)	19.07.96	4.0.993
Exchange Server 4.0 с пакетом обновления 1 (SP1)	1 мая 1996 г.	4.0.838
Exchange Server 4.0 Standard Edition	11 июня 1996 г.	4.0.837

Просмотр состояния обновления программного обеспечения для Exchange Server

Статья • 24.03.2023

> ⓘ **Примечание**
>
> Это предварительная документация для предварительной версии программы, которая может быть изменена и может быть недоступна для всех.

На странице **Обновления программного обеспечения (предварительная версия)** в Центр администрирования Microsoft 365 отображается общий обзор состояния установки Приложения Microsoft 365, обновлений Windows и Exchange Server обновлений и состояния не поддерживается в вашей среде. Обеспечение установки этих обновлений важно, так как они помогают защитить вас от известных уязвимостей. На странице **Обновления программного обеспечения (предварительная версия)** можно определить общее состояние обновления серверов.

На странице **Обновления программного обеспечения (предварительная версия)** есть следующие вкладки, которые помогут вам отслеживать состояние обновлений для устройств:

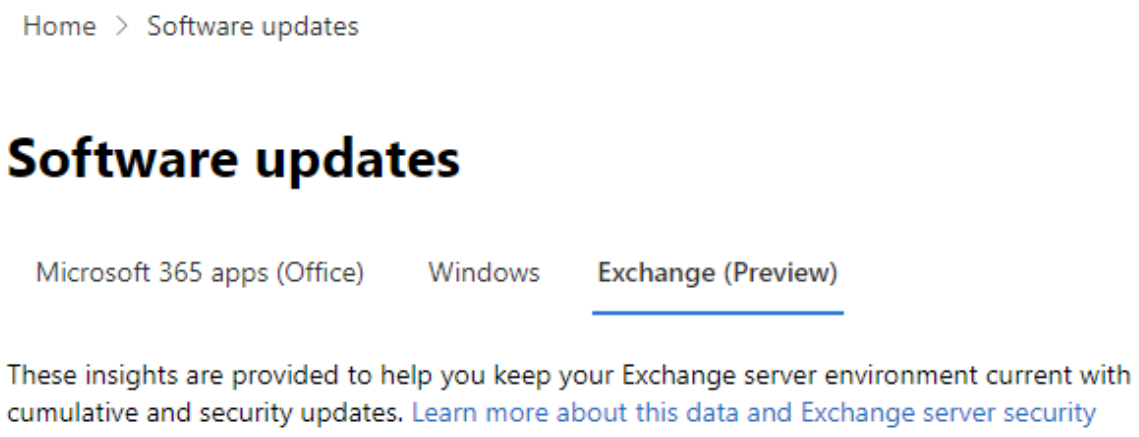
- **Приложения Microsoft 365**. Отображает данные для обновлений системы безопасности для Приложения Microsoft 365. Дополнительные сведения см. в статье Просмотр состояния обновления программного обеспечения для Приложения Microsoft 365 установок.
- **Windows**: отображает данные для накопительных обновлений и обновлений компонентов для клиентов Windows. Дополнительные сведения см. на странице Обновления программного обеспечения Центра администрирования Майкрософт (предварительная версия).
- **Exchange Server**. Отображает данные для накопительных обновлений и обновлений системы безопасности, а также определяет серверы, не поддерживаемые.

Эта статья содержит сведения о **вкладке Exchange Server**.

> **Примечание**
>
> **Видео:** Просмотр презентации сообщества Microsoft Exchange (MEC) на панели мониторинга обновления Exchange Server

Вкладка Exchange Server

Чтобы просмотреть страницу **Обновления программного обеспечения (предварительная версия),** войдите в Центр администрирования Microsoft 365 с учетной записью администратора, а затем перейдите в раздел **Показать все**>**обновления программного обеспечения работоспособности**> (предварительная версия).



> **Совет**
>
> Если в меню не отображается запись об **обновлениях программного обеспечения (предварительная версия),** попробуйте перейти по следующему URL-адресу: https://admin.microsoft.com/Adminportal/Home#/softwareupdates.

На вкладке **Exchange Server** отображаются следующие сведения о серверах в организации, на которых установлены Exchange Server:

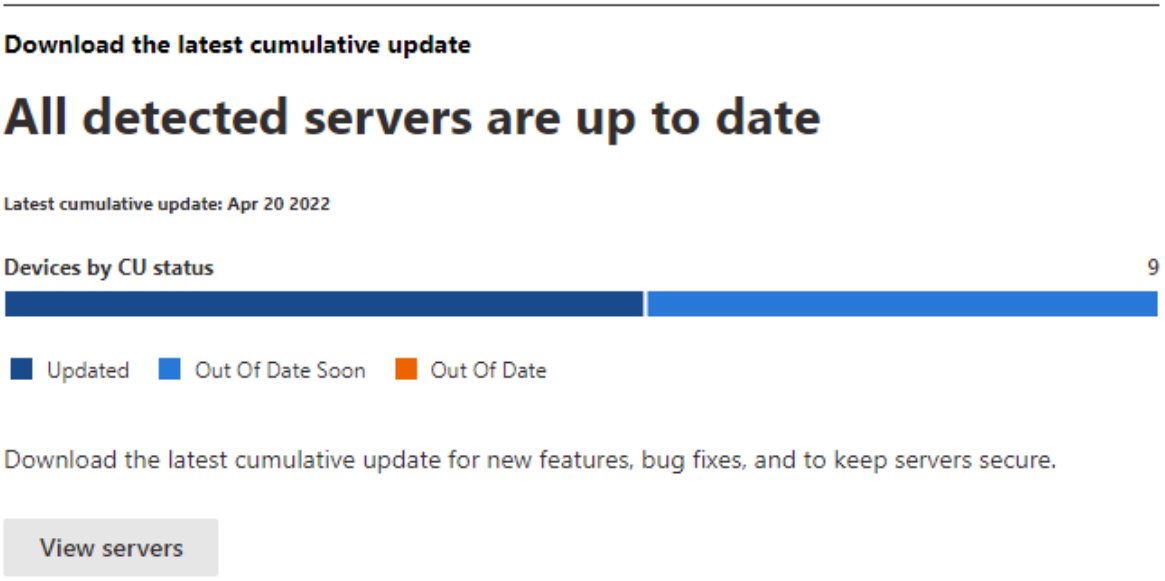
- Сколько серверов Exchange server требует накопительных обновлений
- Сколько серверов Exchange Server требует обновлений для системы безопасности
- Сколько серверов Exchange не поддерживается

На вкладке **Exchange Server** не перечислены конкретные серверы, за которыми стоит одна или несколько сборок.

Накопительные обновления для Exchange Server

Корпорация Майкрософт выпускает накопительные Обновления (CU) для Exchange Server два раза в год. Эти обновления устраняют проблемы, о которые сообщили клиенты. Также могут включать новые функции и функциональные возможности.

Чтобы получить список всех имен серверов, связанных с клиентом, выберите **Просмотреть серверы**.



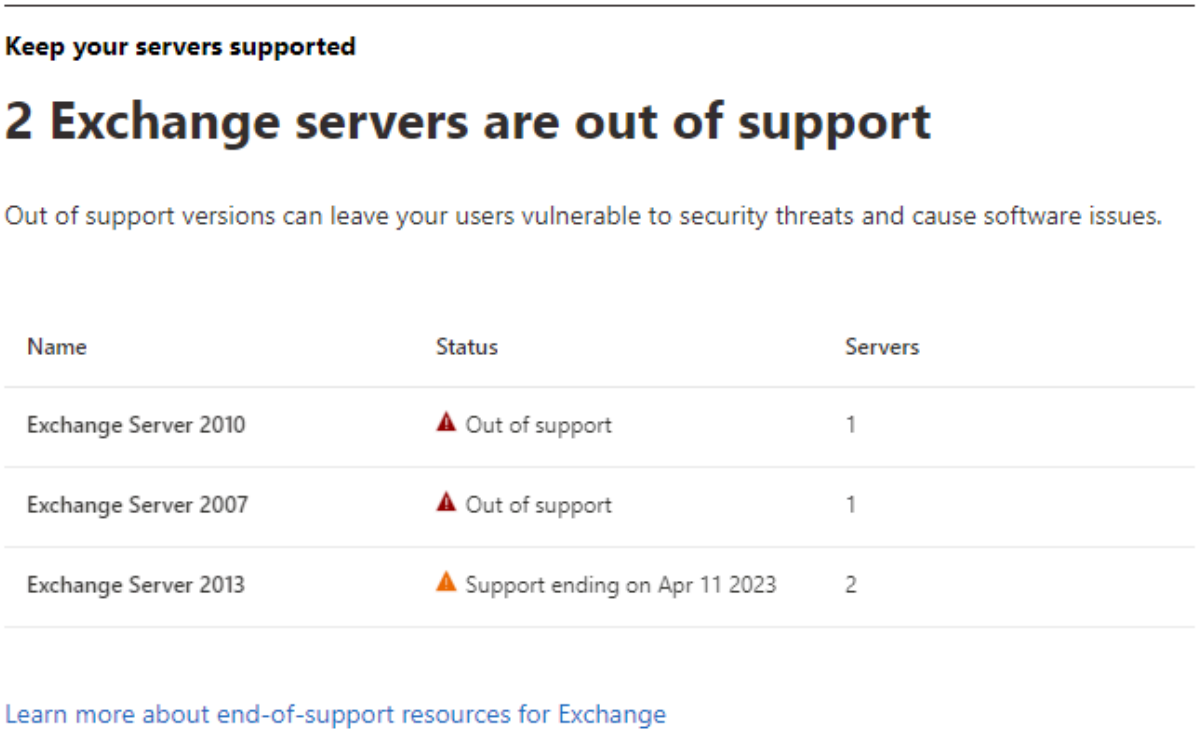
Обновления для системы безопасности для Exchange Server

Обновления для системы безопасности — это пакеты, которые относятся к бюллетеню безопасности, выпущенном корпорацией Майкрософт, или содержат изменения в определениях часовых поясов. При использовании основной поддержки номера SU выпускаются по мере необходимости для последнего выпуска cu и для предыдущего накопительного пакета обновления. При использовании расширенной поддержки номера SU выпускаются по мере необходимости, но только для последней версии CU.

Чтобы получить список всех имен серверов, связанных с клиентом, выберите **Просмотреть серверы**.

Серверы Exchange, которые не поддерживаются

Версии, не поддерживающиеся, могут сделать ваши серверы и данные уязвимыми для угроз безопасности и вызвать проблемы с программным обеспечением. Дополнительные сведения о поддержке и жизненном цикле продуктов см. в Exchange Server матрице поддержки или сведения о жизненном цикле продуктов и служб Майкрософт.



Связанные статьи

- Обновления для Exchange Server
- Номера сборок и даты выпуска Exchange Server
- Таблица поддержки Exchange Server
- Сведения о жизненном цикле продуктов и служб Майкрософт

Часто задаваемые вопросы— панель мониторинга Обновления программного обеспечения Exchange Server

Статья • 24.03.2023

> ⓘ **Примечание**
>
> Эта документация предназначена для предварительной версии программы, которая может быть недоступна для всех пользователей.

ВОПРОС: Где можно найти отчет Обновления программного обеспечения Exchange Server?
ОТВЕТ: Отчет Обновления Exchange Server программного обеспечения можно найти на Центр администрирования Microsoft 365 на *вкладке Обновления > Exchange Server по программному обеспечению работоспособности>*.

ВОПРОС: Почему я не вижу вкладку Exchange Server со своим клиентом?
ОТВЕТ: Отчеты создаются только для клиентов, для которых можно создать отчет, будут видеть вкладку Exchange Server на странице Обновления программного обеспечения.

ВОПРОС: Как создаются отчеты Обновления программного обеспечения?
ОТВЕТ: Отчеты основаны на данных, курируемых с помощью сигналов из нескольких источников. Источники включают журналы обработки веб-службы транспорта Майкрософт, данные, ранее утвержденные клиентами для отправки в Корпорацию Майкрософт, и общедоступные наборы данных, такие как записи DNS. Эти входные данные объединяются для создания этого представления и предназначены для помощи в управлении серверами Exchange. Данные заголовка получения транспорта являются ключевыми для нашей способности включать серверы в отчет. Если поток обработки почты с сервера невелик или отсутствует, он не будет включен в отчет.

ВОПРОС: Вы обращаетесь к локальным серверам в этом процессе?
ОТВЕТ: Нет. Этот процесс не обращается к локальным серверам.

ВОПРОС: Какие факторы определяют, включен ли сервер?
ОТВЕТ: Поток электронной почты в облачных службах Майкрософт или через нее

управляет процессом анализа аналитических сведений. Мы пытаемся связать сервер с клиентом Майкрософт с помощью электронной почты и домена сервера. Одним из ключевых маркеров, используемых для связывания серверов с клиентами, является список обслуживаемых доменов. Серверы, участвующие в доставке, полное доменное имя которых является частью принятого домена для клиента, будут связаны с этим клиентом. В отчете отражаются серверы, связанные с клиентом Microsoft 365 и принятыми доменами, а не с определенной организацией Exchange. Этот автоматизированный анализ также учитывает другие характеристики для достижения высокого уровня уверенности в том, что связь сервера является точной.

ВОПРОС: Какие сведения о серверах предоставляются в отчете?
ОТВЕТ: В отчете основное внимание уделяется количеству серверов по версиям и сборке, включая сведения о том, работают ли на этих серверах последняя накопительная Обновления и Обновления безопасности. Пользователь-администратор может выполнить детализацию до уровня сервера.

ВОПРОС: Почему некоторые из моих серверов не представлены или отображают неверную информацию?
ОТВЕТ: Неверные сведения могут быть по нескольким причинам. Если сервер не отправляет сообщение электронной почты, которое передает облако Майкрософт, анализ аналитических сведений не будет иметь о ней сведений. Этот процесс поддерживает таблицу серверов, которые были "просмотрены" в течение последних 14 дней. Этот процесс уменьшает колебания и представляет клиенту более полный список. Однако этот процесс не является совершенным. Серверы стареют из таблицы и могут быть удалены из списка серверов до тех пор, пока сообщение электронной почты из него не появится снова. Аналогичным образом это поведение может объяснить аналитические данные о том, что сервер становится устаревшим. Определенные конфигурации сервера и сети также могут привести к проблемам с именованием или присвоением. Другая причина неверных сведений заключается в том, что процесс исключает серверы из отчетов, если шаг связи с клиентом не соответствует высокому плану доверия.

ВОПРОС: Существует ли механизм обратной связи для указания ситуаций, когда аналитические сведения неверны?
ОТВЕТ: Да. Используйте кнопку "Отправить отзыв" на странице, объясните проблему и добавьте экран snapshot.

ВОПРОС: Почему вы предоставляете эти аналитические сведения, если они потенциально не идеальны?
ОТВЕТ: Эти отчеты предназначены для предоставления администраторам Exchange

как можно большего количества инструментов, которые помогут им лучше понять их Exchange Server среде. Эти отчеты заполняют пробел сегодня, так как они подчеркивают общую работоспособность обслуживания среды. Мы считаем, что общая ценность этой возможности перевешивает потенциальные негативы. Эта концепция работоспособности будет по-прежнему разрабатываться и включаться в будущее обновление Exchange 2019.

ВОПРОС: Я обновил свои серверы сегодня и не вижу эти изменения, отраженные в отчете. Как часто обновляются данные?
ОТВЕТ: Отчеты обновляются ежедневно, но с данными, которые определяют этот процесс, возникает задержка по времени. Как правило, задержка в данных от 24 до 36 часов. В заголовках отчета указана дата "свежести данных", указывая дату последнего обновления.

ВОПРОС: Выпущено новое обновление сервера; когда она будет отражена в отчетах?
ОТВЕТ: См. приведенный выше вопрос об обновлении данных. Существует задержка в данных и обработке. Как правило, мы стремимся правильно отразить новое обновление в отчетах в течение 24–36 часов после выпуска.

Заметки о выпуске Exchange Server

Статья • 04.04.2023

> **Совет**
>
> Ищете заметки о выпуске Exchange 2013? См **. заметки о выпуске Exchange 2013**.

Добро пожаловать в Microsoft Exchange Server 2019! В этом разделе содержатся важные сведения, которые необходимо знать для успешного развертывания Exchange 2019. Прежде чем приступать к развертыванию, прочтите этот раздел полностью.

Известные проблемы с Exchange Server 2019

При попытке удалить Exchange Server из Windows 2019 Server Core с помощью мастера установки Exchange операция завершится ошибкой. Мастер пытается запустить панель управления Windows для удаления Exchange, но панель управления не существует в Windows Server Core. Чтобы удалить Exchange из Windows Server Core, выполните следующую команду установки из командной строки:

> **Примечание**
>
> - Предыдущий переключатель */IAcceptExchangeServerLicenseTerms* не будет работать начиная с накопительных обновлений (CU) за сентябрь 2021 г. Теперь необходимо использовать */IAcceptExchangeServerLicenseTerms_DiagnosticDataON* или */IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF* для автоматической установки и установки по сценариям.
> - В примерах ниже используется переключатель */IAcceptExchangeServerLicenseTerms_DiagnosticDataON*. Вы можете изменить переключатель на */IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF*.

```
dos
```

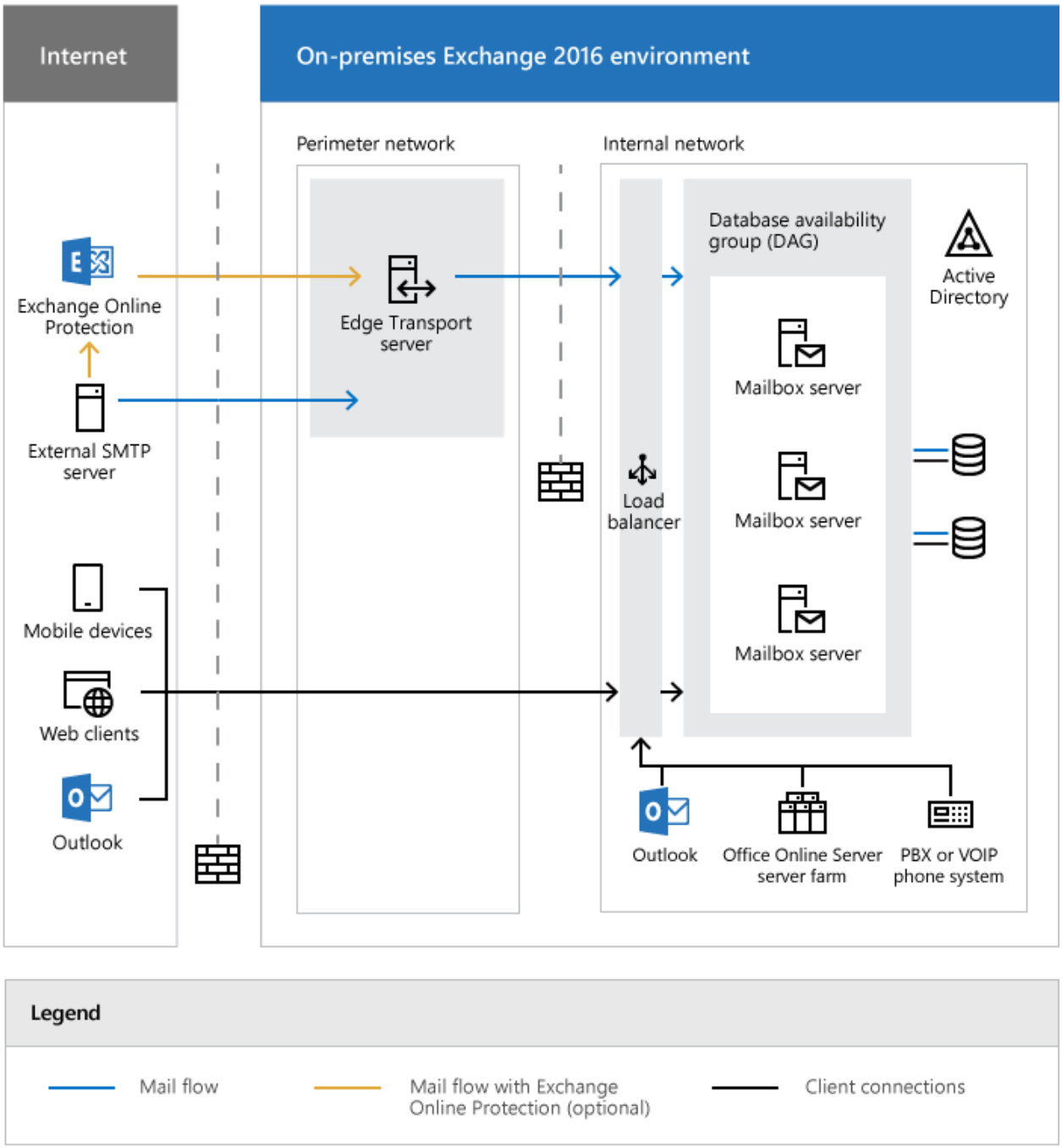
```
Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON
/mode:Uninstall
```

Эта проблема будет устранена в будущем накопительном обновлении для Exchange Server 2019.

Архитектура Exchange

Статья • 04.04.2023

Exchange использует архитектуру с одним стандартным блоком, который предоставляет службы электронной почты для развертываний всех размеров, от небольших организаций до крупнейших многонациональных корпораций. Эта архитектура описана на следующей схеме.



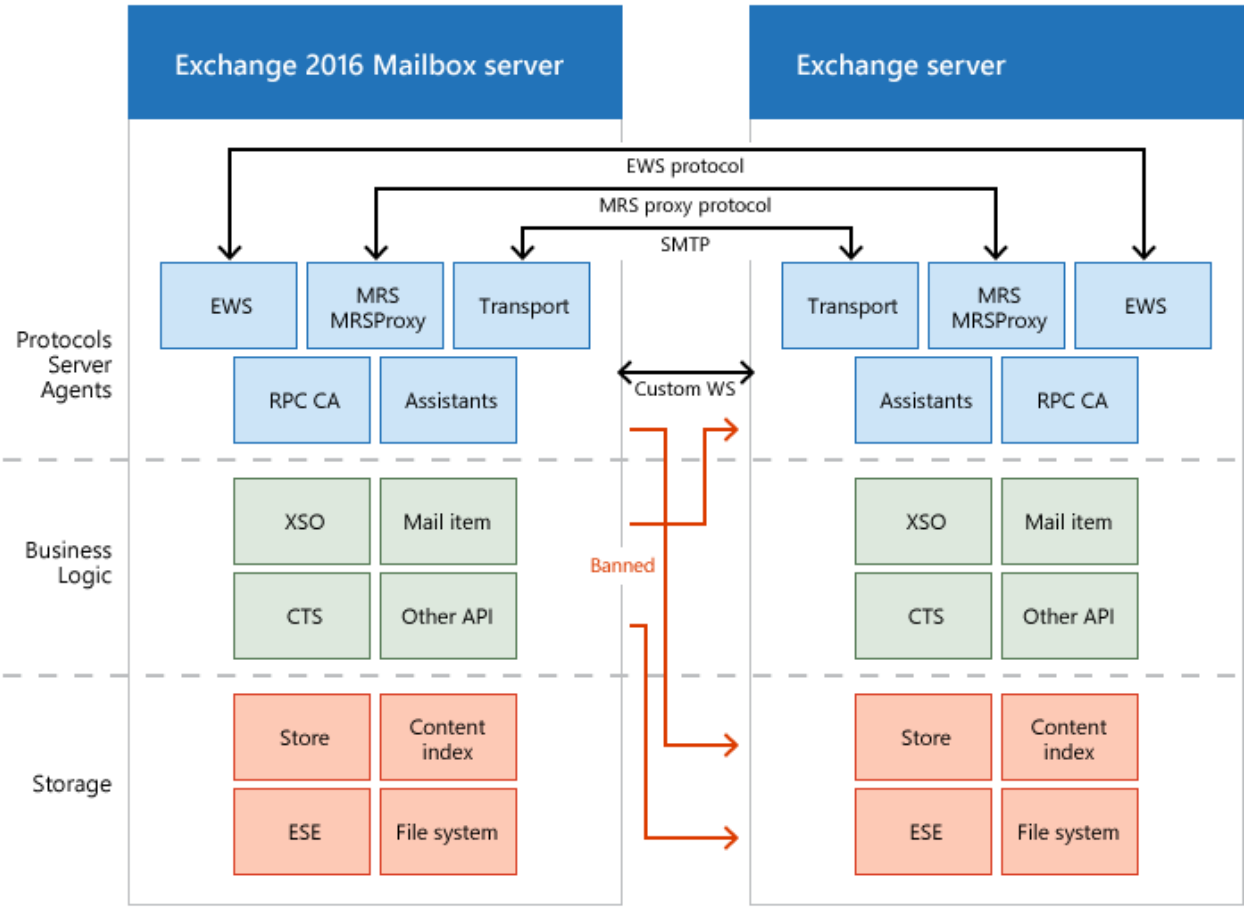
Отдельные компоненты описаны в разделах ниже.

Архитектура каналов связи между серверами

Обмен данными между серверами Exchange и последними и будущими версиями Exchange осуществляется на уровне протокола. Связь на нескольких уровнях не допускается. Такую архитектуру можно описать одной фразой — "каждый сервер представляет собой «остров»". Преимущества такой архитектуры:

- сокращенное время обмена данными между серверами;
- подключение с учетом версий;
- изолированные сбои;
- целостность каждого сервера.

Связь на уровне протокола между серверами Exchange Server показана в следующей схеме.



Архитектура ролей сервера

Exchange использует серверы почтовых ящиков и пограничные транспортные серверы. Они описаны в разделах ниже.

Серверы почтовых ящиков

- Серверы почтовых ящиков содержат службы транспорта для маршрутизации электронной почты. Дополнительные сведения см. в статье Mail flow and the transport pipeline.
- Серверы почтовых ящиков содержат базы данных почтовых ящиков для обработки, предъявления и хранения данных. Дополнительные сведения см. в статье Управление базами данных почтовых ящиков в Exchange Server.
- Серверы почтовых ящиков содержат службы клиентского доступа, которые принимают клиентские подключения для всех протоколов. Внешние такие службы отвечают за маршрутизацию (*проксирование*) подключений к соответствующим внутренним службам на сервере почтовых ящиков. Настроить виртуальный каталог для внутренних служб на сервере почтовых ящиков. Дополнительные сведения см. в разделе Архитектура протокола клиентского доступа далее в этом разделе.
- На серверах почтовых ящиков Exchange 2016 есть службы единой системы обмена сообщениями, которые обеспечивают функции голосовой почты и другие возможности телефонии для почтовых ящиков.

  > ⓘ **Примечание**
  >
  > Единая система обмена сообщениями не доступна в Exchange 2019.

- Вы управляете серверами почтовых ящиков с помощью Центра администрирования Exchange (EAC) и командной консоли Exchange. Дополнительные сведения см. в разделе Центр администрирования Exchange в Exchange Server и Exchange Server PowerShell (командная консоль Exchange).

Пограничные транспортные серверы

- Пограничные транспортные серверы отвечают за поток обработки внешней почты в организации Exchange.
- Пограничные транспортные серверы, как правило, устанавливаются в сети периметра и подписываются на внутреннюю организацию Exchange. Благодаря процессу синхронизации EdgeSync сведения о получателе и другие

данные конфигурации становятся доступными для пограничного транспортного сервера, когда электронные сообщения поступают в организацию Exchange и покидают ее.

- Пограничные транспортные серверы предоставляют правила защиты от нежелательной почты и потока обработки почты, когда почта входит в вашу организацию Exchange и покидает ее. Дополнительные сведения см. в разделе Защита от нежелательной нежелательной информации в Exchange Server

- Управление пограничными транспортными серверами выполняется с помощью командной консоли Exchange. Дополнительные сведения см. в разделе Exchange Server PowerShell (командная оболочка Exchange).

Дополнительные сведения о пограничных транспортных серверах см. в статье Пограничные транспортные серверы.

Архитектура обеспечения высокой доступности

Возможности для обеспечения высокой доступности в Exchange Server описаны в разделах ниже.

Высокая доступность почтовых ящиков

Группа доступности базы данных (DAG) — это основной элемент платформы обеспечения высокой доступности и устойчивости сайта, встроенной в Exchange Server. DAG — это группа серверов почтовых ящиков, на которых размещается набор баз данных и обеспечивается автоматическое восстановление на уровне базы данных из-за сбоев базы данных, сети и сервера. Группы ДОСТУПНОСТИ в Exchange 2016 или более поздних версиях были улучшены по сравнению с Exchange 2013. Дополнительные сведения о группах доступности баз данных см. в разделе Группы доступности баз данных.

Высокая доступность транспорта

- Служба транспорта создает избыточные копии всех сообщений при передаче. Эта функция называется *теневой избыточностью*.

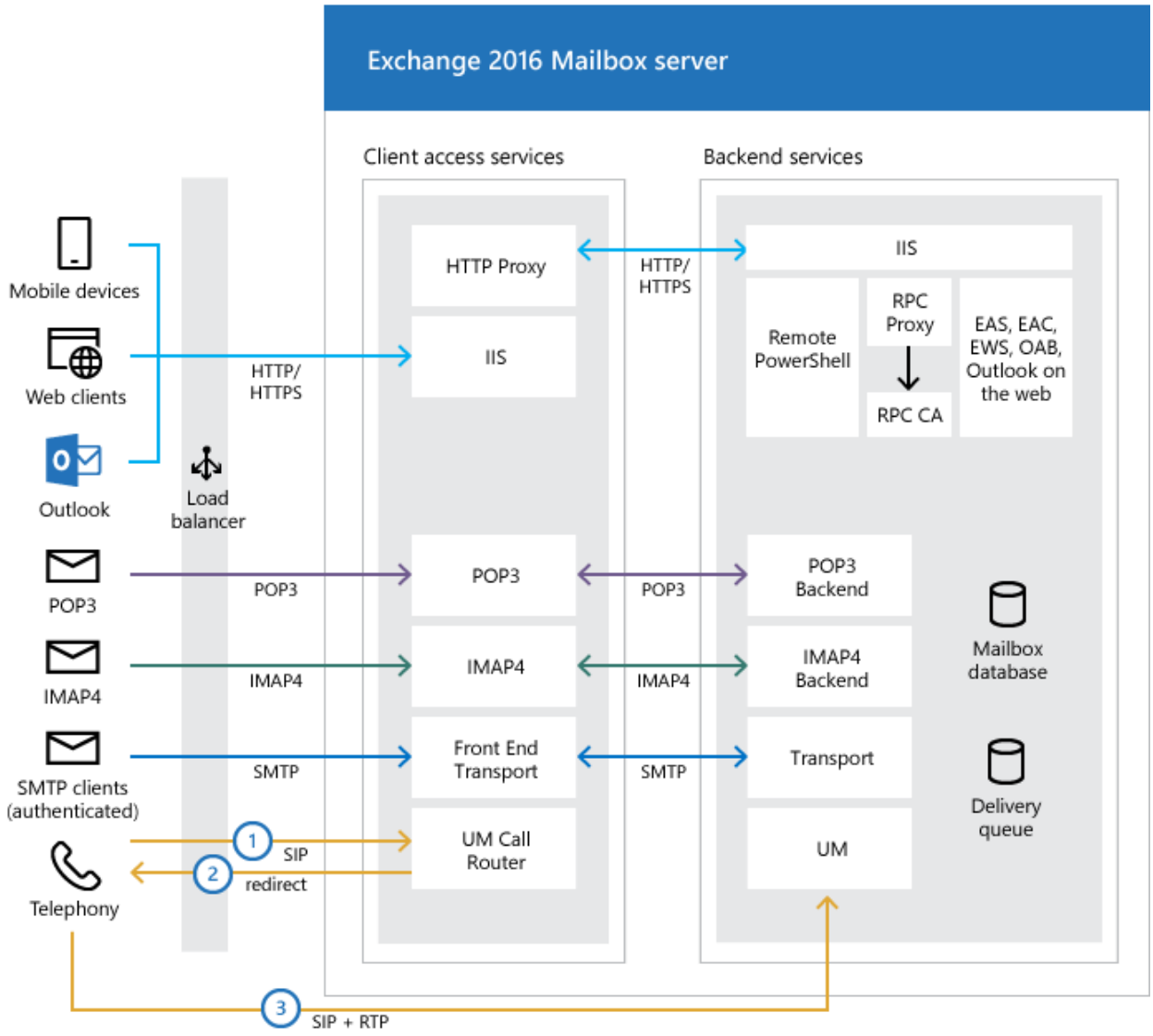
- Служба транспорта создает избыточные копии всех доставленных сообщений. Эта функция называется *сетью безопасности*.

- В Exchange Server DAG представляет границу высокого уровня доступности транспорта. Обеспечить взаимозаменяемость серверов можно с помощью группы обеспечения доступности баз данных, созданной на основе нескольких серверов Active Directory.
- В Exchange Server высокий уровень доступности транспорта — это не просто лучший способ обеспечения избыточности сообщений, так как избыточность не зависит от поддерживаемых функций сервера отправки почты. Таким образом, можно сказать, что Exchange Server пытается гарантировать избыточность сообщений, сохраняя несколько копий сообщений во время и после доставки.

Дополнительные сведения см. в статье Высокая доступность транспорта.

Архитектура протокола клиентского доступа

Службы клиентского доступа на серверах почтовых ящиков Exchange отвечают за прием всех форм клиентских подключений. Службы клиентского доступа (внешний интерфейс) поддерживают эти подключения к внутренним службам на целевом сервере почтовых ящиков (локальном или удаленном сервере почтовых ящиков, на котором хранится активная копия почтового ящика пользователя). Клиенты не подключаются к внутренним службам напрямую. Такой способ подключения показан в схеме ниже.



Используемый клиентом протокол определяет протокол, с помощью которого запрос проксируется к внутренним службам на целевом сервере почтовых ящиков. Например, если клиент подключился с помощью протокола HTTP, сервер почтовых ящиков использует этот протокол для проксирования запроса на целевой сервер почтовых ящиков (защищенный с помощью самозаверяющего SSL-сертификата). Если протокол клиента — это IMAP или POP, то используется один из двух этих протоколов.

В Exchange 2016 запросы телефонии отличаются от других клиентских подключений. Вместо того чтобы проксировать запрос, сервер почтовых ящиков *перенаправляет* его на тот сервер почтовых ящиков, на котором хранится активная копия почтового ящика пользователя. Устройства телефонии должны устанавливать сеансы SIP и RTP непосредственно со службами единой системы обмена сообщениями на целевом сервере почтовых ящиков Exchange 2016.

> ⓘ **Примечание**

Единая система обмена сообщениями не доступна в Exchange 2019.

Изменения архитектуры Exchange

- **Консолидация ролей сервера**. В Exchange 2013 или более ранней версии можно установить роль сервера клиентского доступа и роль сервера почтовых ящиков на отдельных компьютерах. В Exchange 2016 или более поздней версии роль сервера клиентского доступа автоматически устанавливается как часть роли сервера почтовых ящиков, а роль сервера клиентского доступа недоступна как отдельный вариант установки. Это изменение отражает философию совместного расположения ролей сервера Exchange, которая является рекомендуемой практикой, начиная с Exchange 2010. Архитектура сервера Exchange с несколькими ролями дает следующие ощутимые преимущества:

  - Все серверы Exchange Server в вашей среде, за вероятным исключением пограничных транспортных серверов, могут быть полностью одинаковыми. То есть одинаковыми могут быть их аппаратное обеспечение, конфигурация и т. д. Это упрощает закупку аппаратного обеспечения, а также обслуживание серверов Exchange Server и управление ими.

  - Скорее всего, вы сможете использовать меньше физических серверов Exchange. В этом случае снизятся текущие расходы на техническое обслуживание, потребуется меньше лицензий на серверы Exchange, а также ослабятся требования к числу стоек, площади помещения и необходимой мощности.

  - Масштабируемость улучшена, так как вы распределяете рабочую нагрузку между большим количеством физических компьютеров. Во время сбоя нагрузка на остальные серверы Exchange с несколькими ролями возрастает только постепенно, что гарантирует, что другие функции на серверах Exchange не будут негативно затронуты.

  - Отказоустойчивость повышена за счет того, что сервер Exchange с несколькими ролями может выдержать большее число сбоев, связанных с ролью (или службой) клиентского доступа, продолжая при этом функционировать.

- **Улучшения поиска**. Локальный экземпляр поиска теперь может считывать данные из копии локальной базы данных почтового ящика. В результате пассивным экземплярам поиска больше не нужно координировать работу со

своими активными коллегами для обновления индекса, а требования к пропускной способности между активной копией и пассивной копией сократились на 40 % по сравнению с предыдущими версиями Exchange. Кроме того, поиск теперь может выполнять несколько асинхронных операций чтения диска, прежде чем пользователь завершит условие поиска. Это заполняет кэш соответствующими сведениями и обеспечивает задержку запросов поиска в секунду для сетевых клиентов, таких как Outlook в Интернете.

- **Office Online Server предварительная версия для предварительного просмотра документов Outlook в Интернете**. В Exchange 2013 или более ранних версиях Outlook Web App включали просмотр документов WebReady для встроенного предварительного просмотра документов Office и PDF. В Exchange 2016 или более поздней версии Outlook в Интернете использует предварительную версию Office Online Server для предоставления расширенных возможностей предварительного просмотра и редактирования документов. Хотя это обеспечивает согласованное взаимодействие с документами с другими продуктами, такими как SharePoint и Skype для бизнеса, вам потребуется развернуть Office Online Server Preview в локальной среде, если у вас ее еще нет. Дополнительные сведения см. в статье Установка Office Online Server в организации Exchange.

- **MAPI по протоколу HTTP используется по умолчанию для подключений Outlook**: MAPI по протоколу HTTP появилась в Exchange 2013 с пакетом обновления 1 (SP1) и предлагает усовершенствования по сравнению с традиционным методом подключения Outlook Anywhere (RPC через HTTP). В Exchange 2016 или более поздней версии MAPI по протоколу HTTP включен по умолчанию и предоставляет дополнительные элементы управления, такие как возможность включения или отключения MAPI по ПРОТОКОЛу HTTP для каждого пользователя и объявления ее внешним клиентам. Дополнительные сведения см. в статье MAPI/HTTP в Exchange Server.

Серверы почтовых ящиков

Статья • 04.04.2023

В Microsoft Exchange Server 2010 роль сервера почтовых ящиков предназначалась для размещения баз данных почтовых ящиков и общих папок, а также для хранилища сообщений электронной почты. В Exchange Server 2016 и Exchange Server 2019 роль сервера почтовых ящиков содержит транспортные службы для маршрутизации почты, баз данных почтовых ящиков, служб клиентского доступа для приема клиентских подключений и (только в Exchange 2016) компонентов единой системы обмена сообщениями (UM).

Дополнительные сведения о серверах почтовых ящиков Exchange и о том, как они дополняют другие роли сервера, см. в разделе Архитектура Exchange.

Управление серверами почтовых ящиков

О стандартных задачах по управлению серверами почтовых ящиков можно узнать в следующих статьях:

- Управление базами данных почтовых ящиков в Exchange Server
- Управление перемещением локальных почтовых ящиков в Exchange Server
- Подготовка почтовых ящиков для запросов на перемещение между лесами
- Включение конечной точки прокси-сервера MRS для удаленных перемещений

Управление базами данных почтовых ящиков в Exchange Server

Статья • 04.04.2023

Базы данных почтовых ящиков — это модуль, в котором создаются и хранятся почтовые ящики. База данных почтовых ящиков хранится в виде файла базы данных Exchange с расширением EDB. В Exchange 2016 и 2019 каждая база данных почтовых ящиков имеет собственные свойства, которые можно настроить.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 10 минут
- Чтобы открыть Центр администрирования Exchange, см. статью Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Для выполнения этой процедуры или процедур требуются разрешения. Сведения о необходимых разрешениях см. в записи "Базы данных почтовых ящиков" в разделе Разрешения получателей .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Создание базы данных почтовых ящиков

Использование Центра администрирования Exchange для создания базы данных почтовых ящиков

1. В Центре администрирования Exchange перейдите в раздел **Сервер**.

2. Выберите пункт **Базы данных** и нажмите символ +, чтобы создать базу данных.

3. Используйте мастер создания базы данных, чтобы создать базу данных.

Создание базы данных почтовых ящиков в командной консоли Exchange

Пример создания базы данных почтовых ящиков содержится в примере 1 в разделе New-MailboxDatabase.

Как узнать, работает ли этот процесс?

Чтобы убедиться, что база данных успешно создана, выполните следующие задачи:

- В EAC убедитесь, что созданная база данных почтовых ящиков указана на странице **Базы данных** .
- В командной консоли Exchange убедитесь, что база данных была создана на сервере Mailbox01, выполнив следующую команду.

```
PowerShell

Get-MailboxDatabase -Server "Mailbox01"
```

Получение свойств базы данных почтовых ящиков

Дополнительные сведения о синтаксисе и параметрах см. в разделе Get-MailboxDatabase.

Получение свойств базы данных почтовых ящиков в командной консоли Exchange

Пример получения свойств базы данных почтовых ящиков см. в примере 3 в Get-MailboxDatabase.

Как узнать, сработал ли этот процесс?

Чтобы убедиться, что вы успешно получили сведения о базе данных почтового ящика, выполните следующую задачу:

- В командной консоли Exchange убедитесь, что информация о базе данных почтовых ящиков представлена правильно.

Задание свойств базы данных почтовых ящиков

Использование Центра администрирования Exchange для задания свойств базы данных почтовых ящиков

1. В Центре администрирования Exchange откройте раздел **Серверы**.
2. Выберите пункт **Базы данных**, а затем выберите базу данных почтовых ящиков, которую необходимо настроить.
3. Нажмите ✎ чтобы настроить атрибуты базы данных почтовых ящиков.
4. На вкладке **Общие** можно просмотреть состояние базы данных почтовых ящиков, включая путь к базе данных почтовых ящиков, время последней архивации и состояние базы данных почтовых ящиков.

    - **Путь к базе данных**. В этом поле только для чтения отображается полный путь к файлу базы данных Exchange (EDB) для выбранной базы данных почтового ящика. Чтобы просмотреть полный путь, щелкните путь и используйте стрелку вправо. Путь в этом поле нельзя изменить. Чтобы изменить расположение файлов базы данных, используйте командлет Move-DatabasePath.

    - **Последняя полная резервная копия**. В этом поле только для чтения отображаются дата и время последней полной резервной копии базы данных почтовых ящиков.

    - **Последнее добавочное резервное копирование**. В этом поле только для чтения отображаются дата и время последней добавочной резервной копии базы данных почтовых ящиков.

    - **Состояние**. В этом поле только для чтения отображается, подключена или отключена база данных почтовых ящиков.

- **Подключено на сервере**. В этом поле только для чтения отображается, на каком сервере подключена база данных.

> ⓘ **Примечание**
>
> В этой статье содержатся ссылки на термин **master**, который корпорация Майкрософт больше не использует. Когда термин будет удален из программного обеспечения, мы удалим его из этой статьи.

- **Master**: в этом поле только для чтения отображается сервер-источник для базы данных почтовых ящиков. Главным называется сервер почтовых ящиков, на котором размещена активная копия базы данных.
- **Тип образца**. В этом поле только для чтения отображается тип master базы данных почтовых ящиков.
- **Изменено**: в этом поле только для чтения отображаются дата и время последнего изменения базы данных.
- **Серверы, на которых размещена копия этой базы данных**. В этом поле только для чтения отображаются другие серверы с копией этой базы данных.

5. Вкладка **Обслуживание** используется для настройки параметров базы данных почтовых ящиков, включая определение получателя журнала, установку расписания обслуживания и подключение базы данных при запуске.

   - **Получатель журнала**. Нажмите кнопку **Обзор** , чтобы указать получателя, чтобы включить ведение журнала в этой базе данных почтовых ящиков. Удалите указанного получателя, чтобы отключить ведение журнала.
   - **Расписание обслуживания**. Используйте этот список, чтобы выбрать одно из предустановленных расписаний обслуживания. Можно также настроить пользовательское расписание. Чтобы настроить пользовательское расписание, нажмите кнопку **Настроить**.
   - **Включить фоновое обслуживание базы данных (24 x 7 ESE scanning)**: установите этот флажок, чтобы включить проверку базы данных в сети, которая непрерывно выполняется в фоновом режиме. Во время оперативного сканирования вычисляется контрольная сумма базы данных и выполняются операции, позволяющие Exchange находить пропущенное пространство в базе данных и восстанавливать его. Если

этот флажок установлен, Exchange сканирует базу данных один раз в день и выдает предупреждение, если проверку не удается закончить в течение семи дней.

- **Не подключайте эту базу данных при запуске**. Установите этот флажок, чтобы запретить Exchange подключать эту базу данных почтовых ящиков при ее запуске.

- **Эта база данных может быть перезаписана путем восстановления**. Установите этот флажок, чтобы разрешить перезапись базы данных почтовых ящиков во время восстановления.

- **Включить циклическое ведение журнала**. Установите этот флажок, чтобы включить циклическое ведение журнала.

6. Вкладка **Ограничения** используется для указания предельного размера хранилища, интервала предупреждений и параметров удаления для базы данных почтовых ящиков.

    - **Предупреждение о проблеме в (ГБ):** установите этот флажок, чтобы автоматически предупреждать пользователей почтовых ящиков о том, что их почтовый ящик приближается к ограничению хранилища. Чтобы указать максимальный размер почтового ящика, установите этот флажок и укажите размер почтового ящика в гигабайтах (ГБ), при превышении которого пользователям будет отправлено предупреждение по электронной почте. Допустимый интервал значений: от 0 до 2 097 151 МБ (2 ТБ).

    - **Запретить отправку в (ГБ):** установите этот флажок, чтобы запретить пользователям отправлять новые сообщения электронной почты после того, как размер их почтового ящика достигнет указанного ограничения. Чтобы указать этот лимит, установите флажок и введите размер почтового ящика в ГБ, при превышении которого будет запрещена отправка новых сообщений, а пользователю отправлено уведомление. Допустимый интервал значений: от 0 до 2 097 151 МБ (2 ТБ).

    - **Запретить отправку и получение в (ГБ).** Установите этот флажок, чтобы запретить пользователям отправлять и получать сообщения электронной почты после того, как размер их почтового ящика достигнет указанного ограничения. Чтобы указать этот лимит, установите флажок и введите размер почтового ящика в ГБ, при превышении которого будет запрещена отправка и получение сообщений, а пользователю

отправлено уведомление. Допустимый интервал значений: от 0 до 2 097 151 МБ (2 ТБ).

- **Хранить удаленные элементы в течение (дней)**: установите этот флажок, чтобы задать количество дней хранения удаленных элементов в почтовом ящике. Допустимый интервал значений: от 0 до 24 855 дней.

- **Хранить удаленные почтовые ящики в течение (дней)**: установите этот флажок, чтобы задать количество дней хранения удаленных почтовых ящиков. Допустимый интервал значений: от 0 до 24 855 дней.

- **Не удаляйте элементы без возможности восстановления, пока не будет создана резервная копия базы данных**. Установите этот флажок, чтобы запретить удаление почтовых ящиков и сообщений электронной почты до тех пор, пока не будет создана резервная копия базы данных почтовых ящиков.

7. Используйте вкладку **Параметры клиента**, чтобы выбрать автономную адресную книгу (OAB) для почтового ящика:

   - **Автономная адресная книга**. Чтобы выбрать автономную адресную книгу, нажмите кнопку **Обзор**, а затем выберите автономную адресную книгу.

Задание свойств базы данных почтовых ящиков в командной консоли Exchange

Пример задания свойств базы данных почтовых ящиков см. в примере 1 в разделе Set-MailboxDatabase.

Как узнать, что этот процесс сработал?

Чтобы убедиться, что атрибуты успешно заданы, выполните следующие задачи:

- Убедитесь, что изменения сохранены в Центре администрирования Exchange.

- В командной консоли Exchange выполните следующую команду, чтобы извлечь сведения о свойствах базы данных почтовых ящиков.

```
PowerShell

Get-MailboxDatabase -Identity MailboxDatabase01 -Status | Format-List
```

Перемещение пути к базе данных почтовых ящиков

Дополнительные сведения о синтаксисе и параметрах см. в разделе Move-DatabasePath.

Перемещение пути к базе данных почтовых ящиков в командной консоли Exchange

Пример задания свойств базы данных почтовых ящиков см. в примере 1 в разделе Move-DatabasePath.

Как узнать, что этот процесс сработал?

Чтобы убедиться, что путь к базе данных успешно перемещен, выполните следующие действия.

1. В EAC выберите **Серверы**>**Базы данных**, а затем щелкните, чтобы выбрать соответствующий почтовый ящик.
2. Щелкните символ **Ручка** и убедитесь, что путь к базе данных является правильным.

Подключение базы данных почтовых ящиков

Дополнительные сведения о синтаксисе и параметрах см. в разделе Mount-Database.

Подключение базы данных в командной консоли Exchange

Пример подключения базы данных почтовых ящиков содержится в примере 1 в разделе Mount-Database.

Как узнать, сработал ли этот процесс?

Чтобы убедиться, что база данных почтовых ящиков успешно подключена, выполните следующую задачу:

- В командной консоли Exchange выполните следующую команду, чтобы извлечь сведения о свойствах всех баз данных почтовых ящиков.

```
PowerShell

Get-MailboxDatabase -IncludePreExchange2013
```

Отключение базы данных почтовых ящиков

Дополнительные сведения о синтаксисе и параметрах см. в разделе Dismount-Database.

Отключение базы данных почтовых ящиков в командной консоли Exchange

Пример отключения базы данных почтовых ящиков содержится в примере 1 в разделе Dismount-Database.

Как узнать, сработал ли этот процесс?

Чтобы убедиться, что база данных успешно отключена, выполните следующие действия.

1. В EAC выберите **Серверы**>**Базы данных**, а затем щелкните, чтобы выбрать соответствующий почтовый ящик.
2. Щелкните символ **Ручка** и убедитесь, что база данных находится в состоянии **Отключено**.

Удаление базы данных почтовых ящиков

Использование Центра администрирования Exchange для удаления базы данных почтовых ящиков

1. В EAC выберите **Серверы**>**Базы данных**, а затем щелкните, чтобы выбрать соответствующий почтовый ящик.
2. Щелкните **значок Удалить** чтобы удалить базу данных почтовых ящиков.

Удаление базы данных почтовых ящиков в командной консоли Exchange

Дополнительные сведения о синтаксисе и параметрах см. в разделе Remove-MailboxDatabase.

1. Выполните следующую команду, чтобы удалить базу данных почтовых ящиков MyDatabase.

   ```
   PowerShell
   ```

   ```
   Remove-MailboxDatabase -Identity "MyDatabase"
   ```

2. При запросе подтверждения выбранного действия введите **Y**.

3. Когда появится диалоговое окно с сообщением об успешном удалении базы данных, обратите внимание на расположение файла базы данных Exchange (EDB). Если вы хотите удалить этот файл с жесткого диска, сделайте это вручную.

Как узнать, сработал ли этот процесс?

Чтобы убедиться, что база данных почтовых ящиков успешно удалена, выполните следующие задачи:

- В EAC выберите **Серверы**>**Базы данных**.
- Убедитесь, что база данных почтовых ящиков удалена.

Управление перемещением локальных почтовых ящиков в Exchange Server

Статья • 04.04.2023

В Exchange Server основные почтовые ящики и архивные почтовые ящики пользователей могут находиться в разных базах данных. *Запрос на перемещение* — это процесс перемещения почтового ящика из одной базы данных почтовых ящиков в другую. *Локальный запрос на перемещение* — это перемещение почтового ящика, которое происходит в пределах одного леса Active Directory (в отличие от запроса на удаленное перемещение, выполняемого между лесами Active Directory). С помощью процедур, описанных в этой статье, вы можете отправлять локальные запросы на перемещение основных и/или архивных почтовых ящиков. С помощью запроса на перемещение вы можете переместить основной почтовый ящик и связанный с ним архив в одну или разные базы данных.

Следующие компоненты обрабатывают запрос на перемещение почтовых ящиков:

- Служба репликации почтовых ящиков Microsoft Exchange (MRS)
- Прокси-сервер службы репликации почтовых ящиков (прокси-сервер MRS)

Процедуры, описанные в этой статье, помогут вам переместить локальные почтовые ящики. Вы можете использовать командную консоль Exchange и Центр администрирования Exchange (EAC) для перемещения почтовых ящиков в локальной организации.

Дополнительные сведения о перемещении почтовых ящиков и прокси-сервере MRS см. в разделе Перемещение почтовых ящиков в Exchange Server.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 20 минут.
- Дополнительные сведения о доступе и использовании Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Разрешения на перемещение и миграцию почтовых ящиков" в разделе Разрешения получателей.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Создание локальных запросов на перемещение

Вы можете создавать локальные запросы на перемещение:

- одного почтового ящика;
- нескольких почтовых ящиков (такие запросы называются *пакетными запросами на перемещение*);
- Несколько почтовых ящиков, указанных в файле с разделяющими запятыми (CSV) (также известный как *пакет миграции*).

При создании локальных запросов на перемещение в Центре администрирования Exchange (для одного или нескольких почтовых ящиков либо по CSV-файлу), запрос виден командлету **Get-MigrationBatch** в Командная консоль Exchange. После выполнения запроса (автоматически или вручную), результаты для каждого почтового ящика будут видны командлету **Get-MoveRequest**.

При создании локальных запросов на перемещение в Командная консоль Exchange для пакетов миграции используется только командлет **New-MigrationBatch** (почтовые ящики указаны в CSV-файле). Чтобы создать локальные запросы на перемещение, которые не используют CSV-файл (отдельные почтовые ящики или запросы на пакетное перемещение), необходимо использовать командлет **New-MoveRequest** , и эти запросы не отображаются в пакетном командлете **Get-MigrationBatch** (или связанных командлетах ***-MigrationBatch***).

Создание локального запроса на перемещение с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел**Миграция**>**получателей**>, щелкните ➕ а затем выберите **Переместить в другую базу данных**.

2. Откроется мастер **локального перемещения почтовых ящиков**. На странице **Выбор пользователей** настройте один из указанных ниже параметров.

   - **Выберите пользователей, которые нужно переместить**. Выберите одного или нескольких пользователей:

     Примечание. Даже если вам нужно переместить только архивный почтовый ящик пользователя, необходимо выбрать его основной почтовый ящик.

     - Щелкните **Добавить**➕ В появившемся диалоговом окне **Выбор почтового ящика** выберите один или несколько почтовых ящиков. После этого нажмите кнопку **ОК**.

     - Чтобы удалить почтовые ящики из списка, выберите почтовый ящик и нажмите кнопку **Удалить**➖

   - **Укажите пользователей с ПОМОЩЬЮ CSV-файла**. Нажмите кнопку **Обзор** и перейдите к расположению файла с разделителями-запятыми (CSV), в котором указываются перемещаемые почтовые ящики. Дополнительные сведения о требованиях к CSV-файлам для локальных запросов на перемещение см. в статье CSV Files for Mailbox Migration.

   - **Разрешить неизвестные столбцы в CSV-файле**:

     - Если этот флажок не установлен, то при перемещении будут игнорироваться (пропускаться без уведомления) неизвестные столбцы CSV-файла (включая необязательные столбцы, в заголовках которых допущены ошибки). Все неизвестные столбцы считаются дополнительными столбцами, которые не используются.

     - Если этот флажок установлен, миграция не выполняется, если в CSV-файле есть неизвестные столбцы. Этот параметр обеспечивает защиту от ошибок правописания в заголовках обязательных и необязательных столбцов, но CSV-файл не может содержать несвязанные столбцы.

   По завершении нажмите кнопку **Далее**.

3. На странице **Конфигурация перемещения** настройте указанные ниже параметры.

    - **Новое имя пакета миграции**. Введите описательное имя для операции перемещения почтового ящика.
    - **Архивировать**: выберите один из следующих параметров:
        - **Переместить основной и архивный почтовые ящики (в случае наличия)**
        - **Переместить только основной почтовый ящик, не перемещать архивный почтовый ящик**
        - **Переместить только архивный почтовый ящик, не перемещать основной почтовый ящик**
    - **Целевая база данных**. Этот параметр влияет на перемещение почтовых ящиков-получателей.
        - Чтобы указать базу данных для основного почтового ящика, нажмите кнопку **Обзор**. Выберите базу данных в открывшемся диалоговом окне **Выбор базы данных почтовых ящиков**.
        - Если база данных не указана, логика автоматического распределения в Exchange выберет произвольную базу данных на сайте Active Directory.
    - **Целевая архивная база данных**. Этот параметр влияет на перемещение архивных почтовых ящиков.
        - Чтобы указать базу данных для архивного почтового ящика, нажмите кнопку **Обзор**. Выберите базу данных в открывшемся диалоговом окне **Выбор базы данных почтовых ящиков**.
        - Если база данных не указана, архивный почтовый ящик перемещается в то же расположение, что и основной.
    - **Ограничение на недопустимые элементы**. Указывает максимальное число поврежденных элементов, разрешенных в почтовом ящике до сбоя запроса. Значение по умолчанию в EAC — 10. Не указывайте здесь значение больше 50. Если вы хотите установить ограничение в 51 или выше, используйте параметр *BadItemLimit* и параметр *AcceptLargeDataLoss* в командной консоли Exchange.

По завершении нажмите кнопку **Далее**.

4. На странице **Запуск обработки пакета** настройте указанные ниже параметры.

    - **После завершения пакета отчет будет отправлен следующим получателям.** По умолчанию используется учетная запись, используемая для перемещения почтовых ящиков. Нажмите кнопку **Обзор**, чтобы добавить или удалить получателей. После этого нажмите кнопку **OK**.
    - **Выберите предпочтительный вариант для запуска пакета**. Выберите один из следующих параметров:
    - **Запустить обработку пакета вручную позже**
    - **Автоматически запустить пакет**. Это значение по умолчанию.
    - **Выберите предпочтительный вариант для завершения пакета**. Выберите один из следующих параметров:
    - **Завершить обработку пакета вручную**
    - **Автоматическое завершение пакета миграции**. Это значение по умолчанию.

    По завершении нажмите кнопку **Создать**.

Создание локального запроса на перемещение одного или нескольких почтовых ящиков с помощью командной консоли Exchange

В локальном запросе на перемещение отдельного почтового ящика используется командлет **New-MailboxMove**. Однако в локальном запросе на перемещение нескольких почтовых ящиков, указанных не с помощью CSV-файла, также используется командлет **New-MailboxMove**. Локальный запрос на перемещение нескольких почтовых ящиков без использования CSV-файла также называется *пакетным запросом на перемещение*.

Чтобы создать локальный запрос на перемещение отдельного почтового ящика, используйте следующий синтаксис:

PowerShell

```
New-MoveRequest "<DescriptiveName>"] -Identity <MailboxIdentity> [<-
ArchiveOnly | -PrimaryOnly>] [-TargetDatabase <DatabaseIdentity>] [-
```

```
ArchiveTargetDatabase<DatabaseIdentity>] [-Priority <PriorityValue>] [-
BadItemLimit <Value>] [-AcceptLargeDataLoss]
```

В этом примере создается локальный запрос на перемещение со следующими параметрами:

- **Почтовый ящик**: основной почтовый ящик и архивный почтовый ящик (если он существует) для Анжелы Грубер (agruber@contoso.com). Если вы хотите переместить только основной почтовый ящик, используйте параметр *PrimaryOnly* . Если вы хотите переместить только архивный почтовый ящик, используйте параметр *ArchiveOnly* .
- **Целевая база данных для основного почтового ящика**: MBX DB02. Если мы не используем параметр *TargetDatabase* , логика автоматического распространения в Exchange случайным образом выберет базу данных на сайте Active Directory.
- **Целевая база данных для архивного почтового ящика**: MBX DB03. Если не использовать параметр *ArchiveTargetDatabase* или параметр *PrimaryOnly* , база данных архивного почтового ящика будет перемещена в ту же базу данных, что и основной почтовый ящик.

  Если мы используем параметр *ArchiveOnly* без параметра *ArchiveTargetDatabase* , логика автоматического распространения в Exchange случайным образом выберет базу данных на сайте Active Directory.
- **Priority**: `Normal`, так как мы не используем параметр *Priority* .
- **Ограничение на недопустимый элемент**: 10 (значение по умолчанию в командной консоли Exchange равно 0). Так как значение меньше 51, нам не нужно использовать `AcceptLargeDataLoss` параметр .

PowerShell

```
New-MoveRequest -Identity agruber@contoso.com -TargetDatabase "MBX 02" -
ArchiveTargetDatabase "MBX 03" -BadItemLimit 10
```

В этом примере используются похожие параметры, но перемещается только основной почтовый ящик пользователя.

PowerShell

```
New-MoveRequest -Identity agruber@contoso.com -PrimaryOnly -TargetDatabase
"MBX 02" -BadItemLimit 10
```

В этом примере используются похожие параметры, но перемещается только архивный почтовый ящик пользователя.

PowerShell

```
New-MoveRequest -Identity agruber@contoso.com -ArchiveOnly -
ArchiveTargetDatabase "MBX 03" -BadItemLimit 10
```

Подробные сведения о синтаксисе и параметрах см. в статье New-MoveRequest.

Как правило, для пакетного запроса на перемещение используется практически такой же синтаксис, как для запроса на перемещение одного почтового ящика. Основные отличия:

- Параметр *Identity* не используется для указания почтового ящика. Вместо этого используется командлет **Get-Mailbox** или **Get-User**, чтобы создать список перемещаемых почтовых ящиков, а результаты отправляются в командлет **New-MoveRequest**.
- Присвойтие пакету имя перемещения с помощью параметра *BatchName* .

В этом примере создается пакетный запрос на перемещение со следующими параметрами:

- **Почтовые ящики для перемещения**: все почтовые ящики в базе данных с именем MBX DB01.
- **Имя пакета**: MBX DB01 — MBX DB02.
- **Целевая база данных**: MBX DB02. Если бы мы не использовали параметр *TargetDatabase* , логика автоматического распределения в Exchange случайным образом выбирает базы данных на сайте Active Directory.
- **Целевая база данных для архивных почтовых ящиков**: MBX DB02. Так как мы не используем параметр *ArchiveTargetDatabase* или параметр *PrimaryOnly* , база данных архивного почтового ящика перемещается в ту же базу данных, что и основной почтовый ящик.

  Если мы используем параметр *ArchiveOnly* без параметра *ArchiveTargetDatabase* , логика автоматического распространения в Exchange будет случайным образом выбирать базы данных на сайте Active Directory.
- **Приоритет**: `High`

- **Ограничение на недопустимый элемент**: 51 (значение по умолчанию в командной консоли Exchange равно 0), поэтому необходимо также использовать параметр *AcceptLargeDataLoss* .

PowerShell

```
Get-Mailbox -Database "MBX DB01" | New-MoveRequest -BatchName "MBX DB01 to
MBX DB02" -TargetDatabase "MBX DB02" -Priority High -BadItemLimit 51 -
AcceptLargeDataLoss
```

Подробные сведения о синтаксисе и параметрах см. в разделе New-MoveRequest.

Создание локального запроса на перемещение из CSV-файла с помощью командной консоли Exchange

Локальный запрос на перемещение почтовых ящиков, указанных в CSV-файле, называется *пакетом миграции* и использует командлет **New-MigrationBatch** .

Дополнительные сведения о требованиях к CSV-файлам для локальных запросов на перемещение см. в статье CSV Files for Mailbox Migration.

> ⓘ **Примечание**
>
> Все почтовые ящики, указанные в CSV-файле, будут перенесены, даже если они находятся за пределами области RBAC (например, подразделения), что дает администратору разрешения на перенос почтовых ящиков.

Чтобы создать пакет миграции, используйте следующий синтаксис:

PowerShell

```
New-MigrationBatch -Local [-AutoStart] [-AutoComplete] -Name "
<MigrationBatchName>" -CSVData
([System.IO.File]::ReadAllBytes('<PathAndFileName>')) [<-ArchiveOnly | -
PrimaryOnly>] [-TargetDatabases "<MailboxDatabase1>","<MailboxDatabase1>"...
[-TargetArchiveDatabases "<MailboxDatabase1>","<MailboxDatabase1>"...] [-
Priority <PriorityValue>] [-BadItemLimit <Value>] [-AcceptLargeDataLoss]
```

В этом примере создается пакет миграции со следующими параметрами:

- **CSV-файл, указывающий перемещаемые почтовые ящики**: C:\Users\Administrator\Desktop\LocalMove 01.csv. Если вы хотите переместить только основной почтовый ящик, используйте параметр *PrimaryOnly* или

значение `PrimaryOnly` **MailboxType** в CSV-файле. Если вы хотите переместить только архивный почтовый ящик, используйте параметр *ArchiveOnly* или значение `ArchiveOnly` **MailboxType** в CSV-файле.

- **Имя пакета**: LocalMove 01.
- **Целевая база данных**: MBX DB02. Если мы не используем параметр *TargetDatabase* , а базы данных-получатели почтовых ящиков не указаны в CSV-файле, логика автоматического распределения в Exchange случайным образом выбирает базы данных на сайте Active Directory.
- **Целевая база данных для архивных почтовых ящиков**: MBX DB02. Так как мы не используем параметр *ArchiveTargetDatabase* (в команде или CSV-файле), база данных архивного почтового ящика перемещается в ту же базу данных, что и основной почтовый ящик.

  Если мы используем параметр *ArchiveOnly* (в команде или CSV-файле) без использования параметра *ArchiveTargetDatabase* (в команде или CSV-файле), логика автоматического распространения в Exchange будет случайным образом выбирать базы данных на сайте Active Directory.
- **Когда следует начать миграцию**: немедленно, так как мы используем параметр *автозапуска* . Если этот параметр не используется, необходимо использовать командлет **Start-MigrationBatch** , чтобы запустить пакет миграции после его создания.
- **Когда следует завершить миграцию**: после завершения начальной синхронизации почтовых ящиков, так как мы используем параметр *Автозаполнения* . Если этот параметр не используется, необходимо использовать командлет **Complete-MigrationBatch** , чтобы запустить пакет миграции после его создания.
- **Priority**: `Normal`, так как мы не используем параметр *Priority* .
- **Ограничение на недопустимый элемент**: 10 (значение по умолчанию в командной консоли Exchange равно 0). Так как значение меньше 51, нам не нужно использовать `AcceptLargeDataLoss` параметр .

PowerShell

```
New-MigrationBatch -Local -AutoStart -AutoComplete -Name "LocalMove 01" -
CSVData
([System.IO.File]::ReadAllBytes("C:\Users\Administrator\Desktop\LocalMove
01.csv")) -TargetDatabases "MBX DB02" -BadItemLimit 10
```

Как проверить, все ли получилось?

Чтобы убедиться, что локальный запрос на перемещение успешно создан, выполните одно из указанных ниже действий.

- В EAC перейдите в раздел **Миграция получателей**> и проверьте состояние запроса на перемещение (обратите внимание, что может потребоваться нажать Вы можете выбрать запрос на перемещение и просмотреть дополнительные сведения в области сведений или щелкнув
- В EAC перейдите в раздел **Миграция получателей**> и щелкните **Состояние для всех пакетов**.
- Проверьте текст уведомления. Отправитель — Microsoft Outlook. По завершении запроса на перемещение вы получите сообщение с темой `Migration batch <MigrationBatchName> has completed successfully`.
- В Центре администрирования Майкрософт щелкните средства просмотра уведомлений. Чтобы просмотреть состояние запроса.
- В командной консоли Exchange *замените*< *MailboxIdentity*> именем, адресом электронной почты или псевдонимом почтового ящика и выполните следующую команду, чтобы проверить основные значения свойств:

  PowerShell

  ```
  Get-MoveRequest -Identity <MailboxIdentity> | Format-List
  DisplayName,Alias,Status,*database*
  ```

- В командной консоли Exchange замените <*BatchName*> значением имени пакета запроса на перемещение и выполните следующую команду, чтобы проверить основные значения свойств:

  PowerShell

  ```
  Get-MoveRequest -BatchName <BatchName> | Format-List
  DisplayName,Alias,Status,*database*
  ```

  Примечание. Если вы создали запрос на перемещение в EAC, имя пакета будет иметь `MigrationService:<BatchNameValueFromTheEAC>`значение .

- Если вы создали запрос на перемещение в EAC, замените <*BatchName*> указанным значением имени пакета и выполните следующую команду в

командной консоли Exchange, чтобы проверить сводные сведения обо всех почтовых ящиках при перемещении:

```
PowerShell

Get-MigrationUserStatistics -BatchId <BatchName>
```

- Если вы создали запрос на перемещение в EAC, замените *<EmailAddress адресом электронной почты>* перемещенного почтового ящика и выполните следующую команду, чтобы просмотреть подробные сведения о указанном почтовом ящике:

```
PowerShell

Get-MigrationUserStatistics -Identity <EmailAddress> | Format-List
```

Подробнее см. в разделе Get-MigrationUserStatistics.

Отображение пакетов миграции

Пример отображения пакета миграции с помощью командной консоли Exchange см. в примере 2 из статьи Get-MigrationBatch.

Создание межлесного перемещения с помощью пакетного CSV-файла

В этом примере настраивается конечная точка миграции, а затем создается межлесное перемещение — из исходного в целевой лес — с помощью CSV-файла.

```
PowerShell

New-MigrationEndpoint -Name Fabrikam -ExchangeRemote -Autodiscover -
EmailAddress tonysmith@fabrikam.com -Credentials (Get-Credential
fabrikam\tonysmith)
$csvData=
[System.IO.File]::ReadAllBytes("C:\Users\Administrator\Desktop\batch.csv")
New-MigrationBatch -CSVData $csvData -Timezone "Pacific Standard Time" -Name
FabrikamMerger -SourceEndpoint Fabrikam -TargetDeliveryDomain
"mail.contoso.com"
```

Дополнительные сведения о подготовке леса к межлесному перемещению см. в следующих разделах.

- Подготовка почтовых ящиков для запросов на перемещение между лесами
- Prepare Mailboxes for Cross-Forest Moves Using Sample Code
- Подготовка почтовых ящиков к перемещению между лесами с помощью командной консоли Exchange

Подробные сведения о синтаксисе и параметрах см. в разделах New-MigrationBatch и New-MoveRequest.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно завершили миграцию, выполните следующие действия.

- В командной консоли Exchange выполните приведенную ниже команду, чтобы получить сведения о перемещении почтовых ящиков.

```
PowerShell

Get-MigrationUserStatistics -Identity BatchName -Status | Format-List
```

Подробнее см. в разделе Get-MigrationUserStatistics.

Подготовка почтовых ящиков для запросов на перемещение между лесами в Exchange Server

Статья • 04.04.2023

Перемещение почтовых ящиков и миграция почтовых ящиков в Exchange 2016 и Exchange 2019 из одного леса в другой требуют подготовки целевого леса, что упрощается с помощью средств и командлетов Exchange. Exchange 2016 поддерживает перемещение и миграцию почтовых ящиков с помощью командной консоли Exchange, в частности командлетов **New-MoveRequest** и **New-MigrationBatch** . Вы также можете переместить почтовый ящик в Центре администрирования Exchange (EAC).

Чтобы переместить почтовый ящик Exchange из исходного леса в целевой лес Exchange 2016 или Exchange 2019, целевой лес должен содержать допустимого почтового пользователя (также известного как пользователь с поддержкой почты) с указанным набором атрибутов Active Directory.

- В Exchange 2016 можно переместить почтовый ящик Exchange 2010, Exchange 2013 или Exchange 2016 из исходного леса Exchange в целевой лес Exchange 2016. Если в целевом лесу есть хотя бы один сервер почтовых ящиков Exchange 2016, лес считается лесом Exchange 2016.

- В Exchange 2019 можно переместить почтовый ящик Exchange 2013, Exchange 2016 или Exchange 2019 из исходного леса Exchange в целевой лес Exchange 2019. Если в целевом лесу есть хотя бы один сервер почтовых ящиков Exchange 2019, лес считается лесом Exchange 2019.

Чтобы подготовиться к перемещению почтового ящика, необходимо создать почтовых пользователей (также известных как пользователи с поддержкой почты) с необходимыми атрибутами Active Directory в целевом лесу. Существует два рекомендуемых подхода для создания пользователей почты с необходимыми атрибутами:

- Если вы развернули Диспетчер жизненного цикла удостоверений (ILM) для синхронизации глобального списка адресов между лесами, рекомендуется использовать Microsoft Identity Manager 2016 с пакетом обновления 1 (SP1). Мы создали пример кода, который можно использовать для обучения настройке ILM на синхронизацию исходного пользователя почты и целевого пользователя почты.

Дополнительные сведения, включая сведения о загрузке примера кода, см. в разделе Подготовка почтовых ящиков для перемещения между лесами с помощью примера кода.

- Если вы создали целевого почтового пользователя с помощью средства Active Directory, отличного от ILM или Microsoft Identity Integration Server (MIIS), используйте командлет **Update-Recipient** с параметром *Identity* , чтобы создать атрибут **LegacyExchangeDN** для целевого почтового пользователя. Мы создали пример скрипта PowerShell, который выполняет чтение и запись в Active Directory и вызывает командлет **Update-Recipient** .

  Дополнительные сведения об использовании примера сценария см. в статье Подготовка почтовых ящиков к перемещению между лесами с помощью командной консоли Exchange.

После создания целевого почтового пользователя можно выполнить командлеты **New-MoveRequest** или **New-MigrationBatch** , чтобы переместить почтовый ящик в целевой лес Exchange 2016 или Exchange 2019.

Дополнительные сведения об удаленных запросах на перемещение см. в следующих разделах:

- New-MigrationBatch
- New-MoveRequest

В оставшейся части этого раздела описываются атрибуты Active Directory пользователя почты, необходимые для перемещения почтового ящика. Эти атрибуты настраиваются во время использования кода или сценария для подготовки перемещения почтового ящика. Однако их можно также скопировать вручную с помощью редактора Active Directory.

Атрибуты пользователя Active Directory, необходимые для перемещения почтового ящика

Для поддержки удаленного перемещения почтового ящика объект пользователя почты в целевом лесу Exchange должен иметь атрибуты Active Directory, описанные в этом разделе:

- Обязательные атрибуты
- Необязательные атрибуты

- Связанные атрибуты
- Атрибуты связанного пользователя
- Атрибуты почтового ящика ресурсов
- Дополнительные атрибуты

Обязательные атрибуты

В следующей таблице перечислен минимальный набор атрибутов, которые необходимо настроить в ILM для целевого пользователя почты, чтобы командлет **New-MoveRequest** работал правильно.

Атрибуты пользователя почты

Атрибут Active Directory	Действие
displayName	Скопируйте соответствующий атрибут исходного почтового ящика или создайте новое значение.
Mail	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
mailNickname	Скопируйте соответствующий атрибут исходного почтового ящика или создайте новое значение.
msExchArchiveGUID and msExchArchiveName	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchMailboxGUID	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchRecipientDisplayType	-2147483642 десятичное число (эквивалентно 0x80000006 шестнадцатеричной).
msExchRecipientTypeDetails	128 десятичное число (0x80 шестнадцатеричное число).
msExchUserCulture	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchVersion	44220983382016 (десятичный формат).
cn	Скопируйте соответствующий атрибут исходного почтового ящика или создайте новое значение.

Атрибут Active Directory	Действие
proxyAddresses	Скопируйте атрибут **proxyAddresses** исходного почтового ящика. Кроме того, скопируйте значение **LegacyExchangeDN** исходного почтового ящика в качестве адреса X500 в атрибут **proxyAddresses** целевого пользователя почты. **Примечание**. **ProxyAddresses** пользователя исходного почтового ящика должен содержать SMTP-адрес, соответствующий полномочного домена целевого леса. Это позволяет командлету **New-MoveRequest** правильно выбрать **targetAddress** исходного пользователя с включенной поддержкой почты (преобразуемого из пользователя исходного почтового ящика после выполнения запроса на перемещение почтового ящика) для проверки работы маршрутизации почты.
Samaccountname	Скопируйте соответствующий атрибут исходного почтового ящика или создайте новое значение. Убедитесь в том, что данное значение является уникальным в пределах домена целевого леса, к которому относится целевой пользователь почты.
Targetaddress	Задайте адрес SMTP в атрибуте **proxyAddresses** исходного почтового ящика. Этот адрес SMTP должен относиться к заслуживающему доверия домену исходного леса.
userAccountControl	Константная: 514 (эквивалент 0x202, ACCOUNTDISABLE | NORMAL_ACCOUNT).
userPrincipalName.	Скопируйте соответствующий атрибут исходного почтового ящика или создайте новое значение. Поскольку пользователю запрещен вход, данное значение **userPrincipalName** не используется.

Необязательные атрибуты

Для правильной работы командлета **New-MoveRequest** следующие атрибуты не требуются. однако их синхронизация обеспечивает более эффективное взаимодействие с пользователем после перемещения почтового ящика. Поскольку глобальный список адресов в целевом лесе отображает данного целевого пользователя почты, необходимо задать следующие атрибуты для глобального списка адресов.

Атрибуты, связанные с глобальным списком адресов

Атрибут Active Directory пользователя почты	Действие
c	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
co	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
countryCode	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
company	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
department	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
facsimileTelephoneNumber	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
givenName;	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
homePhone	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
info	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
initials	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
l	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
mobile	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchAssistantName	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchHideFromAddressLists	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
otherHomePhone	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
otherTelephone	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.

Атрибут Active Directory пользователя почты	Действие
pager	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
physicalDeliveryOfficeName	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
postalCode	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
sn	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
st	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
streetAddress	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
телефонAssistant	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
telephoneNumber	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
title	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.

Связанные атрибуты

Связанный атрибут — это атрибут Active Directory, который ссылается на другие объекты Active Directory в локальном лесу. Значения связанных атрибутов нельзя напрямую скопировать из почтового ящика в исходном лесе для пользователя почты в целевом лесе. Вместо этого выполните следующие действия.

1. Найдите объекты Active Directory в исходном лесу, на который ссылается атрибут исходного почтового ящика.
2. Найдите соответствующие объекты Active Directory в целевом лесу.
3. Задайте атрибут целевого почтового пользователя для ссылки на объекты Active Directory в целевом лесу.

Связанные атрибуты

Атрибут Active Directory пользователя почты	Действие
altRecipient	Соответствует атрибуту **altRecipient** исходного почтового ящика.
deliverAndRedirect	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика. Данный атрибут является логическим значением, которое необходимо задать вместе с **altRecipient**.
Manager (и его обратные ссылки)	Соответствует атрибуту manager исходного почтового ящика.
MemberOf (обратные ссылки)	Это обратная ссылка атрибута члена группы.
publicDelegates (и его обратные ссылки)	Соответствует атрибуту **publicDelegates** исходного почтового ящика.

Атрибуты связанного пользователя

Если вы хотите переместить почтовый ящик в лес ресурсов Exchange, почтовый ящик в лесу ресурсов считается *связанным почтовым ящиком*. В данном сценарии необходимо создать связанного пользователя почты в (целевом) лесе ресурсов. Чтобы создать связанного пользователя почты, необходимо задать атрибуты, указанные в следующей таблице.

Атрибуты связанного пользователя почты

Атрибут Active Directory	Действие
msExchMasterAccountHistory	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchMasterAccountSid	Если у исходного почтового ящика есть атрибут **msExchMasterAccountSid**, скопируйте его. В противном случае скопируйте атрибут **objectSid** исходного почтового ящика.
msExchRecipientDisplayType	Constant:-1073741818 decimal (эквивалент).`*unsigned* 0xC0000006`

Примечание

Связанный почтовый ящик можно создать только при наличии доверия между исходным и целевым лесом.

Если исходный объект отключен, а атрибут **msExchMasterAccountSid** установлен сам на себя (почтовый ящик ресурсов, общий почтовый ящик), не делайте пометок для целевого пользователя.

Если исходный объект отключен, а атрибут **msExchMasterAccountSid** не задан, то данный почтовый ящик не является допустимым.

Если исходный объект включен, а атрибут **msExchMasterAccountSid** задан, то данный почтовый ящик не является допустимым.

Атрибуты почтового ящика ресурсов

Если вы хотите переместить почтовый ящик ресурса в лес Exchange, необходимо задать атрибуты, показанные в следующей таблице, для целевого почтового пользователя.

Атрибуты почтового ящика ресурсов

Атрибут Active Directory пользователя почты	Действие
msExchRecipientDisplayType	Если исходный почтовый ящик является конференц-залом: Константная: -2147481850 десятичное число (эквивалентно `*unsigned* 0x80000706`). Если исходный почтовый ящик является почтовым ящиком оборудования: константная: -2147481594 десятичное число (эквивалентно `*unsigned* 0x80000806`).
msExchResourceCapacity	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchResourceDisplay	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchResourceMetaData	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchResourceSearchProperties	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.

Дополнительные атрибуты

Атрибуты почтового ящика ресурсов

Атрибуты Active Directory пользователя почты	Описание
comment	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
deletedItemFlags	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
delivContLength	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
departmentNumber	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
description	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
division	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
Employeeid	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
employeeNumber	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
employeeType	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
extensionAttribute1-15	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
homePostalAddress	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
internationalISDNNumber	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.

Атрибуты Active Directory пользователя почты	Описание
ipPhone	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
language	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
lmPwdHistory	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
Localeid	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
mAPIRecipient	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
middleName	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msDS-PhoneticCompanyName	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msDS-PhoneticDepartment	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msDS-PhoneticDisplayName	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msDS-PhoneticFirstName	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msDS-PhoneticLastName	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchBlockedSendersHash	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.

Атрибуты Active Directory пользователя почты	Описание
msExchELCExpirySuspensionEnd	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchELCExpirySuspensionStart	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchELCMailboxFlags	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchExternalOOFOptions	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchMessageHygieneFlags	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchMessageHygieneSCLDeleteThreshold	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchMessageHygieneSCLJunkThreshold	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchMessageHygieneSCLQuarantineThreshold	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchMessageHygieneSCLRejectThreshold	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchMDBRulesQuota	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchPoliciesExcluded	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchSafeRecipientsHash	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.

Атрибуты Active Directory пользователя почты	Описание
msExchSafeSendersHash	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
msExchUMSpokenName	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
otherFacsimileTelephoneNumber	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
otherIpPhone	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
otherMobile	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
otherPager	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
preferredDeliveryMethod	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
personalPager	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
personalTitle	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
photo	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
pOPCharacterSet	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
pOPContentFormat	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.

Атрибуты Active Directory пользователя почты	Описание
postalAddress	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
postOfficeBox	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
primaryInternationalISDNNumber	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
primaryTelexNumber	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
showInAdvancedViewOnly	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
street	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
terminalServer	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
textEncodedORAddress	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
thumbnailLogo	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
thumbnailPhoto	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
url	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
userCert	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.

Атрибуты Active Directory пользователя почты	Описание
userCertificate	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
userSMIMECertificate	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.
wWWHomePage	Непосредственно скопируйте соответствующий атрибут исходного почтового ящика.

Подготовка почтовых ящиков к перемещению между лесами с помощью командной консоли Exchange

Статья • 04.04.2023

Exchange Server поддерживает перемещение и миграцию почтовых ящиков с помощью командлетов **New-MoveRequest** и **New-MigrationBatch** командной консоли Exchange. Вы также можете переместить почтовый ящик в Центре администрирования Exchange (EAC).

- В Exchange 2016 можно переместить почтовый ящик Exchange 2010, Exchange 2013 или Exchange 2016 из исходного леса Exchange в целевой лес Exchange 2016.
- В Exchange 2019 можно переместить почтовый ящик Exchange 2013, Exchange 2016 или Exchange 2019 из исходного леса Exchange в целевой лес Exchange 2019.

Чтобы выполнить командлеты **New-MoveRequest** и **New-MigrationBatch**, пользователь почты должен существовать в конечном лесу Exchange и этого пользователя должен быть минимальный набор требуемых атрибутов Active Directory.

Пример сценария Exchange PowerShell, описанный в этом разделе, поддерживает эту задачу путем синхронизации пользователей почтовых ящиков из исходного леса Exchange с целевыми лесами Exchange в качестве почтовых пользователей (также известных как пользователи с поддержкой почты). Скрипт копирует атрибуты Active Directory пользователей почтовых ящиков в исходном лесу в целевой лес, а затем использует командлет **Update-Recipient** для преобразования целевых объектов в почтовых пользователей.

Дополнительные сведения об использовании и написании скриптов см. в разделе О скриптах. Дополнительные сведения о подготовке к перемещению между лесами см. в разделе Подготовка почтовых ящиков к запросам на перемещение между лесами.

Ищете другие задачи управления, связанные с запросами на удаленное перемещение? См. раздел Управление перемещением локальных почтовых ящиков в Exchange Server.

Что нужно знать перед началом работы

- Найдите скрипт Prepare-MoveRequest.ps1 в папке %ExchangeInstallPath%Scripts. По умолчанию %ExchangeInstallPath% имеет значение C:\Program Files\Microsoft\Exchange Server\V15\ (обратите внимание на значение "\").

- Для выполнения этого примера сценария необходимы следующие компоненты:

  - Исходный лес Exchange (где сейчас находится почтовый ящик).

    - Для целевых лесов Exchange 2016 исходный почтовый ящик может находиться в Exchange 2010, Exchange 2013 или Exchange 2016.

    - Для целевых лесов Exchange 2019 исходный почтовый ящик может находиться в Exchange 2013, Exchange 2016 или Exchange 2019.

  - Целевой лес с установленным Exchange 2016 или Exchange 2019 (куда будет перемещен почтовый ящик).

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование сценария Prepare-MoveRequest.ps1 для подготовки почтовых ящиков к перемещениям между лесами

Запустите скрипт из командной консоли Exchange на сервере почтовых ящиков в целевом лесу Exchange 2016 или Exchange 2019. Сценарий выполнит копирование атрибутов почтового ящика из исходного леса.

Чтобы назначить определенные учетные данные проверки подлинности для удаленного контроллера домена леса, необходимо сначала запустить командлет Windows PowerShell **Get-Credential** и сохранить входные данные пользователя во временной переменной. При выполнении командлета **Get-Credential** он запрашивает имя пользователя и пароль учетной записи, используемой при проверке подлинности на контроллере домена удаленного леса. Затем можно

использовать временную переменную в сценарии Prepare-MoveRequest.ps1. Дополнительные сведения о командлете **Get-Credential** см. в разделе Get-Credential.

> ⓘ **Примечание**
>
> Убедитесь, что при вызове этого сценария для локального и удаленного лесов используются различные учетные данные.

1. Выполните следующие команды, чтобы получить учетные данные локального и удаленного лесов.

```
PowerShell
$LocalCredentials = Get-Credential
```

```
PowerShell
$RemoteCredentials = Get-Credential
```

2. Выполните следующие команды, чтобы передать эти учетные данные в параметры *LocalForestCredential* и *RemoteForestCredential* в скрипте Prepare-MoveRequest.ps1.

```
PowerShell
Prepare-MoveRequest.ps1 -Identity JohnSmith@Fabrikan.com -
RemoteForestDomainController DC001.Fabrikam.com -RemoteForestCredential
$RemoteCredentials -LocalForestDomainController DC001.Contoso.com -
LocalForestCredential $LocalCredentials
```

Набор параметров скрипта

В следующей таблице указан набор параметров для этого сценария.

Параметр	Обязательный	Описание

Параметр	Обязательный	Описание
Identity	Обязательный	Параметр *Identity* однозначно определяет почтовый ящик в исходном лесу. Идентификатор может быть любым из следующих значений: общее имя (CN), псевдоним, свойство **proxyAddress** , свойство **objectGuid** или **свойство DisplayName** .
RemoteForestCredential	Обязательный	Параметр *RemoteForestCredential* указывает администратора, который имеет разрешения на копирование данных из исходного леса Active Directory.
RemoteForestDomainController	Обязательный	Параметр *RemoteForestDomainController* указывает контроллер домена в исходном лесу, где находится почтовый ящик.
DisableEmailAddressPolicy	Необязательный	Параметр *DisableEmailAddressPolicy* указывает, следует ли отключить политику адресов Email (EAP) при создании объекта **MailUser** в целевом лесу. При указании этого параметра политика адресов электронной почты не будет применяться в целевом лесу. **Примечание.** При указании этого параметра объект **MailUser** не будет иметь сопоставления адресов электронной почты в локальном домене леса. Обычно он отмечается с помощью политики адресов электронной почты.
LinkedMailUser	Необязательный	Параметр *LinkedMailUser* указывает, следует ли создать связанный MailUser в локальном лесу для пользователя почтового ящика в удаленном лесу. При указании этого параметра согласно сценарию создается целевой объект **MailUser**, связанный с исходным почтовым ящиком. Если этот параметр не указан, то по сценарию создается обычный целевой объект **MailUser**.

Параметр	Обязательный	Описание
LocalForestCredential	Необязательный	Параметр *LocalForestCredential* указывает администратора с разрешениями на запись данных в целевой лес Active Directory. Рекомендуется указать этот параметр явным образом, чтобы избежать проблем с разрешениями Active Directory. Если в удаленном и локальном лесах настроено отношение доверия, не используйте учетную запись пользователя из удаленного леса в качестве учетных данных локального леса, даже если учетная запись удаленного пользователя имеет разрешение на изменение службы каталогов Active Directory в локальном лесу.
LocalForestDomainController	Необязательный	Параметр *LocalForestDomainController* указывает контроллер домена в целевом лесу, где будет создан почтовый пользователь. Рекомендуется указать этот параметр, чтобы избежать возможных проблем с задержкой репликации контроллера домена в локальном лесу, которые могут произойти при выборе случайного контроллера домена.
MailboxDeliveryDomain	Необязательный	Параметр *MailboxDeliveryDomain* указывает полномочный домен исходного леса, чтобы скрипт смог выбрать правильное свойство **proxyAddress** пользователя исходного почтового ящика в качестве свойства **targetAddress** целевого почтового ящика пользователя. По умолчанию основной SMTP-адрес пользователя исходного почтового ящика устанавливается в качестве свойства **targetAddress** целевого почтового пользователя.

Параметр	Обязательный	Описание
OverWriteLocalObject	Необязательный	Параметр *OverWriteLocalObject* используется для пользователей, созданных средством миграции Active Directory. При этом свойства существующего почтового контакта копируются для нового почтового пользователя. После этого сценарий также копирует для нового почтового пользователя свойства пользователя исходного леса.
TargetMailUserOU	Необязательный	Параметр *TargetMailuserOU* указывает подразделение, в котором будет создан целевой почтовый пользователь.
UseLocalObject	Необязательный	Параметр *UseLocalObject* указывает, следует ли преобразовать существующий локальный объект в требуемого целевого почтового пользователя, если скрипт обнаруживает объект в локальном лесу, конфликтующий с создаваемым пользователем почты.

Примеры

В этом разделе приведено несколько примеров возможного использования сценария Prepare-MoveRequest.ps1.

Пример. Один связанный почтовый пользователь

В этом примере подготавливается один связанный почтовый пользователь в локальном лесу при наличии доверия между удаленным лесом и локальным лесом.

1. Выполните следующие команды, чтобы получить учетные данные локального и удаленного лесов.

```
PowerShell
```

```
$LocalCredentials = Get-Credential
```

```
PowerShell
```

```
$RemoteCredentials = Get-Credential
```

2. Выполните следующую команду, чтобы передать эти учетные данные в параметры *LocalForestCredential* и *RemoteForestCredential* в скрипте Prepare-MoveRequest.ps1.

```
PowerShell

Prepare-MoveRequest.ps1 -Identity JamesAlvord@Contoso.com -
RemoteForestDomainController DC001.Fabrikam.com -RemoteForestCredential
$RemoteCredentials -LocalForestDomainController DC001.Contoso.com -
LocalForestCredential $LocalCredentials -LinkedMailUser
```

Пример. Конвейеризация

В этом примере иллюстрируется поддержка конвейерного режима при указании списка идентификаторов почтового ящика.

1. Выполните следующую команду.

```
PowerShell

$UserCredentials = Get-Credential
```

2. Выполните следующую команду, чтобы передать учетные данные в параметр *RemoteForestCredential* в скрипте Prepare-MoveRequest.ps1.

```
PowerShell

"IanP@Contoso.com", "JoeAn@Contoso.com" | Prepare-MoveRequest.ps1 -
RemoteForestDomainController DC001.Fabrikam.com -RemoteForestCredential
$UserCredentials
```

Пример. Использование файла .csv для массового создания пользователей почты

Вы можете создать файл .csv, содержащий список удостоверений почтовых ящиков из исходного леса, что позволяет передать содержимое этого файла в скрипт для массового создания целевых пользователей почты.

Например, CSV-файл может иметь следующее содержимое:

```
PowerShell

Identity
Ian@contoso.com
```

```
John@contoso.com
Cindy@contoso.com
```

В этом примере вызывается файл .csv для массового создания целевых почтовых пользователей.

1. Выполните следующую команду, чтобы получить учетные данные леса.

   PowerShell

   ```
   $UserCredentials = Get-Credential
   ```

2. Выполните следующую команду, чтобы передать эти учетные данные в параметр *RemoteForestCredential* в сценарии Prepare-MoveRequest.ps1.

   PowerShell

   ```
   Import-Csv Test.csv | Prepare-MoveRequest.ps1 -
   RemoteForestDomainController DC001.Fabrikam.com -RemoteForestCredential
   $UserCredentials
   ```

Поведение скрипта в зависимости от конечного объекта

В этом разделе описывается выполнение скрипта по отношению к нескольким сценариям для конечных объектов.

Дублирование целевого объекта с включенной поддержкой почты

Когда скрипт пытается создать целевого почтового пользователя из исходного почтового ящика и обнаруживает дубликат локального объекта с поддержкой почты, он использует следующую логику:

- Если атрибут **masterAccountSid** пользователя исходного почтового ящика соответствует какому-либо атрибуту **objectSid** или **masterAccountSid** целевого объекта, то:
  - Если целевой объект не включен по почте, скрипт возвращает ошибку, так как скрипт не поддерживает преобразование объекта, который не поддерживает почту, в почтовый пользователь.

    - Если для целевого объекта включена поддержка почты, он является дубликатом.

- Если адрес в свойствах **proxyAddress** (только smtp/x500) пользователя исходного почтового ящика соответствует адресу в свойствах **proxyAddress** (только smtp/x500) целевого объекта, то целевой объект является дубликатом.

Сценарий запрашивает пользователя о дубликатах объектов.

Если целевой объект с поддержкой почты является почтовым пользователем или почтовым контактом, который, скорее всего, создается при развертывании синхронизации глобального списка адресов между лесами, можно снова запустить скрипт с параметром *UseLocalObject* , чтобы использовать целевой объект с поддержкой почты для миграции почтовых ящиков.

Пользователь почты

Если целевой объект является почтовым пользователем, скрипт копирует следующие атрибуты из исходного пользователя почтового ящика в целевой почтовый ящик:

- **msExchMailboxGUID**
- **msExchArchiveGUID**
- **msExchArchiveName**

Если задан параметр *LinkedMailUser* , скрипт копирует атрибут source **objectSid** / **masterAccountSid** .

Почтовый контакт

Если целевой объект является почтовым контактом, скрипт удаляет существующий контакт и копирует все его атрибуты новому почтовому пользователю. Сценарий также копирует следующие атрибуты пользователя исходного почтового ящика:

- **msExchMailboxGUID**
- **msExchArchiveGUID**
- **msExchArchiveName**
- **Samaccountname**

- **userAccountControl** (задано значение 514; эквивалент)`0x202, ACCOUNTDISABLE | NORMAL_ACCOUNT`
- **userPrincipalName.**

Если задан параметр *LinkedMailUser* , скрипт копирует атрибут source **objectSid** / **masterAccountSid** .

Атрибут LegacyExchangeDN

При вызове командлета **Update-Recipient** для преобразования целевого объекта в почтового пользователя для целевого почтового пользователя создается новый атрибут **LegacyExchangeDN** . Скрипт копирует атрибут **LegacyExchangeDN** целевого почтового пользователя в качестве адреса x500 в свойства **proxyAddress** исходного пользователя почтового ящика.

Включение конечной точки прокси-сервера MRS в Exchange Server

Статья • 04.07.2024

Служба репликации почтовых ящиков (MRS) имеет конечную точку прокси-сервера, необходимую для перемещения почтовых ящиков между лесами и удаленной миграции между локальной организацией Exchange и Microsoft 365 или Office 365. Необходимо включить конечную точку прокси-сервера MRS в параметрах виртуального каталога веб-служб Exchange (EWS) на серверах почтовых ящиков Exchange 2016 или Exchange 2019.

Способ включения конечной точки прокси-сервера MRS зависит от типа и направления перемещения почтовых ящиков.

- **Корпоративные перемещения между лесами**. Для перемещений между лесами, инициированных из целевого леса (известного как тип перемещения по *запросу*), необходимо включить конечную точку прокси-сервера MRS на серверах почтовых ящиков в исходном лесу. Для перемещения между лесами, инициируемого из исходного леса (т. н. *принудительного перемещения*), необходимо включить конечную точку прокси-сервера MRS на серверах почтовых ящиков в целевом лесу.

- **Удаленное перемещение миграции между локальной организацией Exchange и Microsoft 365 или Office 365**. Для исходящей и входящей миграции с удаленным перемещением нужно включить конечную точку прокси-сервера MRS на серверах почтовых ящиков в локальной организации Exchange.

- **Поэтапная миграция между локальной организацией Exchange и Microsoft 365 или Office 365**. Для поэтапной миграции в M365 необходимо включить конечную точку прокси-сервера MRS на серверах почтовых ящиков в локальной организации Exchange. Дополнительные сведения о поэтапной миграции см. в статье Выполнение промежуточной миграции электронной почты в Exchange Online.

- **Прямая миграция между локальной организацией Exchange и Microsoft 365 или Office 365**. Для прямой миграции в M365 необходимо включить конечную точку прокси-сервера MRS на серверах почтовых ящиков в локальной организации Exchange. Дополнительные сведения о прямой миграции см. в статье Миграция электронной почты в Exchange Online с помощью метода прямой передачи Exchange.

Примечание. Если вы используете Центр администрирования Exchange (EAC) для перемещения почтовых ящиков, перемещение между лесами и подключение удаленной миграции являются типами перемещения по запросу, так как вы инициируете запрос из целевой среды. Перенос удаленных миграций с удаленным перемещением является типом принудительного перемещения, так как запрос инициируется из исходной среды.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 2 минуты на сервер.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения веб-служб Exchange" раздела Разрешения клиентов и мобильных устройств .
- Если вы развернули несколько серверов почтовых ящиков в организации Exchange, следует включить конечную точку прокси-сервера MRS на каждом сервере почтовых ящиков. При добавлении новых серверов почтовых ящиков обязательно включайте на них конечную точку прокси-сервера MRS. Если конечная точка прокси-сервера MRS включена не на всех серверах почтовых ящиков, перемещение между лесами и миграции с удаленным перемещением могут завершаться с ошибкой.
- Если вы не выполняете перемещение между лесами или миграцию удаленного перемещения, оставьте конечные точки прокси-сервера MRS отключенными на серверах почтовых ящиков, чтобы уменьшить область атак в организации.
- Exchange Online требует проверки подлинности Windows для конечной точки прокси-сервера MRS в виртуальных каталогах веб-служб Exchange (EWS).
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование EAC для включения конечной точки прокси-сервера MRS

1. В EAC перейдите в раздел **Серверы**>**Виртуальные каталоги**.

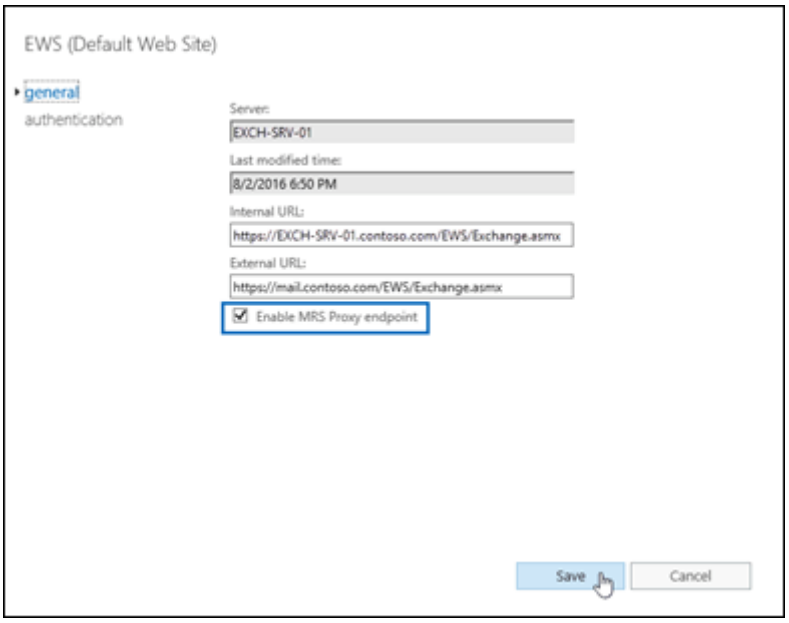
2. Выберите нужный виртуальный каталог EWS.

    - Чтобы отфильтровать серверы Exchange по имени, можно использовать раскрывающийся список **Выбор сервера** .

    - Чтобы отобразить только виртуальные каталоги EWS, выберите **EWS** в раскрывающемся списке **Выбор типа** .

    Выбрав виртуальный каталог EWS, который требуется настроить, нажмите кнопку **Изменить**.✎

3. На открывшейся странице свойств выберите вкладку **Общие**, установите флажок **Включить конечную точку прокси-сервера MRS** и нажмите кнопку **Сохранить**.



Включение конечной точки прокси-сервера MRS с помощью командной консоли Exchange

Чтобы включить конечную точку прокси-сервера MRS, используйте следующий синтаксис:

PowerShell

```
Set-WebServicesVirtualDirectory -Identity "[<Server>\]EWS (Default Web Site)" -MRSProxyEnabled $true
```

В этом примере включается конечная точка прокси-сервера MRS виртуальных каталогов EWS на сервере почтовых ящиков с именем EXCH-SRV-01.

PowerShell

```
Set-WebServicesVirtualDirectory -Identity "EXCH-SRV-01\EWS (Default Web Site)" -MRSProxyEnabled $true
```

В этом примере включается конечная точка прокси-сервера MRS виртуальных каталогов EWS на всех серверах почтовых ящиков в организации Exchange.

PowerShell

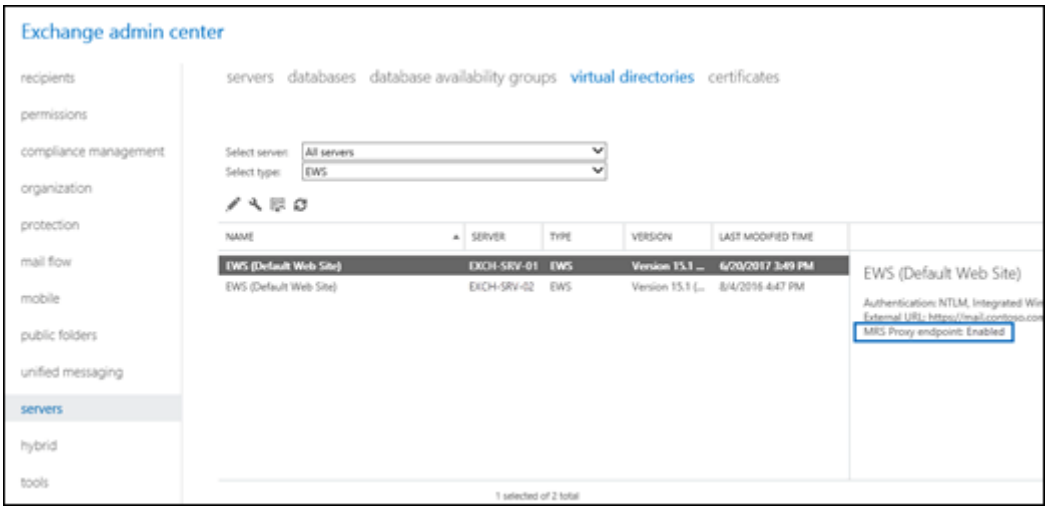
```
Get-WebServicesVirtualDirectory | Set-WebServicesVirtualDirectory -MRSProxyEnabled $true
```

Подробные сведения о синтаксисе и параметрах см. в статье Set-WebServicesVirtualDirectory.

Как проверить, все ли получилось?

Чтобы убедиться, что конечная точка прокси-сервера MRS успешно включена, выполните любое из указанных ниже действий.

- В EAC **перейдите**в раздел**Виртуальные каталоги**> серверов>, выберите виртуальный каталог EWS и убедитесь, что конечная точка прокси-сервера MRS включена в области сведений.



- Выполните эту команду в командной консоли Exchange и убедитесь, что свойство **MRSProxyEnabled** для виртуального каталога EWS имеет значение `True`:

```
PowerShell

Get-WebServicesVirtualDirectory | Format-Table -Auto
Identity,MRSProxyEnabled
```

- Используйте командлет **Test-MigrationServerAvailability** в командной консоли Exchange, чтобы проверить взаимодействие с удаленными серверами, на которые размещаются почтовые ящики, которые требуется переместить (или с серверами в локальной организации Exchange для удаленного переноса из Microsoft 365 или Office 365).

  Замените *<EmailAddress адресом электронной почты>* одного из почтовых ящиков, который требуется переместить, и выполните следующую команду в командной консоли Exchange:

```
```

PowerShell

```
Test-MigrationServerAvailability -ExchangeRemoteMove -Autodiscover -
EmailAddress <EmailAddress> -Credentials (Get-Credential)
```

Для успешного выполнения этой команды должна быть включена конечная точка прокси-сервера MRS.

Подробные сведения о синтаксисе и параметрах см. в статье Test-MigrationServerAvailability.

Повторное создание отсутствующих почтовых ящиков арбитража

Статья • 04.04.2023

Exchange 2016 CU8 или более поздней версии содержит семь специальных системных почтовых ящиков, известных как *почтовые ящики арбитража*. Почтовые ящики арбитража используются для хранения различных типов системных данных и управления рабочим процессом утверждения сообщений. В следующей таблице перечислены все типы почтовых ящиков арбитража и их обязанности.

Имя почтового ящика арбитража	Отображаемое имя	Имеющиеся возможности	Функция
FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042	Федеративный почтовый ящик Microsoft Exchange	none	В этом почтовом ящике хранятся данные, которые используются для обслуживания федерации между различными организациями Exchange. В их число входят службы управления правами, зонды для мониторинга гибридных потоков обработки почты, отклики, уведомления, серверные архивы, управление записями сообщений, а также сведения о доступности в гибридной среде.
Migration.8f3e7716-2011-43e4-96b1-aba62d229136	Миграция Microsoft Exchange	Управление	Здесь хранятся данные службы миграции Exchange, которые используются при перемещении почтовых ящиков в пакетах.

Имя почтового ящика арбитража	Отображаемое имя	Имеющиеся возможности	Функция
SystemMailbox{1f05a927-XXXX-XXXX-XXXX-XXXXXXXXXXXX} (например, SystemMailbox{1f05a927-9350-4efe-a823-5529c2d64109}; большая часть имени почтового ящика уникальна для вашей организации)	Помощник по утверждению Microsoft Exchange	none	Этот почтовый ящик подготовлен к использованию инфраструктурой утверждения Exchange для контроля получателей и работы с автоматическими групповыми запросами на утверждение.
SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}	Microsoft Exchange	ClientExtensions GMGen MailRouting Отслеживание сообщений Oabgen PstProvider UMGrammar UMGrammarReady (только Exchange 2016)	Это так называемый почтовый ящик организации. Он используется для создания автономных адресных книг. Чтобы сбалансировать нагрузку при формировании автономной адресной книги в организации (в том числе для отдаленных друг от друга сайтов), вы можете создать дополнительные почтовые ящики организации.

Имя почтового ящика арбитража	Отображаемое имя	Имеющиеся возможности	Функция
SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}	Microsoft Exchange	UMDataStorage	Системный почтовый ящик обнаружения. Подготовлено для использования функцией электронного обнаружения, которая используется сотрудниками по обеспечению соответствия требованиям для поиска сообщений, соответствующих указанным критериям выбора. Этот почтовый ящик также используется единой системой обмена сообщениями в Exchange 2016 для хранения консоли единой системы обмена сообщениями с файлами и другими сведениями.
SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201} (Exchange 2016 с накопительным пакетом обновления 8 (CU8) и более поздних версий)	Microsoft Exchange	none	Используется для временного хранения зашифрованных сообщений, чтобы внешние пользователи могли читать ее в OWA.
SystemMailbox{2CE34405-31BE-455D-89D7-A7C7DA7A0DAA} (Exchange 2016 с накопительным пакетом обновления 8 (CU8) и более поздних версий)	Microsoft Exchange	none	Этот почтовый ящик содержит функции релевантности каждого сегмента в организации.

Если вам нужно повторно создать один из этих почтовых ящиков арбитража, используйте инструкции, приведенные в этой статье.

Что нужно знать перед началом работы

- Предполагаемое время выполнения: 10 минут на процедуру.
- Чтобы вы могли выполнить эти процедуры, вам должны быть назначены соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения подготовки получателей" раздела Разрешения получателей .
- Для запуска `Setup.exe /PrepareAD` ваша учетная запись должна быть членом группы безопасности Администраторы предприятия.
- Компьютеру, который используется для запуска `Setup.exe /PrepareAD` , требуется доступ к Setup.exe в файлах установки Exchange:
    1. Используйте последнюю скачаную копию ISO-файла образа Exchange или скачайте обновленную копию из Обновления для Exchange Server.
    2. В проводник щелкните правой кнопкой мыши файл ISO-образа Exchange и выберите **Подключить**. Обратите внимание на назначенную букву виртуального DVD-диска.
    3. Откройте окно командной строки Windows. Например:
        - Нажмите клавиши Windows + R, чтобы открыть диалоговое окно **Выполнить**, введите cmd.exe и нажмите кнопку **ОК**.
        - Нажмите кнопку **Пуск**. В поле **Поиск** введите **командная строка**, а затем в списке результатов выберите **Командная строка**.
- Дополнительные сведения об открытии командной консоли Exchange см. в разделе Открытие командной консоли Exchange.
- Дополнительные сведения о запуске программы установки Exchange в автоматическом режиме см. в статье Использование автоматического режима в программе установки Exchange.

> ⓘ **Примечание**
>
> - Предыдущий переключатель */IAcceptExchangeServerLicenseTerms* не будет работать начиная с накопительных обновлений (CU) за сентябрь 2021 г. Теперь необходимо использовать */IAcceptExchangeServerLicenseTerms_DiagnosticDataON* или */IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF* для автоматической установки и установки по сценариям.
> - В примерах ниже используется переключатель */IAcceptExchangeServerLicenseTerms_DiagnosticDataON*. Вы можете

изменить переключатель на *IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF*.

Повторное создание почтового ящика арбитража

Воспользуйтесь приведенными ниже инструкциями, чтобы повторно создать почтовый ящик арбитража определенного типа.

Повторное создание федеративного почтового ящика Microsoft Exchange

Чтобы повторно создать почтовый ящик арбитража FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042, выполните следующие команды:

1. Если почтовый ящик отсутствует, выполните следующую команду в окне командной строки Windows:

   ```dos
   <Virtual DVD drive letter>:\Setup.exe
   /IAcceptExchangeServerLicenseTerms_DiagnosticDataON /PrepareAD
   ```

   Например:

   ```dos
   E:\Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON
   /PrepareAD
   ```

2. В командной консоли Exchange выполните следующую команду:

   ```PowerShell
   Enable-Mailbox -Identity "FederatedEmail.4c1f4d8b-8179-4148-93bf-
   00a95fa1e042" -Arbitration
   ```

Как повторно создать почтовый ящик миграции в Microsoft Exchange

Чтобы повторно создать почтовый ящик арбитража Migration.8f3e7716-2011-43e4-96b1-aba62d229136, выполните следующие команды:

1. Если почтовый ящик отсутствует, выполните следующую команду в окне командной строки Windows:

   ```dos
   <Virtual DVD drive letter>:\Setup.exe
   /IAcceptExchangeServerLicenseTerms_DiagnosticDataON /PrepareAD
   ```

   Например:

   ```dos
   E:\Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON
   /PrepareAD
   ```

2. В командной оболочке Exchange выполните следующую команду:

   ```PowerShell
   Enable-Mailbox -Identity "Migration.8f3e7716-2011-43e4-96b1-
   aba62d229136" -Arbitration
   ```

3. В командной консоли Exchange задайте для почтового ящика сохраненные возможности (msExchCapabilityIdentifiers), выполнив следующую команду:

   ```PowerShell
   Set-Mailbox -Identity "Migration.8f3e7716-2011-43e4-96b1-aba62d229136"
   -Arbitration -Management $true -Force
   ```

Повторное создание почтового ящика помощника по утверждению Microsoft Exchange

Чтобы повторно создать почтовый ящик арбитража SystemMailbox{1f05a927-XXXX-XXXX-XXXX-XXXXXXXXXXXXXX}, выполните следующие команды:

1. Если почтовый ящик отсутствует, выполните следующую команду в окне командной строки Windows:

   ```dos
   ```

```
<Virtual DVD drive letter>:\Setup.exe
/IAcceptExchangeServerLicenseTerms_DiagnosticDataON /PrepareAD
```

Например:

```dos
E:\Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON
/PrepareAD
```

2. В командной консоли Exchange выполните следующую команду:

```PowerShell
Get-User -ResultSize Unlimited | where {$_.Name -like
"SystemMailbox{1f05a927*"} | Enable-Mailbox -Arbitration
```

Как повторно создать почтовый ящик организации для автономных адресных книг в Microsoft Exchange

Чтобы повторно создать почтовый ящик арбитража SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}, выполните следующие команды:

1. Если почтовый ящик отсутствует, выполните следующую команду в окне командной строки Windows:

```dos
<Virtual DVD drive letter>:\Setup.exe
/IAcceptExchangeServerLicenseTerms_DiagnosticDataON /PrepareAD
```

Например:

```dos
E:\Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON
/PrepareAD
```

2. В командной консоли Exchange выполните следующую команду:

```PowerShell
```

```
Enable-Mailbox -Identity "SystemMailbox{bb558c35-97f1-4cb9-8ff7-
d53741dc928c}" -Arbitration
```

3. В командной консоли Exchange задайте для почтового ящика сохраненные возможности (msExchCapabilityIdentifiers), выполнив следующую команду:

```
PowerShell

Get-Mailbox "SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}" -
Arbitration | Set-Mailbox -Arbitration -UMGrammar $true -OABGen $true -
GMGen $true -ClientExtensions $true -MessageTracking $true -PstProvider
$true -MaxSendSize 1GB -Force
```

4. В командной консоли Exchange добавьте необходимые возможности в почтовый ящик, выполнив следующие команды:

```
PowerShell

$OABMBX = Get-Mailbox "SystemMailbox{bb558c35-97f1-4cb9-8ff7-
d53741dc928c}" -Arbitration; Set-ADUser $OABMBX.SamAccountName -Add
@{"msExchCapabilityIdentifiers"="40","42","43","44","47","51","52","46"
}
```

Как повторно создать системный почтовый ящик обнаружения в Microsoft Exchange

Чтобы повторно создать почтовый ящик арбитража SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}, выполните следующие команды:

1. Если почтовый ящик отсутствует, выполните следующую команду в окне командной строки Windows:

```
dos

<Virtual DVD drive letter>:\Setup.exe
/IAcceptExchangeServerLicenseTerms_DiagnosticDataON /PrepareAD
```

   Например:

```
dos

E:\Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON
/PrepareAD
```

2. В командной оболочке Exchange выполните следующую команду:

```
PowerShell

Enable-Mailbox -Identity "SystemMailbox{e0dc1c29-89c3-4034-b678-
e6c29d823ed9}" -Arbitration
```

3. В командной консоли Exchange задайте для почтового ящика сохраненные возможности (msExchCapabilityIdentifiers), выполнив следующую команду:

```
PowerShell

Set-Mailbox -Identity "SystemMailbox{e0dc1c29-89c3-4034-b678-
e6c29d823ed9}" -Arbitration -UMDataStorage $true -Force
```

Повторное создание системных почтовых ящиков Microsoft Exchange 2016 с накопительным пакетом обновления 8 (CU8) и более поздних версий

Чтобы повторно создать почтовый ящик арбитража SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201} и SystemMailbox{2CE34405-31BE-455D-89D7-A7C7DA7A0DAA}, выполните следующие команды:

1. Если почтовые ящики отсутствуют, выполните следующую команду в окне командной строки Windows:

```
dos

<Virtual DVD drive letter>:\Setup.exe
/IAcceptExchangeServerLicenseTerms_DiagnosticDataON /PrepareAD
```

   Например:

```
dos

E:\Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON
/PrepareAD
```

2. В командной оболочке Exchange выполните следующую команду:

```
PowerShell

Enable-Mailbox -Identity "SystemMailbox{D0E409A0-AF9B-4720-92FE-
AAC869B0D201}" -Arbitration
```

```
Enable-Mailbox -Identity "SystemMailbox{2CE34405-31BE-455D-89D7-
A7C7DA7A0DAA}" -Arbitration
```

3. В командной консоли Exchange задайте для почтового ящика сохраненные возможности (msExchCapabilityIdentifiers), выполнив следующую команду:

```
PowerShell

$ShardMBX = Get-Mailbox -Identity "SystemMailbox{2CE34405-31BE-455D-
89D7-A7C7DA7A0DAA}" -Arbitration
Set-Mailbox -Identity "SystemMailbox{2CE34405-31BE-455D-89D7-
A7C7DA7A0DAA}" -Arbitration
Set-ADUser $ShardMBX.SamAccountName -Add
@{"msExchCapabilityIdentifiers"="66"}
Set-ADUser $ShardMBX.SamAccountName -Add
@{"msExchMessageHygieneSCLDeleteThreshold"="9"}
Set-ADUser $ShardMBX.SamAccountName -Add
@{"msExchMessageHygieneSCLJunkThreshold"="4"}
Set-ADUser $ShardMBX.SamAccountName -Add
@{"msExchMessageHygieneSCLQuarantineThreshold"="9"}
Set-ADUser $ShardMBX.SamAccountName -Add
@{"msExchMessageHygieneSCLRejectThreshold"="7"}
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно создали почтовый ящик арбитража, задайте область поиска для поиска по всему лесу Active Directory, а затем используйте командлет **Get-Mailbox** с параметром *Арбитраж* , чтобы получить системные почтовые ящики.

```
PowerShell

Set-ADServerSettings -ViewEntireForest $true; Get-Mailbox -Arbitration |
Format-Table Name,DisplayName
```

Просмотрите результаты выполнения команды, чтобы убедиться в том, что необходимый системный почтовый ящик был создан. Для этого вы можете использовать имя или отображаемое имя из таблицы выше.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server** .

Управляемое хранилище в Exchange Server

Статья • 04.04.2023

Управляемое хранилище — это название процессов хранилища сведений (также известного как Хранилище) в Exchange Server 2016 г. и Exchange Server 2019 г. Введенное в Exchange Server 2013 г. управляемое хранилище использует модель контроллера или рабочего процесса, которая обеспечивает изоляцию процессов хранения и ускоряющую отработку отказа базы данных. Управляемое хранилище также использует механизм кэширования статической базы данных, который заменяет алгоритм динамического буфера в предыдущих версиях Exchange.

Многопроцессная модель, используемая Управляемым хранилищем, состоит из следующих процессов на сервере почтовых ящиков:

- Процесс контроллера службы с одним хранилищем для всего сервера Exchange (Microsoft.Exchange.Store.Service.exe, также известный как MSExchangeIS).

- Один рабочий процесс для каждой подключенной базы данных (Microsoft.Exchange.Store.Worker.exe). После подключения базы данных создается экземпляр нового рабочего процесса, который обслуживает только эту базу данных. После отключения базы данных ее рабочий процесс завершается.

Например, если на сервере почтовых ящиков подключено 40 баз данных почтовых ящиков, для управляемого хранилища будет запущен 41 процесс: по одному для каждой базы данных и по одному для контроллера процесса службы хранилища. Контроллер процессов хранилища отслеживает работоспособность всех рабочих процессов хранилища на сервере. Принудительное или неожиданное завершение Microsoft.Exchange.Store.Service.exe приводит к немедленной отработке отказа всех активных копий базы данных на сервере.

Управляемое хранилище также тесно интегрировано со службой репликации Microsoft Exchange (MSExchangeRepl.exe) и Active Manager. Процесс контроллера, рабочие процессы и служба репликации работают вместе, чтобы обеспечить большую доступность и надежность, как описано в следующем списке.

- **Процесс службы репликации Microsoft Exchange (MSExchangeRepl.exe)**:

    - Отвечает за выдачу операций подключения и отключения в Store.

- Инициирует действие восстановления при сбоях хранилища или базы данных, о чем сообщают магазин, подсистема расширяемого хранилища (ESE) и управляемые средства реагирования на доступность.
- Обнаруживает непредвиденные сбои базы данных.
- Предоставляет административный интерфейс для задач управления.

- **Хранение процесса или контроллера службы (Microsoft.Exchange.Store.Service.exe):**
  - Управляет временем существования каждого рабочего процесса на основе операций подключения и отключения, полученных от службы репликации.
  - Обрабатывает входящие запросы от диспетчера управления службами Windows.
  - Регистрирует элементы сбоя при обнаружении проблем с рабочим процессом в хранилище (например, зависание или непредвиденный выход).
  - Завершает хранение рабочих процессов в ответном событии отработки отказа.

- **Рабочий процесс хранилища (Microsoft.Exchange.Store.Worker.exe):**
  - Отвечает за выполнение операций RPC для почтовых ящиков в базе данных.
  - Экземпляр конечной точки RPC в рабочем процессе — это GUID базы данных.
  - Предоставляет кэш базы данных для базы данных.

Алгоритм кэширования статической базы данных

Управляемое хранилище использует очень простой и простой алгоритм для определения кэша базы данных по сравнению с *динамическим выделением буфера* , который использовался в предыдущих версиях Exchange. Память, выделенная для каждого кэша базы данных (т. е. каждого рабочего процесса хранилища), основана на количестве локальных копий базы данных и настроенном значении параметра *MaximumActiveDatabases* в **командлете Set-MailboxServer** (значение по умолчанию — $null или пусто). Если значение *MaximumActiveDatabases* больше, чем количество

текущих копий базы данных, то вычисление кэша основано на количестве копий базы данных.

Статический алгоритм выделяет память для кэша ESE каждого рабочего процесса хранения в зависимости от объема физического ОЗУ, установленного на сервере. Это относится к *целевому объекту максимального кэша* базы данных. 25 % от общего объема памяти сервера выделяется кэшу ESE и называется *целевым размером кэша сервера*.

> ⓘ **Примечание**
>
> Вы можете переопределить целевой размер кэша сервера и, следовательно, объем памяти, выделенный хранилищу для кэша ESE, с помощью `msExchESEParamCacheSizeMax` атрибута объекта *InformationStore* в Active Directory (настроенное значение — количество 32 КБ страниц, выделяемых во всех процессах хранилища).

Для активных и пассивных копий выделяется статический объем этого кэша. Для рабочих процессов хранилища максимальный целевой кэш выделяется только при обслуживании копии активной базы данных. Для копий пассивных баз данных выделяется 20 % максимального целевого кэша. Остальную часть резервирует хранилище и выделяет ее для рабочих процессов при переходе базы данных из пассивного в активное состояние.

Максимальный целевой кэш рассчитывается только во время запуска хранилища. Потому в случае добавления или удаления баз данных или их копий необходимо перезапустить службу контроллера хранилища (MSExchangeIS) для соответствующей регулировки кэша. Если служба не перезапущена, новые базы данных будут иметь меньший размер кэша, чем базы данных, существовавшие до последнего запуска службы. В этом сценарии сумма целевых значений размера кэша базы данных, скорее всего, превысит целевой размер кэша сервера до перезапуска MSExchangeIS.

Пример вычислений кэша базы данных

Ниже приведены примеры вычислений кэширования баз данных, основанных на памяти и конфигурации базы данных сервера почтовых ящиков.

Пример 1

Конфигурация сервера почтовых ящиков:

- 48 ГБ памяти
- Две активные базы данных и две пассивные базы данных
- Параметр *MaximumActiveDatabases*: не настроен

Объем кэша базы данных составляет 3 ГБ для каждого активного рабочего процесса копирования базы данных и 0,6 ГБ для каждого пассивного рабочего процесса копирования базы данных. Вот как вычисляются эти значения:

- **Целевой размер кэша сервера**: 25 % объема памяти: 48 ГБ * 0,25 = **12 ГБ**.
- **Целевой максимальный размер кэша базы данных**. Разделите целевой размер кэша сервера на общее количество активных и пассивных баз данных: 12 ГБ / 4 базы данных = **3 ГБ**.
- **Память, используемая для пассивных копий базы данных**: 20 % целевого значения максимального кэша базы данных: 3 ГБ * 0,20 = **0,6 ГБ**.

Из 12 ГБ памяти, назначенной целевому размеру кэша сервера:

- 7,2 ГБ будет использоваться рабочими процессами базы данных.
- Хранилище сведений зарезервирует 4,8 ГБ для двух пассивных копий базы данных на случай, если они станут активными. В этом случае они будут использовать максимальный целевой кэш размером 3 ГБ.

Пример 2

Конфигурация сервера почтовых ящиков:

- 48 ГБ памяти
- Две активные базы данных и две пассивные базы данных
- *Параметр MaximumActiveDatabases* : 2

Объем кэша базы данных составляет 5 ГБ для каждого активного рабочего процесса копирования базы данных и 0,2 ГБ для каждого пассивного рабочего процесса копирования базы данных. Вот как вычисляются эти значения:

- **Целевой размер кэша сервера**: 25 % объема памяти: 48 ГБ * 0,25 = **12 ГБ**.
- **Целевой максимальный размер кэша базы данных**. Разделите целевой размер кэша сервера на сумму:

    - Количество активных баз данных
    - 20 % от числа пассивных баз данных

    12 ГБ / (2A + (2P * 0,20)) = **5 ГБ**

- **Память, используемая для пассивных копий базы данных**: 20 % целевого значения максимального кэша базы данных: 5 ГБ * 0,20 = **1 ГБ**.

Из 12 ГБ памяти, назначенной целевому размеру кэша сервера:

- 12 ГБ будет использоваться рабочими процессами базы данных
- Хранилище сведений не будет зарезервировано памяти для двух пассивных копий базы данных, так как они не могут стать активными копиями (*параметр MaximumActiveDatabases* настроен со значением 2, а на сервере уже есть 2 активные копии базы данных).

Ограничения управляемого хранилища в Exchange Server

Статья • 04.04.2023

Управляемое хранилище в Exchange Server 2016 и Exchange Server 2019 годах — это имя для процессов хранилища сведений (также известного как Store), которые управляют базами данных почтовых ящиков. Управляемое хранилище имеет ограничения на подключение и использование, которые не позволяют одному приложению или одному пользователю использовать все доступные подключения, что может привести к простою. В этом разделе описаны ограничения и способы их изменения.

Дополнительные сведения об управляемом хранилище см. в разделе Управляемое хранилище в Exchange Server.

> ⓘ **Примечание**
>
> Максимальное число подключений по учетным записям администратора составляет 64 000 сеансов.
>
> Exchange Online ограничения (включая ограничения управляемого хранилища) описаны в **разделе ограничения Exchange Online**.

Терминология

Знание приведенных ниже терминов поможет вам получить общее представление о типах соединений, упоминаемых в этой статье.

- **Сеансы**

  Сеансы представляют подключения, используемые службами и клиентскими приложениями (например, Microsoft Outlook) для подключения к Управляемому магазину. У служб и клиентов может быть одновременно открыто несколько сеансов. Термины *подключения* и *сеансы* являются взаимозаменяемыми.

- **Потоков**

  Потоки представляют одновременно выполняемые запросы к управляемому хранилищу. Например, если пользователь откроет папку в Outlook, Outlook

выполнит запрос к управляемому хранилищу от имени этого пользователя. Этот выполняющийся запрос представляет собой один поток.

Для всех клиентов максимальное число потоков **на базу данных почтовых ящиков** составляет 50. Исключением является служба доступности, для которой количество потоков на пользователя ограничено 16.

Ограничения сеансов

Ограничения сеансов зависят от подключений к каждой базе данных почтовых ящиков на сервере.

Типы ограничений подключения:

- **Максимальное число сеансов на процесс**. Максимальное число сеансов, которое служба Exchange может одновременно открывать в базе данных почтовых ящиков.
- **Максимальное число сеансов пользователей на процесс**. Максимальное число сеансов для определенного протокола для одного пользователя.

Типы клиентских подключений к Управляемому хранилищу и ограничения на основе этих подключений описаны в следующей таблице.

Тип клиента	**Максимальное количество сеансов на базу данных почтовых ящиков**	**Количество пользовательских сеансов по умолчанию на одну базу данных почтовых ящиков**
Администратор	10000	н/д
Служба доступности	10000	16
Индексирование содержимого	10000	н/д
Exchange ActiveSync	н/д	16
Веб-службы Exchange	н/д	16
Управление	н/д	16
MAPI on the Middle Tier (MoMT)	н/д	32
MSExchangeMailboxAssistants: события	10000	н/д

Тип клиента	Максимальное количество сеансов на базу данных почтовых ящиков	Количество пользовательских сеансов по умолчанию на одну базу данных почтовых ящиков
MSExchangeMailboxAssistants: контроль по времени	10000	н/д
Удаленный вызов процедур MSExchange	н/д	16
Outlook в Интернете (прежнее название — Outlook Web App)	н/д	16
Протоколы POP3 и IMAP4	н/д	16
Transport	10000	н/д
Единая система обмена сообщениями (только Для Exchange 2016)	н/д	16
Другие	н/д	16

Используйте следующую процедуру, чтобы изменить ограничения сеансов по умолчанию.

Примечания.

- При изменении ограничения сеанса необходимо изменить это ограничение на всех серверах почтовых ящиков в группе доступности базы данных (DAG). Если не внести идентичные изменения на всех серверах, результаты будут противоречивыми.
- Чтобы увеличить ограничение сеанса в службах клиентского доступа (внешний интерфейс), необходимо использовать командлет Set-ThrottlingPolicy в командной консоли Exchange.

> ⚠ **Предупреждение**
>
> Неправильное изменение реестра может привести к серьезным неполадкам, требующим переустановки операционной системы. Проблемы, возникшие в результате неправильного изменения реестра, могут оказаться неустранимыми. Перед внесением изменений в реестр выполните резервное копирование всех важных данных.

1. Откройте редактор реестра. Например, нажмите клавишу Windows + R, а затем запустите **regedit**.

2. Перейдите в следующее расположение в реестре:

   \\HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Services\MSExchangeIS\ParametersSystem.

3. Выберите подраздел **ParametersSystem**, нажмите кнопку **Изменить>,** а затем выберите **Значение DWORD (32-разрядное).**

   Новое значение создается как **Новое значение 1** на панели справа.

4. Переименуйте новую клавишу на одно из следующих значений и нажмите клавишу ВВОД:

   - **Максимальное число разрешенных сеансов на пользователя**. Это ограничение указывает максимально допустимые сеансы на пользователя.

   - **Максимальное число разрешенных сеансов службы на пользователя**. Это ограничение указывает максимально допустимое количество сеансов службы на пользователя.

   - **Максимальное число разрешенных сеансов Exchange на службу**. Это ограничение указывает максимально допустимое количество сеансов Exchange для каждой службы. Значение по умолчанию составляет 10 000.

5. Выберите новый ключ и нажмите кнопку **Изменить>.**

6. В открывшемся диалоговом окне переключите **базовое** значение на **Десятичное** и введите новое ограничение сеанса в поле **Значение данных** .

   После этого нажмите кнопку **OK**.

Ограничения на открытие элементов

Ограничения открытых элементов представляют собой максимальное количество элементов, которые можно открывать в одном почтовом ящике за один сеанс. Однако пользователь может открыть несколько сеансов одновременно. Например, если пользователь открыл два сеанса, он может открыть 1000 папок.

Ограничения открытых элементов описаны в следующей таблице.

Тип элемента	Тип объекта реестра	Максимальное количество открытых за сеанс элементов
Представление списка управления доступом	objtACLView	500
Вложение	objtAttachment	500
Представление вложения	objtAttachmentView	500
CStream	objtCStream	Неприменимо
Папка	objtFolder	500
Представление папки	objtFolderView	500
Целевой поток FX	objtFXDstStrm	500
Исходный поток FX	objtFXSrcStrm	500
Сообщение	objtMessage	250
Представление сообщения	objtMessageView	500
Уведомление	objtNotify	500,000
Представление правила	objtRulesView	Неприменимо
Поток	objtStream	250

Можно ограничить максимальное количество ресурсов, которые клиент MAPI (например, Outlook) может использовать одновременно.

Примечание. При изменении ограничения сеанса необходимо изменить это ограничение на всех серверах почтовых ящиков в группе доступности базы данных (DAG). Если не внести идентичные изменения на всех серверах, результаты будут противоречивыми.

> **⚠ Предупреждение**
>
> Неправильное изменение реестра может привести к серьезным неполадкам, требующим переустановки операционной системы. Проблемы, возникшие в результате неправильного изменения реестра, могут оказаться неустранимыми. Перед внесением изменений в реестр выполните резервное копирование всех важных данных.

1. Откройте редактор реестра. Например, нажмите клавишу Windows + R, а затем запустите **regedit**.

2. Перейдите в следующее расположение в реестре:

   \\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\ParametersSystem

3. Выберите подраздел **ParametersSystem** , нажмите кнопку **Изменить**>**создать**, а затем выберите **Ключ**.

   Новое значение создается как **Новый ключ No 1** на левой панели.

4. Переименуйте новый ключ в **MaxObjsPerMapiSession** и нажмите клавишу ВВОД.

5. Выберите подраздел **MaxObjsPerMapiSession**, нажмите кнопку **Изменить**>**,** а затем выберите **Значение DWORD (32-бит).**

   Новый ключ создается как **Новое значение 1** в правой области.

6. Переименуйте ключ в соответствии со значениями **типа объекта Реестра** в таблице. Например, чтобы изменить количество сообщений, которые можно открыть, введите *objtMessage* и нажмите клавишу ВВОД.

7. Выберите новый ключ и нажмите кнопку **Изменить**>**.**

8. В открывшемся диалоговом окне переключите **базовое** значение на **Десятичное** и введите новое ограничение в поле **Значение данных** . Например, введите **350** , чтобы увеличить значение *objtMessage*.

   После этого нажмите кнопку **OK**.

9. Перезапустите службу Microsoft Exchange Information Store, выполнив следующую команду в Windows PowerShell или командной консоли Exchange:

   PowerShell

   ```
   Restart-Service MSExchangeIS
   ```

Ограничения на размер элемента

Ограничения размеров элементов — это ограничения, накладываемые на элементы в почтовых ящиках пользователей. Эти ограничения настраиваются с помощью параметров *MaxSendSize* и *MaxReceiveSize* в командлете Set-Mailbox в командной консоли Exchange.

Тип элемента	Ограничение
Сообщение (сохраненное)	Максимальный размер SendLimit, ReceiveLimit
Сообщение (отправленное)	Максимальный размер SendLimit

Exchange Server: пограничные транспортные серверы

Статья • 04.04.2023

Пограничные транспортные серверы обрабатывают все потоки входящей и исходящей почты в Интернете, предоставляя почтовые ретрансляторы и интеллектуальные службы узлов для вашей организации Exchange. Агенты, запущенные на пограничном транспортном сервере, создают дополнительные уровни защиты сообщений и безопасности. Эти агенты обеспечивают защиту от нежелательной почты и применяют правила потока обработки почты (также известные как правила транспорта) для управления потоком обработки почты. Все эти функции работают вместе, чтобы свести к минимуму уязвимость внутреннего Exchange к угрозам в Интернете.

Так как пограничный транспортный сервер установлен в сети периметра, он никогда не является участником внутреннего леса Active Directory вашей организации и не имеет доступа к данным Active Directory. Однако пограничному транспортному серверу требуются данные, которые находятся в Active Directory: например, сведения о соединителе для потока обработки почты и сведения о получателях для задач поиска получателей с защитой от нежелательной почты. Данные синхронизируются с пограничным транспортным сервером с помощью службы Microsoft Exchange EdgeSync (EdgeSync). EdgeSync — это коллекция процессов, выполняемых на сервере почтовых ящиков Exchange 2016 или Exchange 2019 для создания односторонняя репликация данных о получателях и конфигурации из Active Directory в экземпляр служб Active Directory облегченного доступа к каталогам (AD LDS) на пограничном транспортном сервере. EdgeSync копирует только сведения, необходимые пограничному транспортному серверу для выполнения задач настройки защиты от нежелательной почты и включения сквозного потока обработки почты. Для поддержания актуальности данных в AD LDS EdgeSync выполняет запланированные обновления. Дополнительные сведения о подписках Edge и EdgeSync см. в разделе Подписки Edge.

Можно устанавливать несколько пограничных транспортных серверов на периметре сети. Развертывание более одного пограничного транспортного сервера обеспечивает избыточность и отказоустойчивость для потока входящих сообщений. Можно распределить нагрузку трафика SMTP в своей организации между пограничными транспортными серверами, определив несколько записей MX с одинаковым значением приоритета для домена электронной почты. Согласованность конфигурации между несколькими пограничными

транспортными серверами может быть достигнута с помощью сценариев клонирования конфигурации.

Роль пограничного транспортного сервера позволяет управлять следующими сценариями обработки сообщений.

Поток почты Интернета

Пограничные транспортные серверы принимают сообщения, поступающие в организацию Exchange из Интернета. После обработки сообщений пограничным транспортным сервером почта направляется на внутренний сервер почтовых ящиков Exchange. сначала в транспортную службу переднего плана, а затем в транспортную службу.

Все сообщения, отправляемые в Интернет из организации, направляются на пограничные транспортные серверы после обработки сообщений транспортной службой на сервере почтовых ящиков Exchange. Можно настроить пограничный транспортный сервер на использование DNS для разрешения записей источника Mail Exchanger (MX) для внешних доменов SMTP или можно настроить пограничный транспортный сервер для переадресации сообщений на промежуточный узел для разрешения DNS.

Защита от нежелательной почты

В Exchange Server функции защиты от спама предоставляют службы для блокировки нежелательной коммерческой электронной почты (спама) на периметре сети.

Отправители нежелательной почты применяют различные методики, чтобы доставить свои сообщения в организации. Пограничные транспортные серверы помогает предотвратить получение пользователями нежелательной почты путем использования коллекции агентов, которые совместно обеспечивают разные уровни фильтрации нежелательной почты и защиты от нее. Установка интервалов искусственной задержки ответов на соединителях делает попытки сбора электронной почты неэффективными.

Правила потока обработки почты на пограничных транспортных серверах

Правила потока обработки почты на пограничных транспортных серверах используются для управления потоком сообщений, отправляемых или полученных из Интернета. Правила потока обработки почты настраиваются на каждом пограничном транспортном сервере для защиты корпоративных сетевых ресурсов и данных путем применения действия к сообщениям, отвечающим указанным условиям. Условия правила потока обработки почты основаны на данных, таких как конкретные слова или текстовые шаблоны в теме сообщения, тексте, заголовке или из адреса. уровень достоверности нежелательной почты (SCL); или тип вложения. Действия определяют параметры обработки сообщения при выполнении заданного условия. Возможные действия включают карантин сообщения, удаление или отклонение сообщения, присоединение дополнительных получателей или регистрацию события в журнале. Необязательные исключения позволяют предотвратить применение действия к конкретным сообщениям.

Перезапись адресов

Перезапись адресов обеспечивает единообразие представления адресов для внешних получателей. Перезапись адресов настраивается на пограничных транспортных серверах для изменения адресов SMTP входящих и исходящих сообщений. Перезапись адресов особенно полезна для новых организаций, которые нуждаются в единообразном представлении адресов электронной почты.

Пограничные подписки в Exchange Server

Статья • 04.04.2023

Пограничные подписки используются для заполнения экземпляра служб Active Directory облегченного доступа к каталогам (AD LDS) на пограничном транспортном сервере данными службы Active Directory. Хотя пограничную подписку создавать необязательно, подписка пограничного транспортного сервера на организацию Exchange упрощает управление и расширяет возможности защиты от нежелательной почты. Пограничную подписку необходимо создавать, если планируется использовать поиск получателей или объединение списков надежных отправителей либо защищать связь по протоколу SMTP с доменами партнеров с помощью протокола Mutual TLS (MTLS).

> ⓘ **Примечание**
>
> Подписка Edge является обязательной, если пограничный транспорт должен обрабатывать гибридный поток обработки почты. Заголовки организации повышаются только между пограничными транспортными серверами и серверами почтовых ящиков с помощью проверки подлинности с прямым доверием (также называется Mutual TLS). Для этого метода проверки подлинности требуется подписка Edge.

Процесс пограничной подписки

Пограничный транспортный сервер не имеет прямого доступа к Active Directory. Сведения о конфигурации и получателях, которые пограничный транспортный сервер использует для обработки сообщений, хранятся локально в службах AD LDS. При создании пограничной подписки обеспечивается надежная автоматическая репликация сведений из Active Directory в AD LDS. Процесс пограничной подписки подготавливает учетные данные, используемые для установки безопасного подключения LDAP между внутренними серверами почтовых ящиков Exchange и подписанным пограничным транспортным сервером. Служба Microsoft Exchange EdgeSync (EdgeSync), запущенная на серверах почтовых ящиков, выполняет периодическую односторонней синхронизацию для передачи актуальных данных в AD LDS. Тем самым уменьшается количество задач администрирования, выполняемых в сети периметра, за счет возможности настройки сервера почтовых

ящиков с последующей синхронизацией этих данных на пограничном транспортном сервере.

Вы подписываете пограничный транспортный сервер на сайт Active Directory, содержащий серверы почтовых ящиков, которые отвечают за передачу сообщений на пограничные транспортные серверы и их получение оттуда. В процессе пограничной подписки создается членство на сайте Active Directory для пограничного транспортного сервера. Это членство позволяет серверам почтовых ящиков в организации Exchange ретранслировать сообщения на пограничный транспортный сервер для доставки в Интернет без настройки явных соединителей отправки.

На один сайт Active Directory могут быть подписаны несколько пограничных транспортных серверов. При этом пограничный транспортный сервер нельзя подписать на несколько сайтов Active Directory. Если развернуто несколько пограничных транспортных серверов, каждый из них должен быть подписан на отдельный сайт Active Directory. Для каждого пограничного транспортного сервера требуется индивидуальная пограничная подписка.

Чтобы развернуть пограничный транспортный сервер и подписать его на сайт Active Directory, сделайте следующее:

1. Установите роль пограничного транспортного сервера.
2. Выполните подготовку к пограничной подписке:
    - Лицензируйте пограничный транспортный сервер.
    - Откройте порты в брандмауэре для потока обработки почты и синхронизации EdgeSync.
    - Убедитесь в том, что серверы почтовых ящиков и пограничный транспортный сервер могут находить друг друга с помощью разрешения имен DNS.
    - На сервере почтовых ящиков настройте объекты и параметры, которые необходимо реплицировать на пограничный транспортный сервер.
3. На пограничном транспортном сервере создайте и экспортируйте файл пограничной подписки, выполнив командлет **New-EdgeSubscription**.
4. Скопируйте файл пограничной подписки на сервер почтовых ящиков или в общий файловый ресурс, доступный на сайте Active Directory, где расположены серверы почтовых ящиков.

5. Импортируйте файл пограничной подписки на сайт Active Directory, выполнив командлет **New-EdgeSubscription** на сервере почтовых ящиков.

Подготовка пограничной подписки

Прежде чем вы сможете подписать пограничный транспортный сервер на свою организацию Exchange, необходимо убедиться, что инфраструктура и серверы почтовых ящиков подготовлены к синхронизации EdgeSync. Чтобы подготовиться к EdgeSync, необходимо:

- **Лицензирование пограничного транспортного сервера**. Сведения о лицензировании для пограничного транспортного сервера записываются при создании пограничной подписки. Подписанные пограничные транспортные серверы должны быть подписаны на организацию Exchange после применения лицензионного ключа на пограничном транспортном сервере. Если лицензионный ключ применяется к пограничному транспортному серверу после выполнения процесса пограничной подписки, сведения о лицензировании не будут обновляться в организации Exchange, и вам потребуется повторно подписаться на пограничный транспортный сервер.

- **Убедитесь, что необходимые порты открыты в брандмауэре**. Следующие порты используются подписанными пограничными транспортными серверами:

  - **SMTP**. Порт 25/TCP должен быть открыт для входящего и исходящего потока почты между Интернетом и пограничным транспортным сервером, а также между пограничным транспортным сервером и внутренней организацией Exchange.

  - **Secure LDAP**. Нестандартный порт 50636/TCP используется для синхронизации каталогов с серверов почтовых ящиков в AD LDS на пограничном транспортном сервере. Этот порт необходим для успешной синхронизации EdgeSync.

    > ⓘ **Примечание**
    >
    > TCP-порт 50389 используется локально протоколом LDAP для привязки экземпляра AD LDS. Этот порт не обязательно должен быть открыть в брандмауэре — он используется локально на пограничном транспортном сервере.

Если для вашей среды требуются определенные порты, можно изменить порты, используемые AD LDS, с помощью скрипта, предоставленного `ConfigureAdam.ps1` в Exchange. Измените порты, прежде чем создавать пограничную подписку. Если изменить настройки портов после создания пограничной подписки, необходимо удалить пограничную подписку и создать другую.

- **Убедитесь, что узел DNS правильно разрешает имена с пограничного транспортного сервера на серверы почтовых ящиков и наоборот.**

- **Настройте приведенные ниже параметры транспорта, которые будут распространены на пограничный транспортный сервер.**

  - **Внутренние SMTP-серверы**. *И*спользуйте параметр *InternalSMTPServers* в командлете Set-TransportConfig, чтобы указать список **IP-адресов внутренних SMTP-серверов** или диапазонов IP-адресов, которые будут игнорироваться агентами идентификатора отправителя и фильтрации подключений на пограничном транспортном сервере.

  - **Обслуживаемые домены**. Настройте все полномочные домены, внутренние домены ретранслятора и домены внешнего ретранслятора.

  - **Удаленные домены**. Настройте параметры для объекта удаленного домена по умолчанию (используется для получателей во всех удаленных доменах) и настройте объекты удаленного домена в соответствии с требованиями для получателей в определенных удаленных доменах.

Создание и экспорт файла пограничной подписки на пограничном транспортном сервере

При создании файла пограничной подписки (путем выполнения командлета **New-EdgeSubscription** на пограничном транспортном сервере) выполняются следующие действия:

- Создается учетная запись AD LDS, которая называется учетной записью репликации начальной загрузки EdgeSync (ESBRA). Эти учетные данные ESBRA используются для проверки подлинности первого подключения EdgeSync к пограничному транспортному серверу. Срок действия учетной записи истекает через 24 часа после создания. Поэтому процесс подписки из пяти этапов, описанный в предыдущем разделе, необходимо выполнить в течение 24 часов. Если срок действия учетной записи ESBRA истечет до завершения процесса пограничной подписки, потребуется повторно выполнить

командлет **New-EdgeSubscription**, чтобы создать новый файл пограничной подписки.

- Учетные данные ESBRA извлекаются из службы AD LDS и записываются в файл пограничной подписки. В файл пограничной подписки также экспортируется открытый ключ самозаверяющего сертификата пограничного транспортного сервера. Учетные данные, записываемые в файл пограничной подписки, зависят от сервера, с которого экспортировался файл.
- Все ранее созданные объекты конфигурации на пограничном транспортном сервере, которые будет реплицироваться в AD LDS из службы каталогов Active Directory, удаляются из AD LDS, а командлеты Командная консоль Exchange, используемые для настройки этих объектов, отключаются. Однако для просмотра этих объектов по-прежнему можно использовать командлеты **Get-*** . При выполнении командлета **New-EdgeSubscription** на пограничном транспортном сервере отключаются приведенные ниже командлеты.
  - **Set-SendConnector**
  - **New-SendConnector**
  - **Remove-SendConnector**
  - **New-AcceptedDomain**
  - **Set-AcceptedDomain**
  - **Remove-AcceptedDomain**
  - **New-RemoteDomain**
  - **Set-RemoteDomain**
  - **Remove-RemoteDomain**

В этом примере создается и экспортируется файл пограничной подписки на пограничном транспортном сервере.

PowerShell

```
New-EdgeSubscription -FileName "C:\Data\EdgeSubscriptionInfo.xml"
```

ⓘ Примечание

При выполнении командлета **New-EdgeSubscription** на пограничном транспортном сервере появляется запрос на подтверждение отключения команд и перезаписи конфигурации на пограничном транспортном сервере. Чтобы обойти это подтверждение, необходимо использовать параметр *Force* . Этот параметр полезен при использовании командлета **New-EdgeSubscription** в сценарии. Параметр *Force* также можно использовать для перезаписи существующего файла при повторной подписке на пограничный транспортный сервер.

Импорт файла пограничной подписки на сервере почтовых ящиков

При импорте файла пограничной подписки на сайт Active Directory с помощью командлета **New-EdgeSubscription** на сервере почтовых ящиков выполняются следующие действия:

- Создается файл пограничной подписки с присоединением пограничного транспортного сервера к организации Exchange. EdgeSync будет распространять данные конфигурации на этот пограничный транспортный сервер, создавая объект конфигурации Edge в Active Directory.
- Каждый сервер почтовых ящиков на сайте Active Directory получает уведомление от Active Directory о том, что подписан новый пограничный транспортный сервер. Сервер почтовых ящиков получает ESBRA из файла пограничной подписки. После этого сервер почтовых ящиков шифрует ESBRA с использованием открытого ключа самозаверяющего сертификата пограничного транспортного сервера. Зашифрованные учетные данные затем записываются в объект пограничной конфигурации.
- Каждый сервер почтовых ящиков также шифрует ESBRA с помощью собственного открытого ключа и сохраняет учетные данные в своем объекте конфигурации.
- Учетные записи репликации EdgeSync (ESRA) создаются в Active Directory для каждой пары пограничных Transport-Mailbox серверов. Каждый сервер почтовых ящиков хранит свои учетные данные ESRA в качестве атрибута объекта конфигурации сервера почтовых ящиков.
- Соединители отправки создаются автоматически для ретрансляции сообщений, исходящих с пограничного транспортного сервера в Интернет, и для входящих сообщений с пограничного транспортного сервера в

организацию Exchange. Дополнительные сведения см. в разделе Send connectors created automatically by the Edge Subscription этой статьи.

- Служба Microsoft Exchange EdgeSync, которая работает на серверах почтовых ящиков, использует учетные данные ESBRA для установки безопасного подключения LDAP между сервером почтовых ящиков и пограничным транспортным сервером и выполняет начальную репликацию данных. В службу AD LDS реплицируются следующие данные:
  - данные топологии;
  - данные конфигурации;
  - данные получателей;
  - учетные данные ESRA.
- Служба учетных данных Microsoft Exchange, которая выполняется на пограничном транспортном сервере, устанавливает учетные данные ESRA. Эти учетные данные используются для проверки подлинности и защиты последующих соединений синхронизации.
- Установлено расписание синхронизации EdgeSync.
- Служба Microsoft Exchange EdgeSync, запущенная на серверах почтовых ящиков на сайте Active Directory с подпиской, выполняет односторонняя репликацию данных из Active Directory в AD LDS по регулярному расписанию. Вы также можете использовать командлет **Start-EdgeSynchronization** , чтобы переопределить расписание синхронизации EdgeSync и немедленно начать синхронизацию.

В этом примере выполняется подписка пограничного транспортного сервера на указанный сайт и автоматически создается соединитель отправки в Интернет и соединитель отправки с пограничного транспортного сервера на серверы почтовых ящиков.

PowerShell

```
New-EdgeSubscription -FileData
([System.IO.File]::ReadAllBytes('C:\Data\EdgeSubscriptionInfo.xml')) -Site
"Default-First-Site-Name"
```

Примечание

Значениями по умолчанию параметров *CreateInternetSendConnector* и *CreateInboundSendConnector* являются `$true`, поэтому их не нужно использовать в этой команде.

Соединители отправки, автоматически создаваемые пограничной подпиской

По умолчанию при импорте файла пограничной подписки на сервер почтовых ящиков автоматически создаются соединители отправки, необходимые для обеспечения непрерывного потока обработки почты между Интернетом и организацией Exchange, при этом все существующие соединители отправки на пограничном транспортном сервере удаляются.

Пограничная подписка создает следующие соединители отправки:

- Соединитель отправки с именем EdgeSync — inbound to <*Site Name*> , настроенный для ретрансляции сообщений с пограничного транспортного сервера в организацию Exchange.
- Соединитель Отправки с именем EdgeSync — <*имя*> сайта в Интернет, настроенный для передачи сообщений из организации Exchange в Интернет.

кроме того, подписка пограничного транспортного сервера на организацию Exchange позволяет серверам почтовых ящиков на подписанном сайте Active Directory использовать невидимый и неявный внутриорганизационный соединитель отправки для ретрансляции сообщений на пограничный транспортный сервер.

Соединитель входящей почты для приема сообщений из Интернета

При выполнении командлета **New-EdgeSubscription** на сервере почтовых ящиков *параметру CreateInboundSendConnector* присваивается значение `$true`. При этом создается соединитель отправки, необходимый для отправки сообщений с пограничного транспортного сервера в организацию Exchange. В таблице ниже показана конфигурация этого соединителя отправки.

Конфигурация автоматически создаваемого соединителя отправки для входящих подключений

Свойство	Значение
Название	EdgeSync — входящий трафик к *<имени сайта>*
AddressSpaces	`SMTP:--;1` Значение `--` в адресном пространстве представляет все полномочные и внутренние обслуживаемые домены ретранслятора для организации Exchange. Все сообщения, которые получает пограничный транспортный сервер для этих обслуживаемых доменов и обслуживаемых доменов, маршрутизируются на данный соединитель отправки и ретранслируются на промежуточные узлы.
SourceTransportServers	*<Имя подписки Edge>*
Enabled	True
DNSRoutingEnabled	False
SmartHosts	`--` Значение `--` в списке интеллектуальных узлов представляет все серверы почтовых ящиков на сайте Active Directory с подпиской. Все серверы почтовых ящиков, добавленные на сайт Active Directory с подпиской после создания пограничной подписки, не участвуют в процессе синхронизации EdgeSync. Тем не менее они автоматически добавляются в список промежуточных узлов для автоматически создаваемого соединителя отправки для входящих подключений. Если на подписанном сайте Active Directory расположено несколько серверов почтовых ящиков, входящие подключения будут распределяться между промежуточными сайтами для балансировки нагрузки.

На момент создания адресное пространство и список промежуточных узлов автоматически создаваемого соединителя отправки для входящих подключений изменить нельзя. Однако при создании пограничной подписки для параметра *CreateInboundSendConnector* можно задать значение `$false` . Это позволяет вручную настроить соединитель отправки с пограничного транспортного сервера в организацию Exchange.

Соединитель исходящей почты для отправки сообщений в Интернет

При выполнении командлета **New-EdgeSubscription** на сервере почтовых ящиков *параметру CreateInternetSendConnector* присваивается значение `$true`. При этом создается соединитель отправки, необходимый для отправки сообщений из организации Exchange в Интернет. В следующей таблице показана конфигурация по умолчанию для этого соединителя отправки.

Конфигурация автоматически создаваемого соединителя отправки для Интернета

Свойство	Значение
Название	EdgeSync — <*имя*> сайта в Интернет
AddressSpaces	`SMTP:*;100`
SourceTransportServers	*<Имя подписки Edge>* Имя пограничной подписки совпадает с именем подписанного пограничного транспортного сервера.
Enabled	True
DNSRoutingEnabled	True
DomainSecureEnabled	True

Если на один сайт Active Directory подписано несколько пограничных транспортных серверов, дополнительные соединители отправки для Интернета не создаются. Вместо этого все пограничные подписки добавляются к одному соединителю отправки в качестве исходного сервера. Это обеспечивает балансировку нагрузки исходящих подключений к Интернету на подписанных пограничных транспортных серверах.

Соединитель отправки для исходящих подключений настроен на отправку сообщений электронной почты из организации Exchange на все удаленные SMTP-домены и использует маршрутизацию DNS для разрешения имен доменов в записи ресурсов MX.

Сведения о службе EdgeSync

После подписки на пограничный транспортный сервер на сайт Active Directory EdgeSync реплицирует данные конфигурации и получателей на пограничные транспортные серверы. Эта служба реплицирует из Active Directory в AD LDS следующие данные:

- конфигурация соединителя отправки;
- обслуживаемые домены;
- удаленные домены;
- списки надежных отправителей;

- списки заблокированных отправителей;
- получатели;
- список доменов отправки и получения, используемых для безопасного обмена данными с партнерами в домене;
- список SMTP-серверов, которые являются внутренними в конфигурации транспорта организации;
- Список серверов почтовых ящиков на подписанном сайте Active Directory

EdgeSync использует взаимно прошедший проверку подлинности и авторизованный защищенный канал LDAP для передачи данных с сервера почтовых ящиков на пограничный транспортный сервер.

Для репликации данных в AD LDS сервер почтовых ящиков выполняет привязку к серверу глобального каталога для получения обновленных данных. EdgeSync инициирует безопасный сеанс LDAP между сервером почтовых ящиков и подписанным пограничным транспортным сервером через нестандартный TCP-порт 50636.

При первой подписке пограничного транспортного сервера на сайт Active Directory время первоначальной репликации, при которой происходит заполнение служб AD LDS данными из Active Directory, зависит от количества данных в службе каталогов, и может составлять 5 минут и больше. После начальной репликации EdgeSync синхронизирует только новые и измененные объекты и удаляет все удаленные объекты.

Расписание синхронизации

Расписания синхронизации различных типов данных различаются. Расписание синхронизации EdgeSync задает максимальный интервал между синхронизациями EdgeSync. Синхронизация EdgeSync выполняется через следующие интервалы:

- Данные конфигурации: 3 минуты.
- Данные получателей: 5 минут.
- Данные топологии: 5 минут.

Эти интервалы можно изменить с помощью командлета **Set-EdgeSyncServiceConfig**. Использование командлета **Start-EdgeSynchronization** на сервере почтовых ящиков для принудительной синхронизации подписки Edge

переопределяет таймер для следующей запланированной синхронизации EdgeSync и немедленно запускает EdgeSync.

Выбор серверов почтовых ящиков

Каждый подписанный пограничный транспортный сервер связан с определенным сайтом Active Directory. Если на сайте имеется несколько серверов почтовых ящиков, то любой из них может реплицировать данные на подписанные пограничные транспортные серверы. Чтобы избежать состязания между серверами почтовых ящиков при синхронизации, выбор основного сервера почтовых ящиков происходит, как описано ниже.

1. Первоначальную репликацию выполняет сервер почтовых ящиков на сайте Active Directory, который первым выполнил сканирование топологии и обнаружил новую пограничную подписку. Поскольку такое обнаружение зависит от времени сканирования топологии, любой сервер почтовых ящиков на сайте может выполнить первоначальную репликацию.

2. Сервер почтовых ящиков, выполняющий начальную репликацию, устанавливает параметр аренды EdgeSync и устанавливает блокировку для подписки Edge. Благодаря аренде этот сервер почтовых ящиков считается основным сервером, предоставляющим службы синхронизации для данного пограничного транспортного сервера. Блокировка не позволяет EdgeSync, работающему на другом сервере почтовых ящиков, перебирать параметр аренды.

3. Параметр аренды EdgeSync длится один час. В течение этого часа никакая другая служба EdgeSync не может взять на себя этот параметр, если не будет запущена ручная синхронизация до конца часа. Если предпочтительный сервер почтовых ящиков недоступен для предоставления службы EdgeSync во время запуска синхронизации вручную, после пятиминутного ожидания блокировка освобождается, и другая служба EdgeSync может взять на себя возможность аренды и выполнить синхронизацию.

4. Если синхронизация не запущена вручную, синхронизация выполняется на основе расписания синхронизации EdgeSync. Если предпочтительный сервер недоступен при выполнении запланированной синхронизации, после пятиминутного ожидания блокировка освобождается, и другая служба EdgeSync может взять на себя возможность аренды и выполнить синхронизацию.

Этот метод блокировки и аренды предотвращает одновременное отправку данных на один и тот же пограничный транспортный сервер несколькими экземплярами EdgeSync.

Примечания.

- В организациях Exchange 2016, если у вас также есть транспортные серверы концентратора Exchange 2010 на сайте Active Directory с подпиской, серверы почтовых ящиков Exchange 2016 всегда будут иметь приоритет и выполнять репликацию.

- При подписке пограничного транспортного сервера на сайт Active Directory все серверы почтовых ящиков, установленные на этом сайте Active Directory в это время, могут участвовать в процессе синхронизации EdgeSync. Если один из этих серверов удален, служба EdgeSync, запущенная на остальных серверах почтовых ящиков, продолжит процесс синхронизации данных. Однако при последующей установке новых серверов почтовых ящиков на сайте Active Directory они не будут автоматически участвовать в синхронизации EdgeSync. Кроме того, они не будут автоматически добавлены во внутреннюю группу доставки пограничного сервера. Если вы хотите включить эти новые серверы почтовых ящиков для участия в синхронизации EdgeSync и автоматическом потоке обработки почты edge to Mailbox, вам потребуется снова подписаться на пограничный транспортный сервер.

В следующей таблице перечислены свойства EdgeSync, связанные с блокировкой и арендой. Для настройки этих свойств можно использовать командлет **Set-EdgeSyncServiceConfig**.

Свойства аренды EdgeSync

Параметр	**Значение по умолчанию**	**Описание**
LockDuration	`00:05:00` (5 минут)	Этот параметр определяет, как долго конкретная служба EdgeSync получит блокировку. Если служба EdgeSync на сервере почтовых ящиков, удерживающая эту блокировку, не отвечает, через пять минут служба EdgeSync на другом сервере почтовых ящиков возьмет на себя аренду. Принудительная немедленная синхронизация EdgeSync не переопределяет этот параметр.

Параметр	Значение по умолчанию	Описание
OptionDuration	`01:00:00` (1 час)	Этот параметр определяет, как долго служба EdgeSync может объявить вариант аренды на пограничном транспортном сервере. Если служба EdgeSync, содержащая аренду, недоступна и не перезапускается в течение этого периода, ни одна другая служба Exchange EdgeSync не возьмет на себя возможность аренды, если не будет принудительной синхронизации EdgeSync.
LockRenewalDuration	`00:01:00` (1 минута)	Этот параметр определяет частоту обновления поля блокировки, когда служба EdgeSync получает блокировку пограничного транспортного сервера.

Процедуры для пограничных подписок

Статья • 04.04.2023

После подписки на пограничный транспортный сервер на сайт Active Directory в организации Exchange, как описано в разделе Пограничные подписки, может потребоваться выполнить задачи обслуживания в пограничной подписке. Эти задачи описаны в этом разделе.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 10 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи EdgeSync и в разделе "Пограничные транспортные серверы" раздела Разрешения потока обработки почты .

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Удаление пограничной подписки

Вам иногда может понадобиться удалить пограничную подписку из организации Exchange или из организации Exchange и пограничного транспортного сервера. Если вы планируете позже повторно подписать пограничный транспортный сервер на организацию Exchange, не удаляйте с него пограничную подписку. При удалении пограничной подписки с пограничного транспортного сервера из AD LDS удаляются все реплицированные данные. При большом количестве данных получателей эта операция может занять продолжительное время.

Чтобы полностью удалить edge-подписку, необходимо выполнить эту процедуру на пограничном транспортном сервере, который требуется удалить, и на сервере почтовых ящиков Exchange 2016 или Exchange 2019 на сайте Active Directory, на котором подписан пограничный транспортный сервер.

После удаления пограничной подписки прекращается синхронизация данных из служб AD LDS. Все учетные записи, загруженные в службы AD LDS, удаляются, а пограничный транспортный сервер удаляется из списка исходных серверов любого соединителя отправки. Функции пограничного транспортного сервера, которые основываются на данных Active Directory, больше не будут доступны для использования.

1. Для удаления пограничной подписки с пограничного транспортного сервера используйте приведенный ниже синтаксис.

   ```
   PowerShell

   Remove-EdgeSubscription <EdgeTransportServerIdentity>
   ```

   Например, чтобы удалить пограничную подписку с пограничного транспортного сервера Edge01, выполните указанную ниже команду.

   ```
   PowerShell

   Remove-EdgeSubscription Edge01
   ```

2. Для удаления пограничной подписки с сервера почтовых ящиков используйте приведенный ниже синтаксис.

   ```
   PowerShell

   Remove-EdgeSubscription <EdgeTransportServerIdentity>
   ```

   Например, чтобы удалить подписку Edge для пограничного транспортного сервера с именем Edge01 на сервере почтовых ящиков на сайте Active Directory, подписанном, выполните следующую команду.

   ```
   PowerShell

   Remove-EdgeSubscription Edge01
   ```

Пограничную подписку понадобится удалить в указанных ниже случаях.

- Необходимо, чтобы пограничный транспортный сервер больше не участвовал в синхронизации EdgeSync. Вам понадобится удалить пограничную подписку с пограничного транспортного сервера и из организации Exchange.

- Пограничный транспортный сервер списывается. В этом сценарии пограничную подписку необходимо удалить только из организации Exchange. При удалении с компьютера роли пограничного транспортного сервера также будет удален экземпляр служб AD LDS и все данные Active Directory, которые хранятся в AD LDS.

- Вы хотите изменить сопоставление с сайтом Active Directory для пограничной подписки. Вам понадобится удалить пограничную подписку только из организации Exchange. После удаления пограничной подписки из организации Exchange можно повторно подписать пограничный транспортный сервер на другой сайт Active Directory.

После удаления пограничной подписки из организации Exchange выполняются приведенные ниже действия.

- Прекращается синхронизация данных из Active Directory в AD LDS.

- Учетные записи ESRA удаляются как из Active Directory, так и из служб AD LDS.

- Пограничный транспортный сервер удаляется из свойства *SourceTransportServers* любого соединителя отправки.

- Соединитель отправки входящих подключений с пограничного транспортного сервера в организацию Exchange, создаваемый автоматически, удаляется из служб AD LDS.

После удаления пограничной подписки с пограничного транспортного сервера выполняются приведенные ниже действия.

- Вы больше не можете использовать возможности пограничного транспортного сервера, которые основываются на данных Active Directory.

- Реплицированные данные удаляются из служб AD LDS.

- Задачи, которые были отключены при создании пограничной подписки, включаются повторно для поддержки локальной настройки.

Повторная подписка пограничного транспортного сервера

Иногда может потребоваться повторно подписать пограничный транспортный сервер на сайт Active Directory. При повторном создании пограничной подписки создаются новые учетные данные, и вам необходимо выполнить полный процесс

подписки Edge. Вам потребуется повторно подписаться на пограничный транспортный сервер, если:

- Вы добавляете новые серверы почтовых ящиков на подписанный сайт Active Directory и хотите включить их в синхронизацию EdgeSync.
- После создания пограничной подписки вы применили лицензионный ключ для пограничного транспортного сервера. Сведения о лицензировании для пограничного транспортного сервера записываются при создании пограничной подписки. Подписанные пограничные транспортные серверы отображаются как лицензированные, только если они подписаны на организацию Exchange после применения лицензионного ключа на пограничном транспортном сервере. Если лицензионный ключ применяется к пограничному транспортному серверу после выполнения процесса пограничной подписки, сведения о лицензировании не будут обновлены в организации Exchange, и вам потребуется повторно подписаться на пограничный транспортный сервер.
- Учетные данные ESRA скомпрометированы.

> ⓘ **Важно!**
>
> Чтобы повторно подписаться на пограничный транспортный сервер, экспортируйте новый файл подписки Edge на пограничный транспортный сервер, а затем импортируйте XML-файл на сервер почтовых ящиков. Вам потребуется повторно подписать пограничный транспортный сервер на тот же сайт Active Directory, на который он был изначально подписан. Вам не нужно сначала удалять исходную подписку Edge. процесс повторной подписки перезапишет существующую подписку Edge.

Добавление или удаление сервера почтовых ящиков

Если вы добавите сервер почтовых ящиков на сайт Active Directory, на который уже подписан пограничный транспортный сервер, новый сервер почтовых ящиков не будет автоматически включен в синхронизацию EdgeSync. Чтобы включить только что развернутый сервер почтовых ящиков в синхронизацию EdgeSync, необходимо повторно подписать каждый пограничный транспортный сервер на сайт Active Directory.

Удаление сервера почтовых ящиков из сайта Active Directory, на который подписан пограничный транспортный сервер, не влияет на синхронизацию EdgeSync, если этот сервер почтовых ящиков не является единственным подобным сервером на этом сайте. При удалении всех серверов почтовых ящиков из сайта Active Directory, на который подписаны пограничные транспортные серверы, такие пограничные транспортные серверы становятся потерянными.

Запуск EdgeSync вручную

Вам может понадобиться запустить EdgeSync вручную, если вы внесли значительные изменения в конфигурацию или получателей в службе каталогов Active Directory и хотите немедленно синхронизировать эти изменения. Вы можете запустить полную синхронизацию или синхронизировать только изменения, внесенные после последней репликации.

При синхронизации EdgeSync вручную сбрасывается расписание синхронизации EdgeSync. Время следующей автоматической синхронизации зависит от того, когда вы запустили синхронизацию вручную.

Чтобы вручную запустить EdgeSync, используйте приведенный ниже синтаксис.

PowerShell

```
Start-EdgeSynchronization [-Server <MailboxServerIdentity>] [-TargetServer
<EdgeTransportServerIdentity> [-ForceFullSync]
```

В примере ниже показано, как запустить синхронизацию EdgeSync со следующими параметрами:

- Синхронизация инициируется с сервера почтовых ящиков Exchange с именем Mailbox01.
- Все пограничные транспортные серверы синхронизированы.
- Синхронизированы только изменения с момента последней репликации.

PowerShell

```
Start-EdgeSynchronization -Server Mailbox01
```

В примере ниже показано, как запустить EdgeSync со следующими параметрами:

- Синхронизация запускается с локального сервера почтовых ящиков.

- Синхронизирован только пограничный транспортный сервер с именем Edge03.
- Все данные получателя и конфигурации полностью синхронизированы.

```
PowerShell

Start-EdgeSynchronization -TargetServer Edge03 -ForceFullSync
```

Проверка результатов EdgeSync

Для проверки пограничной синхронизации можно использовать командлет **Test-EdgeSynchronization**. Этот командлет выводит отчет о состоянии синхронизации подписанных пограничных транспортных серверов.

Выходные данные этого командлета позволяют узнать, какие объекты на пограничном транспортном сервере не синхронизованы. Задача выполняет сравнение данных, хранящихся в службе каталогов Active Directory, с данными, которые хранятся в службах AD LDS, и выводит отчет о расхождениях в данных.

Параметр *ExcludeRecipientTest* можно использовать в командлете **Test-EdgeSynchronization** , чтобы исключить проверку синхронизации данных получателя. Если включить этот параметр, проверяется только синхронизация объектов конфигурации. Проверка данных получателей занимает больше времени, чем проверка только данных конфигурации.

Проверка результатов EdgeSync для одного получателя

Чтобы проверить результаты EdgeSync для одного получателя, используйте приведенный ниже синтаксис на сервере почтовых ящиков на подписанном сайте Active Directory.

```
PowerShell

Test-EdgeSynchronization -VerifyRecipient <emailaddress>
```

В этом примере проверяются результаты EdgeSync для пользователя kate@contoso.com.

```
PowerShell
```

```
Test-EdgeSynchronization -VerifyRecipient kate@contoso.com
```

Настройка потока электронной почты через пограничные транспортные серверы без использования EdgeSync

Статья • 04.04.2023

Мы рекомендуем использовать процесс пограничной подписки для создания потока почты между организацией Exchange и пограничным транспортным сервером, как описано в разделе Пограничные подписки. Однако иногда невозможно подписать пограничный транспортный сервер на организацию Exchange. Чтобы вручную установить поток обработки почты между вашей организацией Exchange и неподписанным пограничным транспортным сервером, необходимо вручную создать и (или) изменить следующие соединители отправки и получения:

На пограничном транспортном сервере:

- Создайте выделенный соединитель отправки только для отправки сообщений в Интернет.
- Создайте выделенный соединитель отправки, чтобы отправлять сообщения только на серверы почтовых ящиков в организации Exchange. [1]
- Создание выделенного соединителя получения для получения сообщений только с серверов почтовых ящиков в организации[Exchange 2]
- Измените соединитель получения по умолчанию, чтобы принимать только сообщения из Интернета.

На сервере почтовых ящиков:

- Создание выделенного соединителя отправки для ретрансляции исходящих сообщений на пограничный транспортный сервер

[1] Соединитель отправки, созданный подпиской EdgeSync для доставки электронной почты в организацию Exchange, настроен для использования проверки подлинности Exchange Server (GSSAPI). Подписка EdgeSync определяет пограничный транспортный сервер как сервер Exchange для внутреннего леса Active Directory, что также позволяет Exchange Server проверку подлинности. По определению, в этом сценарии нет подписки EdgeSync, поэтому вам потребуется импровизировать:

- Вы можете настроить обычную проверку подлинности по протоколу TLS, чтобы обеспечить проверку подлинности и шифрование трафика электронной почты между пограничным транспортным сервером и внутренней организацией Exchange. Этот метод имеет следующие проблемы:

    - Необходимо настроить учетную запись Active Directory, принадлежащую к универсальной группе безопасности серверов Exchange Server, для проверки подлинности в соединителе Отправки сообщений, который передает сообщения с пограничного транспортного сервера во внутреннюю организацию Exchange. Обязательно защитите учетные данные учетной записи, и вы можете настроить учетную запись так, чтобы разрешить вход только на определенных компьютерах. Вам также потребуется локальная учетная запись на пограничном транспортном сервере для проверки подлинности на соединителе Отправки, который ретранслирует сообщения из внутренней организации Exchange на пограничный транспортный сервер.

    - Сообщения, поступающие от этих соединителей отправки, будут рассматриваться конечным сервером почтовых ящиков как SMTP с проверкой подлинности. Это означает, что соединитель получения по умолчанию с именем Client Frontend <ServerName> в транспортной службе переднего плана будет принимать сообщения через порт 587, а сообщения принимаются во внутренней транспортной службе с помощью соединителя получения по умолчанию с именем Client Proxy <ServerName> через порт 465.

    - Чтобы обеспечить шифрование, необходимо использовать сертификат. Самозаверяющий сертификат на пограничном транспортном сервере не будет распознана внутренней организацией Exchange (опять же, подписка EdgeSync обычно отвечает за это). Необходимо вручную импортировать самозаверяющий сертификат в каждый почтовый ящик или использовать сертификат из доверенного стороннего центра сертификации.

- Если вы не хотите, чтобы сообщения, поступающие с пограничного транспортного сервера, были идентифицированы как SMTP с проверкой подлинности и, следовательно, с помощью соответствующих клиентских соединителей получения, в качестве метода проверки подлинности можно использовать метод externally Secured. Это означает, что трафик электронной почты между *пограничным транспортным сервером* и внутренней организацией Exchange не проходит проверку подлинности или не шифруется Exchange. При использовании этого метода **необходимо** настроить и использовать внешний метод шифрования (например, IPsec или VPN).

[2] Вместо выделенного соединителя получения можно настроить и использовать соединитель получения по умолчанию на пограничном транспортном сервере для входящих интернет-сообщений и входящих сообщений с внутренних серверов почтовых ящиков (подписка EdgeSync использует этот соединитель получения для обоих подключений).

Дополнительные сведения о отправке соединителей см. в разделе Отправка соединителей. Дополнительные сведения о соединителях получения см. в разделе Соединители получения.

Перед началом работы

- Предполагаемое время выполнения задачи: 30 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Отправка соединителей", в записи "Отправка соединителей - пограничный транспорт" и в записи "Получение соединителей - пограничный транспорт" в разделе Разрешения потока обработки почты .
- На пограничных транспортных серверах можно использовать командную консоль Exchange только для создания соединителей отправки и получения. На серверах почтовых ящиков для создания соединителей отправки можно использовать Центр администрирования Exchange (EAC) или командную консоль Exchange.

  Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

  Сведения об открытии и использовании Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server.
- Базовая конфигурация пограничного транспортного сервера в сети периметра должна разрешать общедоступные домены для электронной почты в Интернете и внутренние имена узлов для внутренней электронной почты. Это можно сделать разными способами, но можно настроить сетевой адаптер, подключенный к сегменту внешней (общедоступной) сети, для использования общедоступного DNS-сервера, а сетевой адаптер, подключенный к сегменту внутренней (частной) сети, использовать DNS-сервер в сети периметра.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**.

Процедуры для пограничного транспортного сервера

Шаг 1. Создание выделенного соединителя отправки только для отправки сообщений в Интернет

Этот соединитель отправки должен иметь следующие характеристики:

- **Имя**: в Интернет (или любое описательное имя)
- **Тип использования**: Интернет
- **Адресные пространства**: "*" (все домены)
- **Параметры сети**. Используйте записи DNS MX для автоматической маршрутизации почты. При определенной конфигурации сети можно также отправлять почту через промежуточный узел. Затем интеллектуальный узел направляет почту в Интернет.

Чтобы создать соединитель отправки, настроенный для отправки сообщений в Интернет, выполните следующую команду:

PowerShell

```
New-SendConnector -Name "To Internet" -AddressSpaces * -Usage Internet -
DNSRoutingEnabled $true
```

Подробные сведения о синтаксисе и параметрах см. в статье New-SendConnector.

Шаг 2. Создание выделенного соединителя отправки для отправки сообщений только в организацию Exchange

Этот соединитель отправки должен иметь следующие характеристики:

- **Имя**: во внутреннюю организацию (или любое описательное имя)
- **Тип использования**: Внутренний
- **Адресные пространства**: `--` (указывает все обслуживаемые домены для организации Exchange)
- DNS-маршрутизация отключена (маршрутизация промежуточного узла включена).
- **Интеллектуальные узлы**: полное доменное имя одного или нескольких серверов почтовых ящиков в качестве интеллектуальных узлов. Например: mbxserver01.contoso.com и mbxserver02.contoso.com.
- **Методы проверки подлинности интеллектуального узла**: обычная проверка подлинности по протоколу TLS
- **Учетные данные проверки подлинности интеллектуального узла**. Учетные данные учетной записи пользователя во внутреннем домене, который входит в универсальную группу безопасности серверов Exchange Server. Для хранения учетных данных используйте командлет **Get-Credential**. Используйте формат*Имя пользователя> домена<\ >или имя участника-пользователя (имя участника-пользователя; например,) для ввода имени<* пользователя. chris@contoso.com

Чтобы создать соединитель для отправки сообщений в организацию Exchange, замените промежуточные узлы серверами почтовых ящиков в организации и выполните следующую команду:

PowerShell

```
New-SendConnector -Name "To Internal Org" -Usage Internal -AddressSpaces "--
" -DNSRoutingEnabled $false -SmartHosts
mbxserver01.contoso.com,mbxserver02.contoso.com -SmartHostAuthMechanism
BasicAuthRequireTLS -AuthenticationCredential (Get-Credential)
```

Подробные сведения о синтаксисе и параметрах см. в разделе New-SendConnector.

Шаг 3. Изменение соединителя получения по умолчанию так, чтобы он принимал только сообщения из Интернета

Внесите следующие изменения в конфигурацию соединителя получения по умолчанию:

- Измените имя, чтобы указать, что соединитель будет использоваться исключительно для получения электронной почты из Интернета (по умолчанию используется имя внутреннего соединителя *<получения ServerName>*).
- Измените сетевые привязки, чтобы принимать сообщения только с сетевого адаптера, доступного из Интернета (например, 10.1.1.1 и стандартного TCP-порта SMTP 25).

Чтобы изменить соединитель получения по умолчанию так, чтобы он принимал только сообщения из Интернета, *замените ServerName>* и привязыв его к имени пограничного транспортного сервера и конфигурации внешнего сетевого адаптера, а затем выполните следующую команду:<

PowerShell

```
Set-ReceiveConnector -Identity "Default internal Receive connector
ServerName>" -Name "From Internet" -Bindings 10.1.1.1:25
```

Подробные сведения о синтаксисе и параметрах см. в статье Set-ReceiveConnector.

Шаг 4. Создание выделенного соединителя получения для приема только сообщений из организации Exchange

Этот соединитель приема должен иметь указанные ниже характеристики.

- **Имя**: из внутренней организации (или любое описательное имя)
- **Тип использования**: Внутренний
- **Привязки локальной сети**: внутренний сетевой адаптер (например, 10.1.1.2 и стандартное значение TCP-порта SMTP 25).
- **Параметры удаленной сети**: IP-адрес одного или нескольких серверов почтовых ящиков в организации Exchange. Например: 192.168.5.10 и 192.168.5.20.
- **Методы проверки подлинности**: TLS, обычная проверка подлинности, обычная проверка подлинности через TLS и проверка подлинности Exchange Server.

Чтобы создать соединитель получения для приема сообщений только из организации Exchange, замените привязки и диапазоны удаленных IP-адресов

своими значениями и выполните следующую команду:

PowerShell

```
New-ReceiveConnector -Name "From Internal Org" -Usage Internal -
AuthMechanism TLS,BasicAuth,BasicAuthRequireTLS,ExchangeServer -Bindings
10.1.1.2:25 -RemoteIPRanges 192.168.5.10,192.168.5.20
```

Подробные сведения о синтаксисе и параметрах см. в статье New-ReceiveConnector.

Как проверить, все ли получилось?

Чтобы убедиться, что необходимые соединители отправки и получения успешно настроены на пограничном транспортном сервере, выполните следующую команду на пограничном транспортном сервере и проверьте значения свойств:

PowerShell

```
Get-SendConnector | Format-List
Name,Usage,AddressSpaces,SourceTransportServers,DSNRoutingEnabled,SmartHosts
,SmartHostAuthMechanism; Get-ReceiveConnector | Format-List
Name,Usage,AuthMechanism,Bindings,RemoteIPRanges
```

Процедуры сервера почтовых ящиков

Не нужно изменять соединители получения по умолчанию на серверах почтовых ящиков. Дополнительные сведения о соединителях получения по умолчанию на серверах почтовых ящиков см. в этом разделе.

Шаг 5. Создание выделенного соединителя отправки для отправки исходящих сообщений на пограничный транспортный сервер

Этот соединитель отправки должен иметь следующие характеристики:

- **Имя**: к краю (или любое описательное имя)
- **Тип использования**: Внутренний
- **Адресные пространства**: "*" (все внешние домены)
- DNS-маршрутизация отключена (маршрутизация промежуточного узла включена).

- **Интеллектуальные узлы**: IP-адрес или полное доменное имя пограничного транспортного сервера. Например: пограничный_сервер01.contoso.net.
- **Исходные серверы**: полное доменное имя одного или нескольких серверов почтовых ящиков. Например: mbxserver01.contoso.com и mbxserver02.contoso.com.
- **Методы проверки подлинности интеллектуального узла**: обычная проверка подлинности по протоколу TLS.
- **Учетные данные проверки подлинности интеллектуального узла**. Учетные данные учетной записи пользователя на пограничном транспортном сервере.

Создание соединителя для отправки исходящих сообщений на пограничный транспортный сервер в Центре администрирования Exchange

1. В EAC перейдите в раздел**Отправка соединителейпотока**> обработки почты и нажмите кнопку **Добавить**➕ Откроется мастер **создания соединителя отправки**.
2. На первой странице настройте следующие параметры:
   - **Имя**: введите в edge.
   - **Тип**: выберите **Внутренний**.

   Нажмите кнопку **Далее**.
3. На следующей странице выберите **Маршрутизировать почту через смарт-узлы** и нажмите кнопку **Добавить**➕ В появившемся диалоговом окне **Добавление интеллектуального узла** определите пограничный транспортный сервер, используя одно из следующих значений:
   - **IP-адрес**: например, 10.1.1.2.
   - **Полное доменное имя (FQDN):** например, edge01.contoso.net. Обратите внимание, что исходные серверы почтовых ящиков для соединителя отправки должны иметь возможность разрешать пограничный транспортный сервер в DNS с помощью этого FQDN. В противном случае используйте IP-адрес.

   Нажмите **Сохранить**.

4. На следующей странице, в разделе **Проверка подлинности промежуточных узлов**, выберите **Обычная проверка подлинности** и настройте эти дополнительные параметры:

    - Выберите **Предлагать обычную проверку подлинности только после запуска TLS**
    - В полях **Имя пользователя** и **Пароль** введите данные учетной записи локального пользователя на пограничном транспортном сервере.

    Нажмите кнопку **Далее**.

5. На следующей странице в разделе **Адресное пространство** нажмите кнопку **Добавить**➕ В открывшемся диалоговом окне **Добавление домена** введите следующие сведения:

    - **Тип**: убедитесь, что выбран smtp.
    - **Полное доменное имя (FQDN):** введите звездочку (*), чтобы указать, что соединитель отправки используется для всех внешних доменов.
    - **Затраты**: убедитесь, что введено значение 1. Чем ниже значение, тем предпочтительнее будет маршрут.

    Нажмите **Сохранить**.

6. На предыдущей странице имеется параметр **Соединитель отправки с заданной областью**, который важен, если серверы Exchange установлены на нескольких сайтах Active Directory в организации:

    - Если не выбрать **соединитель отправки с областью** действия, соединитель будет использоваться всеми транспортными серверами (серверами почтовых ящиков Exchange 2019, серверами почтовых ящиков Exchange 2016, серверами почтовых ящиков Exchange 2013 и транспортными серверами-концентраторами Exchange 2010) во всем лесу Active Directory. Это значение используется по умолчанию.
    - Если вы выберите **Соединитель отправки с заданной областью**, соединитель смогут использовать только другие транспортные серверы на том же сайте Active Directory.

    Нажмите кнопку **Далее**.

7. На следующей странице в разделе **Исходный сервер** нажмите кнопку **Добавить**➕ В появившемся диалоговом окне **Выбор сервера** выберите один

или несколько серверов почтовых ящиков, которые нужно использовать для отправки исходящей почты через пограничный транспортный сервер. Выберите сервер почтовых ящиков и нажмите кнопку **Добавить** (> повторить столько раз), нажмите кнопку **OK** и нажмите кнопку **Готово**.

Создание соединителя для отправки исходящих сообщений на пограничный транспортный сервер в командной консоли Exchange

Чтобы создать соединитель для отправки исходящих сообщений на пограничный транспортный сервер, замените промежуточные узлы и исходные серверы почтовых ящиков своими значениями и выполните следующую команду:

PowerShell

```
New-SendConnector -Name "To Edge" -Usage Internal -AddressSpaces * -
DNSRoutingEnabled $false -SmartHosts edge01.contoso.com -
SourceTransportServers mbxserver01.contoso.com,mbxserver02.contoso.com -
SmartHostAuthMechanism BasicAuthRequireTLS -AuthenticationCredential (Get-
Credential)
```

Подробные сведения о синтаксисе и параметрах см. в статье New-SendConnector.

Как проверить, все ли получилось?

Чтобы убедиться, что соединитель для отправки исходящих сообщений на пограничный транспортный сервер успешно создан, выполните одно из следующих действий:

- В EAC перейдите к разделу**Отправка соединителей** потока >**обработки почты**, выберите значок Отправить соединитель с именем в Edge > щелкните ✎ и проверьте значения свойств.
- В командной консоли Exchange выполните следующую команду на сервере почтовых ящиков и проверьте значения свойств:

  PowerShell

  ```
  Get-SendConnector -Identity "To Edge" | Format-List
  Usage,AddressSpaces,DSNRoutingEnabled,SmartHosts,SourceTransportServers
  ,SmartHostAuthMechanism
  ```

Exchange Server: перезапись адресов на пограничных транспортных серверах

Статья • 04.04.2023

Перезапись адресов в Exchange Server изменяет адреса электронной почты отправителей и получателей в сообщениях, которые входят в организацию или покидают их через пограничный транспортный сервер. Функции переопределения выполняют два агента транспорта на пограничном транспортном сервере: агент переопределения адресов входящих сообщений и агент переопределения адресов исходящих сообщений. Основная причина переопределения адресов исходящих сообщений — предоставить единый, согласованный домен электронной почты внешним получателям. Основная причина переопределения адресов входящих сообщений — доставка сообщений нужным получателям.

Создаваемая *запись переопределения адресов* указывает внутренние адреса (адреса электронной почты, которые вы хотите изменить) и внешние адреса (необходимые конечные адреса электронной почты). Вы можете указать, следует ли переопределять адреса электронной почты во входящих и исходящих сообщениях или только исходящих сообщениях. Вы можете создать записи для записи адресов для одного пользователя (chris@contoso.com в support@contoso.com), одного домена (contoso.com для fabrikam.com) или для нескольких поддоменов с исключениями (*.fabrikam.com для contoso.com, за исключением legal.fabrikam.com).

> **ⓘ Важно!**
>
> Вне зависимости от того, как вы планируете использовать переопределение адресов, вам необходимо убедиться, что полученные адреса электронной почты уникальны в вашей организации, чтобы исключить появление дубликатов. При переопределении адресов не проверяется уникальность переопределенных адресов электронной почты.

> **ⓘ Важно!**
>
> Подписывание DKIM не поддерживается для исходящих сообщений электронной почты с использованием перезаписных адресов, как это происходит до процесса перезаписи адресов. Если вашей организации

требуется подписывание DKIM для исходящей электронной почты, имейте в виду, что проверка DKIM завершится ошибкой после перезаписи адресов.

Сведения о настройке перезаписи адресов см. в статье Процедуры переопределения адресов на пограничных транспортных серверах.

Сценарии переопределения адресов

Приведенные ниже сценарии содержат примеры того, как вы можете использовать переопределение адресов.

- **Консолидация групп**. Некоторые организации сегментируют свои внутренние предприятия на отдельные домены, основанные на бизнес-требованиях или технических требованиях. При такой конфигурации сообщения электронной почты могут выглядеть так, как будто они отправляются отдельными группами или даже разными организациями.

  В примере ниже показано, как организация Contoso, Ltd. может скрыть свои внутренние поддомены от внешних получателей.

  - Исходящие сообщения из доменов northamerica.contoso.com, europe.contoso.com и asia.contoso.com переопределяются таким образом, чтобы все они выглядели как исходящие из одного домена contoso.com. Все сообщения переопределяются при прохождении через пограничные транспортные серверы, которые обеспечивают связь по протоколу SMTP между всей организацией и Интернетом.

  - Пограничный транспортный сервер ретранслирует входящие сообщения, адресованные получателям contoso.com, на сервер почтовых ящиков. Сообщение доставляется нужному получателю на основе прокси-адреса, настроенного в почтовом ящике получателя.

- **Слияния и поглощения**. Приобретенная компания может продолжать работать как отдельный бизнес, но вы можете использовать перезапись адресов, чтобы две организации выглядели так, как если бы они были одной интегрированной организацией.

  В примере ниже показано, как организация Contoso, Ltd. может скрыть домен электронной почты недавно приобретенной компании Fourth Coffee.

  - Contoso, Ltd. хочет, чтобы все исходящие сообщения от организации Exchange Компании Fourth Coffee отображались так, как если бы они были

получены от contoso.com. Все сообщения от обеих организаций отправляются через пограничные транспортные серверы Contoso, Ltd., на которых адреса сообщений электронной почты переопределяются с *user*@fourthcoffee.com на *user*@contoso.com.

    - Входящие сообщения *в user*@contoso.com перезаписываются и направляются в почтовые ящики *user*@fourthcoffee.com. Входящие сообщения, отправляемые *пользователю*@fourthcoffee.com, направляются непосредственно на почтовые серверы Fourth Coffee.

- **Партнеры**. Многие организации используют внешних партнеров для предоставления услуг своим клиентам, другим организациям или собственной организации. Во избежание путаницы организация может заменить домен электронной почты организации-партнера своим собственным доменом.

  В приведенном ниже примере показано, как компания Contoso, Ltd. может скрыть домен электронной почты партнера.

    - Contoso, Ltd. предоставляет поддержку более крупной организации Wingtip Toys. Wingtip Toys хочет унифицировать электронную почту для своих клиентов, и ей требуется, чтобы все сообщения от сотрудников службы поддержки Contoso, Ltd. отображались так, как если бы они были отправлены от Wingtip Toys. Все исходящие сообщения, связанные с Wingtip Toys, отправляются через пограничные транспортные серверы, а все contoso.com адреса электронной почты переписываются на wingtiptoys.com адреса электронной почты.

    - Входящие сообщения для support@wingtiptoys.com принимаются пограничными транспортными серверами Wingtip Toy, перезаписываются, а затем направляются на support@contoso.com адрес электронной почты.

Изменение свойств сообщений вследствие переопределения адресов

Стандартное SMTP-сообщение электронной почты состоит из *конверта сообщения* и его содержимого. Конверт сообщения содержит сведения, которые требуются для передачи и доставки сообщения между SMTP-серверами обмена сообщениями. Содержимое сообщения разделяется на поля заголовка сообщения, которые в совокупности называются *заголовком сообщения*, и текста сообщения. Конверт сообщения описан в документе RFC 2821, а заголовок сообщения — в документе RFC 2822.

При создании сообщения электронной почты и его отправке сообщение содержит основные сведения, требуемые для соответствия стандартам SMTP, например: отправитель, получатель, время и дата написания сообщения, необязательная строка темы и необязательный текст сообщения. Эти сведения содержатся в самом сообщении, а также, по определению, в его заголовке.

Почтовый сервер отправителя создает конверт сообщения с использованием сведений об отправителе и получателе, которые содержатся в заголовке сообщения. Затем сервер обмена сообщениями передает сообщение в Интернет для доставки на почтовый сервер получателя. Получатели не видят конверт сообщения, так как он создается в процессе передачи сообщения и фактически не является частью самого сообщения.

При переопределении адресов адрес электронной почты меняется вследствие переопределения определенных полей в заголовке или конверте сообщения. При переопределении адресов изменения вносятся в несколько полей в исходящих сообщениях электронной почты и только в одно поле — во входящих. В таблице ниже приведены поля заголовка SMTP, переопределяемые в исходящих и входящих сообщениях.

Поля сообщения, переопределяемые в исходящих и входящих сообщениях

Имя поля	**Расположение**	**Исходящие сообщения**	**Входящие сообщения**
MAIL FROM	Конверт сообщения	Перезаписывается	Не перезаписывается
RCPT TO	Конверт сообщения	Не перезаписывается	Перезаписывается
Кому	Заголовок сообщения	Не перезаписывается	Перезаписывается
Cc	Заголовок сообщения	Перезаписывается	Перезаписывается
From	Заголовок сообщения	Перезаписывается	Не перезаписывается
Sender	Заголовок сообщения	Перезаписывается	Не перезаписывается
Reply-To	Заголовок сообщения	Перезаписывается	Не перезаписывается

Имя поля	Расположение	Исходящие сообщения	Входящие сообщения
Return-Receipt-To	Заголовок сообщения	Перезаписывается	Не перезаписывается
Disposition-Notification-To	Заголовок сообщения	Перезаписывается	Не перезаписывается
Resent-From	Заголовок сообщения	Перезаписывается	Не перезаписывается
Resent-Sender	Заголовок сообщения	Перезаписывается	Не перезаписывается

Что не изменяется при переопределении адресов

При переопределении адресов не изменяются какие-либо заголовки сообщений, которые нарушили бы работу протокола SMTP. Например, изменение определенных полей заголовков может оказать влияние на обнаружение зацикливания маршрутизации, сделать цифровую подпись недопустимой или предотвратить чтение защищенного правами сообщения. Поэтому, при переопределении адресов не изменяются приведенные ниже поля заголовков.

- **Return-Path**
- **Received**
- **Message-ID**
- **X-MS-TNEF-Correlator**
- **Content-Type Boundary=string**
- Поля заголовков, расположенные в разделах MIME

При переопределении адресов игнорируются домены, которыми не управляет организация Exchange. Другими словами, домен должен быть настроен в организации Exchange в качестве заслуживающего доверия обслуживаемого домена. Переопределение не заслуживающих доверия доменов приведет к неконтролируемой ретрансляции сообщений.

Перезапись адресов также не изменяет поля заголовков сообщений, внедренных в другое сообщение. Отправители и получатели ожидают, что внедренные

сообщения останутся нетронутыми и будут доставлены без изменений до тех пор, пока сообщения не активируют правила потока обработки почты (также известные как правила транспорта), реализованные между отправителем и получателем.

Особенности переопределения адресов исходящих сообщений

При переопределении адресов исходящих сообщений на пограничном транспортном сервере изменяется адрес электронной почты отправителя, когда сообщение покидает организацию Exchange. Перезапись адресов только для исходящего трафика можно настроить для одного пользователя (chris@contoso.com в support@contoso.com), или для одного домена (contoso.com для fabrikam.com). Необходимо настроить переопределение адресов исходящих сообщений для нескольких поддоменов (*.fabrikam.com to .contoso.com).

Переопределенный адрес электронной почты необходимо настроить в качестве прокси-адреса для затронутых получателей. Например, если laura@sales.contoso.com переписать laura@contoso.comв , адрес laura@contoso.com прокси-сервера необходимо настроить в почтовом ящике Лоры. Это обеспечивает правильную доставку ответов и входящих сообщений.

Особенности переопределения адресов входящих и исходящих сообщений

Входящий и исходящий или *двунаправленный* адрес переопределения на пограничном транспортном сервере изменяет адрес электронной почты отправителя, так как сообщения покидают организацию Exchange, а адрес электронной почты получателя в качестве сообщений входит в организацию Exchange.

Двунаправленное перезапись адресов можно настроить для одного пользователя (chris@contoso.com в support@contoso.com), а для одного домена (contoso.com для fabrikam.com). Нельзя настроить двунаправленное перезапись адресов для нескольких поддоменов (*.fabrikam.com для contoso.com).

Особенности переопределения адресов электронной почты в нескольких доменах

При сведении нескольких внутренних доменов или поддоменов в один внешний домен придерживайтесь приведенных ниже рекомендаций.

- **Проверка уникальных псевдонимов**. Все псевдонимы электронной почты (часть слева от знака @) должны быть уникальными во всех поддоменах. Например, если имеется joe@sales.contoso.com, не может быть joe@marketing.contoso.com , так как перезаписанный адрес электронной почты для обоих пользователей будет иметь значение joe@contoso.com.

- **Добавление прокси-адресов**. Переопределенный адрес электронной почты необходимо настроить в качестве прокси-адреса для всех затронутых отправителей в затронутых доменах. Например, если joe@sales.contoso.com перезаписывается в joe@contoso.com, необходимо добавить адрес joe@contoso.com прокси-сервера в почтовый ящик Joe. Это обеспечивает правильную доставку ответов и входящих сообщений.

- **Почтовые контакты для организаций, не** относящихся к Exchange. Если вы переписываете адреса электронной почты из почтовой системы, отличной от Exchange, необходимо создать почтовые контакты в Exchange, чтобы представлять пользователей в системе электронной почты, отличной от Exchange. Эти контакты электронной почты должны содержать исходные и переопределенные адреса электронной почты. Например, если joe@unix.contoso.com параметр перезаписывается в joe@contoso.com, необходимо создать почтовый контакт с joe@unix.contoso.com в качестве внешнего адреса электронной почты и joe@contoso.com в качестве прокси-адреса.

Проверяйте уникальность псевдонимов.

Если вы переопределяете адреса электронной почты в нескольких поддоменах, убедитесь, что все псевдонимы электронной почты уникальны во всех поддоменах. В качестве примера рассмотрим следующую конфигурацию.

Предположим, что в поддоменах sales.contoso.com, marketing.contoso.com и research.contoso.com имеются приведенные ниже адреса пользователей.

- maria@sales.contoso.com
- chris@sales.contoso.com
- david@marketing.contoso.com
- brian@marketing.contoso.com

- chris@research.contoso.com
- adam@research.contoso.com

Предположим, вы хотите переопределить поддомены sales.contoso.com, marketing.contoso.com и research.contoso.com на один домен contoso.com.

Когда адреса электронной почты в каждом поддомене переписываются, возникает конфликт между chris@sales.contoso.com и chris@research.contoso.com, так как оба адреса электронной почты перезаписываются в chris@contoso.com. Чтобы устранить это, необходимо изменить адрес электронной почты одного из затронутых получателей. Например, можно изменить chris@research.contoso.com на christopher@research.contoso.com , чтобы адрес электронной почты был перезаписан в christopher@contoso.com.

Приоритет записей переопределения адресов

Если адрес электронной почты пользователя соответствует нескольким записям переопределения адресов, он переопределяется только один раз в соответствии с наиболее близким соответствием. В списке ниже приведен порядок применения записей переопределения адресов в соответствии с приоритетом (от самого высокого к самому низкому).

1. **Отдельные адреса электронной почты**. Запись перезаписи адреса адреса настраивается для перезаписи адреса john@contoso.com электронной почты на support@contoso.com.
2. **Сопоставление доменов или поддоменов**. Запись перезаписи адреса адреса настраивается для перезаписи всех contoso.com адресов электронной почты в northwindtraders.com или всех sales.contoso.com адресов электронной почты в contoso.com.
3. **Выравнивание домена**. Запись перезаписи адреса настраивается для перезаписи *.contoso.com адресов электронной почты в contoso.com.

Например, рассмотрим пограничный транспортный сервер, на котором настроены приведенные ниже записи переопределения адресов исходящей почты.

- Адреса электронной почты *.contoso.com переопределяются на contoso.com.
- Адреса электронной почты japan.sales.contoso.com переопределяются на contoso.jp.

Если masato@japan.sales.contoso.com отправляет сообщение электронной почты, адрес переписывается в masato@contoso.jp, так как эта запись наиболее точно соответствует адресу электронной почты отправителя.

Сообщения с цифровой подписью, зашифрованные и защищенные правами

Переопределение адресов не должно затрагивать большинство подписанных, зашифрованных или защищенных правами сообщений. Если переопределение адресов может сделать недопустимым или иным образом изменить состояние безопасности сообщений этих типов, переопределение адресов не применяется.

Приведенные ниже значения можно переопределять, поскольку сведения не относятся к подписи, шифрованию сообщения или защите прав.

- Поля в конверте сообщения.
- Заголовки верхнего уровня в тексте сообщения.

Приведенные ниже значения не переопределяются, поскольку сведения относятся к подписи, шифрованию сообщения или защите прав.

- Поля заголовков, расположенные в разделах MIME, которые можно подписать.
- Строковый параметр границы типа содержимого MIME.

Процедуры переопределения адресов на пограничных транспортных серверах

Статья • 04.04.2023

На пограничных транспортных серверах можно создать записи переопределения адресов, которые будут применяться к отдельному получателю, к определенному домену или поддомену либо к нескольким поддоменам. Переопределение адресов может применяться только к исходящим сообщениям или входящим и исходящим сообщениям одновременно (двунаправленное переопределение адресов). Создавая записи переопределения адресов, помните о приведенном ниже.

- Убедитесь, что в организации используются уникальные адреса электронной почты, полученные в результате.
- В значениях адресов электронной почты поддерживаются только буквенные строки.
- Подстановочный знак (*) поддерживается только во внутреннем адресе (адресах, которые нужно изменить). При использовании подстановочного знака допускается следующий синтаксис: ***.contoso.com**. Запрещено использовать значения ***contoso.com** или **sales.*.com**.
- При использовании подстановочного знака необходимо настроить перезапись адресов только как исходящий (необходимо задать для параметра *OutboundOnly* значение `$true`), а для перезаписи адресов только для исходящего трафика требуется настроить перезаписанный адрес электронной почты в качестве прокси-адреса для затронутых получателей.
- По умолчанию перезапись адресов является двунаправленной для одного получателя или для определенного домена или поддомена (значение по умолчанию для параметра *OutboundOnly* — `$false`).

Дополнительные сведения о переопределении адресов см. в разделе Переопределение адресов на пограничных транспортных серверах.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 10 минут.

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Пограничные транспортные серверы" раздела Разрешения потока обработки почты .
- Для выполнения этой процедуры можно использовать только PowerShell. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Соблюдайте осторожность при настройке переопределения адресов. Любые внесенные изменения применяются немедленно после выполнения команды. Попробуйте выполнить команду с помощью параметра *WhatIf*. Дополнительные сведения о параметре *WhatIf* см. в разделе WhatIf and Confirm.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Включение и выключение переопределения адресов с помощью Командная консоль Exchange

Чтобы полностью включить или отключить переопределение адресов, необходимо включить либо отключить его агенты. По умолчанию агенты переопределения адресов включены на пограничном транспортном сервере.

Чтобы отключить переопределение адресов, выполните следующую команду:

PowerShell

```
Disable-TransportAgent "Address Rewriting Inbound Agent"; Disable-
TransportAgent "Address Rewriting Outbound Agent"
```

Чтобы включить переопределение адресов, выполните следующую команду:

PowerShell

```
Enable-TransportAgent "Address Rewriting Inbound Agent"; Enable-
TransportAgent "Address Rewriting Outbound Agent"
```

Как проверить, все ли получилось?

Для проверки успешности включения или выключения переопределения адресов выполните следующую команду, чтобы проверить значение свойства **Enabled**:

PowerShell

```
Get-TransportAgent "Address Rewriting *"
```

Просмотр записей переопределения адресов с помощью Командная консоль Exchange

Чтобы просмотреть сводный список всех записей переопределения адресов, выполните приведенную ниже команду.

PowerShell

```
Get-AddressRewriteEntry
```

Чтобы просмотреть сведения о записи переопределения адресов, используйте указанный ниже синтаксис.

PowerShell

```
Get-AddressRewriteEntry <AddressRewriteEntryIdentity> | Format-List
```

В примере ниже показаны сведения о записи переопределения адресов "Rewrite Contoso.com to Northwindtraders.com".

PowerShell

```
Get-AddressRewriteEntry "Rewrite Contoso.com to Northwindtraders.com" |
Format-List
```

Дополнительные сведения см. в статье Get-AddressRewriteEntry.

Создание записей переопределения адресов с помощью Командная консоль Exchange

Переопределение адресов электронной почты отдельных получателей

Чтобы переопределить адрес электронной почты для отдельного получателя, используйте указанный ниже синтаксис.

PowerShell

```
New-AddressRewriteEntry -Name "<Descriptive Name>" -InternalAddress
<internal email address> -ExternalAddress <external email address> [-
OutboundOnly <$true | $false>]
```

В этом примере перезаписывается адрес электронной почты всех сообщений, входящих и покидающих организацию Exchange для joe@contoso.com. Исходящие сообщения перезаписываются, поэтому они, как представляется, поступают из support@nortwindtraders.com. Входящие сообщения, отправляемые support@northwindtraders.com в, перезаписываются joe@contoso.com в для доставки получателю (по умолчанию параметр *OutboundOnly*).`$false`

PowerShell

```
New-AddressRewriteEntry -Name "joe@contoso.com to
support@northwindtraders.com" -InternalAddress joe@contoso.com -
ExternalAddress support@northwindtraders.com
```

Переопределение адресов электронной почты для отдельного домена или поддомена

Чтобы переопределить адреса электронной почты для отдельного домена или поддомена, используйте следующий синтаксис:

PowerShell

```
New-AddressRewriteEntry -Name "<Descriptive Name>" -InternalAddress <domain
or subdomain> -ExternalAddress <domain> [-OutboundOnly <$true | $false>]
```

В этом примере переопределяются адреса электронной почты всех входящих и исходящих сообщений организации Exchange для пользователей в домене

contoso.com. Исходящие сообщения переопределяются таким образом, что они приходят с домена fabrikam.com. Входящие сообщения, отправляемые на fabrikam.com адреса электронной почты, перезаписываются в contoso.com для доставки получателям (параметр *OutboundOnly* по `$false` умолчанию).

PowerShell

```
New-AddressRewriteEntry -Name "Contoso to Fabrikam" -InternalAddress
contoso.com -ExternalAddress fabrikam.com
```

В этом примере переопределяются адреса электронной почты всех исходящих сообщений организации Exchange в поддомене sales.contoso.com. Исходящие сообщения переопределяются таким образом, что они приходят с домена contoso.com. Входящие сообщения, отправляемые по адресам электронной почты contoso.com, не переопределяются.

PowerShell

```
New-AddressRewriteEntry -Name "sales.contoso.com to contoso.com" -
InternalAddress sales.contoso.com -ExternalAddress contoso.com -OutboundOnly
$true
```

Переопределение адресов электронной почты для нескольких поддоменов

Чтобы переопределить адреса электронной почты в домене или всех поддоменах, используйте следующий синтаксис:

PowerShell

```
New-AddressRewriteEntry -Name "<Descriptive Name>" -InternalAddress *.
<domain> -ExternalAddress <domain> -OutboundOnly $true [-ExceptionList
<domain1,domain2...>]
```

В этом ниже переопределяются адреса электронной почты всех исходящих сообщений организации Exchange в домене contoso.com и всех поддоменах. Исходящие сообщения переопределяются таким образом, что они приходят с домена contoso.com. Входящие сообщения, отправляемые получателям contoso.com, нельзя переписать, так как в параметре *InternalAddress используется подстановочный* знак.

PowerShell

```
New-AddressRewriteEntry -Name "Rewrite all contoso.com subdomains" -
InternalAddress *.contoso.com -ExternalAddress contoso.com -OutboundOnly
$true
```

Единственное отличие данного примера от предыдущего состоит в том, что сообщения, отправляемые в поддоменах legal.contoso.com и corp.contoso.com, не переопределяются.

PowerShell

```
New-AddressRewriteEntry -Name "Rewrite all contoso.com subdomains except
legal.contoso.com and corp.contoso.com" -InternalAddress *.contoso.com -
ExternalAddress contoso.com -OutboundOnly $true -ExceptionList
legal.contoso.com,corp.contoso.com
```

Дополнительные сведения см. в статье New-AddressRewriteEntry.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно создали записи переопределения адресов, выполните приведенные ниже действия.

1. Замените <*AddressRewriteEntryIdentity*> именем записи переопределения адреса и выполните следующую команду, чтобы проверить значения свойств:

   PowerShell

   ```
   Get-AddressRewriteEntry <AddressRewriteEntryIdentity> | Format-List
   ```

2. Отправьте проверочное сообщение на внешний почтовый ящик из почтового ящика, на который влияет запись переопределения адресов. Убедитесь, что проверочное сообщение приходит с переопределенного адреса электронной почты.

3. Ответьте на проверочное сообщение из внешнего почтового ящика. Убедитесь, что ответ доставлен в исходный почтовый ящик.

Изменение записей переопределения адресов с помощью Командная консоль Exchange

Параметры конфигурации, доступные при изменении существующей записи переопределения адресов, не отличаются от параметров конфигурации, которые применяются при создании новой записи переопределения адресов.

Изменение записи переопределения адресов для отдельного получателя

Чтобы изменить запись переопределения адреса электронной почты для отдельного получателя, используйте указанный ниже синтаксис.

PowerShell

```
Set-AddressRewriteEntry <AddressRewriteEntryIdentity> [-Name "<Descriptive
Name>"] [-InternalAddress <internal email address>] [-ExternalAddress
<external email address>] [-OutboundOnly <$true | $false>]
```

В этом примере изменяются следующие свойства записи перезаписи адреса с именем "joe@contoso.com на support@nortwindtraders.com":

- Изменяет внешний адрес на support@northwindtraders.net.
- Изменяет имя записи переопределения адреса на "joe@contoso.com на support@northwindtraders.net".
- Изменяет значение *OutboundOnly* на `$true`. Обратите внимание, что это изменение требует настройки support@northwindtraders.net в качестве прокси-адреса в почтовом ящике Joe.

PowerShell

```
Set-AddressRewriteEntry "joe@contoso.com to support@nortwindtraders.com" -
Name "joe@contoso.com to support@northwindtraders.net" -ExternalAddress
support@northwindtraders.net -OutboundOnly $true
```

Изменение записи переопределения адресов для отдельного домена или поддомена

Чтобы изменить запись переопределения адресов электронной почты в отдельном домене или поддомене, используйте следующий синтаксис:

PowerShell

```
Set-AddressRewriteEntry <AddressRewriteEntryIdentity> [-Name "<Descriptive
Name>"] [-InternalAddress <domain or subdomain>] [-ExternalAddress <domain>]
[-OutboundOnly <$true | $false>]
```

В этом примере изменяется значение внутреннего адреса записи переопределения адресов "Northwind Traders to Contoso".

PowerShell

```
Set-AddressRewriteEntry "Northwindtraders to Contoso" -InternalAddress
northwindtraders.net
```

Изменение записи переопределения адресов для нескольких доменов

Чтобы изменить запись переопределения адресов электронной почты в домене и всех поддоменах, используйте следующий синтаксис:

PowerShell

```
Set-AddressRewriteEntry <AddressRewriteEntryIdentity> [-Name "<Descriptive
Name>"] [-InternalAddress *.<domain>] [-ExternalAddress <domain>] [-
ExceptionList <list of domains>]
```

Чтобы заменить значения в существующем списке исключений для записи переопределения адресов, используйте следующий синтаксис:

PowerShell

```
Set-AddressRewriteEntry <AddressRewriteEntryIdentity> -ExceptionList
<domain1,domain2,...>
```

В этом примере заменяется существующий список исключений для записи переопределения адресов "Contoso to Northwind Traders"; при этом заменяются значения marketing.contoso.com и legal.contoso.com.

PowerShell

```
Set-AddressRewriteEntry "Contoso to Northwind Traders" -ExceptionList
sales.contoso.com,legal.contoso.com
```

Чтобы добавить или удалить значения в списке исключений, не изменяя в нем другие записи, используйте следующий синтаксис:

```
PowerShell

Set-AddressRewriteEntry <AddressRewriteEntryIdentity> -ExceptionList @{Add="
<domain1>","<domain2>"...; Remove="<domain3>","<domain4>"...}
```

В этом примере в список исключений записи переопределения адресов "Contoso to Northwind Traders" вносятся следующие изменения: добавляется значение finance.contoso.com и удаляется значение marketing.contoso.com.

```
PowerShell

Set-AddressRewriteEntry "Contoso to Northwind Traders" -ExceptionList
@{Add="finanace.contoso.com"; Remove="marketing.contoso.com"}
```

Дополнительные сведения см. в статье Set-AddressRewriteEntry.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно изменили запись переопределения адресов, выполните приведенные ниже действия.

1. Замените *<AddressRewriteEntryIdentity>* именем записи переопределения адреса и выполните следующую команду, чтобы проверить значения свойств:

   ```
   PowerShell

   Get-AddressRewriteEntry <AddressRewriteEntryIdentity> | Format-List
   ```

2. Отправьте проверочное сообщение на внешний почтовый ящик из почтового ящика, на который влияет запись переопределения адресов. Убедитесь, что проверочное сообщение приходит с переопределенного адреса электронной почты.

3. Ответьте на проверочное сообщение из внешнего почтового ящика. Убедитесь, что ответ доставлен в исходный почтовый ящик.

Удаление записей переопределения адресов с помощью Командная консоль Exchange

Чтобы удалить отдельную запись переопределения адресов, используйте указанный ниже синтаксис.

PowerShell

```
Remove-AddressRewriteEntry <AddressRewriteEntryIdentity>
```

В этом примере удаляется запись переопределения адресов "Contoso.com to Northwindtraders.com".

PowerShell

```
Remove-AddressRewriteEntry "Contoso.com to Northwindtraders.com"
```

Чтобы удалить несколько записей переопределения адресов, используйте указанный ниже синтаксис.

PowerShell

```
Get-AddressRewriteEntry [<search criteria>] | Remove-AddressRewriteEntry [-
WhatIf]
```

В этом примере удаляются все записи переопределения адресов.

PowerShell

```
Get-AddressRewriteEntry | Remove-AddressRewriteEntry
```

В этом примере имитируется удаление записей переопределения адресов, в именах которых содержится текст "to contoso.com". Параметр *WhatIf* позволяет просмотреть результат без фиксации изменений.

PowerShell

```
Get-AddressRewriteEntry "*to contoso.com" | Remove-AddressRewriteEntry -
WhatIf
```

Если результат вас устраивает, выполните команду еще раз без переключателя *WhatIf* , чтобы удалить записи перезаписи адресов.

PowerShell

```
Get-AddressRewriteEntry "*to contoso.com" | Remove-AddressRewriteEntry
```

Дополнительные сведения см. в статье Remove-AddressRewriteEntry.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно удалили запись переопределения адресов, выполните приведенные ниже действия.

1. Выполните команду `Get-AddressRewriteEntry` и убедитесь, что удаленные записи перезаписи адресов отсутствуют в списке.

2. Отправьте проверочное сообщение на внешний почтовый ящик из почтового ящика, на который влияет запись переопределения адресов. Убедитесь, что удаленная запись переопределения адресов не затрагивает проверочное сообщение.

3. Ответьте на проверочное сообщение из внешнего почтового ящика. Убедитесь, что ответ доставлен в исходный почтовый ящик, а удаленная запись переопределения адресов не затрагивает сообщение.

Импорт записей переопределения адресов на пограничных транспортных серверах в Exchange Server

Статья • 04.04.2023

С помощью файла данных с разделителями-запятыми (CSV) вы можете массово создавать или импортировать данные перезаписи адресов в пограничный транспортный сервер. В списке ниже представлено описание часто используемых сценариев, в соответствии с которыми необходимо выполнить следующие действия.

- Замена решения перезаписи адреса с помощью пограничного транспортного сервера.
- Заключение соглашения со сторонним поставщиком решений, по условиям которого вы должны выполнить переопределение своих адресов электронной почты.
- Вы приобрели другую организацию и вам необходимо временно переопределить адреса электронной почты в приобретенной организации.

Для создания CSV-файла можно использовать приложение электронной таблицы, например Microsoft Excel. Отформатируйте файл, как описано в этом разделе, и сохраните его как CSV-файл.

В первой строке или *строке заголовков* CSV-файла перечисляются имена параметров. Параметры разделяются запятыми. Описание обязательных и дополнительных параметров представлено в таблице ниже.

Параметр	**Обязательный или дополнительный**	**Описание**
Name	Обязательный	Уникальное, описательное имя записи для замены адреса.

Параметр	Обязательный или дополнительный	Описание
InternalAddress	Обязательный	Адрес, который требуется изменить. Можно использовать следующие значения: • Один адрес электронной почты (chris@contoso.com) • Отдельный домен или поддомен (contoso.com или sales.contoso.com) • Домен и все поддомены (*.contoso.com)
ExternalAddress	Обязательный	Желаемый адрес электронной почты. Можно использовать следующие значения: • Один адрес электронной почты, если вы указали один адрес электронной почты для *InternalAddress*. • Один домен или поддомен для всех остальных значений *InternalAddress*
ExceptionList	Необязательный	Доступно только при перезаписи адресов электронной почты в домене и всех поддоменах (*.contoso.com). Указывает одни или несколько поддоменов, которые требуется исключить из перезаписи адресов. Заключите значение в двойные кавычки и разделяйте отдельные значения запятыми. Например, `"marketing.contoso.com"` или `"marketing.contoso.com,legal.contoso.com"`.
OutboundOnly	Необязательный	`False` означает, что адреса записаны на входящие и исходящие почтовые сообщения. `True` означает, что адреса перезаписаны только на исходящие почтовые сообщения, и необходимо вручную настроить перезаписанный адрес электронной почты в качестве адреса прокси-сервера для затронутых получателей. Значение по умолчанию — `False`, но необходимо задать для него значение `True` , если *InternalAddress содержит подстановочный* знак (*.contoso.com). Значение параметра *OutboundOnly* в CSV-файле равно `True` или `False`, а не `$True` .`$False`

Каждая строка под строкой заголовков представляет отдельную запись переопределения адресов. Значения в каждой строке должны следовать в том же порядке, что и имена параметров в строке заголовков. Значения разделяются запятыми.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 15 минут.
- Убедитесь, что вы понимаете последствия перезаписи адресов. Например, переопределенный адрес электронной почты должен быть уникальным в вашей организации Exchange, и может потребоваться настроить прокси-адреса для затронутых получателей. Дополнительные сведения см. в разделах Перезапись адресов на пограничных транспортных серверах и Процедуры переопределения адресов на пограничных транспортных серверах.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Агент перезаписи адресов" в разделе Разрешения потока обработки почты .
- При наличии нескольких пограничных транспортных серверов мы рекомендуем выполнить указанные в этом разделе процедуры, чтобы импортировать записи переопределения адресов на один пограничный транспортный сервер, а затем клонировать конфигурацию этого пограничного транспортного сервера на другие пограничные транспортные серверы в организации. Дополнительные сведения о клонировании пограничного транспортного сервера см. в разделе Using Edge Transport Server Cloned Configuration.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Шаг 1. Создайте CSV-файл.

После создания CSV-файла следует учесть перечисленные ниже моменты.

- Если вы указываете значения для дополнительных параметров в CSV-файле, каждая строка должна включать значение в этом столбце. Если вы хотите создать несколько записей переопределения адресов, где дополнительные параметры будут только у некоторых записей, вам необходимо разделить эти

записи переопределения адресов в отдельные CSV-файлы, а затем отдельно импортировать каждый CSV-файл.

- Если CSV-файл содержит символы, не входящие в набор ASCII, сохраните его в кодировке UTF-8 или иной кодировке Юникода. Сохранить CSV-файл в кодировке UTF-8 или другой кодировке Юникода может оказаться проще, если язык системы соответствует языку, используемому в CSV-файле.

В следующем примере показано заполнение CSV-файла с помощью необязательных параметров *ExceptionList* и *OutboundOnly*.

CSV

```
Name,InternalAddress,ExternalAddress,ExceptionList,OutboundOnly
"Wingtip
UK",*.wingtiptoys.co.uk,tailspintoys.com,"legal.wingtiptoys.co.uk,finance.wi
ngtiptoys.co.uk,support.wingtiptoys.co.uk",True
"Wingtip
USA",*.wingtiptoys.com,tailspintoys.com,"legal.wingtiptoys.com,finance.wingt
iptoys.com,support.wingtiptoys.com,corp.wingtiptoys.com",True
"Wingtip
Canada",*.wingtiptoys.ca,tailspintoys.com,"legal.wingtiptoys.ca,finance.wing
tiptoys.ca,support.wingtiptoys.ca",True
```

Шаг 2. Импортирование CSV-файла.

Чтобы импортировать CSV-файл, используйте следующий синтаксис.

PowerShell

```
Import-Csv <FileNameAndPath> | ForEach {New-AddressRewriteEntry -Name
$_.Name -InternalAddress $_.InternalAddress -ExternalAddress
$_.ExternalAddress -OutboundOnly ([Bool]::Parse($_.OutboundOnly)) -
ExceptionList $_.ExceptionList}
```

В этом примере показан импорт записей для замены адреса из папки C:\My Documents\ImportAddressRewriteEntries.csv.

CSV

```
Import-Csv "C:\My Documents\ImportAddressRewriteEntries.csv" | ForEach {New-
AddressRewriteEntry -Name $_.Name -InternalAddress $_.InternalAddress -
ExternalAddress $_.ExternalAddress -OutboundOnly
([Bool]::Parse($_.OutboundOnly)) -ExceptionList $_.ExceptionList}
```

Как проверить, что шаг выполнен?

Чтобы убедиться, что записи переопределения адресов были импортированы из CSV-файла успешно, выполните любое из приведенных ниже действий.

- Чтобы просмотреть все записи переопределения адресов, выполните следующую команду:

  PowerShell

  ```
  Get-AddressRewriteEntry
  ```

- Чтобы просмотреть сведения о конкретной записи перезаписи адреса, замените *<AddressRewriteIdentity>* именем записи переопределения адреса и выполните следующую команду:

  PowerShell

  ```
  Get-AddressRewriteEntry "<AddressRewriteIdentity>" | Format-List
  ```

Службы клиентского доступа

Статья • 04.04.2023

В Exchange Server службы клиентского доступа на серверах почтовых ящиков предоставляют службы проверки подлинности и прокси-сервера для внутренних и внешних клиентских подключений. Службы клиентского доступа не имеют состояния, поэтому данные не помещаются в очередь и не хранятся в них. В Exchange Server службы клиентского доступа являются частью сервера почтовых ящиков, поэтому вы не можете настроить автономный сервер клиентского доступа, как в предыдущих версиях Exchange. Дополнительные сведения см. в разделе Архитектура протокола клиентского доступа.

Подключение клиента в Exchange 2016 и Exchange 2019 аналогично Exchange 2013, но отличается от Exchange 2010:

- Клиенты Outlook используют протокол MAPI/HTTP или Мобильный Outlook (RPC/HTTP). В Exchange 2016 и Exchange 2019 mapi через HTTP включен по умолчанию.
- Exchange 2016 и Exchange 2019 требуется меньше пространств имен для устойчивых к сайту решений, чем Exchange 2010. Дополнительные сведения см. в статье Планирование пространства имен в Exchange 2016.

Функциональность служб клиентского доступа

Службы клиентского доступа в Exchange Server работают как front door, допуская все запросы на подключение клиентов и перенаправляя их в правильную базу данных почтовых ящиков. Службы клиентского доступа обеспечивают безопасность сети (например, с помощью шифрования TLS) и управляют клиентскими подключениями благодаря перенаправлению или проксированию. Службы клиентского доступа обеспечивают проверку подлинности клиентских подключений и обычно проксируют запрос на подключение серверу почтовых ящиков, на котором хранится активная копия почтового ящика пользователя. В некоторых случаях службы клиентского доступа могут перенаправить запрос аналогичным службам на другом сервере Exchange Server, который расположен в другом месте или имеет более позднюю версию Exchange.

Службы клиентского доступа имеют следующие функции:

- **Службы без отслеживания состояния**. В предыдущих версиях Exchange для многих протоколов клиентского доступа требовалось сходство сеансов. Например, Outlook Web App в Exchange 2010 требует, чтобы все запросы от определенного клиента обрабатывались определенным сервером клиентского доступа в массиве серверов клиентского доступа с балансировкой нагрузки. В Exchange 2016 и Exchange 2019 службы клиентского доступа не имеют состояния. Другими словами, так как вся обработка для почтового ящика выполняется во внутренних службах на сервере почтовых ящиков, не имеет значения, какой экземпляр службы клиентского доступа в массиве служб клиентского доступа получает каждый отдельный клиентский запрос. Это означает, что сходство сеансов больше не требуется на уровне подсистемы балансировки нагрузки. Это позволяет сбалансировать входящие подключения к службам клиентского доступа с помощью простых методов балансировки нагрузки, таких как циклический перебор DNS. Это также позволяет устройствам аппаратной балансировки нагрузки поддерживать значительно больше одновременных подключений. Дополнительные сведения см. в статье Балансировка нагрузки в Exchange 2016.

- **Пул подключений**. Службы клиентского доступа обрабатывают проверку подлинности клиента и отправляют данные **authN** в сервере почтовых ящиков. Учетная запись, используемая службами клиентского доступа для подключения к внутренним службам на серверах почтовых ящиков, является привилегированной учетной записью, которая входит в группу серверов Exchange Server. Это позволяет службам клиентского доступа эффективно пулировать подключения к серверным службам на серверах почтовых ящиков. Массив служб клиентского доступа может обрабатывать миллионы клиентских подключений из Интернета, но гораздо меньше подключений используется для прокси-запросов к внутренним службам на серверах почтовых ящиков, чем в Exchange 2010. Это повышает эффективность обработки и сквозную задержку.

> ⓘ **Примечание**
>
> Не путайте массив служб клиентского доступа с массивом сервера клиентского доступа RPC, который использовался для клиентских подключений RPC через TCP в Exchange 2010. В Exchange 2016 и Exchange 2019 массив служб клиентского доступа просто указывает на группу служб клиентского доступа с балансировкой нагрузки на серверах Exchange 2016 или Exchange 2019.

Задачи управления в службах клиентского доступа

- **Цифровые сертификаты**. Хотя Exchange Server использует самозаверяемые сертификаты для шифрования и проверки подлинности подключений между серверами Exchange, необходимо установить и настроить сертификаты для шифрования клиентских подключений. Дополнительные сведения см. в статье Цифровые сертификаты и шифрование в Exchange Server.

- **Проверка подлинности Kerberos для служб клиентского доступа с балансировкой нагрузки**. Дополнительные сведения см. в статье Настройка проверки подлинности Kerberos для служб клиентского доступа с балансировкой нагрузки.

Центр администрирования Exchange в Exchange Server

Статья • 11.02.2025

Центр администрирования Exchange (EAC) — это веб-консоль управления в Exchange Server, оптимизированный для локальных, сетевых и гибридных развертываний Exchange. Центр администрирования Exchange впервые появился в Exchange Server 2013, заменив консоль управления Exchange (EMC) и панель управления Exchange (ECP), которые являлись интерфейсами управления в Exchange Server 2010.

Ищете Exchange Online версию этой статьи? См. раздел Центр администрирования Exchange в Exchange Online.

Ищете автономную версию Exchange Online Protection (EOP) этой статьи? См. раздел Центр администрирования Exchange в EOP.

Вход в Центр администрирования Exchange

URL-адрес Центра администрирования Exchange управляется виртуальным каталогом Службы IIS (IIS) под названием ECP, который располагается в службах клиентского доступа (интерфейсных службах) на сервере почтовых ящиков. Да, виртуальный каталог называется ECP, а не EAC.

- **Внутренний URL-адрес**. По умолчанию это значение содержит полное доменное имя (FQDN) сервера Exchange в формате `https://<ServerFQDN>/ecp`. Например, `https://mailbox01.contoso.com/ecp`. Для доступа к EAC в веб-браузере на самом сервере Exchange Server можно использовать значение `https://localhost/ecp`.

- **Внешний URL-адрес**. По умолчанию это значение не настроено. Для подключения к Центру администрирования Exchange через Интернет, необходимо настроить указанные ниже параметры.

  - Внешний URL-адрес для виртуального каталога ECP. Дополнительные сведения см. в разделе Шаг 4. Настройка внешних URL-адресовв статье Настройка потока обработки почты и клиентского доступа на серверах Exchange Server.

  - Соответствующую запись в общедоступном DNS.

- Сертификат TLS, содержащий или соответствующий записи имени узла. Скорее всего, этот сертификат является сертификатом с альтернативным именем субъекта (SAN) или подстановочным знаком, так как большинство клиентских служб доступны на одном веб-сайте на сервере Exchange Server. Дополнительные сведения см. в статье Требования к сертификатам для служб Exchange.

  После настройки параметров общее значение внешнего URL-адреса для EAC будет выглядеть так: `https://mail.contoso.com/ecp`.

  Примечание. Внешним пользователям, подключающимся к Outlook в Интернете (ранее Outlook Web App), также требуется доступ к EAC для доступа к собственной странице **параметров**. Вы можете отключить доступ внешнего администратора к EAC, но при этом разрешить пользователям доступ к странице **параметров** в Outlook в Интернете. Дополнительные сведения см. в статье Отключение доступа к Центру администрирования Exchange.

Самый простой способ найти значения внутренних и внешних URL-адресов для Центра администрирования Exchange (без использования**виртуальных каталоговсерверов**> в самом EAC) — использовать командлет **Get-EcpVirtualDirectory** в командной консоли Exchange. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

В приведенных примерах показано, как найти значения внутренних и внешних URL-адресов виртуальных каталогов Центра администрирования Exchange в вашей организации.

- Чтобы найти значения для всех серверов Exchange в организации, выполните следующую команду:

```
PowerShell

Get-EcpVirtualDirectory | Format-List Server,Name,*Url
```

- Чтобы найти значения на сервере с именем `Mailbox01`, выполните следующую команду:

```
PowerShell

Get-EcpVirtualDirectory | Format-List Name,*Url
```

- Чтобы найти значение для виртуального каталога `ecp (Default Web Site)` на сервере с именем `Mailbox01`, выполните следующую команду.

  PowerShell

  ```
  Get-EcpVirtualDirectory -Identity "Mailbox01\ecp (Default Web Site)" |
  Format-List *Url
  ```

Дополнительные сведения см. в статье Get-EcpVirtualDirectory.

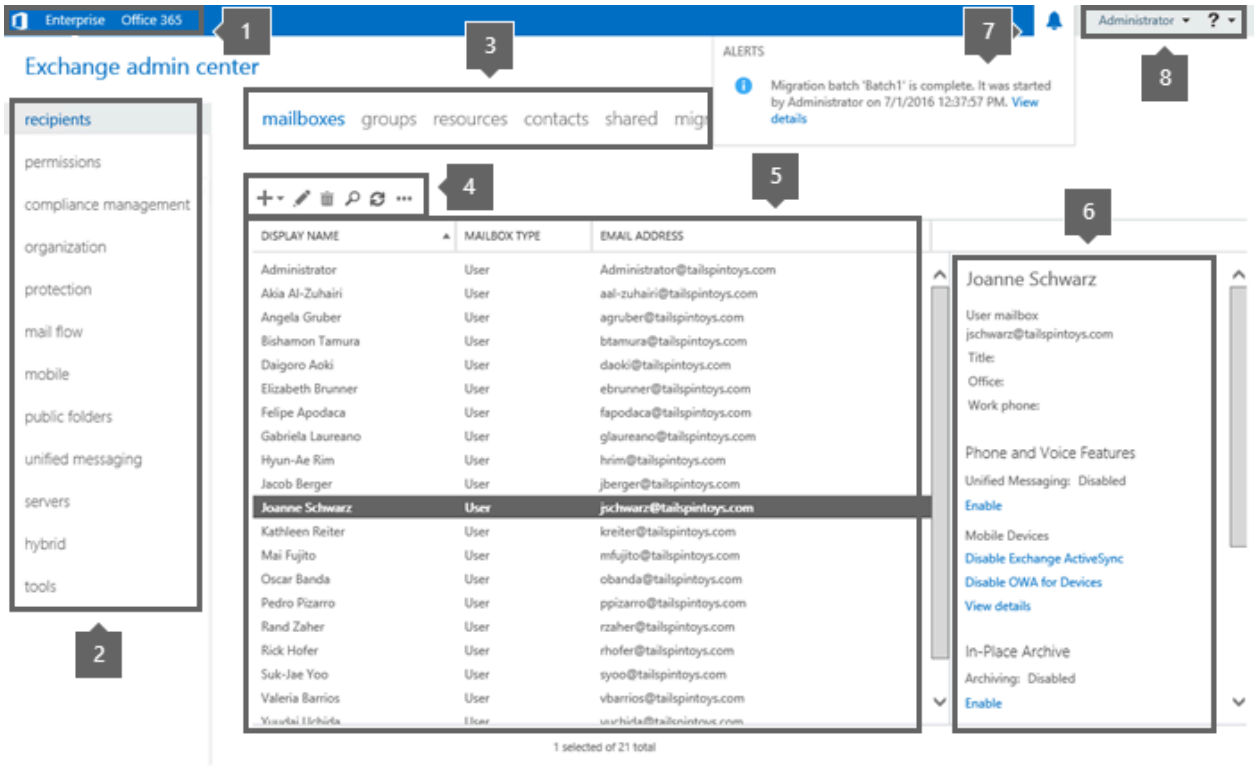
В Exchange 2016, если вы находитесь в среде сосуществования с Exchange 2010, расположение почтового ящика управляет поведением по умолчанию для открытия EAC или ECP:

- Если ваш почтовый ящик находится на сервере почтовых ящиков Exchange 2010, то по умолчанию для Exchange 2010 открывается панель управления Exchange. Вы можете войти в Центр администрирования Exchange, добавив версию Exchange в URL-адрес (значение версии — 15 как для Exchange 2013, так и для Exchange 2016). Например, чтобы получить доступ к EAC через службы клиентского доступа (внешний) на сервере почтовых ящиков с именем `Mailbox01`, используйте следующий URL-адрес: `https://Mailbox01/ecp/?ExchClientVer=15`.

- Если почтовый ящик находится на сервере почтовых ящиков Exchange 2016 и вы хотите получить доступ к ECP на сервере клиентского доступа Exchange 2010 с именем CAS01, используйте следующий URL-адрес: `https://CAS01/ecp/?ExchClientVer=14`.

Общие элементы пользовательского интерфейса в Центре администрирования Exchange

В этом разделе рассматриваются элементы пользовательского интерфейса, которые являются общими для Центра администрирования Exchange.



1. Распределенная навигация

Распределенная навигация позволяет легко переключаться между Exchange Online и локальными развертываниями Exchange. Если у вас нет Exchange Online организации, **Office 365** ссылке вы перейдете на страницу, где сравниваются планы и цены на службы Microsoft 365 и Office 365.

2. Панель "Функции"

Область функций — это первый уровень навигации для большинства задач, выполняемых в EAC, и организована по следующим функциональным областям:

- **Получатели**. Управление почтовыми ящиками, группами, почтовыми ящиками ресурсов (почтовыми ящиками помещений и оборудования), контактами, общими почтовыми ящиками и переносами почтовых ящиков. Дополнительные сведения см. в следующих статьях:
    - Создание почтовых ящиков пользователей в Exchange Server и управление почтовыми ящиками пользователей
    - Управление группами рассылки и управление динамическими группами рассылки
    - Создание почтовых ящиков помещений и управление ими
    - Manage mail contacts и Manage mail users.

    - Создание общих почтовых ящиков в Центре администрирования Exchange

- Разрешения. Управление **ролями** администратора управления доступом на основе ролей (RBAC), ролями пользователей и политиками Outlook в Интернете. Дополнительные сведения см. в следующих статьях.

    - Управление группами ролей , Управление участниками группы ролей и Управление политиками назначения ролей.

    - Просмотр или настройка свойств политики почтовых ящиков Outlook в Интернете

- **Управление соответствием требованиям**. Здесь вы управляете In-Place обнаружением электронных данных, хранением In-Place, аудитом (ведение журнала аудита почтовых ящиков и ведение журнала аудита администратора), защитой от потери данных (DLP), политиками хранения, тегами хранения и правилами журнала. Дополнительные сведения см. в следующих статьях:

    - Обнаружение электронных данных на месте в Exchange Server, удержаниена месте и удержание для судебного разбирательства в Exchange Server

    - Ведение журнала аудита почтовых ящиков в Exchange Server и ведение аудита администратора в Exchange Server

    - Защита от потери данных в Exchange Server

    - Политики хранения и Теги хранения.

    - Ведение журнала в Exchange Server

- **Организация**: управление федеративной службой общего доступа, приложениями Outlook и списками адресов. Дополнительные сведения см. в следующих статьях:

    - Общий доступ

    - Установка или удаление надстроек для Outlook для организации Exchange 2013

    - Списки адресов в Exchange Server

- **Защита**. Управление защитой от вредоносных программ в организации. Дополнительные сведения см. в разделе Защита от вредоносных программ в Exchange Server.

- **Поток обработки почты**. Управление правилами потока обработки почты (также известными как правила транспорта), отчетами о доставке, принятыми доменами, удаленными доменами, политиками адресов электронной почты, соединителями получения и соединителями отправки. Дополнительные сведения см. в следующих статьях:
  - Правила потока обработки почты в Exchange Server
  - Отслеживание сообщений при помощи отчетов о доставке
  - Списки адресов в Exchange Server
  - Обслуживаемые домены в Exchange Server
  - Удаленные домены
  - Email адреса политик в Exchange Server
  - Соединители получения
  - Соединители отправки
- **Мобильные устройства**. Управление мобильными устройствами, которые разрешено подключать к вашей организации. Можно управлять доступом к мобильным устройствам и политиками почтовых ящиков мобильных устройств. Дополнительные сведения см. в следующих статьях:
  - Мобильные устройства
  - Политики почтовых ящиков мобильных устройств
- **Общедоступные папки**. Управление общедоступными папками и почтовыми ящиками общедоступных папок. Дополнительные сведения см. в разделе Общедоступные папки.
- **Единая система обмена сообщениями**: управление абонентской группой единой системы обмена сообщениями и IP-шлюзами единой системы обмена сообщениями. (UM недоступна в Exchange 2019.) Дополнительные сведения см. в следующих статьях:
  - Абонентские группы единой системы обмена сообщениями
  - IP-шлюзы единой системы обмена сообщениями
- **Серверы**. Просмотр параметров сервера, баз данных, групп доступности баз данных (DAG), виртуальных каталогов и сертификатов и управление ими. Дополнительные сведения см. в следующих статьях:

- POP3 и IMAP4 в Exchange Server
- Настройка режима запуска на сервере клиентского доступа и настройка режима запуска на сервере почтовых ящиков
- Интервалы повторной отправки, повторной передачи и истечения срока действия сообщений
- Настройка отслеживания сообщений , настройка ведения журнала подключений в Exchange Server и ведение журнала протокола
- Управление мобильным Outlook
- Управление копиями базы данных почтовых ящиков
- Управление группами доступности базы данных
- Управление виртуальными каталогами
- Процедуры сертификатов в Exchange Server

- **Гибридная**. Настройка и настройка гибридной организации.

3. Вкладки

На вкладке **Настройка** можно запустить мастер гибридной конфигурации или изменить параметры существующего гибридного развертывания.

4. Панель инструментов

При выборе большинства вкладок отображается панель инструментов. Она содержит значки, которые выполняют определенные действия. Наиболее распространенные значки и их действия описаны в таблице ниже. Чтобы увидеть действие, связанное со значком (название значка), просто наведите на него указатель мыши.

Развернуть таблицу

Значок	Имя	Действие
+	"Добавить", "Создать"	Создание нового объекта. Некоторые из этих значков имеют связанную стрелку вниз, чтобы отобразить дополнительные объекты, которые можно создать. Например, в **почтовых ящиках получателей**при щелчке стрелки вниз в качестве дополнительных >

Значок	Имя	Действие
		параметров отображаются **почтовый ящик пользователя** и **связанный почтовый ящик**.
	Изменить	Изменение объекта.
	Удалить	Удаление объекта. Некоторые значки удаления имеют стрелку вниз, чтобы отобразить дополнительные параметры.
	Поиск	Открытие поля поиска, в которое можно ввести текст, чтобы найти объект в длинном списке объектов.
	Обновление	Обновление представления списка.
	Дополнительные параметры	Просмотр дополнительных действий, которые можно выполнить для объектов этой вкладки. Например, в**почтовых ящиках**>**получателей**, щелкнув этот значок, отображаются следующие параметры: **Отключить**, **Добавить и удалить столбцы**, **Экспортировать данные в CSV-файл**, **Подключить почтовый ящик** и **Расширенный поиск**.
	Стрелка вверх и стрелка вниз	Перемещение объекта вверх или вниз в списке, если важен порядок. Например, в потоке >**обработки почтыEmail политики адресов** щелкните стрелку вверх, чтобы переместить политику выше в списке, что повышает приоритет политики, указывая, какая политика применяется в первую очередь. Кроме того, можно использовать эти стрелки для навигации по иерархии общедоступных папок, а также для перемещения правила вверх или вниз в списке.
	Копировать	Копирование объекта, чтобы отредактировать его, сохранив при этом исходный объект без изменений. Например, в **разделе Разрешения**>**Администратор роли** выберите роль в представлении списка, а затем щелкните этот значок, чтобы создать новую группу ролей на основе существующей.
	Удалить	Удаление элемента из списка. Например, в диалоговом окне **Разрешения общедоступных папок** можно удалить пользователей из списка пользователей, которые могут получить доступ к папке. Для этого выберите пользователя и щелкните этот значок.

5. Представление списка

Во вкладках, содержащих много объектов, эти объекты отображаются в виде списка. Количество отображаемых объектов в списках Центра администрирования

Exchange ограничено и составляет приблизительно 20 000 объектов. Этот список разбит на страницы, так что можно быстро перейти к нужным результатам. В представлении списка **Получатели** можно также настроить размер страницы и экспортировать данные в CSV-файл.

6. Область сведений

При выборе объекта в представлении списка в области сведений отображается подробная информация об этом объекте. Для некоторых типов объектов в области сведений также отображаются быстрые задачи управления. Например, если перейти к разделу **Почтовые ящики получателей**> и выбрать почтовый ящик в представлении списка, в области сведений (среди других параметров) отобразится параметр для включения или отключения архива для этого почтового ящика.

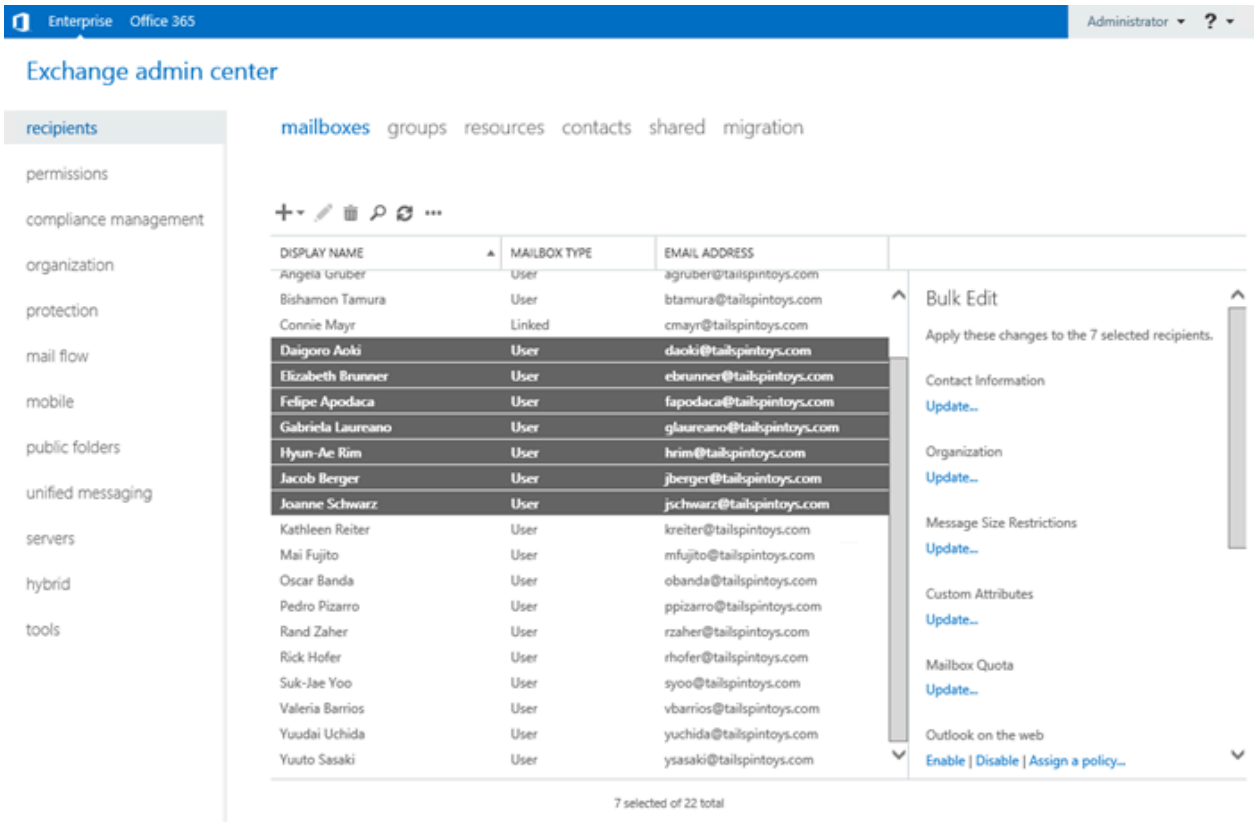
Некоторые типы объектов также разрешают массовое редактирование нескольких объектов в области сведений. Вы можете выбрать несколько объектов в представлении списка, выбрав объект и выполнив одно из следующих действий:

- Удерживая клавишу SHIFT, выберите объект дальше в списке.

  или

- Удерживая нажатой клавишу CTRL, при выборе каждого объекта.

Если для выбранных типов объектов доступно массовое изменение, в области сведений отображаются доступные параметры. Например, в **разделе Почтовые ящики**> получателей при выборе нескольких почтовых ящиков одного типа заголовок области сведений изменяется на **Массовое изменение**, и вы можете обновить контактные и организационные сведения, настраиваемые атрибуты, квоты почтовых ящиков, параметры Outlook в Интернете и многое другое.



7. Уведомления

EAC включает средство просмотра уведомлений, которое отображает сведения о следующих элементах:

- сертификатах, у которых истек или же скоро истечет срок действия;
- состоянии перемещения и миграции почтовых ящиков (также известных как задачи службы репликации почтовых ящиков). Вы также можете использовать средство просмотра уведомлений для получения Уведомления по электронной почте об этих задачах.
- Экспорт содержимого почтового ящика в PST-файлы.

Чтобы отобразить или скрыть средство просмотра уведомлений, щелкните значок (🔔

Уведомления — это оповещения, отправляемые в почтовый ящик арбитража с именем `FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042`. Центр администрирования Exchange проверяет почтовый ящик на наличие оповещений каждые 30 секунд. Уведомления остаются в почтовом ящике арбитража до тех пор, пока они не будут удалены отправляющим их компонентом или до истечения срока их действия (удалены помощником по управляемым папкам через 30 дней).

Можно также использовать командлет **Get-Notification** в Командная консоль Exchange, чтобы получить дополнительные сведения об уведомлениях, и командлет **Set-Notification**, чтобы запросить получение уведомлений по электронной почте в будущем.

8. Иконка "Я" и справка

Иконка "Я" позволяет выйти из Центра администрирования Exchange и войти в него как другой пользователь, нажав раскрывающееся меню возле имени вашей учетной записи.

Щелкните значок справки (?), чтобы просмотреть содержимое справки для вкладки, на которую вы сейчас находитесь. Если выбрать в раскрывающемся меню рядом со значком справки, можно выполнить следующие действия:

- **Отключить всплывающий элемент справки**. Пузырек справки отображает контекстную справку для полей при создании или изменении объектов в EAC. В этом окне можно выключить или включить всплывающую справку для всех полей в Центре администрирования Exchange.
- **Консоль производительности**. В консоли производительности отображается множество счетчиков, связанных с производительностью EAC.
- **Авторские права** и **конфиденциальность**. Выберите эти ссылки, чтобы прочитать сведения об авторских правах и конфиденциальности для Exchange Server.

Поддерживаемые браузеры

Список поддерживаемых веб-браузеров для доступа к EAC можно найти в матрице поддержки Exchange Server. Веб-браузеры, которых нет в списке, не поддерживаются. Обратите внимание, что сторонние подключаемые модули могут вызвать проблемы с EAC в поддерживаемых браузерах.

Exchange Server. Отключение доступа к Центру администрирования Exchange

Статья • 04.04.2023

Центр администрирования Exchange (EAC) — это основной интерфейс управления для Exchange 2013 или более поздней версии. Дополнительные сведения см. в разделе Центр администрирования Exchange в Exchange Server. По умолчанию доступ к EAC не ограничен, а доступ к Outlook в Интернете (официально известной как Outlook Web App) на сервере Exchange Server с выходом в Интернет также предоставляет доступ к EAC. Для входа в EAC по-прежнему требуются действительные учетные данные, но организациям может потребоваться ограничить доступ к EAC для клиентских подключений из Интернета.

В Exchange Server 2019 г. можно использовать правила клиентского доступа, чтобы заблокировать доступ клиентов к EAC. Дополнительные сведения см. в разделе Правила клиентского доступа в Exchange Server.

Служба автообнаружения в Exchange Server

Статья • 17.10.2023

Служба автообнаружения минимизирует действия по настройке и развертыванию пользователей, предоставляя клиентам доступ к функциям Exchange. Для клиентов веб-служб Exchange (EWS) автообнаружение обычно используется, чтобы найти URL-адрес конечной точки EWS. Однако служба автообнаружения также может предоставлять сведения для настройки клиентов, использующих другие протоколы. Автообнаружение работает как с защищенными, так и не защищенными брандмауэром клиентскими приложениями, подходит для сценариев с лесом ресурсов и несколькими лесами.

В Exchange 2016 появились изменения в службах, которые ранее обрабатывались несколькими серверами. Теперь сервер почтовых ящиков предоставляет службы клиентского доступа, поэтому вы не сможете настроить отдельный сервер клиентского доступа, как в предыдущих версиях Exchange. Служба автообнаружения в Exchange 2016 и Exchange 2019 возможна по следующим причинам:

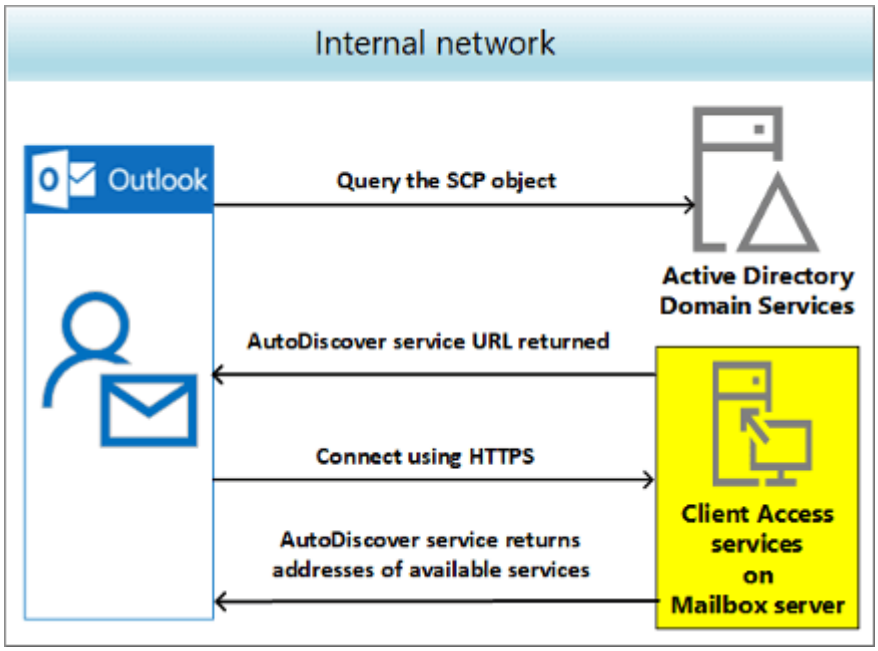
- Exchange создает виртуальный каталог с именем `autodiscover` на веб-сайте по умолчанию в службах IIS.
- Active Directory хранит и предоставляет достоверные URL-адреса для компьютеров, присоединенных к домену.
- Службы клиентского доступа на серверах почтовых ящиков предоставляют службы проверки подлинности и прокси-сервера для внутренних и внешних клиентских подключений.
- Outlook настраивает службы только с именем пользователя и паролем.

> ⓘ **Примечание**
>
> Справочные сведения для пользователей, касающиеся подключения клиента Outlook к серверу Exchange Server, см. в статье о **настройке электронной почты Outlook**.

Службы автообнаружения и Active Directory

Exchange хранит в Active Directory конфигурацию серверов Exchange в организации, а также сведения о почтовых ящиках пользователей. Перед установкой Exchange Server необходимо подготовить лес Active Directory и его домены. Если вы не знакомы с лесами или доменами Exchange, см. шаг 3. Подготовка доменов Active Directory.

Exchange автоматически создает при установке виртуальный каталог `autodiscover` в IIS, веб-сайт служб внешнего клиентского доступа, к которому подключаются клиенты. Это позволяет Outlook обнаруживать параметры почтовых ящиков Exchange, чтобы пользователям не приходилось вручную настраивать дополнительные параметры.



Одновременно с виртуальным каталогом службы автообнаружения в Active Directory создается объект точки подключения службы (SCP). SCP хранит и предоставляет заслуживающие доверия URL-адреса службы автообнаружения для компьютеров, присоединенных к домену.

Вам нужно обновить объект SCP, чтобы он указывал на сервер Exchange. Это требуется потому, что серверы Exchange предоставляют клиентам дополнительные сведения автообнаружения для улучшения процесса обнаружения. Дополнительные сведения см. в статье Set-ClientAccessService.

> ⓘ **Важно!**
>
> Для запуска командлета **Set-ClientAccessService** требуются специальные разрешения. Сведения о необходимых разрешениях для запуска командлетов и использования параметров в организации см. в статье **Find the permissions required to run any Exchange cmdlet**.

Автообнаружение упрощает получение информации, необходимой для подключения к почтовым ящикам на серверах Exchange Server. Объекты SCP находят подходящие серверы или конечные точки автообнаружения для пользователей, для которых вы получаете параметры. Объекты SCP в AD DS упрощают поиск серверов автообнаружения для присоединенных к домену клиентов.

Exchange публикует два типа объектов SCP для службы автообнаружения:

- **Указатели SCP**. Содержит сведения, указывающие на определенные серверы LDAP, которые должны использоваться для поиска объектов SCP автообнаружения для домена пользователя. GUID указателей SCP: 67661d7F-8FC4-4fa7-BFAC-E1D7794C1F68.

- **URL-адреса SCP**: содержит URL-адреса конечных точек автообнаружения. URL-адреса SCP помечены следующим идентификатором GUID: 77378F46-2C66-4aa9-A6A6-3E7A48B19596

Объект SCP содержит достоверный список URL-адресов службы автообнаружения для леса. Дополнительные сведения о поиске конечных точек службы автообнаружения см. в статье Создание списка конечных точек автообнаружения.

Клиентское подключение в Exchange 2016 и Exchange 2019 аналогично Exchange 2013 и отличается от Exchange 2010. В Exchange 2016 и 2019 MAPI по протоколу HTTP включен по умолчанию, когда ранее клиенты Outlook использовали Outlook Anywhere (RPC через HTTP). Exchange 2016 и 2019 требует меньше пространства имен для устойчивых к сайту решений, чем Exchange 2010, что сокращается до двух по сравнению с ранее необходимыми семи пространствами имен. Дополнительные сведения о пространстве имен и Exchange Server см. в блоге Планирование пространства имен в Exchange 2016 .

В зависимости от того, настроена ли служба автообнаружения на отдельном сайте, URL-адрес службы автообнаружения будет иметь одно из следующих значений, где `//<SMTP-address-domain>` — основной адрес домена SMTP:

- `https://<SMTP-address-domain>/autodiscover/autodiscover.xml`

- `https://autodiscover.<smtp-address-domain>/autodiscover/autodiscover.xml`

Например, если адрес электронной почты пользователя — tony@contoso.com, основной адрес домена SMTP contoso.com.

Клиентские приложения используют службу автообнаружения при первом запуске приложения. Например, при первом запуске приложения веб-служб Exchange

(EWS) оно настраивается с помощью службы автообнаружения. Для компьютера пользователя, подключенного к домену contoso.com и размещенного на региональном сайте Active Directory Longview, приложение создает список этих конечных точек службы автообнаружения.

Конечная точка	Создана на основе
https://longview.contoso.com/autodiscover/autodiscover.xml	Результаты SCP
https://email.contoso.com/autodiscover/autodiscover.xml	Результаты SCP
https://newark.contoso.com/autodiscover/autodiscover.xml	Результаты SCP
https://contoso.com/autodiscover/autodiscover.exc	Электронный адрес
https://autodiscover.contoso.com/autodiscover/autodiscover	Электронный адрес

Дополнительные сведения об объектах SCP см. в разделе Публикация с помощью точек подключения служб.

Автообнаружение в DNS

Exchange представила требования к пространству имен для автообнаружения в Exchange 2010, и для сертификатов требовалось несколько из них. В сценарии устойчивости сервера требуются все перечисленные ниже элементы:

- Основное пространство имен IP центра обработки данных.
- Дополнительное пространство имен IP центра обработки данных.
- Основное пространство имен Outlook Web App восстановления размещения
- Дополнительное пространство имен Outlook Web App восстановления размещения
- Пространство имен транспорта (для SMTP)
- Основное пространство имен для клиентского доступа через RPC, которое нужно центру обработки данных.
- Дополнительное пространство имен для клиентского доступа через RPC, которое нужно центру обработки данных.

Сценарии устойчивости сервера были улучшены, что сократило пять пространств имен до двух. Причина состоит в том, что Exchange больше не нужны пространства имен для клиентского доступа через RPC, а службы клиентского доступа

перенаправляют запросы на сервер почтовых ящиков, на котором размещается активная база данных почтовых ящиков. Сервер почтовых ящиков на одном сайте Active Directory может выполнять прокси-сервер сеанса на сервере почтовых ящиков другого сайта Active Directory.

Это означает, что уникальные пространства имен больше не требуются для *каждого* центра данных. Например, для пары центров обработки данных вам нужно только одно пространство имен — mail.contoso.com, а не mail.contoso.com и mail2.contoso.com. Кроме того, для сценариев активации, в которых используются группы обеспечения доступности баз данных, больше не нужны пространства имен восстановления размещения.

Все, что нужно, чтобы настроить автообнаружение для домена, — это создать запись ресурса CNAME во внешней (общедоступной) DNS. Записи CNAME позволяют скрыть детали реализации сети от клиентов, которые к ней подключаются. Записи CNAME, используемые в сети, позволяют пользователям применять более простой URI (mail.domain.com, а не host.examplemachinename.domain.com).

Запись CNAME (запись канонического имени) — это DNS-эквивалент ярлыка в Windows или псевдонима в Mac OS. Запись CNAME — это псевдоним записи A, которая сопоставляет IP-адрес с целевым сервером. Например, если ваш домен — contoso.com, создается запись CNAME для autodiscover.contoso.com. Имя в записи CNAME должно соответствовать имени в сертификате. Записи CNAME можно использовать только для имен узлов. Записи CNAME хоть и указывают псевдонимы, но не заменяют URL-адрес в строке браузера. Когда сертификат проверяется по URL-адресу, вы получаете ошибку с предупреждением, но все равно можете получить доступ к службе.

Типичная запись CNAME выглядит указанным ниже образом.

- Имя: autodiscover.
- Срок жизни: 3600 с.
- Тип записи ресурса: CNAME.
- Целевой объект: доступное извне имя FQDN для сервера почтовых ящиков (например, mail.contoso.com).

В этом примере autodiscover.contoso.com разрешается в mail.contoso.com. Дополнительные сведения см. в разделе Шаг 4. Настройка внешних URL-адресовв статье Настройка потока обработки почты и клиентского доступа на серверах Exchange Server.

Рекомендуем создать записи CNAME автообнаружения для всех доменов учетной записи, в том числе псевдонимов доменов и обслуживаемых доменов. Запись SRV или CNAME необходимо создать там, где размещается ваш домен. Только после этого можно синхронизировать автономную адресную книгу, отобразить сведения о доступности и включить функцию "Нет на рабочем месте" в Outlook.

Записи SRV позволяют указать расположение серверов для определенной службы, протокола и домена DNS. Например, если в вашем домене два веб-сервера, вы можете создать записи SRV, указывающие, какие узлы выполняют функции веб-серверов. Сопоставители затем могут извлечь все записи SRV для веб-серверов.

Типичная запись SRV выглядит указанным ниже образом.

- Служба: "_autodiscover".
- Протокол: "._tcp".
- Номер порта: 443.
- Узел: mail.contoso.com.
- Приоритет: 0.
- Вес: 0.

В этом примере пространство имен сервера Outlook — mail.contoso.com.

Дополнительные сведения о записях CNAME и SRV см. в блоге команды Exchange планирование пространства имен в Exchange 2016.

Службы автообнаружения в Outlook

Клиент Outlook может выполнять аутентификацию в Active Directory и искать объекты SCP автообнаружения, используя только учетные данные пользователя. После получения и перечисления экземпляров службы автообнаружения клиент подключается к службам клиентского доступа (интерфейсным) на первом сервере почтовых ящиков в перечисленном списке. Затем клиент собирает данные профиля в формате XML, необходимые для подключения к почтовому ящику пользователя и доступным компонентам Exchange.

> ⓘ **Примечание**
>
> В зависимости от требований поставщика DNS в качестве имени узла может потребоваться добавить полное доменное имя (FQDN). В этом случае, если

ваш домен — contoso.com, вашим именем узла будет autodiscover.contoso.com, а не autodiscover.com.

Для доменного имени нужно настроить специальную запись DNS, которая указывает на сервер, предоставляющий службы автообнаружения, чтобы учетные записи Exchange корректно работали в Outlook. В случае внешнего доступа или при использовании DNS клиент находит службу автообнаружения в Интернете по основному адресу домена SMTP, входящему в электронный адрес пользователя.

Служба автообнаружения использует один из этих четырех методов для настройки почтового клиента. Первые два подходят для небольших организаций с одним пространством имен SMTP. Последние два предназначены для организаций с несколькими пространствами имен SMTP.

- Адрес для подключения: https://contoso.com/AutoDiscover/AutoDiscover.xml .
- Адрес для подключения: https://autodiscover.contoso.com/AutoDiscover/AutoDiscover.xml .
- URL-адрес автообнаружения для перенаправления: https://autodiscover.contoso.com/autodiscover/autodiscover.xml .
- Поиск записи SRV DNS.

Некоторые имена узлов и URL-адреса можно настроить с помощью Центра администрирования Exchange (EAC) и командной консоли Exchange, в то время как для других требуется использовать PowerShell. Дополнительные сведения об этом см. в статье Настройка потока обработки почты и доступа клиентов.

С помощью службы автообнаружения Outlook находит новую точку подключения на базе почтового ящика пользователя. То есть идентификатор автообнаружения состоит из GUID, символа @ и доменного имени из основного SMTP-адреса пользователя. Служба автообнаружения возвращает клиенту следующую информацию:

- отображаемое имя пользователя;
- индивидуальные параметры каждого внутреннего или внешнего подключения;
- сведения о расположении почтового ящика пользователя (сервере почтовых ящиков, который содержит активную копию почтового ящика);

- URL-адреса различных функций Outlook, которые управляют такими функциями, как сведения о доступности, единая система обмена сообщениями (UM) в Exchange 2016 (но не в Exchange 2019) и автономная адресная книга (OAB)
- параметры сервера Мобильный Outlook.

Необходимо убедиться, что вы настроили правильные внешние URL-адреса для виртуальных каталогов следующих служб. В приведенной ниже таблице показаны значения, необходимые для домена электронной почты contoso.com.

Служба	Командная консоль Exchange	Изменение
Автономная адресная книга	`Get-OabVirtualDirectory | Set-OabVirtualDirectory -ExternalURL https://mail.companycontoso.com/oab`	Виртуальные каталоги автономной адресной книги, используемые в IIS
Веб-службы Exchange	`Get-WebServicesVirtualDirectory | Set-WebServicesVirtualDirectory -ExternalURL https://mail.companycontoso.com/ews/exchange.asmx`	Виртуальные каталоги веб-служб Exchange в IIS
Мобильный Outlook (RPC/HTTP)	`Get-OutlookAnywhere | Set-OutlookAnywhere -ExternalHostname mail.contoso.com -ExternalClientsRequireSsl $true`	Виртуальные каталоги мобильного Outlook в IIS

Программный интерфейс для обмена сообщениями (MAPI) по протоколу HTTP (Exchange 2013 с пакетом обновления 1 (SP1) или более поздней версии)	`Get-MapiVirtualDirectory | Set-MapiVirtualDirectory -ExternalURL https://mail.companycontoso.com/mapi`
	
	`Set-OrganizationConfig -MapiHttpEnabled $true`
		Виртуальные каталоги MAPI в IIS

Щелкните имя службы в приведенной выше таблице, чтобы узнать больше о том, как получить или обновить эти URL-адреса.

При изменении сведений об Exchange outlook использует службу автообнаружения для автоматической перенастройки профиля пользователя. Например, если почтовый ящик пользователя перемещен. Или клиент не может подключиться к

почтовому ящику пользователя или к доступным функциям Exchange, Outlook свяжется со службой автообнаружения и автоматически обновит профиль пользователя, включив в него сведения, необходимые для подключения к почтовому ящику и функциям Exchange.

Другие клиенты

Служба автообнаружения — предпочтительный метод поиска всех служб в Skype для бизнеса Server 2015 г. При успешном подключении она возвращает URL-адреса всех веб-служб в домашнем пуле пользователя, в том числе службы Mobility Service, или Mcx (так называется виртуальный каталог, создаваемый для службы в IIS), Lync Web App и веб-планировщика. Однако и внутренний, и внешний URL-адреса службы Mobility Service связаны с внешним полным доменным именем веб-служб. Поэтому мобильное устройство всегда подключается к службе Mobility Service извне, используя обратный прокси-сервер, независимо от того, является ли оно внешним по отношению к сети. Служба автообнаружения также возвращает ссылки на Internal/UCWA, External/UCWA и UCWA. UCWA — это веб-компонент Unified Communications Web API.

Настройка служб автообнаружения

Автообнаружение работает как с защищенными, так и не защищенными брандмауэром клиентскими приложениями, подходит для сценариев с лесом ресурсов и несколькими лесами. В случае клиентов EWS служба автообнаружения обычно используется для поиска URL-адреса конечной точки EWS, но она также может предоставлять информацию для настройки клиентов, использующих другие протоколы.

При установке Exchange Server на сервер автоматически устанавливается самозаверяющий сертификат, созданный и подписанный сервером Exchange Server. Однако вы также можете создать дополнительные самозаверяющие сертификаты для других служб.

Создание запроса на сертификат — это первый шаг при установке нового сертификата на сервер Exchange Server для настройки шифрования TLS для одной или нескольких служб Exchange. Такой запрос позволяет получить сертификат из центра сертификации (ЦС). Дополнительную информацию см. в следующих статьях:

- Цифровые сертификаты и шифрование в Exchange Server
- Создание запроса на сертификат Exchange Server для центра сертификации

> **Примечание**
>
> Вы можете проверить службу автообнаружения с помощью средства **Microsoft Remote Connectivity Analyzer**. Протестировав подключение, также выберите параметр "Outlook Connectivity" (Подключение Outlook), чтобы выполнить соответствующую проверку. Если она не будет пройдена, возможно, вам потребуется настроить внешние URL-адреса в Exchange. Из результатов Microsoft Remote Connectivity Analyzer должно быть понятно, почему не удалось установить подключение. Как правило, ошибка подключения означает, что для виртуальных каталогов служб Outlook не настроены правильные внешние URL-адреса.

Управление службами автообнаружения

В развертываниях, в которых клиенты подключаются к нескольким серверам Exchange Server, объект SCP автообнаружения создается для служб клиентского доступа (интерфейсных) на каждом сервере почтовых ящиков. Объект SCP содержит атрибут ServiceBindingInfo с полным доменным именем сервера Exchange, к которому подключается клиент в форме `https://<ExchangeServer>/autodiscover/autodiscover.xml` (например, `https://cas01/autodiscover/autodiscover.xml`).

Вы можете запустить тесты автообнаружения Exchange ActiveSync и автообнаружения Outlook в анализаторе удаленного подключения Майкрософт. Если пользователь использует локальную беспроводную сеть для подключения к Exchange, он должен выполнить оба теста, чтобы убедиться, что локальная сеть разрешает подключения к конечным точкам ActiveSync.

Вы можете получить справку по планированию и развертыванию служб автообнаружения в рамках развертывания Exchange в разделе Планирование и развертывание для Exchange Server.

Балансировка нагрузки в Exchange Server

Статья • 04.04.2023

Балансировка нагрузки в Exchange 2016 и более поздних версиях основана на платформе Майкрософт для обеспечения высокой доступности и устойчивости сети, доступной в Exchange 2013. В сочетании с доступностью сторонних решений для балансировки нагрузки (аппаратного и программного обеспечения) существует несколько вариантов реализации балансировки нагрузки в организации Exchange.

С изменениями архитектуры Exchange в Exchange 2013 появились роли сервера почтовых ящиков и сервера клиентского доступа. Для сравнения, в Exchange 2010 службы клиентского доступа, почтовые ящики, транспортный концентратор и единая система обмена сообщениями находились на разных серверах.

Используя минимальные роли сервера, Exchange 2016 и 2019 обеспечивает:

- упрощенное развертывание, так как на сервере почтовых ящиков устанавливаются службы клиентского доступа и роли пограничных транспортных серверов;
- Поток обработки почты управляется в транспортном конвейере, который представляет собой коллекцию служб, подключений, очередей и компонентов, которые направляют сообщения в классификатор транспортной службы на сервере почтовых ящиков.
- высокий уровень доступности за счет развертывания подсистем балансировки нагрузки для распределения клиентского трафика.

Стандарт протокола HTTP, представленный в Exchange 2013, означает, что сходство сеансов больше не требуется в Exchange 2016 и Exchange 2019. Сходство сеансов обеспечивает постоянное подключение к службам с поддержкой обмена сообщениями, чтобы пользователю не нужно было повторно ввести имя пользователя и пароль несколько раз.

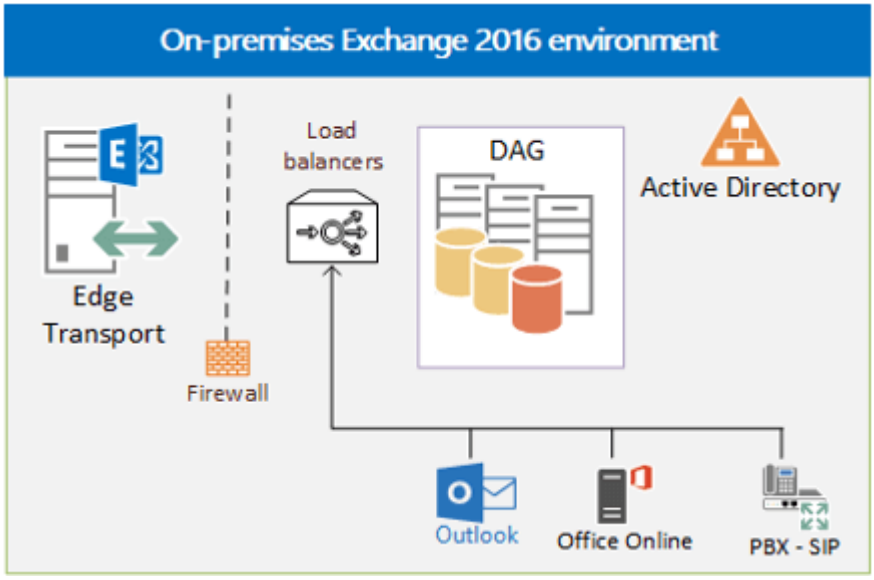
Ранее Exchange 2007 и Exchange 2010 поддерживали протокол RPC через HTTP для Мобильный Outlook. В Exchange 2013 появился протокол MAPI через HTTP, но по умолчанию он был отключен. Теперь он включен по умолчанию в Exchange 2016 и Exchange 2019.

При использовании протокола HTTP все собственные клиенты подключаются по протоколу HTTP и HTTP в Exchange Server. Этот стандартный протокол устраняет

необходимость в сходстве, которое ранее требовалось, чтобы избежать нового запроса учетных данных пользователя, когда балансировка нагрузки перенаправляла подключение на другой сервер.

Роли сервера в Exchange Server

Сокращение числа ролей сервера для Exchange 2016 и Exchange 2019 упрощает реализацию Exchange и требования к оборудованию. Число ролей сервера в Exchange 2016 и 2019 сокращается с семи до двух: сервера почтовых ящиков и пограничного транспортного сервера. Роль сервера почтовых ящиков включает службы клиентского доступа, а пограничный транспортный сервер обеспечивает безопасный поток обработки почты в Exchange 2016 и Exchange 2019, как и в более ранних версиях Exchange.



В Exchange 2013 роль сервера клиентского доступа гарантировала, что когда пользователь пытался получить доступ к своему почтовому ящику, сервер проксировал запрос обратно на сервер почтовых ящиков, обслуживающий почтовый ящик этого пользователя. В связи с этим такие службы, как Outlook в Интернете (предыдущее название — Outlook Web App), отрисовывались в самом почтовом ящике, избавляя от необходимости в сходстве.

Те же функции остаются в Exchange 2016 и Exchange 2019. Если на двух серверах почтовых ящиков размещены разные почтовые ящики, при необходимости они могут проксировать трафик друг для друга. Сервер почтовых ящиков, на котором размещена активная копия почтового ящика, обслуживает пользователя, получающего доступ к нему, даже если этот пользователь подключается к другому серверу.

Дополнительные сведения об изменениях роли сервера в Exchange Server см. в статье Exchange Server архитектуре.

Роль сервера	Службы
Сервер почтовых ящиков	Использует службу EdgeSync для управления односторонней репликацией сведений о получении и конфигурации из Active Directory в экземпляр служб Active Directory облегченного доступа к каталогам на пограничном транспортном сервере. Копирует только сведения, необходимые для того, чтобы пограничный транспорт выполнял антиспам и включил сквозной поток обработки почты.
Пограничный транспортный сервер	Управляет потоком обработки почты в Интернет и из него с помощью: • Ретранслятор почты • Интеллектуальное размещение. • Агенты, которые предоставляют больше служб защиты от нежелательной проверки. • Агенты, которые применяют транспорт для управления потоком обработки почты. Не является членом леса Active Directory.

Хотя пограничный транспортный сервер и не является обязательным, он находится в сети периметра, как и в более ранних версиях Exchange, для обеспечения безопасного входящего и исходящего потока почты для организации Exchange.

Дополнительные сведения о транспортной службе см. в статье Общие сведения о транспортной службе на пограничных транспортных серверах.

Протоколы в Exchange Server

Начиная с Exchange 2016, все собственные клиенты Exchange используют протокол HTTP для подключения к указанной службе с файлами cookie HTTP, предоставляемыми пользователю при входе в систему, которые шифруются с помощью SSL-сертификата служб клиентского доступа. Вошедший пользователь может возобновить сеанс на другом сервере почтовых ящиков, где работают службы клиентского доступа, не проходя проверку подлинности заново. Серверы, использующие тот же SSL-сертификат, могут расшифровать файл cookie для проверки подлинности клиента.

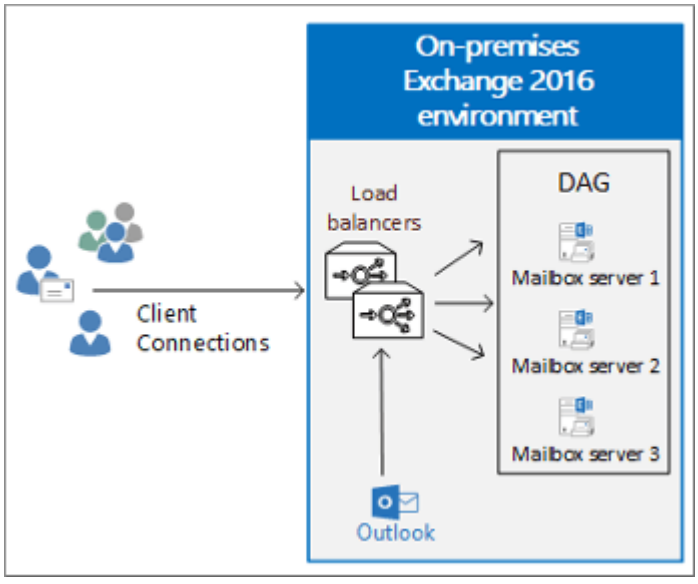
Протокол HTTP позволяет использовать проверки работоспособности служб и приложений в сети Exchange. В зависимости от используемого решения для балансировки нагрузки вы можете реализовать зонды для проверки работоспособности различных компонентов системы.

Благодаря тому, что для клиентского доступа используется только протокол HTTP, балансировка нагрузки также становится проще. При желании для балансировки нагрузки трафика Exchange можно использовать DNS. Вы предоставите клиенту IP-адрес каждого сервера почтовых ящиков, а HTTP-клиент будет обрабатывать работу. В случае отказа сервера Exchange протокол пытается подключиться к другому серверу. Однако существуют недостатки балансировки нагрузки в DNS, описанные в следующем разделе *Параметры балансировки нагрузки в Exchange Server*.

Дополнительные сведения о HTTP и Exchange Server см. в статье MAPI через HTTP в Exchange Server.

Параметры балансировки нагрузки в Exchange Server

В приведенном ниже примере на нескольких серверах в группе обеспечения доступности баз данных размещаются серверы почтовых ящиков, где работают службы клиентского доступа. Это обеспечивает высокий уровень доступности, а серверы Exchange занимают меньше места. Клиент подключается к подсистеме балансировки нагрузки, а не напрямую к серверам Exchange. Для пар подсистемы балансировки нагрузки не требуется, однако рекомендуется развертывать их в кластерах, чтобы повысить устойчивость сети.



Помните, что группы обеспечения доступности баз данных используют службы кластеров Microsoft. Эти службы не могут быть включены на том же сервере, что и балансировка сетевой нагрузки (NLB) Windows. Следовательно, если используются группы обеспечения доступности баз данных, включить Windows NLB нельзя. В

таком случае можно воспользоваться сторонними программами и решениями для виртуальных модулей.

Использование DNS — самый простой способ балансировки нагрузки трафика Exchange. При балансировке нагрузки с помощью DNS достаточно предоставить клиентам IP-адреса всех серверов почтовых ящиков. После этого DNS распределит трафик на серверы почтовых ящиков путем циклического перебора. В случае полного отказа одного сервера Exchange HTTP-клиент может подключиться к другому.

Простота достигается дорогой ценой, однако в этом случае циклический перебор DNS не является действительно балансировкой нагрузки трафика, так как нет способа программно убедиться, что каждый сервер получает справедливую долю трафика. Кроме того, отсутствует мониторинг уровня обслуживания, поэтому при сбое одной службы клиенты не будут автоматически перенаправляться в доступную службу. Например, если Outlook в Интернете находится в режиме сбоя, клиенты видят страницу ошибки.

Для балансировки нагрузки с помощью DNS при внешней публикации требуется больше внешних IP-адресов. Это означает, что каждому серверу Exchange в организации потребуется внешний IP-адрес.

Существуют более элегантные решения для балансировки нагрузки трафика, например оборудование, распределяющее клиентский трафик с помощью транспортного уровня 4 или прикладного уровня 7. Подсистемы балансировки нагрузки отслеживают каждую клиентную службу Exchange, и в случае сбоя службы подсистемы балансировки нагрузки могут направлять трафик на другой сервер и перевести проблемный сервер в автономный режим. Кроме того, некоторая степень балансировки нагрузки гарантирует, что ни одному из серверов почтовых ящиков не приходится проксировать большую часть операций клиентского доступа.

Для управления трафиком службы балансировки нагрузки могут использовать 4-й или 7-й уровень либо их сочетание. У каждого решения есть свои преимущества и недостатки.

- Подсистемы балансировки нагрузки 4-го уровня работают на транспортном уровне, направляя трафик без проверки содержимого.

  Так как эти подсистемы не проверяют содержимое трафика, передача занимает меньше времени. Однако для этого приходится идти на компромиссы. Подсистемам балансировки нагрузки 4-го уровня известны

только IP-адрес, протокол и TCP-порт. Зная только один IP-адрес, подсистема балансировки нагрузки может наблюдать только за одной службой.

Преимущества балансировки нагрузки уровня 4:

- низкие требования к ресурсам (проверка содержимого не выполняется);
- распределение трафика на транспортном уровне.

  Риск использования решений 4-го уровня состоит в том, что если в случае сбоя службы сервер по-прежнему будет доступен, клиенты смогут подключаться к неисправной службе. Это означает, что для устойчивой реализации 4-го уровня необходимо несколько IP-адресов с отдельными пространствами имен HTTP для каждой службы, например owa.contoso.com, eas.contoso.com, mapi.contoso.com, чтобы обеспечить мониторинг на уровне служб.

- Подсистемы балансировки нагрузки 7-го уровня работают на прикладном уровне. Они могут проверять содержимое трафика и направлять его соответствующим образом.

  Подсистемы балансировки нагрузки 7-го уровня не предоставляют повышенную производительность, характерную для балансировки нагрузки на 4-м уровне, но обеспечивают простоту за счет единого пространства имен (например, mail.contoso.com) и мониторинга отдельных служб. Подсистемы балансировки нагрузки 7-го уровня анализируют HTTP-путь, например /owa or /Microsoft-Server-ActiveSync, or /mapi,, и могут направлять трафик на рабочие серверы в соответствии с данными мониторинга.

  Преимущества балансировки нагрузки уровня 7:

  - требуется только один IP-адрес;
  - проверка содержимого и возможность направления трафика;
  - уведомления об отказе служб, которые можно переводить в автономный режим;
  - завершение SSL-запросов в подсистеме балансировки нагрузки;
  - распределение трафика на прикладном уровне и анализ целевого URL-адреса.

SSL-запросы должны завершаться в подсистеме балансировки нагрузки, которая будет центральным расположением для защиты от атак с использованием SSL.

Некоторые порты, для которых требуется балансировка нагрузки (например, для протоколов IMAP4 и POP3), могут даже не использоваться в организации Exchange.

TCP-порт	Роли	Применение
25	Почтовый ящик	Входящая почта SMTP
587	Mailbox	Входящий SMTP для клиентов
110	Почтовый ящик	Клиенты POP3
143	Почтовый ящик	Клиенты IMAP4
443	Mailbox	HTTPS (Outlook в Интернете, автообнаружения, веб-службы, ActiveSync, MAPI через HTTP, RPC через HTTP, OAB, EAC)
993	Почтовый ящик	Защищенные клиенты IMAP4
995	Почтовый ящик	Защищенные клиенты POP3

Сценарии развертывания балансировки нагрузки в Exchange Server

Exchange 2016 предоставляет значительную гибкость для пространства имен и архитектуры балансировки нагрузки. Учитывая разнообразие вариантов развертывания для подсистем балансировки нагрузки в организации Exchange — от простого DNS до сложных сторонних решений 4-го и 7-го уровней, — рекомендуем изучить их все, исходя из потребностей организации.

У описанных ниже сценариев есть свои преимущества и ограничения. Понимание их особенностей — ключ к реализации решения, идеально подходящего для вашей организации Exchange.

- **Сценарий А**. Одно пространство имен без сходства сеансов: уровень 4 или 7
- **Сценарий Б**. Одно пространство имен без сходства сеансов: уровень 7
- **Сценарий В**. Одно пространство имен со сходством сеансов, уровень 7

- **Сценарий Г**. Несколько пространств имен без сходства сеансов, уровень 4

Сценарий А. Одно пространство имен без сходства сеансов: уровень 4 или 7

В этом сценарии 4-го уровня в клиентах HTTP развертывается одно пространство имен — mail.contoso.com. Подсистема балансировки нагрузки не сохраняет сходство сеансов. Так как это решение уровня 4, подсистема балансировки нагрузки настроена для проверки работоспособности только одного виртуального каталога, так как она не может отличить Outlook в Интернете запросов от запросов RPC.

С точки зрения подсистемы балансировки нагрузки в этом примере работоспособность выполняется для каждого сервера, а не для каждого протокола для указанного пространства имен. Администраторы должны будут выбрать, какой виртуальный каталог они должны выбрать для пробы работоспособности. Рекомендуется выбрать широко используемый виртуальный каталог. Например, если большинство пользователей используют Outlook в Интернете, выберите виртуальный каталог Outlook в Интернете в пробе работоспособности.

Пока ответ проверки работоспособности Outlook в Интернете работоспособности, подсистема балансировки нагрузки сохраняет целевой сервер почтовых ящиков в пуле балансировки нагрузки. Однако если проверка работоспособности Outlook в Интернете по какой-либо причине завершается сбоем, подсистема балансировки нагрузки удаляет целевой сервер почтовых ящиков из пула балансировки нагрузки для всех запросов, связанных с этим пространством имен. Это означает, что в случае сбоя пробы работоспособности все запросы клиента для этого пространства имен направляются на другой сервер независимо от протокола.

Сценарий Б. Одно пространство имен без сходства сеансов: уровень 7

В этом сценарии 7-го уровня для всех клиентов HTTP развертывается одно пространство имен — mail.contoso.com. Подсистема балансировки нагрузки не сохраняет сходство сеансов. Так как подсистема балансировки нагрузки настроена для уровня 7, происходит завершение SSL, а подсистема балансировки нагрузки знает URL-адрес назначения.

Мы рекомендуем эту конфигурацию для Exchange 2016 и Exchange 2019. Подсистема балансировки нагрузки настроена для проверки работоспособности конечных серверов почтовых ящиков в пуле балансировки нагрузки, а проба работоспособности настраивается для каждого виртуального каталога.

Например, пока ответ проверки работоспособности Outlook в Интернете работоспособности, подсистема балансировки нагрузки будет хранить целевой

сервер почтовых ящиков в пуле балансировки нагрузки Outlook в Интернете. Однако если проверка работоспособности Outlook в Интернете по какой-либо причине завершается сбоем, подсистема балансировки нагрузки удаляет целевой сервер почтовых ящиков из пула балансировки нагрузки для Outlook в Интернете запросов. В этом примере работоспособность проверяется для каждого протокола, то есть в случае неудачной проверки работоспособности только соответствующий клиентский протокол перенаправляется на другой сервер.

Сценарий В. Одно пространство имен со сходством сеансов, уровень 7

В этом сценарии 7-го уровня для всех клиентов HTTP развертывается одно пространство имен — mail.contoso.com. Так как подсистема балансировки нагрузки настроена для 7-го уровня, SSL-запросы завершаются, а подсистеме балансировки нагрузки известен целевой URL-адрес. Подсистема балансировки нагрузки также настроена для проверки работоспособности целевых серверов почтовых ящиков в пуле балансировки нагрузки. Для каждого виртуального каталога настроен зонд проверки работоспособности.

Однако отключение сходства сеансов приводит к снижению производительности и уровня использования. Это связано с тем, что для более активного использования параметров сходства, балансировки нагрузки на основе файлов cookie или идентификатора сеанса ssl требуется больше обработки и ресурсов. Мы рекомендуем узнать у поставщика, как сходство сеансов влияет на масштабируемость балансировки нагрузки.

Как и в предыдущем сценарии, пока ответ проверки работоспособности Outlook в Интернете работоспособности, подсистема балансировки нагрузки сохраняет целевой сервер почтовых ящиков в пуле балансировки нагрузки Outlook в Интернете. Однако если проверка работоспособности Outlook в Интернете по какой-либо причине завершается сбоем, подсистема балансировки нагрузки удаляет целевой сервер почтовых ящиков из пула балансировки нагрузки для Outlook в Интернете запросов. В этом случае работоспособность проверяется для каждого протокола, то есть в случае неудачной проверки работоспособности только соответствующий клиентский протокол направляется на другой сервер.

Сценарий Г. Несколько пространств имен без сходства сеансов

Последний сценарий с несколькими пространствами имен без сходства сеансов обеспечивает проверку работоспособности отдельных протоколов и возможности 4-го уровня. Для каждого клиента HTTP развертывается уникальное пространство имен. Например, можно настроить клиенты HTTP по адресам mail.contoso.com, mapi.contoso.com и eas.contoso.com.

Этот сценарий обеспечивает проверку работоспособности по протоколу, не требуя сложной логики балансировки нагрузки. Подсистема балансировки нагрузки использует уровень 4 и не настроена для поддержания сходства сеансов. Конфигурация подсистемы балансировки нагрузки проверяет работоспособность целевых серверов почтовых ящиков в пуле балансировки нагрузки. В этом параметре пробы работоспособности настраиваются для определения работоспособности каждого виртуального каталога, так как каждый виртуальный каталог имеет уникальное пространство имен. Так как он настроен для уровня 4, подсистема балансировки нагрузки не знает, к URL-адресу осуществляется доступ, но результат будет таким, как если бы он знал. Так как работоспособность зависит от каждого протокола, в случае сбоя пробы работоспособности на другой сервер направляется только затронутый клиентский протокол.

Балансировка нагрузки и управляемая доступность в Exchange Server

Наблюдение за доступными серверами и службами — ключ к созданию сетей с высоким уровнем доступности. Так как некоторые решения балансировки нагрузки не имеют сведений о целевом URL-адресе или содержимом запроса, это может привести к сложностям для проб работоспособности Exchange.

Exchange 2016 и Exchange 2019 включают встроенное решение для мониторинга, известное как управляемая доступность. Управляемая доступность, также известная как активный мониторинг или локальный активный мониторинг, представляет собой интеграцию встроенных действий мониторинга и восстановления с платформой высокого уровня доступности Exchange.

Служба управляемой доступности включает автономное отвечающее устройство. При вызове автономного отвечающего устройства соответствующий протокол (или сервер) удаляется из службы.

Чтобы подсистемы балансировки нагрузки не направляли трафик на сервер почтовых ящиков, управляемый доступностью, помеченный как автономный, необходимо настроить пробы работоспособности подсистемы балансировки нагрузки для проверки <virtualdirectory>/healthcheck.htm, например `<https://mail.contoso.com/owa/healthcheck.htm>`.

Дополнительные сведения об управляемой доступности см. в статье Управляемое обеспечение доступности.

Настройка проверки подлинности Kerberos для служб клиентского доступа с балансировкой нагрузки

Статья • 04.04.2023

Чтобы использовать проверку подлинности Kerberos с серверами почтовых ящиков с балансировкой нагрузки, на которых выполняются службы клиентского доступа, необходимо выполнить действия по настройке, описанные в этой статье.

Создание учетных данных альтернативной учетной записи службы в доменных службах Active Directory

Все серверы Exchange, на которые запущены службы клиентского доступа с одинаковыми пространствами имен и URL-адресами, должны использовать одни и те же *учетные данные альтернативной учетной записи службы* или (учетные данные ASA). Как правило, достаточно иметь одну учетную запись для леса для каждой версии Exchange.

> ⓘ **Важно!**
>
> Exchange 2010 и Exchange 2016 не могут использовать одинаковые учетные данные ASA. Если учетные данные ASA были созданы для Exchange 2010, необходимо создать новую для Exchange 2016.
>
> Хотя для общих пространств имен поддерживаются записи CNAME, Майкрософт рекомендует использовать записи A. Так клиент будет правильно отправлять запрос билета Kerberos (по общему имени, а не полному доменному имени сервера).

> ⓘ **Примечание**
>
> Групповые управляемые учетные записи служб (gMSA) не поддерживаются в локальных Exchange Server средах и поэтому не могут использоваться в этом сценарии.

При настройке учетных данных ASA помните о следующем.

- **Тип учетной записи**. Рекомендуется создать учетную запись компьютера вместо учетной записи пользователя. Ученая запись компьютера не поддерживает интерактивный вход и может использовать более простые политики безопасности, чем учетная запись пользователя. При создании учетной записи компьютера срок действия пароля не истекает, но мы все равно рекомендуем периодически обновлять пароль. Локальная групповая политика может определять максимальный срок хранения учетных записей компьютера и использовать скрипты для периодического удаления учетных записей компьютера, не соответствующих текущим политикам. Локальная политика безопасности также определяет, когда необходимо изменить пароль. Хотя мы рекомендуем использовать учетную запись компьютера, вы можете создать учетную запись пользователя.

- **Имя учетной записи**. Нет никаких требований к имени учетной записи. Можно использовать любое имя, соответствующее схеме именования.

- **Группа учетных записей**. Учетной записи, используемой для учетных данных ASA, не требуются специальные привилегии безопасности. Если вы используете учетную запись компьютера, она должна быть только членом группы безопасности "Компьютеры домена". Если вы используете учетную запись пользователя, она должна быть только членом группы безопасности "Пользователи домена".

- **Пароль учетной записи**. Пароль, указанный при создании учетной записи, будет использоваться. Поэтому следует указать сложный пароль и, соответствующий требованиям к паролю в организации.

Создание учетных данных ASA как учетной записи компьютера

1. На присоединенном к домену компьютере выполните команду Оболочка Windows PowerShell или Командная консоль Exchange.

   Импортируйте модуль Active Directory с помощью командлета **Import-Module**.

   ```
   PowerShell
   ```

   ```
   Import-Module ActiveDirectory
   ```

2. Выполните командлет **New-ADComputer**, чтобы создать учетную запись компьютера Active Directory, используя следующий синтаксис:

```
PowerShell

New-ADComputer [-Name] <string> [-AccountPassword <SecureString>] [-
AllowReversiblePasswordEncryption <System.Nullable[boolean]>] [-
Description <string>] [-Enabled <System.Nullable[bool]>]
```

Пример:

```
PowerShell

New-ADComputer -Name EXCH2016ASA -AccountPassword (Read-Host 'Enter
password' -AsSecureString) -Description 'Alternate Service Account
credentials for Exchange' -Enabled:$True -SamAccountName EXCH2016ASA
```

Где *EXCH2016ASA* — это имя учетной записи, описание *учетных данных альтернативной учетной записи службы для Exchange* — это все, что вы хотите, а значение параметра *SamAccountName* , в данном случае *EXCH2016ASA*, должно быть уникальным в вашем каталоге.

3. С помощью командлета **Set-ADComputer** можно включить поддержку шифра AES 256, используемого в Kerberos, используя следующий синтаксис:

```
PowerShell

Set-ADComputer [-Name] <string> [-add @{<attributename>="<value>"]
```

Пример:

```
PowerShell

Set-ADComputer EXCH2016ASA -add @{"msDS-SupportedEncryptionTypes"="28"}
```

Где *EXCH2016ASA* — это имя учетной записи, а атрибут для изменения — *msDS-SupportedEncryptionTypes* с десятичным значением 28, что позволяет использовать следующие шифры: RC4-HMAC, AES128-CTS-HMAC-HMAC-SHA1-96, AES256-CTS-HMAC-SHA1-96.

Дополнительные сведения об этих командлетах см. в статьях Import-Module и New-ADComputer.

Сценарии с несколькими лесами

Если у вас есть развертывание между лесами или лесом ресурсов и у вас есть пользователи, которые находятся за пределами леса Active Directory, содержащего Exchange, необходимо настроить отношения доверия между лесами. Кроме того, для каждого леса в развертывании необходимо настроить правило маршрутизации, которое обеспечивает доверие между всеми суффиксами имен в лесу и между лесами. Дополнительные сведения об управлении отношениями доверия между лесами см. в разделе Настройка партнерских организаций.

Определение имен участников-служб для связи с учетными данными ASA

После создания учетных данных ASA необходимо связать имена субъектов-служб Exchange с учетными данными ASA. Список имен субъектов-служб Exchange зависит от текущей конфигурации, но должен содержать следующие имена:

- http/: используйте это имя **субъекта-службы** для Outlook Anywhere, MAPI через HTTP, веб-служб Exchange, автообнаружения и автономной адресной книги.

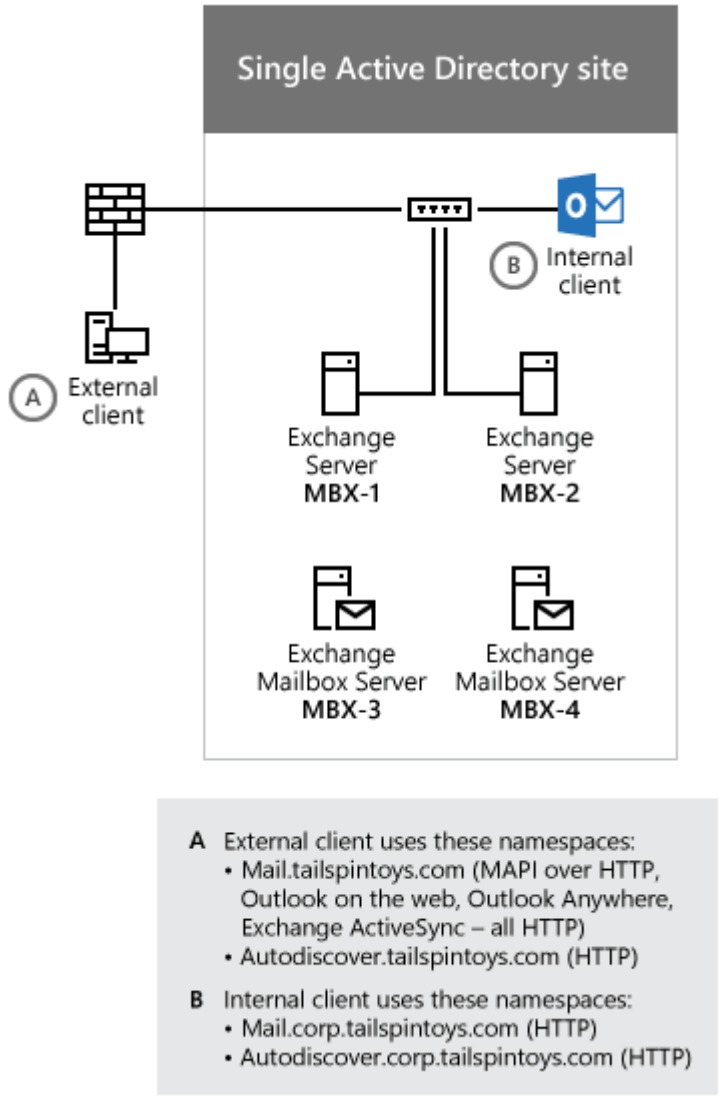
Значения имени субъекта-службы должны соответствовать имени службы в подсистеме балансировки сетевой нагрузки, а не на отдельных серверах. Чтобы лучше определить используемые значения SPN, рассмотрите следующие сценарии:

- Одиночный сайт Active Directory
- Несколько сайтов Active Directory

В каждом из этих сценариев предполагается, что полные доменные имена с балансировкой нагрузки были развернуты для внутренних URL-адресов, внешних URL-адресов и внутренних URI-кодов автообнаружения, используемых серверами со службами клиентского доступа.

Одиночный сайт Active Directory

Если вы используете один сайт Active Directory, ваша среда может походить на изображенную на следующем рисунке:

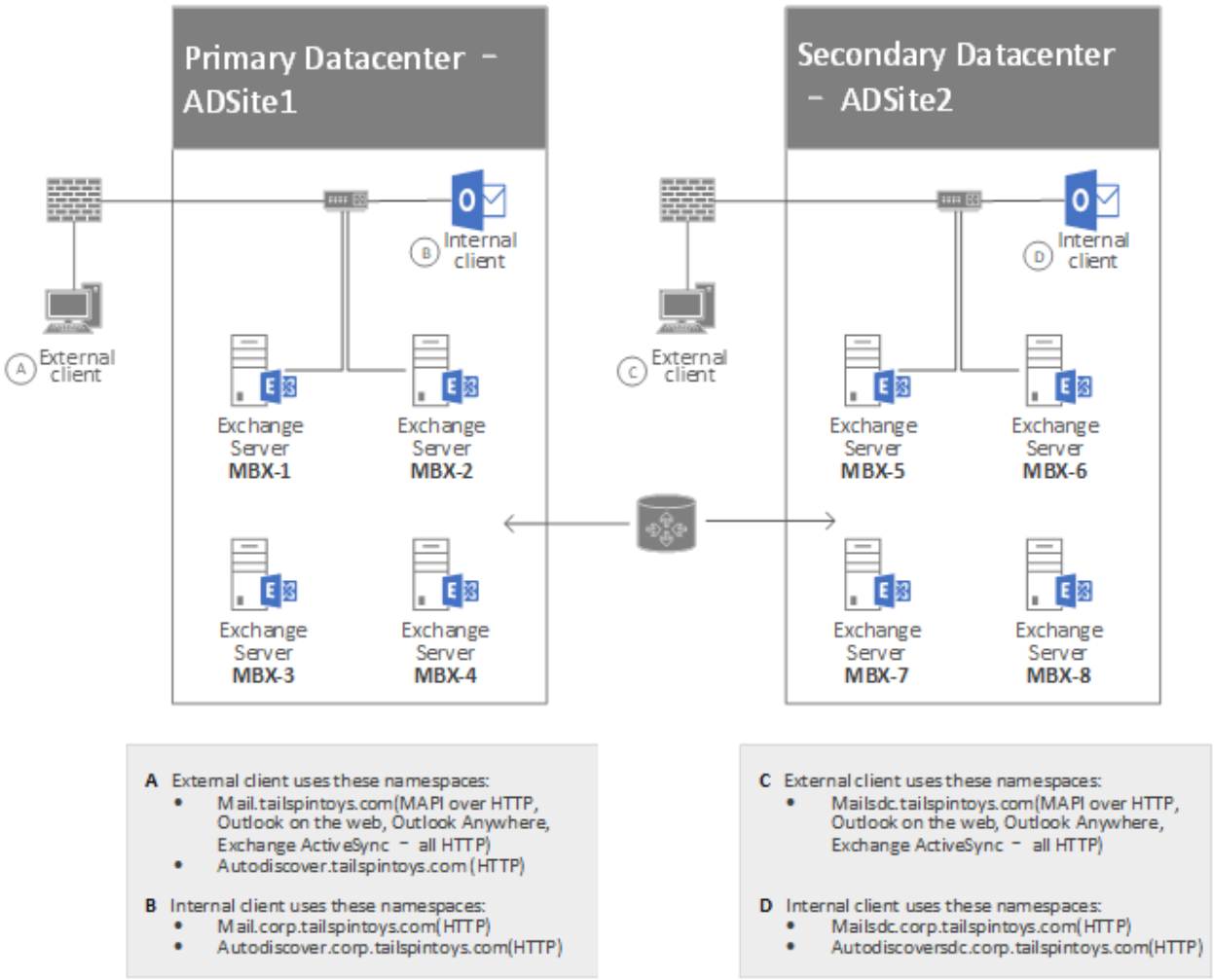


На основе полных доменных имен, используемых внутренними клиентами Outlook на предыдущем рисунке, необходимо связать следующие имена субъектов-служб с учетными данными ASA:

- http/mail.corp.tailspintoys.com
- http/autodiscover.corp.tailspintoys.com

Несколько сайтов Active Directory

Если вы используете несколько сайт Active Directory, ваша среда может походить на изображенную на следующем рисунке:



На основе полных доменных имен, используемых клиентами Outlook на предыдущем рисунке, необходимо связать следующие имена субъектов-служб с учетными данными ASA, которые используются серверами почтовых ящиков, на которых запущены службы клиентского доступа в ADSite 1:

- http/mail.corp.tailspintoys.com
- http/autodiscover.corp.tailspintoys.com

Кроме того, необходимо связать следующие имена субъектов-служб с учетными данными ASA, которые используются серверами почтовых ящиков, на которых запущены службы клиентского доступа в ADSite 2:

- http/mailsdc.corp.tailspintoys.com
- http/autodiscoversdc.corp.tailspintoys.com

Настройка и проверка конфигурации учетных данных ASA на всех серверах со службами клиентского доступа

После создания учетной записи необходимо убедиться, что учетная запись реплицирована на все контроллеры домена AD DS. В частности, учетная запись должна присутствовать на каждом сервере со службами клиентского доступа, которые будут использовать учетные данные ASA. Затем настройте учетную запись как учетные данные ASA на всех серверах со службами клиентского доступа в развертывании.

Для этого используйте командную консоль Exchange, как описано в одной из следующих процедур:

- Развертывание учетных данных ASA на первом сервере Exchange Server, на котором выполняются службы клиентского доступа
- Развертывание учетных данных ASA на последующих серверах Exchange, на которых запущены службы клиентского доступа

Единственный поддерживаемый метод развертывания учетных данных ASA — использовать сценарий RollAlternateServiceAcountPassword.ps1. Дополнительные сведения и необходимые разрешения для запуска скрипта см. в статье Использование скрипта RollAlternateserviceAccountCredential.ps1 в оболочке. После выполнения этого сценария рекомендуем убедиться, что все целевые серверы правильно обновлены.

Развертывание учетных данных ASA на первом сервере Exchange Server, на котором запущены службы клиентского доступа.

1. Откройте командную консоль Exchange на сервере Exchange 2016 или Exchange 2019.

2. Измените каталоги на *<Каталог> установки Exchange 2016*\V15\Scripts.

3. Выполните следующую команду, чтобы развернуть учетные данные ASA на первом сервере Exchange 2016 или Exchange 2019 со службами клиентского доступа:

   PowerShell

   ```
   .\RollAlternateServiceAccountPassword.ps1 -ToSpecificServer cas-
   1.corp.tailspintoys.com -GenerateNewPasswordFor tailspin\EXCH2016ASA$
   ```

4. На вопрос, изменять ли пароль для учетной записи альтернативной службы, выберите **Да**.

Ниже представлен пример выходных данных после запуска сценария RollAlternateServiceAccountPassword.ps1.

Выходные данные

```
========== Starting at 01/12/2016 10:17:47 ==========
Creating a new session for implicit remoting of "Get-ExchangeServer"
command...
Destination servers that will be updated:
Name                                                          PSComputerName
----                                                          --------------
cas-1                                                    cas-
1.corp.tailspintoys.com
Credentials that will be pushed to every server in the specified scope
(recent first):
UserName
Password
--------
--------
tailspin\EXCH2016ASA$
System.Security.SecureString
Prior to pushing new credentials, all existing credentials that are invalid
or no longer work will be removed from  the destination servers.
Pushing credentials to server mbx-1
Setting a new password on Alternate Service Account in Active Directory
Password change
Do you want to change password for tailspin\EXCH2016ASA$ in Active Directory
at this time?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
Preparing to update Active Directory with a new password for
tailspin\EXCH2016ASA$ ...
Resetting a password in the Active Directory for tailspin\EXCH2016ASA$ ...
New password was successfully set to Active Directory.
Retrieving the current Alternate Service Account configuration from servers
in scope
Alternate Service Account properties:
StructuralObjectClass QualifiedUserName Last Pwd Update       SPNs
--------------------- ----------------- ---------------       ----
computer              tailspin\EXCH2016ASA$   1/12/2016 10:19:53 AM
Per-server Alternate Service Account configuration as of the time of script
completion:
   Array: {mail.corp.tailspintoys.com}
Identity  AlternateServiceAccountConfiguration
--------  ------------------------------------
cas-1 Latest: 1/12/2016 10:19:22 AM, tailspin\EXCH2016ASA$
          ...
========== Finished at 01/12/2016 10:20:00 ==========
        THE SCRIPT HAS SUCCEEDED
```

Развертывание учетных данных ASA на другом сервере Exchange, на котором выполняются службы

клиентского доступа

1. Откройте командную консоль Exchange на сервере Exchange 2016 или Exchange 2019.

2. Измените каталоги на *<Каталог> установки Exchange 2016*\V15\Scripts.

3. Выполните следующую команду, чтобы развернуть учетные данные ASA на другом сервере Exchange 2016 или Exchange 2019 со службами клиентского доступа:

   PowerShell

   ```
   .\RollAlternateServiceAccountPassword.ps1 -ToSpecificServer cas-
   2.corp.tailspintoys.com -CopyFrom cas-1.corp.tailspintoys.com
   ```

4. Повторите шаг 3 для всех серверов со службами клиентского доступа, на которых нужно развернуть учетные данные ASA.

Ниже представлен пример выходных данных после запуска сценария RollAlternateServiceAccountPassword.ps1.

Выходные данные

```
========== Starting at 01/12/2016 10:34:35 ==========
Destination servers that will be updated:
Name                                                          PSComputerName
----                                                          --------------
cas-2                                                 cas-
2.corp.tailspintoys.com
Credentials that will be pushed to every server in the specified scope
(recent first):
UserName
Password
--------
--------
tailspin\EXCH2016ASA$
System.Security.SecureString
Prior to pushing new credentials, all existing credentials will be removed
from the destination servers.
Pushing credentials to server mbx-2
Retrieving the current Alternate Service Account configuration from servers
in scope
Alternate Service Account properties:
StructuralObjectClass QualifiedUserName Last Pwd Update       SPNs
--------------------- ----------------- ---------------       ----
computer              tailspin\EXCH2016ASA$   1/12/2016 10:19:53 AM
Per-server Alternate Service Account configuration as of the time of script
completion:
   Array: cas-2.corp.tailspintoys.com
```

```
Identity  AlternateServiceAccountConfiguration
--------  ----------------------------------
cas-2 Latest: 1/12/2016 10:37:59 AM, tailspin\EXCH2016ASA$
          ...
========== Finished at 01/12/2016 10:38:13 ==========
        THE SCRIPT HAS SUCCEEDED
```

Проверка развертывания учетных данных ASA

- Откройте командную консоль Exchange на сервере Exchange 2016 или Exchange 2019.
- Выполните следующую команду, чтобы проверить настройки на сервере со службами клиентского доступа:

  PowerShell

  ```
  Get-ClientAccessServer CAS-3 -
  IncludeAlternateServiceAccountCredentialStatus | Format-List Name,
  AlternateServiceAccountConfiguration
  ```

- Повторите шаг 2 на всех серверах со службами клиентского доступа, на которых нужно проверить развертывание учетных данных ASA.

Ниже приводится пример выходных данных после запуска команды Get-ClientAccessServer, если учетные данные ASA еще не были заданы.

Выходные данные

```
Name                                : CAS-1
AlternateServiceAccountConfiguration : Latest: 1/12/2016 10:19:22 AM,
tailspin\EXCH2016ASA$
                                      Previous: <Not set>
                                         ...
```

Ниже приводится пример выходных данных после запуска команды Get-ClientAccessServer, если учетные данные ASA уже были заданы. Возвращаются учетные данные ASA, а также дата и время их установки.

Выходные данные

```
Name                                : CAS-3
AlternateServiceAccountConfiguration : Latest: 1/12/2016 10:19:22 AM,
tailspin\EXCH2016ASA$
                                      Previous: 7/15/2015 12:58:35 PM,
```

```
tailspin\oldSharedServiceAccountName$
                                                ...
```

Связывание имен участников-служб (SPN) с учетными данными ASA

> ⓘ **Важно!**
>
> Не связывайте имена субъектов-служб с учетными данными ASA, пока не развернете эти учетные данные по крайней мере в одном Exchange Server, как описано выше в статье **Развертывание учетных данных ASA на первом сервере Exchange Server, на котором запущены службы клиентского доступа**. В противном случае выполнить проверку подлинности Kerberos не удастся.

Прежде чем связать имена субъектов-служб с учетными данными ASA, необходимо убедиться, что целевые имена субъектов-служб еще не связаны с другой учетной записью в лесу. Учетные данные ASA должны быть единственной учетной записью в лесу, с которой связаны эти имена субъектов-служб. Чтобы убедиться, что имена участников-служб не назначены другим учетным записям в лесу, выполните команду **setspn** в командной строке.

Проверка связи имени участника-службы с учетной записи в лесу с помощью команды setspn

1. Нажмите кнопку **Пуск**. В поле **Поиск** введите **командная строка**, а затем в списке результатов выберите **Командная строка**.

2. Введите следующую команду:

   Консоль

   ```
   setspn -F -Q <SPN>
   ```

   Где <SPN> — это имя участника-службы, которое требуется связать с учетными данными ASA. Например:

   Консоль

   ```
   setspn -F -Q http/mail.corp.tailspintoys.com
   ```

Команда должна не возвратить никаких данных. Если она возвратит данные, значит, это имя участника службы уже сопоставлено с другой учетной записью. Повторите этот шаг один раз для каждого имени субъекта-службы, которое необходимо связать с учетными данными ASA.

Сопоставление имени участника-службы с учетными данными ASA с помощью команды setspn

1. Нажмите кнопку **Пуск**. В поле **Поиска** введите **Командная строка**, а затем выберите **Командная строка** в списке результатов.

2. Введите следующую команду:

   ```
   Консоль
   setspn -S <SPN> <Account>$
   ```

   Где <SPN> — это имя участника-службы, которое требуется связать с учетными данными ASA, а <Account> — это учетная запись, связанная с учетными данными ASA. Например:

   ```
   Консоль
   setspn -S http/mail.corp.tailspintoys.com tailspin\EXCH2016ASA$
   ```

   Выполните эту команду один раз для каждого имени субъекта-службы, которое нужно связать с учетными данными ASA.

Проверка связи имен участников-служб с учетными данными ASA с помощью команды setspn

1. Нажмите кнопку **Пуск**. В поле **Поиска** введите **Командная строка**, а затем выберите **Командная строка** в списке результатов.

2. Введите следующую команду:

   ```
   Консоль
   setspn -L <Account>$
   ```

   Где <Account> — это учетная запись, связанная с учетными данными ASA. Например:

Консоль

```
setspn -L tailspin\EXCH2016ASA$
```

Эту команду необходимо выполнить только один раз.

Включение проверки подлинности Kerberos для клиентов Outlook

1. Откройте командную консоль Exchange на сервере Exchange 2016 или Exchange 2019.

2. Чтобы включить проверку подлинности Kerberos для клиентов Outlook Anywhere, выполните следующую команду на сервере Exchange 2016 или Exchange 2019, на котором выполняются службы клиентского доступа:

   PowerShell

   ```
   Get-OutlookAnywhere -Server CAS-1 | Set-OutlookAnywhere -
   InternalClientAuthenticationMethod  Negotiate
   ```

3. Чтобы включить проверку подлинности Kerberos для MAPI через HTTP-клиенты, выполните следующую команду на сервере Exchange 2016 или Exchange 2019 со службами клиентского доступа:

   PowerShell

   ```
   Get-MapiVirtualDirectory -Server CAS-1 | Set-MapiVirtualDirectory -
   IISAuthenticationMethods Ntlm,Negotiate
   ```

   В гибридных средах с Exchange Online или при внутреннем использовании OAuth выполните следующие команды на сервере Exchange 2016 или Exchange 2019 со службами клиентского доступа:

   PowerShell

   ```
   $mapidir = Get-MapiVirtualDirectory -Server CAS-1
   $mapidir | Set-MapiVirtualDirectory -IISAuthenticationMethods
   ($mapidir.IISAuthenticationMethods +='Negotiate')
   ```

4. Повторите шаги 2 и 3 для каждого сервера Exchange 2016 или Exchange 2019 со службами клиентского доступа, для которых требуется включить проверку

подлинности Kerberos.

Проверка проверки подлинности Kerberos клиента Exchange

После успешной настройки Kerberos и учетных данных ASA убедитесь, что клиенты могут успешно пройти проверку подлинности, как описано в этих задачах.

Проверка работы службы Microsoft Exchange Service Host

Служба узла службы Microsoft Exchange (MSExchangeServiceHost) на сервере, на котором выполняются службы клиентского доступа, отвечает за управление учетными данными ASA. Если эта служба не запущена, проверка подлинности Kerberos невозможна. По умолчанию служба запускается автоматически при включении компьютера.

Чтобы убедиться, что служба Microsoft Exchange Service Host запущена:

1. Нажмите кнопку **Пуск**, введите **services.msc** и выберите **services.msc** из списка.
2. В окне **Службы** найдите службу **Microsoft Exchange Service Host**.
3. Состояние службы должно быть указано как **Работает**. Если состояние отличается от **Работает**, щелкните службу правой кнопкой мыши и выберите команду **Пуск**.

Проверка Kerberos на сервере, на котором запущены службы клиентского доступа

При настройке учетных данных ASA на каждом сервере, на котором выполняются службы клиентского доступа, вы выполнили командлет **Set-ClientAccessServer** . После выполнения этого командлета можно использовать журналы для проверки успешного подключения Kerberos.

Проверка правильности работы Kerberos с помощью файла журнала HttpProxy

1. В текстовом редакторе перейдите к папке, где хранится журнал HttpProxy. По умолчанию этот файл находится в следующей папке:

%ExchangeInstallPath%\Logging\HttpProxy\RpcHttp

2. Откройте последний файл журнала и найдите слово **Negotiate**. Строка в файле журнала должна выглядеть примерно следующим образом:

```
2014-02-19T13:30:49.219Z,e19d08f4-e04c-42da-a6be-
b7484b396db0,15,0,775,22,,RpcHttp,mail.corp.tailspintoys.com,/rpc/rpcpr
oxy.dll,,Negotiate,True,tailspin\Wendy,tailspintoys.com,MailboxGuid~ad4
4b1e0-e44f-4a16-9396-
3a437f594f88,MSRPC,192.168.1.77,EXCH1,200,200,,RPC_OUT_DATA,Proxy,exch2
.tailspintoys.com,15.00.0775.000,IntraForest,MailboxGuidWithDomain,,,,7
6,462,1,,1,1,,0,,0,,0,0,16272.3359,0,0,3,0,23,0,25,0,16280,1,16274,1623
0,16233,16234,16282,?ad44b1e0-e44f-4a16-9396-
3a437f594f88@tailspintoys.com:6001,,BeginRequest=2014-02-
19T13:30:32.946Z;BeginGetRequestStream=2014-02-
19T13:30:32.946Z;OnRequestStreamReady=2014-02-
19T13:30:32.946Z;BeginGetResponse=2014-02-
19T13:30:32.946Z;OnResponseReady=2014-02-
19T13:30:32.977Z;EndGetResponse=2014-02-
19T13:30:32.977Z;,PossibleException=IOException;
```

Если вы видите, что значение **AuthenticationType** равно **Negotiate**, сервер успешно создает подключения с проверкой подлинности Kerberos.

Обслуживание учетных данных ASA

Если необходимо периодически обновлять пароль для учетных данных ASA, выполните действия по настройке учетных данных ASA, описанные в этой статье. Также для регулярного обновления пароля можно настроить запланированную задачу. Отслеживайте выполнение этой запланированной задачи для проверки своевременного переключения паролей и предотвращения возможных простоев проверки подлинности.

Отключение проверки подлинности Kerberos

Чтобы настроить прекращение использования Kerberos на серверах со службами клиентского доступа, отключите или удалите имена субъектов-служб из учетных данных ASA. Если имена субъектов-служб удалены, проверка подлинности Kerberos не будет выполняться вашими клиентами, а клиенты, настроенные на использование проверки подлинности Negotiate, будут использовать NTLM. Клиенты, настроенные для использования только Kerberos, не смогут

подключиться. После удаления имен субъектов-служб также следует удалить учетную запись.

Удаление учетных данных ASA

1. Откройте командную консоль Exchange на сервере Exchange 2016 или Exchange 2019 и выполните следующую команду:

   ```
   PowerShell
   ```

   ```
   Set-ClientAccessServer CAS-1 -RemoveAlternateServiceAccountCredentials
   ```

2. Хотя и не сразу, но вам потребуется перезапустить все клиентские компьютеры, чтобы удалить кэш билетов Kerberos с компьютера.

Цифровые сертификаты и шифрование в Exchange Server

Статья • 04.04.2023

Шифрование и цифровые сертификаты очень важны в любой организации. По умолчанию Exchange Server настроен для шифрования обмена данными между внутренними серверами Exchange и между службами Exchange на локальном сервере с помощью ПРОТОКОЛА TLS. Но администраторы Exchange должны сами настроить шифрование связи с внутренними и внешними клиентами (компьютерами и мобильными устройствами) и внешними серверами обмена сообщениями.

> ⓘ **Примечание**
>
> Exchange Server 2019 г. внесены важные изменения для повышения безопасности подключений клиентов и серверов. Настройка по умолчанию для шифрования поддерживает только TLS 1.2 и не поддерживает более ранние алгоритмы (а именно, DES, 3DES, RC2, RC4 и MD5). В ней также настроены алгоритмы обмена ключами эллиптических кривых, обладающие приоритетом над алгоритмами неэллиптических кривых. В Exchange Server 2016 и более поздних версиях все параметры шифрования наследуются из настройки, указанной в операционной системе. Дополнительные сведения см. в **руководстве по Exchange Server TLS** .

В этой статье описаны доступные типы сертификатов, конфигурация по умолчанию для сертификатов в Exchange и рекомендации по дополнительным сертификатам, которые необходимо использовать с Exchange.

Процедуры, необходимые для сертификатов в Exchange Server, см. в разделе Процедуры сертификатов в Exchange Server.

Обзор цифровых сертификатов

Цифровые сертификаты — это файлы, которые используются аналогично паролям для подтверждения подлинности пользователя или компьютера. С их помощью создается зашифрованный канал, по которому осуществляется взаимодействие с клиентами. Сертификат — это цифровой документ, выпускаемый центром сертификации; он подтверждает подлинность держателя сертификата и позволяет сторонам взаимодействовать безопасным способом, используя шифрование.

Цифровые сертификаты используются в следующих целях:

- **Шифрование**. Они помогают защитить данные, которые обмениваются от кражи или незаконного изменения.
- **Проверка подлинности**. Они проверяют, что их владельцы (люди, веб-сайты и даже сетевые устройства, такие как маршрутизаторы) действительно являются тем, за кого они претендуют. Обычно проверка подлинности является односторонней (исходный объект проверяет удостоверение целевого объекта), но также возможна взаимная проверка подлинности TLS.

Сертификаты могут быть выданы для нескольких применений. Например, проверка подлинности веб-пользователей, проверка подлинности веб-сервера, безопасные и многоцелевые расширения электронной почты (S/MIME), безопасность по протоколу ИНТЕРНЕТ (IPsec) и подписывание кода.

Сертификат содержит открытый ключ, который он связывает с удостоверением владельца (пользователя, компьютера или службы) соответствующего закрытого ключа. Открытый и закрытый ключи используются клиентом и сервером для шифрования данных перед их передачей. Для пользователей, компьютеров и служб Windows доверие в центре сертификации устанавливается, если корневой сертификат определен в хранилище доверенных корневых сертификатов, а сертификат содержит допустимый путь сертификации. Сертификат считается действительным, если он не отозван (его нет в списке отзыва сертификатов ЦС) и не истек срок его действия.

Ниже описаны три основных типа цифровых сертификатов.

Тип	Описание	Преимущества	Недостатки

Тип	Описание	Преимущества	Недостатки
Самозаверяющий сертификат	Сертификат подписывается приложением, которое его создает.	Затраты (бесплатно).	Клиентские компьютеры и мобильные устройства не доверяют такому сертификату по умолчанию. Его нужно вручную добавить в хранилище доверенных корневых сертификатов на всех клиентских компьютерах и устройствах, но внести изменения в хранилище доверенных корневых сертификатов можно не на всех мобильных устройствах. Не все службы работают с самозаверяющими сертификатами. Трудно создать инфраструктуру для управления жизненным циклом сертификатов. Например, самозаверяющие сертификаты нельзя отозвать.
Сертификат, выданный внутренним ЦС	Сертификат выдается инфраструктурой открытых ключей (PKI) в вашей организации. Примером являются службы сертификатов Active Directory (AD CS). Дополнительные сведения см. в статье Обзор служб сертификатов Active Directory.	Позволяет организациям выдавать собственные сертификаты. Дешевле сертификатов из коммерческого ЦС.	Сложность в развертывании и обслуживании PKI. Клиентские компьютеры и мобильные устройства не доверяют такому сертификату по умолчанию. Его нужно вручную добавить в хранилище доверенных корневых сертификатов на всех клиентских компьютерах и устройствах, но внести изменения в хранилище доверенных корневых сертификатов можно не на всех мобильных устройствах.

Тип	Описание	Преимущества	Недостатки
Сертификат, выданный коммерческим ЦС	Сертификат приобретается у доверенного коммерческого ЦС.	Упрощенное развертывание сертификатов, так как им автоматически доверяют все клиенты, устройства и серверы.	Затраты. Нужно заранее все спланировать, чтобы свести к минимуму количество необходимых сертификатов.

Держатель сертификата должен быть точно определен в сертификате, чтобы другие клиенты, устройства и серверы могли его идентифицировать. В таблице ниже описаны три основных способа достижения этой цели.

Метод	Описание	Преимущества	Недостатки
Соответствие темы сертификата	Поле **Subject** сертификата содержит общее имя (CN) узла. Например, сертификат, выданный www.contoso.com, можно использовать для веб-сайта https://www.contoso.com.	Совместим со всеми клиентами, устройствами и службами. Обособление. Отзыв сертификата для узла не влияет на другие узлы.	Количество необходимых сертификатов. Сертификат можно использовать только для указанного узла. Например, вы не можете использовать сертификат www.contoso.com для ftp.contoso.com, даже если службы установлены на том же сервере. Сложность. На веб-сервере для каждого сертификата требуется собственная привязка к IP-адресу.

Метод	Описание	Преимущества	Недостатки
Соответствие альтернативного имени субъекта (SAN) сертификата	В дополнение к полю **Subject**, поле **Subject Alternative Name** сертификата содержит список нескольких имен узлов. Например: • www.contoso.com • ftp.contoso.com • ftp.eu.fabirkam.net	Удобство. Один сертификат можно использовать для нескольких узлов в отдельных доменах. Большинство клиентов, устройств и служб поддерживают сертификаты SAN. Аудит и безопасность. Вы точно знаете, какие узлы могут использовать сертификат SAN.	Требуется дополнительное планирование. При создании сертификата необходимо указать список узлов. Отсутствие обособления. Нельзя выборочно отзывать сертификаты для указанных узлов, не влияя на все узлы в сертификате.

Метод	Описание	Преимущества	Недостатки
Соответствие группового сертификата	Поле **Subject** сертификата содержит общее имя в виде подстановочного знака (*) и одного домена или поддомена. Например, *.contoso.com или *.eu.contoso.com. Групповой сертификат *.contoso.com можно использовать для: • www.contoso.com • ftp.contoso.com • mail.contoso.com	Гибкость. Вам не нужно указывать список узлов при запросе сертификата, и вы можете использовать сертификат для любого количества узлов, которое может потребоваться в будущем.	Групповые сертификаты нельзя использовать с другими доменами верхнего уровня. Например, групповой сертификат *.contoso.com нельзя использовать для узлов *.contoso.net. Групповые сертификаты можно использовать только для имен узлов на уровне подстановочного знака. Например, нельзя использовать сертификат *.contoso.com для www.eu.contoso.com. Кроме того, сертификат *.eu.contoso.com нельзя использовать для www.uk.eu.contoso.com. Старые клиенты, устройства, приложения и службы могут не поддерживать групповые сертификаты. Подстановочные знаки нельзя использовать с сертификатами высокой надежности. Требуется тщательный аудит и контроль. Компрометация группового сертификата влияет на все узлы в указанном домене.

Сертификаты в Exchange

При установке Exchange 2016 или Exchange 2019 на сервере Exchange создаются и устанавливаются два самозаверяющего сертификата. Microsoft Windows создает и устанавливает третий самозаверяющий сертификат для службы веб-управления в

службах IIS. Эти сертификаты видны в Центре администрирования Exchange (EAC) и командной консоли Exchange и описаны в таблице ниже.

Имя	Comments
Microsoft Exchange	Этому самозаверяющему сертификату Exchange присущи следующие возможности: • Сертификат автоматически становится доверенным для всех остальных серверов Exchange в организации. Сюда входят все пограничные транспортные серверы, подписанные организацией Exchange. • Сертификат автоматически включается для всех служб Exchange, кроме единой системы обмена сообщениями, и используется для шифрования внутренней связи между серверами Exchange, службами Exchange на одном компьютере и клиентскими подключениями, которые передаются из служб клиентского доступа на серверы почтовых ящиков. (**Примечание**. UM недоступна в Exchange 2019.) • Сертификат автоматически активируется для входящих подключений с внешних серверов обмена сообщениями SMTP и исходящих подключений к внешним серверам обмена сообщениями SMTP. Эта конфигурация по умолчанию позволяет Exchange предоставлять *оппортунистические протоколы TLS* для всех входящих и исходящих SMTP-подключений. Exchange пытается зашифровать сеанс SMTP на внешнем сервере обмена сообщениями, но если внешний сервер не поддерживает шифрование TLS, сеанс не шифруется. • Сертификат не обеспечивает шифрованную связь с внутренними или внешними клиентами. Клиенты и серверы не доверяют самозаверяющему сертификату Exchange, так как сертификат не определен в их хранилищах доверенных корневых сертификатов.
Сертификат проверки подлинности Microsoft Exchange Server	Этот самозаверяющий сертификат Exchange используется для проверки подлинности между серверами и интеграции с помощью OAuth. Дополнительные сведения см. в статье Планирование интеграции Exchange Server с SharePoint и Skype для бизнеса.
WMSVC	Этот самозаверяющий сертификат Windows используется службой веб-управления IIS для удаленного управления веб-сервером и связанными с ним веб-сайтами и приложениями. Если вы удалите этот сертификат и не выберете действительный сертификат, служба веб-управления не запустится. Наличие службы в этом состоянии может помешать установке обновлений Exchange или удалению Exchange с сервера. Инструкции по устранению этой проблемы см. в разделе Идентификатор события 1007 — проверка подлинности службы веб-управления IIS.

Свойства этих самозаверяющих сертификатов описаны в разделе Свойства самозаверяющих сертификатов по умолчанию.

Ниже описано, что нужно учитывать при управлении сертификатами в Exchange.

- Для шифрования сетевого трафика между серверами Exchange и службами в вашей организации не нужно заменять самозаверяющий сертификат Microsoft Exchange.
- Дополнительные сертификаты необходимы для шифрования подключений к серверам Exchange с помощью внутренних и внешних клиентов.
- Дополнительные сертификаты необходимы для принудительного шифрования SMTP-подключений между серверами Exchange и внешними серверами обмена сообщениями.

Следующие элементы планирования и развертывания для Exchange Server являются важными факторами, определяющими требования к сертификатам:

- **Балансировка нагрузки**. Планируется ли завершить зашифрованный канал на подсистеме балансировки нагрузки или обратном прокси-сервере, использовать подсистемы балансировки нагрузки уровня 4 или 7, а также использовать сходство сеансов или нет сопоставления сеансов? Дополнительные сведения см. в статье Балансировка нагрузки в Exchange 2016.
- **Планирование пространства имен**. Какие версии Exchange существуют, используете ли вы модель ограниченного или неограниченного пространства имен, а также используете ли вы разделенный dns (настраивая разные *IP-адреса* для одного узла на основе внутреннего и внешнего доступа)? Дополнительные сведения см. в статье Планирование пространства имен в Exchange 2016.
- **Подключение клиентов**. Какие службы будут использовать клиенты (веб-службы, POP, IMAP и т. д.) и какие версии Exchange используются? Дополнительную информацию см. в следующих статьях:
  - Подключения клиентов в смешанной среде Exchange 2016 и Exchange 2013
  - Подключения клиентов в смешанной среде Exchange 2016 и Exchange 2010
  - Подключения клиентов в смешанной среде Exchange 2016 и другие версии Exchange

Требования к сертификатам для служб Exchange Server

Службы Exchange, которым могут быть назначены сертификаты, описаны в приведенной ниже таблице.

Служба	Описание
IIS (HTTP)	По умолчанию следующие службы предлагаются на веб-сайте по умолчанию в службах клиентского доступа на сервере почтовых ящиков и используются клиентами для подключения к Exchange: • Автообнаружение • Exchange ActiveSync • Центр администрирования Exchange • веб-службы Exchange • Распространение автономных адресных книг • Мобильный Outlook (протокол RPC через HTTP) • MAPI Outlook через HTTP • Outlook в Интернете • Удаленная оболочка PowerShell* Так как с веб-сайтом можно связать только один сертификат, все DNS-имена, используемые клиентами для подключения к этим службам, необходимо указать в сертификате. Для этого можно использовать сертификат SAN или групповой сертификат.
POP или IMAP	Сертификаты, используемые для POP или IMAP, могут отличаться от сертификата, используемого для IIS. Однако для упрощения администрирования рекомендуется также включить в сертификат IIS имена узлов, используемые для POP или IMAP, и использовать один сертификат для всех этих служб.

Служба	Описание
SMTP	SMTP-подключения от клиентов или серверов обмена сообщениями принимаются одним или несколькими соединителями получения, настроенными в транспортной службе переднего плана на сервере Exchange Server. Подробнее см. в разделе Соединители получения. Чтобы требовать шифрование TLS для SMTP-подключений, можно использовать отдельный сертификат для каждого соединителя получения. Сертификат должен включать DNS-имя, которое используется клиентами SMTP или серверами для подключения к соединителю получения. Чтобы упростить управление сертификатами, рекомендуется включить все DNS-имена, для которых требуется поддержка трафика TLS, в один сертификат. Сведения о необходимости *взаимной проверки подлинности TLS*, при которой SMTP-подключения между исходным и целевым серверами шифруются и проходят проверку подлинности, см. в разделе Безопасность домена.
Единая система обмена сообщениями	Дополнительные сведения см. в статье Deploying Certificates for UM. **Примечание**. UM недоступна в Exchange 2019.
Гибридное развертывание с помощью Microsoft 365 или Office 365	Дополнительные сведения см. в статье Certificate Requirements for Hybrid Deployments.
Secure/Multipurpose Internet Mail Extensions (S/MIME)	Дополнительные сведения см. в статье S/MIME для подписи и шифрования сообщений.

* Проверка подлинности Kerberos и шифрование Kerberos используются для удаленного доступа PowerShell из Центра администрирования Exchange и командной консоли Exchange. Поэтому не нужно настраивать сертификаты для использования с удаленной оболочкой PowerShell, если вы подключаетесь непосредственно к серверу Exchange (а не к пространству имен с балансировкой нагрузки). Чтобы использовать удаленный PowerShell для подключения к серверу Exchange Server с компьютера, который не является членом домена, или для подключения из Интернета, необходимо настроить сертификаты для использования с удаленной оболочкой PowerShell.

Рекомендации по сертификатам Exchange

Хотя конфигурация цифровых сертификатов в организации изменяется в зависимости от текущих потребностей, эти рекомендации помогут вам подобрать

оптимальную конфигурацию цифровых сертификатов.

- **Используйте как можно меньше сертификатов**. Скорее всего, это означает использование сертификатов SAN или сертификатов с подстановочными знаками. Что касается взаимодействия с Exchange, то оба варианта функционально эквивалентны. Решение о том, следует ли использовать сертификат SAN и сертификат с подстановочными знаками, больше связано с ключевыми возможностями или ограничениями (реальными или воспринимаемыми) для каждого типа сертификата, как описано в обзоре цифровых сертификатов.

  Например, если все общие имена будут находиться на одном уровне contoso.com, не имеет значения, какой сертификат использовать (SAN или групповой). Но для autodiscover.contoso.com, autodiscover.fabrikam.com и autodiscover.northamerica.contoso.com необходимо использовать сертификат SAN.

- **Использование сертификатов из коммерческого ЦС для подключений клиентов и внешних серверов**. Хотя вы можете настроить большинство клиентов, чтобы доверять любому сертификату или издателю сертификата, гораздо проще использовать сертификат из коммерческого ЦС для клиентских подключений к серверам Exchange. Для доверия сертификату, выданному коммерческим ЦС, на клиенте не требуется настройка. Многие коммерческие ЦС предлагают сертификаты, настроенные специально для Exchange. Вы можете использовать EAC или командную консоль Exchange для создания запросов на сертификаты, которые работают с большинством коммерческих ЦС.

- **Выберите правильный коммерческий ЦС**: сравните цены на сертификаты и функции между ЦС. Например:

  - Убедитесь, что центру сертификации доверяют клиенты (операционные системы, браузеры и мобильные устройства), которые подключаются к серверам Exchange.

  - Убедитесь, что ЦС поддерживает необходимый вам сертификат. Например, не все ЦС поддерживают сертификаты SAN, ЦС может ограничивать количество допустимых общих имен в сертификате SAN или взимать дополнительную плату исходя из количества общих имен в сертификате SAN.

  - Узнайте, предоставляет ли ЦС льготный период, в течение которого в сертификаты SAN можно бесплатно добавлять дополнительные общие

имена.

  - Убедитесь, что лицензия позволяет использовать сертификат на нужном количестве серверов. Некоторые ЦС позволяют использовать сертификат только на одном сервере.

- **Использование мастера сертификатов Exchange**. При создании сертификатов часто возникает ошибка, когда вы забываете одно или несколько распространенных имен, необходимых для служб, которые вы хотите использовать. Мастер сертификатов в Центре администрирования Exchange помогает включить правильный список общих имен в запрос на сертификат. Мастер позволяет указать службы, которые будут использовать сертификат, и включает общие имена, необходимые для этих служб. Запустите мастер сертификатов, когда вы развернули исходный набор серверов Exchange 2016 или Exchange 2019 и определили, какие имена узлов следует использовать для различных служб для развертывания.

- **Используйте как можно меньше имен узлов**. Минимизация количества имен узлов в сертификатах SAN снижает сложность управления сертификатами. Не обязайте включать имена узлов отдельных серверов Exchange в сертификаты SAN, если это не требуется для предполагаемого использования сертификата. Как правило, необходимо включать только DNS-имена, которые предоставляются внутренним клиентам, внешним клиентам или внешним серверам, которые используют сертификат для подключения к Exchange.

  Для простой Exchange Server организации с именем Contoso это гипотетический пример минимальных необходимых имен узлов:

  - **mail.contoso.com**. Это имя узла охватывает большинство подключений к Exchange, включая Outlook, Outlook в Интернете, распространение автономной адресной адресной области, веб-службы Exchange, Центр администрирования Exchange и Exchange ActiveSync.

  - **autodiscover.contoso.com**. Это конкретное имя узла требуется клиентам, поддерживающим автообнаружения, включая Outlook, Exchange ActiveSync и клиенты веб-служб Exchange. Дополнительные сведения см. в разделе Служба автообнаружения.

Свойства самозаверяющих сертификатов по умолчанию

Наиболее интересные свойства самозаверяющих сертификатов по умолчанию, которые отображаются в Центре администрирования Exchange и/или командной консоли Exchange на сервере Exchange, описаны в таблице ниже.

Свойство	**Microsoft Exchange**	**Сертификат проверки подлинности Microsoft Exchange Server**	**WMSVC**
Тема	`CN=<ServerName>` (например, `CN=Mailbox01`)	`CN=Microsoft Exchange Server Auth Certificate`	`CN=WMSvc-<ServerName>` (например, `CN=WMSvc-Mailbox01`)
Альтернативные имена субъектов (домены сертификатов)	*<ServerName>* (например, Mailbox01) *<ServerFQDN>* (например, Mailbox01.contoso.com)	none	`WMSvc-<ServerName>` (например, `WMSvc-Mailbox01`)
Имеет закрытый ключ (HasPrivateKey)	**Да** (True)	**Да** (True)	**Да** (True)
PrivateKeyExportable*	Неверно	Да	Да
EnhancedKeyUsageList*	Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)	Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)	Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)
Службы IIS*	`IIS://<ServerName>/W3SVC/1, IIS://<ServerName>/W3SVC/2` (например, `IIS://Mailbox01/W3SVC/1, IIS://Mailbox01/W3SVC/2`)	none	none
IsSelfSigned	Да	Да	Да
Издатель	`CN=<ServerName>` (например, `CN=Mailbox01`)	`CN=Microsoft Exchange Server Auth Certificate`	`CN=WMSvc-<ServerName>` (например, `CN=WMSvc-Mailbox01`)

Свойство	Microsoft Exchange	Сертификат проверки подлинности Microsoft Exchange Server	WMSVC
NotBefore	Дата и время установки Exchange.	Дата и время установки Exchange.	Даты и время установки службы веб-управления IIS.
Срок действия истекает (NotAfter)	Через 5 лет после `NotBefore`.	Через 5 лет после `NotBefore`.	Через 10 лет после `NotBefore`.
Размер открытого ключа (PublicKeySize)	2048	2048	2048
RootCAType	Системный реестр	Нет	Реестр
Службы	IMAP, POP, IIS, SMTP	SMTP	Нет

* Эти свойства не отображаются в стандартном представлении командной консоли Exchange. Чтобы просмотреть их, необходимо указать имя свойства (точное или с использованием подстановочных знаков) с помощью командлетов **Format-Table** или **Format-List**. Например:

- `Get-ExchangeCertificate -Thumbprint <Thumbprint> | Format-List *`
- `Get-ExchangeCertificate -Thumbprint <Thumbprint> | Format-Table -Auto FriendlyName,*PrivateKey*`

Дополнительные сведения см. в разделе Get-ExchangeCertificate.

Дополнительные сведения о самозаверяющих сертификатах по умолчанию, которые отображаются в диспетчере сертификатов Windows, приведены в таблице ниже.

Свойство	Microsoft Exchange	Сертификат проверки подлинности Microsoft Exchange Server	WMSVC
Алгоритм подписи	sha256RSA[1]	sha256RSA[1]	sha256RSA[1]
Хэш-алгоритм подписи	sha256[1]	sha256[1]	sha256[1]

Свойство	Microsoft Exchange	Сертификат проверки подлинности Microsoft Exchange Server	WMSVC
Использование ключа	Цифровая подпись, шифрование ключа (a0)	Цифровая подпись, шифрование ключа (a0)	Цифровая подпись, шифрование ключа (a0), шифрование данных (b0 00 00 00)
Основные ограничения	`Subject Type=End Entity` `Path Length Constraint=None`	`Subject Type=End Entity` `Path Length Constraint=None`	н/д
Алгоритм отпечатка	sha256[1]	sha256[1]	sha256[1]

[1] Применяется к новым установкам Exchange 2016 с накопительным обновлением 22 или более поздней версии и Накопительным пакетом обновления 11 для Exchange 2019 или более поздней версии. Дополнительные сведения см. в разделе Exchange Server сертификатов 2019 и 2016, созданных во время установки, используют хэш SHA-1.

Как правило, диспетчер сертификатов Windows не используется для управления сертификатами Exchange (используется Центр администрирования Exchange или Командная консоль Exchange). Обратите внимание, что сертификат WMSVC не является сертификатом Exchange.

Процедуры сертификатов в Exchange Server

Статья • 04.04.2023

Чтобы обеспечить инфраструктуру безопасного обмена сообщениями для предприятия, необходимо правильно установить и настроить сертификаты. В Exchange Server вы можете управлять сертификатами в Центре администрирования Exchange (EAC) и в командной консоли Exchange. Управлять сертификатами в Центре администрирования Exchange удобнее, чем в консоли управления Exchange в Exchange Server 2010. В частности:

- Требуется меньше сертификатов.
- Требуется меньше взаимодействия с сертификатами.
- Администраторы могут централизованно устанавливать сертификаты и управлять ими на всех серверах Exchange в организации.

Дополнительные сведения о сертификатах в Exchange см. в статье Цифровые сертификаты и шифрование в Exchange Server.

Задачи, связанные с управлением сертификатами в Exchange, описаны в приведенной ниже таблице.

Задача	**EAC**	**Командная консоль Exchange**	**Статья**	**Comments**
Создание самозаверяющего сертификата на сервере Exchange	**Серверов**>**Сертификаты**>щелкните ➕>>**Создание самозаверяющего сертификата**	**New-ExchangeCertificate**	Создание самозаверяющего сертификата Exchange Server	Вы можете создавать самозаверяющие сертификаты и настраивать их для служб Exchange за один шаг.
Создание запроса на сертификат (также называемого запросом подписи сертификата) для центра сертификации (ЦС).	**Серверов**>**Сертификаты**>щелкните ➕>>**Создание запроса на сертификат из центра сертификации**	**New-ExchangeCertificate** с параметром *GenerateRequest* .	Создание запроса на сертификат Exchange Server для центра сертификации	Процедуры одинаковы для внутреннего (например, службы сертификации Active Directory) и коммерческого ЦС.
Выполнение ожидающего запроса сертификата на сервере Exchange	**Серверов**>**Сертификаты**>Выберите сервер>, выберите запрос > сертификата, щелкните ссылку **Завершить** в области сведений.	**Import-ExchangeCertificate**	Выполнение ожидающего запроса на сертификат Exchange Server	После того как вы получите файл или несколько файлов сертификата из ЦС, установите их на сервере Exchange.

Задача	EAC	Командная консоль Exchange	Статья	Comments
Назначение сертификата службам Exchange	**Серверов**>**Сертификаты**> выберите сервер>, щелкните ✎ >> Вкладка "**Службы**".	**Enable-ExchangeCertificate**	Назначение сертификатов службам Exchange Server	Процедуры одинаковы для самозаверяющих сертификатов и сертификатов, выданных ЦС. Сертификаты, выданные ЦС, можно назначить службам Exchange только после выполнения ожидающего запроса сертификата (установки сертификата на сервер Exchange).
Удаление существующего сертификата или запроса сертификата с сервера Exchange	**Серверов**>**Сертификаты**> Выберите сервер>, щелкните 🗑 сертификат > Удалить.	**Remove-ExchangeCertificate**	н/д	Процедуры одинаковы для самозаверяющих сертификатов, запросов сертификатов и сертификатов, выданных ЦС.
Обновление существующего сертификата на сервере Exchange	**Серверов**>**Сертификаты**> выберите сервер>, выберите сертификат>, нажмите кнопку **Продлить** в области сведений.	**Get-ExchangeCertificate** и **New-ExchangeCertificate**	Продление сертификата Exchange Server	Самозаверяющие сертификаты продлеваются за одно действие. Для сертификатов, выданных ЦС, создайте запрос на продление сертификата и отправьте его в ЦС. Если срок действия сертификата на любом сервере Exchange в организации скоро истечет, в Центре администрирования Exchange отображается предупреждение.

Задача	EAC	Командная консоль Exchange	Статья	Comments
Экспорт существующего сертификата или запроса сертификата с сервера Exchange	**Серверов**>**Сертификаты**> Выберите сервер>, выберите значок Сертификат >**Дополнительные параметры**•••>**Экспорт сертификата Exchange**	**Export-ExchangeCertificate**	Экспорт сертификата с сервера Exchange	Вы можете экспортировать только действительные (неиспользовавшиеся) сертификаты, если свойство **PrivateKeyExportable** имеет значение `True`. Ожидающие запросы сертификата можно экспортировать только в командной консоли Exchange. Вы не можете импортировать экспортированный ожидающий запрос сертификата.
Импорт (установка) сертификата на сервер Exchange	**Серверов**>**Сертификаты**> Выберите значок **Дополнительные параметры** сервера >••• >**Импорт сертификата Exchange**	**Import-ExchangeCertificate**	Import or install a certificate on an Exchange server	Импортируйте сертификат, экспортированный с другого сервера.

Задача	EAC	Командная консоль Exchange	Статья	Comments
Просмотр существующих сертификатов или запросов сертификатов на сервере Exchange или просмотр сведений о сертификате или запросе сертификата	**Серверов** > **Сертификаты** > выберите сервер Для получения сведений о конкретном сертификате или запросе сертификата выберите элемент из списка и нажмите кнопку **Изменить**.	**Get-ExchangeCertificate**	н/д	Некоторые свойства сертификата отображаются в области сведений в Центре администрирования Exchange, когда вы выбираете сертификат или запрос сертификата из списка. Некоторые свойства сертификата не отображаются в стандартном представлении в командной консоли Exchange. Чтобы просмотреть их, необходимо указать имя свойства (точное или с использованием подстановочных знаков) с помощью командлетов **Format-Table** или **Format-List**. Дополнительные сведения см. в разделе Get-ExchangeCertificate.

Создание запроса на сертификат Exchange Server для центра сертификации

Статья • 04.04.2023

Создание запроса на сертификат — это первый шаг при установке нового сертификата на сервер Exchange Server для настройки шифрования TLS для одной или нескольких служб Exchange. Такой запрос позволяет получить сертификат из центра сертификации (ЦС). Процедуры одинаковы для получения сертификатов из внутреннего ЦС (например, служб сертификатов Active Directory) или из коммерческого ЦС. После создания запроса на сертификат вы отправляете результат в центр сертификации, а последний использует эти сведения для выдачи фактического сертификата, который можно установить позже.

Запросы на сертификаты можно создавать в Центре администрирования Exchange (EAC) или в командной консоли Exchange. Мастер **создания сертификатов Exchange** в EAC может помочь в выборе имен узлов, необходимых в сертификате.

Что нужно знать перед началом работы

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Дополнительные сведения о необходимых разрешениях см. в записи "Безопасность служб клиентского доступа" статьи Разрешения для клиентов и мобильных устройств .
- Предполагаемое время выполнения: 5 минут на каждый новый запрос. Однако требуется больше времени, прежде чем запрос приведет к выдаче сертификата. Дополнительные сведения см. в разделе Дальнейшие действия.
- Следует тщательно выбрать тип сертификата, который вам требуется, и имена узлов, которые необходимо в нем указать. Дополнительные сведения см. в статье Цифровые сертификаты и шифрование в Exchange Server.
- Всегда проверяйте требования центра сертификации к запросам на сертификаты. Exchange создает файл запроса PKCS #10 (REQ- файл), который использует кодировку Base64 (по умолчанию) или Distinguished Encoding Rules (DER) с открытым ключом RSA 1024, 2048 (по умолчанию) или 4096 битами. Параметры кодирования и открытого ключа доступны только в командной

консоли Exchange. Дополнительные сведения см. в статье New-ExchangeCertificate.

- В EAC необходимо сохранить файл запроса сертификата по UNC-пути (`\\<Server>\<Share>\` или `\\<LocalServerName>\c$\`). В командной консоли Exchange вы можете указать локальный путь.
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Дополнительные сведения о сочетаниях клавиш, которые могут применяться к процедурам, описанным в этой статье, см. в разделе Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование Центра администрирования Exchange для создания нового запроса на сертификат

> **Примечание**
>
> Запрос сертификата ECP не рекомендуется использовать в Exchange 2019 CU12 и более поздних версий, а также в Exchange 2016 с накопительным пакетом обновления 23 (CU23) и более поздних версий.

1. Откройте EAC и перейдите в раздел **Сертификаты серверов**>.
2. В раскрывающемся списке **Выбор сервера** выберите сервер Exchange Server, на котором требуется установить сертификат, а затем щелкните **Добавить**+

Запустится мастер **Создание сертификата Exchange**.

3. На странице **Этот мастер создаст новый сертификат или файл запроса сертификата** , убедитесь, что выбран параметр **Создать запрос на сертификат из центра сертификации** , а затем нажмите кнопку **Далее**.

> ⓘ **Примечание**
>
> Сведения о создании самозаверяющего сертификата см. в статье **Создание самозаверяющего сертификата Exchange Server**.

4. На странице **Понятное имя этого сертификата** введите описательное имя сертификата и нажмите кнопку **Далее**.

5. На странице **Запрос группового сертификата** выберите одно из следующего:

   - **Если требуется сертификат с подстановочными знаками**: выберите **Запросить сертификат с подстановочным знаком** и введите подстановочный знак (*) и домен в поле **Корневой домен** , например *.contoso.com или *.eu.contoso.com. По завершении нажмите кнопку **Далее**.
   - **Если требуется сертификат альтернативного имени субъекта (SAN):** не выбирайте параметры на этой странице и нажмите кнопку **Далее**.
   - **Если требуется сертификат для одного узла**: не выбирайте параметры на этой странице и нажмите кнопку **Далее**.

6. На странице **Запрос сертификата в хранилище на этом сервере** выберите **Обзор** и выберите сервер Exchange Server, на котором вы хотите сохранить запрос сертификата (где требуется установить сертификат). Затем нажмите **кнопки ОК** и **Далее**.

> ⓘ **Примечание**
>
> Шаги 7 и 8 применимы только к запросу на сертификат SAN или сертификат для одного узла. Если вы выбрали вариант **Запрос группового сертификата**, переходите к шагу 9.

Откроется страница **Укажите домены, которые нужно включить в сертификат** . Эта страница по сути представляет собой лист, на котором можно определить внутренние и внешние имена узлов, необходимые в сертификате для следующих служб Exchange:

- Outlook в Интернете
- Формирование автономной адресной книги (OAB)
- веб-службы Exchange
- Exchange ActiveSync
- Автообнаружение

- POP
- IMAP
- Мобильный Outlook

7. Введите значение для каждой службы в зависимости от расположения (внутренней или внешней). Затем мастер определяет имена узлов, необходимые в сертификате, и сведения отображаются на следующей странице.

8. Если вы хотите изменить значение службы, выберите **Изменить** (✎ и введите значение имени узла, которое вы хотите использовать (или удалите значение). По завершении нажмите кнопку **Далее**.

   > ⓘ **Примечание**
   >
   > Если вы уже определили необходимые имена узлов, вам не нужно заполнять поля на этой странице. Вместо этого нажмите кнопку **Далее** , чтобы вручную ввести имена узлов на следующей странице.

В **зависимости от выбранных значений на странице сертификата будут включены следующие домены** . На этой странице перечислены имена узлов, которые будут включены в запрос сертификата. Имя узла, используемое в поле **Тема** сертификата, выделено полужирным шрифтом, что трудно увидеть, если выбрано это имя узла.

9. Проверьте записи имени узла, необходимые в сертификате, сославшись на выбранные на предыдущей странице.

   Если вы не хотите рассматривать этот список имен узлов для включения в запрос на сертификат, перейдите к шагу 10.

10. Проигнорируйте значения с последней страницы и добавьте, измените или удалите значения имени узла, выполнив следующие действия: а. **Если вам нужен сертификат SAN**: чтобы выбрать имя узла для поля **"Субъект** " сертификата, выберите значение и выберите **Задать в качестве общего имени** (флажок). После этого значение должно быть выделено полужирным шрифтом. Б. **Если требуется сертификат для одного имени узла**: выберите другие значения по одному и нажмите **кнопку Удалить** (━

    > ⓘ **Примечание**

Вы не можете удалить полужирное значение имени узла, которое будет использоваться для поля **Тема** сертификата. Сначала необходимо выбрать или добавить другое имя узла, а затем установите флажок **Задать как общее имя** . Изменения, внесенные на этой странице, могут быть потеряны, если нажать кнопку **Назад** .

11. На странице **Укажите сведения об организации** введите следующую информацию:

- **Название организации**
- **Название отдела**
- **Город или населенный пункт**
- **Область, республика, край, округ**
- **Название страны или региона**

> ⓘ **Примечание**
>
> Эти значения X.500 включены в поле **Тема** сертификата. Хотя для продолжения работы в каждом поле требуется значение, ЦС может не заботиться об определенных полях (например, **название отдела**), в то время как другие поля важны (например, **название страны или региона** и **название организации**). Установите флажок **Требования к субъекту** вашего ЦС.

12. По завершении нажмите кнопку **Далее**.

13. На странице **Сохранить запрос сертификата в следующий файл** введите UNC-путь и имя файла для запроса сертификата, например `\\FileServer01\Data\ExchCertRequest.req`. По завершении нажмите кнопку **Готово**.

После этого запрос сертификата появится в списке сертификатов Exchange со статусом **Ожидает**. Дополнительные сведения о следующих шагах см. в разделе Дальнейшие действия .

Создание запроса на сертификат с помощью командной консоли Exchange

Чтобы создать новый запрос для сертификата с подстановочными знаками, сертификата SAN или сертификата для одного узла, используйте следующий синтаксис:

- Если необходимо отправить *содержимое* файла запроса сертификата в ЦС, используйте следующий синтаксис для создания файла запроса в кодировке Base64:

```
PowerShell

$txtrequest = New-ExchangeCertificate -PrivateKeyExportable $True -
GenerateRequest [-FriendlyName <DescriptiveName>] -SubjectName C=
<CountryOrRegion>[,S=<StateOrProvince>,L=<LocalityOrCity>,O=
<Organization>,OU=<Department>],CN=<HostNameOrFQDN> [-DomainName
<Host1>,<Host2>...] [-KeySize <1024 | 2048 | 4096>] [-Server
<ServerIdentity>]
[System.IO.File]::WriteAllBytes('<FilePathOrUNCPath>\<FileName>.req',
[System.Text.Encoding]::Unicode.GetBytes($txtrequest))
```

- Если необходимо отправить *файл запроса сертификата* в ЦС, используйте следующий синтаксис для создания файла запроса в кодировке DER:

```
PowerShell

$binrequest = New-ExchangeCertificate -PrivateKeyExportable $True -
GenerateRequest -BinaryEncoded [-FriendlyName <DescriptiveName>] -
SubjectName C=<CountryOrRegion>[,S=<StateOrProvince>,L=
<LocalityOrCity>,O=<Organization>,OU=<Department>],CN=<HostNameOrFQDN>
[-DomainName <Host1>,<Host2>...] [-KeySize <1024 | 2048 | 4096>] [-
Server <ServerIdentity>]
[System.IO.File]::WriteAllBytes('<FilePathOrUNCPath>\<FileName>.pfx',
$binrequest.FileData)
```

> ⓘ **Примечание**
>
> Единственной обязательной частью значения параметра X.500 *SubjectName* (поле **Subject** сертификата) для выполнения команды является `CN=<HostNameOrFQDN>`. Но всегда следует включать `C=<CountryOrRegion>` значение. В противном случае вы не сможете обновить сертификат. Установите флажок **Требования к субъекту** вашего ЦС. Если параметр *KeySize* не используется, запрос на сертификат содержит 2048-разрядный открытый ключ RSA. Если параметр *Server* не используется, команда выполняется на локальном сервере Exchange Server.

Дополнительные сведения о синтаксисе и параметрах см. в разделе New-ExchangeCertificate.

Запрос на сертификат с подстановочными знаками

В этих примерах создаются файлы запросов на сертификат для сертификатов с подстановочными знаками со следующими свойствами:

- **SubjectName**: *.contoso.com в США, для которого требуется значение `C=US,CN=*.contoso.com`.
- **RequestFile**: `\\FileServer01\Data\Contoso Wildcard Cert.<cer or pfx>`
- **FriendlyName**: Contoso.com сертификат с подстановочными знаками

Чтобы создать файл запроса в кодировке Base64 для сертификата с подстановочными знаками, выполните следующую команду:

PowerShell

```
$txtrequest = New-ExchangeCertificate -PrivateKeyExportable $True -
GenerateRequest -FriendlyName "Contoso.com Wildcard Cert" -SubjectName
"C=US,CN=*.contoso.com"
[System.IO.File]::WriteAllBytes('\\FileServer01\Data\Contoso Wildcard
Cert.req', [System.Text.Encoding]::Unicode.GetBytes($txtrequest))
```

Чтобы создать файл запроса в кодировке DER для сертификата с подстановочными знаками, выполните следующую команду:

PowerShell

```
$binrequest = New-ExchangeCertificate -PrivateKeyExportable $True -
GenerateRequest -BinaryEncoded -FriendlyName "Contoso.com Wildcard Cert" -
SubjectName "C=US,CN=*.contoso.com"
[System.IO.File]::WriteAllBytes('\\FileServer01\Data\Contoso Wildcard
Cert.pfx', $binrequest.FileData)
```

Запрос сертификата SAN

В этих примерах создаются файлы запросов сертификатов для сертификатов SAN со следующими свойствами:

- **SubjectName**: mail.contoso.com в США, для которого требуется значение `C=US,CN=mail.contoso.com`. Это значение CN автоматически включается в параметр *DomainName* (поле "**Альтернативное имя субъекта** ").
- Значения полей **другого альтернативного имени субъекта** :
  - autodiscover.contoso.com
  - legacy.contoso.com
  - mail.contoso.net
  - autodiscover.contoso.net
  - legacy.contoso.net

- **RequestFile**: `\\FileServer01\Data\Contoso SAN Cert.<cer or pfx>`
- **FriendlyName**: Contoso.com сертификат SAN
- **DomainName**: список доменов, разделенных запятыми

Чтобы создать файл запроса в кодировке Base64 для сертификата SAN, выполните следующую команду:

PowerShell

```
$txtrequest = New-ExchangeCertificate -PrivateKeyExportable $True -
GenerateRequest -FriendlyName "Contoso.com SAN Cert" -SubjectName
"C=US,CN=mail.contoso.com" -DomainName
autodiscover.contoso.com,legacy.contoso.com,mail.contoso.net,autodiscover.co
ntoso.net,legacy.contoso.net
[System.IO.File]::WriteAllBytes('\\FileServer01\Data\Contoso SAN Cert.req',
[System.Text.Encoding]::Unicode.GetBytes($txtrequest))
```

Чтобы создать файл запроса в кодировке DER для сертификата SAN, выполните следующую команду:

PowerShell

```
$binrequest = New-ExchangeCertificate -PrivateKeyExportable $True -
GenerateRequest -BinaryEncoded -FriendlyName "Contoso.com SAN Cert" -
SubjectName "C=US,CN=mail.contoso.com" -DomainName
autodiscover.contoso.com,legacy.contoso.com,mail.contoso.net,autodiscover.co
ntoso.net,legacy.contoso.net
[System.IO.File]::WriteAllBytes('\\FileServer01\Data\Contoso SAN Cert.pfx',
$binrequest.FileData)
```

Запрос на сертификат с одним субъектом

В этих примерах создаются файлы запросов сертификатов для сертификатов с одним субъектом со следующими свойствами:

- **SubjectName**: mail.contoso.com в США, для которого требуется значение `C=US,CN=mail.contoso.com`.
- **RequestFile**: `\\FileServer01\Data\Mail.contoso.com Cert.<cer or pfx>`
- **FriendlyName**: Mail.contoso.com Cert

Чтобы создать файл запроса в кодировке Base64 для сертификата с одним субъектом, выполните следующую команду:

PowerShell

```
$txtrequest = New-ExchangeCertificate -PrivateKeyExportable $True -
GenerateRequest -FriendlyName "Mail.contoso.com Cert" -SubjectName
"C=US,CN=mail.contoso.com"
[System.IO.File]::WriteAllBytes('\\FileServer01\Data\Mail.contoso.com
Cert.req', [System.Text.Encoding]::Unicode.GetBytes($txtrequest))
```

Чтобы создать файл запроса в кодировке DER для сертификата с одним субъектом, выполните следующую команду:

PowerShell

```
$binrequest = New-ExchangeCertificate -PrivateKeyExportable $True -
GenerateRequest -BinaryEncoded -FriendlyName "Mail.contoso.com Cert" -
SubjectName "C=US,CN=mail.contoso.com"
[System.IO.File]::WriteAllBytes('\\FileServer01\Data\Mail.contoso.com
Cert.pfx', $binrequest.FileData)
```

Как узнать, что эти команды работали?

Чтобы убедиться, что вы успешно создали новый запрос на сертификат, выполните одно из следующих действий:

- В центре администрирования Exchange в разделе **Сертификаты серверов**> проверьте, выбран ли сервер, на котором хранится запрос сертификата. Запрос должен находиться в списке сертификатов со значением параметра **Status** , заданным как **Ожидание запроса**.
- В командной консоли Exchange на сервере, где хранится запрос сертификата, выполните следующую команду:

  PowerShell

  ```
  Get-ExchangeCertificate | where {$_.Status -eq "PendingRequest" -and
  $_.IsSelfSigned -eq $false} | Format-List
  FriendlyName,Subject,CertificateDomains,Thumbprint
  ```

Дальнейшие действия

Содержимое файла запроса сертификата в кодировке Base64 выглядит так, как описано ниже.

text

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEBjCCAu4CAQAwYzEWMBQGA1UEAwwNKi5jb250b3NvLmNvbTELMAkGA1UECwwC
SVQxEDAOBgNVBAoMB0NvbnRvc28xEDAOBgNVBAcMB1NlYXR0bGUxCzAJBgNVBAgM
AldBMQswCQYDVQQGEwJVUzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ANZFK6JxcQMEBitJcEC82vCvr6251o28CMmrpIkl7Z0MnkCrU+BMTLBuZnIgaLvb
jlzORvH6DP/dbyR8gQEAHVrXVWdr3AJIRbqQXWwN++BM5b2O6lIrA8w41XwGNu6r
dtddi+POf8UYwot7PXw6wDsbKaTs1ePVK/0XdemdJCFIXNfCT8LY4p/KryQAyquo
XDa+Acbx7TRxG2kXNAxgPGve+mvyCyizbugXAJIz4nugJ2k/X1kGYDc7f/b80tCv
bPTcGCr09ScsbKmsQcqJ7UxiX2tScpO5AQxNxJHGL+bA6+96FBjPnFZaqPbFgI74
N6hmZdSEDgQlaGfLEGjZBGMCAwEAAaCCAVwwGgYKKwYBBAGCNw0CAzEMFgo2LjEu
NzYwMS4yMEwGCSqGSIb3DQEJDjE/MD0wDgYDVR0PAQH/BAQDAgWgMAwGA1UdEwEB
/wQCMAAwHQYDVR0OBBYEFNRw1o74zcuGyky33rl7WChgdQrlMHIGCisGAQQBgjcN
AgIxZDBiAgEBHloATQBpAGMAcgBvAHMAbwBmAHQAIABSAFMAQQAgAFMAQwBoAGEA
bgBuAGUAbAAgAEMAcgB5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkA
ZABlAHIDAQAwfAYJKwYBBAGCNxUUMW8wbQIBBQwrRVhIUi0zMjQ4LkVYSFItMzI0
OGRvbS5leHRlc3QubWljcm9zb2Z0LmNvbQwXRVhIUi0zMjQ4RE9NXEVYSFItMzI0
OCQMIk1pY3Jvc29mdC5FeGNoYW5nZS5TZXJ2aWNlSG9zdC5leGUwDQYJKoZIhvcN
AQEFBQADggEBAL63qVj1m2mBz53+nilnlFweOlcltXoxaF28+Kf0hrJVbH5a2Jme
tS0iKU8YXU3mZ3NnWco+5ea024f9awMIzg4z/heE5yEUFf9UtwRGSOc84r2QexPa
zT/rveTTcbliKU0EFhporl3C2uuBCdAewyLj+/k0hABH3djnmMONG6NyC5f+wMun
kkH5naiSLdsTYbq8jkWYuSqL0qdhtmauqWeAPpA0hKDkQk5eDWpOGx3mgxiaQumo
Rqw6dmQ+o8TC+lE3Tvgdfv47A84X8H7Y9h8liS4h0OfbsgEQb8LcM0YHD6yvPgcD
JCmt8A7JFHF9u6mghjiKlXaZ/i+2l10Wsu8=
-----END NEW CERTIFICATE REQUEST-----
```

Вам нужно отправить эту информацию в центр сертификации. Способ отправки зависит от ЦС, но обычно содержимое файла отправляется в сообщении электронной почты или в форме запроса сертификата на веб-сайте ЦС.

Если центр сертификации требует, чтобы запрос на сертификат был в двоичном формате в кодировке DER (если использовался командлет **New-ExchangeCertificate** с параметром *BinaryEncoded*), в центр сертификации обычно требуется отправить сам файл запроса на сертификат.

После получения сертификата от центра сертификации необходимо завершить ожидающий запрос на сертификат. Дополнительные сведения см. в разделе Выполнение ожидающего запроса на сертификат Exchange Server.

Выполнение ожидающего запроса на сертификат Exchange Server

Статья • 24.03.2023

Выполнение ожидающего запроса сертификата (также известного как запрос подписи сертификата или CSR) — это следующий шаг при настройке шифрования TLS в Exchange Server. Получив сертификат из центра сертификации (ЦС), установите его на сервере Exchange, чтобы выполнить ожидающий запрос сертификата.

Вы можете выполнить ожидающий запрос сертификата в Центре администрирования Exchange (EAC) или командной консоли Exchange. Запросы новых сертификатов и запросы на обновление сертификатов выполняются одинаково. Процедуры также одинаковы как для сертификатов, выданных внутренним (например, службами сертификации Active Directory) и коммерческим ЦС.

ЦС может прислать вам один или несколько файлов сертификатов следующих типов:

- **Файлы сертификатов PKCS #12**. Это двоичные файлы сертификатов, которые имеют расширения CER, CRT, DER, P12 или PFX и требуют пароля, если файл содержит закрытый ключ или цепочку доверия. ЦС может выдать вам для установки только один двоичный файл сертификата (защищенный паролем) или несколько корневых или промежуточных двоичных файлов сертификатов, которые также необходимо установить.
- **Файлы сертификатов PKCS #7**. Это текстовые файлы сертификатов с расширениями P7B или P7C. Эти файлы содержат текст: `-----BEGIN CERTIFICATE-----` и `-----END CERTIFICATE-----` или `-----BEGIN PKCS7-----` и `-----END PKCS7-----`. Если вместе с двоичным файлом сертификата ЦС присылает вам файл цепочки сертификатов, его также необходимо установить.

> ⓘ **Примечание**
>
> Задачи управления сертификатами удаляются из EAC для Exchange Server 2016 CU23 и Exchange Server 2019 CU12. Используйте процедуру командной консоли Exchange для экспорта или импорта сертификата из этих версий.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Процедуры, описанные в этом разделе, требуют создания нового запроса сертификата на сервере Exchange Server, отправки запроса сертификата в ЦС и получения сертификата из ЦС. Дополнительные сведения см. в статье Создание запроса на сертификат Exchange Server для центра сертификации.
- В EAC необходимо получить файл сертификата из UNC-пути (`\\<Server>\<Share>` или `\\<LocalServerName>\c$\`). В командной консоли Exchange вы можете использовать локальный путь к файлу.
- Если вы обновите или замените сертификат, который был выпущен центром сертификации на подписанном пограничном транспортном сервере, вам нужно будет удалить старый сертификат, а затем удалить и заново создать пограничную подписку. Дополнительные сведения см. в разделе Процесс пограничной подписки.
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Безопасность служб клиентского доступа" в разделе Разрешения клиентов и мобильных устройств .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Выполнить ожидающий запрос сертификата с помощью Центра администрирования Exchange

1. Откройте EAC и перейдите в раздел **Сертификаты серверов**>.

2. В списке **Выберите сервер** выберите сервер Exchange, где находится ожидающий запрос сертификата.

3. Ожидающий запрос сертификата имеет следующие свойства:

   - В списке сертификатов в поле **Статус** указано значение **Ожидающий запрос**.

   - При выборе запроса сертификата из списка в области сведений появляется ссылка **Выполнить**.

   Выберите ожидающий запрос сертификата, который требуется выполнить, и нажмите ссылку **Выполнить** в области сведений.

4. На открывшейся странице **Выполнить ожидающий запрос** в поле **Файл для импорта** введите UNC-путь и имя файла сертификата. Например, `\\FileServer01\Data\ContosoCert.cer`. После этого нажмите кнопку **OK**.

Запрос сертификата становится сертификатом в списке сертификатов Exchange со значением **СостояниеДопустимо**. Дальнейшие действия см. в разделе Дальнейшие действия.

Выполнить ожидающий запрос сертификата с помощью командной консоли Exchange

Чтобы выполнить ожидающий запрос на сертификат, используйте следующий синтаксис:

PowerShell

```
Import-ExchangeCertificate -FileData
([System.IO.File]::ReadAllBytes('<FilePathOrUNCPath>')) [-Password
(ConvertTo-SecureString -String '<Password> ' -AsPlainText -Force)] [-
PrivateKeyExportable <$true | $false>] [-Server <ServerIdentity>]
```

Этот синтаксис используется со следующими типами файлов сертификатов:

- Двоичные файлы сертификатов (файлы PKCS #12 с расширениями CER, CRT, .der, .p12 или PFX).
- Цепочка файлов сертификатов (текстовые файлы PKCS No 7 с расширениями P7B или P7C).

В этом примере импортируется двоичный файл `\\FileServer01\Data\Contoso Cert.cer` сертификата, защищенный паролем P@ssw0rd1 на локальном сервере

Exchange Server.

PowerShell

```
Import-ExchangeCertificate -FileData
([System.IO.File]::ReadAllBytes('\\FileServer01\Data\Contoso Cert.cer')) -
Password (ConvertTo-SecureString -String 'P@ssw0rd1' -AsPlainText -Force)
```

В этом примере импортируется текстовый файл `\\FileServer01\Data\Chain of Certificates.p7b` сертификата на локальный сервер Exchange Server.

PowerShell

```
Import-ExchangeCertificate -FileData
([System.IO.File]::ReadAllBytes('\\FileServer01\Data\Chain of
Certificates.p7b'))
```

Примечания:

- Параметр *FileData* принимает локальные пути, если файл сертификата находится на сервере Exchange Server, где выполняется команда, и это тот же сервер, на котором требуется импортировать сертификат. В противном случае используйте UNC-путь.
- Если вы хотите экспортировать сертификат с сервера, на который вы его импортируете, необходимо использовать параметр *PrivateKeyExportable* со значением `$true`.
- Дополнительные сведения см. в статье Import-ExchangeCertificate.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно выполнили запрос сертификата и установили сертификат на сервере Exchange, выполните одно из следующих действий:

- В центре администрирования Exchange в разделе **Сертификаты серверов**> убедитесь, что выбран сервер, на котором установлен сертификат. В списке серверов убедитесь, что сертификат имеет **статусДействительный**.

- В командной консоли Exchange на сервере, где вы установили сертификат, выполните следующую команду и убедитесь, что сертификат указан в списке:

  PowerShell

  ```
  Get-ExchangeCertificate | where {$_.Status -eq "Valid" -and
  $_.IsSelfSigned -eq $false} | Format-List
  ```

```
FriendlyName,Subject,CertificateDomains,Thumbprint
```

Дальнейшие действия

После завершения ожидающего запроса на сертификат путем установки сертификата на сервере необходимо назначить сертификат одной или нескольким службам Exchange, прежде чем сервер Exchange сможет использовать сертификат для шифрования. Дополнительные сведения см. в статье Назначение сертификатов службам Exchange.

Назначение сертификатов службам Exchange Server

Статья • 04.04.2023

После установки сертификата на сервере Exchange Server необходимо назначить сертификат одной или нескольким службам Exchange, прежде чем сервер Exchange сможет использовать сертификат для шифрования. Вы можете назначать сертификаты службам через Центр администрирования Exchange (EAC) или командную консоль Exchange. Назначение сертификата службе невозможно удалить. Если вы больше не хотите использовать сертификат для определенной службы, назначьте ей другой сертификат и удалите ненужный.

В следующей таблице описаны доступные службы Exchange.

Служба	**Использует**
Службы IIS	Шифрование TLS для внутренних и внешних клиентских подключений, использующих HTTP. Вот некоторые из них: Автообнаружение Exchange ActiveSync Центр администрирования Exchange веб-службы Exchange Распространение автономных адресных книг Мобильный Outlook (протокол RPC через HTTP) MAPI Outlook через HTTP Outlook в Интернете
IMAP	Шифрование TLS для клиентских подключений по протоколу IMAP4. Не назначайте групповой сертификат службе IMAP4. Используйте командлет **Set-ImapSettings** для настройки полного доменного имени (FQDN), с помощью которого клиенты подключаются к службе IMAP4.
POP	Шифрование TLS для клиентских подключений по протоколу POP3. Не назначайте групповой сертификат службе POP3. Используйте командлет **Set-PopSettings** для настройки полного доменного имени (FQDN), с помощью которого клиенты подключаются к службе POP3.
SMTP	Шифрование TLS для внешних подключений к клиентам и серверам по протоколу SMTP Проверка подлинности Mutual TLS между Exchange и другими серверами обмена сообщениями. При назначении сертификата SMTP вам будет предложено заменить самозаверяющий сертификат Exchange по умолчанию, используемый для шифрования smtp-связи между внутренними серверами Exchange. Обычно заменять сертификат SMTP по умолчанию не нужно.

Служба	Использует
Единая система обмена сообщениями	Шифрование TLS для клиентских подключений к серверной службе единой системы обмена сообщениями на серверах почтовых ящиков Exchange 2016. Вы можете назначить сертификат службе единой системы обмена сообщениями, только если используется режим запуска TLS или "Двойной". Если используется режим запуска по умолчанию TCP, вы не можете назначить сертификат этой службе. (**Примечание**. UM недоступна в Exchange 2019. Дополнительные сведения см. в статье Configure the Startup Mode on a Mailbox Server.
Маршрутизатор звонков единой системы обмена сообщениями (UMCallRouter)	Шифрование TLS для клиентских подключений к службе маршрутизатора вызовов единой системы обмена сообщениями в службах клиентского доступа на серверах почтовых ящиков Exchange 2016. Вы можете назначить сертификат службе маршрутизатора звонков единой системы обмена сообщениями, только если используется режим запуска TLS или "Двойной". Если используется режим запуска по умолчанию TCP, вы не можете назначить сертификат этой службе. (**Примечание**. UM недоступна в Exchange 2019. Дополнительные сведения см. в статье Configure the Startup Mode on a Client Access Server.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- После выполнения процедур, описанных в этом разделе, может потребоваться перезапустить службы IIS. В некоторых сценариях Exchange может продолжать использовать предыдущий сертификат для шифрования и расшифровки файла cookie, который используется для проверки подлинности Outlook в Интернете (ранее — Outlook Web App). Рекомендуется перезапускать СЛУЖБЫ IIS в средах, использующих балансировку нагрузки уровня 4.
- Если вы обновите или замените сертификат, который был выпущен центром сертификации на подписанном пограничном транспортном сервере, вам нужно будет удалить старый сертификат, а затем удалить и заново создать пограничную подписку. Дополнительные сведения см. в разделе Процесс пограничной подписки.
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи

"Безопасность служб клиентского доступа" в разделе Разрешения клиентов и мобильных устройств .

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Назначить сертификат службам Exchange с помощью Центра администрирования Exchange

1. Откройте EAC и перейдите в раздел **Сертификаты серверов**>.
2. В списке **Выберите сервер** выберите сервер Exchange, где находится сертификат.
3. Выберите сертификат, который нужно настроить, и нажмите кнопку **Изменить** Сертификат должен иметь **статусДействительный**.
4. Выберите службы на вкладке **Службы** в разделе **Укажите службы, которым вы хотите назначить этот сертификат**. Обратите внимание, что вы можете только добавлять службы, но не удалять их. По завершении нажмите кнопку **Сохранить**.

Назначить сертификат службам Exchange с помощью командной консоли Exchange

Чтобы назначить сертификат службам Exchange, используйте следующий синтаксис:

PowerShell

```
Enable-ExchangeCertificate -Thumbprint <Thumbprint> -Services <Service1>,
<Service2>... [-Server <ServerIdentity>]
```

В этом примере сертификат, имеющий значение `434AC224C8459924B26521298CE8834C514856AB` отпечатка, назначается службам POP, IMAP, IIS и SMTP.

PowerShell

```
Enable-ExchangeCertificate -Thumbprint
434AC224C8459924B26521298CE8834C514856AB -Services POP,IMAP,IIS,SMTP
```

Значение отпечатка сертификата можно найти с помощью командлета **Get-ExchangeCertificate**.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно назначили сертификат одной или нескольким службам Exchange, выполните одно из следующих действий:

- В центре администрирования Exchange в разделе **Сертификаты серверов**> убедитесь, что выбран сервер, на котором установлен сертификат. Выберите сертификат и убедитесь, что свойство **Назначено службам** в области сведений содержит выбранные службы.
- В командной консоли Exchange на сервере, где вы установили сертификат, выполните следующую команду, чтобы проверить службы Exchange для сертификата:

  PowerShell

  ```
  Get-ExchangeCertificate | Format-List
  FriendlyName,Subject,CertificateDomains,Thumbprint,Services
  ```

Создание самозаверяющего сертификата Exchange Server

Статья • 04.04.2023

При установке Exchange Server на сервер автоматически устанавливается самозаверяющий сертификат, созданный и подписанный самим сервером Exchange Server. Но вы также можете создать и использовать дополнительные самозаверяющие сертификаты.

Вы можете создавать самозаверяющие сертификаты в Центре администрирования Exchange (EAC) или командной консоли Exchange.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Самозаверяющие сертификаты Exchange хорошо работают для шифрования обмена данными между внутренними серверами Exchange, но не так хорошо для шифрования внешних подключений, так как клиенты, серверы и службы не доверяют автоматически самозаверяющим сертификатам Exchange. Сведения о создании запроса на сертификат (также известного как запрос подписи сертификата или CSR) для коммерческого центра сертификации, которому автоматически доверяют все клиенты, серверы и службы, см. в статье Создание Exchange Server запроса на сертификат для центра сертификации.
- При создании самозаверяющего сертификата с помощью командлета **New-ExchangeCertificate** его можно назначить службам Exchange во время создания сертификата. Дополнительные сведения о службах Exchange см. в статье Назначение сертификатов Exchange Server службам.
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Безопасность служб клиентского доступа" в разделе Разрешения клиентов и мобильных устройств .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Создать самозаверяющий сертификат Exchange с помощью Центра администрирования Exchange

1. Откройте EAC и перейдите в раздел **Сертификаты серверов**>.
2. В списке **Выбор сервера** выберите сервер Exchange Server, на котором требуется установить сертификат, и нажмите кнопку **Добавить**➕
3. Запустится мастер **Создание сертификата Exchange**. На странице **Этот мастер создаст новый сертификат или файл запроса на сертификат** выберите **Создать самозаверяющий сертификат** и нажмите кнопку **Далее**.

   Примечание: Сведения о создании нового запроса на сертификат для центра сертификации см. в статье Создание Exchange Server запроса на сертификат для центра сертификации.
4. На странице **Понятное имя для этого сертификата** введите понятное имя сертификата и нажмите кнопку **Далее**.
5. На странице **Укажите серверы, к которым требуется применить этот сертификат, щелкните**➕

   На открывшейся странице **Выберите сервер** выберите сервер Exchange, на который необходимо установить сертификат, и нажмите **Добавить - >**. Повторите этот шаг нужное количество раз. Завершив выбор серверов, нажмите кнопку **ОК**.

   По завершении нажмите кнопку **Далее**.
6. Страница **Укажите домены, которые вы хотите включить в свой сертификат** — это лист, на котором можно определить необходимые имена внутренних и внешних узлов для следующих служб Exchange:

   - Outlook в Интернете

- Формирование автономной адресной книги (OAB)
- веб-службы Exchange
- Exchange ActiveSync
- Автообнаружение
- POP
- IMAP
- Мобильный Outlook

  Если вы введете значения для каждой службы на основе расположения (внутренней или внешней), мастер определит необходимые имена узлов, и они отобразятся на следующей странице. Чтобы изменить значение службы, нажмите кнопку **Изменить** (и введите значение имени узла, которое вы хотите использовать (или удалите значение). По завершении нажмите кнопку **Далее**.

  Если вы уже определили необходимые имена узлов, вам не нужно заполнять поля на этой странице. Вместо этого нажмите кнопку **Далее**, чтобы вручную ввести имена узлов на следующей странице.

7. **В зависимости от выбранных значений на странице сертификата будут включены следующие домены,** в котором перечислены имена узлов, которые будут включены в самозаверяющий сертификат. The host name that's used in the certificate's **Subject** field is bold, which can be hard to see if that host name is selected. You can verify the host name entries that are required in the certificate based on the selections that you made on the previous page. Or, you can ignore the values from the last page and add, edit, or remove host name values.

   - Если требуется сертификат SAN, укажите в поле **Subject** одно общее имя (CN). Чтобы выбрать имя узла для поля **Subject** сертификата, выберите значение и установите флажок **Задать как общее имя**. После этого значение должно быть выделено полужирным шрифтом.
   - Если требуется сертификат для одного имени узла, выберите другие значения по одному и нажмите кнопку **Удалить** (

     По завершении работы на этой странице нажмите кнопку **Готово**.

Примечания:

- Имя узла, выделенное полужирным шрифтом, будет использоваться для поля **Subject** сертификата, и его невозможно удалить. Сначала необходимо выбрать или добавить другое имя узла, а затем установить флажок **Задать как общее имя**.
- Если нажать кнопку **Назад**, изменения, внесенные на этой странице, могут быть потеряны.

Создать самозаверяющий сертификат Exchange с помощью командной консоли Exchange

Чтобы создать самозаверяющий сертификат Exchange, используйте следующий синтаксис:

PowerShell

```
New-ExchangeCertificate [-FriendlyName <DescriptiveName>] [-SubjectName [C=
<CountryOrRegion>,S=<StateOrProvince>,L=<LocalityOrCity>,O=
<Organization>,OU=<Department>],CN=<HostNameOrFQDN>]] [-DomainName <Host1>,
<Host2>...] [-Services <None | IIS | IMAP | POP | SMTP | UM | UMCallRouter>
[-PrivateKeyExportable < $true | $false>] [-Server <ServerIdentity>] -
[Force]
```

В этом примере создается самозаверяющий сертификат на локальном сервере Exchange со следующими свойствами:

- **Тема**: *<Имя_>сервера*. Например, при выполнении команды на сервере с именем Mailbox01 значение будет `Mailbox01` равно .
- **Альтернативные имена субъектов**: *<ServerName>*, <Полное доменное имя> сервера. Например, `Mailbox01, Mailbox01.contoso.com`.
- **Понятное имя**: Microsoft Exchange
- **Службы**: POP, IMAP, SMTP.

PowerShell

```
New-ExchangeCertificate
```

В этом примере создается самозаверяющий сертификат на локальном сервере Exchange со следующими свойствами:

- **Тема**: Exchange01, для которого требуется значение `CN=Exchange01`. Обратите внимание, что это значение автоматически включается в параметр

DomainName (поле **"Альтернативное имя субъекта "**).

- Дополнительные альтернативные имена субъекта:
  - mail.contoso.com
  - autodiscover.contoso.com
  - Exchange01.contoso.com
  - Exchange02.contoso.com
- **Службы**: SMTP, IIS
- **Понятное имя**: Сертификат Contoso Exchange
- Закрытый ключ можно экспортировать. То есть вы можете экспортировать сертификат с сервера и импортировать его на другие серверы.

PowerShell

```
New-ExchangeCertificate -FriendlyName "Contoso Exchange Certificate" -
SubjectName CN=Exchange01 -DomainName
mail.contoso.com,autodiscover.contoso.com,Exchange01.contoso.com,Exchange02.
contoso.com -Services SMTP,IIS -PrivateKeyExportable $true
```

Примечания:

- Единственной обязательной частью значения параметра X.500 *SubjectName* (поле **subject** сертификата) является `CN=<HostNameOrFQDN>`.
- Некоторые значения параметра *Services* приводят к появлению предупреждений или подтверждений. Дополнительные сведения см. в статье Назначение сертификатов Exchange Server службам.
- Дополнительные сведения см. в статье New-ExchangeCertificate.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно создали самозаверяющий сертификат Exchange, выполните любое из следующих действий:

- В центре администрирования Exchange в разделе **Сертификаты серверов**> убедитесь, что выбран сервер, на котором был создан самозаверяющий сертификат. Сертификат должен быть в списке сертификатов и иметь **статусДействительный**.

- В командной консоли Exchange на сервере, где вы создали самозаверяющий сертификат, выполните следующую команду и проверьте свойства:

  PowerShell

```
Get-ExchangeCertificate | where {$_.Status -eq "Valid" -and
$_.IsSelfSigned -eq $true} | Format-List
FriendlyName,Subject,CertificateDomains,Thumbprint,NotBefore,NotAfter
```

Продление сертификата Exchange Server

Статья • 24.03.2023

У каждого сертификата есть встроенный срок действия. В Exchange Server срок действия самозаверяющего сертификата по умолчанию, установленного на сервере Exchange Server, истекает через 5 лет после установки Exchange на сервере. Для обновления сертификатов Exchange можно использовать Центр администрирования Exchange (EAC) или командную консоль Exchange. Это относится к самозаверяющим сертификатам Exchange и сертификатам, выданным центром сертификации (ЦС).

> ⓘ **Примечание**
>
> Задачи управления сертификатами удаляются из EAC для Exchange Server 2016 CU23 и Exchange Server 2019 CU12. Используйте процедуру командной консоли Exchange для экспорта или импорта сертификата из этих версий.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Если сертификаты выданы ЦС, проверьте требования ЦС к запросам сертификатов. Exchange создает файл запроса PKCS #10 (.req) в кодировке Base64 (по умолчанию) или Distinguished Encoding Rules (DER) с открытым ключом RSA длиной 1024, 2048 (по умолчанию) или 4096 бит. Обратите внимание, что параметры кодирования и открытого ключа доступны только в командной консоли Exchange.
- Сертификат, выданный ЦС, нужно обновлять в выдавшем его ЦС. Если нужно изменить ЦС или возникла проблема при обновлении исходного сертификата, необходимо создать запрос нового сертификата (также известный как запрос подписи сертификата или CSR). Дополнительные сведения см. в статье Создание запроса на сертификат Exchange Server для центра сертификации.

- Если вы обновите или замените сертификат, который был выпущен центром сертификации на подписанном пограничном транспортном сервере, вам нужно будет удалить старый сертификат, а затем удалить и заново создать пограничную подписку. Дополнительные сведения см. в разделе Процесс пограничной подписки.

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Безопасность служб клиентского доступа" в разделе Разрешения клиентов и мобильных устройств .

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Обновление сертификата, выданного центром сертификации

Процедуры одинаковы для сертификатов, выданных внутренним (например, службами сертификации Active Directory) и коммерческим ЦС.

Чтобы обновить сертификат, выданный ЦС, создайте запрос на обновление сертификата и отправьте его в ЦС. Затем ЦС отправляет вам фактический файл сертификата, который необходимо установить на сервере Exchange Server. Почти аналогично выполняется запрос нового сертификата. Инструкции см. в разделе Выполнение ожидающего запроса на сертификат Exchange Server.

Создание запроса на обновление сертификата для центра сертификации с помощью Центра администрирования Exchange

1. Откройте EAC и перейдите в раздел **Сертификаты серверов**>.

2. В списке **Выберите сервер** выберите сервер Exchange с сертификатом, который требуется обновить.

3. В области сведений всех действительных сертификатов есть ссылка **Обновить**, которая отображается при выборе сертификата из списка. Выберите сертификат, который требуется обновить, и нажмите **Обновить** в области сведений.

4. На открывшейся странице **Обновление сертификата Exchange** в поле **Сохранить запрос сертификата в следующий файл** введите UNC-путь и имя файла нового запроса на обновление сертификата. Например, `\\FileServer01\Data\ContosoCertRenewal.req`. После этого нажмите кнопку **OK**.

После этого запрос сертификата появится в списке сертификатов Exchange со статусом **Ожидает**.

Создание запроса на обновление сертификата для центра сертификации с помощью командной консоли Exchange

Чтобы создать новый запрос на продление сертификата для центра сертификации, используйте следующий синтаксис:

- Если необходимо отправить *содержимое* файла запроса на продление сертификата в ЦС, используйте следующий синтаксис для создания файла запроса в кодировке Base64:

  PowerShell

  ```
  $txtrequest = Get-ExchangeCertificate -Thumbprint <Thumbprint> | New-ExchangeCertificate -GenerateRequest [-KeySize <1024 | 2048 | 4096>] [-Server <ServerIdentity>]
  [System.IO.File]::WriteAllBytes('<FilePathOrUNCPath>\<FileName>.req', [System.Text.Encoding]::Unicode.GetBytes($txtrequest))
  ```

- Если необходимо отправить *файл запроса на продление сертификата* в ЦС, используйте следующий синтаксис для создания файла запроса в кодировке DER:

  PowerShell

  ```
  $binrequest = Get-ExchangeCertificate -Thumbprint <Thumbprint> | New-ExchangeCertificate -GenerateRequest -BinaryEncoded [-KeySize <1024 | 2048 | 4096>] [-Server <ServerIdentity>]
  [System.IO.File]::WriteAllBytes('<FilePathOrUNCPath>\<FileName>.pfx', $binrequest.FileData)
  ```

Чтобы найти значение отпечатка сертификата, который требуется обновить, выполните следующую команду:

```
PowerShell

Get-ExchangeCertificate | where {$_.Status -eq "Valid" -and $_.IsSelfSigned -eq $false} | Format-List FriendlyName,Subject,CertificateDomains,Thumbprint,NotBefore,NotAfter
```

Подробные сведения о синтаксисе и параметрах см. в разделах Get-ExchangeCertificate и New-ExchangeCertificate.

Примечания:

- Если параметр *KeySize* не используется, запрос на сертификат содержит 2048-разрядный открытый ключ RSA.
- Если параметр *Server* не используется, команда выполняется на локальном сервере Exchange Server.

В этом примере создается запрос на продление сертификата в кодировке Base64 для существующего сертификата со значением `5DB9879E38E36BCB60B761E29794392B23D1C054` отпечатка :

```
PowerShell

$txtrequest = Get-ExchangeCertificate -Thumbprint 5DB9879E38E36BCB60B761E29794392B23D1C054 | New-ExchangeCertificate -GenerateRequest
[System.IO.File]::WriteAllBytes('\\FileServer01\Data\ContosoCertRenewal.req', [System.Text.Encoding]::Unicode.GetBytes($txtrequest))
```

В этом примере создается запрос на продление сертификата в кодировке DER (двоичный) для того же сертификата:

```
PowerShell

$binrequest = Get-ExchangeCertificate -Thumbprint <Thumbprint> | New-ExchangeCertificate -GenerateRequest -BinaryEncoded
[System.IO.File]::WriteAllBytes('\\FileServer01\Data\ContosoCertRenewal.pfx', $binrequest.FileData)
```

Как узнать, что вы успешно создали запрос на продление сертификата?

Чтобы убедиться, что вы успешно создали запрос на обновление сертификата для центра сертификации, выполните любое из следующих действий:

- В центре администрирования Exchange в разделе **Сертификаты серверов**> убедитесь, что выбран сервер, на котором хранится запрос сертификата. Запрос должен быть в списке сертификатов и иметь **статусОжидающий запрос**.

- В командной консоли Exchange на сервере, где хранится запрос сертификата, выполните следующую команду:

```
PowerShell

Get-ExchangeCertificate | where {$_.Status -eq "PendingRequest" -and
$_.IsSelfSigned -eq $false} | Format-List
FriendlyName,Subject,CertificateDomains,Thumbprint
```

Обновление самозаверяющего сертификата Exchange

Когда вы обновляете самозаверяющий сертификат Exchange, вы, по сути, создаете новый сертификат.

Обновление самозаверяющего сертификата Exchange с помощью Центра администрирования Exchange

1. Откройте EAC и перейдите в раздел **Сертификаты серверов**>.

2. В списке **Выберите сервер** выберите сервер Exchange с сертификатом, который требуется обновить.

3. В области сведений всех действительных сертификатов есть ссылка **Обновить**, которая отображается при выборе сертификата из списка. Выберите сертификат, который требуется обновить, и нажмите **Обновить** в области сведений.

4. На открывшейся странице **Обновление сертификата Exchange** проверьте нередактируемый список служб Exchange, которым назначен существующий сертификат, и нажмите кнопку **OK**.

Обновление самозаверяющего сертификата Exchange с помощью командной консоли Exchange

Чтобы обновить самозаверяющий сертификат, используйте следующий синтаксис:

```
PowerShell

Get-ExchangeCertificate -Thumbprint <Thumbprint> | New-ExchangeCertificate
[-Force] [-PrivateKeyExportable <$true | $false>]
```

Чтобы найти значение отпечатка сертификата, который требуется обновить, выполните следующую команду:

```
PowerShell

Get-ExchangeCertificate | where {$_.IsSelfSigned -eq $true} | Format-List
FriendlyName,Subject,CertificateDomains,Thumbprint,NotBefore,NotAfter
```

В этом примере обновляется самозаверяющий сертификат на локальном сервере Exchange, при этом используются следующие параметры:

- Значение отпечатка для существующего самозаверяющего сертификата для продления : `BC37CBE2E59566BFF7D01FEAC9B6517841475F2D`
- Параметр *Force* заменяет исходный самозаверяющий сертификат без запроса на подтверждение.
- Закрытый ключ можно экспортировать. То есть вы можете экспортировать сертификат и импортировать его на другие серверы.

```
PowerShell

Get-ExchangeCertificate -Thumbprint BC37CBE2E59566BFF7D01FEAC9B6517841475F2D
| New-ExchangeCertificate -Force -PrivateKeyExportable $true
```

Как узнать, что вы успешно обновили самозаверяющий сертификат Exchange?

Чтобы убедиться, что вы успешно обновили самозаверяющий сертификат Exchange, выполните одно из следующих действий:

- В центре администрирования Exchange в разделе **Сертификаты серверов**> убедитесь, что выбран сервер, на котором установлен сертификат. В списке серверов убедитесь, что сертификат имеет **статусДействительный**.

- В командной консоли Exchange на сервере, на котором вы обновили самозаверяющий сертификат, выполните следующую команду, чтобы проверить значения свойств:

```
PowerShell

Get-ExchangeCertificate | where {$_.Status -eq "Valid" -and $_.IsSelfSigned
-eq $true} | Format-List
FriendlyName,Subject,CertificateDomains,Thumbprint,NotBefore,NotAfter
```

> ⓘ **Важно!**
>
> Удаление, продление или назначение служб сертификату может привести к удалению сертификата с серверной части Exchange и веб-сайта по умолчанию. Важно проверить привязки сертификатов и применить правильные сертификаты.

Дополнительные ресурсы

Не удается открыть OWA, ECP или EMS после удаления самозаверяющего сертификата с веб-сайта серверной части Exchange

Экспорт сертификата с сервера Exchange

Статья • 24.03.2023

Сертификат можно экспортировать с сервера Exchange Server в качестве резервной копии или импортировать сертификат на другие клиенты, устройства или серверы. Сертификаты можно экспортировать в Центре администрирования Exchange (EAC) или в командной консоли Exchange. Полученный файл сертификата представляет собой защищенный паролем двоичный файл PKCS #12, который содержит закрытый ключ сертификата и подходит для импорта (установки) на других серверах.

> **Примечание**
>
> Задачи управления сертификатами удаляются из EAC для Exchange Server 2016 CU23 и Exchange Server 2019 CU12. Используйте процедуру командной консоли Exchange для экспорта или импорта сертификата из этих версий.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- В EAC необходимо экспортировать файл сертификата в UNC-путь (`\\<Server>\<Share>\` или `\\<LocalServerName>\c$\`). В командной консоли Exchange вы можете указать локальный путь.
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Безопасность служб клиентского доступа" в разделе Разрешения клиентов и мобильных устройств .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование Центра администрирования Exchange для экспорта сертификата

1. Откройте EAC и перейдите в раздел **Сертификаты серверов**>.
2. В списке **Выбор сервера** выберите сервер Exchange Server, содержащий сертификат, щелкните значок **Дополнительные параметры**••• выберите **Экспорт сертификата Exchange**.
3. На открывшейся странице **Экспорт сертификата Exchange** введите следующие сведения:

   - **Файл для экспорта**: введите UNC-путь и имя файла сертификата. Пример: `\\FileServer01\Data\Fabrikam.pfx`
   - **Пароль**. При экспорте сертификата с закрытым ключом необходимо указать пароль. Экспорт сертификата с закрытым ключом позволяет импортировать его на другие серверы.

   После этого нажмите кнопку **OK**.

Экспорт сертификата с помощью Центра администрирования Exchange

Чтобы экспортировать двоичный файл сертификата, который можно импортировать на другие клиенты или серверы, используйте следующий синтаксис:

PowerShell

```
$cert = Export-ExchangeCertificate -Thumbprint <Thumbprint> -BinaryEncoded -
Password (ConvertTo-SecureString -String '<Password>' -AsPlainText -Force)
[-Server <ServerIdentity>]
[System.IO.File]::WriteAllBytes('<FilePathOrUNCPath>\<FileName>.pfx',
$cert.FileData)
```

В этом примере сертификат экспортируется с локального сервера Exchange в файл с помощью следующих параметров:

- Сертификат со значением `5113ae0233a72fccb75b1d0198628675333d010e` отпечатка экспортируется в файл `C:\Data\Fabrikam.pfx` на том же сервере, где выполняется команда.
- Экспортируемый файл сертификата кодируется с помощью кодировки DER (а не Base64).
- Пароль для файла сертификата — `P@ssw0rd1`.

PowerShell

```
$cert = Export-ExchangeCertificate -Thumbprint
5113ae0233a72fccb75b1d0198628675333d010e -BinaryEncoded -Password
(ConvertTo-SecureString -String 'P@ssw0rd1' -AsPlainText -Force)
[System.IO.File]::WriteAllBytes('C:\Data\Fabrikam.pfx', $cert.FileData)
```

Чтобы экспортировать ожидающий запрос на сертификат (также известный как запрос подписи сертификата или CSR), используйте следующий синтаксис:

PowerShell

```
$txtcert = Export-ExchangeCertificate -Thumbprint <Thumbprint> [-Server
<ServerName>]
[System.IO.File]::WriteAllBytes('<FilePathOrUNCPath>\<FileName>.req',
[System.Text.Encoding]::Unicode.GetBytes($txtcert))
```

В этом примере выполняется экспорт ожидающего запроса на сертификат с локального сервера Exchange в файл со следующими параметрами:

- Сертификат, имеющий значение `72570529B260E556349F3403F5CF5819D19B3B58` отпечатка, экспортируется в файл `\\FileServer01\Data\Fabrikam.req`.
- Экспортированный файл сертификата имеет кодировку Base64.

PowerShell

```
$txtcert = Export-ExchangeCertificate -Thumbprint
72570529B260E556349F3403F5CF5819D19B3B58
[System.IO.File]::WriteAllBytes('\\FileServer01\Data\Fabrikam.req',
[System.Text.Encoding]::Unicode.GetBytes($txtcert))
```

Подробные сведения о синтаксисе и параметрах см. в разделе Export-ExchangeCertificate.

Примечания.

- Ожидающий запрос на сертификат можно экспортировать, если необходимо повторно отправить запрос на сертификат в центр сертификации и не удается

найти исходный файл запроса на сертификат.

- При экспорте запроса на сертификат обычно не требуется использовать параметр *Password* или параметр *BinaryEncoded* , а запрос сохраняется в REQ-файле.
- Вы не можете импортировать экспортированный запрос на сертификат на другой сервер.

Как проверить, все ли получилось?

Чтобы убедиться, что сертификат успешно экспортирован с сервера Exchange Server, попробуйте импортировать файл сертификата на другой сервер. Дополнительные сведения см. в статье Импорт или установка сертификата на сервере Exchange Server.

Import or install a certificate on an Exchange server

Статья • 24.03.2023

Чтобы включить шифрование для одной или нескольких служб Exchange, сервер Exchange должен использовать сертификат. Обмен данными SMTP между внутренними серверами Exchange шифруется самозаверяющим сертификатом по умолчанию, установленным на сервере Exchange Server. Чтобы зашифровать обмен данными с внутренними или внешними клиентами, серверами или службами, скорее всего, потребуется использовать сертификат, которому автоматически доверяют все клиенты, службы и серверы, которые подключаются к вашей организации Exchange. Дополнительные сведения см. в статье Требования к сертификатам для служб Exchange.

Вы можете импортировать (установить) сертификаты на серверах Exchange в Центре администрирования Exchange (EAC) или в командной консоли Exchange.

На сервере Exchange server можно импортировать следующие типы файлов сертификатов:

- **Файлы сертификатов PKCS #12**. Это двоичные файлы сертификатов, которые имеют расширения CER, CRT, DER, P12 или PFX и требуют пароля, если файл содержит закрытый ключ или цепочку доверия. Ниже приведены примеры таких типов файлов:

  - Самозаверяющие сертификаты, экспортированные с других серверов Exchange с помощью Центра администрирования Exchange или **Export-ExchangeCertificate** со значением `$true` параметра *PrivateKeyExportable* . Дополнительные сведения см. в статье Export a certificate from an Exchange server.

  - Сертификаты, выданные центром сертификации (внутренний ЦС, например службы сертификатов Active Directory, или коммерческий ЦС).

  - Сертификаты, экспортированные с других серверов (например, Skype для бизнеса Server).

- **Файлы сертификатов PKCS #7**. Это текстовые файлы сертификатов с расширениями P7B или P7C. Эти файлы содержат текст: `-----BEGIN CERTIFICATE-----` и `-----END CERTIFICATE-----` или `-----BEGIN PKCS7-----` и `-----END PKCS7-----`. Вместе с двоичным файлом сертификата центр сертификации

может отправить вам файл цепочки сертификатов, который также необходимо установить.

> **Примечание**
>
> Задачи управления сертификатами удаляются из EAC для Exchange Server 2016 CU23 и Exchange Server 2019 CU12. Используйте процедуру командной консоли Exchange для экспорта или импорта сертификата из этих версий.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- В EAC необходимо импортировать файл сертификата из UNC-пути (`\\<Server>\<Share>\` или `\\<LocalServerName>\c$\`). В командной консоли Exchange вы можете указать локальный путь.
- В Центре администрирования Exchange можно импортировать файл сертификата на несколько серверов Exchange одновременно (шаг 4 в процедуре).
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Безопасность служб клиентского доступа" в разделе Разрешения клиентов и мобильных устройств .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование Центра администрирования Exchange для импорта сертификата на одном

или нескольких серверах Exchange

1. Откройте EAC и перейдите в раздел **Сертификаты серверов**>.

2. В списке **Выбор сервера** выберите сервер Exchange Server, на котором требуется установить сертификат, щелкните значок **Дополнительные параметры**••• выберите **Импорт сертификата Exchange**.

3. Запустится мастер **Импорт сертификата Exchange**. На странице **Этот мастер импортирует сертификат из файла** введите следующую информацию:

   - **Файл для импорта**: введите UNC-путь и имя файла сертификата. Пример: `\\FileServer01\Data\Fabrikam.cer`

   - **Пароль**. Если файл сертификата содержит закрытый ключ или цепочку доверия, файл защищен паролем. Введите пароль в это поле.

   По завершении нажмите кнопку **Далее**.

4. На странице **Укажите серверы, к которым требуется применить этот сертификат, щелкните**➕

   На открывшейся странице **Выберите сервер** выберите сервер Exchange, на который необходимо установить сертификат, и нажмите **Добавить** - >. Повторите этот шаг нужное количество раз. Завершив выбор серверов, нажмите кнопку **OK**.

   Закончив, нажмите кнопку **Готово**. Дальнейшие действия см. в разделе Дальнейшие действия.

Импорт сертификата на сервер Exchange Server с помощью командной консоли Exchange

Чтобы импортировать файл сертификата, используйте следующий синтаксис:

PowerShell

```
Import-ExchangeCertificate -FileData
([System.IO.File]::ReadAllBytes('<FilePathOrUNCPath>')) [-Password
(ConvertTo-SecureString -String '<Password> ' -AsPlainText -Force)] [-
PrivateKeyExportable <$true | $false>] [-Server <ServerIdentity>]
```

Этот синтаксис используется со следующими типами файлов сертификатов:

- Двоичные файлы сертификатов (файлы PKCS #12 с расширениями CER, CRT, .der, .p12 или PFX).
- Цепочка файлов сертификатов (текстовые файлы PKCS No 7 с расширениями P7B или P7C).

В этом примере импортируется файл `\\FileServer01\Data\Fabrikam.pfx` сертификата, защищенный паролем P@ssw0rd1 на локальном сервере Exchange Server.

PowerShell

```
Import-ExchangeCertificate -FileData
([System.IO.File]::ReadAllBytes('\\FileServer01\Data\Fabrikam.pfx')) -
Password (ConvertTo-SecureString -String 'P@ssw0rd1' -AsPlainText -Force)
```

В этом примере импортируется файл `\\FileServer01\Data\Chain of Certificates.p7b` цепочки сертификатов .

PowerShell

```
Import-ExchangeCertificate -FileData
([System.IO.File]::ReadAllBytes('\\FileServer01\Data\Chain of
Certificates.p7b'))
```

Подробные сведения о синтаксисе и параметрах см. в разделе Import-ExchangeCertificate.

Примечания:

- Эту процедуру необходимо повторить на каждом сервере Exchange Server, где требуется импортировать сертификат (выполните команду на сервере или используйте параметр *Server*).
- Параметр *FileData* принимает локальные пути, если файл сертификата находится на сервере Exchange Server, где выполняется команда, и это тот же сервер, на котором требуется импортировать сертификат. В противном случае используйте UNC-путь.
- Если вы хотите экспортировать сертификат с сервера, на который вы его импортируете, необходимо использовать параметр *PrivateKeyExportable* со значением `$true`.

Как проверить, все ли получилось?

Чтобы убедиться, что сертификат успешно импортирован (установлен) на сервере Exchange Server, выполните одно из следующих действий:

- В центре администрирования Exchange в разделе **Сертификаты серверов**> убедитесь, что выбран сервер, на котором установлен сертификат. Сертификат должен быть в списке сертификатов и иметь **статусДействительный**.
- В командной консоли Exchange на сервере, где установлен сертификат, выполните следующую команду:

```
PowerShell

Get-ExchangeCertificate | where {$_.Status -eq "Valid"} | Format-List
FriendlyName,Subject,CertificateDomains,Thumbprint,NotBefore,NotAfter
```

Дальнейшие действия

После установки сертификата на сервере необходимо назначить сертификат одной или нескольким службам Exchange, прежде чем сервер Exchange сможет использовать сертификат для шифрования. Дополнительные сведения см. в статье Назначение сертификатов Exchange Server службам.

Настройка ограничений на размер сообщений для клиента в Exchange Server

Статья • 04.04.2023

В Exchange Server существует несколько различных ограничений на размер сообщений, которые применяются к сообщениям по мере их перемещения по вашей организации. Дополнительные сведения см. в статье Размер сообщений и ограничения получателей в Exchange Server.

Однако существуют ограничения на размер сообщений клиента, которые можно настроить для Outlook в Интернете (прежнее название — Outlook Web App) и почтовых клиентов, использующих Exchange ActiveSync или веб-службы Exchange (EWS). Если изменить ограничения на размер сообщений организации, соединителя или пользователя Exchange, скорее всего, потребуется изменить ограничения для Outlook в Интернете, ActiveSync и EWS. Эти ограничения описаны в таблицах ниже. Чтобы изменить ограничения на размер сообщений для определенного типа клиентов, необходимо изменить **все** значения, указанные в таблице.

> **Примечание**
>
> Для любого ограничения на размер сообщений необходимо задать значение, которое превышает требуемый фактический размер. Это из-за кодировки Base 64 вложений и других двоичных данных. При кодировании Base64 размер сообщения увеличивается приблизительно на 33 %, поэтому указываемое значение должно быть на 33 % больше требуемого фактического размера сообщения. Например, если вы зададите 64 МБ как максимальный размер сообщения, реальный его размер будет составлять приблизительно 48 МБ или меньше.

ActiveSync

Службы	Файл конфигурации	Ключи и значения по умолчанию	Size
Служба клиентского доступа (интерфейсная)	`%ExchangeInstallPath%FrontEnd\HttpProxy\Sync\web.config`	`maxAllowedContentLength="30000000"` (отсутствует по умолчанию; см. примечания)	В байтах
Служба клиентского доступа (интерфейсная)	`%ExchangeInstallPath%FrontEnd\HttpProxy\Sync\web.config`	`maxRequestLength="10240"`	В килобайтах
Внутренняя служба	`%ExchangeInstallPath%ClientAccess\Sync\web.config`	`maxAllowedContentLength="30000000 bytes"` (отсутствует по умолчанию; см. примечания)	В байтах
Внутренняя служба	`%ExchangeInstallPath%ClientAccess\Sync\web.config`	`maxRequestLength="10240"`	В килобайтах
Внутренняя служба	`%ExchangeInstallPath%ClientAccess\Sync\web.config`	`<add key="MaxDocumentDataSize" value="10240000">`	В байтах

Комментарии к ограничениям для ActiveSync

По умолчанию ключ *maxAllowedContentLength* в файлах `web.config` для ActiveSync отсутствует. Однако максимальный размер сообщения для ActiveSync зависит от значения **maxAllowedContentLength** , применяемого ко всем веб-сайтам на сервере. Значение по умолчанию — 30 000 000 байтов. Чтобы просмотреть эти значения для ActiveSync на серверах почтовых ящиков в диспетчере IIS, выполните следующие действия.

1. Выполните одно из следующих действий:

   - На веб-сайте клиентского доступа (внешний интерфейс) откройте **диспетчер IIS**, перейдите в раздел **Сайты**>**Веб-сайт по умолчанию** и выберите **Microsoft-Server-ActiveSync**.
   - Для внутреннего веб-сайта откройте **диспетчер IIS**, перейдите в **раздел Сервернаячасть Сайта**> Exchange и выберите **Microsoft-Server-ActiveSync**.

2. Убедитесь, что в нижней части окна выбрана вкладка **Представление компонентов** , и дважды щелкните **редактор конфигурации** в разделе **Управление** .

3. Щелкните стрелку раскрывающегося списка в поле **Раздел** , **перейдите к system.webServer**>**security** и выберите **requestFiltering**.

4. В результатах разверните список **requestLimits**, после чего отобразится пункт **maxAllowedContentLength** и значение по умолчанию 30 000 000 (в байтах).

Чтобы изменить значение **maxAllowedContentLength**, введите новое значение в байтах и выберите элемент **Применить**. Необходимо также изменить значение для веб-сайта клиентского доступа и внутреннего веб-сайта.

Примечание. Вы можете изменить тот же параметр в диспетчере IIS в разделе **Сайты**>**По умолчанию Веб-сайт**>**Microsoft-Server-ActiveSync** или**Серверная часть**>**exchange сайтов**>**Microsoft-Server-ActiveSync**, а затем **запрос фильтрации** в разделе >**IISИзменить параметры компонентов** в области >**ДействияМаксимальная разрешенная длина содержимого (байт)** в разделе **Ограничения запросов**.

После изменения значения в диспетчере IIS новый ключ *maxAllowedContentLength* записывается в соответствующий файл клиентского доступа или серверной части web.config файл, описанный в таблице.

Веб-службы Exchange

Служба	Файл конфигурации	Ключи и значения по умолчанию	Size
Служба клиентского доступа (интерфейсная)	`%ExchangeInstallPath%FrontEnd\HttpProxy\ews\web.config`	`maxAllowedContentLength="67108864"`	В байтах
Внутренняя служба	`%ExchangeInstallPath%ClientAccess\exchweb\ews\web.config`	`maxAllowedContentLength="67108864"`	В байтах
Внутренняя служба	`%ExchangeInstallPath%ClientAccess\exchweb\ews\web.config`	14 экземпляров `maxReceivedMessageSize="67108864"` (для различных сочетаний привязок http/https и методов проверки подлинности)	В байтах

Комментарии к ограничениям для EWS

- В серверном `web.config` файле есть два экземпляра значения `maxReceivedMessageSize="1048576"` для привязок **UMLegacyMessageEncoderSoap11Element** , которые не нужно изменять.
- *maxRequestLength* — это параметр ASP.NET, который есть в обоих файлах web.config, но не используется веб-службами Exchange, поэтому вам не нужно его изменять.

Outlook в Интернете

Служба	Файл конфигурации	Ключи и значения по умолчанию	Size
Служба клиентского доступа (интерфейсная)	`%ExchangeInstallPath%FrontEnd\HttpProxy\owa\web.config`	`maxAllowedContentLength="35000000"`	В байтах
Служба клиентского доступа (интерфейсная)	`%ExchangeInstallPath%FrontEnd\HttpProxy\owa\web.config`	`maxRequestLength="35000"`	В килобайтах
Внутренняя служба	`%ExchangeInstallPath%ClientAccess\Owa\web.config`	`maxAllowedContentLength="35000000"`	В байтах
Внутренняя служба	`%ExchangeInstallPath%ClientAccess\Owa\web.config`	`maxRequestLength="35000"`	В килобайтах
Внутренняя служба	`%ExchangeInstallPath%ClientAccess\Owa\web.config`	2 экземпляра `maxReceivedMessageSize="35000000"` (для привязок HTTP и HTTPS)	В байтах
Внутренняя служба	`%ExchangeInstallPath%ClientAccess\Owa\web.config`	2 экземпляра `maxStringContentLength="35000000"` (для привязок HTTP и HTTPS)	В байтах

Комментарии к ограничениям для Outlook в Интернете

- Во внутреннем `web.config` файле есть экземпляр значения `maxStringContentLength="102400"` для привязки **MsOnlineShellService** , который не требуется изменять.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 15 минут.
- Разрешения Exchange не применяются к процедурам, описанным в этом разделе. Эти процедуры выполняются в операционной системе сервера Exchange.
- Изменения, сохраненные в файле конфигурации web.config, применяются после перезапуска служб IIS.
- Чтобы учитывать увеличение размера на 33 % при кодировании Base64, умножьте нужный максимальный размер в мегабайтах на 4/3. Чтобы преобразовать это значение в килобайты, умножьте его на 1024. Чтобы преобразовать значение в байты, умножьте его на 1048756 (1024*1024). Обратите внимание, что увеличение размера из-за кодирования Base64 может

превышать 33 % и зависит от нескольких факторов, например размера файла вложения, типа, сжатия и почтового клиента.

- Все настраиваемые параметры Exchange или IIS, внесенные в файлы конфигурации приложения Exchange XML на сервере Exchange Server (например, web.config файлы или EdgeTransport.exe.config файл), **будут перезаписаны** при установке exchange CU. Обязательно сохраните эти сведения, чтобы можно было легко повторно применить параметры после установки. После установки exchange CU необходимо повторно настроить эти параметры.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**.

Настройка ограничения на размер сообщений для определенного клиента с помощью "Блокнота"

1. Откройте соответствующие файлы web.config в "Блокноте". Например, чтобы открыть файлы web.config для клиентов веб-служб Exchange, выполните указанные ниже команды.

   Консоль

   ```
   Notepad %ExchangeInstallPath%ClientAccess\exchweb\ews\web.config
   ```

   Консоль

   ```
   Notepad %ExchangeInstallPath%FrontEnd\HttpProxy\ews\web.config
   ```

2. Найдите нужные ключи в соответствующих файлах web.config, как описано в таблицах, приведенных выше в этом разделе. Например, для клиентов EWS найдите ключ *maxAllowedContentLength* в файлах клиентского доступа и серверной части web.config и всех 14 экземпляров значения `maxReceivedMessageSize="67108864"` в серверном web.config файле.

   ```
   <requestLimits maxAllowedContentLength="67108864" />
   ...maxReceivedMessageSize="67108864"...
   ```

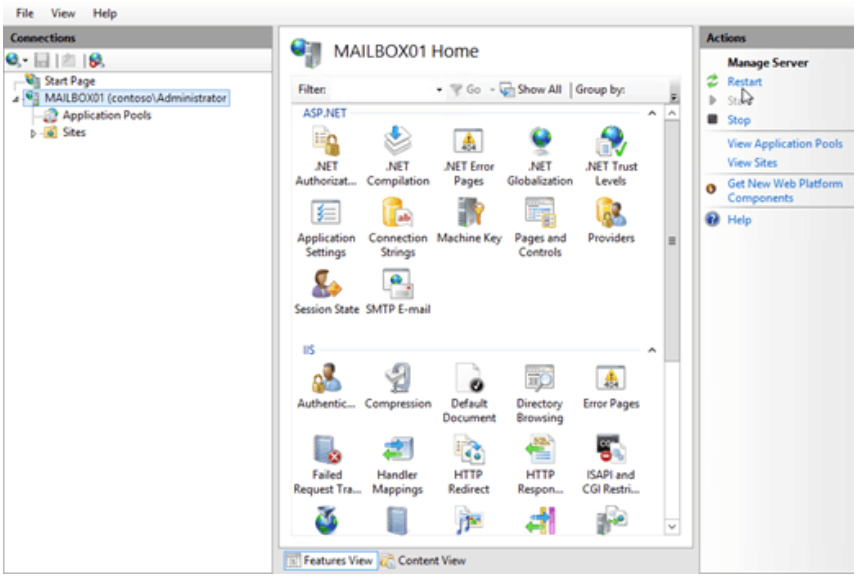
   Например, чтобы разрешить максимальный размер сообщения в кодировке Base64 примерно 64 МБ, измените все экземпляры `67108864` на `89478486` (64*4/3*1048756):

   ```
   <requestLimits maxAllowedContentLength="89478486" />
   ...maxReceivedMessageSize="89478486"...
   ```

3. По завершении сохраните и закройте файлы web.config.

4. Перезапустите IIS на сервере Exchange одним из указанных способов:

   - В диспетчере IIS выберите сервера, а затем в панели **действий** нажмите **Перезапустить**.



   - Выполните следующие команды в командной строке с повышенными привилегиями (окно командной строки, открываемое путем выбора **запуска от имени администратора**):

```
Консоль
net stop w3svc /y
```

```
Консоль
net start w3svc
```

Настройка ограничений на размер сообщений для определенного клиента в командной строке

Настроить ограничения на размер сообщений для конкретных клиентов можно не только в "Блокноте", но и в командной строке. Откройте командную строку с повышенными привилегиями на сервере Exchange Server (используйте для этого команду **Запуск от имени администратора**) и выполните соответствующие команды для настройки нужных ограничений.

> ⓘ **Примечание**
>
> - В командах указываются значения размера по умолчанию, потому вам нужно будет их изменить.
> - Обратите внимание на то, в каких единицах задано значение — в байтах или в килобайтах.

ActiveSync

```
```

```
%windir%\system32\inetsrv\appcmd.exe set config "Default Web Site/Microsoft-Server-ActiveSync/" -
section:system.webServer/security/requestFiltering
/requestLimits.maxAllowedContentLength:30000000
%windir%\system32\inetsrv\appcmd.exe set config "Default Web Site/Microsoft-Server-ActiveSync/" -
section:system.web/httpRuntime /maxRequestLength:10240
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/Microsoft-Server-ActiveSync/"
-section:system.webServer/security/requestFiltering
/requestLimits.maxAllowedContentLength:30000000
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/Microsoft-Server-ActiveSync/"
-section:system.web/httpRuntime /maxRequestLength:10240
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/Microsoft-Server-ActiveSync/"
-section:appSettings /[key='MaxDocumentDataSize'].value:10240000
```

Веб-службы Exchange

```
%windir%\system32\inetsrv\appcmd.exe set config "Default Web Site/ews/" -
section:system.webServer/security/requestFiltering
/requestLimits.maxAllowedContentLength:67108864
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/ews/" -
section:system.webServer/security/requestFiltering
/requestLimits.maxAllowedContentLength:67108864
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/ews/" -
section:system.serviceModel/bindings /customBinding.
[name='EWSAnonymousHttpsBinding'].httpsTransport.maxReceivedMessageSize:67108864
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/ews/" -
section:system.serviceModel/bindings /customBinding.
[name='EWSAnonymousHttpBinding'].httpTransport.maxReceivedMessageSize:67108864
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/ews/" -
section:system.serviceModel/bindings /customBinding.
[name='EWSBasicHttpsBinding'].httpsTransport.maxReceivedMessageSize:67108864
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/ews/" -
section:system.serviceModel/bindings /customBinding.
[name='EWSBasicHttpBinding'].httpTransport.maxReceivedMessageSize:67108864
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/ews/" -
section:system.serviceModel/bindings /customBinding.
[name='EWSNegotiateHttpsBinding'].httpsTransport.maxReceivedMessageSize:67108864
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/ews/" -
section:system.serviceModel/bindings /customBinding.
[name='EWSNegotiateHttpBinding'].httpTransport.maxReceivedMessageSize:67108864
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/ews/" -
section:system.serviceModel/bindings /customBinding.
[name='EWSWSSecurityHttpsBinding'].httpsTransport.maxReceivedMessageSize:67108864
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/ews/" -
section:system.serviceModel/bindings /customBinding.
[name='EWSWSSecurityHttpBinding'].httpTransport.maxReceivedMessageSize:67108864
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/ews/" -
section:system.serviceModel/bindings /customBinding.
[name='EWSWSSecuritySymmetricKeyHttpsBinding'].httpsTransport.maxReceivedMessageSize:67108864
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/ews/" -
section:system.serviceModel/bindings /customBinding.
[name='EWSWSSecuritySymmetricKeyHttpBinding'].httpTransport.maxReceivedMessageSize:67108864
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/ews/" -
section:system.serviceModel/bindings /customBinding.
[name='EWSWSSecurityX509CertHttpsBinding'].httpsTransport.maxReceivedMessageSize:67108864
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/ews/" -
section:system.serviceModel/bindings /customBinding.
[name='EWSWSSecurityX509CertHttpBinding'].httpTransport.maxReceivedMessageSize:67108864
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/ews/" -
section:system.serviceModel/bindings /webHttpBinding.
[name='EWSStreamingNegotiateHttpsBinding'].maxReceivedMessageSize:67108864
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/ews/" -
```

```
section:system.serviceModel/bindings /webHttpBinding.
[name='EWSStreamingNegotiateHttpBinding'].maxReceivedMessageSize:67108864
```

Outlook в Интернете

```
%windir%\system32\inetsrv\appcmd.exe set config "Default Web Site/owa/" -
section:system.webServer/security/requestFiltering
/requestLimits.maxAllowedContentLength:35000000
%windir%\system32\inetsrv\appcmd.exe set config "Default Web Site/owa/" -
section:system.web/httpRuntime /maxRequestLength:35000
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/owa/" -
section:system.webServer/security/requestFiltering
/requestLimits.maxAllowedContentLength:35000000
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/owa/" -
section:system.web/httpRuntime /maxRequestLength:35000
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/owa/" -
section:system.serviceModel/bindings /webHttpBinding.
[name='httpsBinding'].maxReceivedMessageSize:35000000
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/owa/" -
section:system.serviceModel/bindings /webHttpBinding.
[name='httpBinding'].maxReceivedMessageSize:35000000
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/owa/" -
section:system.serviceModel/bindings /webHttpBinding.
[name='httpsBinding'].readerQuotas.maxStringContentLength:35000000
%windir%\system32\inetsrv\appcmd.exe set config "Exchange Back End/owa/" -
section:system.serviceModel/bindings /webHttpBinding.
[name='httpBinding'].readerQuotas.maxStringContentLength:35000000
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно настроили ограничение размера сообщения для определенного клиента, отправьте тестовое сообщение в почтовый ящик с помощью затронутого клиента. Вы можете использовать несколько небольших вложений или одно большое, чтобы тестовые сообщения были приблизительно на 33 % меньше заданного вами значения. Например, если указать значение 85 МБ, реалистичный максимальный размер сообщения будет равен приблизительно 64 МБ.

Служба доступности в Exchange Server

Статья • 04.04.2023

Служба доступности предоставляет сведения о доступности для клиентов Outlook и Outlook в Интернете (прежнее название — Outlook Web App). Эта служба расширяет для информационных работников возможности ведения календаря и планирования собраний, предоставляя надежные, согласованные и актуальные сведения о доступности.

Outlook и Outlook в Интернете используют службу доступности для выполнения следующих задач:

- Получение текущих сведений о доступности для почтовых ящиков Exchange
- Получение текущих сведений о доступности из других организаций Exchange
- Получение опубликованных сведений о доступности из общедоступных папок для почтовых ящиков в предыдущих версиях Exchange
- просмотр рабочих часов участников;
- отображение предложений по времени проведения собраний.

Принцип работы службы доступности в Exchange Server

Служба доступности получает сведения о доступности непосредственно из целевого почтового ящика Exchange.

Outlook использует службу автообнаружения Exchange для получения URL-адреса службы доступности. Дополнительные сведения о службе автообнаружения см. в разделе Служба автообнаружения.

Настроить службу доступности можно только в командной консоли Exchange. Для этой цели не подойдет Центр администрирования Exchange (EAC).

API службы доступности доступен как веб-служба, чтобы позволить разработчикам создавать сторонние средства интеграции.

Служба доступности и сообщения автоматического ответа

Служба доступности предоставляет доступ к автоматическим ответам, отправляемым пользователями в случае их длительного отсутствия на рабочем месте.

Специалисты по обработке данных могут использовать функцию автоматических ответов (ранее называлась "Отсутствие на рабочем месте") в приложениях Outlook и Outlook в Интернете, чтобы оповестить других пользователей о том, что они не смогут отвечать на сообщения электронной почты. Эта функция упрощает настройку и управление автоматическими ответными сообщениями как для информационных работников, так и для администраторов.

Способы получения сведений о доступности

В следующей таблице перечислены способы получения сведений о доступности в различных топологиях с одним лесом.

Client	**Получение сведений о доступности исходного почтового ящика**	**Целевой почтовый ящик**	**Способ получения сведений о занятости**
Outlook 2010 или более поздней версии;	Exchange 2010 или более поздней версии	Exchange 2010 или более поздней версии	Служба доступности считывает сведения о занятости из целевого почтового ящика.
Outlook в Интернете или Outlook Web App	Exchange 2010 или более поздней версии	Exchange 2010 или более поздней версии	Outlook в Интернете или Outlook Web App вызывает API службы доступности, который считывает сведения о доступности из целевого почтового ящика.

Настройка службы доступности для топологий между лесами в Exchange Server

Статья • 04.04.2023

Служба доступности улучшает сведения о доступности информационных работников, предоставляя клиентам Outlook безопасные, согласованные и актуальные сведения о доступности. По умолчанию эта служба устанавливается вместе с Exchange Server. В топологиях перекрестного леса, в которых все подключенные клиенты работают с Outlook, восстановить сведения о доступности можно только с помощью службы доступности. С помощью командной консоли Exchange можно настроить службу доступности для топологий между лесами.

> ⓘ **Примечание**
>
> Вы не можете использовать Центр администрирования Exchange (EAC) для настройки службы доступности для топологий между лесами.

Использование службы доступности в доверенных и недоверенных лесах

Можно использовать службу доступности в топологиях "перекрестный лес" в лесах с отношением доверия или без него. Тип сведений о доступности зависит от того, используете ли вы доверенный или недоверенный лес.

Доверенные леса. В доверенных лесах можно настроить службу доступности для получения сведений о доступности для каждого пользователя. Если служба доступности настроена на извлечение сведений о доступности для конкретных пользователей, служба может создавать перекрестные запросы между лесами от имени конкретного пользователя. Это позволяет пользователю в удаленном лесу извлекать подробные сведения о доступности для всех, кто не находится в том же лесу.

Ненадежные леса. В ненадежных лесах можно настроить службу доступности только для получения сведений о доступности на уровне всей организации. Если служба доступности создает перекрестные запросы о доступности между лесами на уровне организации, сведения о доступности возвращаются для каждого

пользователя организации. В недоверенных лесах невозможно контролировать уровень сведений о доступности, которые возвращаются для конкретного пользователя.

Настройка Windows для межлесных топологий

По умолчанию глобальный список адресов (GAL) содержит получателей почты из одного леса. В среде перекрестного леса рекомендуется использовать Microsoft Identity Lifecycle Manager (ILM) 2007 с пакетом дополнительных компонентов 1 (FP1), чтобы обеспечить, что глобальный список адресов в любом отдельном лесу содержит получателей электронной почты из других лесов. ILM 2007 с пакетом дополнительных компонентов 1 (FP1) создает пользователей почты, представляющих получателей из других лесов, таким образом позволяя пользователям видеть этих адресатов в своих глобальных списках адресов и отправлять им почту. Например, пользователи из леса A выглядят как пользователь почты в лесу B и наоборот. Затем пользователи в целевом лесу для отправки почты могут выбирать объект пользователя почты, представляющий адресата из другого леса.

Чтобы разрешить синхронизацию глобальных списков адресов, создаются агенты управления, которые импортируют обладающих электронной почтой пользователей, контакты и группы из назначенных служб Active Directory в централизованный метакаталог. В метакаталоге объекты, для которых предусмотрено использование почты, представлены как пользователи почты. Группы представлены как контакты без какого-либо связанного членства. Агенты управления затем экспортируют этих пользователей почты в подразделение указанного конечного леса.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут.
- Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записях "Разрешения службы доступности" в разделе Разрешения клиентов и мобильных устройств .

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.
- Существуют дополнительные рекомендации, когда целевой лес Exchange Server 2013 или Exchange Server 2016. Дополнительные сведения см. в разделе Поиск между лесами, свободными и занятыми, если целевой лес Exchange Server 2013 или Exchange Server 2016.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование командной консоли Exchange для настройки сведений о доступности и доступности для каждого пользователя в доверенной топологии между лесами

В этом примере служба доступности настраивается на получение сведений о доступности для конкретного пользователя на сервере почтовых ящиков в целевом лесу.

PowerShell

```
Get-MailboxServer | Add-ADPermission -Accessrights Extendedright -
Extendedrights "ms-Exch-EPI-Token-Serialization" -User "<Remote Forest
Domain>\Exchange servers"
```

В этом примере определяются методы доступа к сведениям о доступности, которые используются службой доступности на локальном сервере почтовых ящиков в исходном лесу. Локальный сервер почтовых ящиков настроен на получение доступа к сведениям о доступности из леса ContosoForest.com для конкретного пользователя. В этом примере для извлечения сведений о доступности используется учетная запись службы.

PowerShell

```
Add-AvailabilityAddressSpace -Forestname ContosoForest.com -AccessMethod
PerUserFB -UseServiceAccount $true
```

> ⓘ **Примечание**
>
> Чтобы настроить двунаправленную доступность между лесами, повторите эти действия в командной консоли Exchange для целевого леса.

Если вы решили настроить доступность между лесами с доверием, а также использовать учетную запись службы (вместо указания учетных данных для всей организации или пользователя), необходимо расширить разрешения, как показано в примере в следующем разделе "Использование командной консоли Exchange для настройки доступности между доверенными лесами с помощью учетной записи службы". Выполнение этой процедуры в целевом лесу дает серверам почтовых ящиков в исходном лесу разрешение на сериализацию исходного контекста пользователя.

Использование командной консоли Exchange для настройки доступности между доверенными лесами с помощью учетной записи службы

В этом примере настраивается надежная межлесная доступность с учетной записью службы.

PowerShell

```
Get-MailboxServer | Add-ADPermission -Accessrights Extendedright -
Extendedright "ms-Exch-EPI-Token-Serialization" -User "<Remote Forest
Domain>\Exchange servers"
```

Подробные сведения о синтаксисе и параметрах см. в следующих разделах.

- Get-MailboxServer
- Add-ADPermission
- Add-AvailabilityAddressSpace
- Set-AvailabilityConfig

Использование командной консоли Exchange для настройки сведений о доступности и доступности в ненадежной топологии между лесами

В этом примере создается учетная запись объекта настройки доступности для всей организации, чтобы настроить уровень доступа к сведениям о доступности в целевом лесу.

PowerShell

```
Set-AvailabilityConfig -OrgWideAccount "Contoso.com\User"
```

В этом примере добавляется объект конфигурации адресного пространства доступности для исходного леса, и вам будет предложено ввести учетные данные для пользователя всей организации в Contoso.com домене.

PowerShell

```
Add-AvailabilityAddressspace -Forestname Contoso.com -Accessmethod OrgWideFB
-Credential (Get-Credential)
```

Планирование и развертывание Exchange Server

Статья • 07.05.2024

Эта статья содержит ссылки на статьи и сведения о планировании и последующем развертывании Exchange Server 2016 или Exchange Server 2019 году.

> **ⓘ Важно!**
>
> Прежде чем приступить к развертыванию, ознакомьтесь с **заметками о выпуске для Exchange Server** разделов. Заметки о выпуске содержат важную информацию о проблемах, которые могут возникнуть во время и после развертывания.

> **Совет**
>
> В дополнение к этой статье рекомендуется использовать **помощник по развертыванию Microsoft Exchange Server**. Используйте это средство для создания настраиваемого контрольного списка для планирования, установки или обновления Exchange. Руководство доступно для нескольких сценариев, включая локальное, гибридное или облачное развертывание.

Планирование для Exchange Server

Используйте сведения, доступные по следующим ссылкам, чтобы спланировать развертывание Exchange Server 2016 или Exchange Server 2019 в вашей организации.

> **ⓘ Важно!**
>
> Сведения об установке Exchange Server 2019 в тестовой среде см. в разделе **Установка тестовой среды Exchange 2016 или Exchange 2019** далее в этой статье.

Архитектура Exchange

> Сведения о ролях сервера почтовых ящиков и пограничного транспортного сервера и других возможностях в Exchange.

Требования к системе для Exchange Server

> Изучите требования к системе, которые должны быть выполнены в вашей организации, прежде чем вы сможете установить Exchange Server.

Предварительные требования для Exchange Server

> Узнайте о функциях Windows Server и другом программном обеспечении, которое необходимо установить для успешной установки Exchange Server.

Active Directory

> Узнайте, как Exchange Server использует Active Directory и как развертывание Active Directory влияет на развертывание Exchange Server.

Защита от нежелательной почты и вредоносных программ в Exchange Server

> Узнайте о встроенных параметрах защиты от нежелательной защиты и защиты от вредоносных программ в Exchange Server.

Гибридные развертывания Exchange Server

> Сведения о планировании гибридного развертывания между Microsoft 365 или Office 365 и локальной организацией Exchange.

Виртуализация Exchange Server

> Узнайте, как развернуть Exchange Server в виртуализированной среде.

Разработки для Exchange Online и Exchange

> Сведения об интерфейсах программирования приложений (API), доступных для приложений, использующих Exchange Server 2019.

Создание тестовой среды Exchange 2016 или Exchange 2019

Перед установкой первого сервера Exchange Server рекомендуется установить Exchange Server в изолированной тестовой среде. Это позволит снизить риск отрицательных последствий для рабочей среды и риск простоя пользователей.

Тестовая среда будет выступать в качестве "подтверждения концепции" для новой структуры Exchange и позволит перейти вперед или откатить все реализации перед развертыванием Exchange Server в рабочих средах. Наличие эксклюзивной тестовой среды для проверки и тестирования позволяет выполнять предварительные проверки для будущих рабочих сред. Устанавливая сначала в тестовой среде, мы считаем, что ваша организация будет иметь более высокую вероятность успеха в полной реализации в рабочей среде.

Многие организации могут понести значительные затраты на создание испытательной лаборатории из-за необходимости дублирования рабочей среды. Чтобы снизить затраты на оборудование, связанные с лабораторией прототипов, рекомендуется использовать виртуализацию с помощью технологий Hyper-V в Windows Server. Технология Hyper-V позволяет выполнить виртуализацию сервера, благодаря которой возможен запуск нескольких виртуальных операционных систем на одном компьютере.

Подробные сведения о Hyper-V см. в статье Виртуализация серверов. Сведения о поддержке корпорацией Майкрософт рабочих серверов Exchange в программном обеспечении аппаратной виртуализации см. в разделе Exchange Server виртуализации.

Развертывание Exchange 2016 или Exchange 2019

На этапе развертывания вы устанавливаете Exchange Server в организации. Прежде чем приступить к этапу развертывания, следует спланировать организацию Exchange. Дополнительные сведения см. в разделе Планирование Exchange Server выше в этой статье.

Используйте сведения, доступные по следующим ссылкам, чтобы помочь в развертывании Exchange Server.

Подготовка Active Directory и доменов для Exchange

> Узнайте о действиях, необходимых для подготовки леса Active Directory к Exchange 2019, а также об изменениях, внесенных в лес Exchange Server установки.

Установка серверов почтовых ящиков Exchange с помощью мастера

> Сведения об использовании мастера для установки серверов почтовых ящиков.

Всегда устанавливайте **последний накопительный пакет обновления Exchange** (CU) (номера сборок и даты выпуска Exchange Server | Документация Майкрософт). Нет необходимости устанавливать сборку RTM или предыдущие сборки, а затем обновлять до последней версии cu. Это связано с тем, что каждый CU является полной сборкой продукта.

Перед запуском сервера в сети обновитесь с помощью **последнего обновления для системы безопасности Exchange** (SU). Выполните проверку с помощью сценария средства проверки работоспособности Exchange: https://aka.ms/ExchangeHealthChecker.

Использование автоматического режима в программе установки Exchange

> Сведения об использовании автоматической установки в командной строке для установки, удаления, обновления и восстановления серверов Exchange.

Установка пограничных транспортных серверов Exchange с помощью мастера

> Сведения об использовании мастера для установки пограничных транспортных серверов в сети периметра.

Обновление Exchange до последнего накопительного пакета обновления

> Узнайте о поиске и установке последней версии cu для серверов Exchange в организации.

Поддерживайте серверы в наиболее **актуальном** состоянии. Всегда в последнем выпуске Exchange CU или последнем выпуске -1 CU.

1. Эта страница содержит ссылки на последние накопительные пакеты обновления Exchange: Номера сборок и даты выпуска Exchange Server | Документация Майкрософт.

2. См. статью: Обновление Exchange до последнего накопительного пакета обновления | Документация Майкрософт.

Убедитесь**, что клиентский компонент Центра обновления Windows/Центр обновления Майкрософт** (WU/MU) включен, и рассмотрите возможность

дальнейшего включения **автоматического обновления** для получения единиц обновления.

Используйте **командную строку с повышенными привилегиями** для запуска любого накопительного пакета обновления или обновления для системы безопасности. Если при запуске установки обновления возникают проблемы, см. раздел https://aka.ms/exupdatefaq.

Периодически запускайте скрипт **средства проверки работоспособности Exchange**, чтобы проверка, если установлены последние номера SU Exchange: https://aka.ms/ExchangeHealthChecker.

Гибридные развертывания Exchange Server

> Сведения о развертывании Exchange Server в существующем гибридном развертывании см. в этой статье.

Задачи после установки Exchange Server

> Сведения о задачах после установки для завершения установки Exchange Server.

Программа установки Exchange

Для установки и обслуживания различных выпусков и версий Exchange Server можно использовать различные типы и режимы установки Exchange Server.

Выпуски и версии Exchange

Служба Exchange доступна в двух серверных версиях: Standard Edition и Enterprise Edition. Устанавливаемая версия определяется ключом продукта (единственная доступная загрузка позволяет установить обе версии). Дополнительные сведения см. в разделе Лицензирование Exchange: вопросы и ответы.

Типы установки Exchange Server

Для установки Exchange Server доступны следующие варианты:

- **Мастер установки Exchange.** Если запустить программу Setup.exe без параметров командной строки, отобразится интерактивный интерфейс, в котором можно использовать мастер установки Exchange 2019.

- **Автоматическая установка Exchange.** Если запустить программу Setup.exe с параметрами командной строки, можно установить Exchange в интерактивной командной строке или с помощью скрипта.

Режимы настройки Exchange Server

Программа установки Exchange поддерживает указанные ниже режимы.

- **Установка**: установите новую роль сервера (сервер почтовых ящиков, пограничный транспортный сервер или средства управления). Этот режим доступен в мастере установки Exchange и автоматической настройке.

- **Удалить**. Удалите установку Exchange с компьютера. Этот режим можно использовать как в мастере установки Exchange, так и в автоматической установке.

- **Обновление**. Установите накопительный пакет обновления на существующем сервере Exchange Server. Этот режим можно использовать как в мастере установки Exchange, так и в автоматической установке.

  > ⓘ **Примечание**
  >
  > Exchange не поддерживает обновления на месте с предыдущих версий. Этот режим используется только для установки CU.

- **RecoverServer**. После катастрофического сбоя необходимо восстановить данные с сервера Exchange Server. Для этого установите новый сервер Windows с тем же полным доменным именем, что и сервер, на котором произошел сбой (например, mailbox01.contoso.com), а затем запустите программу установки Exchange с параметром */Mode:RecoverServer* без указания ролей сервера Exchange.

  Программа установки обнаруживает объект Exchange Server в Active Directory и автоматически устанавливает соответствующие файлы и конфигурацию. После восстановления сервера можно восстановить базы данных и повторно настроить дополнительные параметры. Чтобы запустить в режиме **RecoverServer, выполните следующее** :

  - на сервере не должно быть установленной службы Exchange;
  - в Active Directory должен существовать объект сервера Exchange;
  - можно использовать только автоматическую установку.

Примечание

Чтобы перейти в другой режим программы установки, следует завершить работу с текущим режимом.

Требования к системе для Exchange Server

Статья • 11.02.2025

Перед установкой Exchange Server 2019 мы рекомендуем ознакомиться с этим разделом, чтобы убедиться, что сеть, оборудование, программное обеспечение, клиенты и другие элементы соответствуют требованиям Exchange 2019. Кроме того, убедитесь, что вы понимаете сценарии сосуществования, поддерживаемые для Exchange 2019 и более ранних версий Exchange.

> **Примечание**
>
> Для Exchange Server 2019 установок в китайском регионе установите обновление безопасности Exchange Server августа 2019 г. (или более поздней версии), чтобы включить расширенную поддержку символов.

Сведения об установке Exchange 2019 см. в статье Развертывание новых установок Exchange.

Поддерживаемые сценарии сосуществования для Exchange 2019

Поддерживаемые сценарии сосуществования между Exchange 2019 и более ранними поддерживаемыми версиями Exchange Server описаны в следующей таблице:

Развернуть таблицу

Версия Exchange	Сосуществование организации Exchange 2019
Exchange 2016	Поддерживается для Exchange 2016 с накопительным пакетом обновления CU11 или более поздней версии на всех серверах Exchange 2016 в организации, в том числе пограничных транспортных серверах.

Поддерживаемые сценарии гибридных развертываний для Exchange 2019

Exchange 2019 поддерживает гибридные развертывания с организациями Microsoft 365. Дополнительные сведения о гибридных развертываниях см. в разделе Hybrid Deployment Prerequisites.

Требования к сети и серверам каталогов для Exchange 2019

В таблице ниже приведены требования к сети и серверам каталогов в организации Exchange 2019.

Развернуть таблицу

Компонент	Требования
Контроллеры доменов	Все контроллеры домена в лесу должны работать под управлением одной из поддерживаемых версий Windows Server. Полный список поддерживаемых операционных систем контроллера домена можно найти в матрице поддержки Exchange Server.
Лес Active Directory	Полный список поддерживаемых функциональных уровней леса можно найти в матрице поддержки Exchange Server.
Сайт Active Directory	Сайт Active Directory, на котором устанавливается Exchange Server, должен содержать по крайней мере один записываемый контроллер домена, который также является сервером глобального каталога. В противном случае установка завершится ошибкой. Кроме того, нельзя установить сервер Exchange Server, а затем удалить контроллер домена с сайта Active Directory.
Пространство имен DNS	Exchange 2019 поддерживает следующие пространства имен DNS: • Смежные • Несмежные • Одноуровневые домены • Несвязанные Дополнительные сведения о пространствах имен DNS, которые поддерживает Exchange, см. в статье KB2269838.
IPv6	Exchange 2019 поддерживает протокол IPv6 только в том случае, если IPv4 также установлен и включен на сервере Exchange Server. Если вы развертываете Exchange в этой конфигурации и ваша сеть поддерживает IPv4 и IPv6, все серверы Exchange могут отправлять и получать данные с устройств, серверов и клиентов, использующих IPv6-адреса. Дополнительные сведения см. в статье IPv6 Support in Exchange 2013.

Архитектура сервера каталогов для Exchange 2019

Контроллеры домена Active Directory на 64-разрядном оборудовании с 64-разрядной версией Windows Server повысят производительность службы каталогов для Exchange 2019.

Установка Exchange 2019 на серверах каталогов

По соображениям безопасности и производительности не рекомендуется устанавливать Exchange 2019 на серверах Active Directory. Установите Exchange 2019 только на рядовые серверы.

Дополнительные сведения о проблемах, с которыми вы столкнетесь при установке Exchange на сервере каталогов, см. в статье Установка Exchange на контроллере домена не рекомендуется [WarningInstallExchangeRolesOnDomainController]. После установки Exchange изменение роли сервера с рядового сервера на сервер каталогов или наоборот не поддерживается.

Требования к оборудованию для Exchange 2019

Сведения о том, как выполнить развертывание Exchange в виртуальной среде, см. в статье Виртуализация Exchange Server.

Развернуть таблицу

Компонент	Требования	Примечания
Процессор	Один из следующих типов 64-разрядных процессоров: • Процессор Intel, поддерживающий технологию Intel 64 (прежнее название — Intel EM64T). • Процессор AMD, поддерживающий платформу AMD64. **Примечания**. • Процессоры Intel Itanium IA64 не поддерживаются.	Сведения о поддерживаемых операционных системах см. в разделе Поддерживаемые операционные системы для Exchange 2019 далее в этом разделе.

Компонент	Требования	Примечания
	• На физических компьютерах рекомендуется использовать до 2 сокетов процессора.	
Память	Зависит от роли сервера Exchange: • **Сервер почтовых ящиков** (рекомендуется не менее 128 ГБ). • **Пограничный транспортный сервер** (рекомендуется не менее 64 ГБ).	Exchange 2019 поддерживает большой размер памяти (до 256 ГБ).
Размер файла подкачки	Задайте одинаковый минимальный и максимальный размер файла подкачки: 25 % от установленной памяти.	Нет
Дисковое пространство	• Как минимум 30 ГБ свободного места на диске, на котором устанавливаете Exchange. • Как минимум 200 МБ свободного дискового пространства на системном диске. • Как минимум 500 МБ свободного места на диске, на котором хранится база данных очереди сообщений.	Нет
Разрешение экрана	1024 x 768 пикселей (XGA) или выше	Нет
Файловая система	**NTFS**. Требуется для разделов, содержащих следующие типы файлов: • Системный раздел. • Двоичные файлы Exchange. • Файлы, созданные при ведении журнала диагностики Exchange. • Файлы базы данных транспорта (например, базы данных очереди почты).	Нет

Компонент	Требования	Примечания
	ReFS. Поддерживается для разделов, содержащих следующие типы файлов Exchange: • Базы данных почтовых ящиков. • Журналы транзакций. • Файлы транспортной базы данных (например, база данных очереди почты) .	

Поддерживаемые операционные системы для Exchange 2019

Полный список поддерживаемых операционных систем можно найти в матрице поддержки Exchange Server.

Поддерживаемые версии PowerShell для серверов Exchange 2019

Серверы Exchange 2019 поддерживают версию PowerShell, включенную в выпуск Windows Server, где установлен Exchange. Не устанавливайте автономные загрузки Windows Management Framework (WMF) или PowerShell на серверах Exchange.

Установка другого программного обеспечения на серверах Exchange 2019

Установка клиентского и серверного программного обеспечения Office на серверах Exchange (например, SharePoint Server, Skype для бизнеса Server, Office Online Server или Project Server) не поддерживается. Другое программное обеспечение, которое необходимо установить на сервере Exchange 2019, должно работать на том же компьютере, что и Exchange Server.

Поддерживаемые версии .NET Framework для Exchange 2019

Рекомендуется использовать последнюю версию платформа .NET Framework, поддерживаемую устанавливаемым выпуском Exchange.

Полный список поддерживаемых версий платформа .NET Framework можно найти в матрице поддержки Exchange Server.

Поддерживаемые клиенты (с последними обновлениями) в Exchange 2019

Полный список поддерживаемых почтовых клиентов можно найти в матрице поддержки Exchange Server.

Интеграция Lync или Skype для бизнеса Server с Exchange 2019

Если вы интегрируете функции присутствия и обмена мгновенными сообщениями Lync с Exchange Server, требуется Lync Server 2013 с накопительным пакетом обновления 10 или более поздней версии. Если вы интегрируете функции присутствия и обмена мгновенными сообщениями Skype для бизнеса с Exchange Server, требуется Skype для бизнеса Server с накопительным пакетом обновления 7 или более поздней версии.

Сторонние клиенты Exchange

Exchange Server предлагает несколько известных протоколов и публикует API, для которых сторонние поставщики часто пишут клиенты.

Майкрософт не дает никаких гарантий, ни явно выраженных, ни подразумеваемых, в отношении общего соответствия, пригодности, совместимости или безопасности создаваемых сторонними разработчиками клиентов.

Если вы хотите использовать сторонний клиент, который использует наши протоколы или API, мы рекомендуем тщательно изучить и проверить все рекомендации (функциональные возможности, безопасность, обслуживание, управление и т. д.) перед развертыванием клиента в рабочей области предприятия. Мы также рекомендуем убедиться, что сторонний поставщик предлагает соответствующее соглашение о поддержке Enterprise (ESA).

Предварительные требования для Exchange Server

Статья • 11.02.2025

Обзор

В этой статье приведены шаги для выполнения всех необходимых предварительных требований к операционной системе Windows Server для установки серверов почтовых ящиков и пограничных транспортных серверов Exchange Server 2016 и Exchange Server 2019, а также предварительных требований к Windows для установки средств управления Exchange на клиентских компьютерах с ОС Windows.

Подготовив среду для Exchange Server, используйте помощник по развертыванию Microsoft Exchange Server для дальнейших действий в фактическом развертывании. Сведения о гибридных развертываниях см. в разделе Exchange Server гибридных развертываний.

Сведения о фактической установке Exchange Server см. в статье Развертывание новых установок Exchange.

Что нужно знать перед началом работы

В этом разделе содержатся исчерпывающие рекомендации и самые актуальные сведения о компонентах, необходимых для Exchange Server. Эти компоненты являются необходимыми предварительными условиями для правильной работы Exchange Server.

- Убедитесь, что служба Active Directory соответствует требованиям к Exchange 2016 или Exchange 2019.
- Чтобы обеспечить совместимость и оптимальную производительность, обязательно используйте поддерживаемые операционные системы для Exchange Server.
- Перед установкой Exchange Server убедитесь, что на компьютере установлены последние обновления Windows.
- Служба удаленного реестра должна иметь значение `Automatic` и не должна иметь значение `Disabled`. Рекомендации по безопасности см. в статье

Рекомендации по безопасности, касающиеся удаленного реестра.

Windows Server предварительные требования для Exchange 2019

Требования к установке Exchange 2019 в поддерживаемых операционных системах (ОС) описаны в следующих разделах. Для установки необходимых компонентов Windows для Exchange 2019 рекомендуется использовать один из следующих методов:

- `/InstallWindowsComponents` Используйте параметр в режиме автоматической установки.
- Установите флажок в мастере установки Exchange, чтобы выполнить предварительные условия в отношении Windows.

Если вы используете один из указанных ниже вариантов, не нужно перезагружать компьютер после добавления компонентов Windows.

Подготовка Active Directory в Exchange 2019

Вы можете использовать любой рядовой сервер из домена Active Directory для подготовки Active Directory к Exchange 2019. Чтобы подготовить Active Directory с помощью графического пользовательского интерфейса (GUI), необходимо установить роль Средства управления Exchange.

1. Компьютеру, который используется для подготовки Active Directory, требуется следующее программное обеспечение:

   a. Поддерживаемая версия платформа .NET Framework

      При установке на Windows Server Core необходимо использовать `/q` параметр для установки этого пакета. Кроме того, можно использовать параметр для `/log [PATH]` включения ведения журнала при необходимости.

   b. Распространяемый пакет Visual C++ для Visual Studio 2012

      Если вы используете автоматическую установку из командной строки для подготовки Active Directory, этот пакет не требуется. Общие сведения о последних поддерживаемых версиях и дополнительные сведения см. в статье Подготовка Active Directory и доменов.

Требования к системе для пакета Распространяемый компонент Visual C++ явно не упоминание поддержку последних версий Windows Server. Однако распространяемый пакет безопасен для установки в этих версиях Windows.

2. Установите средства удаленного администрирования сервера (RSAT) для доменные службы Active Directory (ADDS), выполнив следующую команду в Windows PowerShell:

```
PowerShell

Install-WindowsFeature RSAT-ADDS
```

Средства управления Exchange 2019

1. Установите следующее программное обеспечение:

   a. Поддерживаемая версия платформа .NET Framework

   b. Распространяемый пакет Visual C++ для Visual Studio 2012

   Требования к системе для пакета Распространяемый компонент Visual C++ явно не упоминание поддержку последних версий Windows Server. Однако распространяемый пакет безопасен для установки в этих версиях Windows.

2. Установите следующие компоненты Windows:
   a. Если вы хотите установить средства управления Exchange Server в поддерживаемой ОС Windows Server, обязательно установите следующие компоненты Windows:

```
PowerShell

Install-WindowsFeature -Name Web-Mgmt-Console, Web-Metabase
```

   b. Если вы хотите установить средства управления Exchange Server в поддерживаемой клиентской ОС Windows, обязательно установите следующие компоненты Windows:

```
PowerShell

Enable-WindowsOptionalFeature -Online -FeatureName IIS-
ManagementConsole, IIS-Metabase -All
```

Роль сервера почтовых ящиков Exchange 2019

1. Установите следующее программное обеспечение:

    a. Поддерживаемая версия платформа .NET Framework

    При установке на Windows Server Core необходимо использовать `/q` параметр для установки этого пакета. Кроме того, можно использовать параметр для `/log [PATH]` включения ведения журнала при необходимости.

    b. Распространяемый пакет Visual C++ для Visual Studio 2012

    c. Пакет Распространяемый компонент Visual C++ для Visual Studio 2013

    Требования к системе для пакета Распространяемый компонент Visual C++ явно не упоминание поддержку последних версий Windows Server. Однако распространяемый пакет безопасен для установки в этих версиях Windows.

2. Добавьте необходимые компоненты Skype для бизнеса Server:

    a. Установите компонент Windows Server Media Foundation, выполнив следующую команду в Windows PowerShell:

    ```
    PowerShell

    Install-WindowsFeature Server-Media-Foundation
    ```

    b. Установите Управляемый API Unified Communications 4.0. Этот пакет доступен для скачивания и находится в папке `\UCMARedist` на Exchange Server носителе.

    При установке на Windows Server Core необходимо использовать пакет установки, расположенный в `\UCMARedist` на распределенном носителе. Чтобы установить пакет с помощью PowerShell, выполните следующую команду:

    ```
    PowerShell

    .\UCMARunTimeSetup.exe -q
    ```

3. Если вы не собираетесь использовать программу установки Exchange для установки необходимых компонентов Windows (в мастере или из командной строки), выполните одну из указанных ниже команд в Windows PowerShell.
    a. Возможности Windows:
        i. Работа с рабочими столами:

PowerShell

```
Install-WindowsFeature Server-Media-Foundation, NET-Framework-45-Core, NET-Framework-45-ASPNET, NET-WCF-HTTP-Activation45, NET-WCF-Pipe-Activation45, NET-WCF-TCP-Activation45, NET-WCF-TCP-PortSharing45, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-Clustering-Mgmt, RSAT-Clustering-PowerShell, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity-Foundation, RSAT-ADDS
```

ii. Server Core:

PowerShell

```
Install-WindowsFeature Server-Media-Foundation, NET-Framework-45-Core, NET-Framework-45-ASPNET, NET-WCF-HTTP-Activation45, NET-WCF-Pipe-Activation45, NET-WCF-TCP-Activation45, NET-WCF-TCP-PortSharing45, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-Clustering-PowerShell, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Metabase, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, RSAT-ADDS
```

iii. (Необязательно) Удаление MSMQ. Компонент Windows Message Queuing (MSMQ) больше не является обязательным для Exchange Server и может быть безопасно удален, если он установлен в настоящее время:

PowerShell

```
Remove-WindowsFeature NET-WCF-MSMQ-Activation45, MSMQ
```

b. Модуль перезаписи URL-адресов IIS

Роль пограничного транспортного сервера Exchange 2019

1. Установите следующее программное обеспечение:

   a. Поддерживаемая версия платформа .NET Framework

При установке на Windows Server Core необходимо использовать `/q` параметр для установки этого пакета. Кроме того, можно использовать параметр для `/log [PATH]` включения ведения журнала при необходимости.

b. Распространяемый пакет Visual C++ для Visual Studio 2012

Требования к системе для пакета Распространяемый компонент Visual C++ явно не упоминание поддержку последних версий Windows Server. Однако распространяемый пакет безопасен для установки в этих версиях Windows.

2. Если вы не собираетесь использовать программу установки Exchange для установки необходимых компонентов Windows (в мастере или из командной строки), выполните указанную ниже команду в Windows PowerShell.

```
PowerShell

Install-WindowsFeature ADLDS
```

Установка Office Online Server в организации Exchange

Статья • 04.04.2023

Необязательным предварительным условием для Exchange 2016 с накопительным пакетом обновления 1 (CU1) или более поздней версии, а также для Exchange 2019 является установка Office Online Server на одном или нескольких серверах в организации. Office Online Server позволяет пользователям просматривать поддерживаемые вложения файлов в Outlook в Интернете (ранее — Outlook Web App) без предварительного скачивания и локальной установки программы. Если вы не установите Office Online Server, пользователям Outlook придется скачивать вложения на локальные компьютеры и открывать их в локальном приложении.

> ⓘ **Примечание**
>
> Продукт Office Online Server доступен для скачивания в рамках соглашения о корпоративном лицензировании. Если у вас нет соглашения о корпоративном лицензировании, вы можете пропустить инструкции на этом шаге. Если вы не установите Office Online Server, пользователям Outlook придется скачивать вложения на компьютер; они не смогут просматривать их в Outlook.

Конечную точку Office Online Server можно настроить в двух местах в Exchange 2016 и более поздних версиях: на уровне организации и на уровне сервера почтовых ящиков. Выбор зависит от размера организации и расположения серверов и пользователей.

- **Организация**. Ниже указана пара причин, по которым может потребоваться настроить конечную точку Office Online Server на уровне организации.
    - **Развертывание на одном сервере или в одном расположении**. Конечную точку можно настроить на уровне организации, если все серверы почтовых ящиков Exchange 2016 расположены в одном и том же расположении, а вы не планируете распределять серверы Office Online Server по разным географическим областям.
    - **Резервный вариант для крупных развертываний**. Вы можете настроить конечную точку на уровне организации в качестве резервной, если конечная точка, настроенная на сервере почтовых ящиков, недоступна. Если сервер Office веб-приложения недоступен, клиент попытается подключиться к конечной точке, настроенной на уровне организации.

Примечания.

- Если в вашей организации есть серверы Exchange 2013, не настраивайте конечную точку на уровне организации. Если сделать это, серверы Exchange 2013 будут пытаться подключиться к серверу Office Online Server. Эта функция не поддерживается.
- Office Online Server не поддерживает предварительный просмотр вложений в сообщениях S/MIME в Outlook в Интернете.

- **Сервер почтовых ящиков**. Если вы хотите распределить клиентские запросы между двумя или более Office Online Server серверами, если вы хотите географически распределить Office Online Server серверах или если у вас есть Exchange 2013 в организации, настройте конечные точки на уровне сервера почтовых ящиков Exchange. При настройке конечной точки на уровне сервера почтовые ящики, расположенные на этом сервере, будут отправлять запросы на настроенный сервер Office Online Server.

Чтобы пользователи вне вашей сети могли просматривать поддерживаемые вложения в Outlook, Office Online Server должен быть доступен из Интернета. Необходимо открыть TCP-порт 443 в брандмауэре и переадресовать его на сервер Office Online Server. Если развернуто более одного сервера Office Online Server, у каждого из них должно быть собственное полное доменное имя (FQDN). Каждый сервер также должен быть доступен из Интернета через TCP-порт 443.

Требования к системе для Office Online Server

Для настройки Office Online Server необходимы:

- Windows Server 2012 R2 или Windows Server 2016
- Exchange 2016 с накопительным пакетом обновления 1 (CU1) или более поздней версии или Exchange 2019

  > ⓘ **Примечание**
  >
  > Если вы используете Windows Server 2016, вам потребуется Exchange 2016 с накопительным пакетом обновления 3 (CU3) или более поздней версии, как описано в статье **Предварительные требования для Exchange Server**.

- Microsoft .NET Framework 4.5.2

- Распространяемый компонент Visual C++ для Visual Studio 2015
- Распространяемые пакеты Visual C++ для Visual Studio 2013
- Microsoft.IdentityModel.Extention.dll
- все доступные обновления Windows.

> ⓘ **Примечание**
>
> Office Online Server невозможно установить на сервере Exchange Server, сервере SharePoint Server, контроллере домена Active Directory или другом компьютере, на котором уже установлены приложения.

Установка Office Online Server

1. Чтобы установить Office Online Server, сначала выполните шаги 1–3, описанные в разделе **Подготовка серверов для запуска Office Online Server** статьи Развертывание Office Online Server.

2. Получите и импортируйте SSL-сертификат с полными доменными именами сервера Office Online Server. Если ваша организация использует разделенную конфигурацию DNS, в сертификате необходимо задать одно полное доменное имя. Например, oos.contoso.com. Если внутренние и внешние полные доменные имена различаются, в сертификате необходимо задать оба имени. Например, oos.internal.contoso.com и oos.contoso.com.

3. Настройте записи DNS так, чтобы полные доменные имена сертификата указывали на Office Online Server. Если вы используете разные DNS-серверы для внутренних и внешних пользователей, на каждом сервере необходимо указать соответствующее полное доменное имя.

4. Откройте Windows PowerShell и выполните указанные ниже команды. При выполнении команд замените примеры полных доменных имен и понятного имени сертификата своими.

   PowerShell

   ```
   New-OfficeWebAppsFarm -InternalURL "https://oos.contoso.com" -
   ExternalURL "https://oos.contoso.com" -CertificateName "Office Online
   Server Preview Certificate"`
   ```

> ⓘ **Примечание**
>
> Вы можете настроить разные внутренние и внешние URL-адреса, но на следующем шаге вы увидите, что можно настроить только один URL-адрес для Exchange. В этом случае, если вы используете внутренний URL-адрес на следующем шаге, эта функция будет работать только внутри, и внешние пользователи получат непредвиденное сообщение об ошибке. Если вы используете внешний URL-адрес, эта функция будет работать только для внешних пользователей, а внутренние пользователи получат непредвиденное сообщение об ошибке.

Настройка конечной точки Office Online Server на уровне сервера почтовых ящиков

После того как вы настроили сервер Office Online Server, выполните указанные ниже действия на сервере Exchange 2016. Это позволит Outlook отправлять запросы на сервер Office Online Server.

1. Откройте командную консоль Exchange и выполните указанную ниже команду. Замените имя сервера и URL-адрес из примера на собственные.

```
PowerShell

Set-MailboxServer MBX -WacDiscoveryEndpoint
"https://oos.contoso.com/hosting/discovery"
```

2. Перезапустите MsExchangeOwaAppPool, выполнив следующую команду:

```
PowerShell

Restart-WebAppPool MsExchangeOwaAppPool
```

Настройка конечной точки Office Online Server на уровне организации

После того как вы настроили сервер Office Online Server, выполните указанные ниже действия на сервере Exchange 2016. Это позволит Outlook отправлять запросы на сервер Office Online Server.

1. Откройте командную консоль Exchange и выполните указанную ниже команду. Замените пример URL-адреса своим.

```
PowerShell

Set-OrganizationConfig -WacDiscoveryEndpoint
"https://oos.internal.contoso.com/hosting/discovery"
```

> ⓘ **Важно!**
>
> Если в вашей организации есть серверы Exchange 2013, не настраивайте конечную точку на уровне организации. Если сделать это, серверы Exchange 2013 будут пытаться подключиться к серверу Office Online Server. Эта функция не поддерживается.

2. Перезапустите MsExchangeOwaAppPool, выполнив указанную ниже команду.

```
PowerShell

Restart-WebAppPool MsExchangeOwaAppPool
```

Служба каталогов Active Directory в организациях Exchange Server

Статья • 04.04.2023

Exchange Server 2016 г. и Exchange Server 2019 г. используют Active Directory для хранения сведений о каталогах и совместного использования с Windows. Начиная с Exchange 2013, мы внесли некоторые изменения в работу Exchange с Active Directory. Эти изменения описаны в этом разделе.

Драйвер Active Directory

Драйвер Active Directory — это один из базовых компонентов сервера Microsoft Exchange, позволяющий службам Exchange создавать, изменять, удалять и запрашивать данные доменных служб Active Directory. В Exchange 2013 и более поздних версий весь доступ к Active Directory выполняется с помощью самого драйвера Active Directory. В предыдущих версиях Exchange возможность поиска в каталоге для таких компонентов, как SMTP, агент передачи сообщений (MTA) и хранилище Exchange обеспечивала служба DSAccess.

Драйвер Active Directory также использует сервер топологии Microsoft Exchange Active Directory (MSExchangeADTopology), который позволяет драйверу Active Directory использовать данные топологии доступа к службе каталогов (DSAccess). Эти данные включают список доступных контроллеров домена и серверов глобального каталога, доступных для обработки запросов Exchange. Дополнительные сведения о драйвере Active Directory см. в разделе доменные службы Active Directory.

Изменения схемы Active Directory

Exchange добавляет новые атрибуты в схему службы домена Active Directory, а также вносит другие изменения в существующие классы и атрибуты. Дополнительные сведения об изменениях Active Directory при установке Exchange см. в статье Изменения схемы Active Directory в Exchange Server.

Дополнительные сведения

Дополнительные сведения о том, как Exchange хранит и получает сведения в Active Directory и как можно планировать доступ к ним, см. в статье Доступ к Active

Directory в Exchange Server.

Дополнительные сведения о структуре леса Active Directory см. в руководстве по разработке для AD DS.

Дополнительные сведения о компьютерах с ОС Windows в домене Active Directory и развертывании Exchange 2013 или более поздней версии в домене, который имеет несвязанное пространство имен, см. в статье Сценарии несвязанных пространств имен.

Доступ серверов Exchange Server к Active Directory

Статья • 04.04.2023

Exchange Server 2016 г. и Exchange Server 2019 г. все сведения о конфигурации и получателях хранятся в базе данных службы каталогов Active Directory. Когда серверу Exchange server требуются сведения о получателях конфигурации организации Exchange, он запрашивает Active Directory. Серверы Active Directory должны быть доступны для правильной работы Exchange.

В этом разделе объясняется, как Exchange сохраняет и извлекает сведения в Active Directory, чтобы можно было спланировать доступ к Active Directory. В этом разделе также рассматриваются проблемы, о которых следует знать при попытке восстановить удаленные объекты Exchange Active Directory.

Данные Exchange, хранящиеся в службе Active Directory

База данных Active Directory хранит информацию в логических разделах трех типов, описанных далее:

- Раздел схемы
- Раздел конфигурации
- Раздел домена

Раздел схемы

Раздел схемы используется для хранения двух типов сведений:

- **Классы схемы** определяют все типы объектов, которые могут создаваться и храниться в Active Directory.
- **Атрибуты схемы** определяют все свойства, которые могут использоваться для описания объектов, хранящихся в Active Directory.

При установке первого сервера Exchange Server в лесу (или запуске процесса подготовки Active Directory) процесс подготовки Active Directory добавляет в схему Active Directory множество классов и атрибутов. Классы, добавленные в схему, используются для создания объектов Exchange (например, агентов и

соединителей). Эти атрибуты используются для настройки объектов Exchange, а также пользователей и групп с поддержкой почты. Эти атрибуты включают свойства, такие как параметры Outlook в Интернете (ранее известные как Outlook Web App).

Каждый контроллер домена и сервер глобального каталога в лесу содержит полную реплику раздела схемы.

Дополнительные сведения об изменении схемы в Exchange см. в статье Изменения схемы Active Directory в Exchange Server.

Раздел конфигурации

Раздел конфигурации используется для хранения сведений о конфигурации в масштабах леса. Эти сведения о конфигурации включают конфигурацию сайтов Active Directory, глобальные параметры Exchange, параметры транспорта, политики почтовых ящиков и абонентские группы единой системы обмена сообщениями. Каждый тип сведений о конфигурации хранится в контейнере раздела конфигурации. Сведения о конфигурации Exchange хранятся в подпапке внутри контейнера "Службы" раздела конфигурации. Типы сведений, хранящихся в этом контейнере, включают:

- Списки адресов
- Политики почтовых ящиков адресной книги
- Административные группы
- Параметры клиентского доступа
- Подключения
- Параметры мобильного почтового ящика
- Глобальные параметры
- Параметры мониторинга
- Системные политики
- Контейнер политик хранения
- Параметры транспорта

Каждый контроллер домена и сервер глобального каталога в лесу содержит полную реплику раздела конфигурации.

Раздел домена

Раздел домена используется для хранения информации в контейнерах по умолчанию и в подразделениях, создаваемых администратором Active Directory. В этих контейнерах содержатся объекты, относящиеся к домену. Эти данные включают объекты системы Exchange и сведения о компьютерах, пользователях и группах в домене. При установке Exchange Exchange обновляет объекты в этом разделе для поддержки функций Exchange. Эта функциональность влияет на хранение и использование сведений о получателях.

Каждый контроллер домена содержит полную реплику раздела домена, для которого он является удостоверяющим. Каждый сервер глобального каталога в лесу содержит подмножество сведений каждого раздела домена в лесу.

Доступ Exchange к данным в службе Active Directory

Exchange использует API Active Directory для доступа к информации, хранящейся в Active Directory. Эта служба считывает сведения из всех разделов Active Directory. Извлекаемые данные кэшируются и используются серверами Exchange для обнаружения расположения сайта Active Directory всех служб Exchange в организации.

Дополнительные сведения о топологии и обнаружении служб в Exchange 2013 или поздних версиях см. в разделе Планирование использования сайтов Active Directory для маршрутизации почты.

Exchange — это приложение с поддержкой сайта Active Directory, которое предпочитает взаимодействовать с серверами каталогов, расположенными на том же сайте, что и сервер Exchange Server, для оптимизации сетевого трафика. Каждый сервер Exchange должен взаимодействовать с Active Directory для получения сведений о получателях и других серверах Exchange. Серверы почтовых ящиков хранят сведения о конфигурации пользователей почтовых ящиков и хранилищах почтовых ящиков в Active Directory. Кроме того, сервер почтовых ящиков хранит в Active Directory сведения о протоколах клиентского доступа, транспортной службе, базах данных почтовых ящиков и т. д. Сервер почтовых ящиков отвечает за все действия с активными почтовыми ящиками на сервере.

По умолчанию при запуске Exchange Server он привязывается к случайно выбранному контроллеру домена и серверу глобального каталога на собственном сайте. Выбранные серверы каталогов можно просмотреть при помощи командлета

Get-ExchangeServer в командной консоли Exchange. С помощью **командлета Set-ExchangeServer** можно также настроить статический список контроллеров домена, к которым должен привязаться сервер Exchange 2016, или список контроллеров домена, которые следует исключить.

> ⓘ **Важно!**
>
> Сервер Exchange Server невозможно развернуть на сайте, который содержит исключительно серверы каталогов, доступных только для чтения.

Восстановление удаленных объектов Exchange

Корзина Active Directory позволяет минимизировать простои службы каталогов, а также сохранять и восстанавливать случайно удаленные объекты Active Directory без восстановления данных Active Directory из резервных копий, перезапуска доменных служб Active Directory (AD DS) или перезагрузки контроллеров домена.

Самое важное, что необходимо знать о восстановлении удаленных объектов Exchange, связанных с Active Directory, — это то, что объекты Exchange не могут существовать отдельно друг от друга. Например, при включении поддержки почты для пользователя выполняется расчет различных политик или ссылок на основе текущей конфигурации Exchange. При восстановлении удаленного объекта конфигурации Exchange или объекта получателя могут произойти две неполадки.

- Конфликты. Некоторые атрибуты Exchange должны быть **уникальными** в лесу. Например, все адреса электронной почты объекта с поддержкой почты (также известные как прокси-адреса) должны быть уникальными. Два разных объекта с поддержкой почты не могут иметь одинаковый адрес электронной почты. Active Directory не применяет уникальность прокси-адреса (средства администрирования Exchange проверяют уникальность). Политики адресов электронной почты Exchange также автоматически устраняют возможные конфликты в назначениях адресов прокси-серверов, основанных на определенных правилах. Таким образом, восстановление объекта пользователя Exchange может привести к конфликту с адресами прокси-сервера или другими атрибутами, которые должны быть уникальными.

- **Неправильные настройки**. В Exchange есть автоматические правила, которые назначают различные политики или параметры. Если пользователь удаляет получателя, а затем изменяет правила или политики, восстановление объекта

пользователя Exchange может привести к назначению пользователя неправильной политике (или даже несуществующей политике).

Следующие инструкции помогут минимизировать проблемы при восстановлении удаленных объектов, связанных с Exchange.

- Не восстанавливайте объект конфигурации Exchange, если он был удален с помощью средств управления Exchange. Вместо этого снова создайте объект с помощью средств управления Exchange (Центр администрирования Exchange или командная консоль Exchange).

- При удалении объекта конфигурации Exchange без использования средств управления Exchange, восстановите его как можно скорее. Чем больше административных изменений и изменений конфигурации будет внесено после удаления, тем больше вероятность того, что восстановление объектов приведет к неправильной настройке.

- При восстановлении удаленных получателей Exchange (контактов, пользователей или групп рассылки) внимательно отслеживайте возникновением конфликтов и ошибок, связанных с восстановленными объектами. Если политики Exchange или другие параметры конфигурации получателей были изменены после удаления, повторно примените текущие политики к восстановленным получателям, чтобы убедиться, что они настроены правильно.

Дополнительные сведения

Корзина Active Directory — пошаговое руководство

Знакомство с улучшениями центра администрирования Active Directory (уровень 100)

Усовершенствованное управление доменными службами Active Directory с использованием центра администрирования Active Directory (уровень 200)

Изменения схемы Active Directory в Exchange Server

Статья • 04.04.2023

В этом справочном разделе приводится сводка изменений схемы Active Directory, внесенных при установке Exchange Server 2016 или Exchange Server 2019 в организации. Дополнительные сведения об изменениях схемы Active Directory см. в LDF-файлах. LDF-файлы находятся в каталоге \Setup\Data\ в файлах установки Exchange.

Обновления схемы Exchange являются накопительными. Каждое накопительное обновление (CU) включает все изменения, которые были включены в предыдущие выпуски. Это означает, что при пропуске накопительного пакета обновления может потребоваться применить обновления схемы, даже если устанавливаемая cu-пакет обновления не содержит собственных изменений.

Установленный текущий выпуск Exchange 2019	**Устанавливаемый новый выпуск Exchange 2019**	**Требуются ли обновления схемы?**
Окончательная первоначальная версия	Накопительный пакет обновления 4 — Накопительный пакет обновления 9	**Да**, обновления схемы требуются. Нужно применить обновления схемы из накопительного пакета обновления 8 (CU8).
Накопительный пакет обновления 8	Накопительный пакет обновления 9 — Накопительный пакет обновления 11	**Да**, обновления схемы требуются. Нужно применить обновления схемы из накопительного пакета обновления 10 (CU10).

> ⓘ **Примечание**
>
> Изменения схемы Active Directory, описанные в этом разделе, могут применяться не ко всем выпускам версии Exchange 2019. Сведения об успешной подготовке Active Directory см. в разделе **Версии Exchange Active Directorystатьи Подготовка Active Directory и доменов для Exchange 2019**.

Изменения схемы Active Directory в Exchange 2019 CU13

В схему Active Directory в Exchange 2019 с накопительным пакетом обновления 13 (CU13) изменения не вносятся.

Изменения схемы Active Directory Exchange 2019 CU12

Никаких изменений в схему Active Directory в Exchange 2019 CU12 не вносится.

Изменения схемы Active Directory в накопительном пакете обновления 11 для Exchange 2019

Накопительный пакет обновления 11 (CU11) для Exchange 2019 не содержит изменений схемы Active Directory.

Изменения схемы Active Directory в накопительном пакете обновления 10 для Exchange 2019

В этом разделе перечислены изменения, внесенные в схему Active Directory при установке Exchange 2019 CU10. Он включает следующие подразделы:

- Классы, измененные в накопительном пакете обновления 10 для Exchange 2019

Классы, измененные в накопительном пакете обновления 10 для Exchange 2019

В этом разделе содержатся классы, измененные в накопительном пакете обновления 10 для Exchange 2019.

Класс	Изменение	Атрибут или класс
`ms-Exch-Storage-Group`	удаление: `possSuperiors`	`computer`

Изменения схемы Active Directory в накопительном пакете обновления 9 (CU9) для Exchange 2019

Накопительный пакет обновления 9 (CU9) для Exchange 2019 не содержит изменений схемы Active Directory.

Изменения схемы Active Directory в накопительном пакете обновления 8 (CU8) для Exchange 2019

В этом разделе описаны изменения, которые вносятся в схему Active Directory при установке накопительного пакета обновления 8 (CU8) для Exchange 2019. Он включает следующие подразделы:

- Классы, измененные в накопительном пакете обновления 8 (CU8) для Exchange 2019
- Атрибуты, добавленные в накопительном пакете обновления 8 (CU8) для Exchange 2019

Классы, измененные в накопительном пакете обновления 8 (CU8) для Exchange 2019

В этом разделе содержатся классы, измененные в накопительном пакете обновления 8 (CU8) для Exchange 2019.

Класс	Изменение	Атрибут или класс
`ms-Exch-Auth-Auth-Server`	добавление: `mayContain`	`msExchCoexistenceDomains`

Атрибуты, добавленные в накопительном пакете обновления 8 (CU8) для Exchange 2019

В этом разделе указаны атрибуты, добавленные в накопительном пакете обновления 8 (CU8) для Exchange 2019.

- ms-Exch-Coexistence-Domains

Изменения схемы Active Directory в накопительном пакете обновления 7 (CU7) для Exchange 2019

Накопительный пакет обновления 7 (CU7) для Exchange 2019 не содержит изменений схемы Active Directory.

Изменения схемы Active Directory в накопительном пакете обновления 6 (CU6) для Exchange 2019

Накопительный пакет обновления 6 (CU6) для Exchange 2019 не содержит изменений схемы Active Directory.

Изменения схемы Active Directory в накопительном пакете обновления 5 для Exchange 2019

Накопительный пакет обновления 5 (CU5) для Exchange 2019 не содержит изменений схемы Active Directory.

Изменения схемы Active Directory в накопительном пакете обновления 4 для Exchange 2019

Накопительный пакет обновления 4 (CU4) для Exchange 2019 не содержит изменений схемы Active Directory.

Изменения схемы Active Directory в накопительном пакете обновления 3 для Exchange 2019

Накопительный пакет обновления 3 (CU3) для Exchange 2019 не содержит изменений схемы Active Directory.

Изменения схемы Active Directory в накопительном пакете обновления 2 для Exchange 2019

Накопительный пакет обновления 2 (CU2) для Exchange 2019 не содержит изменений схемы Active Directory.

Изменения схемы Active Directory в накопительном пакете обновления 1 для Exchange 2019

Накопительный пакет обновления 1 (CU1) для Exchange 2019 не содержит изменений схемы Active Directory.

Однако сокращены разрешения Active Directory: объект AdminSDHolder в домене обновлен для удаления ACE "Разрешить", предоставляющего группе Exchange Trusted Subsystem право "Записать DACL" для наследуемых типов объектов Group. Дополнительные сведения см. в статье базы знаний 4490059.

Изменения схемы Active Directory в окончательной первоначальной версии Exchange 2019

В этом разделе перечислены изменения, внесенные в схему Active Directory при установке Exchange 2019 RTM. Он включает следующие подразделы:

- Классы, добавленные в окончательной первоначальной версии Exchange 2019
- Классы, измененные в окончательной первоначальной версии Exchange 2019
- Атрибуты, добавленные в окончательной первоначальной версии Exchange 2019
- Атрибуты глобального каталога, добавленные в окончательной первоначальной версии Exchange 2019
- Атрибуты, измененные в окончательной первоначальной версии Exchange 2019
- Идентификаторы объектов, добавленные в окончательной первоначальной версии Exchange 2019
- Индексированные атрибуты, добавленные в окончательной первоначальной версии Exchange 2019
- Наборы свойств, измененные в окончательной первоначальной версии Exchange 2019
- Идентификаторы MAPI, добавленные в окончательной первоначальной версии Exchange 2019
- Расширенные права, добавленные в окончательной первоначальной версии Exchange 2019

> **Примечание**
>
> В ознакомительной и окончательной первоначальной версиях Exchange 2019 используется одинаковая схема Active Directory.

Классы, добавленные в окончательной первоначальной версии Exchange 2019

Класс	Изменение
`Exch-Mapi-Virtual-Directory`	`ntdsSchemaAdd`
`Exch-Push-Notifications-App`	`ntdsSchemaAdd`
`ms-Exch-Account-Forest`	`ntdsSchemaAdd`

Класс	Изменение
`ms-Exch-ActiveSync-Device-Autoblock-Threshold`	`ntdsSchemaAdd`
`ms-Exch-Auth-Auth-Config`	`ntdsSchemaAdd`
`ms-Exch-Auth-Auth-Server`	`ntdsSchemaAdd`
`ms-Exch-Auth-Partner-Application`	`ntdsSchemaAdd`
`ms-Exch-Auth-Policy`	`ntdsSchemaAdd`
`ms-Exch-Client-Access-Rule`	`ntdsSchemaModify`
`ms-Exch-Config-Settings`	`ntdsSchemaAdd`
`ms-Exch-Encryption-Virtual-Directory`	`ntdsSchemaAdd`
`ms-Exch-Exchange-Transport-Server`	`ntdsSchemaAdd`
`ms-Exch-Hosted-Content-Filter-Config`	`ntdsSchemaAdd`
`ms-Exch-Http-Delivery-Connector`	`ntdsSchemaAdd`
`ms-Exch-Hygiene-Configuration`	`ntdsSchemaAdd`
`ms-Exch-Intra-Organization-Connector`	`ntdsSchemaModify`
`ms-Exch-Mailbox-Policy`	`ntdsSchemaAdd`
`ms-Exch-Mailflow-Policy`	`ntdsSchemaAdd`
`ms-Exch-Mailflow-Policy-Collection`	`ntdsSchemaAdd`
`ms-Exch-Malware-Filter-Config`	`ntdsSchemaAdd`
`ms-Exch-MSO-Forward-Sync-Divergence`	`ntdsSchemaAdd`
`ms-Exch-MSO-Sync-Service-Instance`	`ntdsSchemaAdd`
`ms-Exch-Organization-Upgrade-Policy`	`ntdsSchemaAdd`
`ms-Exch-Protocol-Cfg-SIP-Container`	`ntdsSchemaAdd`
`ms-Exch-Protocol-Cfg-SIP-FE-Server`	`ntdsSchemaAdd`
`ms-Exch-Resource-Policy`	`ntdsSchemaAdd`
`ms-Exch-Safe-Attachment-Protection-Config`	`ntdsSchemaAdd`
`ms-Exch-Smart-Links-Protection-Config`	`ntdsSchemaAdd`
`ms-Exch-Team-Mailbox-Provisioning-Policy`	`ntdsSchemaAdd`
`ms-Exch-Throttling-Policy`	`ntdsSchemaModify`
`ms-Exch-Unified-Policy`	`ntdsSchemaAdd`

Класс	Изменение
`ms-Exch-Unified-Rule`	`ntdsSchemaAdd`
`ms-Exch-Workload-Policy`	`ntdsSchemaAdd`

Классы, измененные в окончательной первоначальной версии Exchange 2019

Класс	Изменение	Атрибут или класс
`Mail-Recipient`	добавление: `mayContain`	`msExchAdministrativeUnitLink`
`Mail-Recipient`	добавление: `mayContain`	`msExchAuthPolicyLink`
`Mail-Recipient`	добавление: `mayContain`	`msExchImmutableSid`
`Mail-Recipient`	добавление: `mayContain`	`msExchUGEventSubscriptionLink`
`ms-Exch-Base-Class`	добавление: `mayContain`	`msExchUserHoldPolicies`
`ms-Exch-Configuration-Unit-Container`	добавление: `mayContain`	`msExchAuthPolicyLink`
`ms-Exch-Configuration-Unit-Container`	добавление: `mayContain`	`msExchMSOForwardSyncReplayList`
`ms-Exch-Container`	добавление: `mayContain`	`msExchScopeFlags`
`ms-Exch-Mail-Storage`	добавление: `mayContain`	`msExchDataEncryptionPolicyLink`
`ms-Exch-Organization-Container`	добавление: `mayContain`	`msExchDataEncryptionPolicyLink`
`Exch-Accepted-Domain`	добавление: `mayContain`	`msExchOfflineOrgIdHomeRealmRecord`
`Exch-Base-Class`	добавление: `mayContain`	`msExchCapabilityIdentifiers`
`Exch-Base-Class`	добавление: `mayContain`	`msExchObjectID`
`Exch-Base-Class`	добавление: `mayContain`	`msExchProvisioningTags`
`Exch-Configuration-Unit-Container`	добавление: `mayContain`	`msExchArchiveRelease`
`Exch-Configuration-Unit-Container`	добавление: `mayContain`	`msExchMailboxRelease`

Класс	Изменение	Атрибут или класс
`Exch-Exchange-Server`	добавление: `mayContain`	`msExchArchiveRelease`
`Exch-Exchange-Server`	добавление: `mayContain`	`msExchMailboxRelease`
`Exch-MDB-Availability-Group`	добавление: `mayContain`	`msExchEvictedMembersLink`
`Exch-OAB`	добавление: `mayContain`	`msExchLastUpdateTime`
`Exch-OWA-Mailbox-Policy`	добавление: `mayContain`	`msExchConfigurationXML`
`Exch-OWA-Virtual-Directory`	добавление: `mayContain`	`msExchConfigurationXML`
`Exch-On-Premises-Organization`	добавление: `mayContain`	`msExchTrustedDomainLink`
`Exch-Organization-Container`	добавление: `mayContain`	`msExchMaxABP`
`Exch-Organization-Container`	добавление: `mayContain`	`msExchMaxOAB`
`Exch-Organization-Container`	добавление: `mayContain`	`pFContacts`
`Exch-Team-Mailbox-Provisioning-Policy`	добавление: `mayContain`	`msExchConfigurationXML`
`Group`	добавление: `auxiliaryClass`	`msExchMailStorage`
`Mail-Recipient`	добавление: `mayContain`	`msExchLocalizationFlags`
`Mail-Recipient`	добавление: `mayContain`	`msExchRoleGroupType`
`Mail-Recipient`	добавление: `mayContain`	`ms-DS-GeoCoordinates-Altitude`
`Mail-Recipient`	добавление: `mayContain`	`ms-DS-GeoCoordinates-Latitude`
`Mail-Recipient`	добавление: `mayContain`	`ms-DS-GeoCoordinates-Longitude`
`Mail-Recipient`	добавление: `mayContain`	`msExchRecipientSoftDeletedStatus`
`Mail-Recipient`	добавление: `mayContain`	`msExchWhenSoftDeletedTime`
`Mail-Recipient`	добавление: `mayContain`	`msExchHomeMTASL`
`Mail-Recipient`	добавление: `mayContain`	`msExchMailboxMoveSourceArchiveMDBLinkSL`
`Mail-Recipient`	добавление: `mayContain`	`msExchMailboxMoveSourceMDBLinkSL`
`Mail-Recipient`	добавление: `mayContain`	`msExchMailboxMoveTargetArchiveMDBLinkSL`

Класс	Изменение	Атрибут или класс
`Mail-Recipient`	добавление:`mayContain`	`msExchMailboxMoveTargetMDBLinkSL`
`Mail-Recipient`	добавление:`mayContain`	`ms-exch-group-external-member-count`
`Mail-Recipient`	добавление:`mayContain`	`ms-exch-group-member-count`
`Mail-Recipient`	добавление:`mayContain`	`msExchGroupExternalMemberCount`
`Mail-Recipient`	добавление:`mayContain`	`msExchGroupMemberCount`
`Mail-Recipient`	добавление:`mayContain`	`msExchShadowWhenSoftDeletedTime`
`Mail-Recipient`	добавление:`mayContain`	`msExchPublicFolderMailbox`
`Mail-Recipient`	добавление:`mayContain`	`msExchPublicFolderSmtpAddress`
`Mail-Recipient`	добавление: `mayContain`	`msExchAuxMailboxParentObjectIdLink`
`Mail-Recipient`	добавление: `mayContain`	`msExchStsRefreshTokensValidFrom`
`Mail-Recipient`	добавление:`mayContain`	`msDS-ExternalDirectoryObjectId`
`Mail-Recipient`	добавление:`mayContain`	`msExchGroupSecurityFlags`
`Mail-Recipient`	добавление:`mayContain`	`msExchMultiMailboxDatabasesLink`
`Ms-Exch-Organization-Container`	добавление:`mayContain`	`ms-exch-organization-flags-2`
`Top`	добавление:`mayContain`	`msExchMultiMailboxDatabasesBL`
`Top`	добавление:`mayContain`	`msExchMultiMailboxLocationsBL`
`Top`	добавление:`mayContain`	`msExchAccountForestBL`
`Top`	добавление:`mayContain`	`msExchTrustedDomainBL`
`Top`	добавление:`mayContain`	`msExchAcceptedDomainBL`
`Top`	добавление:`mayContain`	`msExchHygieneConfigurationMalwareBL`
`Top`	добавление:`mayContain`	`msExchHygieneConfigurationSpamBL`
`Top`	добавление:`mayContain`	`msExchEvictedMembersBL`
`Top`	добавление: `mayContain`	`msExchOABGeneratingMailboxBL`
`Top`	добавление: `mayContain`	`msExchAuxMailboxParentObjectIdBL`
`Top`	добавление: `mayContain`	`msExchAdministrativeUnitBL`

Класс	Изменение	Атрибут или класс
`Top`	добавление: `mayContain`	`msExchAuthPolicyBL`
`Top`	добавление: `mayContain`	`msExchDataEncryptionPolicyBL`
`Top`	добавление: `mayContain`	`msExchUGEventSubscriptionBL`
`ms-Exch-Accepted-Domain`	добавление: `mayContain`	`msExchHygieneConfigurationLink`
`ms-Exch-Accepted-Domain`	добавление: `mayContain`	`msExchTransportResellerSettingsLinkSL`
`ms-Exch-Account-Forest`	`possSuperiors`	`msExchContainer`
`ms-Exch-Account-Forest`	добавление: `mayContain`	`msExchPartnerId`
`ms-Exch-Active-Sync-Device`	добавление: `mayContain`	`msExchDeviceClientType`
`ms-Exch-Availability-Address-Space`	добавление: `mayContain`	`msExchFedTargetAutodiscoverEPR`
`ms-Exch-Base-Class`	добавление: `mayContain`	`msExchDirsyncAuthorityMetadata`
`ms-Exch-Base-Class`	добавление: `mayContain`	`msExchDirsyncStatusAck`
`ms-Exch-Base-Class`	добавление: `mayContain`	`msExchEdgeSyncConfigFlags`
`ms-Exch-Base-Class`	добавление: `mayContain`	`msExchHABRootDepaPreviewentLink`
`ms-Exch-Base-Class`	добавление: `mayContain`	`msExchDefaultPublicFolderMailbox`
`ms-Exch-Base-Class`	добавление: `mayContain`	`msExchForestModeFlag`
`ms-Exch-Base-Class`	добавление: `mayContain`	`msExchELCMailboxFlags`
`ms-Exch-Base-Class`	добавление: `mayContain`	`msExchCanaryData0`
`ms-Exch-Base-Class`	добавление: `mayContain`	`msExchCanaryData1`
`ms-Exch-Base-Class`	добавление: `mayContain`	`msExchCanaryData2`
`ms-Exch-Base-Class`	добавление: `mayContain`	`msExchCorrelationId`
`ms-Exch-Base-Class`	добавление: `mayContain`	`msExchTenantCountry`
`ms-Exch-Base-Class`	добавление: `mayContain`	`msExchConfigurationXML`
`ms-Exch-Base-Class`	добавление: `mayContain`	`msExchMultiMailboxGUIDs`

Класс	Изменение	Атрибут или класс
`ms-Exch-Base-Class`	добавление: `mayContain`	`msExchMultiMailboxLocationsLink`
`ms-Exch-Coexistence-Relationship`	добавление: `mayContain`	`msExchCoexistenceOnPremisesSmartHost`
`ms-Exch-Coexistence-Relationship`	добавление: `mayContain`	`msExchCoexistenceSecureMailCertificateThumbprint`
`ms-Exch-Coexistence-Relationship`	добавление: `mayContain`	`msExchCoexistenceTransportServers`
`ms-Exch-Configuration-Unit-Container`	добавление: `mayContain`	`msExchDirsyncStatus`
`ms-Exch-Configuration-Unit-Container`	добавление: `mayContain`	`msExchIsDirsyncStatusPending`
`ms-Exch-Configuration-Unit-Container`	добавление: `mayContain`	`msExchDirSyncServiceInstance`
`ms-Exch-Configuration-Unit-Container`	добавление: `mayContain`	`msExchOrganizationUpgradePolicyLink`
`ms-Exch-Configuration-Unit-Container`	добавление: `mayContain`	`msExchManagementSiteLinkSL`
`ms-Exch-Configuration-Unit-Container`	добавление: `mayContain`	`msExchOrganizationUpgradePolicyLinkSL`
`ms-Exch-Configuration-Unit-Container`	добавление: `mayContain`	`msExchRelocateTenantCompletionTargetVector`
`ms-Exch-Configuration-Unit-Container`	добавление: `mayContain`	`msExchRelocateTenantFlags`
`ms-Exch-Configuration-Unit-Container`	добавление: `mayContain`	`msExchRelocateTenantSafeLockdownSchedule`
`ms-Exch-Configuration-Unit-Container`	добавление: `mayContain`	`msExchRelocateTenantSourceForest`
`ms-Exch-Configuration-Unit-Container`	добавление: `mayContain`	`msExchRelocateTenantStartLockdown`
`ms-Exch-Configuration-Unit-Container`	добавление: `mayContain`	`msExchRelocateTenantStartRetired`
`ms-Exch-Configuration-Unit-Container`	добавление: `mayContain`	`msExchRelocateTenantStartSync`
`ms-Exch-Configuration-Unit-Container`	добавление: `mayContain`	`msExchRelocateTenantStatus`

Класс	Изменение	Атрибут или класс
`ms-Exch-Configuration-Unit-Container`	добавление:`mayContain`	`msExchRelocateTenantTargetForest`
`ms-Exch-Configuration-Unit-Container`	добавление:`mayContain`	`msExchRelocateTenantTransitionCounter`
`ms-Exch-Configuration-Unit-Container`	добавление:`mayContain`	`msExchSyncCookie`
`ms-Exch-Control-Point-Config`	добавление:`mayContain`	`msExchRMSOnlineCertificationLocationUrl`
`ms-Exch-Control-Point-Config`	добавление:`mayContain`	`msExchRMSOnlineKeySharingLocationUrl`
`ms-Exch-Control-Point-Config`	добавление:`mayContain`	`msExchRMSOnlineLicensingLocationUrl`
`ms-Exch-Custom-Attributes`	добавление:`mayContain`	`msExchExtensionCustomAttribute1`
`ms-Exch-Custom-Attributes`	добавление:`mayContain`	`msExchExtensionCustomAttribute2`
`ms-Exch-Custom-Attributes`	добавление:`mayContain`	`msExchExtensionCustomAttribute3`
`ms-Exch-Custom-Attributes`	добавление:`mayContain`	`msExchExtensionCustomAttribute4`
`ms-Exch-Custom-Attributes`	добавление:`mayContain`	`msExchExtensionCustomAttribute5`
`ms-Exch-Domain-Content-Config`	добавление:`mayContain`	`msExchContentByteEncoderTypeFor7BitCharsets`
`ms-Exch-Domain-Content-Config`	добавление:`mayContain`	`msExchContentPreferredInternetCodePageForShiftJis`
`ms-Exch-Domain-Content-Config`	добавление:`mayContain`	`msExchContentRequiredCharSetCoverage`
`ms-Exch-Exchange-Server`	добавление:`mayContain`	`msExchWorkloadManagementPolicyLink`
`ms-Exch-Exchange-Server`	добавление:`mayContain`	`msExchMalwareFilteringDeferAttempts`
`ms-Exch-Exchange-Server`	добавление:`mayContain`	`msExchMalwareFilteringDeferWaitTime`
`ms-Exch-Exchange-Server`	добавление:`mayContain`	`msExchMalwareFilteringFlags`

Класс	Изменение	Атрибут или класс
`ms-Exch-Exchange-Server`	добавление:`mayContain`	`msExchMalwareFilteringPrimaryUpdatePath`
`ms-Exch-Exchange-Server`	добавление:`mayContain`	`msExchMalwareFilteringSecondaryUpdatePath`
`ms-Exch-Exchange-Server`	добавление:`mayContain`	`msExchMalwareFilteringUpdateFrequency`
`ms-Exch-Exchange-Server`	добавление:`mayContain`	`msExchMalwareFilteringUpdateTimeout`
`ms-Exch-Exchange-Server`	добавление:`mayContain`	`msExchMalwareFilteringScanTimeout`
`ms-Exch-Fed-OrgId`	добавление:`mayContain`	`msExchFedDelegationTrustSL`
`ms-Exch-Hosted-Content-Filter-Config`	добавление:`mayContain`	`msExchSpamCountryBlockList`
`ms-Exch-Hosted-Content-Filter-Config`	добавление:`mayContain`	`msExchSpamLanguageBlockList`
`ms-Exch-Hosted-Content-Filter-Config`	добавление:`mayContain`	`msExchSpamNotifyOutboundRecipients`
`ms-Exch-Hosted-Content-Filter-Config`	добавление:`mayContain`	`msExchSpamDigestFrequency`
`ms-Exch-Hosted-Content-Filter-Config`	добавление:`mayContain`	`msExchSpamQuarantineRetention`
`ms-Exch-MDB`	добавление:`mayContain`	`msExchCalendarLoggingQuota`
`ms-Exch-MRS-Request`	добавление:`mayContain`	`msExchMailboxMoveSourceMDBLinkSL`
`ms-Exch-MRS-Request`	добавление:`mayContain`	`msExchMailboxMoveStorageMDBLinkSL`
`ms-Exch-MRS-Request`	добавление:`mayContain`	`msExchMailboxMoveTargetMDBLinkSL`
`ms-Exch-MSO-Sync-Service-Instance`	добавление:`mayContain`	`msExchMSOForwardSyncNonRecipientCookie`
`ms-Exch-MSO-Sync-Service-Instance`	добавление:`mayContain`	`msExchMSOForwardSyncRecipientCookie`
`ms-Exch-MSO-Sync-Service-Instance`	добавление:`mayContain`	`msExchMSOForwardSyncReplayList`
`ms-Exch-MSO-Sync-Service-Instance`	добавление:`mayContain`	`msExchAccountForestLink`

Класс	Изменение	Атрибут или класс
`ms-Exch-MSO-Sync-Service-Instance`	добавление: `mayContain`	`msExchActiveInstanceSleepInterval`
`ms-Exch-MSO-Sync-Service-Instance`	добавление: `mayContain`	`msExchPassiveInstanceSleepInterval`
`ms-Exch-MSO-Sync-Service-Instance`	добавление: `mayContain`	`msExchSyncDaemonMaxVersion`
`ms-Exch-MSO-Sync-Service-Instance`	добавление: `mayContain`	`msExchSyncDaemonMinVersion`
`ms-Exch-MSO-Sync-Service-Instance`	добавление: `mayContain`	`msExchSyncServiceInstanceNewTenantMaxVersion`
`ms-Exch-MSO-Sync-Service-Instance`	добавление: `mayContain`	`msExchSyncServiceInstanceNewTenantMinVersion`
`ms-Exch-Mail-Gateway`	добавление: `mayContain`	`msExchHomeMDBSL`
`ms-Exch-Mail-Gateway`	добавление: `mayContain`	`msExchHomeMTASL`
`ms-Exch-Mail-Storage`	добавление: `mayContain`	`msExchPreviousArchiveDatabase`
`ms-Exch-Mail-Storage`	добавление: `mayContain`	`msExchTeamMailboxExpiration`
`ms-Exch-Mail-Storage`	добавление: `mayContain`	`msExchTeamMailboxOwners`
`ms-Exch-Mail-Storage`	добавление: `mayContain`	`msExchTeamMailboxSharePointLinkedBy`
`ms-Exch-Mail-Storage`	добавление: `mayContain`	`msExchTeamMailboxSharePointUrl`
`ms-Exch-Mail-Storage`	добавление: `mayContain`	`msExchTeamMailboxShowInClientList`
`ms-Exch-Mail-Storage`	добавление: `mayContain`	`msExchCalendarLoggingQuota`
`ms-Exch-Mail-Storage`	добавление: `mayContain`	`msExchArchiveDatabaseLinkSL`
`ms-Exch-Mail-Storage`	добавление: `mayContain`	`msExchDisabledArchiveDatabaseLinkSL`
`ms-Exch-Mail-Storage`	добавление: `mayContain`	`msExchHomeMDBSL`
`ms-Exch-Mail-Storage`	добавление: `mayContain`	`msExchMailboxMoveTargetMDBLinkSL`
`ms-Exch-Mail-Storage`	добавление: `mayContain`	`msExchPreviousArchiveDatabaseSL`
`ms-Exch-Mail-Storage`	добавление: `mayContain`	`msExchPreviousHomeMDBSL`
`ms-Exch-Mail-Storage`	добавление: `mayContain`	`msExchMailboxContainerGuid`
`ms-Exch-Mail-Storage`	добавление: `mayContain`	`msExchUnifiedMailbox`

Класс	Изменение	Атрибут или класс
`ms-Exch-Mail-Storage`	добавление: `mayContain`	`msExchUserCulture`
`ms-Exch-Mailflow-Policy`	добавление: `mayContain`	`msExchImmutableId`
`ms-Exch-Malware-Filter-Config`	добавление: `mayContain`	`msExchMalwareFilterConfigExternalSenderAdminAddress`
`ms-Exch-Malware-Filter-Config`	добавление: `mayContain`	`msExchMalwareFilterConfigInternalSenderAdminAddress`
`ms-Exch-OAB`	добавление: `mayContain`	`msExchOffLineABServerSL`
`ms-Exch-OAB`	добавление: `mayContain`	`msExchOABGeneratingMailboxLink`
`ms-Exch-OWA-Mailbox-Policy`	добавление: `mayContain`	`msExchOWASetPhotoURL`
`ms-Exch-OWA-Virtual-Directory`	добавление: `mayContain`	`msExchOWASetPhotoURL`
`ms-Exch-Organization-Container`	добавление: `mayContain`	`msExchOrganizationFlags2`
`ms-Exch-Organization-Container`	добавление: `mayContain`	`msExchUMAvailableLanguages`
`ms-Exch-Organization-Container`	добавление: `mayContain`	`msExchWACDiscoveryEndpoint`
`ms-Exch-Organization-Container`	добавление: `mayContain`	`msExchAdfsAuthenticationRawConfiguration`
`ms-Exch-Organization-Container`	добавление: `mayContain`	`msExchServiceEndPointURL`
`ms-Exch-Private-MDB`	добавление: `mayContain`	`msExchMailboxDatabaseTransportFlags`
`ms-Exch-Public-Folder`	добавление: `mayContain`	`msExchPublicFolderEntryId`
`ms-Exch-Resource-Policy`	добавление: `mayContain`	`msExchCustomerExpectationCritical`
`ms-Exch-Resource-Policy`	добавление: `mayContain`	`msExchDiscretionaryCritical`
`ms-Exch-Resource-Policy`	добавление: `mayContain`	`msExchInternalMaintenanceCritical`
`ms-Exch-Resource-Policy`	добавление: `mayContain`	`msExchUrgentCritical`

Класс	Изменение	Атрибут или класс
`ms-Exch-Routing-Group-Connector`	добавление:`mayContain`	`msExchHomeMTASL`
`ms-Exch-Safe-Attachment-Protection-Config`	добавление:`mayContain`	`msExchMalwareFilterConfigFlags`
`ms-Exch-Safe-Attachment-Protection-Config`	добавление:`mayContain`	`msExchMalwareFilterConfigFromAddress`
`ms-Exch-Safe-Attachment-Protection-Config`	добавление:`mayContain`	`msExchMalwareFilterConfigInternalBody`
`ms-Exch-Safe-Attachment-Protection-Config`	добавление:`mayContain`	`msExchMalwareFilterConfigInternalSenderAdminAddress`
`ms-Exch-Safe-Attachment-Protection-Config`	добавление:`mayContain`	`msExchMalwareFilterConfigInternalSubject`
`ms-Exch-Safe-Attachment-Protection-Config`	добавление:`mayContain`	`msExchMalwareFilteringScanTimeout`
`ms-Exch-Safe-Attachment-Protection-Config`	добавление:`mayContain`	`msExchMalwareFilteringUpdateFrequency`
`ms-Exch-Site-Connector`	добавление:`mayContain`	`msExchHomeMTASL`
`ms-Exch-Smart-Links-Protection-Config`	добавление:`mayContain`	`msExchAddressRewriteExceptionList`
`ms-Exch-Smart-Links-Protection-Config`	добавление:`mayContain`	`msExchSpamFlags`
`ms-Exch-Tenant-Perimeter-Settings`	добавление:`mayContain`	`msExchTransportResellerSettingsLinkSL`
`ms-Exch-Throttling-Policy`	добавление:`mayContain`	`msExchThrottlingPolicyFlags`
`ms-Exch-Throttling-Policy`	добавление:`mayContain`	`msExchAnonymousThrottlingPolicyStateEx`
`ms-Exch-Throttling-Policy`	добавление:`mayContain`	`msExchEASThrottlingPolicyStateEx`
`ms-Exch-Throttling-Policy`	добавление:`mayContain`	`msExchEWSThrottlingPolicyStateEx`

Класс	Изменение	Атрибут или класс
`ms-Exch-Throttling-Policy`	добавление:`mayContain`	`msExchGeneralThrottlingPolicyStateEx`
`ms-Exch-Throttling-Policy`	добавление:`mayContain`	`msExchIMAPThrottlingPolicyStateEx`
`ms-Exch-Throttling-Policy`	добавление:`mayContain`	`msExchOWAThrottlingPolicyStateEx`
`ms-Exch-Throttling-Policy`	добавление:`mayContain`	`msExchPOPThrottlingPolicyStateEx`
`ms-Exch-Throttling-Policy`	добавление:`mayContain`	`msExchPowershellThrottlingPolicyStateEx`
`ms-Exch-Throttling-Policy`	добавление:`mayContain`	`msExchRCAThrottlingPolicyStateEx`
`ms-Exch-Transport-Rule`	добавление:`mayContain`	`msExchTransportRuleImmutableId`
`ms-Exch-Transport-Rule`	добавление:`mayContain`	`msExchImmutableId`
`ms-Exch-Transport-Settings`	добавление:`mayContain`	`msExchTranspoPreviewaxRetriesForLocalSiteShadow`
`ms-Exch-Transport-Settings`	добавление:`mayContain`	`msExchTranspoPreviewaxRetriesForRemoteSiteShadow`
`ms-Exch-Transport-Settings`	добавление:`mayContain`	`msExchConfigurationXML`
`ms-Exch-Virtual-Directory`	добавление:`mayContain`	`msExchMRSProxyFlags`
`ms-Exch-Virtual-Directory`	добавление:`mayContain`	`msExchMRSProxyMaxConnections`

Атрибуты, добавленные в окончательной первоначальной версии Exchange 2019

- `ms-DS-External-Directory-Object-Id`
- `ms-DS-GeoCoordinates-Altitude`
- `ms-DS-GeoCoordinates-Latitude`
- `ms-DS-GeoCoordinates-Longitude`
- `ms-Exch-Accepted-Domain-BL`
- `ms-Exch-Account-Forest-BL`
- `ms-Exch-Account-Forest-Link`
- `ms-Exch-ActiveSync-Device-AutoBlock-Duration`
- `ms-Exch-ActiveSync-Device-Autoblock-Threshold-Incidence-Duration`

- `ms-Exch-ActiveSync-Device-Autoblock-Threshold-Incidence-Limit`
- `ms-Exch-ActiveSync-Device-Autoblock-Threshold-Type`
- `ms-Exch-Adfs-Authentication-Raw-Configuration`
- `ms-Exch-Administrative-Unit-BL`
- `ms-Exch-Administrative-Unit-Link`
- `ms-Exch-Anonymous-Throttling-Policy-State-Ex`
- `ms-Exch-Archive-Database-Link-SL`
- `ms-Exch-Auth-Application-Identifier`
- `ms-Exch-Auth-App-Secret`
- `ms-Exch-Auth-Authorization-Url`
- `ms-Exch-Auth-Auth-Server-Type`
- `ms-Exch-Auth-Certificate-Data`
- `ms-Exch-Auth-Certificate-Thumbprint`
- `ms-Exch-Auth-Flags`
- `ms-Exch-Auth-Issuer-Name`
- `ms-Exch-Auth-Issuing-Url`
- `ms-Exch-Auth-Linked-Account`
- `ms-Exch-Auth-Metadata-Url`
- `ms-Exch-Auth-Policy-BL`
- `ms-Exch-Auth-Policy-Link`
- `ms-Exch-Auth-Realm`
- `ms-Exch-Aux-Mailbox-Parent-Object-Id-BL`
- `ms-Exch-Aux-Mailbox-Parent-Object-Id-Link`
- `ms-Exch-Canary-Data-0`
- `ms-Exch-Canary-Data-1`
- `ms-Exch-Canary-Data-2`
- `ms-Exch-Content-Byte-Encoder-Type-For-7-Bit-Charsets`
- `ms-Exch-Content-Preferred-Internet-Code-Page-For-Shift-Jis`
- `ms-Exch-Content-Required-Char-Set-Coverage`
- `ms-Exch-Correlation-Id`
- `ms-Exch-Customer-Expectation-Critical`
- `ms-Exch-Customer-Expectation-Overloaded`
- `ms-Exch-Customer-Expectation-Underloaded`
- `ms-Exch-Data-Encryption-Policy-BL`
- `ms-Exch-Data-Encryption-Policy-Link`
- `ms-Exch-Default-Public-Folder-Mailbox`
- `ms-Exch-Device-Client-Type`
- `ms-Exch-Dirsync-Authority-Metadata`
- `ms-Exch-Dir-Sync-Service-Instance`
- `ms-Exch-Dirsync-Status`
- `ms-Exch-Dirsync-Status-Ack`

- `ms-Exch-Disabled-Archive-Database-Link-SL`
- `ms-Exch-Discretionary-Critical`
- `ms-Exch-Discretionary-Overloaded`
- `ms-Exch-Discretionary-Underloaded`
- `ms-Exch-EAS-Throttling-Policy-State-Ex`
- `ms-Exch-Edge-Sync-Config-Flags`
- `ms-Exch-Encryption-Throttling-Policy-State-Ex`
- `ms-Exch-EWS-Throttling-Policy-State-Ex`
- `ms-Exch-Extension-Custom-Attribute-1`
- `ms-Exch-Extension-Custom-Attribute-2`
- `ms-Exch-Extension-Custom-Attribute-3`
- `ms-Exch-Extension-Custom-Attribute-4`
- `ms-Exch-Extension-Custom-Attribute-5`
- `ms-Exch-External-Directory-Object-Class`
- `ms-Exch-Fed-Delegation-Trust-SL`
- `ms-Exch-Forest-Mode-Flag`
- `ms-Exch-General-Throttling-Policy-State-Ex`
- `ms-Exch-Group-External-Member-Count`
- `ms-Exch-Group-Member-Count`
- `ms-Exch-Group-Security-Flags`
- `ms-Exch-Home-MDB-SL`
- `ms-Exch-Home-MTA-SL`
- `ms-Exch-Hosted-Content-Filter-Config-Link`
- `ms-Exch-Hygiene-Configuration-Link`
- `ms-Exch-Hygiene-Configuration-Malware-BL`
- `ms-Exch-Hygiene-Configuration-Spam-BL`
- `ms-Exch-IMAP-Throttling-Policy-State-Ex`
- `ms-Exch-Immutable-Sid`
- `ms-Exch-Internal-Maintenance-Critical`
- `ms-Exch-Internal-Maintenance-Overloaded`
- `ms-Exch-Internal-Maintenance-Underloaded`
- `ms-Exch-Is-Dirsync-Status-Pending,`
- `ms-Exch-Localization-Flags`
- `ms-Exch-Mailbox-Database-Transport-Flags`
- `ms-Exch-Mailbox-Move-Source-Archive-MDB-Link-SL`
- `ms-Exch-Mailbox-Move-Source-MDB-Link-SL`
- `ms-Exch-Mailbox-Move-Storage-MDB-Link-SL`
- `ms-Exch-Mailbox-Move-Target-Archive-MDB-Link-SL`
- `ms-Exch-Mailbox-Move-Target-MDB-Link-SL`
- `ms-Exch-Mailflow-Policy-Countries`
- `ms-Exch-Mailflow-Policy-Keywords`

- `ms-Exch-Mailflow-Policy-Publisher-Name`
- `ms-Exch-Mailflow-Policy-Transport-Rules-Template-Xml`
- `ms-Exch-Mailflow-Policy-Version`
- `ms-Exch-Malware-Filter-Config-Alert-Text`
- `ms-Exch-Malware-Filter-Config-External-Body`
- `ms-Exch-Malware-Filter-Config-External-Sender-Admin-Address`
- `ms-Exch-Malware-Filter-Config-External-Subject`
- `ms-Exch-Malware-Filter-Config-Flags`
- `ms-Exch-Malware-Filter-Config-From-Address`
- `ms-Exch-Malware-Filter-Config-From-Name`
- `ms-Exch-Malware-Filter-Config-Internal-Body`
- `ms-Exch-Malware-Filter-Config-Internal-Sender-Admin-Address`
- `ms-Exch-Malware-Filter-Config-Internal-Subject`
- `ms-Exch-Malware-Filter-Config-Link`
- `ms-Exch-Malware-Filtering-Defer-Attempts`
- `ms-Exch-Malware-Filtering-Defer-Wait-Time`
- `ms-Exch-Malware-Filtering-Flags`
- `ms-Exch-Malware-Filtering-Primary-Update-Path`
- `ms-Exch-Malware-Filtering-Scan-Timeout`
- `ms-Exch-Malware-Filtering-Secondary-Update-Path`
- `ms-Exch-Malware-Filtering-Update-Frequency`
- `ms-Exch-Malware-Filtering-Update-Timeout`
- `ms-Exch-Management-Site-Link-SL`
- `ms-Exch-MRS-Proxy-Flags`
- `ms-Exch-MRS-Proxy-Max-Connections`
- `ms-Exch-MSO-Forward-Sync-Divergence-Count`
- `ms-Exch-MSO-Forward-Sync-Divergence-Related-Object-Link`
- `ms-Exch-MSO-Forward-Sync-Divergence-Timestamp`
- `ms-Exch-Multi-Mailbox-Databases-BL`
- `ms-Exch-Multi-Mailbox-Databases-Link`
- `ms-Exch-Multi-Mailbox-GUID`
- `ms-Exch-Multi-Mailbox-Locations-BL`
- `ms-Exch-Multi-Mailbox-Locations-Link`
- `ms-Exch-OAB-Generating-Mailbox-BL`
- `ms-Exch-OAB-Generating-Mailbox-Link`
- `ms-Exch-Off-Line-AB-Server-SL`
- `ms-Exch-Organization-Flags-2`
- `ms-Exch-Organization-Upgrade-Policy-BL`
- `ms-Exch-Organization-Upgrade-Policy-Date`
- `ms-Exch-Organization-Upgrade-Policy-Enabled`
- `ms-Exch-Organization-Upgrade-Policy-Link`

- `ms-Exch-Organization-Upgrade-Policy-Link-SL`
- `ms-Exch-Organization-Upgrade-Policy-MaxMailboxes`
- `ms-Exch-Organization-Upgrade-Policy-Priority`
- `ms-Exch-Organization-Upgrade-Policy-Source-Version`
- `ms-Exch-Organization-Upgrade-Policy-Status`
- `ms-Exch-Organization-Upgrade-Policy-Target-Version`
- `ms-Exch-OWA-Set-Photo-URL`
- `ms-Exch-OWA-Throttling-Policy-State-Ex`
- `ms-Exch-POP-Throttling-Policy-State-Ex`
- `ms-Exch-Powershell-Throttling-Policy-State-Ex`
- `ms-Exch-Previous-Archive-Database`
- `ms-Exch-Previous-Archive-Database-SL`
- `ms-Exch-Previous-Home-MDB-SL`
- `ms-Exch-Public-Folder-EntryId`
- `ms-Exch-Public-Folder-Mailbox`
- `ms-Exch-Public-Folder-Smtp-Address`
- `ms-Exch-RCA-Throttling-Policy-State-Ex`
- `ms-Exch-Recipient-SoftDeleted-Status`
- `ms-Exch-Relocate-Tenant-Completion-Target-Vector`
- `ms-Exch-Relocate-Tenant-Flags`
- `ms-Exch-Relocate-Tenant-Safe-Lockdown-Schedule`
- `ms-Exch-Relocate-Tenant-Source-Forest`
- `ms-Exch-Relocate-Tenant-Start-Lockdown`
- `ms-Exch-Relocate-Tenant-Start-Retired`
- `ms-Exch-Relocate-Tenant-Start-Sync`
- `ms-Exch-Relocate-Tenant-Status`
- `ms-Exch-Relocate-Tenant-Target-Forest`
- `ms-Exch-Relocate-Tenant-Transition-Counter`
- `ms-Exch-Resource-Type`
- `ms-Exch-RMS-Computer-Accounts-Link-SL`
- `ms-Exch-RMSOnline-Certification-Location-Url`
- `ms-Exch-RMSOnline-Key-Sharing-Location-Url`
- `ms-Exch-RMSOnline-Licensing-Location-Url`
- `ms-Exch-RoleGroup-Type`
- `ms-Exch-Service-End-Point-URL`
- `ms-Exch-Shadow-When-Soft-Deleted-Time`
- `ms-Exch-Spam-Add-Header`
- `ms-Exch-Spam-Asf-Settings`
- `ms-Exch-Spam-Asf-Test-Bcc-Address`
- `ms-Exch-Spam-Country-Block-List`
- `ms-Exch-Spam-Digest-Frequency`

- `ms-Exch-Spam-False-Positive-Cc`
- `ms-Exch-Spam-Flags`
- `ms-Exch-Spam-Language-Block-List`
- `ms-Exch-Spam-Modify-Subject`
- `ms-Exch-Spam-Notify-Outbound-Recipients`
- `ms-Exch-Spam-Outbound-Spam-Cc`
- `ms-Exch-Spam-Quarantine-Retention`
- `ms-Exch-Spam-Redirect-Address`
- `ms-Exch-Sts-Refresh-Tokens-Valid-From`
- `ms-Exch-Sync-Cookie`
- `ms-Exch-Sync-Service-Instance-New-Tenant-Max-Version`
- `ms-Exch-Sync-Service-Instance-New-Tenant-Min-Version`
- `ms-Exch-Team-Mailbox-Expiration`
- `ms-Exch-Team-Mailbox-Expiry-Days`
- `ms-Exch-Team-Mailbox-Owners`
- `ms-Exch-Team-Mailbox-SharePoint-Linked-By`
- `ms-Exch-Team-Mailbox-SharePoint-Url`
- `ms-Exch-Team-Mailbox-Show-In-Client-List`
- `ms-Exch-Tenant-Country`
- `ms-Exch-Throttling-Policy-Flags`
- `ms-Exch-Transport-MaxRetriesForLocalSiteShadow`
- `ms-Exch-Transport-MaxRetriesForRemoteSiteShadow`
- `ms-Exch-Transport-Reseller-Settings-Link-SL`
- `ms-Exch-Transport-Rule-Immutable-Id`
- `ms-Exch-Trusted-Domain-BL`
- `ms-Exch-Trusted-Domain-Link`
- `ms-Exch-UG-Event-Subscription-BL`
- `ms-Exch-UG-Event-Subscription-Link`
- `ms-Exch-UG-Member-BL`
- `ms-Exch-UG-Member-Link`
- `ms-Exch-Urgent-Critical`
- `ms-Exch-Urgent-Overloaded`
- `ms-Exch-Urgent-Underloaded`
- `ms-Exch-WAC-Discovery-Endpoint`
- `ms-Exch-When-Soft-Deleted-Time`
- `ms-Exch-Workload-Classification`
- `ms-Exch-Workload-Management-Is-Enabled`
- `ms-Exch-Workload-Management-Policy`
- `ms-Exch-Workload-Management-Policy-BL`
- `ms-Exch-Workload-Management-Policy-Link`

Атрибуты глобального каталога, добавленные в окончательной первоначальной версии Exchange 2019

- `ms-Exch-Administrative-Unit-BL`
- `ms-Exch-Administrative-Unit-Link`
- `ms-Exch-Archive-Database-Link-SL`
- `ms-Exch-Auth-Policy-Link`
- `ms-Exch-Correlation-Id`
- `ms-Exch-Data-Encryption-Policy-BL`
- `ms-Exch-Data-Encryption-Policy-Link`
- `ms-Exch-Default-Public-Folder-Mailbox`
- `ms-Exch-Device-Client-Type`
- `ms-Exch-Dirsync-Authority-Metadata`
- `ms-Exch-Dirsync-Status`
- `ms-Exch-Dirsync-Status-Ack`
- `ms-Exch-Disabled-Archive-Database-Link-SL`
- `ms-Exch-Edge-Sync-Config-Flags`
- `ms-Exch-EvictedMembers-Link`
- `ms-Exch-EvictedMembers-BL`
- `ms-Exch-Extension-Custom-Attribute-1`
- `ms-Exch-Extension-Custom-Attribute-2`
- `ms-Exch-Extension-Custom-Attribute-3`
- `ms-Exch-Extension-Custom-Attribute-4`
- `ms-Exch-Extension-Custom-Attribute-5`
- `ms-Exch-Group-External-Member-Count`
- `ms-Exch-Group-Member-Count`
- `ms-Exch-HAB-Root-DepaPreviewent-Link`
- `ms-Exch-Home-MDB-SL`
- `ms-Exch-Home-MTA-SL`
- `ms-Exch-Is-Dirsync-Status-Pending`
- `ms-Exch-Localization-Flags`
- `ms-Exch-Mailbox-Container-Guid`
- `ms-Exch-Mailbox-Move-Source-Archive-MDB-Link-SL`
- `ms-Exch-Mailbox-Move-Source-MDB-Link-SL`
- `ms-Exch-Mailbox-Move-Storage-MDB-Link-SL`
- `ms-Exch-Mailbox-Move-Target-Archive-MDB-Link-SL`
- `ms-Exch-Mailbox-Move-Target-MDB-Link-SL`
- `ms-Exch-Offline-OrgId-Home-Realm-Record`
- `ms-Exch-Previous-Archive-Database`
- `ms-Exch-Previous-Archive-Database-SL`
- `ms-Exch-Previous-Home-MDB-SL`

- `ms-Exch-Recipient-SoftDeleted-Status`
- `ms-Exch-Relocate-Tenant-Completion-Target-Vector,`
- `ms-Exch-Relocate-Tenant-Flags`
- `ms-Exch-Relocate-Tenant-Safe-Lockdown-Schedule`
- `ms-Exch-Relocate-Tenant-Source-Forest`
- `ms-Exch-Relocate-Tenant-Start-Lockdown`
- `ms-Exch-Relocate-Tenant-Start-Retired`
- `ms-Exch-Relocate-Tenant-Start-Sync`
- `ms-Exch-Relocate-Tenant-Status`
- `ms-Exch-Relocate-Tenant-Target-Forest`
- `ms-Exch-Relocate-Tenant-Transition-Counter`
- `ms-Exch-RMS-Computer-Accounts-Link-SL`
- `ms-Exch-RoleGroup-Type`
- `ms-Exch-Sync-Cookie`
- `ms-Exch-Team-Mailbox-Expiration`
- `ms-Exch-Team-Mailbox-Expiry-Days`
- `ms-Exch-Team-Mailbox-Owners`
- `ms-Exch-Team-Mailbox-SharePoint-Linked-By`
- `ms-Exch-Team-Mailbox-SharePoint-Url`
- `ms-Exch-Team-Mailbox-Show-In-Client-List`
- `ms-Exch-UG-Event-Subscription-BL`
- `ms-Exch-UG-Event-Subscription-Link`
- `ms-Exch-Unified-Mailbox`
- `ms-Exch-When-Soft-Deleted-Time

Атрибуты, измененные в окончательной первоначальной версии Exchange 2019

Класс	Изменение	Атрибут или класс
`Exch-Configuration-Unit-Container`	`rangeUpper`	15254
`Exch-Mailflow-Policy-Transport-Rules-Template-Xml`	`rangeUpper`	256000
`Mail-Recipient`	Замена: `mayContain`	`msExchUGMemberLink`
`ms-Exch-Accepted-Domain-Name`	замена: `searchFlags`	9

Класс	Изменение	Атрибут или класс
`ms-Exch-Archive-GUID`	замена: `searchFlags`	9
`ms-Exch-Bypass-Audit`	замена: `searchFlags`	19
`ms-Exch-Coexistence-On-Premises-Smart-Host`	`ntdsSchemaAdd`	`attributeID: 1.2.840.113556.1.4.7000.102.51992` `isMemberOfPartialAttributeSet: FALSE` (не в глобальном каталоге) `searchFlags: 0` (без индекса)
`ms-Exch-Coexistence-Secure-Mail-Certificate-Thumbprint`	`ntdsSchemaAdd`	`attributeID: 1.2.840.113556.1.4.7000.102.51991` `isMemberOfPartialAttributeSet: FALSE` (не в глобальном каталоге) `searchFlags: 0` (без индекса)
`ms-Exch-Coexistence-Secure-Mail-Certificate-Thumbprintms-Exch-Sync-Cookie`	`rangeUpper`	1024
`ms-Exch-Coexistence-Transport-Servers`	`ntdsSchemaAdd`	`attributeID: 1.2.840.113556.1.4.7000.102.51990` `isMemberOfPartialAttributeSet: FALSE` (не в глобальном каталоге) `searchFlags: 0` (без индекса)
`ms-Exch-ELC-Mailbox-Flags`	замена: `attributeSecurityGuid`	`F6SzsVXskUGzJ7cuM+OK8g==`
`ms-Exch-Extension-Custom-Attribute-1`	`isMemberOfPartialAttributeSet:`	`TRUE`
`ms-Exch-Extension-Custom-Attribute-2`	`isMemberOfPartialAttributeSet:`	`TRUE`
`ms-Exch-Extension-Custom-Attribute-3`	`isMemberOfPartialAttributeSet:`	`TRUE`
`ms-Exch-Extension-Custom-Attribute-4`	`isMemberOfPartialAttributeSet:`	`TRUE`

Класс	Изменение	Атрибут или класс
`ms-Exch-Extension-Custom-Attribute-5`	`isMemberOfPartialAttributeSet`	`TRUE`
`ms-Exch-Group-External-Member-Count`	`ntdsSchemaModify`	`isMemberOfPartialAttributeSet: TRUE MAPIID:36066`
`ms-Exch-Group-Member-Count`	`ntdsSchemaModify`	замена: `isMemberOfPartialAttributeSetisMemberOfPartialAttributeSet: TRUE MAPIID: 36067`
`ms-Exch-Group-Security-Flags`	`ntdsSchemaModify`	замена: `mapiId: 36111`
`ms-Exch-HAB-Root-DepaPreviewent-Link`	замена: `isMemberOfPartialAttributeSet`	`TRUE`
`ms-Exch-Mailbox-Audit-Enable`	замена: `searchFlags`	19
`ms-Exch-Malware-Filtering-Update-Frequency`	`rangeUpper`	38880
`ms-Exch-MSO-Forward-Sync-Non-Recipient-Cookie`	`rangeUpper`	20480
`ms-Exch-MSO-Forward-Sync-Recipient-Cookie`	`rangeUpper`	20480
`ms-Exch-Role-Entries`	`rangeUpper`	8192
`ms-Exch-Schema-Version-Pt`	`rangeUpper`	15137
`ms-Exch-Schema-Version-Pt`	`rangeUpper`	15281

Класс	Изменение	Атрибут или класс
`Ms-exch-schema-version-pt`	`rangeUpper`	15292
`ms-Exch-Smtp-Receive-Tls-Certificate-Name`	Замена: `rangeUpper`	1024
`ms-Exch-Smtp-TLS-Certificate`	замена: `rangeUpper`	1024
`ms-Exch-Sync-Cookie`	`rangeUpper`	262144
`Top`	Замена: `mayContain`	`msExchUGMemberBL`

Идентификаторы объектов, добавленные в окончательной первоначальной версии Exchange 2019

Когда вы устанавливаете окончательную первоначальную версию Exchange 2019, добавляются следующие идентификаторы объектов классов:

- 1.2.840.113556.1.5.7000.62.50161
- 1.2.840.113556.1.5.7000.62.50162
- 1.2.840.113556.1.5.7000.62.50163
- 1.2.840.113556.1.5.7000.62.50164
- 1.2.840.113556.1.5.7000.62.50165
- 1.2.840.113556.1.5.7000.62.50166
- 1.2.840.113556.1.5.7000.62.50167
- 1.2.840.113556.1.5.7000.62.50170
- 1.2.840.113556.1.5.7000.62.50171
- 1.2.840.113556.1.5.7000.62.50172
- 1.2.840.113556.1.5.7000.62.50173
- 1.2.840.113556.1.5.7000.62.50174
- 1.2.840.113556.1.5.7000.62.50176
- 1.2.840.113556.1.5.7000.62.50177
- 1.2.840.113556.1.5.7000.62.50178
- 1.2.840.113556.1.5.7000.62.50187
- 1.2.840.113556.1.5.7000.62.50188
- 1.2.840.113556.1.5.7000.62.50189
- 1.2.840.113556.1.5.7000.62.50190
- 1.2.840.113556.1.5.7000.62.50191
- 1.2.840.113556.1.5.7000.62.50192
- 1.2.840.113556.1.5.7000.62.50202

- 1.2.840.113556.1.5.7000.62.50203
- 1.2.840.113556.1.5.7000.62.50204
- 1.2.840.113556.1.5.7000.62.50205
- 1.2.840.113556.1.5.7000.62.50212
- 1.2.840.113556.1.5.7000.62.50213
- 1.2.840.113556.1.5.7000.62.50214

Когда вы устанавливаете окончательную первоначальную версию Exchange 2019, добавляются следующие идентификаторы объектов атрибутов:

- 1.2.840.113556.1.4.2183
- 1.2.840.113556.1.4.2184
- 1.2.840.113556.1.4.2185
- 1.2.840.113556.1.4.7000.102.51773
- 1.2.840.113556.1.4.7000.102.51774
- 1.2.840.113556.1.4.7000.102.51775
- 1.2.840.113556.1.4.7000.102.51786
- 1.2.840.113556.1.4.7000.102.51787
- 1.2.840.113556.1.4.7000.102.51788
- 1.2.840.113556.1.4.7000.102.51789
- 1.2.840.113556.1.4.7000.102.51790
- 1.2.840.113556.1.4.7000.102.51791
- 1.2.840.113556.1.4.7000.102.51792
- 1.2.840.113556.1.4.7000.102.51794
- 1.2.840.113556.1.4.7000.102.51795
- 1.2.840.113556.1.4.7000.102.51796
- 1.2.840.113556.1.4.7000.102.51797
- 1.2.840.113556.1.4.7000.102.51798
- 1.2.840.113556.1.4.7000.102.51799
- 1.2.840.113556.1.4.7000.102.51800
- 1.2.840.113556.1.4.7000.102.51801
- 1.2.840.113556.1.4.7000.102.51805
- 1.2.840.113556.1.4.7000.102.51806
- 1.2.840.113556.1.4.7000.102.51807
- 1.2.840.113556.1.4.7000.102.51808
- 1.2.840.113556.1.4.7000.102.51809
- 1.2.840.113556.1.4.7000.102.51810
- 1.2.840.113556.1.4.7000.102.51811
- 1.2.840.113556.1.4.7000.102.51812
- 1.2.840.113556.1.4.7000.102.51813
- 1.2.840.113556.1.4.7000.102.51814
- 1.2.840.113556.1.4.7000.102.51815
- 1.2.840.113556.1.4.7000.102.51816
- 1.2.840.113556.1.4.7000.102.51818
- 1.2.840.113556.1.4.7000.102.51819

- 1.2.840.113556.1.4.7000.102.51820
- 1.2.840.113556.1.4.7000.102.51821
- 1.2.840.113556.1.4.7000.102.51822
- 1.2.840.113556.1.4.7000.102.51823
- 1.2.840.113556.1.4.7000.102.51824
- 1.2.840.113556.1.4.7000.102.51826
- 1.2.840.113556.1.4.7000.102.51827
- 1.2.840.113556.1.4.7000.102.51829
- 1.2.840.113556.1.4.7000.102.51830
- 1.2.840.113556.1.4.7000.102.51832
- 1.2.840.113556.1.4.7000.102.51833
- 1.2.840.113556.1.4.7000.102.51836
- 1.2.840.113556.1.4.7000.102.51837
- 1.2.840.113556.1.4.7000.102.51838
- 1.2.840.113556.1.4.7000.102.51839
- 1.2.840.113556.1.4.7000.102.51840
- 1.2.840.113556.1.4.7000.102.51851
- 1.2.840.113556.1.4.7000.102.51852
- 1.2.840.113556.1.4.7000.102.51859
- 1.2.840.113556.1.4.7000.102.51860
- 1.2.840.113556.1.4.7000.102.51861
- 1.2.840.113556.1.4.7000.102.51862
- 1.2.840.113556.1.4.7000.102.51863
- 1.2.840.113556.1.4.7000.102.51864
- 1.2.840.113556.1.4.7000.102.51865
- 1.2.840.113556.1.4.7000.102.51866
- 1.2.840.113556.1.4.7000.102.51867
- 1.2.840.113556.1.4.7000.102.51868
- 1.2.840.113556.1.4.7000.102.51869
- 1.2.840.113556.1.4.7000.102.51870
- 1.2.840.113556.1.4.7000.102.51871
- 1.2.840.113556.1.4.7000.102.51872
- 1.2.840.113556.1.4.7000.102.51873
- 1.2.840.113556.1.4.7000.102.51874
- 1.2.840.113556.1.4.7000.102.51875
- 1.2.840.113556.1.4.7000.102.51876
- 1.2.840.113556.1.4.7000.102.51877
- 1.2.840.113556.1.4.7000.102.51878
- 1.2.840.113556.1.4.7000.102.51879
- 1.2.840.113556.1.4.7000.102.51880
- 1.2.840.113556.1.4.7000.102.51881
- 1.2.840.113556.1.4.7000.102.51882
- 1.2.840.113556.1.4.7000.102.51883
- 1.2.840.113556.1.4.7000.102.51914

- 1.2.840.113556.1.4.7000.102.51915
- 1.2.840.113556.1.4.7000.102.51916
- 1.2.840.113556.1.4.7000.102.51917
- 1.2.840.113556.1.4.7000.102.51918
- 1.2.840.113556.1.4.7000.102.51919
- 1.2.840.113556.1.4.7000.102.51920
- 1.2.840.113556.1.4.7000.102.51921
- 1.2.840.113556.1.4.7000.102.51922
- 1.2.840.113556.1.4.7000.102.51923
- 1.2.840.113556.1.4.7000.102.51924
- 1.2.840.113556.1.4.7000.102.51925
- 1.2.840.113556.1.4.7000.102.51926
- 1.2.840.113556.1.4.7000.102.51927
- 1.2.840.113556.1.4.7000.102.51928
- 1.2.840.113556.1.4.7000.102.51929
- 1.2.840.113556.1.4.7000.102.51930
- 1.2.840.113556.1.4.7000.102.51931
- 1.2.840.113556.1.4.7000.102.51932
- 1.2.840.113556.1.4.7000.102.51933
- 1.2.840.113556.1.4.7000.102.51934
- 1.2.840.113556.1.4.7000.102.51935
- 1.2.840.113556.1.4.7000.102.51936
- 1.2.840.113556.1.4.7000.102.51937
- 1.2.840.113556.1.4.7000.102.51938
- 1.2.840.113556.1.4.7000.102.51939
- 1.2.840.113556.1.4.7000.102.51940
- 1.2.840.113556.1.4.7000.102.51941
- 1.2.840.113556.1.4.7000.102.51942
- 1.2.840.113556.1.4.7000.102.51943
- 1.2.840.113556.1.4.7000.102.51944
- 1.2.840.113556.1.4.7000.102.51945
- 1.2.840.113556.1.4.7000.102.51946
- 1.2.840.113556.1.4.7000.102.51947
- 1.2.840.113556.1.4.7000.102.51948
- 1.2.840.113556.1.4.7000.102.51949
- 1.2.840.113556.1.4.7000.102.51950
- 1.2.840.113556.1.4.7000.102.51951
- 1.2.840.113556.1.4.7000.102.51952
- 1.2.840.113556.1.4.7000.102.51953
- 1.2.840.113556.1.4.7000.102.51954
- 1.2.840.113556.1.4.7000.102.51955
- 1.2.840.113556.1.4.7000.102.51993
- 1.2.840.113556.1.4.7000.102.51994
- 1.2.840.113556.1.4.7000.102.51995

- 1.2.840.113556.1.4.7000.102.51996
- 1.2.840.113556.1.4.7000.102.51997
- 1.2.840.113556.1.4.7000.102.51998
- 1.2.840.113556.1.4.7000.102.52001
- 1.2.840.113556.1.4.7000.102.52002
- 1.2.840.113556.1.4.7000.102.52003
- 1.2.840.113556.1.4.7000.102.52004
- 1.2.840.113556.1.4.7000.102.52005
- 1.2.840.113556.1.4.7000.102.52006
- 1.2.840.113556.1.4.7000.102.52007
- 1.2.840.113556.1.4.7000.102.52008
- 1.2.840.113556.1.4.7000.102.52011
- 1.2.840.113556.1.4.7000.102.52012
- 1.2.840.113556.1.4.7000.102.52013
- 1.2.840.113556.1.4.7000.102.52014
- 1.2.840.113556.1.4.7000.102.52015
- 1.2.840.113556.1.4.7000.102.52016
- 1.2.840.113556.1.4.7000.102.52017
- 1.2.840.113556.1.4.7000.102.52018
- 1.2.840.113556.1.4.7000.102.52019
- 1.2.840.113556.1.4.7000.102.52020
- 1.2.840.113556.1.4.7000.102.52021
- 1.2.840.113556.1.4.7000.102.52022
- 1.2.840.113556.1.4.7000.102.52023
- 1.2.840.113556.1.4.7000.102.52024
- 1.2.840.113556.1.4.7000.102.52029
- 1.2.840.113556.1.4.7000.102.52030
- 1.2.840.113556.1.4.7000.102.52031
- 1.2.840.113556.1.4.7000.102.52032
- 1.2.840.113556.1.4.7000.102.52033
- 1.2.840.113556.1.4.7000.102.52034
- 1.2.840.113556.1.4.7000.102.52035
- 1.2.840.113556.1.4.7000.102.52036
- 1.2.840.113556.1.4.7000.102.52037
- 1.2.840.113556.1.4.7000.102.52039
- 1.2.840.113556.1.4.7000.102.52040
- 1.2.840.113556.1.4.7000.102.52041
- 1.2.840.113556.1.4.7000.102.52042
- 1.2.840.113556.1.4.7000.102.52043
- 1.2.840.113556.1.4.7000.102.52044
- 1.2.840.113556.1.4.7000.102.52045
- 1.2.840.113556.1.4.7000.102.52046
- 1.2.840.113556.1.4.7000.102.52047
- 1.2.840.113556.1.4.7000.102.52048

- 1.2.840.113556.1.4.7000.102.52049
- 1.2.840.113556.1.4.7000.102.52050
- 1.2.840.113556.1.4.7000.102.52051
- 1.2.840.113556.1.4.7000.102.52052
- 1.2.840.113556.1.4.7000.102.52053
- 1.2.840.113556.1.4.7000.102.52054
- 1.2.840.113556.1.4.7000.102.52055
- 1.2.840.113556.1.4.7000.102.52056
- 1.2.840.113556.1.4.7000.102.52057
- 1.2.840.113556.1.4.7000.102.52058
- 1.2.840.113556.1.4.7000.102.52059
- 1.2.840.113556.1.4.7000.102.52060
- 1.2.840.113556.1.4.7000.102.52061
- 1.2.840.113556.1.4.7000.102.52062
- 1.2.840.113556.1.4.7000.102.52063
- 1.2.840.113556.1.4.7000.102.52064
- 1.2.840.113556.1.4.7000.102.52065
- 1.2.840.113556.1.4.7000.102.52109
- 1.2.840.113556.1.4.7000.102.52110
- 1.2.840.113556.1.4.7000.102.52126
- 1.2.840.113556.1.4.7000.102.52127
- 1.2.840.113556.1.4.7000.102.52128
- 1.2.840.113556.1.4.7000.102.52129
- 1.2.840.113556.1.4.7000.102.52130
- 1.2.840.113556.1.4.7000.102.52151
- 1.2.840.113556.1.4.7000.102.52152
- 1.2.840.113556.1.4.7000.102.52155
- 1.2.840.113556.1.4.7000.102.52156
- 1.2.840.113556.1.4.7000.102.52157
- 1.2.840.113556.1.4.7000.102.52158
- 1.2.840.113556.1.4.7000.102.52159
- 1.2.840.113556.1.4.7000.102.52160
- 1.2.840.113556.1.4.7000.102.52161

Индексированные атрибуты, добавленные в окончательной первоначальной версии Exchange 2019

Атрибут	Значение флага поиска
`ms-DS-GeoCoordinates-Altitude`	1
`ms-DS-GeoCoordinates-Latitude`	1
`ms-DS-GeoCoordinates-Longitude`	1

Атрибут	Значение флага поиска
`ms-Exch-Accepted-Domain-Name`	9
`ms-Exch-Archive-GUID`	9
`ms-Exch-Auth-Application-Identifier`	1
`ms-Exch-Auth-Issuer-Name`	1
`ms-Exch-Bypass-Audit`	9
`ms-Exch-Data-Encryption-Policy-Link`	1
`ms-Exch-Default-Public-Folder-Mailbox`	19
`ms-Exch-Device-Client-Type`	1
`ms-Exch-Extension-Custom-Attribute-1`	1
`ms-Exch-Extension-Custom-Attribute-2`	1
`ms-Exch-Extension-Custom-Attribute-3`	1
`ms-Exch-Extension-Custom-Attribute-4`	1
`ms-Exch-Extension-Custom-Attribute-5`	1
`ms-Exch-Home-MDB-SL`	1
`ms-Exch-Home-MTA-SL`	1
`ms-Exch-Is-Dirsync-Status-Pending`	1
`ms-Exch-Mailbox-Audit-Enable`	19
`ms-Exch-Mailbox-Database-Transport-Flags`	16
`ms-Exch-Mailbox-Move-Source-Archive-MDB-Link-SL`	1
`ms-Exch-Mailbox-Move-Source-MDB-Link-SL`	1
`ms-Exch-Mailbox-Move-Target-Archive-MDB-Link-SL`	1
`ms-Exch-Organization-Upgrade-Policy-Link`	1
`ms-Exch-Organization-Upgrade-Policy-Link-SL`	1
`ms-Exch-OWA-Set-Photo-URL`	16
`ms-Exch-Previous-Archive-Database-SL`	8
`ms-Exch-Previous-Home-MDB-SL`	8
`ms-Exch-Provisioning-Tags`	1
`ms-Exch-Public-Folder-EntryId`	24

Атрибут	Значение флага поиска
`ms-Exch-Public-Folder-Mailbox`	24
`ms-Exch-Public-Folder-Smtp-Address`	24
`ms-Exch-Recipient-SoftDeleted-Status`	27
`ms-Exch-Relocate-Tenant-Completion-Target-Vector`	8
`ms-Exch-Relocate-Tenant-Flags`	8
`ms-Exch-Relocate-Tenant-Safe-Lockdown-Schedule`	8
`ms-Exch-Relocate-Tenant-Source-Forest`	9
`ms-Exch-Relocate-Tenant-Start-Lockdown`	8
`ms-Exch-Relocate-Tenant-Start-Retired`	8
`ms-Exch-Relocate-Tenant-Start-Sync`	8
`ms-Exch-Relocate-Tenant-Status,`	9
`ms-Exch-Relocate-Tenant-Target-Forest`	9
`ms-Exch-Relocate-Tenant-Transition-Counter`	8
`ms-Exch-Sync-Cookie`	8
`ms-Exch-Team-Mailbox-Expiration`	16
`ms-Exch-Team-Mailbox-Expiry-Days`	16
`ms-Exch-Team-Mailbox-Owners`	16
`ms-Exch-Team-Mailbox-SharePoint-Linked-By`	16
`ms-Exch-Team-Mailbox-SharePoint-Url`	16
`ms-Exch-Team-Mailbox-Show-In-Client-List`	16
`ms-Exch-Transport-Rule-Immutable-Id`	1
`ms-Exch-When-Soft-Deleted-Time`	17

Наборы свойств, измененные в окончательной первоначальной версии Exchange 2019

При установке окончательной первоначальной версии Exchange 2019 изменяются такие наборы свойств:

- Exchange-Information

Идентификаторы MAPI, добавленные в окончательной первоначальной версии Exchange 2019

Когда вы устанавливаете окончательную первоначальную версию Exchange 2019, добавляются следующие идентификаторы MAPI:

- 36066
- 36067

Расширенные права, добавленные в окончательной первоначальной версии Exchange 2019

В следующей таблице перечислены расширенные права, которые добавляются при установке Exchange 2019 RTM. Установка Exchange 2019 RTM не изменяет существующие расширенные права.

Идентификатор	Значения
`CN=ms-Exch-SMTP-Accept-XProxyFrom,CN=Extended-Rights,<ConfigurationContainerDN>`	`changetype: ntdsSchemaAdddisplayName: Accept XProxyFromobjectClass: controlAccessRightrightsGuid: 5bee2b72-50d7-49c7-ba66-39a25daa1e92validAccesses: 256`

Какие изменения в Active Directory при установке Exchange

Статья • 04.04.2023

При установке Exchange Server 2016 или Exchange Server 2019 в лес Active Directory и домены вносятся изменения для хранения сведений о серверах Exchange, почтовых ящиках и других объектах, связанных с Exchange в организации.

Для подготовки Active Directory для Exchange необходимо выполнить три шага:

1. Расширение схемы Active Directory
2. Подготовка контейнеров, объектов и других элементов Active Directory
3. Подготовка доменов Active Directory

После выполнения всех трех шагов лес Active Directory будет готов к работе с Exchange. В этом разделе объясняется, что делает Exchange на каждом этапе подготовки Active Directory.

Эти изменения можно внести перед установкой первого сервера Exchange 2016 или Exchange 2019 в организации, выполнив команды */PrepareSchema*, */PrepareAD* и */PrepareAllDomains* или */PrepareDomains* с помощью программы установки командной строки Exchange. Инструкции см. в разделе Подготовка Active Directory и доменов для Exchange. Кроме того, эти изменения автоматически вносятся во время установки первого сервера Exchange с помощью мастера установки Exchange. Инструкции см. в статье Установка серверов почтовых ящиков Exchange с помощью мастера установки.

Расширение схемы Active Directory

Расширение схемы Active Directory добавляет и обновляет классы, атрибуты и другие элементы. Эти изменения необходимы, чтобы Exchange могла создавать контейнеры и объекты для хранения сведений об организации Exchange. Так как Exchange вносит много изменений в схему Active Directory, этому шагу посвящен раздел. Чтобы просмотреть все изменения, внесенные в схему, см. статью Изменения схемы Active Directory в Exchange Server.

После расширения схемы путем выполнения команды */PrepareSchema* , команды _/PrepareAD или установки первого сервера Exchange Server с помощью мастера установки Exchange версия схемы устанавливается в **атрибуте ms-Exch-Schema-**

Version-Pt . Чтобы убедиться, что схема Active Directory успешно расширена, можно проверить значение, хранящееся в этом атрибуте. Дополнительные сведения см. в разделе Версии Exchange Active Directory.

Подготовка контейнеров, объектов и других элементов Active Directory

После расширения схемы следующим шагом будет добавление всех контейнеров, объектов, атрибутов и других элементов, используемых Exchange для хранения информации в Active Directory. Большинство изменений, вносимых на этом этапе, применяются ко всему лесу Active Directory. Меньший набор изменений выполняется только в локальном домене Active Directory, где была выполнена команда */PrepareAD* (или где был установлен первый сервер Exchange Server с помощью мастера установки Exchange).

Exchange вносит следующие изменения в лес Active Directory:

- Контейнер Microsoft Exchange создается в разделе CN=Services,CN=Configuration,DC=<*корневой домен*> , если он еще не существует.
- Следующие контейнеры и объекты создаются в разделе CN=<*название*> организации,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*корневой домен*> , если они еще не существуют:
  - CN=Address Lists Container
  - CN=AddressBook Mailbox Policies
  - CN=Addressing
  - CN=Administrative Groups
  - CN=Approval Applications
  - CN=Auth Configuration
  - CN=Availability Configuration
  - CN=Client Access
  - CN=Connections
  - CN=ELC Folders Container

- CN=ELC Mailbox Policies
- CN=ExchangeAssistance
- CN=Federation
- CN=Federation Trusts
- CN=Global Settings
- CN=Hybrid Configuration
- CN=Mobile Mailbox Policies
- CN=Mobile Mailbox Settings
- CN=Monitoring Settings
- CN=OWA Mailbox Policies
- CN=Provisioning Policy Container
- CN=Push Notification Settings
- CN=RBAC
- CN=Recipient Policies
- CN=Remote Accounts Policies Container
- CN=Retention Policies Container
- CN=Retention Policy Tag Container
- CN=ServiceEndpoints
- CN=System Policies
- CN=Team Mailbox Provisioning Policies
- CN=Transport Settings
- Cn=UM AutoAttendant Container (только Exchange 2016)
- Контейнер CN=UM DialPlan (только Exchange 2016)
- Контейнер CN=UM IPGateway (только Exchange 2016)

    - Политики почтовых ящиков единой системы обмена сообщениями (только Для Exchange 2016)
    - CN=Workload Management Settings
- Следующие контейнеры и объекты создаются в разделе CN=Параметры транспорта,CN=<*Название*> организации,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*корневой домен*> , если они еще не существуют:
    - CN=Accepted Domains
    - CN=ControlPoint Config
    - CN=DNS Customization
    - CN=Interceptor Rules
    - CN=Malware Filter
    - CN=Message Classifications
    - CN=Message Hygiene
    - CN=Rules
    - CN=MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e
- Разрешения задаются во всем разделе конфигурации в Active Directory.
- Импортируется файл Rights.ldf. Файл добавляет разрешения, необходимые для установки Exchange и настройки Active Directory.
- Подразделение групп безопасности Microsoft Exchange создается в корневом домене леса и ему назначаются разрешения.
- В подразделении групп безопасности Microsoft Exchange создаются следующие группы, если они не существуют:
    - Управление соответствием требованиям
    - Делегированная установка
    - Управление обнаружением
    - Серверы Exchange
    - Группа безопасности Exchange Trusted Subsystem

    - Разрешения Windows для Exchange
    - ExchangeLegacyInterop
    - Служба поддержки
    - Управление санацией
    - Управляемые серверы доступности
    - Управление организацией
    - Управление общими папками
    - Управление получателями
    - Управление записями
    - Управление сервером
    - Управление организацией только с правом на просмотр
- Новые группы ролей управления (которые отображаются как универсальные группы безопасности (USG) в Active Directory), созданные в подразделении групп безопасности Microsoft Exchange, добавляются в атрибут **otherWellKnownObjects** , хранящийся в контейнере CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<*корневом домене*> .
- Только в Exchange 2016 контакт инициатора голосовой связи единой системы обмена сообщениями создается в контейнере системных объектов Microsoft Exchange корневого домена.
- Для Exchange подготавливается только домен, в котором была выполнена команда */PrepareAD* (или где был установлен первый сервер Exchange Server с помощью мастера установки Exchange). Сведения о том, что делается для подготовки домена Active Directory для Exchange, см. в следующем разделе.

Подготовка доменов Active Directory

Последним шагом подготовки Active Directory для Exchange является подготовка доменов Active Directory, в которых будут установлены серверы Exchange или где будут размещаться пользователи с поддержкой почтовых ящиков (все домены в лесу с помощью команды */PrepareAllDomains* , определенные домены с помощью команды */PrepareDomains* или установка первого сервера Exhange с помощью мастера установки Exchange). Этот шаг выполняется автоматически в домене, где

была выполнена команда *PrepareAD* (или где был установлен первый сервер Exchange Server с помощью мастера установки Exchange).

Exchange вносит изменения в домены Active Directory:

- Контейнер системных объектов Microsoft Exchange создается в разделе корневого домена Active Directory, если он еще не существует.
- Задаются разрешения в контейнере системных объектов Microsoft Exchange для групп безопасности "Серверы Exchange", "Управление организацией" и "Прошедшие проверку".
- Изменение **объекта групповой политики контроллеров домена по умолчанию** для предоставления прав "Управление политикой аудита и журнала безопасности" **серверам Exchange Enterprise.**
- Глобальная группа серверов установки доменов группа домена Exchange создается в текущем домене и размещается в контейнере системных объектов Microsoft Exchange.
- Группа серверов установки доменов Exchange добавляется в универсальную группу безопасности серверов Exchange в корневом домене.
- На уровне домена назначаются разрешения для универсальных групп безопасности "Серверы Exchange" и "Управление организацией".
- Свойство **objectVersion** в контейнере системных объектов Microsoft Exchange в dc=<*root домене*> задано. Чтобы убедиться, что домены Active Directory успешно подготовлены, можно проверить значение, хранящееся в этом атрибуте. Дополнительные сведения см. в разделе Версии Exchange Active Directory.

Подготовка Active Directory и доменов для Exchange Server

Статья • 29.05.2024

Exchange использует Active Directory для хранения сведений о почтовых ящиках и конфигурации серверов Exchange в организации. Перед установкой Exchange Server 2016 или Exchange Server 2019 (даже если в организации установлены более ранние версии Exchange), необходимо подготовить лес Active Directory и его домены для новой версии Exchange. Это можно сделать двумя способами:

- **Позвольте мастеру установки Exchange сделать это за вас**. Если у вас нет большого развертывания Active Directory и у вас нет отдельной команды, которая управляет Active Directory, рекомендуется использовать мастер установки. Ваша учетная запись должна быть членом групп безопасности "Администраторы схемы" и "Администраторы предприятия". Дополнительные сведения об использовании мастера установки см. в статье Установка серверов почтовых ящиков Exchange с помощью мастера установки.

> ⓘ **Важно!**
>
> Если Exchange разворачивается в многосайтовой среде Active Directory и находится на сайте, отличном от сайта контроллера домена, который содержит роль хозяина схемы, вы не сможете подготовить Active Directory с помощью мастера. Вместо этого выполните шаги 1 и 2 в этом разделе.

- **Выполните действия, описанные в этой статье**: Если у вас есть крупное развертывание Active Directory или отдельная команда управляет Active Directory, этот раздел предназначен для вас. Далее описывается управление каждым этапом подготовки и указывается, кто может выполнять тот или иной этап. Например, администраторы Exchange могут не иметь необходимых разрешений для расширения схемы Active Directory.

Сведения о новых атрибутах и классах схемы, которые Exchange добавляет в Active Directory, в том числе с помощью накопительных пакетов обновления (CU), см. в статье Изменения схемы Active Directory в Exchange Server.

Подробные сведения о том, что происходит при подготовке Active Directory для Exchange, см. в статье Какие изменения вносятся в Active Directory при установке Exchange.

Чтобы узнать больше о лесах или доменах Active Directory, см. статью Обзор доменных служб Active Directory.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 10–15 минут или больше (без учета репликации Active Directory) в зависимости от размера организации и количества дочерних доменов.
- Компьютер, который вы используете для выполнения этих процедур, должен соответствовать требованиям к системе для Exchange.
- Сведения о том, как проверить, соответствует ли Active Directory требованиям для Exchange:
  - **Exchange 2019**: Сеть и серверы каталогов для Exchange 2019.
  - **Exchange 2016**: Сеть и серверы каталогов для Exchange 2016.
- Если в вашей организации несколько доменов Active Directory, рекомендуем следующий подход:
  - Выполняйте эти процедуры на сайте Active Directory, содержащем сервер Active Directory с каждого домена.
  - Установите первый сервер Exchange Server на сайте Active Directory, содержащем доступный для записи сервер глобального каталога с каждого домена.
- Компьютер, используемый для выполнения всех процедур из этой статьи, должен иметь доступ к установочному файлу Setup.exe для Exchange.

  1. Скачайте последнюю версию Exchange. Дополнительные сведения см. в разделе Обновления для Exchange Server.
  2. В проводнике щелкните скачанный файл ISO-образа Exchange правой кнопкой мыши и выберите **Подключить**. Обратите внимание на назначенную букву виртуального DVD-диска.
  3. Откройте окно командной строки Windows. Например:
     - Нажмите клавиши Windows + R, чтобы открыть диалоговое окно **Выполнить**, введите cmd.exe и нажмите кнопку **ОК**.
     - Нажмите кнопку **Пуск**. В поле **Поиск** введите **командная строка**, а затем в списке результатов выберите **Командная строка**.

> **Совет**

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу **Exchange Server**.

Примечание

- Предыдущий переключатель */IAcceptExchangeServerLicenseTerms* не будет работать начиная с накопительных обновлений (CU) за сентябрь 2021 г. Теперь необходимо использовать */IAcceptExchangeServerLicenseTerms_DiagnosticDataON* или */IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF* для автоматической установки и установки по сценариям.
- В примерах ниже используется переключатель */IAcceptExchangeServerLicenseTerms_DiagnosticDataON*. Вы можете изменить переключатель на */IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF*.

Этап 1. Расширение схемы Active Directory

Совет

Если у вас нет отдельной команды, которая управляет схемой Active Directory, можно пропустить этот шаг и перейти непосредственно к **шагу 2. Подготовка Active Directory**. Если не расширить схему на этом шаге, команда */PrepareAd* на шаге 2 автоматически расширит схему. Если пропустить этот шаг, требования также будут применяться к шагу 2.

При расширении схемы Active Directory для Exchange действуют следующие требования:

- Ваша учетная запись должна быть членом групп безопасности "Администраторы схемы" и "Администраторы предприятия". Если используется несколько лесов Active Directory, убедитесь, что вы вошли в нужный лес.
- Компьютер должен находиться на том же домене и на том же сайте Active Directory, что и хозяин схемы.

- Если используется параметр */DomainController:<DomainControllerFQDN>*, необходимо указать контроллер домена, являющийся хозяином схемы.
- Единственный поддерживаемый способ расширения схемы для Exchange — использовать Setup.exe с */PrepareSchema*, */PrepareAD* или мастером установки Exchange. Другие способы расширения схемы не поддерживаются.

Чтобы расширить схему для Exchange, выполните следующую команду в окне командной строки Windows:

Консоль

```
<Virtual DVD drive letter>:\Setup.exe
/IAcceptExchangeServerLicenseTerms_DiagnosticDataON /PrepareSchema
```

Например, если установочные файлы Exchange доступны на диске E:, выполните следующую команду:

Консоль

```
E:\Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON
/PrepareSchema
```

> ⓘ **Примечание**
>
> При выполнении этой команды осуществляется проверка необходимых компонентов, которая покажет, какие из них отсутствуют.

После завершения установки расширения схемы необходимо подождать, пока Active Directory реплицирует изменения во все контроллеры домена, прежде чем продолжить. Чтобы проверить ход выполнения репликации, можно использовать `repadmin` средство в Windows Server. Дополнительные сведения об использовании средства см. в `repadmin` разделе Repadmin.

Этап 2. Подготовка Active Directory

После расширения схемы Active Directory можно подготовить другие части Active Directory для Exchange. На этом шаге Exchange создаст контейнеры, объекты и другие элементы в Active Directory для хранения информации. Коллекция контейнеров Exchange, объектов, атрибутов и т. д. называется *организацией Exchange*.

При подготовке Active Directory для Exchange действуют следующие требования:

- Ваша учетная запись должна быть членом группы безопасности "Администраторы предприятия". Если вы пропустили шаг 1, так как хотите, чтобы команда */PrepareAD* расширила схему, учетная запись также должна быть членом группы безопасности "Администраторы схемы".
- Компьютер должен находиться на том же сайте и домене Active Directory, что и хозяин схемы, а также должен быть на связи со всеми доменами в лесу через TCP-порт 389.
- Подождите, пока Active Directory завершит репликацию изменений схемы этапа 1 на все контроллеры доменов, прежде чем подготавливать Active Directory.
- Если вы устанавливаете новую организацию Exchange, необходимо выбрать имя для организации Exchange. Название организации используется внутри Exchange — оно, как правило, невидимо для пользователей, не влияет на функциональность Exchange и не определяет доступные адреса электронной почты.
  - Название организации не должно быть длиннее 64 символов и не может быть пустым.
  - Допустимые символы — от A до Z, от a до z, от 0 до 9, дефис или тире (-) и пробел, но пробелов не должно быть в начале и конце названия.
  - Указанное название организации невозможно изменить.
- Если вы хотите включить разделенные разрешения Active Directory, необходимо также указать `/ActiveDirectorySplitPermissions:true` параметр, как описано здесь.

Чтобы подготовить Active Directory для Exchange, выполните следующую команду в окне командной строки Windows:

Консоль

```
<Virtual DVD drive letter>:\Setup.exe
/IAcceptExchangeServerLicenseTerms_DiagnosticDataON /PrepareAD
/OrganizationName:"<Organization name>"
```

В этом примере используются установочные файлы Exchange на диске E:, а для организации Exchange задано название "Contoso Corporation".

Консоль

```
E:\Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON /PrepareAD
/OrganizationName:"Contoso Corporation"
```

> **ⓘ Важно!**
>
> Если между вашей локальной организацией и Exchange Online настроено гибридное развертывание, добавьте к команде параметр */TenantOrganizationConfig*.
>
> Для существующих сред не нужно использовать параметры */OrganizationName* и */TenantOrganizationConfig*.

Как и на этапе 1, вам придется подождать, пока Active Directory реплицирует изменения с этого этапа на все контроллеры доменов, а с помощью инструмента `repadmin` можно проверять ход выполнения репликации.

Этап 3. Подготовка доменов Active Directory

> **Совет**
>
> Если домен всего один, вы можете пропустить этот шаг, так как команда */PrepareAD* на этапе 2 уже подготовила домен автоматически.

Последним шагом является подготовка домена Active Directory, в котором будут установлены серверы Exchange или где будут размещаться пользователи с поддержкой почты. На этом шаге создаются дополнительные контейнеры и группы безопасности, а также задаются разрешения, чтобы Exchange смог получить к ним доступ.

Если в лесу Active Directory несколько доменов, их можно подготовить следующими способами:

- подготовить все домены в лесу Active Directory;
- Выбор подготавливаемых доменов Active Directory

Независимо от выбранного метода подождите, пока Active Directory завершит репликацию изменений из шага 2 на все контроллеры домена, прежде чем продолжить. В противном случае при попытке подготовить домены может возникнуть ошибка.

Подготовка всех доменов в лесу Active Directory

Чтобы подготовить все домены в лесу Active Directory для Exchange, ваша учетная запись должна состоять в группе "Администраторы предприятия".

Чтобы подготовить все домены в лесу Active Directory, выполните следующую команду в окне командной строки Windows:

Консоль

```
<Virtual DVD drive letter>:\Setup.exe
/IAcceptExchangeServerLicenseTerms_DiagnosticDataON /PrepareAllDomains
```

Например, если установочные файлы Exchange доступны на диске E:, выполните следующую команду:

Консоль

```
E:\Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON
/PrepareAllDomains
```

Выбор подготавливаемых доменов Active Directory

> **Совет**
>
> Это не нужно делать на том домене, где выполнялась команда */PrepareAD* на этапе 2, так как команда */PrepareAD* автоматически подготовила домен.

При подготовке определенных доменов в лесу Active Directory действуют следующие требования:

- Необходимо подготовить каждый домен, где будет установлен сервер Exchange Server.
- Вам потребуется подготовить все домены, на которых есть пользователи, поддерживающие почту, даже если на них нет серверов Exchange Server.
- Ваша учетная запись должна состоять в группе "Администраторы домена" на том домене, который требуется подготовить.
- Если нужный домен был создан **после** выполнения команды /PrepareAD на этапе 2, то ваша учетная запись также должна состоять в группе ролей "Управление организацией" Exchange.

Чтобы подготовить определенный домен в лесу Active Directory, выполните следующую команду в окне командной строки Windows:

Консоль

```
<Virtual DVD drive letter>:\Setup.exe
/IAcceptExchangeServerLicenseTerms_DiagnosticDataON /PrepareDomain[:
<DomainFQDN>]
```

> ⓘ **Примечание**
>
> - Если компьютер является членом домена, который требуется подготовить, можно использовать параметр */PrepareDomain* сам по себе. В противном случае необходимо указать полное доменное имя.
> - Это команду необходимо выполнить для каждого домена Active Directory, где будет установлен сервер Exchange Server или где будут находиться пользователи с включенной поддержкой почты.

В этом примере используются установочные файлы Exchange с диска E:, чтобы подготовить домен engineering.corp.contoso.com:

Консоль

```
E:\Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON
/PrepareDomain:engineering.corp.contoso.com
```

Это тот же пример, но реализованный на компьютере с домена engineering.corp.contoso.com:

Консоль

```
E:\Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON
/PrepareDomain
```

Как убедиться, что все получилось?

Чтобы убедиться, что вы успешно подготовили Active Directory и домены для Exchange, воспользуйтесь одним из следующих способов:

- Используйте редактор ADSI и сведения из таблиц в следующем разделе, чтобы убедиться, что указанные объекты имеют правильные значения для устанавливаемого выпуска Exchange. Дополнительные сведения об изменении ADSI см. в разделе Редактирование ADSI (adsiedit.msc).

> ⊗ **Внимание!**
>
> Никогда не изменяйте значения в редакторе ADSI, если вам не будет предложено сделать это службой поддержки и поддержкой Майкрософт. Изменение значений в редакторе ADSI может нанести непоправимый ущерб организации Exchange и Active Directory.

- Проверьте журнал установки Exchange, чтобы убедиться, что подготовка Active Directory успешно завершена. Дополнительные сведения см. в разделе Проверка установки Exchange. Обратите внимание, что вы не можете использовать командлет **Get-ExchangeServer** , как описано в этом разделе, пока не завершите установку хотя бы одного сервера почтовых ящиков Exchange на сайте Active Directory.

Вы можете использовать, https://aka.ms/ExSetupAssist если при выполнении команд подготовки AD возникает сбой.

Версии Active Directory для Exchange

Таблицы в следующих разделах содержат объекты Exchange в Active Directory, которые обновляются при каждой установке новой версии Exchange (новая установка или накопительный пакет обновления). Вы можете сравнить отображаемые версии объектов со значениями в таблицах, чтобы убедиться, что Exchange успешно обновил Active Directory во время установки.

- **rangeUpper** находится в контексте именования **Schema** (в свойствах контейнера **ms-Exch-Schema-Version-Pt**).
- **objectVersion (Default)** — это атрибут **objectVersion**, находящийся в **контексте именования Default** (в свойствах контейнера **Системные объекты Microsoft Exchange**).
- **objectVersion (Configuration)** — это атрибут **objectVersion**, расположенный в контексте именования **конфигурации** в **службах**>**Microsoft Exchange** в свойствах контейнера **Имя**> **вашей**< **организации Exchange**.

Версии Active Directory для Exchange 2019

Развернуть таблицу

Версия Exchange 2019	rangeUpper	objectVersion (по умолчанию)	objectVersion (конфигурация)
Exchange 2019 с накопительным пакетом обновления 14 (CU14)	17003	13243	16762
Exchange 2019 CU13	17003	13243	16761
Exchange 2019 CU12	17003	13243	16760
Exchange 2019 CU11 с KB5014260	17003	13243	16759
Exchange 2019 с накопительным пакетом обновления 11 (CU11)	17003	13242	16759
Exchange 2019 с накопительным пакетом обновления 10 (CU10)	17003	13241	16758
Exchange 2019 CU9	17002	13240	16757
Exchange 2019 с накопительным пакетом обновления 8 (CU8)	17002	13239	16756
Exchange 2019 с накопительным пакетом обновления 7 (CU7)	17001	13238	16755
Exchange 2019 с накопительным пакетом обновления 6 (CU6)	17001	13237	16754
Exchange 2019 с накопительным пакетом обновления 5 (CU5)	17001	13237	16754
Exchange 2019 с накопительным пакетом обновления 4 (CU4)	17001	13237	16754
Exchange 2019 с накопительным пакетом обновления 3 (CU3)	17001	13237	16754
Exchange 2019 с накопительным пакетом обновления 2 (CU2)	17001	13237	16754
Exchange 2019 с накопительным пакетом обновления 1 (CU1)	17000	13236	16752
Exchange 2019 RTM	17000	13236	16751
Ознакомительная версия Exchange 2019	15332	13236	16213

Развертывание новых установок Exchange

Статья • 04.04.2023

Прежде чем устанавливать Exchange Server, ознакомьтесь со статьей Планирование и развертывание. Она содержит важные сведения о планировании, а также о требованиях к системе и предварительных условиях.

Приведенные ниже статьи содержат сведения о развертывании новых установок Exchange 2019 в организации.

Установка серверов почтовых ящиков Exchange с помощью мастера

Установка Exchange в автоматическом режиме

Установка пограничных транспортных серверов Exchange с помощью мастера

Делегирование установки серверов Exchange Server

Среда разработки и тестирования Exchange в Azure

Завершив установку, см. статью Задачи, выполняемые после установки Exchange.

Установка серверов почтовых ящиков Exchange с помощью мастера установки

Статья • 04.04.2023

Прежде чем установить сервер почтовых ящиков Exchange Server 2016 или Exchange Server 2019, проверьте следующие предварительные требования:

- Проверьте требования к сети, компьютерному оборудованию, операционной системе и программному обеспечению, указанные в статьях Требования к системе для установки Exchange Server и Предварительные требования для Exchange Server.
- Целевой сервер должен быть членом домена Active Directory.
- Для учетной записи, используемой для установки Exchange, требуются следующие разрешения*:
  - **Членство в группе администраторов организации**. Обязательно, если это первый сервер Exchange Server в организации.
  - **Членство в группе администраторов схемы**. Обязательно, если вы еще не расширили схему Active Directory или не подготовили Active Directory для Exchange 2016 или Exchange 2019.
  - **Членство в группе ролей управления организацией Exchange**. Обязательно, если вы уже подготовили домен Active Directory, который будет содержать сервер Exchange Server, либо в организации уже есть другие серверы Exchange Server.

  * Члены группы ролей **Делегированная установка** могут устанавливать Exchange на серверах, которые уже подготовлены в Active Directory администратором Exchange. Для получения дополнительных сведений см. статью Делегирование установки серверов Exchange Server.
- Прочитайте заметки о выпуске в статье Заметки о выпуске Exchange Server.

Дополнительные сведения о планировании и развертывании Exchange см. в статье Планирование и развертывание Exchange Server.

Сведения об установке роли пограничного транспорта на компьютере см. в статье Установка пограничных транспортных серверов Exchange с помощью мастера

установки. Обратите внимание, что эту роль нельзя установить на сервере почтовых ящиков.

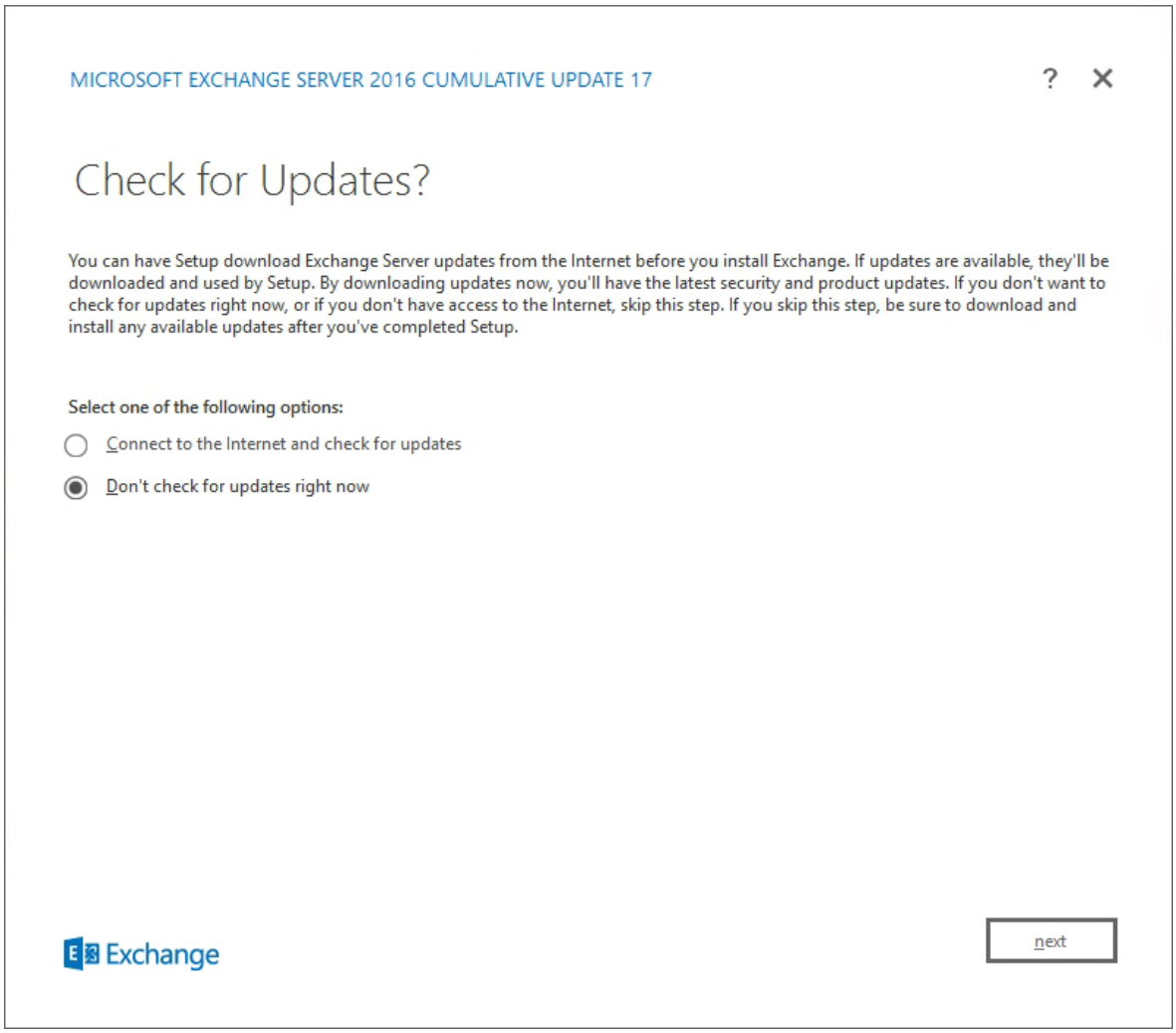
Что нужно знать перед началом работы

- Предполагаемое время для завершения: 60 минут.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

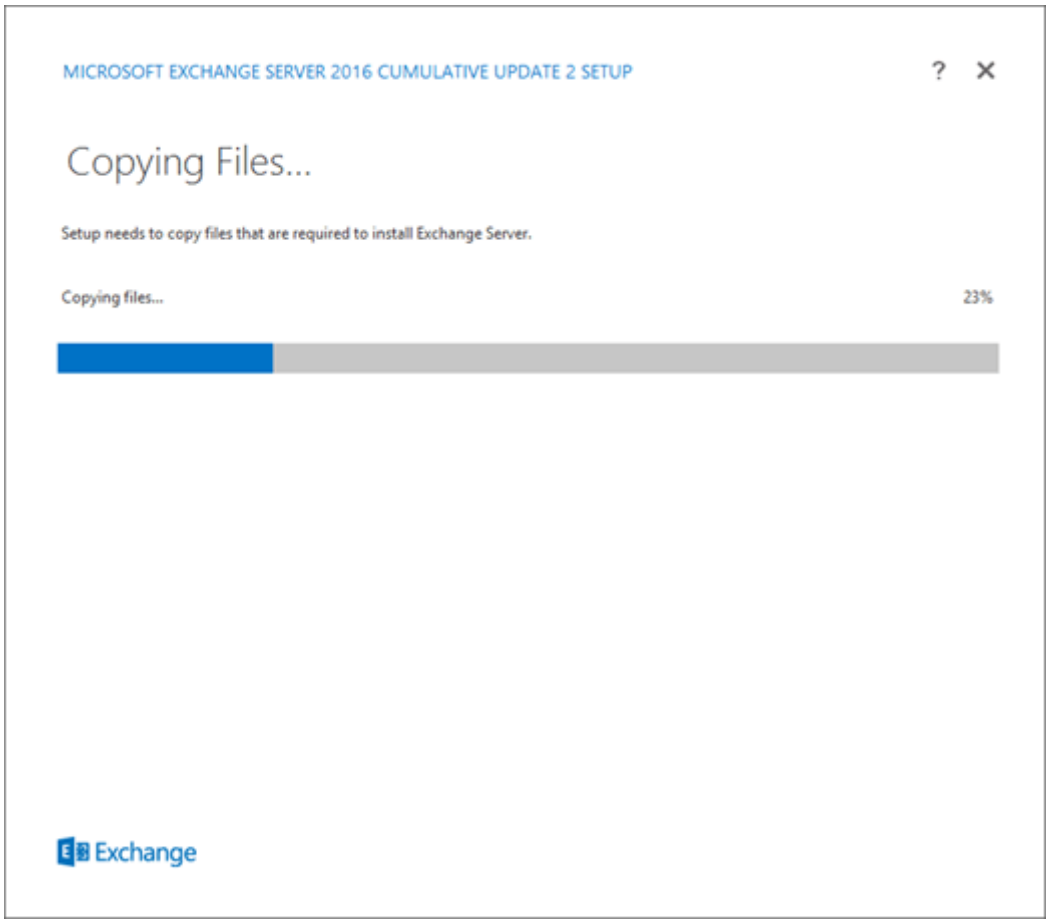
> ⊗ **Внимание!**
>
> После установки Exchange на сервере будет невозможно изменить его имя. Переименование сервера после установки роли сервера Exchange не поддерживается.

Установка роли сервера почтовых ящиков Exchange

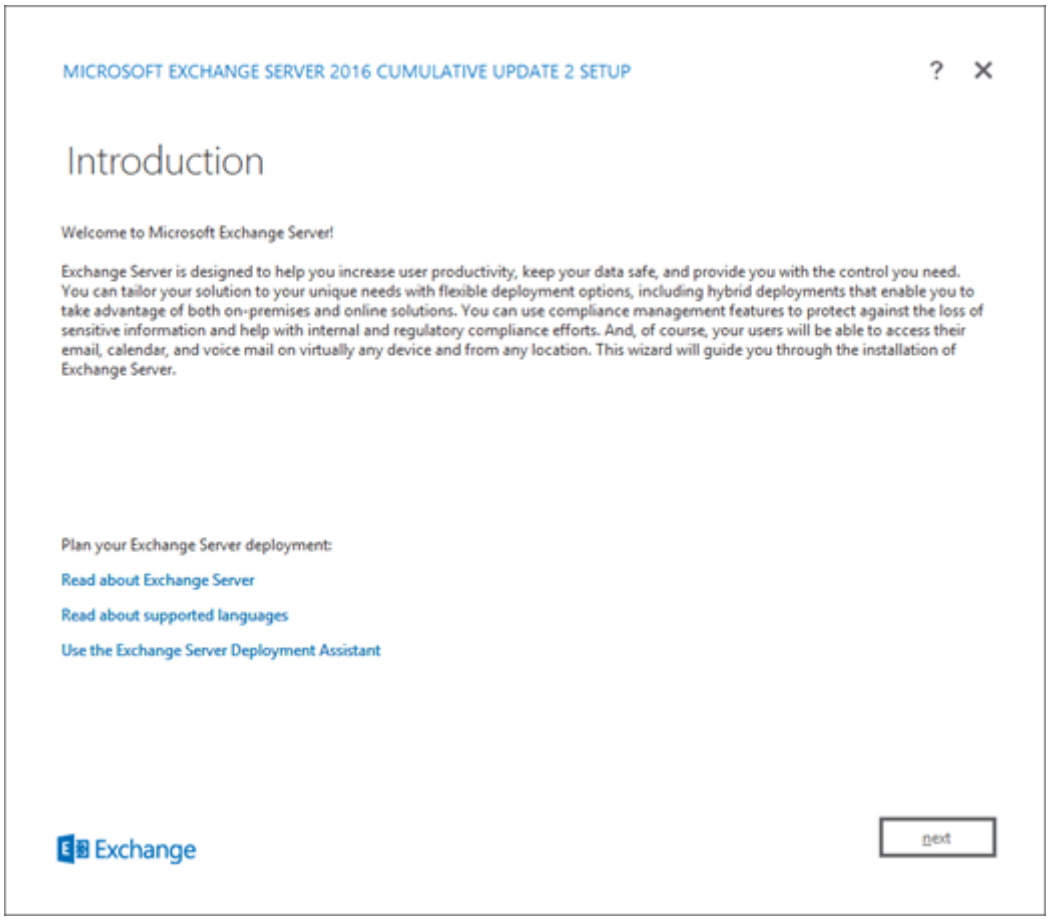
1. Скачайте последнюю версию Exchange. Дополнительные сведения см. в разделе Обновления для Exchange Server.
2. В проводнике щелкните скачанный файл ISO-образа Exchange правой кнопкой мыши и выберите **Подключить**. В появившемся появившемся виртуальном DVD-диске запустите программу установки Exchange, дважды щелкнув `Setup.exe`.
3. Откроется мастер установки Exchange Server. На странице **Проверить наличие обновлений** выберите один из предложенных ниже вариантов и нажмите кнопку **Далее** для продолжения.
    - **Подключитесь к Интернету и проверьте наличие обновлений**. Мы рекомендуем использовать этот параметр, который выполняет поиск обновлений для *устанавливаемой* версии Exchange (не обнаруживает новые накопительные Обновления). При выборе этого варианта вы автоматически будете перенаправлены на страницу **Скачивание обновлений**, где выполняется поиск обновлений. Для продолжения нажмите кнопку **Далее**.
    - **Не проверять обновления сейчас**.



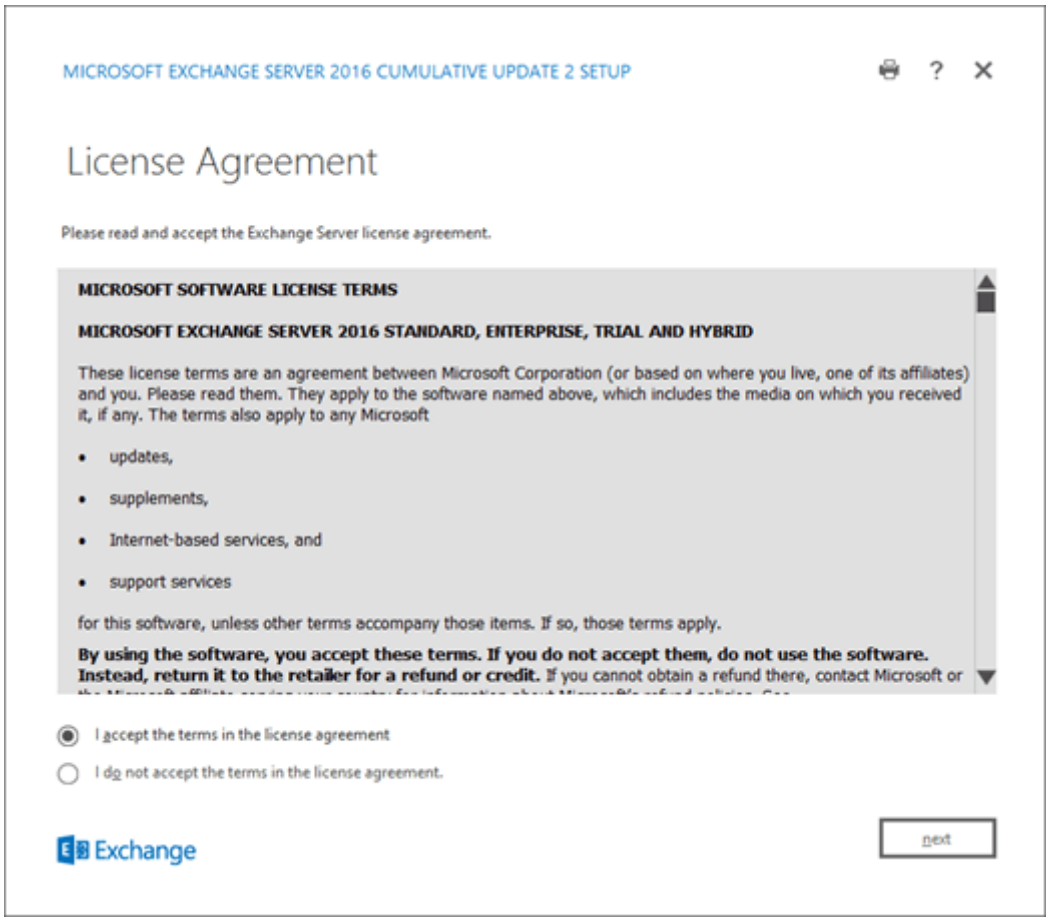
4. На странице **Копирование файлов** отображается ход выполнения копирования файлов на локальный жесткий диск. Как правило, файлы копируются в `%WinDir%\Temp\ExchangeSetup`, но вы можете подтвердить расположение в журнале установки Exchange по адресу `C:\ExchangeSetupLogs\ExchangeSetup.log`.



5. На странице **Введение** рекомендуется перейти по ссылкам планирования развертывания Exchange Server, если вы еще не ознакомились с ними. Для продолжения нажмите кнопку **Далее**.



6. На странице **Лицензионное соглашение** ознакомьтесь с условиями лицензионного соглашения на программное обеспечение, выберите **Я принимаю условия лицензионного соглашения** и нажмите **Далее**, чтобы продолжить.

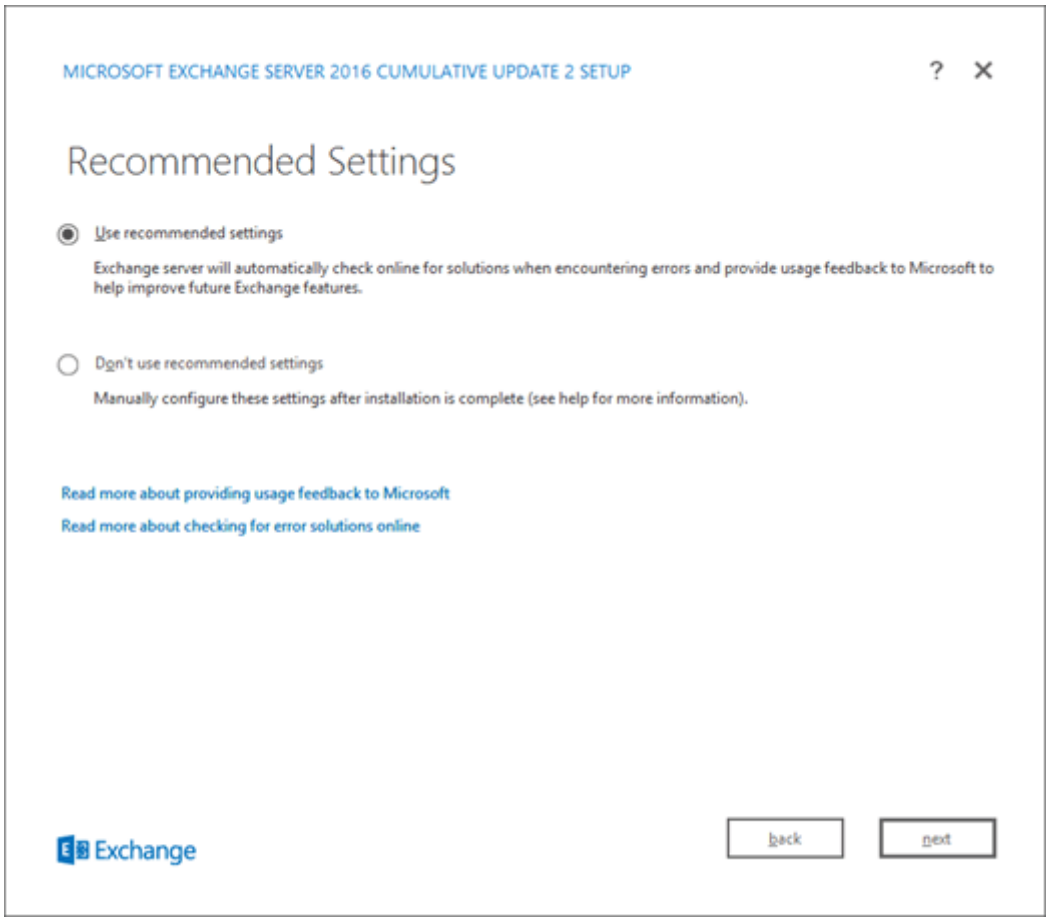


7. На странице **Рекомендуемые параметры** выберите один из следующих параметров:

   - **Использование рекомендуемых параметров**. Exchange автоматически отправляет отчеты об ошибках и сведения об оборудовании компьютера и способах использования Exchange в корпорацию Майкрософт. Для получения сведений о том, что отправляется в корпорацию Майкрософт и как они используются, щелкните **?** или ссылки на справку на странице.

   - **Не использовать рекомендованные параметры**. Эти параметры отключены, но вы в любое время можете включить их после завершения работы программы установки.

   Для продолжения нажмите кнопку **Далее**.

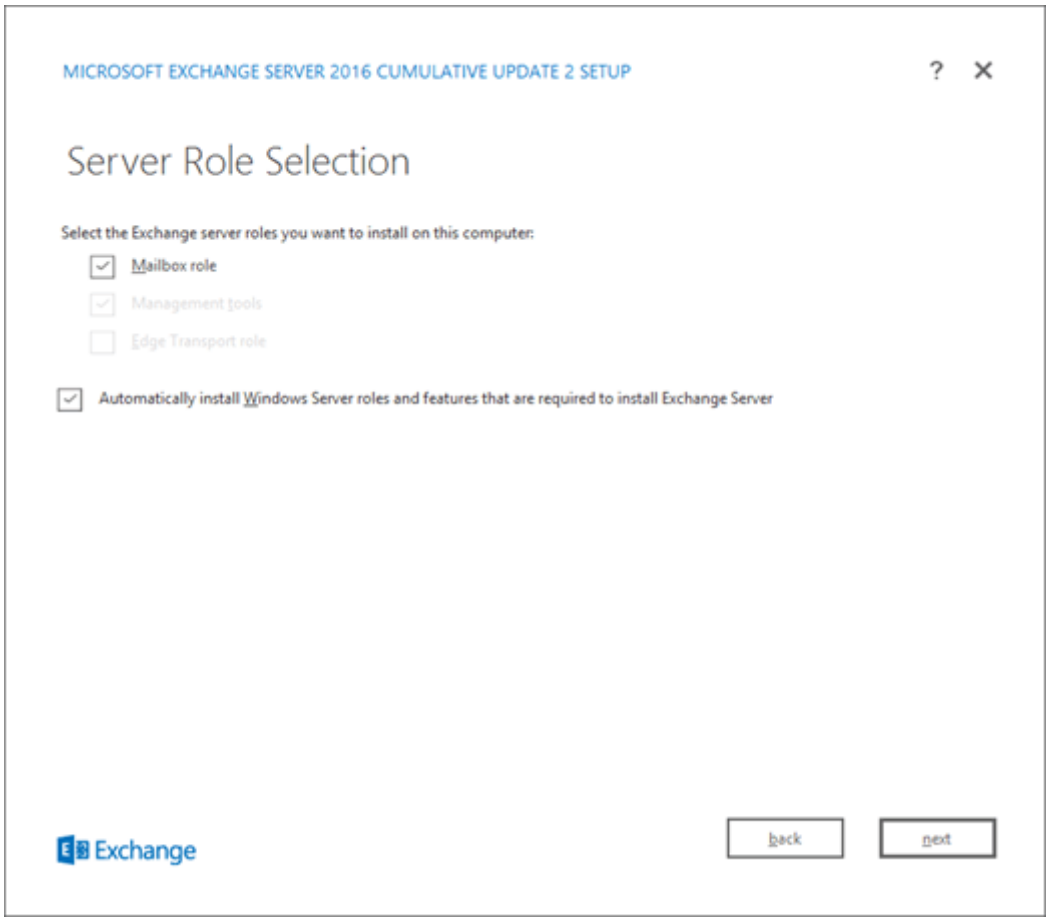


8. На странице **Выбор роли сервера** настройте следующие параметры:

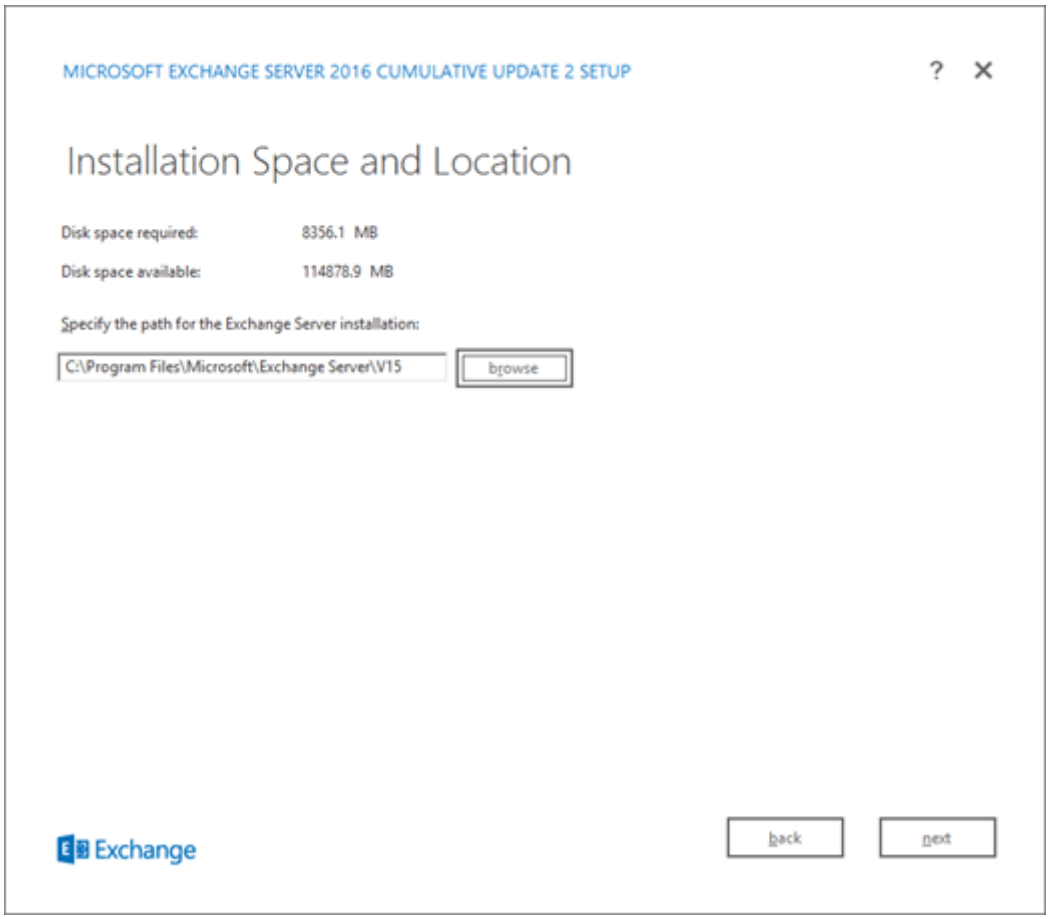
   - **Роль почтового ящика**. При выборе этого варианта также будут автоматически установлены **средства управления**.
   - **Автоматическая установка ролей и компонентов Windows Server, необходимых для установки Exchange**. Выберите этот параметр, чтобы мастер установки установил необходимые компоненты Windows. Для завершения установки некоторых компонентов Windows может потребоваться перезагрузить компьютер. Если этот параметр не выбран, необходимо установить компоненты Windows вручную.

   Примечание. При выборе этого параметра устанавливаются только *компоненты Windows* , необходимые exchange. Другие необходимые компоненты необходимо установить вручную. Дополнительные сведения см. в разделе предварительные требования Exchange Server.

   Для продолжения нажмите кнопку **Далее**.



9. На странице **Место установки и расположение** либо примите расположение установки по умолчанию (`C:\Program Files\Microsoft\Exchange Server\V15`), либо нажмите кнопку **Обзор** , чтобы выбрать новое расположение. Убедитесь, что в расположении для установки службы Exchange достаточно доступного дискового пространства. Для продолжения нажмите кнопку **Далее**.



10. Если это первый сервер Exchange 2016 или Exchange 2019 в вашей организации и вы еще не выполнили действия, описанные в разделе Подготовка Active Directory и доменов для Exchange, вы откроете страницу **Организация Exchange** . На этой странице настройте следующие параметры:

    - **Укажите имя для этой организации Exchange**. Значение по умолчанию — **First Organization**, но для этого значения обычно используется название компании. Название организации используется внутри Exchange — оно, как правило, невидимо для пользователей, не влияет на функциональность Exchange и не определяет доступные адреса электронной почты.

      - Название организации не должно быть длиннее 64 символов и не может быть пустым.

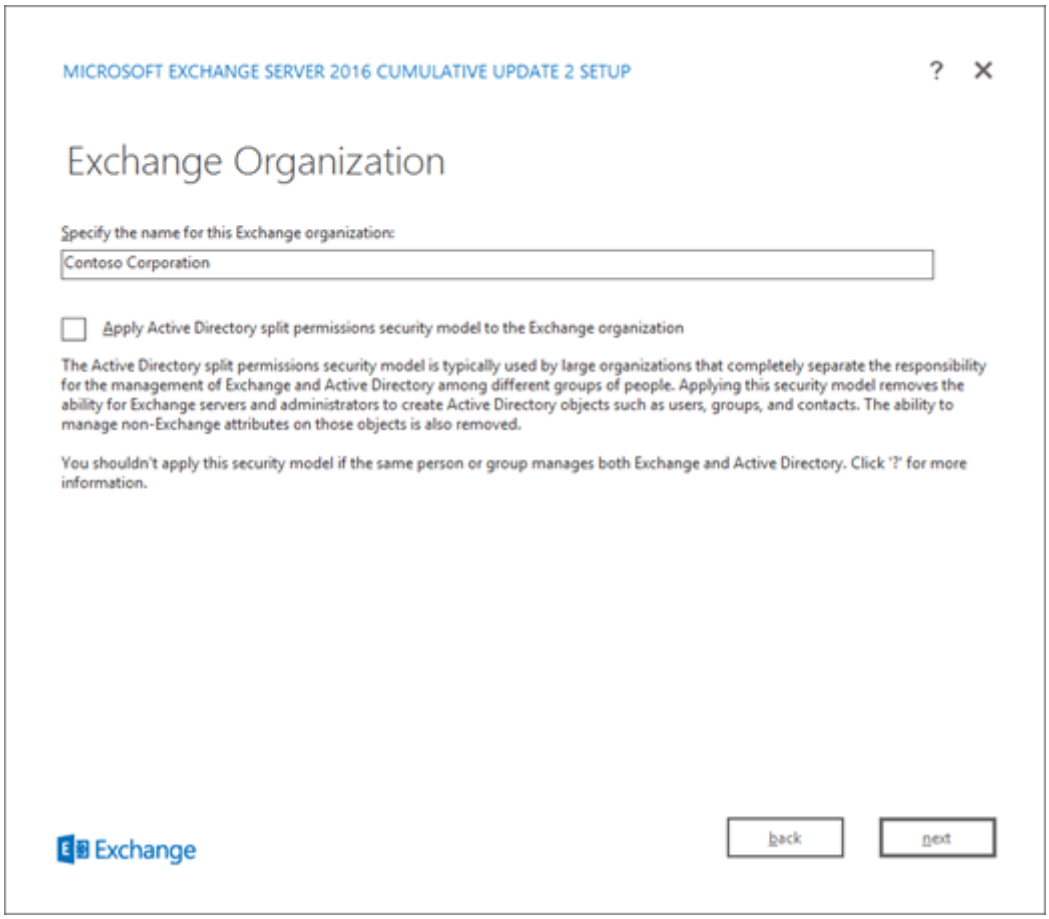
      - Допустимые символы — от A до Z, от a до z, от 0 до 9, дефис или тире (-) и пробел, но пробелов не должно быть в начале и конце названия.

      - Указанное название организации нельзя изменить.

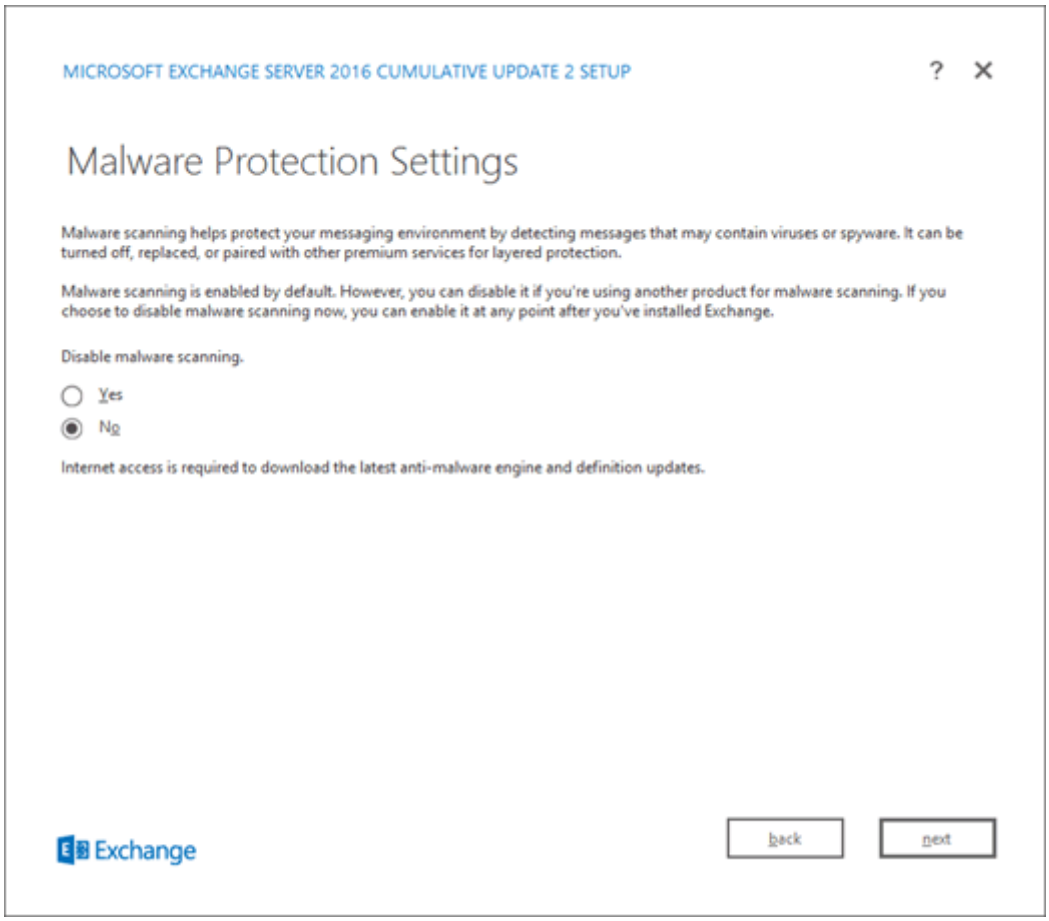
    - **Применение модели безопасности разделенных разрешений Active Directory к организации Exchange**. Большинству организаций не нужно выбирать этот параметр. Если вам нужно разделить управление субъектами безопасности Active Directory и конфигурацию Exchange, вам

могут пригодиться разделенные разрешения. Выберите **?** для получения дополнительных сведений.

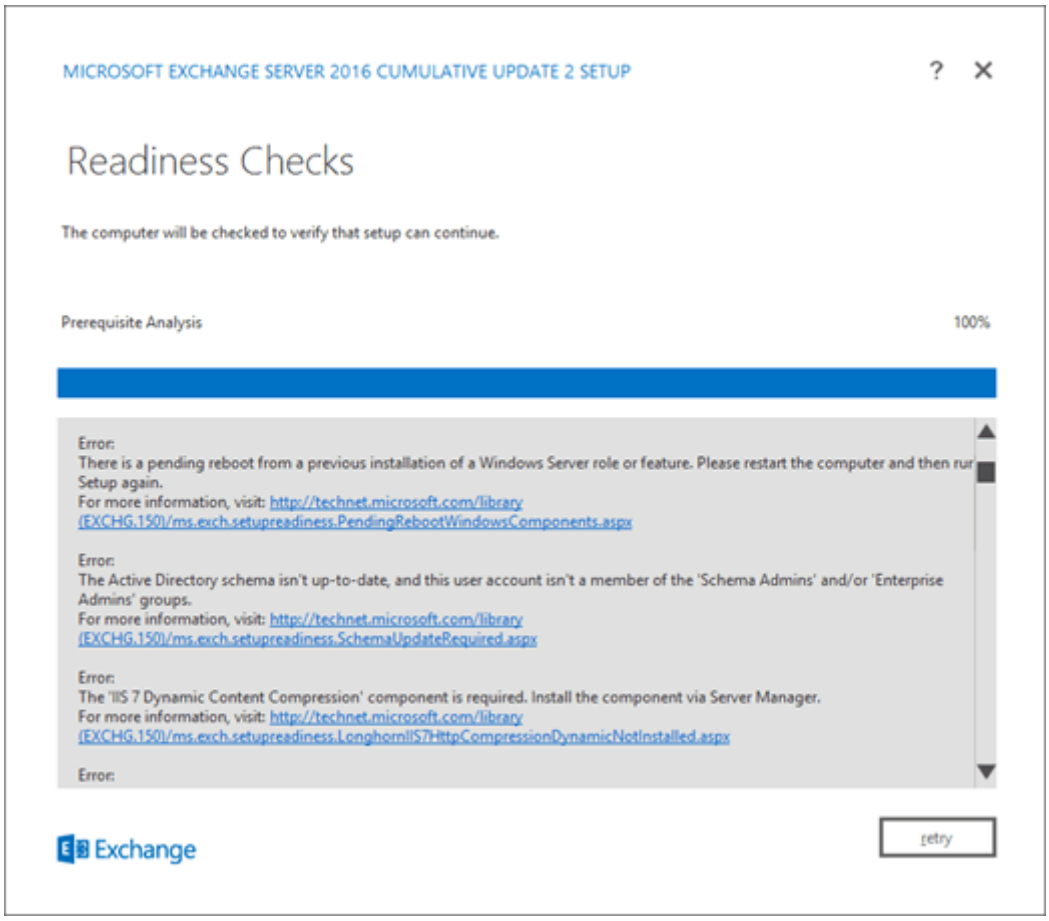
Для продолжения нажмите кнопку **Далее**.



11. На странице **Параметры защиты от вредоносных программ** можно отключить проверку на наличие вредоносных программ. По умолчанию проверка на наличие вредоносных программ включена (выбрано значение **Нет**). Если вы отключите проверку на наличие вредоносных программ, ее можно будет включить позже. Для продолжения нажмите кнопку **Далее**.

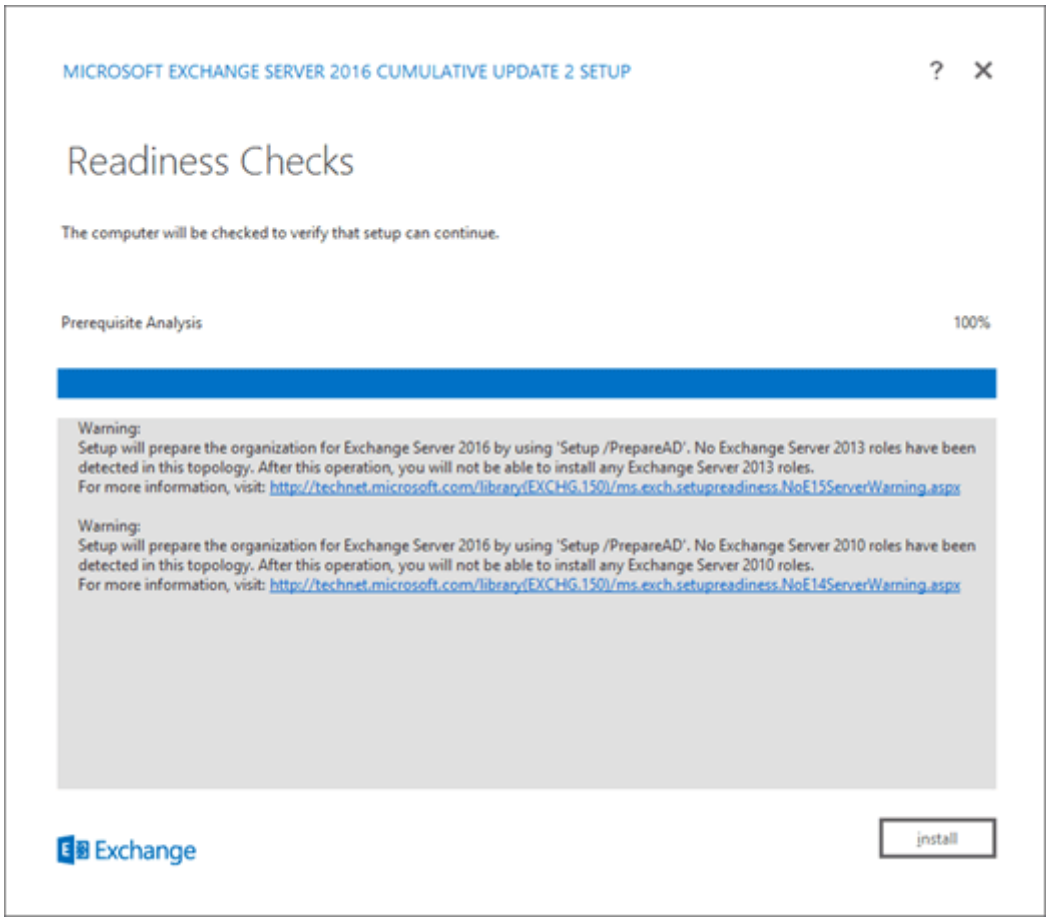


12. На странице **Проверки готовности** убедитесь, что проверки готовности организации и роли сервера выполнены успешно. В противном случае на странице будет отображаться только кнопка **Повторить**.

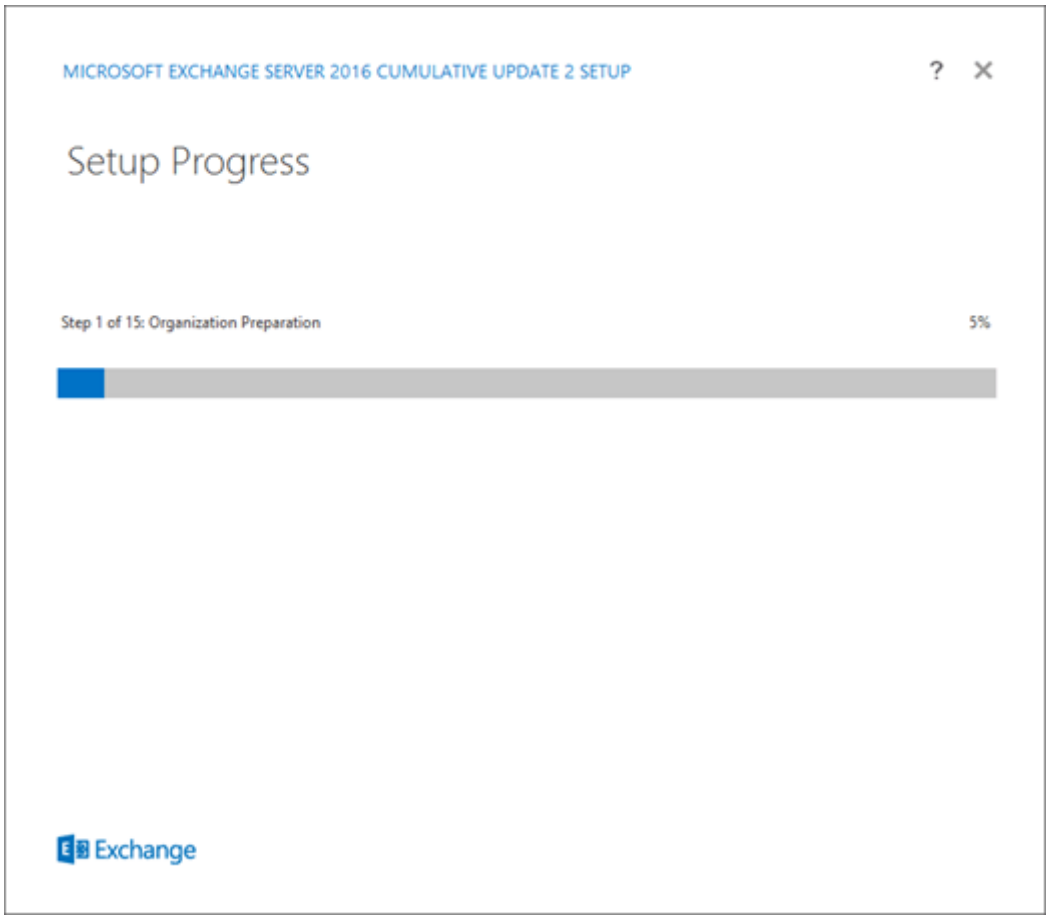


Устранив ошибки, нажмите кнопку **Повторить попытку**, чтобы снова запустить проверки наличия обязательных компонентов. Некоторые ошибки можно исправить, не выходя из программы установки, а для исправления других понадобится перезагрузить компьютер. После перезагрузки компьютера придется начинать с шага 1.

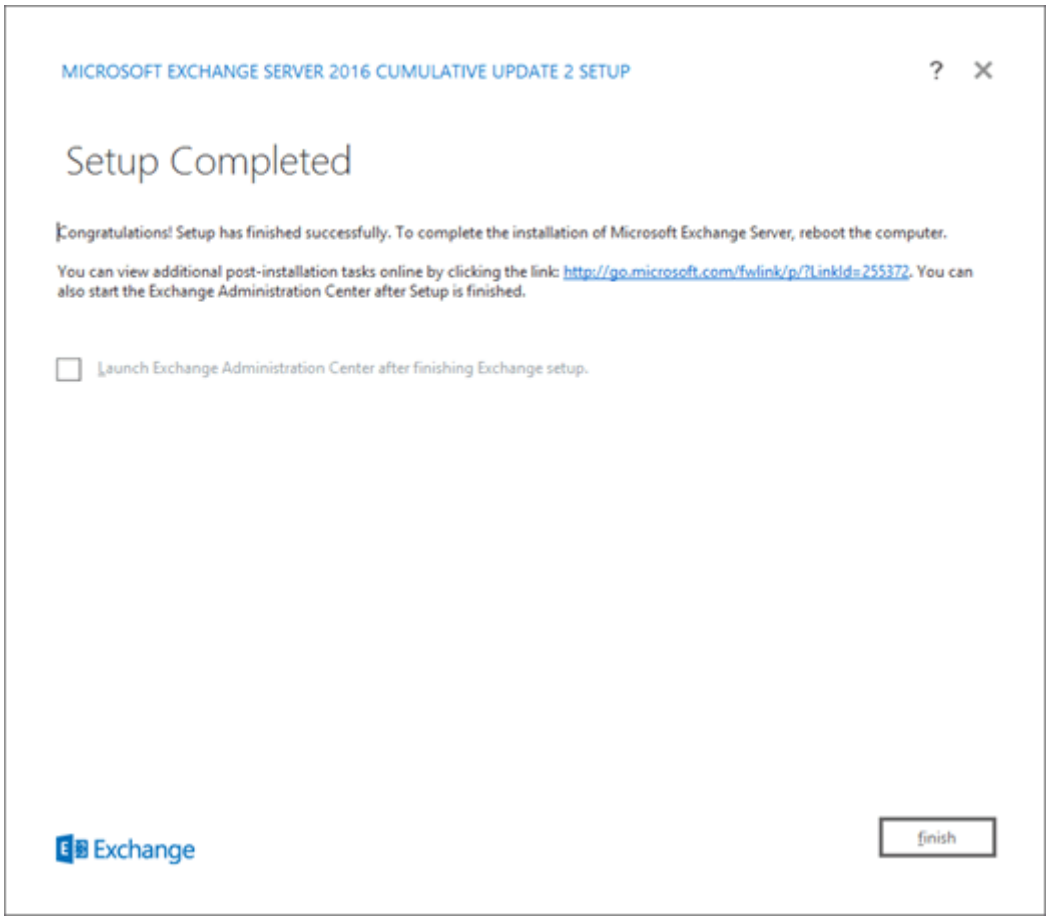
Когда на странице **Проверки готовности** больше не будет ошибок, на месте кнопки **Повторить** появится кнопка **Установить**. Обязательно просмотрите все предупреждения и нажмите кнопку **Установить** , чтобы установить Exchange.



13. На странице **Ход установки** отображается индикатор хода установки.



14. На странице **Установка завершена** нажмите **Готово** и перезагрузите компьютер.



Дальнейшие действия

- Чтобы убедиться в успешности установки Exchange, выполните действия, указанные в статье Проверка установки Exchange.
- Завершите развертывание, выполнив задачи, описанные в статье Задачи, которые необходимо выполнить после установки Exchange.
- Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу Exchange Server.

Установка пограничных транспортных серверов Exchange с помощью мастера

Статья • 04.04.2023

Прежде чем установить пограничный транспортный сервер Exchange Server 2016 или Exchange Server 2019, проверьте следующие предварительные требования:

- Рекомендуется установить пограничные транспортные серверы в сети периметра, которая находится за пределами внутреннего леса Active Directory вашей организации. Установка роли пограничного транспортного сервера на присоединенных к домену компьютерах позволяет управлять только функциями и параметрами Windows. Пограничные транспортные серверы не обращаются напрямую к Active Directory. Вместо этого они используют службы Active Directory облегченного доступа к каталогу (AD LDS) для хранения сведений о конфигурации и получателях. Дополнительные сведения о роли пограничного транспорта см. в разделе Пограничные транспортные серверы.

> ⓘ **Примечание**
>
> Если пограничный транспортный сервер Exchange Server 2019 присоединен к домену, пользователь из этого домена должен запустить командную консоль Exchange. Если локальный пользователь подключается к серверу, командлеты в командной консоли Exchange приведут к отказу в доступе.

- Проверьте требования к сети, компьютерному оборудованию, операционной системе и программному обеспечению, указанные в статьях Требования к системе для установки Exchange Server и Предварительные требования для Exchange Server.

- Убедитесь, что локальная учетная запись на целевом компьютере входит в локальную группу администраторов.

- Прочитайте заметки о выпуске в статье Заметки о выпуске сервера Exchange Server.

Дополнительные сведения о планировании и развертывании Exchange см. в статье Планирование и развертывание Exchange Server.

Сведения об установке роли почтового ящика на компьютере см. в статье Установка серверов почтовых ящиков Exchange с помощью мастера установки. Обратите внимание, что эту роль нельзя установить на сервере почтовых ящиков.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 40 минут.
- На компьютере необходимо настроить основной DNS-суффикс. Например, если полное доменное имя компьютера — edge.contoso.com, то суффиксом DNS компьютера будет contoso.com. Дополнительные сведения см. в разделе Отсутствует основной DNS-суффикс [ms.exch.setupreadiness.FqdnMissing].
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

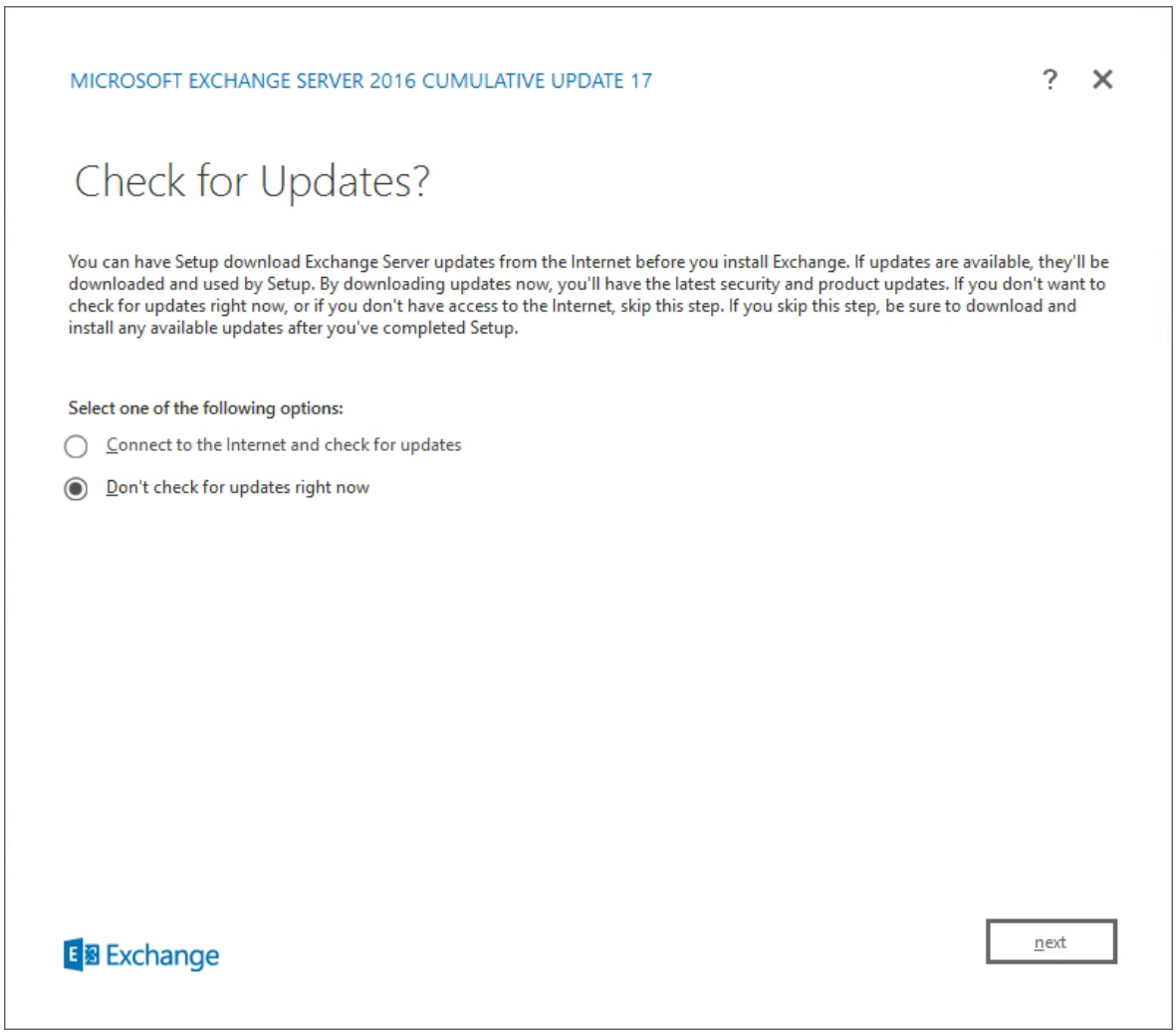
> ⊗ **Внимание!**
>
> После установки Exchange на сервере будет невозможно изменить его имя. Переименование сервера после установки роли сервера Exchange не поддерживается.

Установка роли пограничного транспортного сервера в Exchange

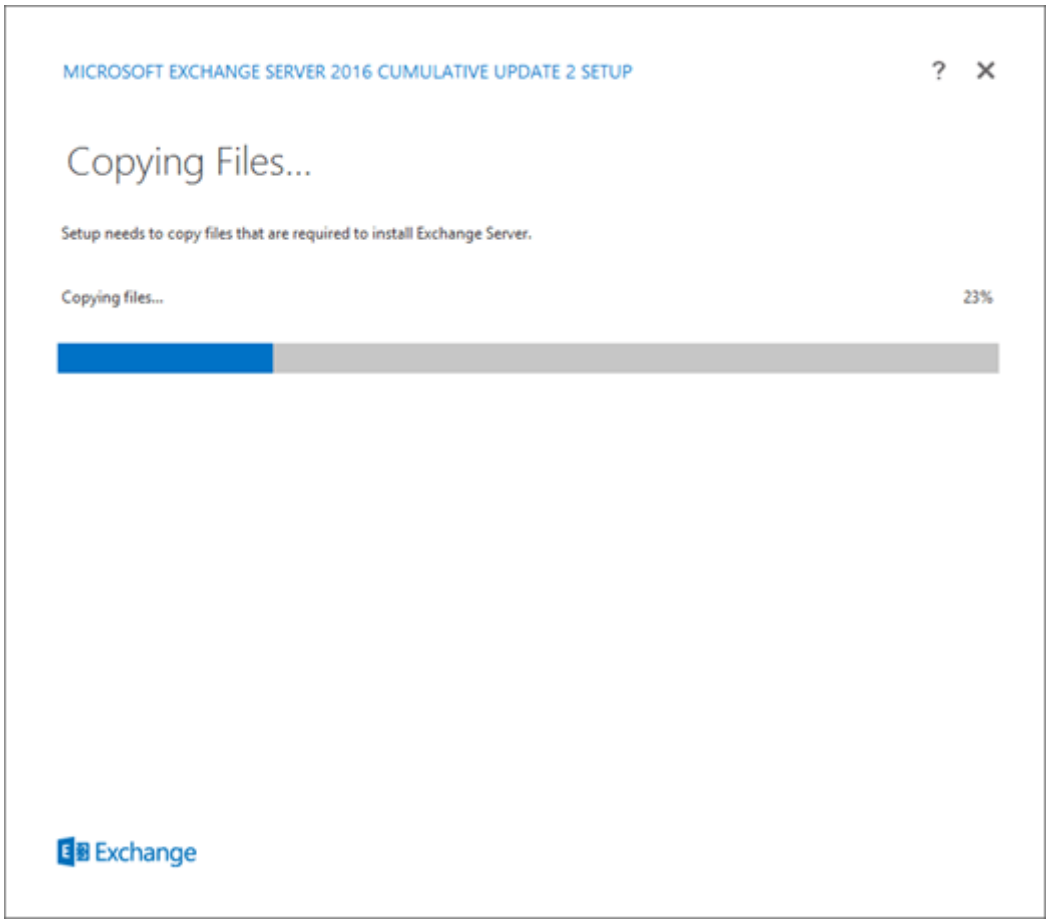
1. Скачайте последнюю версию Exchange. Дополнительные сведения см. в разделе Обновления для Exchange Server.
2. В проводнике щелкните скачанный файл ISO-образа Exchange правой кнопкой мыши и выберите **Подключить**. В появившемся появившемся виртуальном DVD-диске запустите программу установки Exchange, дважды щелкнув `Setup.exe`.
3. Откроется мастер установки Exchange Server. На странице **Проверить наличие обновлений** выберите один из предложенных ниже вариантов и нажмите кнопку **Далее** для продолжения.
    - **Подключитесь к Интернету и проверьте наличие обновлений**. Мы рекомендуем использовать этот параметр, который выполняет поиск обновлений для *устанавливаемой* версии Exchange (не обнаруживает новые накопительные Обновления). При выборе этого варианта вы

автоматически будете перенаправлены на страницу **Скачивание обновлений**, где выполняется поиск обновлений. Для продолжения нажмите кнопку **Далее**.

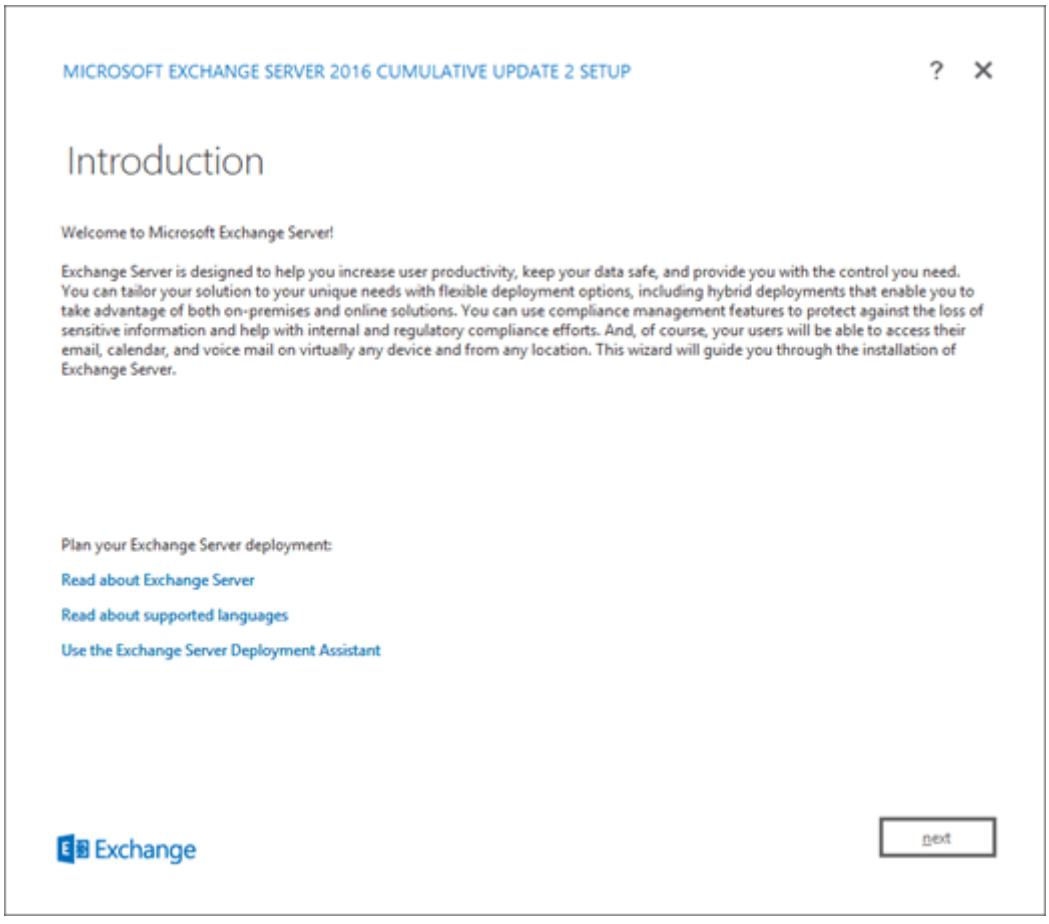
- **Не проверять обновления сейчас**.



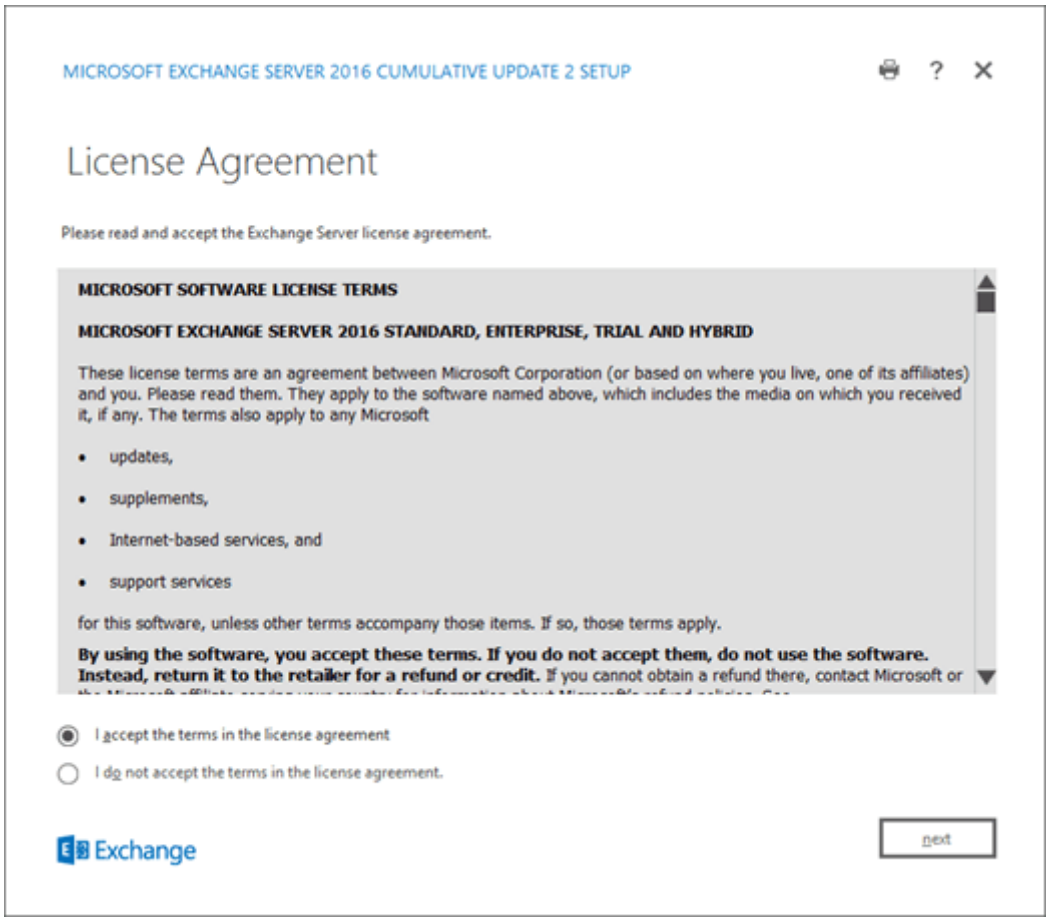
4. На странице **Копирование файлов** отображается ход выполнения копирования файлов на локальный жесткий диск. Как правило, файлы копируются в `%WinDir%\Temp\ExchangeSetup`, но вы можете подтвердить расположение в журнале установки Exchange по адресу `C:\ExchangeSetupLogs\ExchangeSetup.log`.



5. На странице **Введение** рекомендуется перейти по ссылкам планирования развертывания Exchange Server, если вы еще не ознакомились с ними. Для продолжения нажмите кнопку **Далее**.



6. На странице **Лицензионное соглашение** ознакомьтесь с условиями лицензионного соглашения на программное обеспечение, выберите **Я принимаю условия лицензионного соглашения** и нажмите **Далее**, чтобы продолжить.

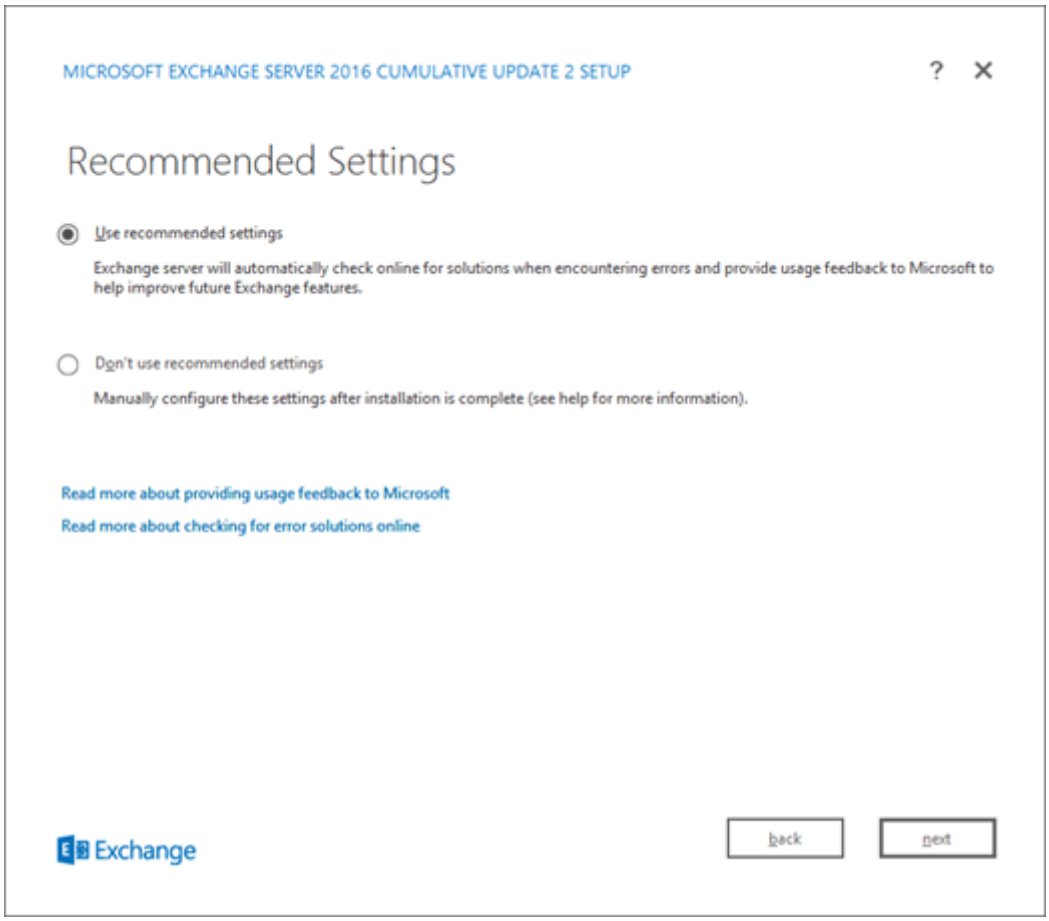


7. На странице **Рекомендуемые параметры** выберите один из следующих параметров:

   - **Использование рекомендуемых параметров**. Exchange автоматически отправляет отчеты об ошибках и сведения об оборудовании компьютера и способах использования Exchange в корпорацию Майкрософт. Для получения сведений о том, что отправляется в корпорацию Майкрософт и как они используются, щелкните **?** или ссылки на справку на странице.

   - **Не использовать рекомендованные параметры**. Эти параметры отключены, но вы в любое время можете включить их после завершения работы программы установки.

   Для продолжения нажмите кнопку **Далее**.



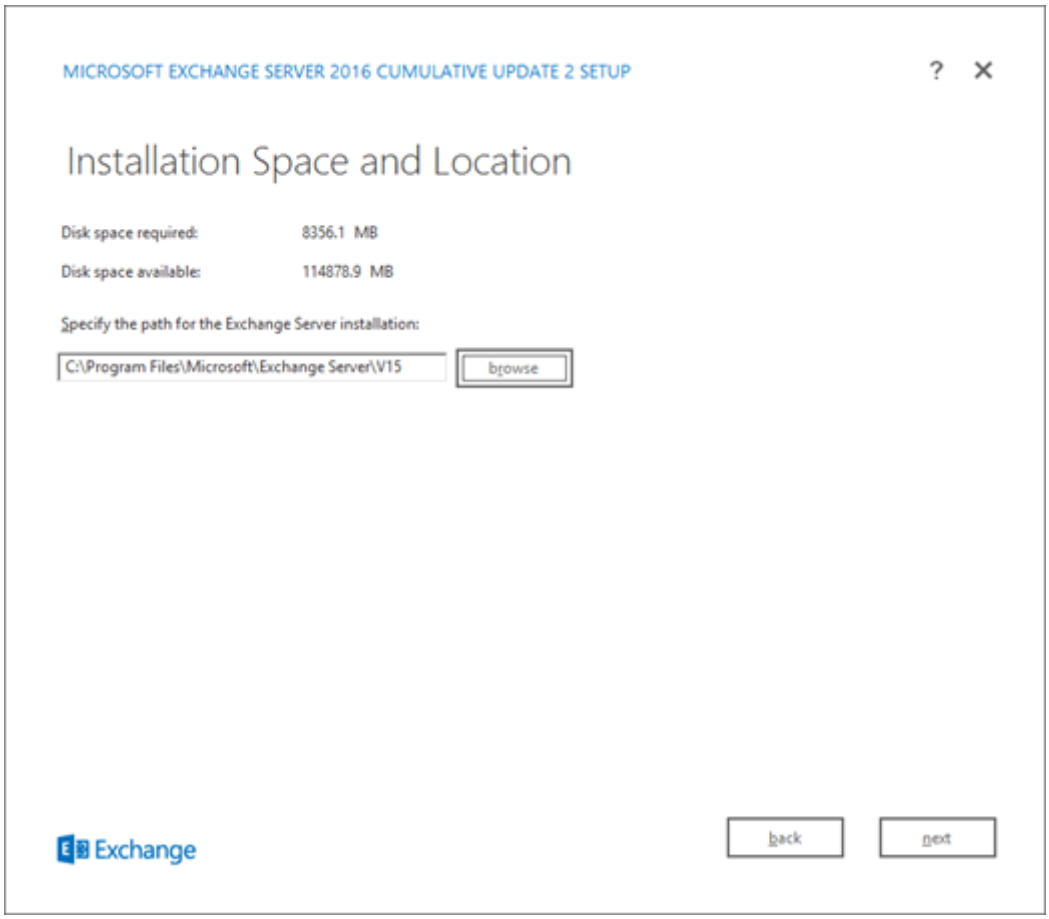
8. На странице **Выбор роли сервера** настройте следующие параметры:

   - **Роль пограничного транспортного сервера**. При выборе этого варианта также будут автоматически установлены **средства управления**.
   - **Автоматическая установка ролей и компонентов Windows Server, необходимых для установки Exchange**. Выберите этот параметр, чтобы мастер установки установил необходимые компоненты Windows. Для завершения установки некоторых компонентов Windows может потребоваться перезагрузить компьютер. Если этот параметр не выбран, необходимо установить компоненты Windows вручную.

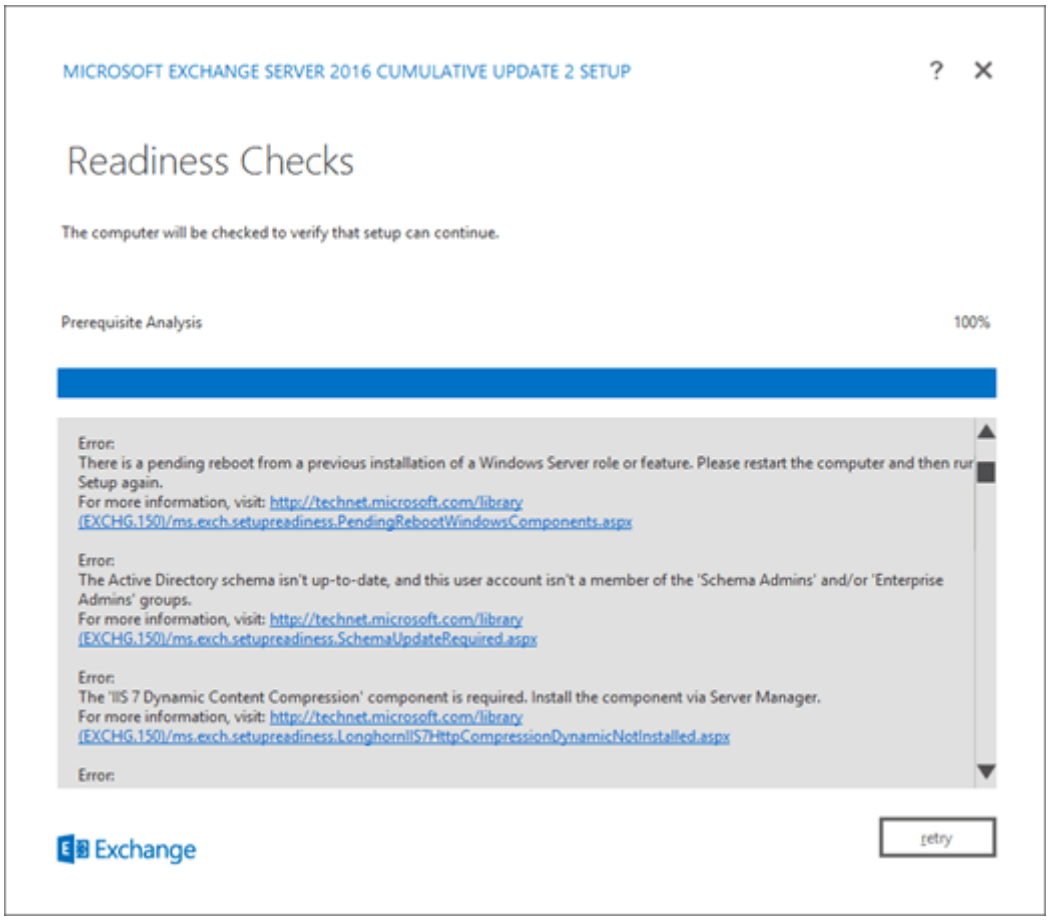
   Примечание. При выборе этого параметра устанавливаются только *компоненты Windows* , необходимые exchange. Другие необходимые компоненты необходимо установить вручную. Дополнительные сведения см. в разделе предварительные требования Exchange Server.

   Для продолжения нажмите кнопку **Далее**.

9. На странице **Место установки и расположение** либо примите расположение установки по умолчанию (`C:\Program Files\Microsoft\Exchange Server\V15`), либо нажмите кнопку **Обзор** , чтобы выбрать новое расположение. Убедитесь, что в расположении для установки службы Exchange достаточно доступного дискового пространства. Для продолжения нажмите кнопку **Далее**.

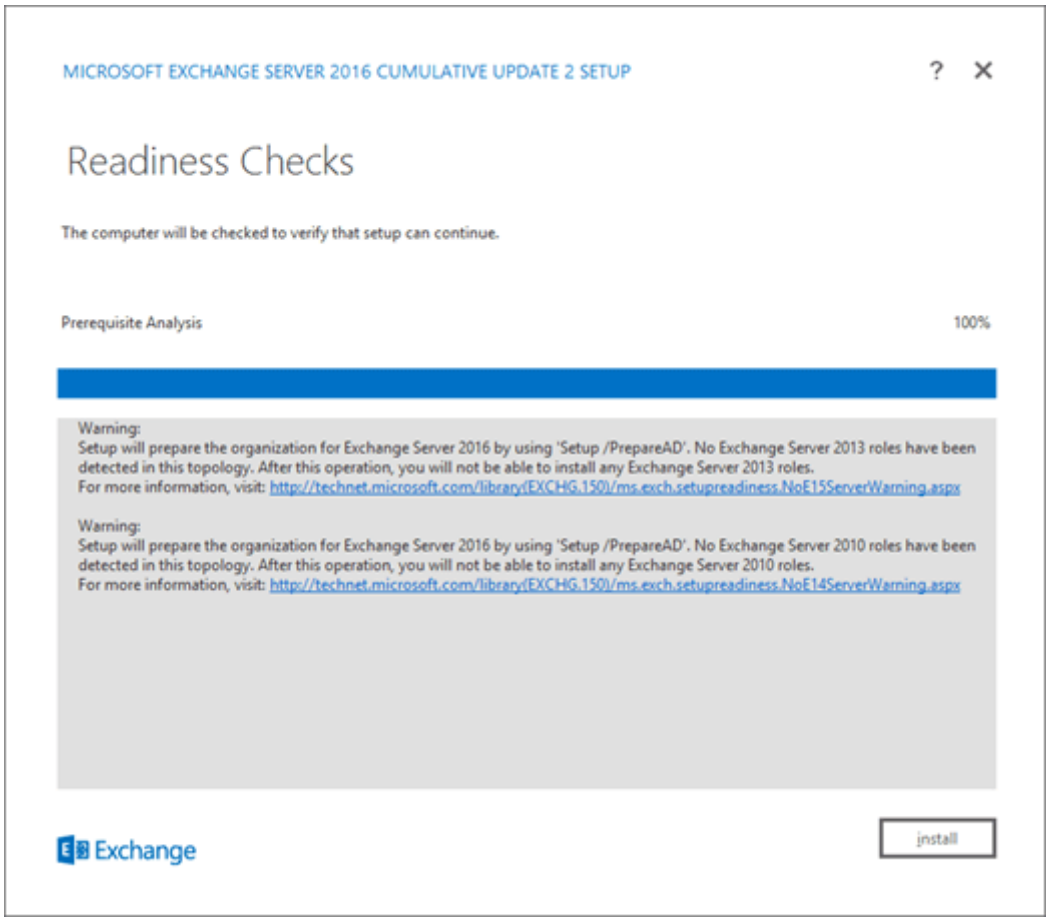


10. На странице **Проверки готовности** убедитесь, что проверки готовности организации и роли сервера выполнены успешно. В противном случае на странице будет отображаться только кнопка **Повторить**.

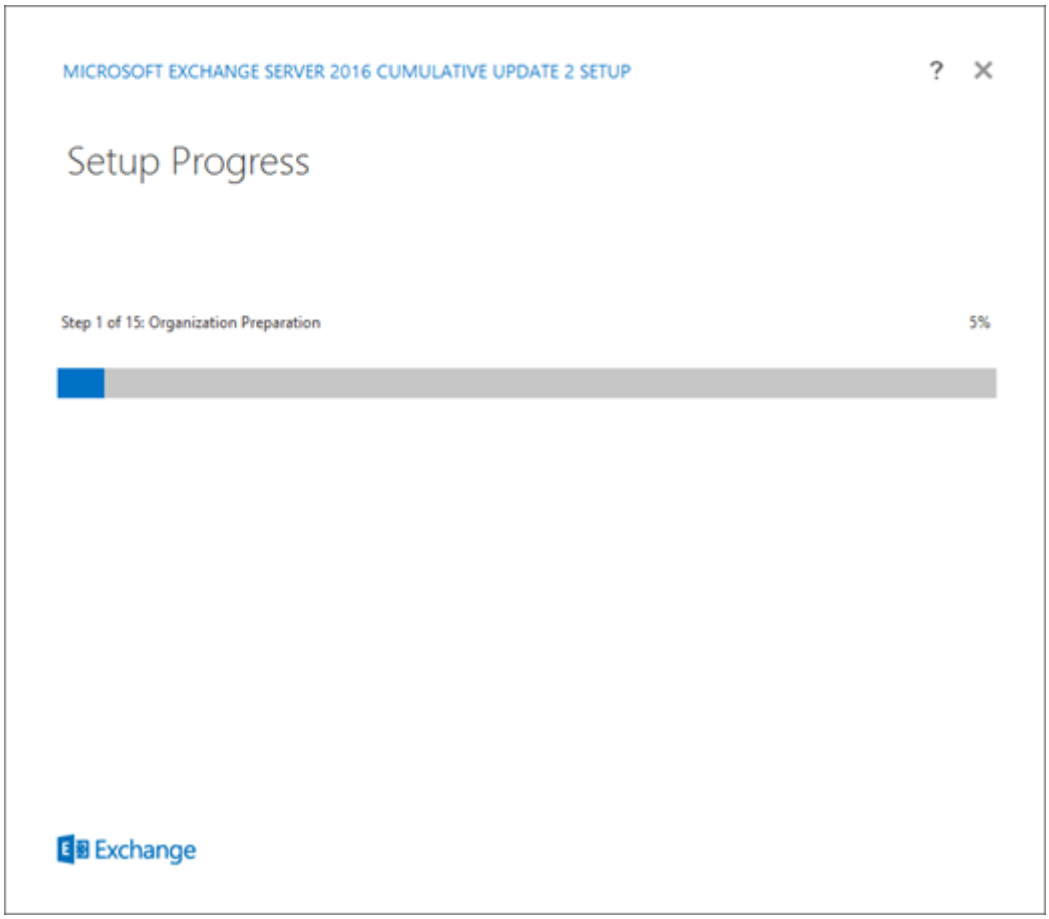


Устранив ошибки, нажмите кнопку **Повторить попытку**, чтобы снова запустить проверки наличия обязательных компонентов. Некоторые ошибки можно исправить, не выходя из программы установки, а для исправления других понадобится перезагрузить компьютер. После перезагрузки компьютера придется начинать с шага 1.

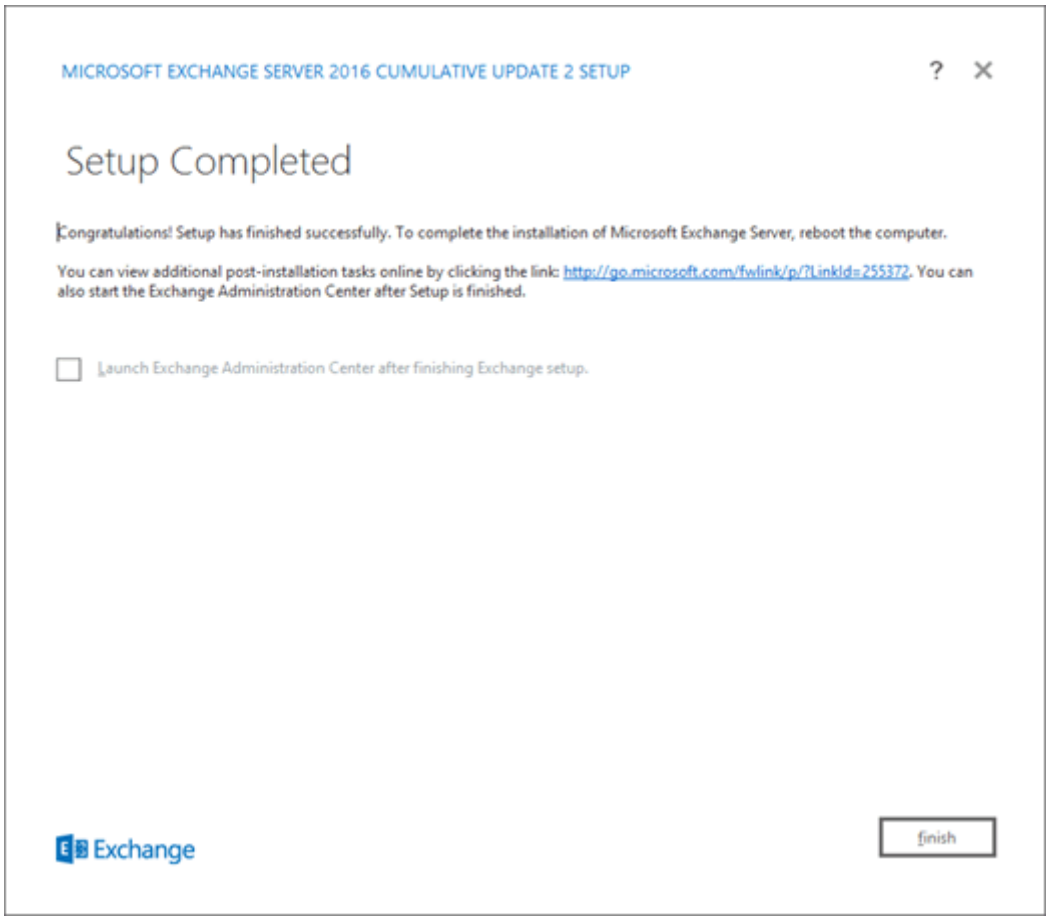
Когда на странице **Проверки готовности** больше не будет ошибок, на месте кнопки **Повторить** появится кнопка **Установить**. Обязательно просмотрите все предупреждения и нажмите кнопку **Установить** , чтобы установить Exchange.



11. На странице **Ход установки** отображается индикатор хода установки.



12. На странице **Установка завершена** нажмите **Готово** и перезагрузите компьютер.



Дальнейшие действия

- Чтобы убедиться в успешности установки Exchange, выполните действия, указанные в статье Проверка установки Exchange.
- Завершите развертывание, выполнив задачи, описанные в статье Задачи, которые необходимо выполнить после установки Exchange.
- Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server .

Использование автоматического режима в программе установки Exchange

Статья • 04.04.2023

Запуск программы установки Exchange из командной строки позволяет автоматизировать установку Exchange и выполнять другие связанные задачи на серверах Exchange Server (например, удалить существующий сервер Exchange Server или восстановить сервер Exchange Server после сбоя).

В этой статье описаны доступные параметры командной строки, а также приводятся примеры их использования.

Дополнительные сведения о планировании для Exchange 2016 или Exchange 2019 см. в статье Планирование и развертывание сервера Exchange Server.

Сведения о задачах, которые необходимо выполнить после установки, см. в статье Задачи после установки сервера Exchange Server.

Основные параметры командной строки для автоматического режима

В приведенной ниже таблице описаны основные параметры командной строки (верхний уровень, определение сценария), доступные в режиме автоматической установки в Exchange 2016 или Exchange 2019:

Параметр	Описание
/IAcceptExchangeServerLicenseTerms	**Примечание.** Начиная с накопительных пакетов обновления за сентябрь 2021 г. этот параметр больше не доступен в Exchange Server 2016 и Exchange Server 2019. Этот параметр необходим во всех командах автоматической установки (при выполнении Setup.exe с любыми дополнительными параметрами). Если вы не используете этот параметр, вы получите сообщение об ошибке. Чтобы ознакомиться с условиями лицензионного соглашения, ознакомьтесь с условиями лицензионного соглашения Майкрософт.
/IAcceptExchangeServerLicenseTerms_DiagnosticDataON /IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF	**Примечание.** Эти параметры доступны начиная с накопительных пакетов обновления за сентябрь 2021 г. для Exchange Server 2016 и Exchange Server 2019. Один из этих параметров необходим во всех командах автоматической установки (при каждом запуске Setup.exe с любыми дополнительными параметрами). Если вы не используете один из этих параметров, вы получите сообщение об ошибке. Чтобы ознакомиться с условиями лицензионного соглашения, ознакомьтесь с условиями лицензионного соглашения Майкрософт. Чтобы принять условия лицензии и отправлять диагностические данные в Майкрософт, используйте параметр с суффиксом *DiagnosticDataON*. Чтобы принять условия лицензии, но не отправлять диагностические данные в Майкрософт, используйте параметр с суффиксом *DiagnosticDataOFF*.
/Mode:<InstallationMode> (или */m:<InstallationMode>*)	Допустимые значения: • **Установка**. Устанавливает Exchange на новом сервере с помощью ролей сервера Exchange, указанных параметром */Roles* . Это значение по умолчанию, если команда не использует параметр */Mode* . • **Uninstall**: удаляет Exchange с рабочего сервера. • **Upgrade**: устанавливает накопительный пакет обновления (CU) на Exchange Server. • **RecoverServer**. Восстанавливает сервер Exchange Server с помощью существующего объекта Exchange Server в Active Directory после катастрофического сбоя оборудования или программного обеспечения на сервере. Инструкции см. в разделе Восстановление серверов Exchange.
/Roles:<ServerRole> (или */Role:<ServerRole>*, или */r:<ServerRole>*)	Этот параметр является обязательным в `/Mode:Install` командах. Допустимые значения: • **Почтовый ящик (или мб):** устанавливает роль сервера почтовых ящиков и средства управления Exchange на локальном сервере. Это значение используется по умолчанию. Это значение нельзя использовать с **EdgeTransport**. • **EdgeTransport (или et)**: устанавливает роль пограничного транспортного сервера и средства управления Exchange на локальном сервере. Это значение нельзя использовать с **почтовым ящиком**. • **ManagementTools (или mt, или t)**: устанавливает средства управления Exchange на клиенты или другие серверы Windows, не под управлением Exchange.

Параметр	Описание
/PrepareAD (или */p*) */PrepareSchema* (или */ps*) */PrepareDomain:<DomainFQDN>* (или */pd:<DomainFQDN>*) */PrepareAllDomains* (или */pad*)	Используйте эти параметры для расширения схемы Active Directory для Exchange, подготовки Active Directory для Exchange и подготовки некоторых или всех доменов Active Directory для Exchange. Дополнительные сведения см. в статье Подготовка Active Directory и доменов для Exchange.
/NewProvisionedServer[:<ServerName>] (или */nprs[:<ServerName>]* */RemoveProvisionedServer:<ServerName>* (или */rprs:<ServerName>*)	Параметр */NewProvisionedServer* создает объект Exchange Server в Active Directory. После этого член группы ролей Делегированная установка может установить Exchange на сервере. Для получения дополнительных сведений см. статью Делегирование установки серверов Exchange Server. Параметр */RemoveProvisionedServer* удаляет подготовленный объект сервера Exchange Server из Active Directory *перед* установкой Exchange на сервер.
/AddUmLanguagePack:<Culture1>,<Culture2>...<CultureN> */RemoveUmLanguagePack:<Culture1>,<Culture2>...<CultureN>*	**Примечание**. Эти параметры недоступны в Exchange 2019. Они доступны только в Exchange 2016. Добавляет или удаляет языковые пакеты единой системы обмена сообщениями (UM) с существующих серверов почтовых ящиков Exchange 2016. Языковые пакеты единой системы обмена сообщениями позволяют абонентам и пользователям голосового доступа Outlook взаимодействовать с системой единой системы обмена сообщениями на этих языках. Вы не можете добавить или удалить языковой пакет en-US. Языковые пакеты можно установить на существующих серверах почтовых ящиков с помощью параметра */AddUmLanguagePack* или запустив UMLanguagePack.< Язык и региональные> параметры.exe файл напрямую. Удалить установленные языковые пакеты можно только с помощью параметра */RemoveUmLanguagePack* . Дополнительные сведения см. в разделе Языки единой системы обмена сообщениями, запросы и приветствия.

Необязательные параметры командной строки для автоматического режима

В приведенной ниже таблице описаны необязательные (вспомогательные) параметры командной строки, доступные в режиме автоматической установки в Exchange 2016 или Exchange 2019:

Параметр	Допустимые значения	Значение по умолчанию	Доступно с	Описание
/ActiveDirectorySplitPermissions:<TrueOrFalse>	True или False	False	Команды `/Mode:Install` `/Roles:Mailbox` или */PrepareAD* для первого сервера Exchange Server в организации.	Указывает модель раздел Дополнительные сведени о разделенных разрешен
/AdamLdapPort:<TCPPortNumber>	Действительный номер порта TCP	50389	Команды `/Mode:Install` `/Roles:EdgeTransport`	Указывает пользовательс Directory облегченного до хранится в реестре по адр `HKEY_LOCAL_MACHINE\SOFTWA`
/AdamSslPort:<TCPPortNumber>	Действительный номер порта TCP	50636	Команды `/Mode:Install` `/Roles:EdgeTransport`	Указывает пользовательс пограничных транспортн `HKEY_LOCAL_MACHINE\SOFTWA`
/AnswerFile:"<PathAndFileName>" (или *af:"<PathAndFileName>"*)	Имя и расположение текстового файла (например, "D:\Server data\answer.txt").	н/д	`/Mode:Install` `/Roles:Mailbox` команды или `/Mode:Install` `/Roles:EdgeTransport`	Используйте этот параме Exchange на нескольких к следующие параметры: *A DoNotStartTransport*, *Enabl OrganizationName*, *Tenant* переключателями в файл одну строку в файле.
/CustomerFeedbackEnabled:<TrueOrFalse>	True или False	False	Команды `/Mode:Install` и */PrepareAD*	Указывает, следует ли раз Майкрософт для улучшен ошибках на сервере посл **Set-ExchangeServer** .

Параметр	Допустимые значения	Значение по умолчанию	Доступно с	Описание
/DbFilePath:"<Path>\<FileName.edb>"	Путь к папке и имя файла EDB (например, "D:\Exchange Database Files\DB01\db01.edb").	**%ExchangeInstallPath%Mailbox\<DatabaseName>\<DatabaseName.edb>**, где: • <DatabaseName> — это **Mailbox Database <10DigitNumber>** , который соответствует имени базы данных по умолчанию **или** значению, указанному с помощью параметра */MdbName* (без расширения имени файла .edb). • %ExchangeInstallPath% — **это %ProgramFiles%\Microsoft\Exchange Server\V15** или расположение, указанное с помощью параметра */TargetDir*.	Команды `/Mode:Install /Roles:Mailbox`	Указывает расположение ящиков. Имя файла базы журнала транзакций базы
/DisableAMFiltering	н/д	н/д	Команды `/Mode:Install /Roles:Mailbox`	Отключает встроенную ф Дополнительные сведени программ в Exchange Serv
/DomainController:<ServerNameOrFQDN> (или */dc:<ServerNameOrFQDN>*)	Имя сервера (например, DC01) или FQDN (например, dc01.contoso.com) контроллера домена.	Случайным образом выбранный контроллер домена на одном сайте Active Directory с целевым сервером, где запущена программа установки.	Все команды */Mode* (за исключением случаев, когда устанавливается пограничный транспортный сервер) или команды */PrepareAD*, */PrepareSchema*, */PrepareDomain* и */PrepareAllDomains*	Указывает контроллер до Active Directory. Контролл или Exchange 2019. Если вы используете этот Active Directory для Exchar сообщение об ошибке.
/DoNotStartTransport	н/д	н/д	Команды `/Mode:Install /Roles:Mailbox`, `/Mode:Install /Roles:EdgeTransport` и `/Mode:RecoverServer`.	Указывает программе уст почты) на серверах почто установки. Этот параметр сервер будет принимать переместить базу данных
/EnableErrorReporting	н/д	Отключено	Команды `/Mode:Install`, `/Mode:Upgrade` и `/Mode:RecoverServer`	Указывает, следует ли раз Вы можете включить или помощью параметра *Erro*
/InstallWindowsComponents	н/д	н/д	Команды `/Mode:Install`	Устанавливает необходим требуется перезагрузка, п
/LogFolderPath:"<Path>"	Путь к папке (например, "E:\Exchange Database Logs").	**%ExchangeInstallPath%Mailbox\<DatabaseName>** , где: • <DatabaseName> — это **Mailbox Database <10DigitNumber>** , который соответствует имени базы данных по умолчанию **или** значению, указанному с помощью параметра */MdbName* (без расширения имени файла .edb). • %ExchangeInstallPath% — **это %ProgramFiles%\Microsoft\Exchange Server\V15** или расположение, указанное с помощью параметра */TargetDir*.	Команды `/Mode:Install /Roles:Mailbox`	Указывает расположение созданной на новом серв помощью параметра */Db*
/MdbName:"<FileName>"	Имя файла базы данных без расширения .edb (например, "db01")	**База данных почтовых ящиков <10DigitNumber>** (например, **База данных почтовых ящиков 0139595516**).	Команды `/Mode:Install /Roles:Mailbox`	Указывает имя первой ба Расположение файлов ба

Параметр	Допустимые значения	Значение по умолчанию	Доступно с	Описание
/OrganizationName:"<Organization Name>" (или */on:"<Organization Name>"*)	Текстовая строка (например, "Корпорация Contoso").	Пусто в настройке командной строки; **Первая организация** в мастере установки Exchange.	Команды `/Mode:Install` `/Roles:Mailbox` или */PrepareAD* для первого сервера Exchange Server в организации.	Название организации ис влияет на функциональнс • Название организац • Допустимые симво должно быть в нача • Указанное название
/SourceDir:"<Path>" (или */s:"<Path>"*)	Путь к папке (например, "Z:\Exchange).	Папка ServerRoles\UnifiedMessaging на установочном носителе Exchange.	Команды */AddUmLanguagePack* в Exchange 2016 (недоступны в Exchange 2019)	Указывает расположение существующие серверы г
/TargetDir:"<Path>" (или */t:"<Path>"*)	Путь к папке (например, "D:\Program Files\Microsoft\Exchange").	**%ProgramFiles%\Microsoft\Exchange Server\V15**	Команды `/Mode:Install` и `/Mode:RecoverServer`	Указывает место установк (например, C:\) или на ди При восстановлении посл пользовательского пути у пользовательский путь вс
/TenantOrganizationConfig:"<Path>"	Путь к папке (например, "C:\Data")	н/д	Команды `/Mode:Install` или */PrepareAD*.	Требуется в гибридных ра чтобы указать расположе организации Microsoft 36 **OrganizationConfig** в Exch
/UpdatesDir:"<Path>" (или */u:"<Path>"*)	Путь к папке (например, "D:\Downloads\Exchange Updates").	Папка обновления в корневой папке установочного носителя Exchange.	Команды `/Mode:Install`, `/Mode:Upgrade`, `/Mode:RecoverServer` и */AddUmLanguagePack*.	Указывает исходное расп можно указать только од Любые языковые пакеты установлены на целевой

Что нужно знать перед началом работы

- Скачайте последнюю версию Exchange на целевом компьютере. Дополнительные сведения см. в разделе Обновления для Exchange Server.
- Проверьте требования к сети, компьютерному оборудованию, операционной системе и программному обеспечению, указанные в статьях Требования к системе для установки Exchange Server и Предварительные требования для Exchange Server.
- Прочитайте заметки о выпуске в статье Заметки о выпуске сервера Exchange Server.

  > ⊗ **Внимание!**
  >
  > После установки Exchange на сервере будет невозможно изменить его имя. Переименование сервера после установки роли сервера Exchange не поддерживается.

- Для серверов почтовых ящиков:
  - Предполагаемое время для завершения: 60 минут.
  - Целевой сервер должен быть членом домена Active Directory.
  - Для учетной записи, которая используется для установки Exchange, нужны следующие разрешения: *.
    - **Членство в группе администраторов организации**. Обязательно, если это первый сервер Exchange Server в организации.
    - **Членство в группе администраторов схемы**. Обязательно, если вы еще не расширили схему Active Directory или не подготовили Active Directory для Exchange.
    - **Членство в группе ролей управления организацией Exchange**. Обязательно, если вы уже подготовили домен Active Directory, который будет содержать сервер Exchange Server, либо в организации уже есть другие серверы Exchange Server.

  * Члены группы ролей **Делегированная установка** могут устанавливать Exchange на серверах, которые уже подготовлены в Active Directory администратором Exchange. Для получения дополнительных сведений см. статью Делегирование установки серверов Exchange Server.
- Для пограничных транспортных серверов:

- Предполагаемое время для завершения: 40 минут.
- Рекомендуется установить пограничные транспортные серверы в сети периметра, которая находится за пределами внутреннего леса Active Directory вашей организации. Установка роли пограничного транспортного сервера на присоединенных к домену компьютерах позволяет управлять только функциями и параметрами Windows. Пограничные транспортные серверы не обращаются напрямую к Active Directory. Вместо этого они используют службы Active Directory облегченного доступа к каталогу (AD LDS) для хранения сведений о конфигурации и получателях. Дополнительные сведения о роли пограничного транспорта см. в разделе Пограничные транспортные серверы.
- Убедитесь, что локальная учетная запись на целевом компьютере входит в локальную группу администраторов на целевом компьютере.
- Необходимо настроить основной суффикс DNS на компьютере. Например, если полное доменное имя компьютера — edge.contoso.com, то суффиксом DNS компьютера будет contoso.com. Дополнительные сведения см. в разделе Отсутствует основной DNS-суффикс [ms.exch.setupreadiness.FqdnMissing].
- В сценариях сосуществования транспортных серверов концентратора Exchange 2010 требуется обновление, прежде чем вы сможете подписать пограничный транспортный сервер Exchange 2016 на сайт Active Directory, содержащий транспортные серверы концентратора Exchange 2010. Если не установить это обновление, подписка EdgeSync будет работать неправильно для транспортного сервера-концентратора Exchange 2010, который участвует в синхронизации EdgeSync. Дополнительные сведения см. в статье Поддерживаемые сценарии сосуществования для Exchange 2016.

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Установка Exchange в автоматическом режиме с помощью Setup.exe

1. На целевом сервере откройте проводник, щелкните правой кнопкой мыши скачанный файл ISO-образа Exchange и выберите **Подключить**. Обратите внимание на назначенную букву виртуального DVD-диска.
2. Откройте окно командной строки Windows. Например:
   - Нажмите клавиши Windows + R, чтобы открыть диалоговое окно **Выполнить**, введите cmd.exe и нажмите кнопку **OK**.
   - Нажмите кнопку **Пуск**. В поле **Поиск** введите **командная строка**, а затем в списке результатов выберите **Командная строка**.
3. В окне командной строки введите следующую команду:

   Консоль

   ```
   <Virtual DVD drive letter>:\Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON [Switches]
   ```

   Программа установки копирует установочные файлы на локальный компьютер.

   Программа установки проверяет выполнение предварительных условий, в том числе относящихся к устанавливаемым ролям сервера. Если выполнены не все предварительные условия, установка будет прекращена с возвратом ошибки, в которой объясняется причина сбоя. Если вы выполнили все предварительные требования, программа установки установит Exchange.
4. После завершения установки Exchange может понадобиться перезапуск сервера.
5. Завершите развертывание, выполнив задачи, описанные в статье Задачи, которые необходимо выполнить после установки сервера Exchange Server.

Примеры автоматического режима

Подготовка Active Directory для Exchange в автоматическом режиме

В этом примере описана настройка "Fabrikam Ltd" в качестве названия организации в Active Directory и подготовка Active Directory для устанавливаемой версии Exchange.

Консоль

```
Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON /PrepareAD /OrganizationName:"Fabrikam Ltd"
```

Дополнительные сведения см. в статье Подготовка Active Directory и доменов для Exchange.

Установка серверов почтовых ящиков в автоматическом режиме

- В этом примере описана установка первого сервера Exchange Server (сервер почтовых ящиков) в организации, указание "Корпорация Contoso" в качестве названия организации Exchange в Active Directory, а также установка средств управления Exchange на локальный сервер.

```
Консоль

Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON /Mode:Install /Roles:Mailbox /on:"Contoso Corporation"
```

- В этом примере описана установка роли сервера почтовых ящиков и средств управления в папку по умолчанию на локальном сервере в организации, где уже выполнена подготовка Active Directory для устанавливаемой версии Exchange.

```
Консоль

Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON /mode:Install /r:MB
```

- В этом примере описана установка роли сервера почтовых ящиков и средств управления в папку "C:\Exchange Server" на локальном сервере.

```
Консоль

Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON /Mode:Install /Role:Mailbox /TargetDir:"C:\Exchange
Server"
```

- В этом примере описана установка роли сервера почтовых ящиков, используя параметры в файле ExchangeConfig.txt.

```
Консоль

Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON /mode:Install /role:Mailbox
/AnswerFile:c:\ExchangeConfig.txt
```

- В этом примере описано использование контроллера домена с именем DC01, с которого выполняется чтение и запись в Active Directory, при установке роли сервера почтовых ящиков и средств управления на локальный сервер.

```
Консоль

Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON /mode:Install /role:Mailbox /DomainController:DC01
```

- В этом примере программа установки Exchange обновляется с помощью исправлений из указанной папки, а затем устанавливается роль сервера почтовых ящиков и средства управления на локальном сервере. В Exchange 2016 языковые пакеты устанавливаются автоматически, только если в этой папке находятся какие-либо языковые пакеты единой системы обмена сообщениями.

```
Консоль

Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON /role:Mailbox /UpdatesDir:"C:\ExchangeServer\New
Patches"
```

Установка пограничных транспортных серверов в автоматическом режиме

- В этом примере описана установка роли пограничного транспортного сервера и средств управления в расположение по умолчанию на локальном сервере.

```
Консоль

Setup.exe /IAcceptExchangeServerLicenseTerms /mode:Install /r:EdgeTransport
```

- В этом примере описана установка роли пограничного транспортного сервера и средств управления в указанную папку на локальном сервере.

```
Консоль
```

```
Setup.exe /IAcceptExchangeServerLicenseTerms /mode:Install /r:ET /TargetDir:"D:\Exchange Server"
```

Удаление Exchange с серверов в автоматического режиме

В этом примере описано полное удаление Exchange с локального компьютера, а также удаление конфигурации Exchange этого сервера из Active Directory.

Консоль

```
Setup.exe /mode:Uninstall
```

Удаление подготовленных объектов сервера Exchange Server из Active Directory в автоматическом режиме

В этом примере описано удаление подготовленного объекта сервера Exchange Server с именем Exchange03 из Active Directory *перед* установкой Exchange на сервер (если установка Exchange на сервер уже выполнена, команда работать не будет).

Консоль

```
Setup.exe /rprs:Exchange03
```

Для получения дополнительных сведений см. статью Делегирование установки серверов Exchange Server.

Добавление пакетов единой системы обмена сообщениями на существующие серверы почтовых ящиков Exchange 2016 и их удаление в автоматическом режиме

> **Примечание**
>
> Эти процедуры в Exchange 2019 недоступны.

- В этом примере описана установка русского и испанского (Испания) языковых пакетов на локальный сервер почтовых ящиков Exchange 2016 из указанной папки.

  Консоль

  ```
  Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON /AddUmLanguagePack:ru-RU,es-ES /SourceDir:"D:\UM
  Language Packs"
  ```

- В этом примере описано удаление корейского языкового пакета с локального сервера почтовых ящиков Exchange 2016.

  Консоль

  ```
  Setup.exe  /RemoveUmLanguagePack:ko-KR
  ```

Дальнейшие действия

- Чтобы убедится в успешности установки Exchange в автоматическом режиме, см. статью Проверка установки сервера Exchange Server.
- Завершите развертывание, выполнив задачи, описанные в статье Задачи, которые необходимо выполнить после установки Exchange.
- Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу Exchange Server.

Делегирование установки серверов Exchange Server

Статья • 04.04.2023

В крупных компаниях пользователи, которые устанавливают и настраивают новые серверы Windows, часто не являются администраторами Exchange. В Exchange 2016 и Exchange 2019 эти пользователи по-прежнему могут устанавливать Exchange на серверах Windows, но только *после* того, как администратор Exchange *подготовит* объект Exchange Server в Active Directory. При подготовке объекта сервера Exchange все необходимые изменения Active Directory выполняются независимо от фактической установки Exchange на сервере. Администратор Exchange может подготовить новый объект Exchange Server за несколько часов или даже дней до установки Exchange.

После того как администратор Exchange подготавливает объект Exchange Server, единственным требованием для установки Exchange на сервере является членство в группе ролей Делегированная установка , которая позволяет участникам устанавливать Exchange на подготовленных серверах. Если это похоже на то, что вы хотите сделать, эта тема для вас.

Что нужно знать перед началом работы

- Предполагаемое время выполнения этой процедуры: менее 10 минут.
- Сервер Exchange Server можно подготовить только из командной строки (автоматическая установка). Вы не можете использовать мастер установки Exchange.
- Вы не можете подготовить первый объект Exchange Server в вашей организации для установки Exchange делегатом. Администратору Exchange необходимо установить первый сервер Exchange в организации. После этого можно подготовить *дополнительные* объекты Exchange Server, чтобы пользователи, не являющиеся администраторами Exchange, могли установить Exchange с помощью делегированной установки.
- Делегированный пользователь не может удалить сервер Exchange. Удалить сервер Exchange может только администратор Exchange.
- Скачайте и используйте последний доступный выпуск Обновления для Exchange Server.

- Чтобы подготовить объект Exchange Server, необходимо быть членом группы ролей Управление организацией .
- Объект Exchange Server можно подготовить в Active Directory с самого целевого сервера или с другого компьютера.
- Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server, Exchange Online или Exchange Online Protection.

Использование командной строки для подготовки серверов Exchange 2019

1. В проводнике щелкните скачанный файл ISO-образа Exchange правой кнопкой мыши и выберите **Подключить**. Обратите внимание на назначенную букву виртуального DVD-диска.
2. Откройте окно командной строки Windows. Например:
   - Нажмите клавиши Windows + R, чтобы открыть диалоговое окно **Выполнить**, введите cmd.exe и нажмите кнопку **ОК**.
   - Нажмите кнопку **Пуск**. В поле **Поиск** введите **командная строка**, а затем в списке результатов выберите **Командная строка**.
3. В окне командной строки введите следующую команду:

> **Примечание**
>
> - Предыдущий переключатель */IAcceptExchangeServerLicenseTerms* не будет работать начиная с накопительных обновлений (CU) за сентябрь 2021 г. Теперь необходимо использовать */IAcceptExchangeServerLicenseTerms_DiagnosticDataON* или */IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF* для автоматической установки и установки по сценариям.
> - В примерах ниже используется переключатель */IAcceptExchangeServerLicenseTerms_DiagnosticDataON*. Вы можете изменить переключатель на */IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF*.

Консоль

```
<Virtual DVD drive letter>:\Setup.exe
/IAcceptExchangeServerLicenseTerms_DiagnosticDataON
/NewProvisionedServer[:<ServerName>]
```

При выполнении команды на целевом сервере можно использовать параметр */NewProvisionedServer* самостоятельно. В противном случае необходимо указать имя сервера для подготовки.

В этом примере файлы установки Exchange на диске E: используются для подготовки сервера Mailbox01:

Консоль

```
E:\Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON
/NewProvisionedServer:Mailbox01
```

В этом примере файлы установки Exchange на диске E: используются для подготовки локального сервера, на котором выполняется команда:

Консоль

```
E:\Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON
/NewProvisionedServer
```

Примечание. Чтобы удалить подготовленный объект Exchange Server из Active Directory *перед* установкой exchange, замените параметр */NewProvisionedServerна /RemoveProvisionedServer*.

4. Добавьте соответствующих пользователей в группу ролей Делегированная установка, чтобы они могли установить Exchange на подготовленном сервере. Сведения о добавлении пользователей в группу ролей см. в статье Добавление участников в группу ролей. Делегаты могут использовать процедуры из раздела Установка серверов почтовых ящиков Exchange с помощью мастера установки , чтобы установить Exchange на подготовленном сервере.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно подготовили сервер Exchange для установки делегата Exchange, выполните следующие действия.

1. В разделе Пользователи & Active Directory Компьютеры выберите **Группы безопасности Microsoft Exchange**, дважды щелкните **Серверы Exchange**, а затем перейдите на вкладку **Участники** .

2. На вкладке **Участники** убедитесь, что подготовленный сервер является членом группы безопасности. Член группы ролей Делегированная установка теперь может установить Exchange на сервере.

Если сервер указан в качестве участника группы безопасности серверов Exchange, он подготовлен правильно. Теперь участники группы ролей "Делегированная установка" могут устанавливать Exchange на этот сервер.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server .

Дополнительные сведения

Администратору Exchange может потребоваться завершить развертывание, выполнив задачи, указанные в задачах Exchange после установки.

Высокоуровневые изменения Active Directory, внесенные при подготовке объекта Exchange Server, описаны в следующем списке.

- A server object is created in the **CN=Servers,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=<Organization Name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Root Domain>** configuration partition.

- В объект сервера в разделе конфигурации добавляются такие элементы управления доступом для группы ролей "Делегированная установка":

  - элемент "Полный доступ" для объекта сервера и его дочерних объектов;

  - элемент управления доступом "Запретить" для расширенного права "Отправить как";

  - элемент управления доступом "Запретить" для расширенного права "Получить как".

  - элемент "Запретить" для разрешений CreateChild и DeleteChild для объектов хранилища общедоступных папок Exchange.

    Примечание. Общедоступные папки администрируются на уровне организации; Таким образом, создание и удаление хранилищ

общедоступных папок осуществляется только администраторами Exchange.

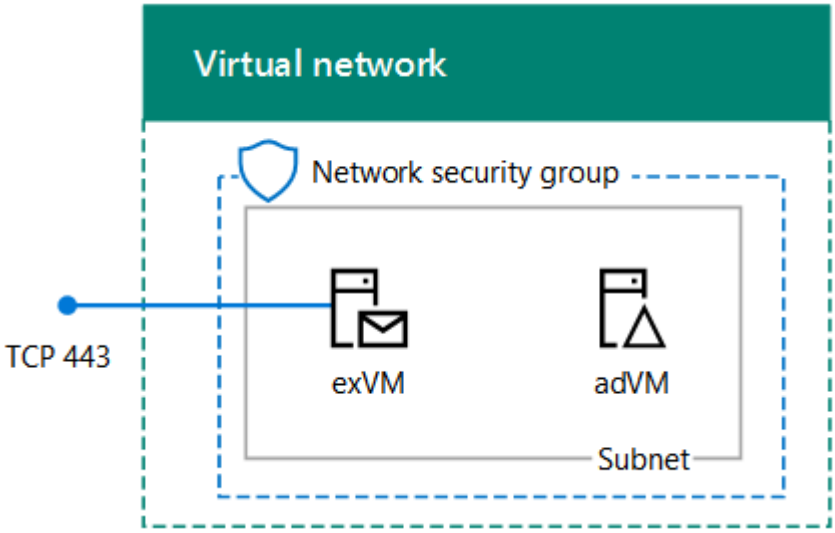
- В группу серверов Exchange добавляется учетная запись компьютера Active Directory для сервера.
- Сервер добавляется в качестве подготовленного сервера в Центре администрирования Exchange (EAC).

Только члены группы ролей "Управление организацией" в Exchange имеют разрешения, необходимые для внесения этих изменений в Active Directory.

Среды разработки и тестирования Exchange в Azure

Статья • 04.04.2023

В этом разделе описывается создание развертывания разработки и тестирования Exchange 2016 или Exchange 2019 в Microsoft Azure. Ниже показана итоговая конфигурация.



Эта конфигурация состоит из одного сервера Exchange Server и контроллера домена Windows Server Active Directory в подсети виртуальной сети Azure. Это обеспечивает основу и общую отправную точку, с которой можно продемонстрировать Exchange и разрабатывать Exchange Server приложения. Конфигурация предназначена только для внутреннего тестирования почты и приложений на сервере Exchange Server. В ней не настроен внешний поток обработки почты.

Процесс настройки этой среды разработки и тестирования состоит из трех перечисленных ниже основных этапов.

1. Настройка виртуальной сети и контроллера домена (adVM).
2. Добавьте сервер Exchange Server (exVM).
3. Настройка Exchange.

Если у вас еще нет подписки Azure, вы можете зарегистрироваться для получения бесплатной пробной версии Azure. Если у вас есть подписка MSDN или Visual Studio, см. статью Ежемесячный кредит Azure для подписчиков Visual Studio.

Примечание

Так как Exchange вносит изменения в схему в Windows Server AD, эта конфигурация не может использовать azure доменные службы Active Directory.

Этап 1. Развертывание виртуальной сети и контроллера домена

Вы можете создать виртуальную сеть Azure с контроллером домена при помощи Azure PowerShell. Указанные ниже команды PowerShell можно выполнить в командной строке или в интегрированной среде сценариев Windows PowerShell. Если вы еще не установили Azure PowerShell, просмотрите статью Начало работы с командлетами Azure PowerShell.

> ⓘ **Примечание**
>
> Эти команды предназначены для Azure PowerShell 1.0.0 или более поздней версии.

1. Войдите в учетную запись Azure.

```
PowerShell

Connect-AzAccount
```

2. Получите имя подписки с помощью следующей команды.

```
PowerShell

Get-AZSubscription | Sort-Object Name | Select-Object Name
```

3. Настройте подписку Azure с помощью указанных ниже команд. Задайте **переменную $subscrName** , заменив все в кавычках, включая < символы и > , правильным именем.

```
PowerShell

$subscrName="<subscription name>"
Select-AzSubscription -SubscriptionName $subscrName
```

4. Создайте новую группу ресурсов. Чтобы выбрать уникальное имя для группы ресурсов, с помощью этой команды отобразите имеющиеся группы ресурсов.

```
PowerShell

Get-AZResourceGroup | Sort-Object ResourceGroupName | Select-Object
ResourceGroupName
```

Создайте группу ресурсов с помощью приведенных ниже команд. Задайте переменные, заменив все символы в кавычках (в том числе символы < и >) правильными именами.

```
PowerShell

$rgName="<resource group name>"
$locName="<location name, such as West US>"
New-AZResourceGroup -Name $rgName -Location $locName
```

5. Виртуальным машинам на основе диспетчера ресурсов требуется соответствующая учетная запись хранения. Для учетной записи хранения необходимо выбрать глобально уникальное имя, *которое содержит только буквы нижнего регистра и цифры*. Для отображения уже существующих учетных записей хранения можно использовать приведенную ниже команду.

```
PowerShell

Get-AZStorageAccount | Sort-Object StorageAccountName | Select-Object
StorageAccountName
```

Чтобы проверить, уникально ли предложенное имя учетной записи хранения, воспользуйтесь приведенной ниже командой.

```
PowerShell

Get-AZStorageAccountNameAvailability "<proposed name>"
```

С помощью указанных ниже команд создайте учетную запись хранения для новой тестовой среды.

```
PowerShell

$saName="<storage account name>"
New-AZStorageAccount -Name $saName -ResourceGroupName $rgName -Type
Standard_LRS -Location $locName
```

6. Создайте виртуальная сеть EXSrvrVnet Azure, который будет размещать подсеть EXSrvrSubnet и защищать ее с помощью группы безопасности сети.

PowerShell

```
$exSubnet=New-AZVirtualNetworkSubnetConfig -Name EXSrvrSubnet -
AddressPrefix 10.0.0.0/24
New-AZVirtualNetwork -Name EXSrvrVnet -ResourceGroupName $rgName -
Location $locName -AddressPrefix 10.0.0.0/16 -Subnet $exSubnet -
DNSServer 10.0.0.4
$rule1 = New-AZNetworkSecurityRuleConfig -Name "RDPTraffic" -
Description "Allow RDP to all VMs on the subnet" -Access Allow -
Protocol Tcp -Direction Inbound -Priority 100 -SourceAddressPrefix
Internet -SourcePortRange * -DestinationAddressPrefix * -
DestinationPortRange 3389
$rule2 = New-AZNetworkSecurityRuleConfig -Name
"ExchangeSecureWebTraffic" -Description "Allow HTTPS to the Exchange
server" -Access Allow -Protocol Tcp -Direction Inbound -Priority 101 -
SourceAddressPrefix Internet -SourcePortRange * -
DestinationAddressPrefix "10.0.0.5/32" -DestinationPortRange 443
New-AZNetworkSecurityGroup -Name EXSrvrSubnet -ResourceGroupName
$rgName -Location $locName -SecurityRules $rule1, $rule2
$vnet=Get-AZVirtualNetwork -ResourceGroupName $rgName -Name EXSrvrVnet
$nsg=Get-AZNetworkSecurityGroup -Name EXSrvrSubnet -ResourceGroupName
$rgName
Set-AZVirtualNetworkSubnetConfig -VirtualNetwork $vnet -Name
EXSrvrSubnet -AddressPrefix "10.0.0.0/24" -NetworkSecurityGroup $nsg
$vnet | Set-AzVirtualNetwork
```

7. Создайте виртуальную машину adVM в Azure. adVM — это контроллер домена для corp.contoso.com Windows Server AD домена и DNS-сервер для виртуальных машин виртуальной сети EXSrvrVnet.

   Прежде всего укажите имя группы ресурсов, расположение Azure и имя учетной записи хранения. Затем выполните указанные ниже команды в командной строке Azure PowerShell на локальном компьютере, чтобы создать виртуальную машину Azure для adVM.

   PowerShell

   ```
   # Create an availability set for domain controller virtual machines
   New-AZAvailabilitySet -ResourceGroupName $rgName -Name
   dcAvailabilitySet -Location $locName -Sku Aligned -
   PlatformUpdateDomainCount 5 -PlatformFaultDomainCount 2
   # Create the domain controller virtual machine
   $vnet=Get-AZVirtualNetwork -Name EXSrvrVnet -ResourceGroupName $rgName
   $pip = New-AZPublicIpAddress -Name adVM-NIC -ResourceGroupName $rgName
   -Location $locName -AllocationMethod Dynamic
   $nic = New-AZNetworkInterface -Name adVM-NIC -ResourceGroupName $rgName
   -Location $locName -SubnetId $vnet.Subnets[0].Id -PublicIpAddressId
   $pip.Id -PrivateIpAddress 10.0.0.4
   $avSet=Get-AZAvailabilitySet -Name dcAvailabilitySet -ResourceGroupName
   $rgName
   $vm=New-AZVMConfig -VMName adVM -VMSize Standard_D1_v2 -
   ```

```
AvailabilitySetId $avSet.Id
$vm=Set-AZVMOSDisk -VM $vm -Name adVM-OS -DiskSizeInGB 128 -
CreateOption FromImage -StorageAccountType "Standard_LRS"
$diskConfig=New-AZDiskConfig -AccountType "Standard_LRS" -Location
$locName -CreateOption Empty -DiskSizeGB 20
$dataDisk1=New-AZDisk -DiskName adVM-DataDisk1 -Disk $diskConfig -
ResourceGroupName $rgName
$vm=Add-AZVMDataDisk -VM $vm -Name adVM-DataDisk1 -CreateOption Attach
-ManagedDiskId $dataDisk1.Id -Lun 1
$cred=Get-Credential -Message "Type the name and password of the local
administrator account for adVM."
$vm=Set-AZVMOperatingSystem -VM $vm -Windows -ComputerName adVM -
Credential $cred -ProvisionVMAgent -EnableAutoUpdate
$vm=Set-AZVMSourceImage -VM $vm -PublisherName MicrosoftWindowsServer -
Offer WindowsServer -Skus 2012-R2-Datacenter -Version "latest"
$vm=Add-AZVMNetworkInterface -VM $vm -Id $nic.Id
New-AZVM -ResourceGroupName $rgName -Location $locName -VM $vm
```

Вам будет предложено ввести имя пользователя и пароль. В этой статье это имя пользователя будет называться ADMIN_NAME. Задайте надежный пароль и запишите имя пользователя и пароль в безопасном месте.

Примечание. Указанный пароль не может быть "pass@word1". Он должен иметь длину 8–123 символа и удовлетворять хотя бы трем из указанных ниже требований к сложности пароля.

- Пароль должен содержать хотя бы одну прописную букву.
- пароль должен содержать хотя бы одну строчную букву;
- пароль должен содержать хотя бы одну цифру;
- пароль должен содержать хотя бы один специальный знак.

На создание виртуальной машины в Azure может потребоваться несколько минут.

Подключение к виртуальной машине контроллера домена с использованием данных учетной записи локального администратора

1. В портал Azure щелкните **Группы** > **<ресурсов имя группы>** > **ресурсов adVM** > **Connect**.
2. Запустите скачанный файл adVM.rdp, а затем щелкните **Подключиться**.
3. В разделе **Безопасность Windows** щелкните **Использовать другую учетную запись**. В поле **Имя пользователя** введите **adVM**<ADMIN_NAME>.

4. В поле **Пароль** укажите пароль учетной записи ADMIN_NAME, а затем нажмите кнопку **OK**.

5. При отображении соответствующего запроса нажмите кнопку **Да**.

6. Добавьте дополнительный диск данных в качестве нового тома с буквой диска F: с помощью этих команд на уровне администратора Windows PowerShell командной строки в adVM.

   PowerShell

   ```
   $disk=Get-Disk | where {$_.PartitionStyle -eq "RAW"}
   $diskNumber=$disk.Number
   Initialize-Disk -Number $diskNumber
   New-Partition -DiskNumber $diskNumber -UseMaximumSize -
   AssignDriveLetter
   Format-Volume -DriveLetter F
   ```

7. Настройте adVM в качестве контроллера домена и DNS-сервера для corp.contoso.com домена. Выполните указанные ниже команды в командной строке Windows PowerShell с правами администратора на виртуальной машине adVM.

   PowerShell

   ```
   Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
   Install-ADDSForest -DomainName corp.contoso.com -DatabasePath "F:\NTDS"
   -SysvolPath "F:\SYSVOL" -LogPath "F:\Logs"
   ```

Обратите внимание, что на выполнение этих команд может потребоваться несколько минут.

После перезапуска виртуальной машины adVM снова подключитесь к ней.

Подключение к виртуальной машине контроллера домена с помощью учетных данных домена

1. В портал Azure щелкните **Группы** >**<ресурсов, имя новой группы>** > **ресурсов adVM** > **Connect**.

2. Запустите скачанный файл adVM.rdp, а затем щелкните **Подключиться**.

3. В разделе **Безопасность Windows** щелкните **Использовать другую учетную запись**. В поле **Имя пользователя** введите **CORP**<ADMIN_NAME>.

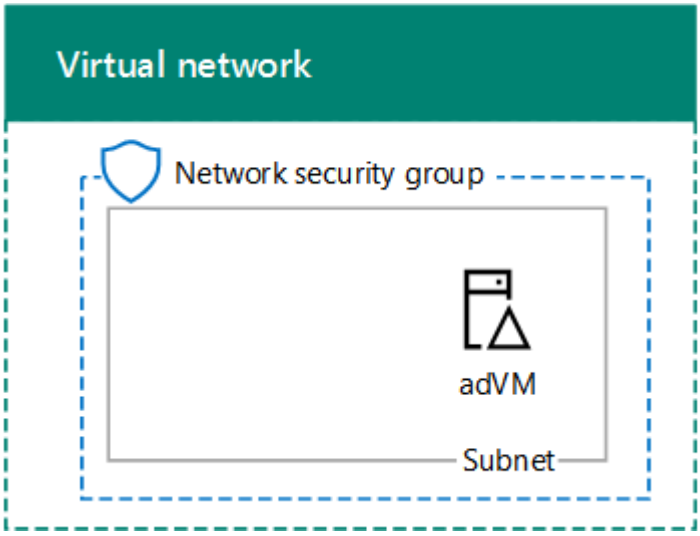
4. В поле **Пароль** укажите пароль учетной записи ADMIN_NAME, а затем нажмите кнопку **OK**.

5. При появлении соответствующего запроса нажмите кнопку **Да**.

6. На рабочем столе откройте командную строку Windows PowerShell с правами администратора и выполните указанную ниже команду.

```
PowerShell

Add-WindowsFeature RSAT-ADDS-Tools
```

Ниже показан результат выполнения этапа 1.



Этап 2. Создание виртуальной машины Exchange

На этом этапе вы создадите виртуальную машину Exchange в виртуальной сети EXSrvrVNet и сделаете ее членом домена CORP.

Чтобы создать виртуальную машину Exchange с Azure PowerShell, сначала войдите в Azure с помощью учетной записи Azure из командной строки Windows PowerShell (при необходимости).

```
PowerShell

Connect-AzAccount
```

Вам необходимо определить глобально уникальное имя DNS для виртуальной машины exVM. Необходимо выбрать глобально уникальное DNS-имя , *содержащее*

только строчные буквы и цифры. Это можно сделать с помощью указанных ниже команд PowerShell.

PowerShell

```
$vmDNSName="<DNS name to test>"
$rgName="<resource group name>"
$locName=(Get-AZResourceGroup -Name $rgName).Location
Test-AZDnsAvailability -DomainQualifiedName $vmDNSName -Location $locName
```

Если отобразится сообщение "True", то указанное имя является глобально уникальным.

Далее заполните значения переменных и запустите получившийся блок команд в командной строке PowerShell.

PowerShell

```
# Set up key variables
$subscrName="<name of your Azure subscription>"
$vmDNSName="<unique, public DNS name for the Exchange server>"
# Set the Azure subscription
Select-AzSubscription -SubscriptionName $subscrName
# Get the Azure location and storage account names
$locName=(Get-AZResourceGroup -Name $rgName).Location
$saName=(Get-AZStorageaccount | Where {$_.ResourceGroupName -eq
$rgName}).StorageAccountName
# Create an availability set for Exchange virtual machines
New-AZAvailabilitySet -ResourceGroupName $rgName -Name exAvailabilitySet -
Location $locName -Sku Aligned  -PlatformUpdateDomainCount 5 -
PlatformFaultDomainCount 2
# Specify the virtual machine name and size
$vmName="exVM"
$vmSize="standard_d8s_v3"
$vnet=Get-AZVirtualNetwork -Name "EXSrvrVnet" -ResourceGroupName $rgName
$avSet=Get-AZAvailabilitySet -Name exAvailabilitySet -ResourceGroupName
$rgName
$vm=New-AZVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId
$avSet.Id
# Create the NIC for the virtual machine
$nicName=$vmName + "-NIC"
$pipName=$vmName + "-PublicIP"
$pip=New-AZPublicIpAddress -Name $pipName -ResourceGroupName $rgName -
DomainNameLabel $vmDNSName -Location $locName -AllocationMethod Dynamic
$nic=New-AZNetworkInterface -Name $nicName -ResourceGroupName $rgName -
Location $locName -SubnetId $vnet.Subnets[0].Id -PublicIpAddressId $pip.Id -
PrivateIpAddress "10.0.0.5"
# Create and configure the virtual machine
$cred=Get-Credential -Message "Type the name and password of the local
administrator account for exVM."
$vm=Set-AZVMOSDisk -VM $vm -Name ($vmName +"-OS") -DiskSizeInGB 128 -
```

```
CreateOption FromImage -StorageAccountType "Standard_LRS"
$vm=Set-AZVMOperatingSystem -VM $vm -Windows -ComputerName $vmName -
Credential $cred -ProvisionVMAgent -EnableAutoUpdate
$vm=Set-AZVMSourceImage -VM $vm -PublisherName MicrosoftWindowsServer -Offer
WindowsServer -Skus 2019-Datacenter -Version "latest"
$vm=Add-AZVMNetworkInterface -VM $vm -Id $nic.Id
New-AZVM -ResourceGroupName $rgName -Location $locName -VM $vm
```

> ⓘ **Примечание**
>
> В этом блоке команд используется стандартная учетная запись хранения, созданная на этапе 1, что позволяет уменьшить стоимость этой среды разработки и тестирования. Для рабочего сервера Exchange Server необходимо использовать учетную запись хранения уровня "Премиум".

На портале Azure подключитесь к виртуальной машине exVM, используя учетные данные учетной записи локального администратора.

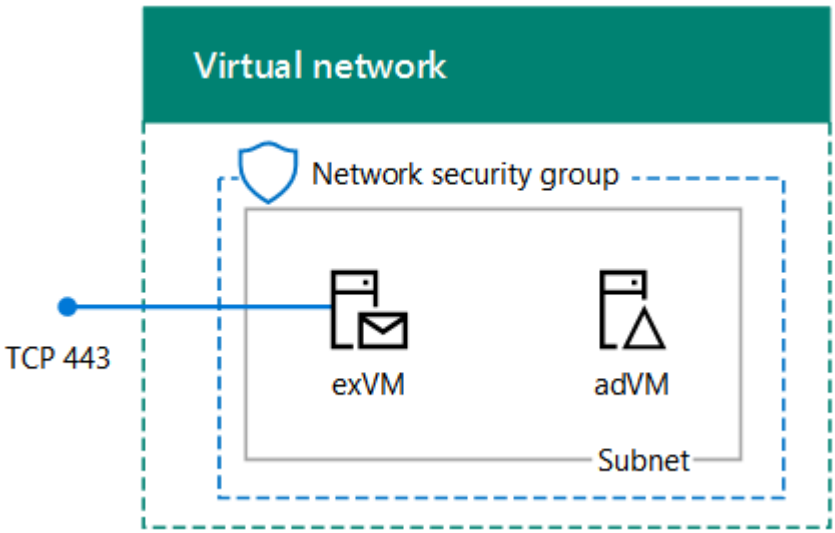
После этого в командной строке Windows PowerShell присоедините виртуальную машину exVM к домену Windows Active Directory с помощью указанных ниже команд.

PowerShell

```
Add-Computer -DomainName "corp.contoso.com"
Restart-Computer
```

Обратите внимание, что после ввода команды **Add-Computer** вам потребуется указать данные учетной записи домена. Используйте учетную запись и пароль CORP\<ADMIN_NAME> .

Ниже показан результат выполнения этапа 2.



Этап 3. Настройка Exchange

На этом этапе вы настроите Exchange в exVM и протестируете доставку почты между двумя почтовыми ящиками.

Подготовка Active Directory для Windows Server

1. В командной строке Windows PowerShell на локальном компьютере выполните следующую команду:

```
PowerShell

Write-Host (Get-AZPublicIpaddress -Name "exVM-PublicIP" -ResourceGroup
$rgName).DnsSettings.Fqdn
```

2. Запишите или скопируйте полное DNS-имя из отображения команды. Это DNS-имя виртуальной машины exVM в Интернете. Это значение потребуется вам позже.

3. При необходимости подключитесь к виртуальной машине adVM с помощью портал Azure, используя учетную запись CORP\<ADMIN_NAME> и пароль.

4. В командной строке Windows PowerShell выполните следующую команду:

```
PowerShell

Get-ADForest | Set-ADForest -UPNSuffixes @{Add="<DNS Name of
Exchange>"}
```

5. Закройте сеанс удаленного рабочего стола виртуальной машины adVM.

Установка Exchange

1. Подключитесь к виртуальной машине exVM с помощью портал Azure с помощью учетной записи и пароля CORP\<ADMIN_NAME>.

2. В виртуальной машине exVM откройте командную строку Windows PowerShell от имени администратора и выполните указанные ниже команды.

```
PowerShell

Install-WindowsFeature NET-Framework-45-Features, RPC-over-HTTP-proxy,
RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-Clustering-Mgmt,
RSAT-Clustering-PowerShell, Web-Mgmt-Console, WAS-Process-Model, Web-
```

```
Asp-Net45, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-
Browsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-
Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-
Lgcy-Mgmt-Console, Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service,
Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression,
Web-Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity-
Foundation, RSAT-ADDS-Tools
Restart-Computer
```

3. Подключитесь к виртуальной машине exVM с помощью портал Azure с помощью учетной записи и пароля CORP\<ADMIN_NAME>.

4. В диспетчер сервера щелкните **Локальный сервер**. В **разделе Свойства** для exVM щелкните **Включено** для **конфигурации усиленной безопасности IE**. В **разделе Конфигурация усиленной безопасности Internet Explorer** нажмите кнопку **Выкл** . для администраторов и пользователей, а затем нажмите кнопку **OK**.

5. На начальном экране щелкните **Internet Explorer** и скачайте средство Unified Communications Managed API 4.0 Runtime по адресу https://www.microsoft.com/download/details.aspx?id=34992 . Когда отобразится соответствующее предложение, щелкните **Запустить**.

6. В программе установки Microsoft Unified Communications Managed API 4.0 Runtime нажмите кнопку **Далее**.

7. Щелкните **Мною прочитаны и приняты условия лицензии**, а затем — **Установить**. На странице **Установка завершена** нажмите кнопку **Готово**.

8. Скачайте последнюю версию Exchange из Internet Explorer. Дополнительные сведения см. в разделе Обновления для Exchange Server.

9. Нажмите кнопку **Сохранить**, чтобы сохранить ISO-файл в папке "Загрузки".

10. Выберите элемент **Открыть папку**, затем щелкните правой кнопкой мыши ISO-файл Exchange и выберите **Подключить**.

11. В виртуальной машине exVM в командной строке Windows PowerShell с правами администратора выполните указанную ниже команду.

> ⓘ **Примечание**
>
> - Предыдущий переключатель */IAcceptExchangeServerLicenseTerms* не будет работать начиная с накопительных обновлений (CU) за сентябрь 2021 г.

Теперь необходимо использовать */IAcceptExchangeServerLicenseTerms_DiagnosticDataON* или */IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF* для автоматической установки и установки по сценариям.

- В примерах ниже используется переключатель */IAcceptExchangeServerLicenseTerms_DiagnosticDataON*. Вы можете изменить переключатель на */IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF*.

PowerShell

```
e:
.\setup.exe /mode:Install /role:Mailbox /OrganizationName:Contoso
/IAcceptExchangeServerLicenseTerms_DiagnosticDataON
Restart-Computer
```

Дождитесь завершения установки Exchange, которая может занять некоторое время, и перезапуска виртуальной машины exVM.

Добавление двух почтовых ящиков на сервер Exchange Server

1. Подключитесь к виртуальной машине exVM с помощью портал Azure с помощью учетной записи и пароля CORP\<ADMIN_NAME>.

2. На начальном экране введите **Exchange**, а затем выберите элемент **Командная консоль Exchange**.

3. Скопируйте указанные ниже команды в Блокнот, вставьте DNS-имя виртуальной машины exVM в Интернете в качестве значения переменной **$dnsName**, а затем скопируйте и вставьте полученные команды в командную консоль Exchange.

   PowerShell

   ```
   $dnsName="<Internet DNS name of the exVM virtual machine>"
   $user1Name="chris@" + $dnsName
   $user2Name="janet@" + $dnsName
   $db=Get-MailboxDatabase
   $dbName=$db.Name
   $password = Read-Host "Enter password" -AsSecureString
   ```

4. Сохраните указанный пароль в надежном месте. Затем создайте два почтовых ящика, выполнив указанные ниже команды.

```
PowerShell

New-Mailbox -UserPrincipalName $user1Name -Alias chris -Database
$dbName -Name ChrisAshton -OrganizationalUnit Users -Password $password
-FirstName Chris -LastName Ashton -DisplayName "Chris Ashton"
New-Mailbox -UserPrincipalName $user2Name -Alias janet -Database
$dbName -Name JanetSchorr -OrganizationalUnit Users -Password $password
-FirstName Janet -LastName Schorr -DisplayName "Janet Schorr"
```

Проверка доставки почты между почтовыми ящиками

1. В браузере на локальном компьютере перейдите на веб-сайт **https://**< Интернет DNS-имя виртуальной машины> exVM **или owa**. Когда отобразится страница ошибки сертификата безопасности веб-сайта, щелкните **Продолжить открытие этого веб-сайта**. Войдите в Outlook, используя учетную запись corp\chris и соответствующий пароль для нее.

2. Когда отобразится предложение указать язык и часовой пояс, выберите необходимые значения и щелкните **Сохранить**.

3. В папке "Входящие" пользователя Chris Ashton щелкните **Создать**. В поле **Кому** введите **janet**, а затем выберите элемент **Поиск в каталоге**. В поле **Тема** введите **Проверочное сообщение**, а затем нажмите кнопку **Отправить**.

4. Щелкните значок пользователя в верхней правой части веб-страницы "Почта", а затем выберите элемент **Выход**.

5. Войдите в Outlook, используя учетную запись corp\janet и соответствующий пароль для нее. Когда отобразится предложение указать язык и часовой пояс, выберите необходимые значения и щелкните **Сохранить**.

6. Убедитесь, что в папке "Входящие" есть проверочное сообщение от пользователя Chris Ashton. Щелкните его, а затем щелкните **Ответить всем**. В тексте сообщения введите **Ответ**, а затем щелкните **Отправить**.

7. Щелкните значок пользователя в верхней правой части веб-страницы "Почта", а затем выберите **Выход**.

8. Войдите в Outlook, используя учетную запись corp\chris и соответствующий пароль для нее. Убедитесь, что в папке "Входящие" есть ответное сообщение от пользователя Janet.

Теперь вы готовы к тестированию функций или приложений Exchange.

Остановка и запуск виртуальных машин

За использование виртуальных машин Azure взимается повременная плата. Чтобы свести к минимуму затраты на среду разработки и тестирования Exchange, используйте следующие команды для остановки виртуальных машин:

PowerShell

```
$rgName="<your resource group name>"
Stop-AZVM -Name exVM -ResourceGroupName $rgName -Force
Stop-AZVM -Name adVM -ResourceGroupName $rgName -Force
```

Чтобы снова запустить их, выполните указанные ниже команды.

PowerShell

```
$rgName="<your resource group name>"
Start-AZVM -Name adVM -ResourceGroupName $rgName
Start-AZVM -Name exVM -ResourceGroupName $rgName
```

См. также

Устранение проблем с исходящим SMTP-подключением в Azure

Развертывание новых установок Exchange

Требования к системе для Exchange Server

Exchange Server

Новые возможности Exchange Server

Руководства по лаборатории тестирования для облачных решений

Обновление Exchange до последнего накопительного пакета обновления

Статья • 04.04.2023

Если вы установили Exchange Server 2016 или Exchange Server 2019, вы можете обновить серверы Exchange до последней версии накопительного обновления (CU). Так как каждый накопительный пакет обновления — это полная установка Exchange, которая включает в себя обновления и изменения из всех предыдущих ЦУ, вам не нужно сначала устанавливать какие-либо предыдущие CU или Exchange 2016 RTM или Exchange 2019 RTM. Дополнительные сведения о последних доступных CU Exchange см. в разделе Обновления для Exchange Server.

> ⊗ **Внимание!**
>
> После обновления Exchange до более новой версии cu вы не сможете удалить новую версию, чтобы отменить изменения до предыдущей версии. При удалении новой версии Exchange с сервера будет полностью удален.

Что нужно знать перед началом работы

- Предполагаемое время выполнения: 180 минут
- Учетная запись, используемая для установки накопительного пакета обновления, требует членства в группе ролей "Управление организацией Exchange". Если накопительный пакет обновления требует обновления схемы Active Directory или подготовки домена, для учетной записи, скорее всего, потребуется больше разрешений. Дополнительные сведения см. в статье Подготовка Active Directory и доменов для Exchange Server.
- Прежде чем устанавливать накопительный пакет обновления, ознакомьтесь с заметками о выпуске .
- Убедитесь, что целевой сервер соответствует потенциально новым требованиям к системе и предварительным требованиям для накопительного пакета обновления. Дополнительные сведения см. в Exchange Server требованиях к системе и Exchange Server предварительных требованиях.

  > ⊗ **Внимание!**

При установке exchange CU **будут перезаписаны** следующие типы настраиваемых параметров:

- Все настраиваемые параметры Exchange или IIS, внесенные в файлы конфигурации приложения Exchange XML на сервере Exchange Server. Например, web.config файлы или файл EdgeTransport.exe.config. Начиная с Exchange Server 2019 с накопительным пакетом обновления 13 для наиболее распространенных изменений файла конфигурации будут автоматически создаваться резервные копии и восстанавливаться. **Дополнительные сведения см. здесь.**
- Настройки параметров TLS/шифра операционной системы.

Обязательно сохраните эти сведения, чтобы можно было легко повторно применить параметры после установки. После установки exchange CU необходимо повторно настроить эти параметры.

- После установки exchange CU необходимо перезагрузить компьютер, чтобы можно было вносить изменения в реестр и операционную систему.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**.

Рекомендации

- Всегда обновляйте серверы как можно более актуально. Это особенно относится к установке нового сервера.
- Всегда устанавливайте последнее накопительное обновление при создании нового сервера.
- Нет необходимости устанавливать сборку RTM или предыдущие сборки, а затем обновлять до последней накопительной версии. Это связано с тем, что каждый накопительный пакет обновления является полной сборкой продукта.
- Перезагрузите сервер заранее.
- Сначала протестируйте новое обновление в нерабочей среде, чтобы избежать проблем в новом обновлении, влияющих на рабочую среду.
- Создайте протестированную и рабочую резервную копию Active Directory и Exchange Server.
- Создайте резервную копию всех настроек и всех настроек. Они не выживут в обновлении.

> ⓘ **Примечание**
>
> Exchange Server 2019 CU13 или более поздней версии будет создавать резервные копии и восстанавливать наиболее распространенные файлы конфигурации. Список сохраненных конфигураций можно найти **здесь**.

- Используйте командную строку с повышенными привилегиями для запуска накопительного обновления.
- Временно отключите все антивирусные программы во время процесса обновления.
- Перезагрузите сервер после завершения обновления.
- Для серверов Exchange Server, установленных в группе доступности базы данных, выполните действия, описанные в разделе Управление группами доступности базы данных в Exchange Server, чтобы перед установкой накопительных обновлений перевести участников DAG в режим обслуживания.

Установка exchange CU с помощью мастера установки

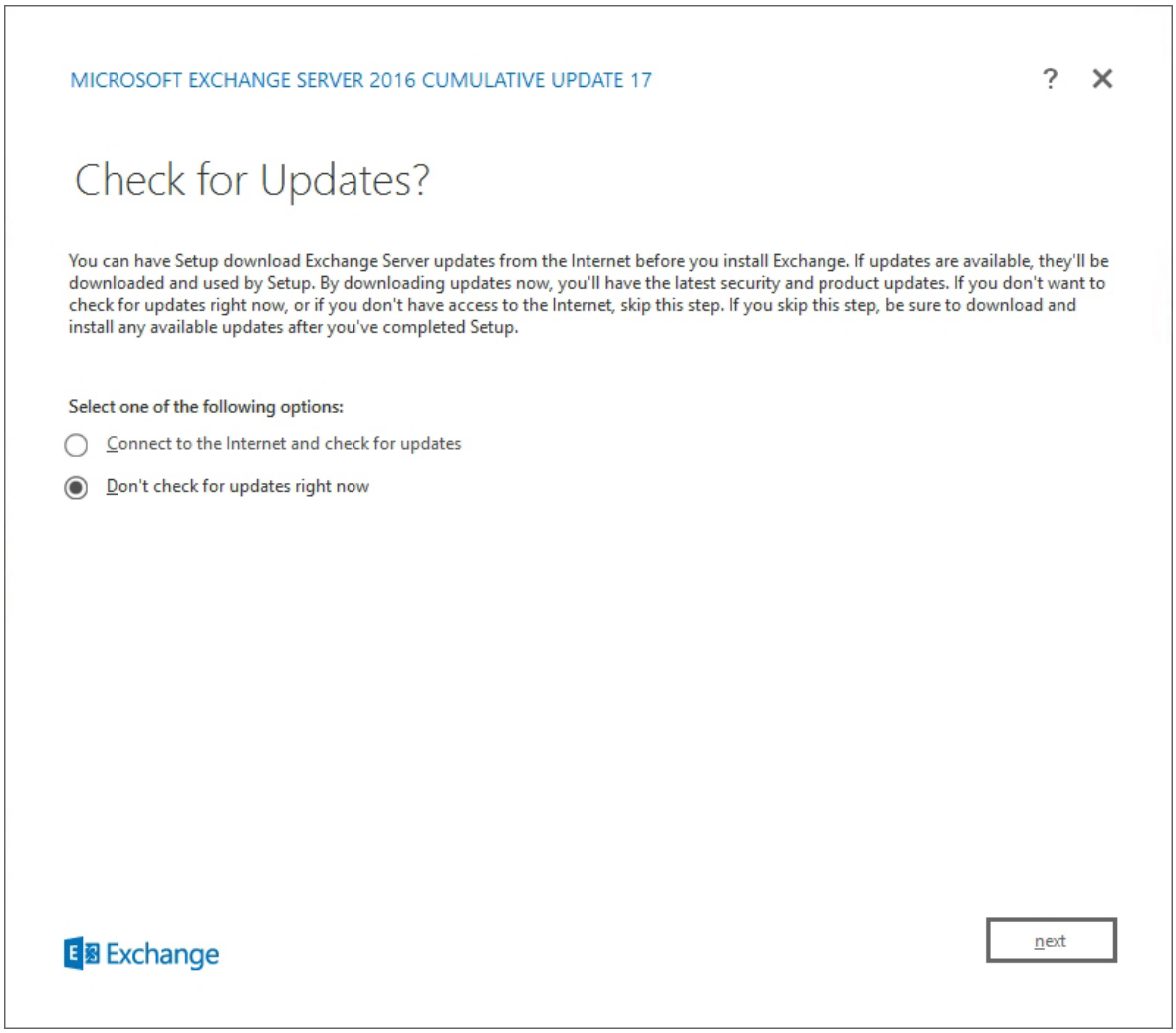
1. Скачайте последнюю версию Exchange на целевом компьютере. Дополнительные сведения см. в разделе Обновления для Exchange Server.

2. В проводник щелкните правой кнопкой мыши скачанный файл ISO-образа Exchange CU и выберите **Подключить**. В появившемся появившемся виртуальном DVD-диске запустите программу установки Exchange, дважды щелкнув `Setup.exe`.

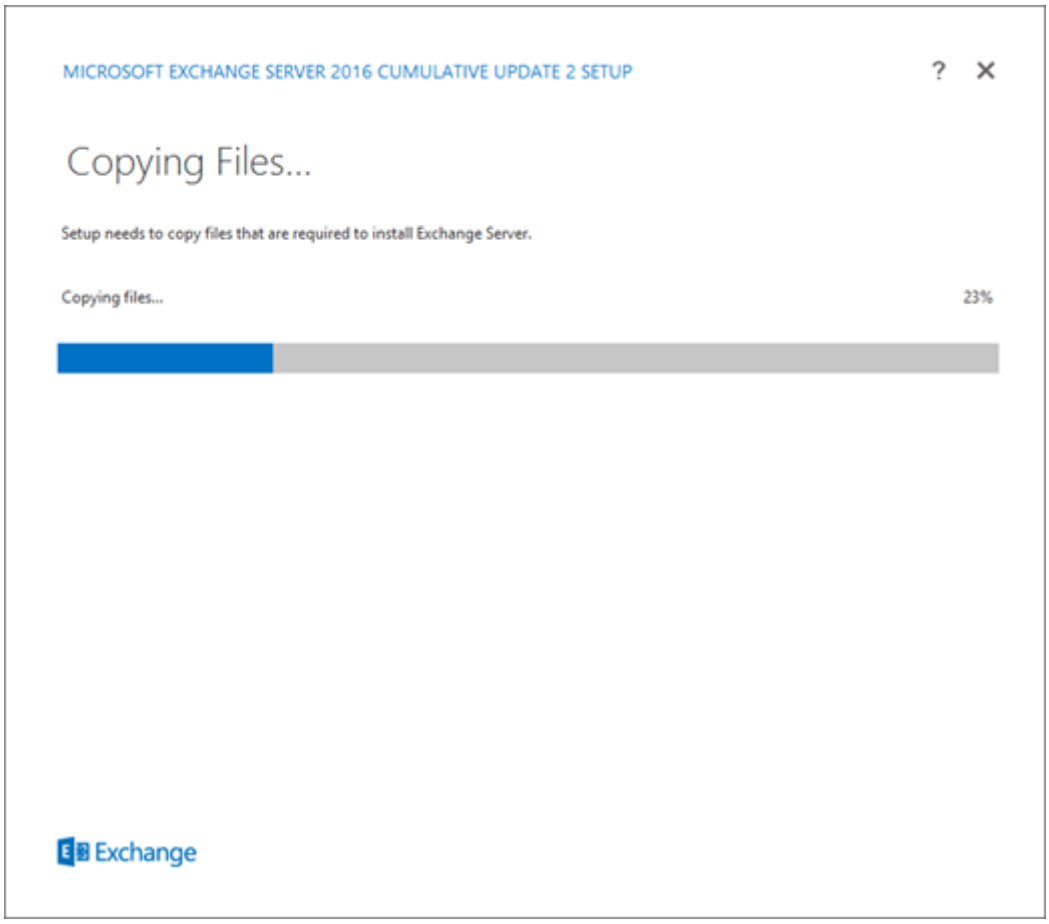
3. Откроется мастер установки Exchange Server. На странице **Проверить наличие обновлений** выберите один из предложенных ниже вариантов и нажмите кнопку **Далее** для продолжения.

    - **Подключение к Интернету и проверка обновлений**. Мы рекомендуем использовать этот параметр, который выполняет поиск обновлений для *устанавливаемой* версии Exchange (не обнаруживает новые ЦУ). При выборе этого варианта вы автоматически будете перенаправлены на страницу **Скачивание обновлений**, где выполняется поиск обновлений. Для продолжения нажмите кнопку **Далее**.

    - **Не проверять обновления сейчас**.

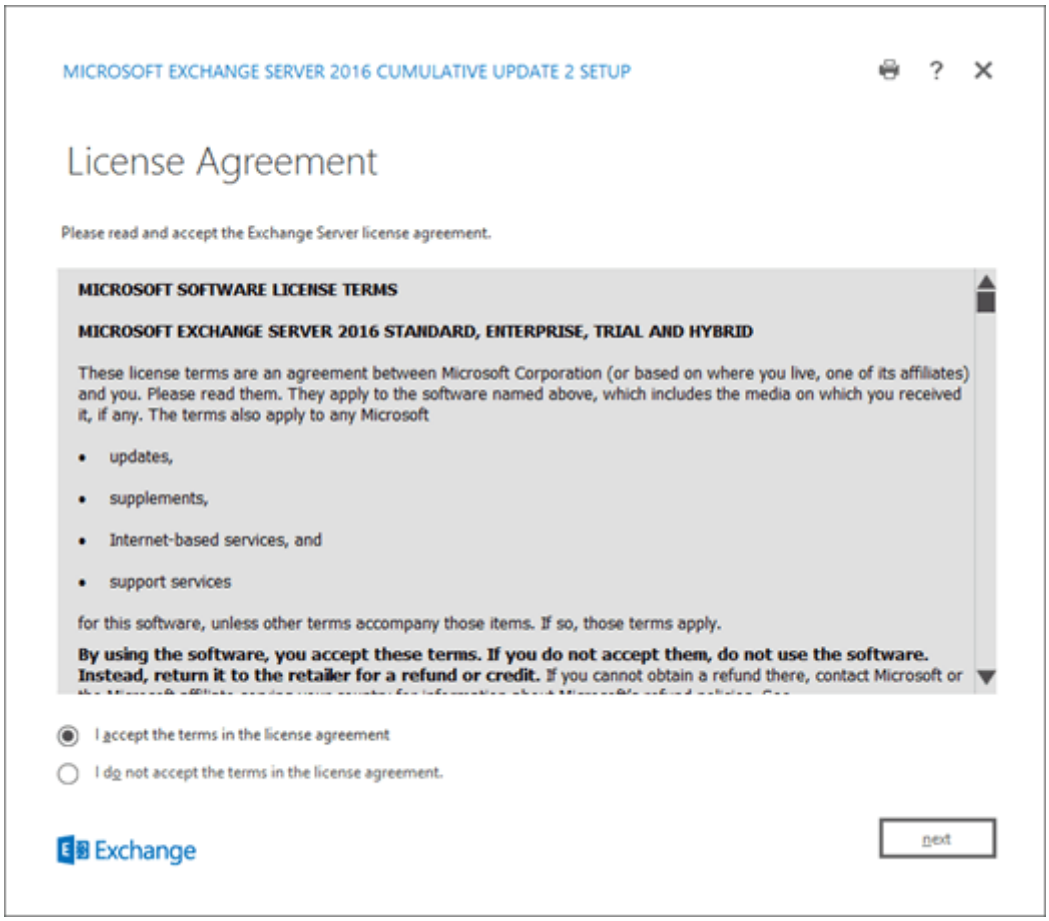


4. На странице **Копирование файлов** отображается ход выполнения копирования файлов на локальный жесткий диск. Как правило, файлы копируются в `%WinDir%\Temp\ExchangeSetup`, но вы можете подтвердить расположение в журнале установки Exchange по адресу `C:\ExchangeSetupLogs\ExchangeSetup.log`.

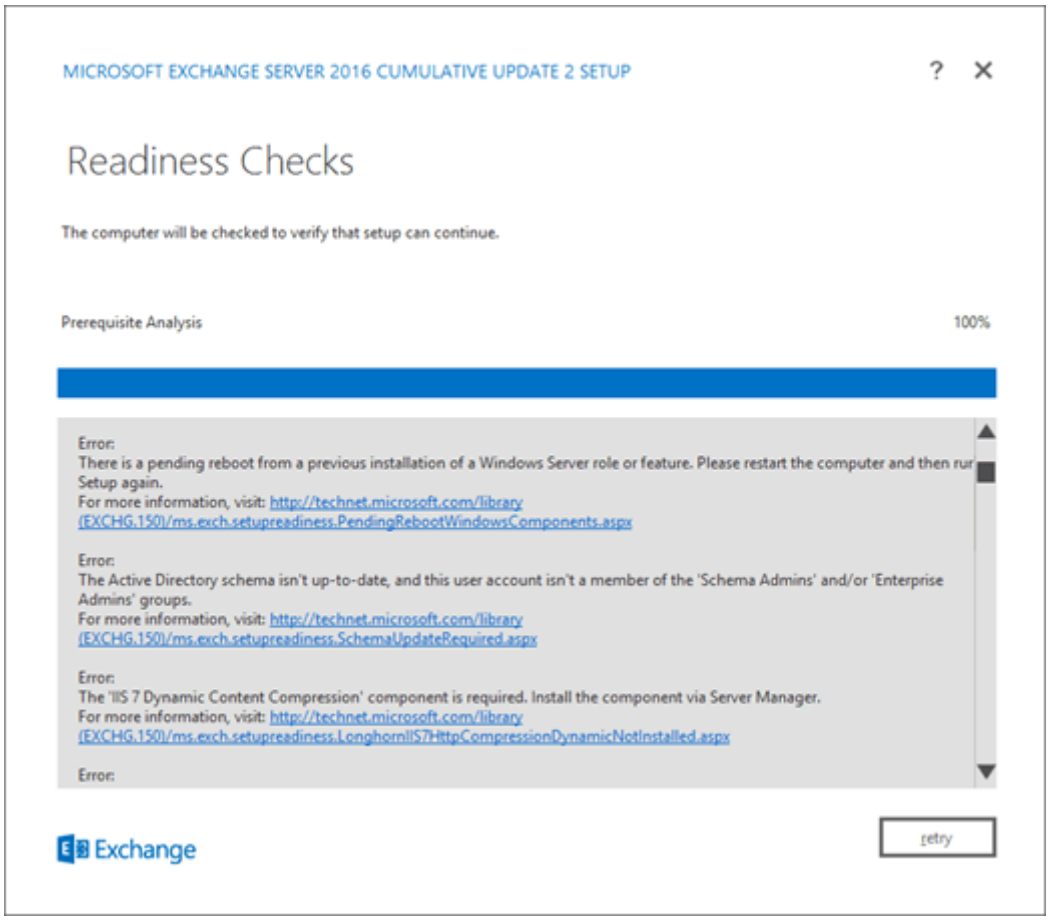


5. На странице **Обновление** показано, что программа установки обнаружила существующую установку Exchange, поэтому вы обновляете Exchange на сервере (не устанавливаете новый сервер Exchange). Для продолжения нажмите кнопку **Далее**.

6. На странице **Лицензионное соглашение** ознакомьтесь с условиями лицензионного соглашения на программное обеспечение, выберите **Я принимаю условия лицензионного соглашения** и нажмите **Далее**, чтобы продолжить.

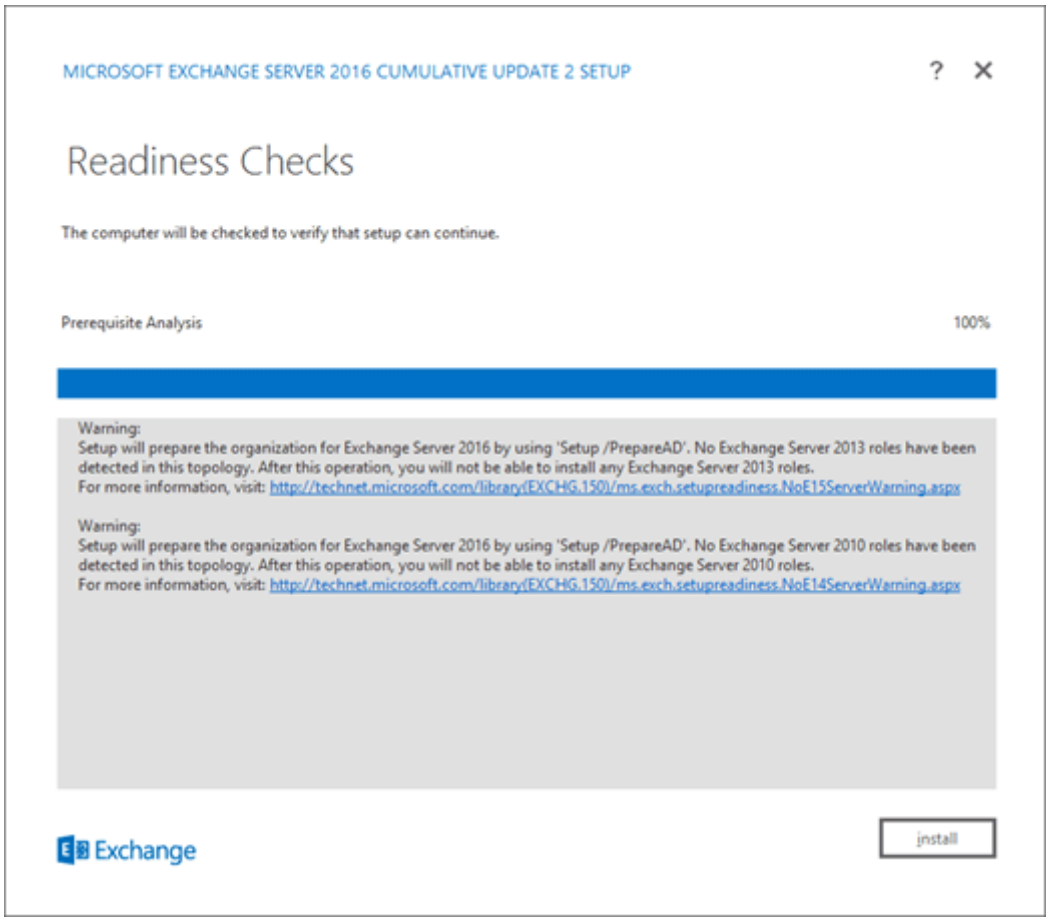


7. На странице **Проверки готовности** убедитесь, что проверки готовности успешно завершены. В противном случае на странице будет отображаться только кнопка **Повторить**.

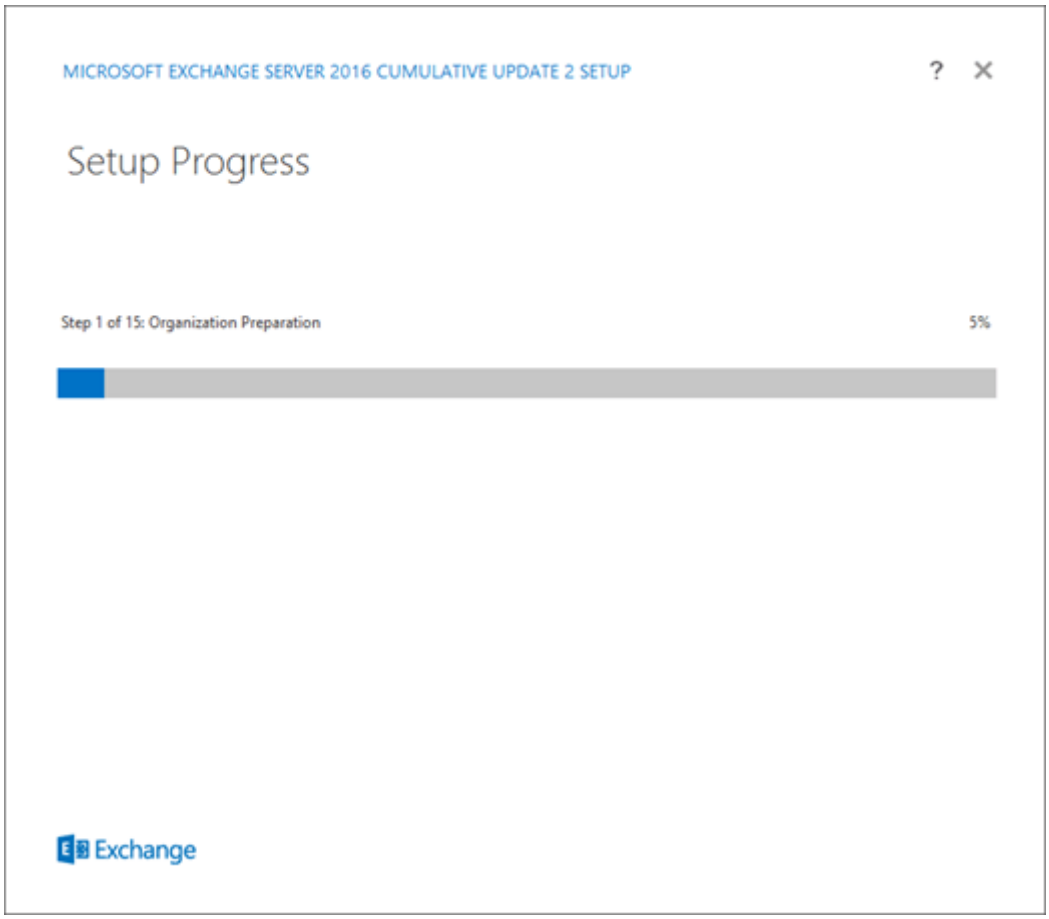


Устранив ошибки, нажмите кнопку **Повторить попытку**, чтобы снова запустить проверки наличия обязательных компонентов. Некоторые ошибки можно исправить, не выходя из программы установки, а для исправления других понадобится перезагрузить компьютер. После перезагрузки компьютера придется начинать с шага 1.

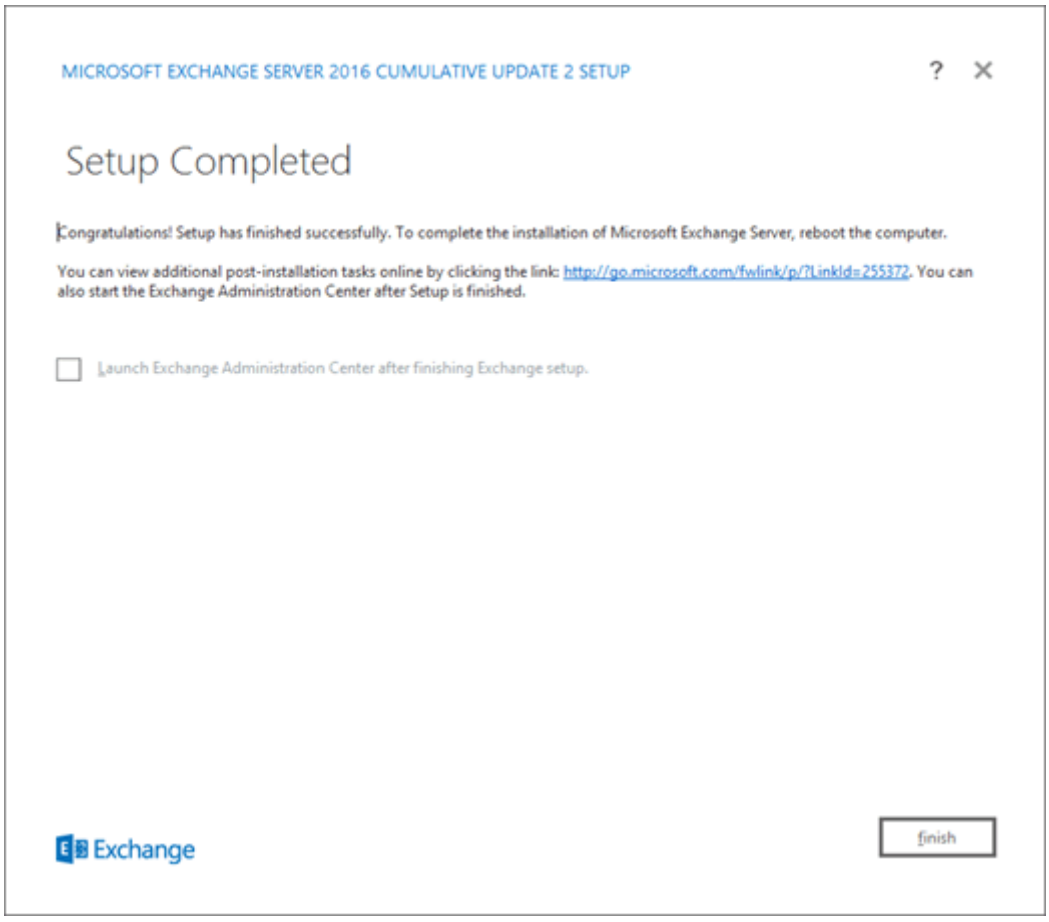
Когда на странице **Проверки готовности** больше не будет ошибок, на месте кнопки **Повторить** появится кнопка **Установить**. Обязательно просмотрите все предупреждения и нажмите кнопку **Установить** , чтобы установить Exchange.



8. На странице **Ход установки** отображается индикатор хода установки.



9. На странице **Установка завершена** нажмите **Готово** и перезагрузите компьютер.



Установка exchange CU с помощью автоматической установки из командной строки

Чтобы установить exchange CU из командной строки, используйте следующий синтаксис:

> ⓘ **Примечание**
>
> - Предыдущий переключатель */IAcceptExchangeServerLicenseTerms* не будет работать начиная с накопительных обновлений (CU) за сентябрь 2021 г. Теперь необходимо использовать */IAcceptExchangeServerLicenseTerms_DiagnosticDataON* или */IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF* для автоматической установки и установки по сценариям.
>
> - В следующих примерах используется параметр */IAcceptExchangeServerLicenseTerms_DiagnosticDataON* . Вы можете изменить переключатель на */IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF*.

Консоль

```
<Virtual DVD drive letter>:\Setup.exe
/IAcceptExchangeServerLicenseTerms_DiagnosticDataON /Mode:Upgrade
[/DomainController:<ServerFQDN>] [/EnableErrorReporting]
```

Примечания.

- Необязательный параметр */DomainController* указывает контроллер домена, который программа установки использует для чтения данных из записи в Active Directory.

- Необязательный параметр */EnableErrorReporting* позволяет программе установки автоматически отправлять критические отчеты об ошибках в корпорацию Майкрософт. Корпорация Майкрософт использует эти сведения для диагностики проблем и предоставления решений.

В этом примере используются файлы exchange CU на диске E: для установки накопительного пакета обновления на локальном сервере, а контроллер домена

dc01.contoso.com для чтения и записи в Active Directory.

Консоль

```
E:\Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON
/Mode:Upgrade /DomainController:dc01.contoso.com
```

Дополнительные сведения о автоматической установке из командной строки см. в разделе Установка Exchange в автоматическом режиме.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно установили exchange CU, см. статью Проверка Exchange Server установки.

сохранение пользовательской конфигурации Exchange Server

Статья • 06.05.2023

Обзор

После установки Exchange Server обычной задачей администратора является настройка параметров, таких как ограничения на размер сообщений клиента. Эти параметры обычно настраиваются в `web.config`, `sharedweb.config` и других файлах конфигурации на сервере Exchange Server.

Сложилось так, что одна из проблем для администраторов Exchange Server заключается в том, что при каждой установке накопительного обновления эти файлы и пользовательские параметры в них перезаписываются программой установки, заставляя администратора создавать резервные копии или восстанавливать их или повторно применить их после каждой установки cu.

При использовании Exchange **Server 2019 CU13 и более поздних версий** программа установки теперь выполняет резервное копирование и восстановление наиболее распространенных файлов конфигурации, чтобы администраторам больше не нужно восстанавливать их вручную или повторно применить их.

Программа установки сохраняет пользовательские конфигурации следующим образом:

1. Программа установки создает резервную копию существующих файлов.
2. Программа установки устанавливает Exchange Server (или обновляет существующие Exchange Server), а существующие файлы перезаписываются конфигурациями и параметрами по умолчанию, присутствующими в программе установки Exchange.
3. Программа установки окончательно восстанавливает соответствующие файлы и пользовательские значения критических ключей, хранящихся в файлах конфигурации preupgrade в новых файлах конфигурации, скопированных из программы установки Exchange.

Программа установки сохраняет наиболее важные параметры конфигурации (если они есть), которые могут включать целые разделы или определенные пары значений ключей.

1. `appSettings` содержит много пар ключевых значений, которые настраивают диапазон параметров приложения (например, путь ведения журнала, размер очереди сообщений и т. д.). Любая пара значений ключей, созданная с помощью `<add key>` тега, сохраняется, если этот раздел присутствует.

   Например, в следующем файле `ClientTunnelExpirationTime` сохраняется.

   ```
   <configuration>
   <appSettings>
       <add key="ClientTunnelExpirationTime" value="30" />
   </appSettings>
   </ configuration>
   ```

2. Весь `proxySettings` раздел является критическим и сохраняется.

3. `maxAllowedContentLength` используется для указания максимальной длины содержимого (в байтах) в запросе.

   ```
   <system.webServer>
       <security>
       <requestFiltering>
           <requestLimits maxAllowedContentLength="4194304" />
       </requestFiltering>
       </security>
   <system.webServer>
   ```

4. `maxRequestLength` используется для указания максимального размера запроса.

   ```
   <system.web>
       <httpRuntime maxRequestLength="4194304" />
   ```

```
</system.web>
```

5. `maxReceivedMessageSize` используется в `systembinding` элементах и `custombinding` для задания максимального размера (в байтах) для сообщения, которое может быть получено в канале, настроенном с помощью этой привязки.
6. `maxStringContentLength` присутствует в элементах `systembinding` и и `customBinding` используется для ограничения максимального размера строки, возвращаемого средством чтения XML.
7. `extendedProtectionPolicy` используется для установки политики расширенной защиты, которая используется сервером для проверки входящих клиентских подключений.
8. `defaultProxy` используется для настройки прокси-сервера HTTP.

Список сохраненных файлов конфигурации вместе с разделами и ключами, сохраненными

Ниже приведен список всех файлов конфигурации, а также разделов и ключей, которые автоматически сохраняются во время обновления CU.

> ⓘ **Примечание**
>
> Устранение рисков правил перезаписи URL-адресов IIS, примененных на уровне каждого сайта или каждого виртуального каталога, не будет сохранено этой функцией и в конечном итоге будет повторно применено службой экстренного устранения рисков Exchange, если они по-прежнему применимы для установленного накопительного пакета обновления. Дополнительные сведения см. здесь.

Развернуть таблицу

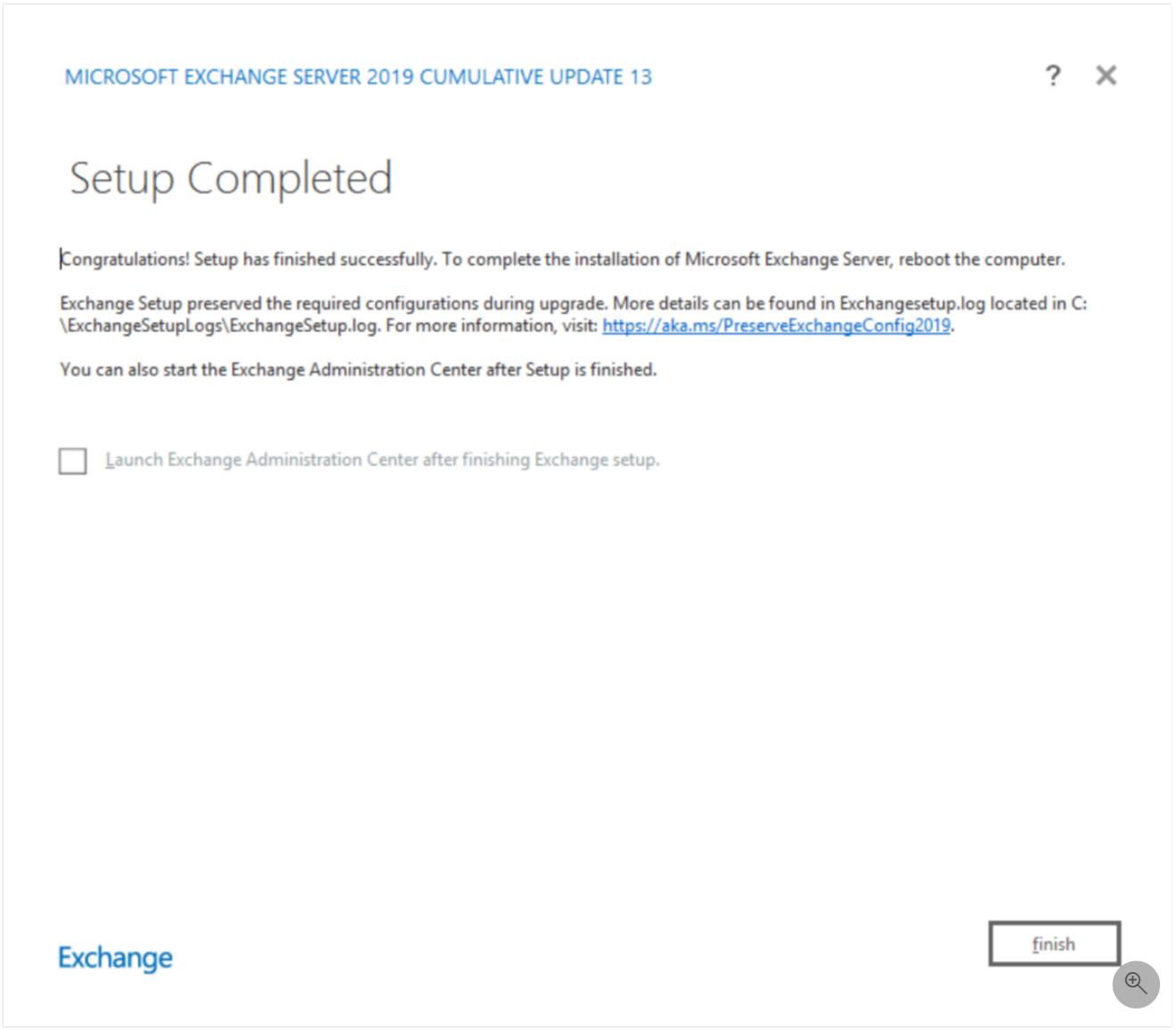
Нет.	Имя файла конфигурации	Разделы, сохраненные	Дополн ключи
1	`<ExchangeInstallPath>\V15\Bin\ComplianceAuditService.exe.config`	appSettings	-
2	`<ExchangeInstallPath>\V15\Bin\EdgeTransport.exe.config`	appSettings	-
3	`<ExchangeInstallPath>\V15\Bin\Microsoft.Exchange.Diagnostics.Service.exe.config`	appSettings	-
4	`<ExchangeInstallPath>\V15\Bin\Microsoft.Exchange.Directory.TopologyService.exe.config`	appSettings	maxRec maxStri
5	`<ExchangeInstallPath>\V15\Bin\Microsoft.Exchange.EdgeSyncSvc.exe.config`	appSettings	-
6	`<ExchangeInstallPath>\V15\Bin\Microsoft.Exchange.Mitigation.Service.exe.config`	appSettings	-
9	`<ExchangeInstallPath>\V15\Bin\Microsoft.Exchange.RpcClientAccess.Service.exe.config`	appSettings, defaultProxy	maxRec maxStri
10	`<ExchangeInstallPath>\V15\Bin\Microsoft.Exchange.Search.Service.exe.config`	appSettings	-
12	`<ExchangeInstallPath>\V15\Bin\Microsoft.Exchange.Servicehost.exe.config`	appSettings, defaultProxy	maxRec maxStri
14	`<ExchangeInstallPath>\V15\Bin\Microsoft.Exchange.Store.Service.exe.config`	appSettings	-
17	`<ExchangeInstallPath>\V15\Bin\MSExchangeCompliance.exe.config`	appSettings	-
18	`<ExchangeInstallPath>\V15\Bin\MSExchangeDelivery.exe.config`	appSettings	-
19	`<ExchangeInstallPath>\V15\Bin\MSExchangeFrontEndTransport.exe.config`	appSettings	-
20	`<ExchangeInstallPath>\V15\Bin\MSExchangeHMHost.exe.config`	appSettings	-
21	`<ExchangeInstallPath>\V15\Bin\MSExchangeHMRecovery.exe.config`	appSettings	-
22	`<ExchangeInstallPath>\V15\Bin\MSExchangeHMWorker.exe.config`	appSettings	-
23	`<ExchangeInstallPath>\V15\Bin\MSExchangeMailboxAssistants.exe.config`	appSettings	-
24	`<ExchangeInstallPath>\V15\Bin\MsExchangeMailboxReplication.exe.config`	appSettings, defaultProxy	maxRec maxStri

Нет.	Имя файла конфигурации	Разделы, сохраненные	Дополн ключи
26	`<ExchangeInstallPath>\V15\Bin\MSExchangeSubmission.exe.config`	appSettings	-
27	`<ExchangeInstallPath>\V15\Bin\MSExchangeThrottling.exe.config`	appSettings	-
28	`<ExchangeInstallPath>\V15\Bin\MSExchangeTransport.exe.config`	appSettings	-
29	`<ExchangeInstallPath>\V15\ClientAccess\PopImap\Microsoft.Exchange.Imap4.exe.config`	appSettings, defaultProxy	-
30	`<ExchangeInstallPath>\V15\ClientAccess\PopImap\Microsoft.Exchange.Imap4Service.exe.config`	appSettings	-
31	`<ExchangeInstallPath>\V15\ClientAccess\PopImap\Microsoft.Exchange.Pop3.exe.config`	appSettings, defaultProxy	-
32	`<ExchangeInstallPath>\V15\ClientAccess\PopImap\Microsoft.Exchange.Pop3Service.exe.config`	appSettings	-
33	`<ExchangeInstallPath>\V15\FrontEnd\PopImap\Microsoft.Exchange.Imap4.exe.config`	appSettings, defaultProxy	-
34	`<ExchangeInstallPath>\V15\FrontEnd\PopImap\Microsoft.Exchange.Imap4Service.exe.config`	appSettings	-
35	`<ExchangeInstallPath>\V15\FrontEnd\PopImap\Microsoft.Exchange.Pop3.exe.config`	appSettings, defaultProxy	-
36	`<ExchangeInstallPath>\V15\FrontEnd\PopImap\Microsoft.Exchange.Pop3Service.exe.config`	appSettings	-
37	`<ExchangeInstallPath>\V15\Bin\Microsoft.Exchange.AddressBook.Service.dll.config`	appSettings	-
38	`<ExchangeInstallPath>\V15\Bin\Microsoft.Exchange.Management.Transport.dll.config`	appSettings	-
39	`<ExchangeInstallPath>\V15\TransportRoles\agents\Antimalware\Microsoft.Exchange.Transport.Agent.Malware.dll.config`	appSettings	-
40	`<ExchangeInstallPath>\V15\Bin\MSExchangeUM.config`	appSettings	-
41	`<ExchangeInstallPath>\V15\ClientAccess\Autodiscover\web.config`	appSettings	maxRec
42	`<ExchangeInstallPath>\V15\ClientAccess\ecp\web.config`	appSettings	maxRec maxStri
43	`<ExchangeInstallPath>\V15\ClientAccess\ecp\DLPPolicy\Web.config`	-	maxRec
44	`<ExchangeInstallPath>\V15\ClientAccess\ecp\Handlers\Web.config`	-	maxRec
45	`<ExchangeInstallPath>\V15\ClientAccess\ecp\PersonalSettings\Web.config`	-	maxRec
46	`<ExchangeInstallPath>\V15\ClientAccess\ecp\UsersGroups\Web.config`	-	maxRec
47	`<ExchangeInstallPath>\V15\ClientAccess\exchweb\ews\web.config`	appSettings, defaultProxy, extendedProtectionPolicy	maxAllc maxRec maxRec maxStri
48	`<ExchangeInstallPath>\V15\ClientAccess\mapi\emsmdb\web.config`	appSettings, defaultProxy	maxAllc maxRec maxRec maxStri
49	`<ExchangeInstallPath>\V15\ClientAccess\mapi\nspi\web.config`	appSettings, defaultProxy	maxAllc maxRec
50	`<ExchangeInstallPath>\V15\ClientAccess\OAB\web.config`	appSettings	-
52	`<ExchangeInstallPath>\V15\ClientAccess\PowerShell\web.config`	appSettings	-
53	`<ExchangeInstallPath>\V15\ClientAccess\PowerShell-Proxy\web.config`	appSettings	-
54	`<ExchangeInstallPath>\V15\ClientAccess\PushNotifications\web.config`	appSettings	maxRec
55	`<ExchangeInstallPath>\V15\ClientAccess\rest\web.config`	appSettings	maxAllc maxRec
56	`<ExchangeInstallPath>\V15\ClientAccess\RpcProxy\web.config`	appSettings	-
57	`<ExchangeInstallPath>\V15\ClientAccess\Sync\web.config`	appSettings, defaultProxy	MaxDoc maxRec maxAllc

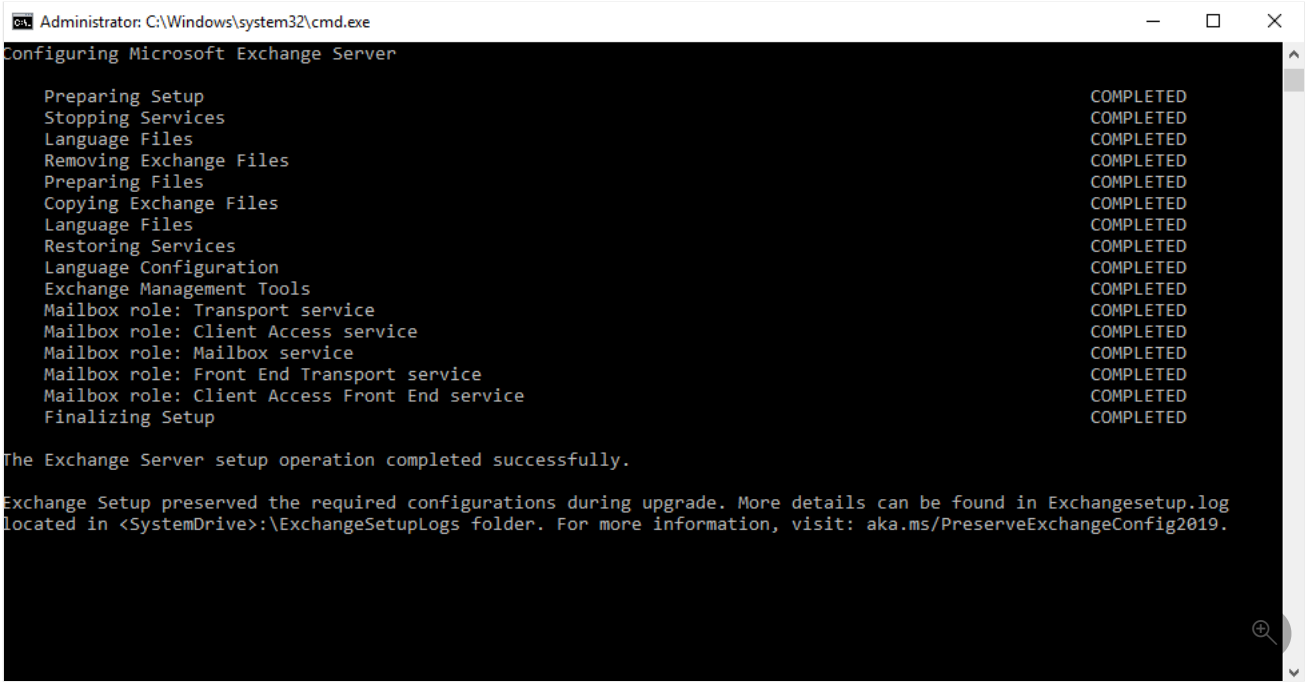
Нет.	Имя файла конфигурации	Разделы, сохраненные	Дополн ключи
58	`<ExchangeInstallPath>\V15\FrontEnd\HttpProxy\autodiscover\web.config`	appSettings	-
59	`<ExchangeInstallPath>\V15\FrontEnd\HttpProxy\ecp\web.config`	appSettings	maxAllo maxRec
60	`<ExchangeInstallPath>\V15\FrontEnd\HttpProxy\ews\web.config`	appSettings	maxAllo maxRec
61	`<ExchangeInstallPath>\V15\FrontEnd\HttpProxy\mapi\web.config`	appSettings	maxAllo maxRec
62	`<ExchangeInstallPath>\V15\FrontEnd\HttpProxy\oab\web.config`	appSettings	-
63	`<ExchangeInstallPath>\V15\FrontEnd\HttpProxy\owa\web.config`	appSettings	maxAllo maxRec
64	`<ExchangeInstallPath>\V15\FrontEnd\HttpProxy\powershell\web.config`	appSettings	-
65	`<ExchangeInstallPath>\V15\FrontEnd\HttpProxy\pushnotifications\web.config`	appSettings	maxAllo maxRec
66	`<ExchangeInstallPath>\V15\FrontEnd\HttpProxy\ReportingWebService\web.config`	appSettings	-
67	`<ExchangeInstallPath>\V15\FrontEnd\HttpProxy\rest\web.config`	appSettings	maxAllo maxRec
68	`<ExchangeInstallPath>\V15\FrontEnd\HttpProxy\rpc\web.config`	appSettings	maxAllo maxRec
69	`<ExchangeInstallPath>\V15\FrontEnd\HttpProxy\sync\web.config`	appSettings	maxRec maxAllo
70	`<ExchangeInstallPath>\V15\FIP-FS\Data\Configuration.xml`	ProxySettings	-
71	`<ExchangeInstallPath>\V15\Bin\Search\Ceres\Runtime\1.0\Noderunner.exe.config`	-	memory

После завершения установки будут отображаться следующие сообщения, указывающие на успешное восстановление всех сохраненных параметров конфигурации.

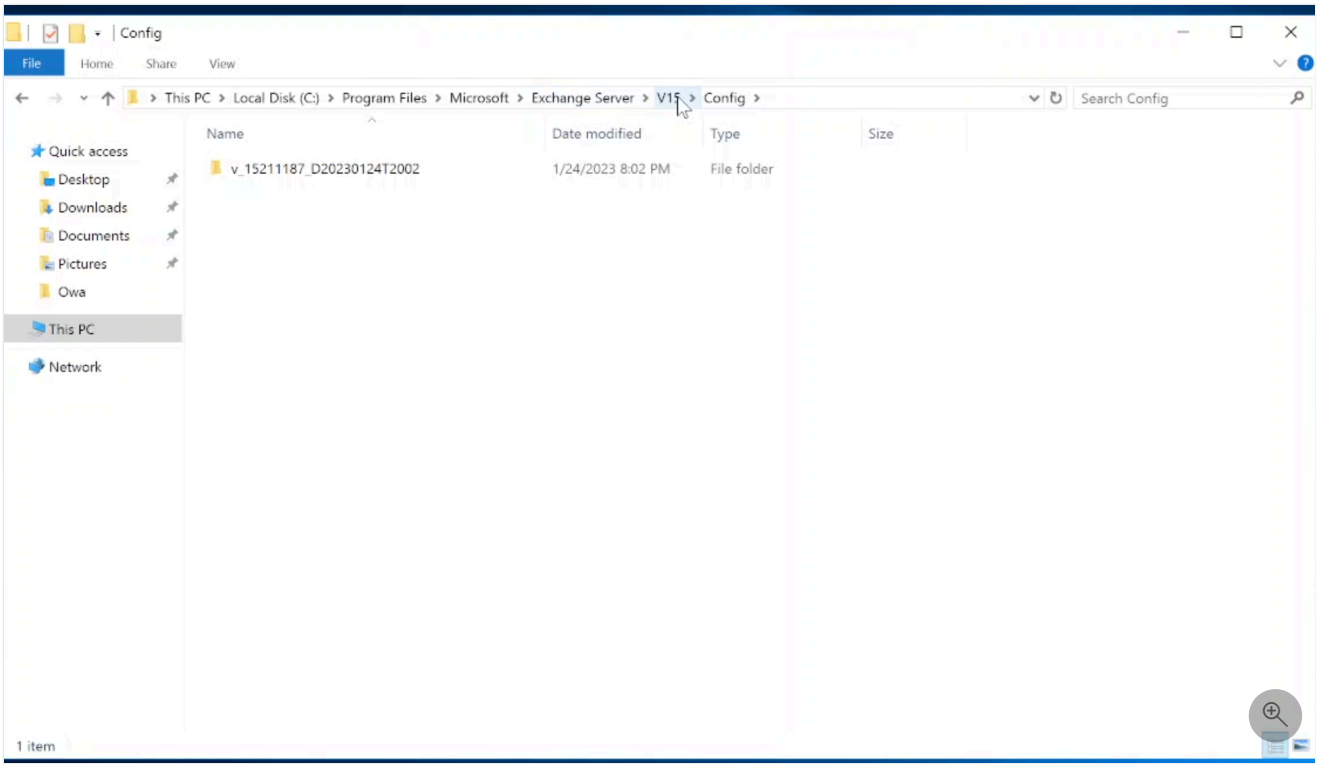
Режим графического пользовательского интерфейса



Автоматический режим



Резервная копия сохраненных файлов конфигурации хранится во `%ProgramFiles%\Microsoft\Exchange Server\V15\Config` вложенных папках, использующих формат именования `v_<ExchangeVersion>_<Timestamp>`.



> **Примечание**
>
> Если эти файлы не требуются после завершения установки, их можно безопасно удалить.

Настройка сохраняет пользовательские параметры по умолчанию. Если вы не хотите использовать эту функцию, ее можно отключить, создав `REG_SZ` запись `DisablePreservation` в разделе `HKLM\SOFTWARE\Microsoft\ExchangeServer\v15\Setup` и задав для нее `1`значение .

Пару "ключ-значение" можно создать, выполнив следующую команду PowerShell:

```PowerShell
New-ItemProperty -Path HKLM:\SOFTWARE\Microsoft\ExchangeServer\v15\Setup -Name "DisablePreservation" -Value 1 -Type String
```

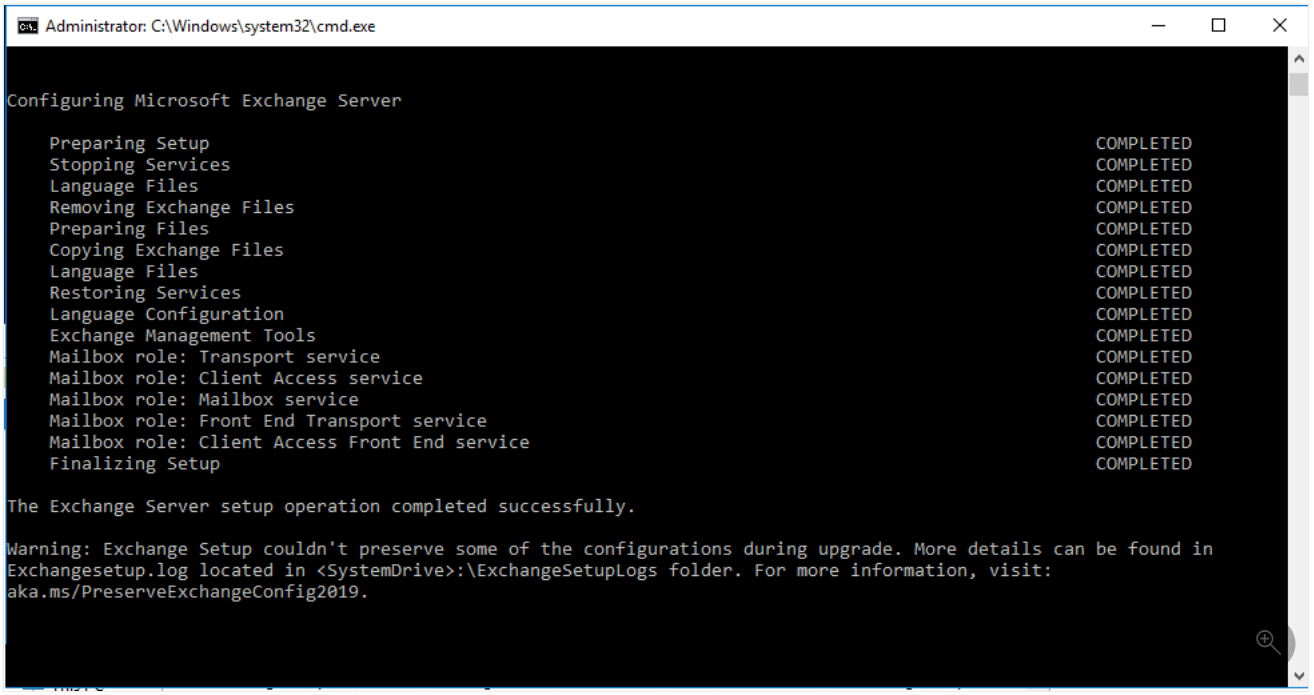
Если программа установки Exchange запускается после установки ключа regkey в `1`, программа установки не будет выполнять резервное копирование и восстановление пары "ключ—значение" ни в одной из конфигураций.

Развернуть таблицу

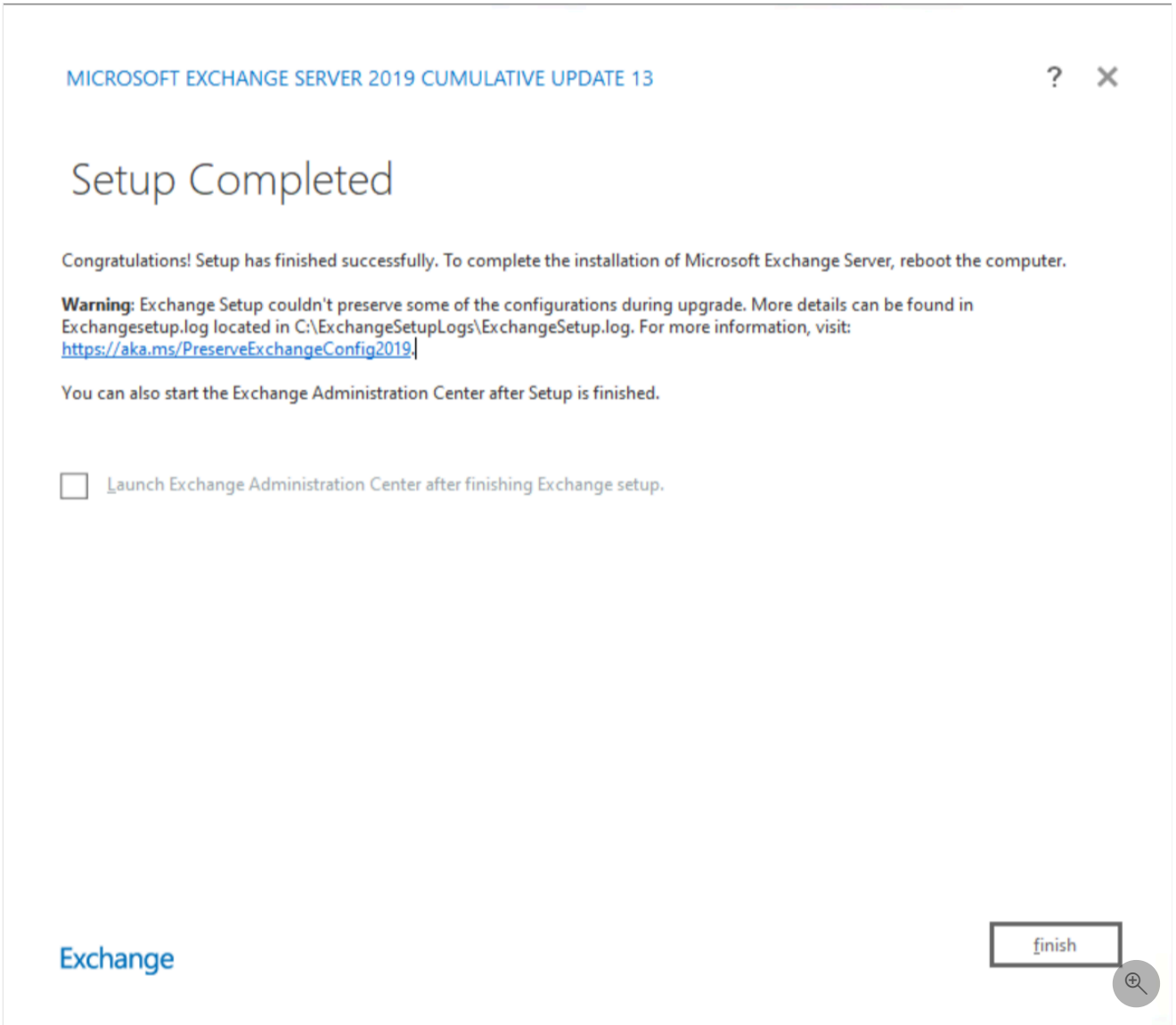
Раздел реестра	Значение реестра	Поведение при настройке Exchange
DisablePreservation (Type: `REG_SZ`)	1	Все пары значений ключей в файлах конфигурации сбрасываются, и резервная копия конфигурации preupgrade не сохраняется (это поведение эквивалентно предыдущим обновлениям cu).
DisablePreservation (Type: `REG_SZ`)	NULL	Программа установки создает резервную копию конфигураций предварительной версии и сохраняет определенную пару "ключ— значение" в конфигурациях preupgrade в новых конфигурациях.
DisablePreservation (Type: `REG_SZ`)	Любое другое значение	Программа установки создает резервную копию конфигураций предварительной версии и сохраняет определенную пару "ключ— значение" в конфигурациях preupgrade в новых конфигурациях.

Если программа установки не может восстановить все параметры до предыдущего состояния, отобразится предупреждение.

Автоматический режим



Режим участников



В качестве следующего шага администраторы могут проанализировать файл журнала установки, чтобы узнать, какие параметры не удалось сохранить. В файле журнала может присутствовать одна или несколько записей, указывающих, какие параметры не удалось сохранить:

1. При чтении файла конфигурации возникло исключение: `<configFileName>`. Пропуск сохранения.
2. Исключение, обнаруженное при сохранении `<Preservation cmdlet name>` изменений в: `<configFileName>`.
3. При проверке схемы файла конфигурации возникло исключение: `<configFileName>`. Пропуск сохранения.
4. `<Preservation cmdlet name>` сбой для: `<configFileName>`

Администраторы могут вручную скопировать любые файлы конфигураций из расположения резервной копии в требуемое расположение, перезаписав файлы, созданные программой установки. Это также восстанавливает эти файлы до состояния, предшествующего установке.

Сообщение об ошибке при обновлении накопительных Обновления в Exchange

Статья • 18.01.2025

В этой статье описывается, как устранить ошибки при попытке установки накопительного обновления или обновления до нее с помощью установки Exchange Server.

Симптомы

Симптомом сбоя обновления накопительного обновления является сообщение об **ошибке AccessDenied** .

Причина

Сообщение об **ошибке AccessDenied** возникает, если встроенные администраторы не имеют разрешений на **запись** для раздела реестра CustomSD при попытке записать или записать событие в журнал приложения.

После сбоя попытки накопительного обновления вы можете заметить следующие данные в журнале установки сразу после завершения задачи **Start-PreFileCopy** :

text

```
[12/05/2022 12:22:06.0909] [1] Ending processing Start-PreFileCopy
[12/05/2022 12:22:06.0914] [0] The log file path for the language pack
removal operation is set to 'C:\ExchangeSetupLogs'.
[12/05/2022 12:22:06.0924] [0] [WARNING] Exception has been thrown by the
target of an invocation.
[12/05/2022 12:22:06.0939] [0] [WARNING] Cannot open log for source
'MSExchangeSetup'. You may not have write access.
[12/05/2022 12:22:06.0939] [0] [WARNING] Access is denied
[12/05/2022 12:22:06.0939] [0] CurrentResult
SetupLauncherHelper.loadassembly:444: 1
[12/05/2022 12:22:06.0939] [0] The Exchange Server setup operation didn't
complete.  More details can be found in ExchangeSetup.log located in the
<SystemDrive>:\ExchangeSetupLogs folder.
[12/05/2022 12:22:06.0939] [0] CurrentResult main.run:235: 1
[12/05/2022 12:22:06.0939] [0] CurrentResult setupbase.maincore:396: 1
[12/05/2022 12:22:06.0939] [0] End of Setup
```

```
[12/05/2022 12:22:06.0939] [0]
*****************************************
```

В рабочем сценарии после задачи **Start-PreFileCopy** в данных журнала установки отображаются следующие строки:

text

```
[04/21/2022 08:31:54.0092] [1] Ending processing Start-PreFileCopy
[04/21/2022 08:31:54.0100] [0] The log file path for the language pack
removal operation is set to 'C:\ExchangeSetupLogs'.
[04/21/2022 08:31:54.0106] [0] **************
[04/21/2022 08:31:54.0106] [0] Setup will run the task 'remove-
InstalledLanguages'
```

Перед удалением и переустановкой языков необходимо записать событие в журнал с идентификатором ID:**1000** с исходной программой установки Microsoft Exchange.

text

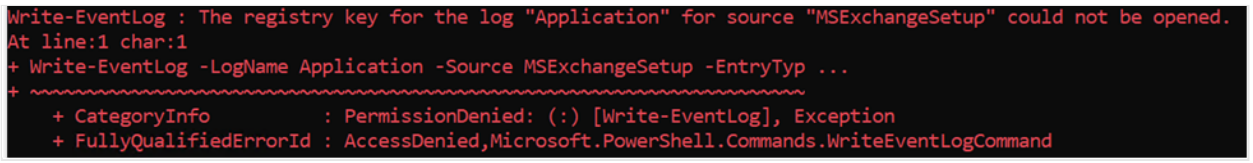
```
Log Name:      Application
Source:        MSExchangeSetup
Date:          12/5/2022 11:33:03 AM
Event ID:      1000
Task Category: Microsoft Exchange Setup
Level:         Information
Keywords:      Classic
User:          N/A
Description: Exchange Setup (build 15.1.2507.6:Languages) was started.
```

Следующая тестовая команда в Windows PowerShell пытается записать событие с идентификатором ID:**1000** в журнал приложения:

PowerShell

```
Write-EventLog -LogName Application -Source MSExchangeSetup -EntryType
Information -EventId 1000 -Message "This is a test message"
```

Если у вас возникла проблема, команда выводит сообщение об **ошибке AccessDenied** , как показано на следующем снимке экрана:



Этот результат указывает на проблему с доступом к журналу приложений для записи события с идентификатором:**1000**.

Если у вас возникла проблема, проверьте выходные данные `CustomSD` раздела реестра, выполнив следующую команду в Windows PowerShell:

PowerShell

```
Get-ItemProperty
"Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog\App
lication"
```

Выходные данные этой команды:

PowerShell

```
PrimaryModule       : Application
DisplayNameFile     : C:\Windows\system32\wevtapi.dll
DisplayNameID       : 256
File                : C:\Windows\system32\winevt\Logs\Application.evtx
MaxSize             : 209715200
Retention           : 0
RestrictGuestAccess : 1
AutoBackupLogFiles  : 0
CustomSD            : O:BAG:SYD:(A;;0xf0005;;;SY)(**A;;0x5;;;BA**)
(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;S-1-5-21-3081388108-1913582122-755921781-
506353)
PSPath              :
Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControl
Set\Services\Eventlog\Application
PSParentPath        :
Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\Sy
stem\CurrentControlSet\Services\Eventlog
PSChildName         : Application
PSProvider          : Microsoft.PowerShell.Core\Registry
```

Существует три отдельных права, которые относятся к журналам событий:

- **Чтение**. Соответствует биту **1** в поле **Права доступа** строки ACE.
- **Запись**: соответствует биту **2** в поле **Права доступа** строки ACE.
- **Очистить**. Соответствует биту **4** в поле **Права доступа** строки ACE.

Если мы попытаемся прочитать поле прав доступа строки `(A;;0x5;;;BA)` ACE , эти права доступа преобразуются в:

- O. Разрешить
- BA: встроенные администраторы
- 0x5: чтение и очистка

Эти результаты показывают, что запись событий в журнал приложений запрещена, что является причиной сообщения **AccessDenied** .

Решение

Чтобы устранить проблему, вызванную сообщением об **ошибке AccessDenied** , сделайте следующее:

1. Обновите права доступа с `(A;;0x5;;;BA)` на `(A;;0x7;;;BA)` в следующих расположениях:

   - `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\System`
   - `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Application`

   При обновлении права доступа предоставляется необходимое разрешение **на запись** .

2. Перезапустите процесс обновления.

Таблица поддержки Exchange Server

Статья • 11.02.2025

Матрица поддержки Microsoft Exchange Server предоставляет администратору Exchange центральный источник сведений о поддерживаемых конфигурациях и версиях Exchange Server.

Поддерживаемые версии и сборки

В следующей таблице перечислены поддерживаемые версии и сборки Exchange Server.

Развернуть таблицу

Версия	Сборки
Exchange Server 2019	CU15 (2025H1) CU14 (2024H1)
Exchange Server 2016	CU23

> ⚠ **Предупреждение**
>
> 11 апреля 2023 года поддержка Exchange Server 2013г. закончилась.

Поддерживаемые операционные системы

В следующей таблице перечислены поддерживаемые операционные системы для Exchange Server и роль средств управления Exchange.

> ⊗ **Внимание!**
>
> Обновление ос сервера на месте между основными версиями (например, с Windows Server 2019 до Windows Server 2022) с установленными Exchange Server не поддерживается.

Развернуть таблицу

Версия	Операционные системы	Server Edition	Параметры установки
Exchange Server 2019	Windows Server 2025 г. Windows Server 2022 Windows Server 2019	Datacenter Стандартный	Возможности рабочего стола Server Core **(рекомендуется)**
Exchange Server 2016	Windows Server 2016 Windows Server 2012 R2 Windows Server 2012	Datacenter Стандартный	Возможности рабочего стола
Средства управления Exchange Server 2019	Windows Server 2025 г. Windows Server 2022 Windows Server 2019 Windows 11 Windows 10 (64-разрядная версия)	Datacenter Стандартный	Возможности рабочего стола
Средства управления Exchange Server 2016	Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows 10 (64-разрядная версия)	Datacenter Стандартный	Возможности рабочего стола

> ⚠ **Предупреждение**
>
> расширенная поддержка Windows Server 2012 и Windows Server 2012 R2 прекращена 10 октября 2023 г. Эти серверы больше не будут получать Безопасность Windows Обновления без ESU. Мы настоятельно рекомендуем выполнить миграцию на поддерживаемую версию как можно скорее!

Поддерживаемые среды Active Directory

В следующей таблице перечислены поддерживаемые среды Active Directory для Exchange Server.

⛶ **Развернуть таблицу**

Версия	Серверы Active Directory	Функциональные уровни леса
Exchange Server 2019	Windows Server 2025 г. Windows Server 2022 Windows Server 2019	Windows Server 2016 Windows Server 2012 R2

Версия	Серверы Active Directory	Функциональные уровни леса
	Windows Server 2016 Windows Server 2012 R2	
Exchange Server 2016	Windows Server 2022 Windows Server 2019 Windows Server 2016 Windows Server 2012 R2 Windows Server 2012	Windows Server 2016 Windows Server 2012 R2 Windows Server 2012

> **Примечание**
>
> Поддержка серверов Active Directory Windows Server 2025 года появилась с Exchange Server 2019 CU14 (2024H1).
> Поддержка серверов Active Directory Windows Server 2022 года появилась в Exchange Server 2019 CU12 (2022H1) и Exchange Server 2016 CU23 (2022H1).
>
> Сервер Active Directory относится как к записываемым серверам глобального каталога (GC), так и к записываемым контроллерам домена (DC). Только для чтения GCs и контроллеры домена только для чтения не поддерживаются.

Поддерживаемые браузеры для Outlook в Интернете

В следующей таблице перечислены поддерживаемые веб-браузеры для использования с Outlook в Интернете (OWA) и Exchange Администратор Center (EAC) в Exchange Server.

Развернуть таблицу

Версия	Браузеры	Поддержка S/MIME
Exchange Server 2019 OWA/ EAC	Microsoft Chromium Edge Microsoft Chromium Edge (режим IE) Microsoft Edge Текущий выпуск Firefox Текущая версия Chrome Текущая версия Safari	Да Да Да Нет Да Нет
Exchange Server 2019 OWA Light	Microsoft Edge Текущая версия Safari	S/MIME недоступен в светлом режиме

Версия	Браузеры	Поддержка S/MIME
Exchange Server 2016 OWA/ EAC	Microsoft Chromium Edge Microsoft Chromium Edge (режим IE) Microsoft Edge Текущий выпуск Firefox Текущая версия Chrome Текущая версия Safari	Нет Да Нет Нет Нет Нет
Exchange Server 2016 OWA Light	Microsoft Edge Текущий выпуск Firefox Текущая версия Chrome Текущая версия Safari	S/MIME недоступен в светлом режиме

Примечание

Текущий выпуск Firefox/Chrome относится к последней или непосредственно предыдущей версии.

Поддерживаемые клиенты Email

В следующей таблице перечислены поддерживаемые почтовые клиенты Майкрософт для Exchange Server.

Развернуть таблицу

Версия	Клиенты
Exchange Server 2019	Приложения Microsoft 365 для предприятий Outlook 2024 Outlook 2021 Outlook 2019 Outlook 2016 Outlook для Mac (Microsoft 365, 2019) Outlook для iOS Outlook для Android
Exchange Server 2016	Приложения Microsoft 365 для предприятий Outlook 2024 Outlook 2021 Outlook 2019 Outlook 2016 Outlook для Mac (Microsoft 365, 2019)

Версия	Клиенты
	Outlook для iOS Outlook для Android

Дополнительные требования и сведения

Exchange Server также предъявляет требования к поддержке для некоторых предварительных требований, а именно платформа .NET Framework и Windows PowerShell.

.NET Framework

Выпуски платформа .NET Framework, которые не перечислены в приведенной ниже таблице, не поддерживаются ни в одном поддерживаемом выпуске Exchange Server. Эти выпуски включают в себя незначительные выпуски и выпуски на уровне исправлений платформа .NET Framework.

Развернуть таблицу

Версия	Windows	.NET Framework
Exchange Server 2019 CU15 (2025H1) Exchange Server 2019 CU14 (2024H1)	Windows Server 2025 г. Windows Server 2022	платформа .NET Framework 4.8.1 **(рекомендуется)** **или** .NET Framework 4.8
Exchange Server 2019 CU15 (2025H1) Exchange Server 2019 CU14 (2024H1)	в Windows Server 2019;	.NET Framework 4.8
Exchange Server 2016 CU23	Любая поддерживаемая ОС	.NET Framework 4.8

Windows PowerShell

Exchange Server 2019 и Exchange Server 2016 поддерживают только версию PowerShell, включенную в Windows Server. Exchange Server не поддерживает использование надстроек Windows Management Framework (WMF) в любой версии Windows PowerShell или Windows. Если существуют другие установленные версии Windows PowerShell или PowerShell Core, поддерживающие параллельную работу, Exchange Server будет использовать только требуемую версию.

Дополнительные сведения см. в следующих ресурсах:

- требования к системе и предварительные требования Exchange Server 2019 г.
- Exchange Server 2016 требования к системе и предварительные требования
- Exchange Server 2013 требования к системе и предварительные требования
- Номера сборок и даты выпуска Exchange Server

Виртуализация Exchange Server

Статья • 04.04.2023

Вы можете развернуть Exchange Server 2016 и Exchange Server 2019 в виртуализированной среде. В этом разделе приводятся общие сведения о сценариях, поддерживаемых для развертывания Exchange на программном обеспечении для аппаратной виртуализации.

Следующие термины используются в этом разделе рассмотрена Exchange виртуализации:

- **Холодная загрузка**. При переводе системы из состояния выключения питания в чистый запуск операционной системы действие является *холодной загрузкой*. Ни одно государство не операционной системы в этом случае сохраняется.

- **Сохраненное состояние**. Если виртуальная машина отключена, гипервизоры обычно имеют возможность сохранить состояние виртуальной машины, поэтому при включении компьютера она возвращается в *это сохраненное состояние* , а не при запуске при холодной загрузке.

- **Плановая миграция**. Когда системный администратор инициирует перемещение виртуальной машины с одного узла низкоуровневой оболочки на другой, действие представляет собой *плановую миграцию*. Действием может быть одна миграция или системный администратор может настроить автоматизацию для перемещения виртуальной машины по времени. Запланированная миграция также может быть результатом какого-либо другого события, которое происходит в системе, кроме сбоя оборудования или программного обеспечения.

  Ключевой момент запланированной миграции заключается в том, что виртуальная машина Exchange работает в обычном режиме и по какой-то причине ее необходимо переместить. Это перемещение можно выполнить с помощью технологии (например, Динамическая миграция или vMotion). Однако если виртуальная машина Exchange или узел низкоуровневой оболочки, где расположена виртуальная машина, испытывает какое-то состояние сбоя, результат не характеризуется как плановая миграция.

Требования к аппаратной виртуализации

Корпорация Майкрософт поддерживает Exchange 2016 и Exchange 2019 в рабочей среде в программном обеспечении для аппаратной виртуализации только при выполнении всех следующих условий:

- Запущено программное обеспечение виртуализации оборудования:
  - Все версии Windows Server с технологией Hyper-V или Microsoft Hyper-V Server
  - Любой сторонний гипервизор, прошедший проверку согласно программе проверки технологий виртуализации для Windows Server.

    > **Примечание**
    >
    > Развертывание Exchange 2016 или Exchange 2019 на поставщиках "инфраструктура как услуга" (IaaS) поддерживается при соблюдении всех требований к поддержке. Если поставщики предоставляют виртуальные машины, эти условия включают в себя полную поддержку гипервизора, используемого для виртуальных машин Exchange, и соответствие инфраструктуры, используемой Exchange, требованиям к производительности, которые были установлены во время определения размера фермы. Развертывание на виртуальных машинах Microsoft Azure поддерживается, если все тома хранилища, используемые для баз данных Exchange и журналов транзакций баз данных (в том числе баз данных транспорта), настроены для хранилища Azure класса Premium.

- Гостевая виртуальная машина Exchange имеет следующие условия:
  - Он работает под управлением Exchange 2016 или Exchange 2019.
  - Он развертывается в поддерживаемой версии Windows Server для Exchange.

Для развертываний Exchange 2016 или Exchange 2019:

- Все роли сервера Exchange поддерживаются в виртуальной машине.
- Виртуальные машины сервера Exchange Server (в том числе виртуальные машины Exchange, входящие в группу обеспечения доступности баз данных) можно сочетать с отказоустойчивой кластеризацией и технологией миграции, если виртуальные машины настроены так, чтобы не сохранять и не восстанавливать состояние на диске при перемещении или переводе в

автономный режим. Все действия на уровне гипервизора, направленные на обеспечение отказоустойчивости, должны приводить к "холодной" загрузке при активации виртуальной машины на целевом узле. Любая плановая миграция должна приводить к завершению работы и "холодной" загрузке или онлайн-миграции с помощью технологий наподобие динамической миграции Hyper-V. Миграция виртуальных машин с использованием гипервизора реализуется поставщиком гипервизора, поэтому следует убедиться, что поставщик проверяет и поддерживает миграцию виртуальных машин Exchange. Корпорация Майкрософт поддерживает динамическую миграцию Hyper-V для этих виртуальных машин.

- На физическом хост-компьютере можно развертывать только программы для управления (например, антивирусные программы, программы для резервного копирования или программы для управления виртуальными машинами). Никакие другие серверные приложения (например, Exchange, SQL Server, Active Directory или SAP) не следует устанавливать на хост-компьютере. Необходимо выделить хост-компьютер для запуска гостевых виртуальных машин.

- Некоторые низкоуровневые оболочки поддерживают функции получения снимков виртуальных машин. В снимке виртуальной машины сохраняется рабочее состояние виртуальной машины. Эта функция позволяет сделать несколько снимков виртуальной машины, а затем возвращаться к любому из предыдущих ее состояний, применяя к ней снимок. Однако снимки виртуальных машин могут быть несовместимы с некоторыми приложениями, поэтому их использование может приводить к неожиданным последствиям в случае серверных приложений, поддерживающих данные о состоянии, таких как Exchange. Как следствие, создание снимков ведомой виртуальной машины Exchange не поддерживается.

- Многие продукты для виртуализации оборудования позволяют указывать количество виртуальных процессоров, которое должно быть выделено каждой из гостевых виртуальных машин. Виртуальные процессоры, расположенные в гостевой виртуальной машине, используют фиксированное число физических ядер в физической системе. Exchange поддерживает отношение числа виртуальных процессоров к числу физических ядер, не превышающее 2:1, хотя рекомендуется отношение 1:1. Например, двухпроцессорная система с четырехъядерными процессорами содержит 8 физических ядер в обслуживающей системе. В системе с такой конфигурацией не следует выделять на все гостевые виртуальные машины более 16 виртуальных процессоров.

- При вычислении общего количества виртуальных процессоров, необходимых для хост-компьютера, также необходимо учитывать требования к операциям ввода-вывода и операционной системе. В большинстве случаев эквивалентное количество виртуальных процессоров, требуемое в несущей операционной системе для системы, в которой находятся виртуальные машины Exchange, равно 2. При расчете общего отношения числа физических ядер к числу виртуальных процессоров это значение следует использовать в качестве базового числа виртуальных процессоров несущей операционной системы. Если при наблюдении за производительностью несущей операционной системы обнаруживается потребление ресурсов процессоров, превышающее ресурсы двух процессоров, следует соответствующим образом сократить количество виртуальных процессоров, назначенное гостевым машинам, и проверить, что общее соотношение виртуальных процессоров к физическим ядрам не превышает 2:1.

- Можно отключить прямую связь гостевых виртуальных машин с адаптерами шины (HBA) Fibre Channel или SCSI, установленными на хост-компьютере. В таком случае необходимо настроить адаптеры в операционной системе хост-компьютера и предоставить логические номера устройств (LUN) гостевым виртуальным машинам как виртуальному или сквозному диску.

- Единственный поддерживаемый способ отправки сообщений электронной почты во внешние домены из вычислительных ресурсов Azure — через ретранслятор SMTP (также называемый интеллектуальным узлом SMTP). Вычислительный ресурс Azure отправляет сообщение ретранслятору SMTP, а затем поставщик ретрансляции SMTP доставляет сообщение на внешний домен. защита Microsoft Exchange Online является одним из поставщиков ретранслятора SMTP, но есть и ряд сторонних поставщиков. Дополнительные сведения см. в статье Устранение неполадок с исходящим подключением по протоколу SMTP в Azure.

Требования к хранилищу хост-компьютера

Минимальные требования к пространству на диске для каждого хост-компьютера описаны в следующем списке:

- Хост-компьютеры в случае некоторых приложений виртуализации оборудования могут требовать дискового пространства для операционной системы и ее компонентов. Дополнительного места также должно быть достаточно для файла подкачки операционной системы, программного обеспечения управления и файлов дампа (для восстановления после сбоя).

- Некоторые низкоуровневые оболочки хранят на хост-компьютере файлы, уникальные для каждой гостевой виртуальной машины. Например, в среде Hyper-V для каждой ведомой машины создается и хранится временный файл памяти (с расширением BIN). Размер каждого BIN-файла равен объему памяти, выделенному ведомой машине. Кроме того, для каждой из ведомых машин на хост-компьютере могут создаваться и храниться другие файлы.

- Если на хост-компьютере работает Windows Server 2012 Hyper-V или Hyper-V 2012, и вы настраиваете отказоустойчивый кластер на основе узла, в котором будут размещаться серверы почтовых ящиков Exchange в DAG, рекомендуется следовать рекомендациям в статье KB2872325 .

Требования к хранилищу Exchange

Требования для ресурсов хранения, подключенных к виртуализированной Exchange сервера существуют следующие:

- Каждой из гостевых машин Exchange должно быть выделено достаточное место в хранилище на хост-компьютере под фиксированный диск с операционной системой гостевой машины, временными файлами памяти и соответствующими файлами виртуальной машины, которые находятся на ведущей машине. Кроме того, для каждой ведомой машины Exchange также необходимо выделить достаточное место для очередей сообщений, а также достаточное место для баз данных и файлов журналов на серверах почтовых ящиков.

- Память, используемая гостевой машиной Exchange для хранения данных Exchange (например, баз данных почтовых ящиков или транспортных очередей), может быть виртуальным хранилищем фиксированного размера (например, фиксированным виртуальным жестким диском VHD или VHDX в среде Hyper-V), динамическим виртуальным хранилищем (при использовании VHDX-файлов с Hyper-V), транзитным хранилищем SCSI или интернет-хранилищем SCSI (iSCSI). Транзитное хранилище — это хранилище, настроенное на уровне узла и выделенное для одной гостевой машины. Все хранилища, используемые гостевым компьютером Exchange для хранения данных Exchange, должны быть хранилищем на уровне блоков, так как Exchange не поддерживает использование томов хранилища, подключенного к сети (NAS), кроме как в сценарии SMB 3.0, описанном далее в этом разделе. Не поддерживается также устройство NAS, представленное для гостевой машины через гипервизор как хранилище уровня блоков.

- Фиксированные виртуальные жесткие диски можно хранить в файлах SMB 3.0 на основе хранилища на уровне блока, если ведомый компьютер работает под управлением Windows Server 2012 Hyper-V (или более поздней версии Hyper-V). Файловые ресурсы SMB 3.0 поддерживаются только для хранения фиксированных виртуальных жестких дисков. Такие файловые ресурсы не могут использоваться для непосредственного хранения данных Exchange. При использовании файловых ресурсов SMB 3.0 для хранения фиксированных виртуальных жестких дисков хранилище для поддержки файлового ресурса необходимо настроить для обеспечения высокой доступности, чтобы гарантировать максимальную доступность службы Exchange.

- Хранилище, используемое сервером Exchange, должно находиться на дисках, отличных от тех, на которых размещается операционная система ведомой виртуальной машины.

- Хранилище iSCSI можно настроить на использование инициатора iSCSI в ведомой виртуальной машине Exchange. Однако производительность в этой конфигурации будет менее высокой, если сетевой стек виртуальной машины ограничен по функциональности (например, не все виртуальные сетевые стеки поддерживают кадры крупного размера).

Требования и рекомендации относительно памяти Exchange

Некоторые гипервизоры могут позволить определенной гостевой машине усиленно использовать объем память (динамически регулировать его), учитывая нужный ей объем, а также потребности других гостевых машин, которыми управляют. Такая технология эффективна для рабочих нагрузок, при которых какому-либо процессу требуется больший объем памяти на короткий период времени (эта память затем может быть распределена для других процессов). Однако эта технология не подходит для рабочих нагрузок, в случае которых память используется на постоянной основе. Exchange (как и многие серверные приложения с оптимизацией производительности, которая включает кэширование данных в памяти) подвержен низкой производительности системы и неприемлемому взаимодействию с клиентом, если он не имеет полного контроля над памятью, выделенной для физической или виртуальной машины, на которой она работает. В результате возможности динамической памяти (усиленного использования памяти) для Exchange не поддерживаются.

Отказоустойчивый кластер на базе узлов и миграция для Exchange

Ниже приведены ответы на некоторые часто задаваемые вопросы о технологии отказоустойчивой кластеризации на основе узлов и миграции с помощью групп daG Exchange.

- **Корпорация Майкрософт поддерживает технологию третьих сторон миграции?**

  Корпорация Майкрософт не может делать заявления о поддержке для интеграции сторонних продуктов гипервизора с помощью этих технологий с Exchange, так как эти технологии не входят в программу проверки виртуализации сервера (SVVP). Программа проверки виртуализации серверов (SVVP) охватывает другие аспекты поддержки сторонних низкоуровневых оболочек корпорацией Майкрософт. Необходимо убедиться, что поставщика низкоуровневой оболочки поддерживает сочетание их миграции и кластеризации технологии с Exchange. Если поставщик низкоуровневой оболочки поддерживает свою технологию миграции с Exchange, корпорация Майкрософт поддерживает Exchange с этой технологией миграции.

- **Каким образом Майкрософт определить индивидуальный отказоустойчивый кластер?**

  Централизованной отказоустойчивой кластеризации называется любая технология, обеспечивающая автоматическое способности реагировать на отказы узла уровня соответствующие виртуальные машины и запустить на альтернативные серверы. Поддерживается использование этой технологии, поскольку, в сценарий сбоя, скоро виртуальной машины с узла на альтернативном начальной холодной загрузки. Эта технология помогает гарантировать, что виртуальная машина не запускается из сохраненного состояния, которое сохраняется на диске, поскольку она будет устаревшей относительно остальных участников группы обеспечения доступности баз данных.

- **Что такое поддержка миграции Microsoft?**

  Технология миграции называется любая технология, которая позволяет перемещении виртуальной машины с одного главного компьютера на другой компьютер. Этот шаг также может являться автоматизированным перемещением, которое выполняется при балансировке нагрузки на ресурсы, но он не связан со сбоями в системе. Миграции поддерживаются, если

виртуальные машины не запускаются из сохраненного состояния, которое сохраняется на диске. Это означает, что технология, которая перемещает виртуальной машины путем передачи государству и памяти виртуальной машины через сеть без простоя поддерживается Exchange. Поставщик сторонней низкоуровневой оболочки должен обеспечить поддержку технологии миграции, а корпорация Майкрософт поддержит использование Exchange в этой конфигурации.

Планирование интеграции Exchange 2016 с SharePoint и Skype для бизнеса

Статья • 04.04.2023

Благодаря интеграции Exchange 2016 с SharePoint Server 2016 и Skype для бизнеса вы можете использовать службы, которые позволяют сохранять и архивировать почту, документы и другой контент, а затем быстро искать их. Вместе эти корпоративные приложения позволяют использовать ряд сценариев, например, eDiscovery и сценарии совместной работы с использованием почтовых ящиков сайтов, благодаря чему ваша организация может сохранять важные данные. В наши дни в большинстве организаций критически важна возможность архивировать почту и документы, а потом при необходимости находить их, чтобы обеспечить соответствие требованиям и нормативным актам. С помощью Exchange 2016 с SharePoint 2016 и Skype для бизнеса вы можете выполнять указанные ниже действия.

- Архивировать почтовые ящики Exchange.
- Архивировать контент Skype для бизнеса.
- Сохранять документы и веб-сайты SharePoint Server 2016.
- Выполнять поиск в хранилищах с помощью eDiscovery.
- Легко выполнять проверку подлинности на серверах.

Центр обнаружения электронных данных, появившийся в SharePoint 2013, позволяет идентифицировать и сохранять контент, формировать коллекции контента, а также обрабатывать и анализировать его. В среде Exchange с помощью функции eDiscovery вы можете архивировать контент, обнаруженный в SharePoint Server 2016, Skype для бизнеса и Exchange. С помощью Центр обнаружения электронных данных вы можете создавать сайты дел eDiscovery, которые используются для упорядочения удержаний на месте, запросов и экспортированных данных для определенных дел.

Exchange 2016, SharePoint Server 2016 и Skype для бизнеса Server использовать стандартный протокол Open Authorization (OAuth) для проверки подлинности между серверами, чтобы обеспечить описанные здесь функции между продуктами. Использование одного и того же протокола позволяет этим приложениям легко и безопасно проходить проверку подлинности друг для друга. Метод авторизации

поддерживает проверку подлинности в качестве приложения с помощью связанной учетной записи и олицетворения пользователя, когда запрос на доступ выполняется в контексте пользователя. Дополнительные сведения об OAuth см. далее в этой статье в разделе Проверка подлинности между серверами с помощью OAuth .

> ⓘ **Примечание**
>
> Если на предприятии используется Lync Server 2013, вы все равно можете в полной мере применять функции, описанные в этой статье.

Архивирование контента Skype для бизнеса в Exchange 2016

С помощью Exchange 2016 и Lync Server 2013, развернутых в организации, вы можете настроить Skype для бизнеса для архивации мгновенных сообщений и содержимого онлайн-собраний, включая общие презентации или документы в почтовом ящике Exchange 2016 пользователя. Архивация Skype для бизнеса данных в Exchange 2016 позволяет применять политики хранения к данным. Архивное Skype для бизнеса содержимое также покрывается при любом поиске eDiscovery. Дополнительные сведения о Skype для бизнеса архивации и ее развертывании см. в следующих разделах:

- Планирование архивации
- Развертывание архивации

Сохранение документов в SharePoint Server 2016

С помощью функции удержания на месте вы можете создать удержание по запросу, чтобы сохранить элементы, соответствующие указанным вами критериям.

Например, удержание для судебного разбирательства сохраняется до тех пор, пока не будут удалены все удаленные элементы, а также исходные версии измененных элементов . При необходимости можно указать длительность удержания, которая сохраняет элемент почтового ящика в течение именованного периода длительности. Длительность периода хранения рассчитывается с даты получения

сообщения или создания элемента почтового ящика. Дополнительные сведения см. в статье Создание или удаление In-Place удержания.

Дополнительные сведения о eDiscovery см. в указанных ниже статьях.

- Обнаружение электронных данных на месте в Exchange Server
- Удержание на месте и удержание для судебного разбирательства в Exchange Server
- Настройка обнаружения электронных данных в SharePoint Server
- Новые возможности обнаружения электронных данных в SharePoint Server
- Настройка Exchange для центра обнаружения электронных данных SharePoint

Поиск в приложениях с использованием eDiscovery

SharePoint Server 2016 предоставляет Центр обнаружения электронных данных, который помогает находить и передавать соответствующее содержимое по мере необходимости в соответствии с нормативными требованиями. Обнаружение электронных данных — это процесс поиска, сохранения, анализа и создания содержимого в цифровом формате, необходимый для судебного разбирательства или расследования. Вы можете использовать обнаружение электронных данных в файлах Exchange 2016, SharePoint Server 2016 и Skype для бизнеса. Вы можете защитить содержимое на месте, которое вы идентифицировали с помощью запросов обнаружения электронных данных, а затем экспортировать результаты в автономный формат для передачи на юридическую проверку. In-Place удержание в обнаружении электронных данных позволяет:

- Защищать контент на месте и в режиме реального времени. При этом вы уменьшите затраты на хранение и не будете оказывать влияние на ежедневную работу своих пользователей.
- Создавать запросы на сбор актуального релевантного контента и статистики и быстро отвечать на вопросы.
- Экспортировать релевантный контент в автономном формате, позволяющем легко переносить данные.

Если ваша организация обязана соблюдать требования по обнаружению данных для юридических целей (связанные с политикой организации, обеспечением

соответствия требованиям или судебными процессами), то с помощью функции обнаружения электронных данных на месте в Exchange Server 2016 вы можете выполнять операции поиска для обнаружения релевантного контента в почтовых ящиках. Вы также можете использовать функцию обнаружения электронных данных на месте в гибридной среде Exchange для поиска в локальных и облачных почтовых ящиках с использованием одной и той же операции поиска.

При настройке проверки подлинности между exchange 2016 и SharePoint Server 2016 в локальных развертываниях администраторы и сотрудники по соответствию требованиям могут использовать Центр обнаружения электронных данных. Дополнительные сведения см. в статье Configure Exchange for SharePoint eDiscovery Center. Если вы используете гибридные развертывания, то см. дополнительные сведения в статье Using Oauth Authentication to Support eDiscovery in an Exchange Hybrid Deployment.

Вы можете идентифицировать и уменьшить набор данных, используя синтаксис ключевых слов, ограничения для свойств и уточнения. Взаимодействие с запросами сосредоточено на статистике по отдельным источникам и фрагментам запросов, чтобы помочь вам принимать решения о содержимом, в который вы ищете. Вы также можете просмотреть контент в SharePoint 2016 и Exchange 2016, чтобы удостовериться, что вы идентифицировали правильный набор результатов.

Проверка подлинности "сервер-сервер" с использованием OAuth

Протокол OAuth используется многими веб-сайтами и веб-службами для предоставления клиентам доступа к ресурсам без необходимости ввода имени пользователя и пароля. Сервер авторизации, которому доверяет владелец ресурса, предоставляет клиенту маркер доступа, который предоставляет доступ к определенному набору ресурсов в течение указанного периода. Exchange 2016 позволяет другим приложениям использовать OAuth для проверки подлинности в Exchange. Вам потребуется настроить приложения в Exchange в качестве партнерских приложений.

Для OAuth и приложений-партнеров Exchange 2016 используются два объекта конфигурации: AuthConfig и конфигурация приложений-партнеров.

- **AuthConfig**: программа установки Exchange 2016 создает AuthConfig для публикации метаданных проверки подлинности. Вам потребуется только управлять AuthConfig, чтобы подготовить новый сертификат, когда будет заканчиваться срок действия текущего сертификата. Когда это случится, вы

сможете обновить имеющийся сертификат и настроить новый сертификат в качестве следующего сертификата в AuthConfig, а также указать дату вступления сертификата в силу.

Программа установки Exchange 2016 создает самозаверяющий сертификат с понятным именем Microsoft Exchange Server Auth Certificate и выполняет репликацию сертификата на все серверы переднего плана в организации Exchange. Отпечаток сертификата указан в конфигурации авторизации для Exchange 2016 наряду с именем его службы, которое является известным GUID, представляющим локальную среду Exchange 2016. Exchange использует конфигурацию авторизации для публикации своего документа с метаданными проверки подлинности.

- **Партнерские приложения**. Вы включаете партнерские приложения путем создания конфигурации партнерского приложения для запроса маркеров доступа из Exchange. Exchange 2016 предоставляет `Configure-EnterprisePartnerApplication.ps1` скрипт, который позволяет быстро и легко создавать конфигурации партнерских приложений и минимизировать ошибки конфигурации.

  Когда Exchange 2016 принимает запрос на доступ от приложения-партнера через веб-службы Exchange (EWS), возникают указанные ниже события.

  - EWS анализирует `www-authenticate` заголовок https-запроса, содержащего маркер доступа, подписанный вызывающим сервером, с помощью закрытого ключа.
  - Модуль проверки подлинности проверяет маркер доступа, используя конфигурацию приложения-партнера.
  - Затем этот модуль дает доступ к ресурсам на основе разрешений RBAC, предоставленных приложению. Если маркер доступа предоставлен от лица пользователя, система проверяет разрешения RBAC, предоставленные пользователю.

    Например, если пользователь выполняет поиск по обнаружению электронных данных с помощью Центра обнаружения электронных данных в SharePoint 2016, Exchange проверяет, является ли пользователь членом группы ролей Управление обнаружением или назначена роль поиска почтовых ящиков, а поисковые почтовые ящики находятся в область назначения роли RBAC. Дополнительные сведения см. в статье Permissions.

Чтобы можно было выпускать маркеры в локальных развертываниях для Exchange 2016, SharePoint Server 2016 и Skype для бизнеса Server 2015, не требуется сервер авторизации. Каждое приложение выпускает самозаверяющие маркеры для доступа к ресурсам, предоставляемым другими приложениями. Приложение, предоставляющее доступ к ресурсам, например Exchange 2016, доверяет самозаверяющим маркерам, которые предоставлены вызывающим приложением. Доверие устанавливается путем создания конфигурации *партнерского приложения* для вызывающего приложения, которая включает в себя ApplicationID, сертификат и AuthMetadataUrl вызывающего приложения. Exchange 2016, SharePoint 2016 и Skype для бизнеса публикуют свой документ с метаданными проверки подлинности по известному URL-адресу.

URL-адреса метаданных проверки подлинности

Сервер	AuthMetadataUrl
Exchange 2016	`https://<serverfqdn>/autodiscover/metadata/json/1`
SharePoint Server 2016	`https://<serverfqdn>/_layouts/15/metadata/json/1`
Skype для бизнеса	`https://<serverfqdn>/metadata/json/1`

В гибридных развертываниях вам необходимо настроить протокол авторизации OAuth между локальной организацией Exchange 2016 и организацией Exchange Online. По умолчанию гибридные развертывания продолжают использовать процесс доверия федерации.

Некоторые функции Exchange 2016 полностью доступны только в вашей организации с использованием нового протокола OAuth. Например, прежде чем использовать In-Place eDiscovery для поиска локальных и облачных почтовых ящиков в гибридной организации Exchange, необходимо настроить проверку подлинности OAuth между локальной службой Exchange и Exchange Online организациями. Мастер гибридной конфигурации не управляет подключением для авторизации OAuth. Дополнительные сведения см. в разделе Configure OAuth Authentication Between Exchange and Exchange Online Organizations.

В сетевых развертываниях Exchange Online, SharePoint Online и Skype для бизнеса Online необходимо настроить для современного подключения проверки подлинности. Современная проверка подлинности обеспечивает вход на основе библиотеки проверки подлинности Active Directory (ADAL) в клиенты Office 2013 для Windows. Клиентские приложения Office 2013 входят в службу Microsoft 365 или Office 365, чтобы получить доступ к Exchange Online, SharePoint Online и Skype для бизнеса Online. Мы рекомендуем включить Exchange Online для современной

проверки подлинности при включении современной проверки подлинности для Skype для бизнеса. Современная проверка подлинности включена по умолчанию в SharePoint Online. Дополнительные сведения см. в статье Включение или отключение современной проверки подлинности для Outlook в Exchange Online.

Ниже указаны состояния современной проверки подлинности для каждой службы.

- Skype для бизнеса Online: по умолчанию ОТКЛЮЧЕНА.
- Skype для бизнеса Online: по умолчанию ОТКЛЮЧЕНА.
- SharePoint Online: по умолчанию ВКЛЮЧЕНА.

> ⓘ **Важно!**
>
> Серверный сертификат проверки подлинности, используемый по умолчанию и созданный Exchange 2016, действует в течение 5 лет. Вы должны проверить, что в конфигурацию авторизации включен текущий сертификат.

Управление почтовыми ящиками сайта SharePoint

Во многих организациях информация хранится в двух разных хранилищах: электронная почта в Exchange и документы в SharePoint. Существует два разных интерфейса для доступа к этим хранилищам. Это создает несвязанный пользовательский интерфейс, который препятствует эффективной совместной работе. Почтовые ящики сайтов в SharePoint позволяют пользователям эффективно работать, объединяя электронную почту Exchange и документы SharePoint. Для пользователей почтовый ящик сайта служит центральным шкафом для подачи документов, предоставляя место для отправки электронных писем и документов проекта, к которым могут обращаться и редактировать только участники сайта. Почтовые ящики сайта отображаются в Outlook 2016, чтобы предоставить пользователям удобный доступ к электронной почте и документам для проектов, о которых они заботятся. С их помощью пользователи могут получить доступ к сообщениям электронной почты и документам для важных проектов.

В почтовом ящике сайта содержимое хранится там, где ему принадлежит. Электронная почта хранится в Exchange, поэтому отображается так же, как в почтовых ящиках пользователей. SharePoint хранит документы, что позволяет совместно авторизировать документы и управление версиями. Exchange синхронизирует достаточно метаданных из SharePoint для создания представления

документа в Outlook (то есть название документа, дата последнего изменения, автор последнего изменения и размер).

Вы можете подготавливать почтовые ящики сайтов и управлять ими из SharePoint Server 2016. Дополнительные сведения, в том числе о настройке почтовых ящиков сайта, см. в указанных ниже статьях.

- Site Mailboxes
- Настройка интеграции электронной почты для фермы SharePoint Server

Управление доступом к единому хранилищу контактов

Функция единого хранилища контактов (UCS) обеспечивает согласованное взаимодействие с контактами в продуктах Office. Эта функция позволяет пользователям хранить все контактные данные в почтовом ящике Exchange 2016, чтобы одни и те же контактные данные были доступны глобально в Skype для бизнеса, SharePoint, Exchange, Outlook и Outlook в Интернете. При развертывании сервераSkype для бизнеса и публикации топологии UCS включается для всех пользователей по умолчанию, и никаких дополнительных действий не требуется. Дополнительные сведения см. в разделе Настройка Skype для бизнеса Server для использования единого хранилища контактов.

Система автоматически переносит контакты на сервер Exchange 2016 в указанных ниже случаях.

- Пользователю назначена политика служб пользователей, свойство UcsAllowed которой имеет значение True (Истина).
- Для пользователя подготовлен почтовый ящик Exchange 2016, и пользователь хотя бы раз выполнял вход в этот почтовый ящик.
- Пользователь входит в систему с помощью клиента Skype для бизнеса с расширенными возможностями.

После установки SharePoint Server 2016 в среде с Exchange 2016 и настройки проверки подлинности между серверами пользователи могут инициировать миграцию существующих контактов с SharePoint 2016 или Skype для бизнеса Server 2015 на Exchange 2016. Дополнительные сведения см. в разделе Планирование и развертывание единого хранилища контактов.

Управление доступом к фотографиям пользователей с высоким разрешением

Функция работы с фотографиями пользователей позволяет хранить фотографии пользователей с высоким разрешением в Exchange 2016, доступ к которому можно получить с помощью клиентских приложений, в том числе Outlook, Outlook в Интернете, SharePoint 2016, Skype для бизнеса и почтовых клиентов для мобильных устройств. Фотографии с низким разрешением также хранятся в Active Directory. Командлет *Set-UserPhoto* сохраняет копию изображения с высоким разрешением в почтовом ящике Exchange пользователя, а копию фотографии с разрешением 64 x 64 пикселей хранится в виде изображения в атрибуте Active Directory thumbnailPhoto.

Как и в случае с UCS, фотографии пользователей позволяют вашей организации поддерживать согласованные фото профиля пользователей, которые могут использоваться клиентскими приложениями, не требуя от каждого приложения собственных фотографий пользователей и различных способов их добавления и управления ими. Пользователи могут управлять своими фотографиями с помощью Outlook в Интернете, SharePoint 2016 или Skype для бизнеса. Дополнительные сведения об управлении фотографиями на Outlook в Интернете см. в статье Изменение сведений о фотографии и учетной записи в Outlook в Интернете.

Exchange Server. Настройка проверки подлинности OAuth в SharePoint 2013 и Lync 2013

Статья • 04.04.2023

Exchange 2016 поддерживает партнерские приложения, такие как SharePoint Server 2016 и Skype для бизнеса Server 2015, используя конфигурацию OAuth со скриптом `Configure-EnterpriseApplication.ps1`. Вы можете автоматизировать эту задачу с помощью скрипта, упростив настройку проверки подлинности для партнерских приложений и уменьшив количество ошибок конфигурации. Этот скрипт делает следующее:

1. настраивает корпоративное партнерское приложение, которое самостоятельно выпускает маркеры OAuth для успешной проверки подлинности в Exchange;
2. назначает роли управления доступом на основе ролей (RBAC) партнерскому приложению для его авторизации на вызов определенных API веб-службы Exchange.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Партнерское приложение должно опубликовать для Exchange 2016 документ метаданных аутентификации, чтобы установить прямое отношение доверия с этим приложением и принимать запросы проверки подлинности.
- В примерах в этом разделе используется следующее расположение каталога по умолчанию: `C:\Program Files\Microsoft\Exchange Server\V15\Scripts`.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Партнерские приложения — настройка" в разделе Разрешения для общего доступа и совместной работы .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Настройка проверки подлинности OAuth с партнерским приложением

В этой процедуре `Configure-EnterpriseApplication.ps1` используется скрипт для настройки проверки подлинности OAuth в партнерских приложениях. Доступ к ресурсам зависит от разрешений, назначенных партнерскому приложению или пользователю, которого оно олицетворяет, с помощью RBAC. После настройки проверки подлинности OAuth из Exchange партнерское приложение сможет использовать ресурсы Exchange 2016.

1. В этом примере настраивается проверка подлинности OAuth для SharePoint 2016.

   Консоль

   ```
   Cd C:\Program Files\Microsoft\Exchange Server\V15\Scripts
   Configure-EnterprisePartnerApplication.ps1 -AuthMetaDataUrl
   https://sharepoint.contoso.com/_layouts/15/metadata/json/1 -
   ApplicationType SharePoint
   ```

2. В этом примере настраивается проверка подлинности OAuth для Skype для бизнеса или Lync Server 2013.

   Консоль

   ```
   Cd C:\Program Files\Microsoft\Exchange Server\V15\Scripts
   Configure-EnterprisePartnerApplication.ps1 -AuthMetaDataUrl
   https://lync.contoso.com/metadata/json/1 -ApplicationType Lync
   ```

Если среде Exchange 2016 также необходим доступ к ресурсам, предлагаемым партнерским приложением, следует настроить проверку подлинности OAuth в партнерском приложении.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно настроили корпоративное партнерское приложение на проверку подлинности в Exchange 2016, выполните командлет Get-PartnerApplication в командной консоли Exchange для получения конфигурации. Вы также можете выполнить командлет Test-OAuthConnectivity, чтобы проверить соединение OAuth с партнерским приложением для пользователя.

Гибридные и локальные развертывания

- В гибридных развертываниях можно использовать проверку подлинности OAuth между локальной организацией Exchange 2016 и Exchange Online организацией. Дополнительные сведения см. в статье Using Oauth Authentication to Support eDiscovery in an Exchange Hybrid Deployment.

- В локальных развертываниях можно настроить проверку подлинности между exchange 2016 и SharePoint 2016, чтобы администраторы и сотрудники по соответствию требованиям могли выполнять поиск в Exchange 2016 с помощью Центра обнаружения электронных данных SharePoint 2016. Дополнительные сведения см. в статье Configure Exchange for SharePoint eDiscovery Center.

Обслуживание сертификата OAuth Exchange Server

Статья • 07.04.2023

Общие сведения

В этой документации описаны действия, необходимые для смены сертификата проверки подлинности Exchange Server без прерывания работы службы Exchange и до истечения срока действия текущего сертификата.

> **Совет**
>
> Можно также использовать скрипт MonitorExchangeAuthCertificate . Он выполняет необходимые действия по автоматической смене сертификата OAuth. Он также может помочь заменить сертификат OAuth, если срок его действия уже истек.

Конфигурация проверки подлинности и сертификат проверки подлинности используются сервером Microsoft Exchange для включения проверки подлинности между серверами с использованием стандарта протокола Open Authorization (OAuth). Дополнительные сведения об этом см. в следующей статье Планирование интеграции Exchange с SharePoint и Skype для бизнеса

Сертификат проверки подлинности также используется несколькими Exchange Server функциями безопасности.

Во время установки первого сервера Exchange Server подпрограмма установки создает самозаверяющий сертификат с понятным именем `Microsoft Exchange Server Auth Certificate`, который затем добавляется в новую конфигурацию проверки подлинности. Этот сертификат автоматически реплицируется на все интерфейсные серверы в организации Exchange. Служба сертификатов Exchange выполняет репликацию, которая является частью `MSExchangeServiceHost` процесса. При добавлении дополнительных серверов в организацию Exchange servicelet выполняется репликация сертификата на все серверы Exchange, которые были добавлены в организацию.

Сертификат, настроенный как текущий сертификат проверки подлинности, можно запросить, выполнив следующий запрос PowerShell (должен быть выполнен в командной консоли Exchange):

PowerShell

```
(Get-AuthConfig).CurrentCertificateThumbprint | Get-ExchangeCertificate |
Format-List Subject, Thumbprint, NotAfter, NotBefore
```

Если вызов завершается ошибкой со следующим предупреждением, это означает, что текущий сертификат проверки подлинности отсутствует на сервере.

`A special Rpc error occurs on server <Servername>: The certificate with thumbprint <AuthCertificateThumbprint> was not found.`

Следуйте инструкциям, приведенным в разделе "Какие действия следует выполнить, если срок действия текущего сертификата уже истек или отсутствует", чтобы исправить.

Сертификат, настроенный как следующий сертификат проверки подлинности, можно запросить следующим образом:

PowerShell

```
(Get-AuthConfig).NextCertificateThumbprint | Get-ExchangeCertificate |
Format-List Subject, Thumbprint, NotAfter, NotBefore
```

Если вызов завершается ошибкой с тем же предупреждением, что и для текущего сертификата проверки подлинности, это означает, что следующий сертификат проверки подлинности не настроен или отсутствует на сервере.

Если срок действия текущего сертификата проверки подлинности скоро истечет, выполните инструкции, описанные в разделе Как сменить сертификат проверки подлинности Exchange Server.

Какие действия следует выполнить, если срок действия текущего сертификата уже истек или отсутствует?

В этом случае необходимо немедленно заменить старый сертификат проверки подлинности новым. Следуйте инструкциям, описанным в разделе о решениях следующей статьи поддержки: Не удается войти в Outlook в Интернете или EAC, если срок действия сертификата OAuth Exchange Server истек.

Смена сертификата проверки подлинности Exchange Server

Важно заменить активный сертификат проверки подлинности новым, прежде чем срок его действия истечет. Это обеспечивает плавный переход на новый сертификат без прерывания работы службы Exchange. Чтобы подготовить и подготовить новый сертификат проверки подлинности, выполните приведенные ниже действия.

> ⓘ **Важно!**
>
> Убедитесь, что у вас установлена последняя Exchange Server накопительного обновления (CU), так как она содержит исправления, влияющие на соответствующую функцию Exchange.

1. Создайте новый сертификат проверки подлинности, выполнив следующую команду:

```
PowerShell

$newAuthCertificate = New-ExchangeCertificate -KeySize 2048 -
PrivateKeyExportable $true -SubjectName "cn=Microsoft Exchange Server
Auth Certificate" -FriendlyName "Microsoft Exchange Server Auth
Certificate" -DomainName @()
```

2. Не перезаписывайте существующий SMTP-сертификат по умолчанию (введите "N" и нажмите клавишу ВВОД):

```
PowerShell

Confirm
Overwrite the existing default SMTP certificate?

Current certificate: '<DefaultSMTPCertificateThumbprint>' (expires
12/30/2027 2:39:08 PM)
Replace it with certificate: '<NewCertificateThumbprint>' (expires
1/5/2028 9:04:48 AM)
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [?] Help (default is
"Y"): N
```

3. Настройте сертификат проверки подлинности, чтобы он стал новым активным через 49 часов.

```
PowerShell
```

```
Set-AuthConfig -NewCertificateThumbprint $newAuthCertificate.Thumbprint
-NewCertificateEffectiveDate (Get-Date).AddHours(49)
```

> ⓘ **Примечание**
>
> В зависимости от размера организации Exchange для развертывания нового сертификата проверки подлинности на всех серверах Exchange может потребоваться некоторое время. Мы рекомендуем запланировать по крайней мере 48 часов, прежде чем только что созданный сертификат проверки подлинности станет активным.

За окончательный процесс публикации сертификата проверки подлинности отвечает сертификат Exchange AuthAdmin, который также является частью `MSExchangeServiceHost` этого процесса. Servicelet выполняется немедленно при перезапуске `MSExchangeServiceHost` службы. Затем он выполняется каждые 12 часов и, если обнаруживает, что `NewCertificateEffectiveDate` достигнут, он публикует новый сертификат проверки подлинности, чтобы сделать его новым активным.

Вы можете запросить последнюю среду выполнения servicelet AuthAdmin, выполнив следующие командлеты PowerShell:

PowerShell

```
[xml]$xml = Get-ExchangeDiagnosticInfo -Process
"Microsoft.Exchange.ServiceHost"
$xml.Diagnostics.Components.AnchorApplication.AnchorServiceComponents.CacheS
cheduler.lastRunTime
```

Каждый запуск служебного модуля AuthAdmin регистрируется в следующем каталоге: `<ExchangeInstallPath>\Logging\AuthAdminLogs`

При успешном завершении смены сертификата проверки подлинности с помощью служебного кода создается новая запись журнала событий:

PowerShell

```
Log Name:      Application
Source:        MSExchange AuthAdmin
Date:          12/29/2022 5:56:13 AM
Event ID:      2014
Task Category: General
Level:         Information
Keywords:      Classic
User:          N/A
```

```
Description:   The current signing certificate for Exchange has been updated
to certificate with thumbprint <NewExchangeCertificateThumbprint>.
```

> ⓘ **Примечание**
>
> Чтобы обеспечить запуск служебной программы AuthAdmin, необходимо включить AuthAdminReadSession, когда серверы Exchange Server установлены в дочернем домене, а системный почтовый ящик находится в корневом домене. В противном случае не удастся запустить служебнуюлет AuthAdmin.

PowerShell

```
Set-OrganizationConfig -EnableAuthAdminReadSession:$true
```

Вопросы и ответы

Вопрос: Требуется ли повторно запустить мастер гибридной конфигурации (HCW) после замены сертификата проверки подлинности?

Ответ: Да, мы настоятельно рекомендуем запустить мастер гибридной конфигурации (HCW) после замены активного сертификата проверки подлинности.

Вопрос: Что делать, если новый сертификат проверки подлинности отсутствует на сервере Exchange Server на другом сайте Active Directory (AD)?

Ответ: Вы можете экспортировать сертификат с помощью командлета Export-ExchangeCertificate и импортировать его через Import-ExchangeCertificate на сервере на другом сайте AD. Сертификат servicelet отвечает за репликацию на остальные серверы Exchange, расположенные на сайте AD.

Задачи после установки Exchange Server

Статья • 04.04.2023

Ознакомьтесь со следующими разделами, чтобы настроить новую организацию Exchange 2016 или Exchange 2016.

Статья	Описание
Введите ключ продукта Exchange	Узнайте, как лицензировать сервер Exchange Server.
Настройка потока обработки почты и клиентского доступа на серверах Exchange Server	Узнайте, как настроить поток обработки почты в Интернете и из нее, а также настроить Exchange для приема клиентских подключений из Интернета.
Проверка Exchange Server установок	Узнайте, как убедиться, что Exchange 2016 успешно установлен в вашей организации.
Установка средств управления Exchange	Узнайте, как установить командную консоль Exchange и панель элементов Exchange на клиентских рабочих станциях или других серверах, отличных от Exchange в вашей организации.
Настройка интеграции обмена мгновенными сообщениями с Outlook в Интернете в Exchange	Узнайте, как настроить интеграцию обмена мгновенными сообщениями между Skype для бизнеса Server и Outlook в Интернете (прежнее название — Outlook Web App).
Изменение расписания создания автономной адресной книги в Exchange	Узнайте, как изменить расписание создания автономной адресной книги (OAB) на определенных серверах Exchange или для всей организации.
Настройка проверки подлинности на основе сертификатов в Exchange 2016	Узнайте, как настроить CBA в Exchange 2016 с накопительным пакетом обновления 1 (CU1) или более поздней версии
Пограничные подписки	Узнайте, как настроить подписку EdgeSync между новым пограничным транспортным сервером в сети периметра и серверами почтовых ящиков Exchange на внутреннем сайте Active Directory.

Примечание.

Если вы включили агент сценариев в организации Exchange и храните настраиваемый файл

%ExchangeInstallPath%Bin\CmdletExtensionAgents\ScriptingAgentConfig.xml на всех серверах почтовых ящиков, необходимо скопировать этот файл на каждый новый сервер почтовых ящиков, развернутый в организации (этот файл не используется на пограничных транспортных серверах).

- Значением по умолчанию %ExchangeInstallationPath% является %ProgramFiles%\Microsoft\Exchange Server\V15, но фактическим значением является место установки Exchange на сервере.

- Имя файла на новом сервере Exchange Server по умолчанию — %ExchangeInstallPath%Bin\CmdletExtensionAgents\ScriptingAgentConfig.xml.sample. В рамках включения агента сценариев в организации необходимо переименовать этот файл, чтобы ScriptingAgentConfig.xml и настроить его или заменить существующим файлом ScriptingAgentConfig.xml.

Дополнительные сведения об агенте скриптов в Exchange 2013 (который по-прежнему относится к Exchange 2016 и 2019) см. в разделе Агент сценариев.

Введите ключ продукта Exchange Server

Статья • 04.04.2023

Ключ продукта сообщает Exchange Server 2016 или Exchange Server 2019 году, что вы приобрели стандартную или выпуск Enterprise лицензию. Если ключа продукта приобретен для лицензии Enterprise Edition, в дополнение к возможностям, доступным в рамках лицензии Standard Edition, вы сможете подключить более пяти баз данных на каждом сервере. Дополнительные сведения о лицензировании Exchange см. в статье Exchange Server выпусков и версий.

Если вы не введете ключ продукта, сервер будет автоматически лицензирован как пробный выпуск. Он будет работать так же, как сервер Exchange Standard Edition, и позволяет изучить Exchange перед покупкой или выполнить тесты в лабораторной среде. Единственное отличие состоит в том, что сервер Exchange, лицензированный как пробный выпуск, можно использовать не больше 180 дней. Если вы хотите продолжать использовать сервер в течение 180 дней, необходимо ввести ключ продукта, иначе Центр администрирования Exchange (EAC) начнет показывать напоминания о том, что вам нужно ввести ключ продукта для лицензирования сервера.

Примечание. Если вы хотите установить или активировать Office, ознакомьтесь со следующими сведениями:

- Установка Office
- Нужна помощь с ключом продукта Office?

Если вы хотите ввести ключ продукта в более старой версии Exchange, ознакомьтесь с разделом Ввод ключа продукта Exchange 2010.

Если вы хотите ввести ключ продукта на сервере Exchange 2016 или Exchange 2019, вы находитесь в нужном месте! Читайте дальше.

Что нужно знать перед началом работы

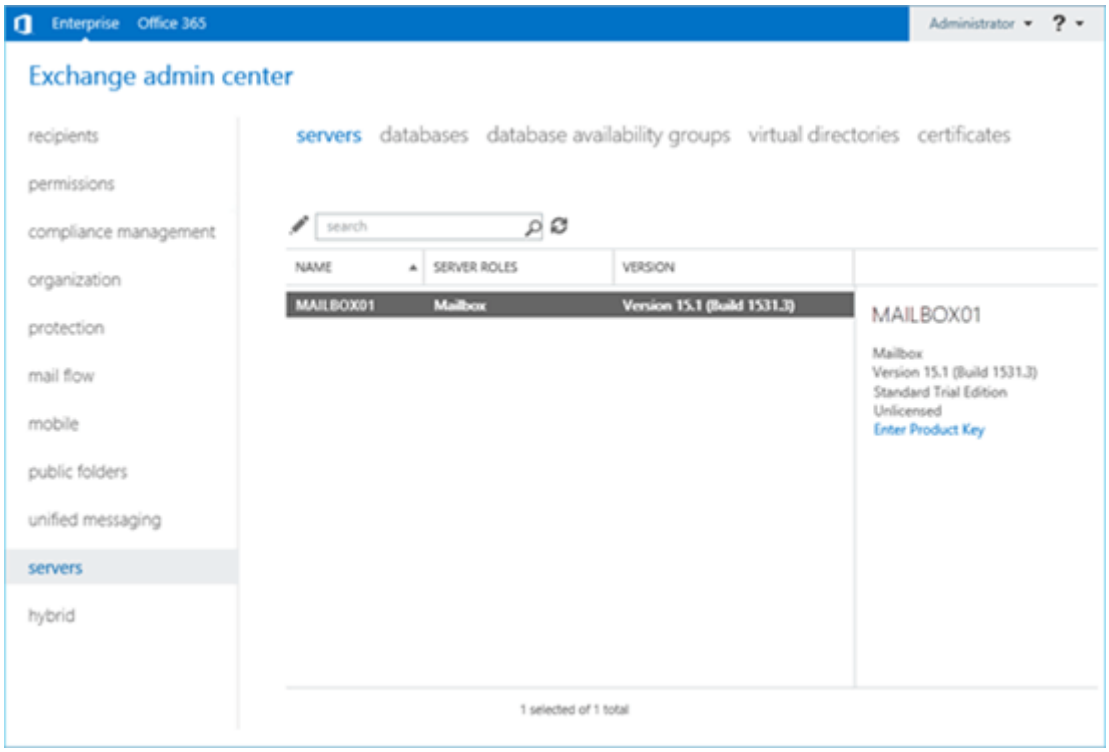
- Предполагаемое время для завершения каждой процедуры: менее 5 минут.
- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Ключ продукта" в разделе "Инфраструктура Exchange и разрешения PowerShell ".
- После лицензирования сервера почтовых ящиков Exchange необходимо перезапустить службу Microsoft Exchange Information Store на сервере после ввода ключа продукта.
- Вы можете перейти с лицензии Standard Edition на выпуск Enterprise лицензию. Вы не можете перейти с выпуск Enterprise лицензии на лицензию Standard Edition без переустановки Exchange.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

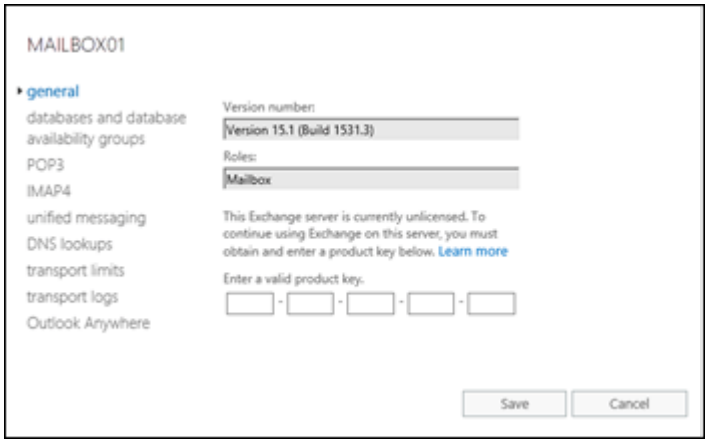
Ввод ключа продукта с помощью Центра администрирования Exchange

1. В EAC. Перейдите в раздел **Серверы**>, выберите сервер, на который требуется лицензия, а затем выполните одно из следующих действий.
   - Щелкните **изменить**.
   - В области сведений щелкните **Ввести ключ продукта**. Обратите внимание, что эта ссылка доступна только для нелицензированных серверов.

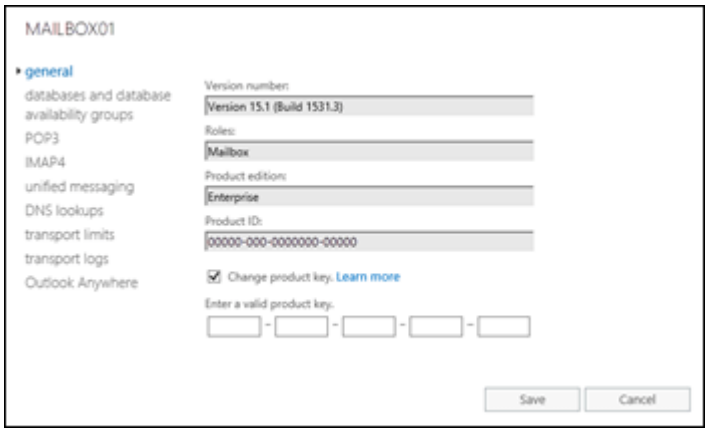


2. Откроется окно свойств сервера Exchange Server. На вкладке **Общие** выполните одно из следующих действий.

   - **Лицензирование нелицензированного сервера**. Введите ключ продукта в текстовых **полях Введите допустимый ключ продукта** .



   - **Изменение или обновление ключа продукта на лицензированном сервере**. Выберите **Изменить ключ продукта** и введите ключ продукта в текстовые поля **Введите допустимый ключ продукта** . Обратите внимание, что вы увидите **изменить ключ продукта** , только если сервер уже лицензирован.



По завершении нажмите кнопку **Сохранить**.

После лицензирования сервера почтовых ящиков выполните следующие действия, чтобы перезапустить службу Microsoft Exchange Information Store.

1. Откройте консоль "Службы Windows" на сервере Exchange Server. Например:

   - Выполните команду `services.msc` из диалогового окна **Запуск** , окна командной строки или командной консоли Exchange.
   - Откройте диспетчер сервера и щелкните **Сервис**>**службы**.

2. В списке служб щелкните правой кнопкой мыши **Microsoft Exchange Information Store** и выберите пункт **Перезапустить**.

Ввод ключа продукта с помощью командной консоли Exchange

Чтобы ввести ключ продукта в командной консоли Exchange, используйте следующий синтаксис:

PowerShell

```
Set-ExchangeServer <ServerName> -ProductKey <ProductKey>
```

Обратите внимание, что эта команда работает для лицензирования нелицензированного сервера или для обновления лицензированного сервера с лицензии Standard Edition до выпуск Enterprise лицензии.

В этом примере лицензирует сервер Exchange с именем Mailbox01.

PowerShell

```
Set-ExchangeServer Mailbox01 -ProductKey 12345-12345-12345-12345-12345
```

Подробные сведения о синтаксисе и параметрах см. в разделе Set-ExchangeServer.

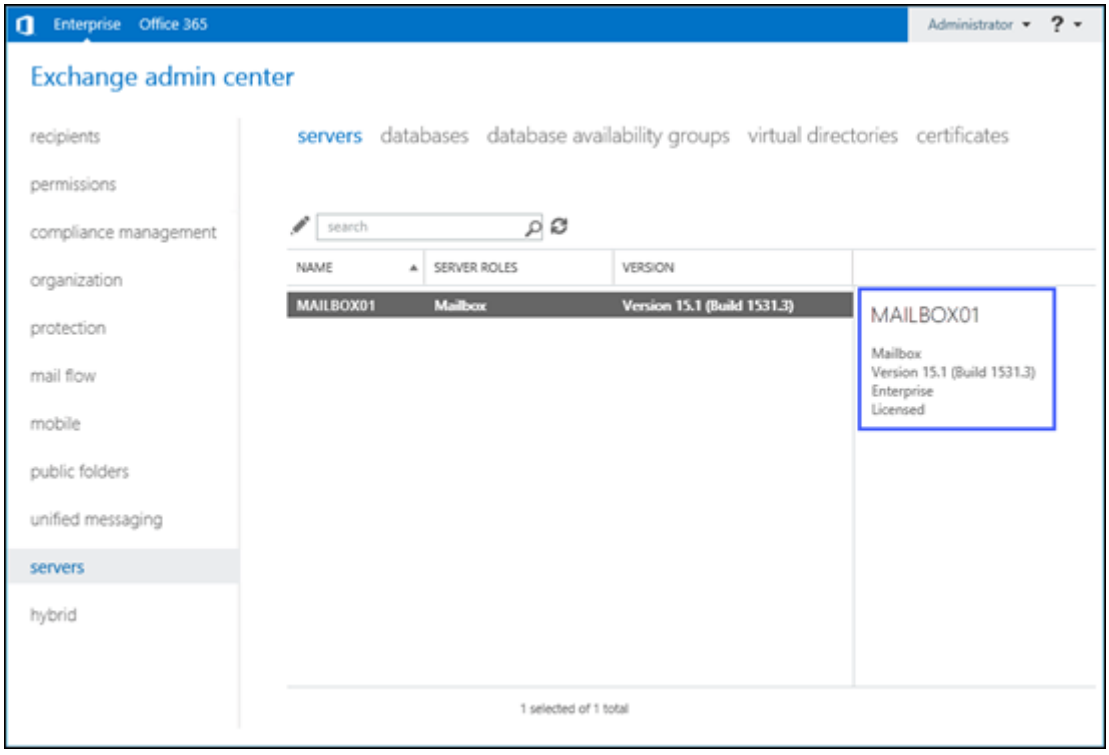
После лицензирования сервера почтовых ящиков выполните следующую команду в командной консоли Exchange, чтобы перезапустить службу Microsoft Exchange Information Store:

```
PowerShell

Restart-Service MSExchangeIS
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно лицензировали Exchange Server, выполните одно из следующих действий:

- В EAC перейдите в раздел **Серверы**> и выберите лицензированный сервер. В области сведений проверьте значение выпуска Exchange (**Стандартный** или **Корпоративный**) и наличие значения **Лицензировано** .



- В командной консоли Exchange *замените*< *serverName*> именем лицензированного сервера Exchange и выполните следующую команду, чтобы проверить значения свойств:

```
PowerShell

Get-ExchangeServer <ServerName> | Format-List Name,Edition,*Trial*
```

- В командной консоли Exchange выполните следующую команду, чтобы просмотреть состояние лицензирования всех серверов Exchange в организации:

```
PowerShell
```

```
Get-ExchangeServer | Format-Table -Auto Name,Edition,*Trial*
```

Настройка потока обработки почты и клиентского доступа на серверах Exchange Server

Статья • 04.04.2023

После установки Exchange Server 2016 или Exchange 2019 в организации необходимо настроить Exchange для потока обработки почты и клиентского доступа. Без этих дополнительных действий вы не сможете отправлять почту в Интернет, а внешние клиенты (например, Microsoft Outlook и устройства Exchange ActiveSync) не смогут подключиться к вашей организации Exchange.

Действия, описанные в этом разделе, предполагают базовой развертывание Exchange с одним сайтом Active Directory и пространством имен SMTP.

> ⓘ **Важно!**
>
> В этом разделе используются примеры значений, таких как Mailbox01, contoso.com, mail.contoso.com и 172.16.10.11. Замените их значениями имен серверов, полных доменных имен и IP-адресов вашей организации.

Дополнительные сведения о задачах управления, связанных с потоком обработки почты, клиентами и устройствами, см. в статьях Поток обработки почты и конвейер транспорта и Клиенты и мобильные устройства.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 50 минут.
- Вы можете получать предупреждения о сертификате при подключении к веб-сайту Центра администрирования Exchange, пока не настроите сертификат SSL на сервере почтовых ящиков. Как это сделать, будет показано далее в этом разделе.
- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Шаг 1. Создание соединителя отправки в Интернет

Перед отправкой почты в Интернет необходимо создать соединитель отправки на сервере почтовых ящиков. Инструкции см. в статье Создание соединителя отправки в Exchange Server отправки почты в Интернет.

Примечание

По умолчанию при установке Exchange создается соединитель получения с именем "Default Frontend <ServerName>_". Этот соединитель принимает анонимные подключения SMTP с внешних серверов. Вам не требуется проводить какую-либо дополнительную настройку, если это вас устраивает. Если вы хотите ограничить входящие подключения с внешних серверов, измените **внешний соединитель получения по умолчанию на <сервере почтовых ящиков>**. Дополнительные сведения см. **в разделе Соединители получения по умолчанию, созданные во время установки**.

Шаг 2. Добавление дополнительных обслуживаемых доменов

По умолчанию Exchange использует домен Active Directory, где для адресов электронной почты выполнялась настройка /PrepareAD. Если вы хотите, чтобы получатели получали и отправляли сообщения в другой домен и из другого домена, необходимо добавить домен в качестве принятого домена. Инструкции см. в разделах Создание принятых доменов и Настройка Exchange для приема почты для нескольких полномочных доменов.

Важно!

Чтобы получать электронную почту из Интернета для домена, вам потребуется запись ресурса MX в общедоступной dns для этого домена. Каждая запись MX должна разрешаться на сервере с выходом в Интернет, который получает электронную почту для вашей организации.

Шаг 3. Настройка политики электронных адресов по умолчанию

Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "политики Email адресов" в разделе разрешения Email адресной книги.

Если вы добавили обслуживаемый домен на предыдущем шаге и хотите, чтобы он добавился для каждого получателя в организации, необходимо обновить политику адресов электронной почты по умолчанию. Инструкции см. в разделах Изменение политик адресов электронной почты и Применение политик адресов электронной почты к получателям.

Примечание

Рекомендуется настроить имя участника-пользователя, которое совпадает с основным адресом электронной почты каждого пользователя. Если не указать имя участника-пользователя, соответствующее адресу электронной почты пользователя, пользователю потребуется вручную указать свой домен\имя пользователя или имя участника-пользователя в дополнение к адресу электронной почты. Если имя участника-пользователя совпадает с адресом электронной почты, Outlook в Интернете (прежнее название — Outlook в Интернете), ActiveSync и Outlook автоматически сопоставляют их адрес электронной почты с их имени участника-пользователя.

Шаг 4. Настройка внешних URL-адресов

Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи " *<Параметры виртуального каталога службы>* " в разделе Разрешения клиентов и мобильных устройств .

Прежде чем клиенты смогут подключаться к новому серверу из Интернета, необходимо настроить внешние домены (или URL-адреса) в виртуальных каталогах

в службах клиентского доступа (внешний интерфейс) на сервере почтовых ящиков, а затем в общедоступных записях DNS. Указанные ниже действия позволяют настроить один и тот же внешний домен для внешних URL-адресов каждого виртуального каталога. Если вам нужно настроить другие внешние домены для внешних URL-адресов одного или нескольких виртуальных каталогов, необходимо указать внешние URL-адреса вручную. Дополнительные сведения см. в разделе Параметры по умолчанию для виртуальных каталогов Exchange.

1. Откройте EAC и **перейдите в раздел Серверы Серверы**>, выберите сервер почтовых ящиков с выходом в Интернет, к которому будут подключаться клиенты, и нажмите кнопку **Изменить**.✏️

2. В открывшемся окне свойств сервера Exchange Server выберите вкладку **Мобильный Outlook** и настройте следующие параметры:

   Укажите имя внешнего узла. Введите доступное извне имя FQDN, с помощью которого внешние клиенты будут подключаться к своим почтовым ящикам (например, mail.contoso.com).

   Укажите имя внутреннего узла. Введите имя FQDN, доступное внутри организации (например, mail.contoso.com).

   По завершении нажмите кнопку **Сохранить**.

3. Перейдите в раздел **Серверы**>**Виртуальные каталоги** выберите **Настроить внешний домен доступа**🔧.

4. В открывшемся окне **Настроить домен внешнего доступа** настройте следующие параметры:

   a. **Выберите серверы почтовых ящиков для использования с внешним URL-адресом: щелкните**➕

   b. В открывшемся диалоговом окне **Выбор сервера** выберите сервер почтовых ящиков, который нужно настроить, и нажмите кнопку **Добавить**. После добавления всех серверов почтовых ящиков, которые требуется настроить, нажмите кнопку **ОК**.

   c. **Введите доменное имя, которое будет использоваться с внешними серверами почтовых ящиков**. Введите внешний домен, который вы хотите применить (например, mail.contoso.com). По завершении нажмите кнопку **Сохранить**.

Некоторые организации используют уникальное полное доменное имя Outlook в Интернете для защиты от будущих изменений в базовом FQDN сервера. Многие

организации используют owa.contoso.com для Outlook в Интернете полное доменное имя вместо mail.contoso.com. Если вы хотите настроить уникальное Outlook в Интернете полное доменное имя, выполните следующие действия. В этом контрольном списке предполагается, что вы настроили уникальное полное доменное имя Outlook в Интернете.

1. Вернитесь в раздел **Серверы**>**Виртуальные каталоги** выберите **owa (веб-сайт по умолчанию)** на сервере, который требуется настроить, и нажмите кнопку **Изменить**.

2. Откроется окно **owa (веб-сайт по умолчанию).** На вкладке **Общие** в поле **Внешний URL-адрес** введите следующие сведения:

   - `https://`
   - Уникальное Outlook в Интернете полное доменное имя, которое вы хотите использовать (например, owa.contoso.com), а затем добавьте /owa. Например, https://owa.contoso.com/owa.
   - `/owa`

   В этом примере конечным значением будет https://owa.contoso.com/owa

   По завершении нажмите кнопку **Сохранить**.

3. Вернитесь в раздел **Серверы**>**Виртуальные каталоги** выберите **ecp (веб-сайт по умолчанию)** на сервере, который требуется настроить, и щелкните

4. В открывшемся окне **ecp (веб-сайт по умолчанию)** введите URL-адрес с предыдущего этапа, добавив значение /ecp вместо /owa (например, https://owa.contoso.com/ecp). По завершении нажмите **Сохранить**.

После настройки внешнего URL-адреса в виртуальных каталогах служб клиентского доступа на сервере почтовых ящиков необходимо настроить общедоступные записи DNS для автообнаружения, Outlook в Интернете и потока обработки почты. Общедоступные записи DNS должны указывать на внешний IP-адрес или полное доменное имя сервера почтовых ящиков с выходом в Интернет и использовать доступные извне полные доменные имена, настроенные на сервере почтовых ящиков. Рекомендуемые записи DNS, которые следует создать для включения потока обработки почты и подключения к внешнему клиенту, описаны в следующей таблице:

Полное доменное имя	Тип записи DNS	Значение

Полное доменное имя	Тип записи DNS	Значение
Contoso.com	MX	Mail.contoso.com
Mail.contoso.com	A	172.16.10.11
Owa.contoso.com	CNAME	Mail.contoso.com
Autodiscover.contoso.com	CNAME	Mail.contoso.com

Как убедиться, что все получилось?

Чтобы убедиться, что вы успешно настроили внешние URL-адреса в виртуальных каталогах служб клиентского доступа на сервере почтовых ящиков, выполните указанные ниже действия.

1. В EAC перейдите в раздел **Серверы**>**Виртуальные каталоги**.
2. В поле **Выберите сервер** укажите сервер почтовых ящиков с выходом в Интернет.
3. Выберите виртуальный каталог, а затем в области сведений проверьте, содержит ли поле **Внешний URL-адрес** правильное полное доменное имя, как в приведенной ниже таблице.

Виртуальный каталог	Значение внешнего URL-адреса
Автообнаружение	Внешний URL-адрес не отображается
ECP	https://owa.contoso.com/ecp
EWS	https://mail.contoso.com/EWS/Exchange.asmx
Microsoft-Server-ActiveSync	https://mail.contoso.com/Microsoft-Server-ActiveSync
OAB	https://mail.contoso.com/OAB
OWA	https://owa.contoso.com/owa
PowerShell	http://mail.contoso.com/PowerShell

Чтобы убедиться, что общедоступные записи DNS успешно настроены, выполните указанные ниже действия.

1. Откройте командную строку и запустите программу `nslookup.exe`.
2. Измените значение на DNS-сервер, который может обращаться с запросами к общедоступной зоне DNS.

3. В `nslookup` найдите запись для всех созданных полных доменных имен. Убедитесь, что для каждого полного доменного имени возвращается правильное значение.

4. Введите `nslookup` `set type=mx` и найдите обслуживаемый домен, добавленный на шаге 1. Убедитесь, что возвращенное значение соответствует полному доменному имени сервера почтовых ящиков.

Шаг 5. Настройка внутренних URL-адресов

Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи " *<Параметры виртуального каталога службы>* " в разделе Разрешения клиентов и мобильных устройств .

Чтобы клиенты могли подключаться к новому серверу из внутренней сети, необходимо настроить внутренние домены (или URL-адреса) в виртуальных каталогах служб клиентского доступа (внешних) на сервере почтовых ящиков, а затем настроить внутренние записи DNS.

Приведенная ниже процедура позволяет выбрать, должны ли пользователи использовать один и тот же URL-адрес в интрасети и Интернете для доступа к серверу Exchange Server или использовать другой URL-адрес. Это решение зависит от существующей схемы адресации или от схемы, которую вы хотите внедрить. Если внедряется новая схема адресации, мы советуем использовать одинаковый URL-адрес для внутренних и внешних URL-адресов. Использование одинаковых URL-адресов упрощает пользователям доступ к серверу Exchange, поскольку им необходимо будет запомнить только один адрес.

Независимо от вашего решения необходимо настроить частную зону DNS для выбранного адресного пространства. Дополнительные сведения об администрировании зон DNS см. в статье Администрирование DNS-сервера.

Дополнительные сведения о внутренних и внешних URL-адресах виртуальных каталогов см. в разделе Параметры по умолчанию для управления виртуальными каталогами ExchangeVirtual Directory Management.

Настройка внутреннего URL-адреса, совпадающего с внешним

1. Откройте консоль управления Exchange на сервере почтовых ящиков.

2. Сохраните имя узла сервера почтовых ящиков в переменной, которая будет использоваться в следующем шаге. Например, Mailbox01.

```
PowerShell

$HostName = "Mailbox01"
```

3. Выполните все приведенные ниже команды в командной консоли Exchange, чтобы задать внутренние URL-адреса, соответствующие внешнему URL-адресу виртуального каталога.

```
PowerShell

Set-EcpVirtualDirectory "$HostName\ECP (Default Web Site)" -InternalUrl
((Get-EcpVirtualDirectory "$HostName\ECP (Default Web
Site)").ExternalUrl)
```

```
PowerShell

Set-WebServicesVirtualDirectory "$HostName\EWS (Default Web Site)" -
InternalUrl ((Get-WebServicesVirtualDirectory "$HostName\EWS (Default
Web Site)").ExternalUrl)
```

```
PowerShell

Set-ActiveSyncVirtualDirectory "$HostName\Microsoft-Server-ActiveSync
(Default Web Site)" -InternalUrl ((Get-ActiveSyncVirtualDirectory
"$HostName\Microsoft-Server-ActiveSync (Default Web
Site)").ExternalUrl)
```

```
PowerShell

Set-OabVirtualDirectory "$HostName\OAB (Default Web Site)" -InternalUrl
((Get-OabVirtualDirectory "$HostName\OAB (Default Web
Site)").ExternalUrl)
```

```
PowerShell

Set-OwaVirtualDirectory "$HostName\OWA (Default Web Site)" -InternalUrl
((Get-OwaVirtualDirectory "$HostName\OWA (Default Web
Site)").ExternalUrl)
```

```
PowerShell
```

```
Set-PowerShellVirtualDirectory "$HostName\PowerShell (Default Web
Site)" -InternalUrl ((Get-PowerShellVirtualDirectory
"$HostName\PowerShell (Default Web Site)").ExternalUrl)
```

Настроив внутренний URL-адрес в виртуальных каталогах сервера почтовых ящиков, настройте частные записи DNS для Outlook в Интернете и других возможностей подключения. В зависимости от конфигурации нужно будет настроить частные DNS-записи так, чтобы они указывали на внутренний или внешний IP-адрес либо полное доменное имя сервера почтовых ящиков. Примеры рекомендуемых записей DNS, которые необходимо создать, описаны в следующей таблице:

Полное доменное имя	**Тип записи DNS**	**Значение**
Mail.contoso.com	CNAME	Mailbox01.corp.contoso.com
Owa.contoso.com	CNAME	Mailbox01.corp.contoso.com

Как убедиться, что все получилось?

Чтобы убедиться, что вы успешно настроили внутренний URL-адрес в виртуальных каталогах сервера почтовых ящиков, сделайте следующее:

1. В EAC перейдите в раздел **Серверы**>**Виртуальные каталоги**.
2. В поле **Выберите сервер** укажите сервер почтовых ящиков с выходом в Интернет.
3. Выберите виртуальный каталог и нажмите кнопку **Изменить**.✎
4. Проверьте, указаны ли в поле **Внутренний URL-адрес** правильное полное доменное имя и служба, как показано в приведенной ниже таблице.

Виртуальный каталог	**Значение внутреннего URL-адреса**
Автообнаружение	Внутренний URL-адрес не отображается
ECP	https://owa.contoso.com/ecp
EWS	https://mail.contoso.com/EWS/Exchange.asmx
Microsoft-Server-ActiveSync	https://mail.contoso.com/Microsoft-Server-ActiveSync
OAB	https://mail.contoso.com/OAB
OWA	https://owa.contoso.com/owa

Виртуальный каталог	Значение внутреннего URL-адреса
PowerShell	http://mail.contoso.com/PowerShell

Чтобы убедиться в том, что частные записи DNS успешно настроены, выполните следующие действия:

1. Откройте командную строку и выполните `nslookup.exe`.
2. Измените значение на DNS-сервер, который может обращаться с запросами к частной зоне DNS.
3. В `nslookup` найдите запись для всех созданных полных доменных имен. Убедитесь, что для каждого полного доменного имени возвращается правильное значение.

Настройка внутреннего URL-адреса, отличающегося от внешнего

1. Откройте EAC и перейдите в раздел **Серверы**>**Виртуальные каталоги**.
2. На сервере почтовых ящиков с выходом в Интернет выберите виртуальный каталог, который требуется настроить, и нажмите кнопку **Изменить**.
3. Откроется окно свойств виртуального каталога. В поле **Внутренний URL-адрес** замените существующее значение имени узла в URL-адресе (вероятно, полное доменное имя сервера почтовых ящиков) новым значением, которое вы хотите использовать (например, internal.contoso.com).

   Например, в свойствах виртуального каталога веб-служб Exchange (EWS) замените текущее значение https://Mailbox01.corp.contoso.com/ews/exchange.asmx на https://internal.contoso.com/ews/exchange.asmx.

   Когда закончите, нажмите кнопку **Сохранить**.
4. Повторите предыдущие действия для каждого виртуального каталога, который требуется изменить.

> **Примечание**
>
> Внутренние URL-адреса виртуальных каталогов ECP и OWA должны быть одинаковыми. Невозможно установить внутренний URL-адрес в

виртуальном каталоге автообнаружения.

После настройки внутреннего URL-адреса в виртуальных каталогах сервера почтовых ящиков необходимо настроить частные записи DNS для Outlook в Интернете и других подключений. В зависимости от конфигурации нужно будет настроить частные DNS-записи так, чтобы они указывали на внутренний или внешний IP-адрес либо полное доменное имя сервера почтовых ящиков. Пример рекомендуемой записи DNS, которую необходимо создать, описан в следующей таблице:

Полное доменное имя	**Тип записи DNS**	**Значение**
internal.contoso.com	CNAME	Mailbox01.corp.contoso.com

Как убедиться, что все получилось?

Чтобы убедиться, что вы успешно настроили внутренние URL-адреса в виртуальных каталогах служб клиентского доступа на сервере почтовых ящиков, выполните указанные ниже действия.

1. В EAC перейдите в раздел **Серверы**>**Виртуальные каталоги**.
2. В поле **Выберите сервер** укажите сервер почтовых ящиков с выходом в Интернет.
3. Выберите виртуальный каталог и нажмите кнопку **Изменить**.✎
4. Проверьте, чтобы в поле **Внутренний URL-адрес** было указано правильное полное доменное имя. Например, вы настроили внутренние URL-адреса для использования internal.contoso.com.

Виртуальный каталог	**Значение внутреннего URL-адреса**
Автообнаружение	Внутренний URL-адрес не отображается
ECP	https://internal.contoso.com/ecp
EWS	https://internal.contoso.com/EWS/Exchange.asmx
Microsoft-Server-ActiveSync	https://internal.contoso.com/Microsoft-Server-ActiveSync
OAB	https://internal.contoso.com/OAB
OWA	https://internal.contoso.com/owa

Виртуальный каталог	Значение внутреннего URL-адреса
PowerShell	http://internal.contoso.com/PowerShell

Чтобы убедиться, что частные записи DNS успешно настроены, выполните указанные ниже действия.

1. Откройте командную строку и запустите программу `nslookup.exe`.
2. Измените значение на DNS-сервер, который может обращаться с запросами к частной зоне DNS.
3. В `nslookup` найдите запись для всех созданных полных доменных имен. Убедитесь, что для каждого полного доменного имени возвращается правильное значение.

Шаг 6. Настройка SSL-сертификата

Для некоторых служб, таких как Мобильный Outlook и Exchange ActiveSync, требуется настройка сертификатов на сервере Exchange Server. Следующие шаги описывают, как настроить SSL-сертификат от стороннего центра сертификации (ЦС):

1. Создайте запрос сертификата Exchange Server для центра сертификации.
    - Следует запросить сертификат у стороннего ЦС, чтобы клиенты автоматически доверяли сертификату. Дополнительные сведения см. в разделе Рекомендации по использованию сертификатов Exchange.
    - Если внутренние и внешние URL-адреса настроены как одинаковые, **Outlook в Интернете (при доступе из Интернета)** и **Outlook в Интернете (при доступе из интрасети)** должны отображать owa.contoso.com. **Автономная адресная** адрес mail.contoso.com **ная** адрес
    - Если заданы внутренние URL-адреса формата internal.contoso.com, в поле **Outlook в Интернете (при доступе через Интернет)** будет показан адрес owa.contoso.com, а в поле **Outlook в Интернете (при доступе через интрасеть)** — адрес internal.contoso.com.
2. Завершение ожидающего запроса на получение сертификата Exchange Server.
3. Назначение сертификатов службам Exchange Server
    - Как минимум, следует выбрать **SMTP** и **IIS**.

- При появлении предупреждения **Перезаписать существующий SMTP-сертификат по умолчанию?** нажмите кнопку **Да**.

Как убедиться, что все получилось?

Чтобы убедиться, что вы успешно добавили новый сертификат, выполните указанные ниже действия.

1. В EAC перейдите в раздел **Сертификаты серверов**>.
2. Выберите новый сертификат и затем в области сведений убедитесь, что выполнены следующие условия:
   - значение параметра **Состояние** равно **Действительный**;
   - в поле **Назначен службам** указаны как минимум **IIS** и **SMTP**.

Как убедиться, что это сработало?

Чтобы убедиться, что вы настроили поток обработки почты и внешний клиентский доступ, выполните указанные ниже действия.

1. Создайте новый профиль в приложении Outlook и/или на устройстве ActiveSync. Убедитесь, что новый профиль успешно создается в Outlook или на мобильном устройстве.
2. В Outlook или на мобильном устройстве отправьте новое сообщение внешнему получателю. Убедитесь, что внешний получатель получил сообщение.
3. В почтовом ящике внешнего получателя ответьте на сообщение, отправленное из почтового ящика Exchange. Убедитесь, что сообщение успешно доставлено в почтовый ящик Exchange.
4. Перейдите по адресу https://owa.contoso.com/owa, чтобы убедиться в отсутствии предупреждений о сертификате.

Проверка Exchange Server установок

Статья • 04.04.2023

После установки Exchange Server 2016 или Exchange Server 2019 рекомендуется проверить установку, выполнив командлет **Get-ExchangeServer** и просмотрив журнал установки Exchange. Если процесс установки завершается сбоем или во время установки возникают ошибки, можно использовать журнал установки, чтобы найти источник проблемы.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server, Exchange Online или Exchange Online Protection.

Выполнение командлета Get-ExchangeServer

Чтобы убедиться, что Exchange успешно установлен, выполните следующие команды в командной консоли Exchange. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.

Эта команда возвращает сводный список имен, сайтов Active Directory, ролей сервера Exchange, выпусков Exchange и версий Exchange всех серверов Exchange в организации.

PowerShell

```
Get-ExchangeServer
```

В этом примере возвращаются дополнительные сведения о сервере Exchange с именем Mailbox01.

PowerShell

```
Get-ExchangeServer -Identity Mailbox01 | Format-List
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Get-ExchangeServer.

Просмотр журнала приложений Windows и журнала установки Exchange

- Программа установки Exchange регистрирует события в **журнале приложений** Windows Server. Этот журнал содержит журнал всех действий, выполняемых системой во время установки Exchange, и всех возникших ошибок (по умолчанию метод ведения журнала имеет значение Verbose). Вы можете использовать **Просмотр событий** Windows для поиска сообщений, связанных с установкой Exchange.

- Журнал установки Exchange доступен на <*системном диске*>:\ExchangeSetupLogs\ExchangeSetup.log (<*системный диск*> — это диск, на котором установлена Windows). Журнал установки отслеживает ход выполнения каждой задачи во время установки и настройки Exchange. Файл содержит сведения о состоянии предварительных требований и проверок готовности системы перед началом установки, ходе установки приложения и изменениях конфигурации, внесенных в систему. Проверьте этот файл журнала, чтобы убедиться, что Exchange установлен должным образом.

Рекомендуется начать проверку журнала приложений Windows и (или) журнала установки Exchange, выполнив поиск ошибок. Если вы нашли запись об ошибке, прочитайте связанный текст, чтобы определить причину ошибки.

Установка средств управления Exchange

Статья • 04.04.2023

Средства управления в Exchange Server 2016 и Exchange Server 2019 включают командную консоль Exchange и панель элементов Exchange. Средства управления можно установить на других клиентских компьютерах или серверах в домене Active Directory, чтобы помочь вам управлять организацией Exchange. Средства управления имеют аналогичные требования к операционной системе, платформа .NET Framework и Windows Management Framework (Windows PowerShell), что и exchange Server. Примечательное исключение: вы можете установить средства управления в клиентских версиях Windows. Дополнительные сведения см. в Exchange Server требованиях к системе и Exchange Server предварительных требованиях.

> **Совет**
>
> Если вы хотите использовать средства управления Exchange для управления получателями без сохранения Exchange Server, см. статью **Управление локальными получателями в гибридной среде с помощью средств управления Exchange**.

> **Примечание**
>
> Средства управления не включают Центр администрирования Exchange (EAC). EAC — это веб-консоль, размещенная на серверах почтовых ящиков Exchange 2016, и, как и любой веб-сайт, вы можете получить доступ к EAC с других компьютеров. Дополнительные сведения о EAC см. в разделе **Центр администрирования Exchange в Exchange Server**.

Для получения дополнительных сведений о командной консоли Exchange см. статью Exchange Server PowerShell (командная консоль Exchange).

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 20 минут

- Компьютеру, на котором требуется установить средства управления Exchange, требуется доступ к Setup.exe в файлах установки Exchange. Сведения о том, как скачать последнюю версию Exchange, см. в разделе Обновления для Exchange Server.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

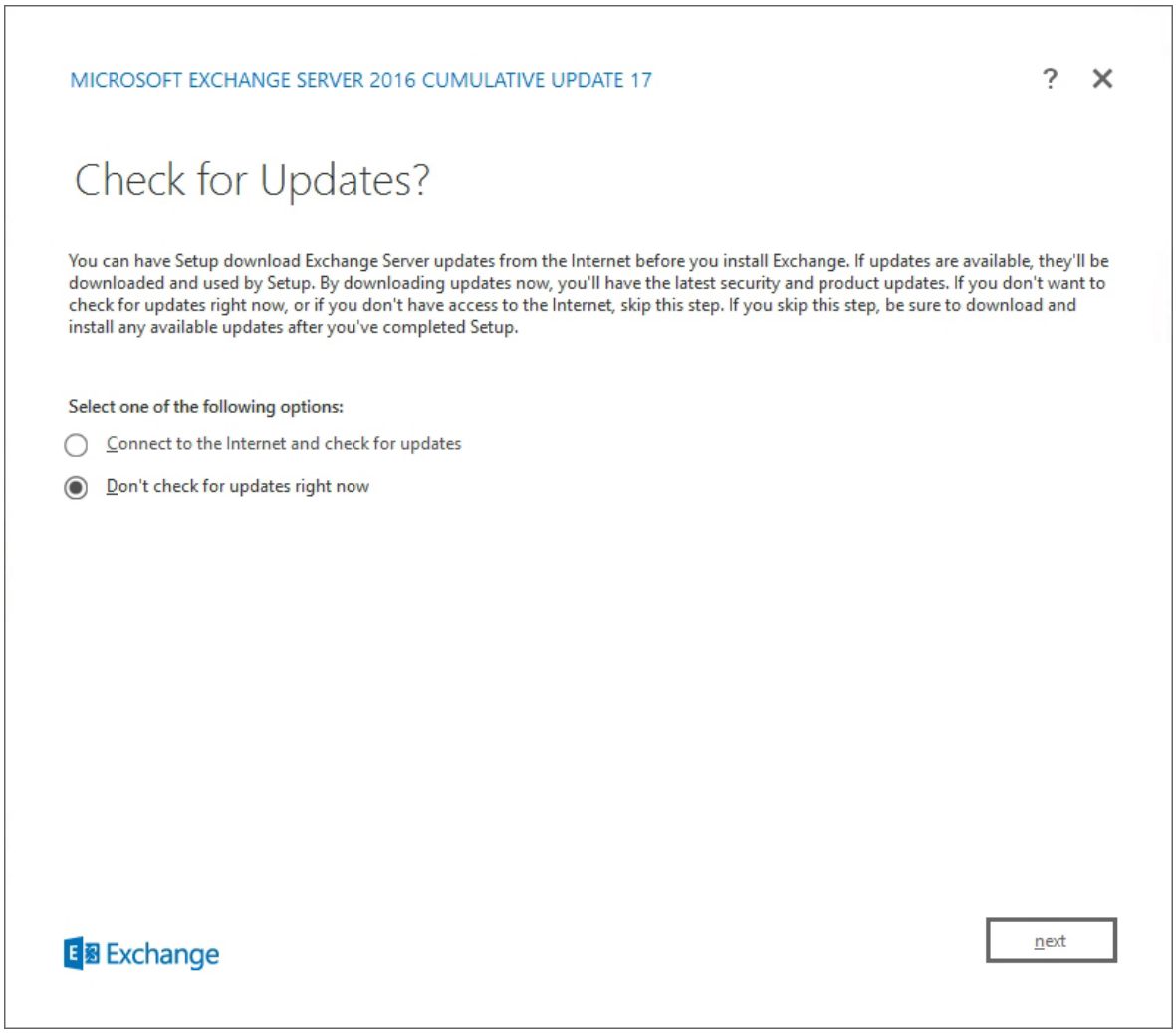
Установка средств управления Exchange с помощью мастера установки Exchange 2016

1. В проводник на компьютере, на котором вы хотите установить средства управления, щелкните правой кнопкой мыши скачанный файл ISO-образа Exchange и выберите **Подключить**. В появившемся появившемся виртуальном DVD-диске запустите программу установки Exchange, дважды щелкнув `Setup.exe`.

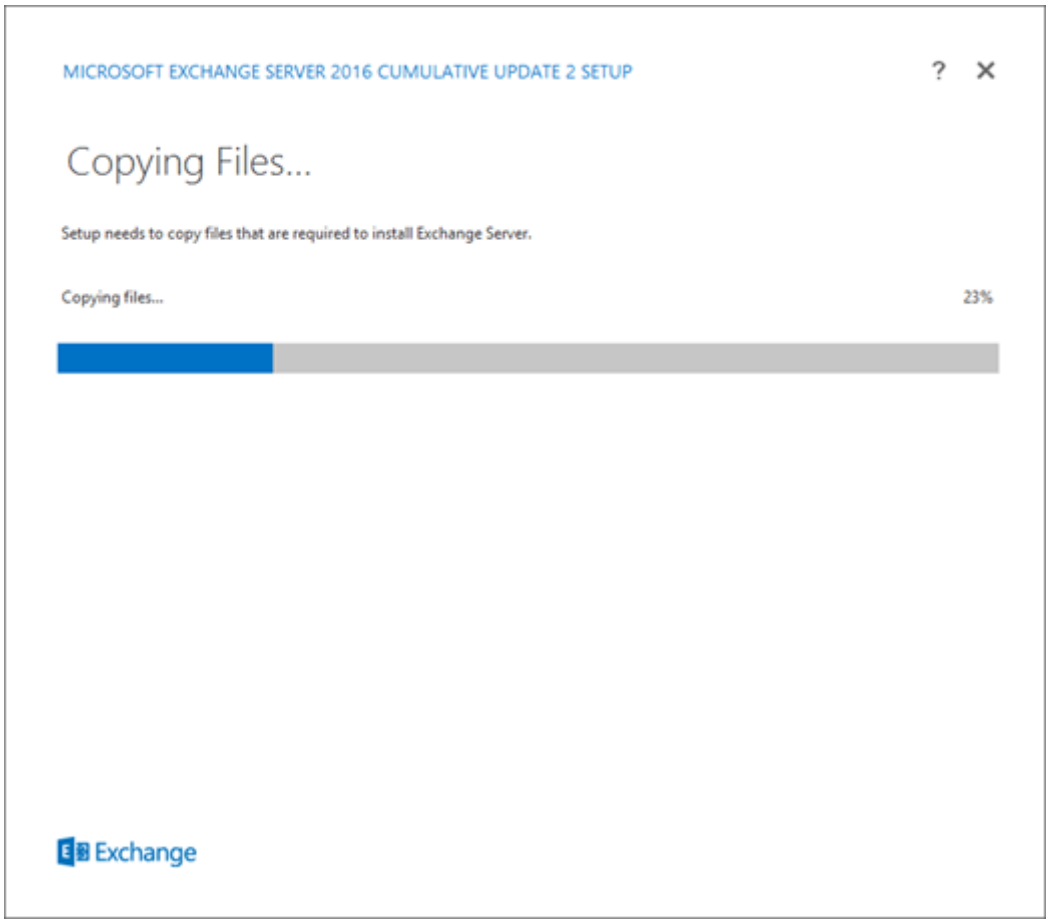
2. Откроется мастер установки Exchange Server. На странице **Проверить наличие обновлений** выберите один из предложенных ниже вариантов и нажмите кнопку **Далее** для продолжения.

   Подключитесь к Интернету и проверьте наличие обновлений. Мы рекомендуем использовать этот параметр, который выполняет поиск обновлений для *устанавливаемой* версии Exchange (не обнаруживает новые накопительные Обновления). При выборе этого варианта вы автоматически будете перенаправлены на страницу **Скачивание обновлений**, где выполняется поиск обновлений. Для продолжения нажмите кнопку **Далее**.

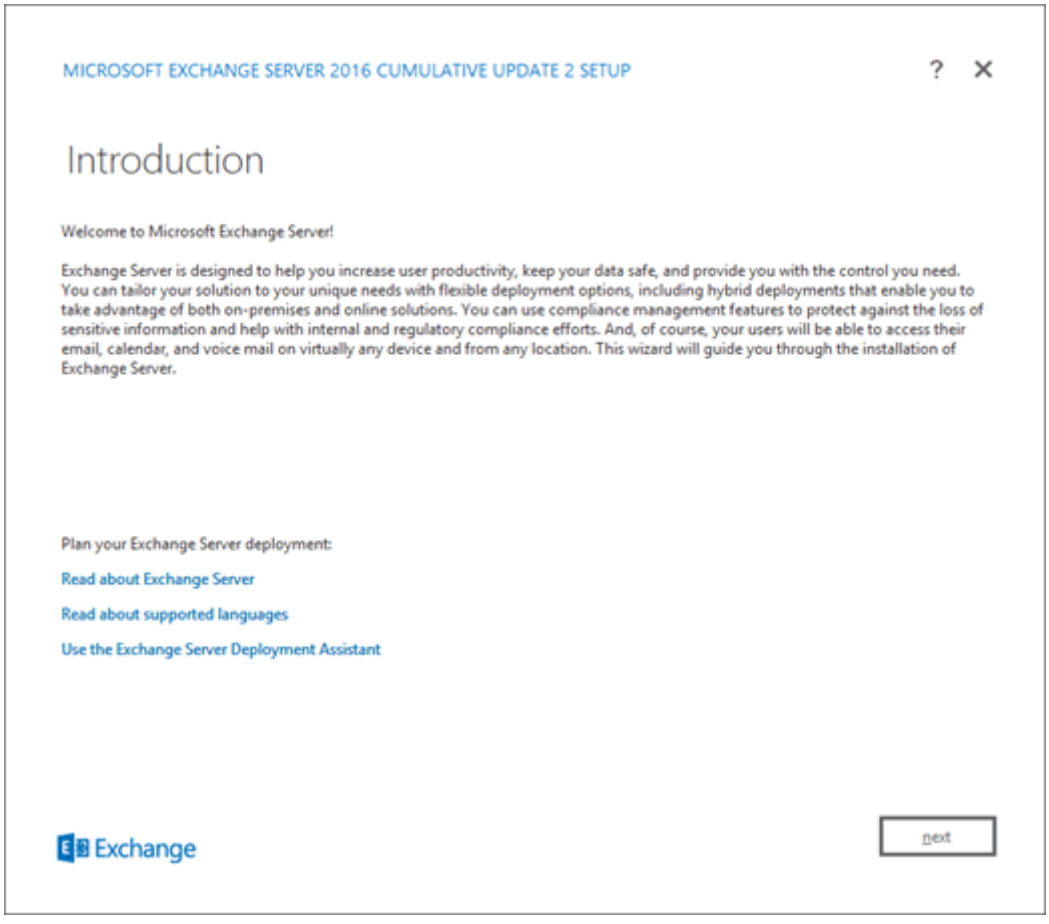
   - **Не проверять обновления сейчас**.



3. На странице **Копирование файлов** отображается ход выполнения копирования файлов на локальный жесткий диск. Как правило, файлы копируются в `%WinDir%\Temp\ExchangeSetup`, но вы можете подтвердить расположение в журнале установки Exchange по адресу `C:\ExchangeSetupLogs\ExchangeSetup.log`.

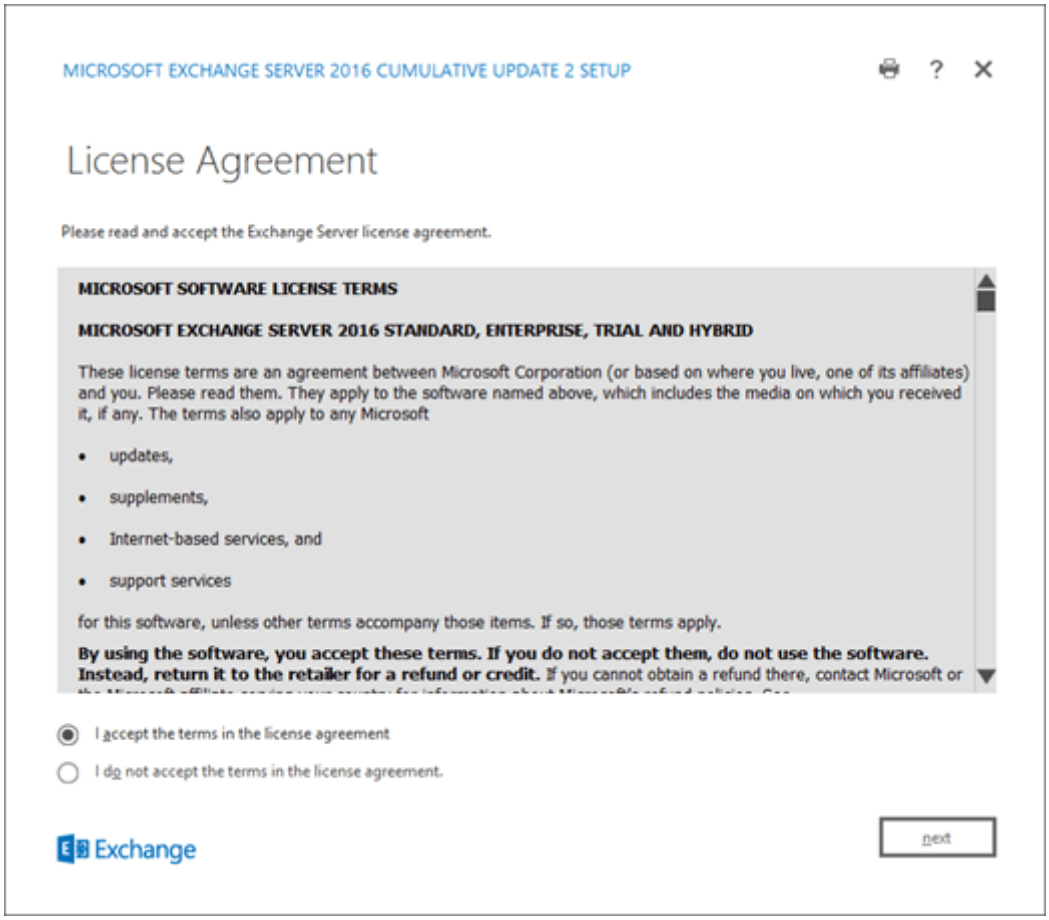


4. На странице **Введение** нажмите кнопку **Далее** для продолжения.



5. На странице **Лицензионное соглашение** ознакомьтесь с условиями лицензионного соглашения на программное обеспечение, выберите **Я**

принимаю условия лицензионного соглашения и нажмите **Далее**, чтобы продолжить.

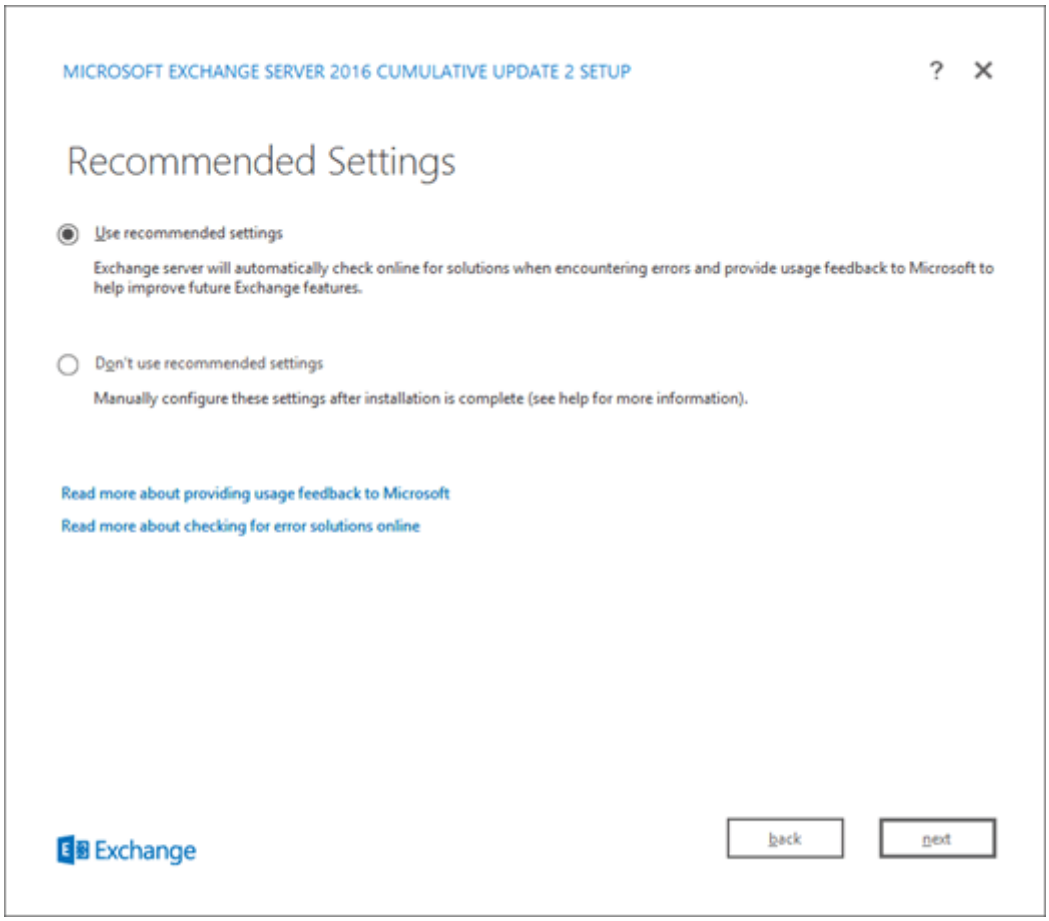


6. На странице **Рекомендуемые параметры** выберите один из следующих параметров:

   - **Использование рекомендуемых параметров**. Exchange автоматически отправляет отчеты об ошибках и сведения об оборудовании компьютера и способах использования Exchange в корпорацию Майкрософт. Для получения сведений о том, что отправляется в корпорацию Майкрософт и как они используются, щелкните **?** или ссылки на справку на странице.

   - **Не использовать рекомендованные параметры**. Эти параметры отключены, но вы в любое время можете включить их после завершения работы программы установки.

   Для продолжения нажмите кнопку **Далее**.

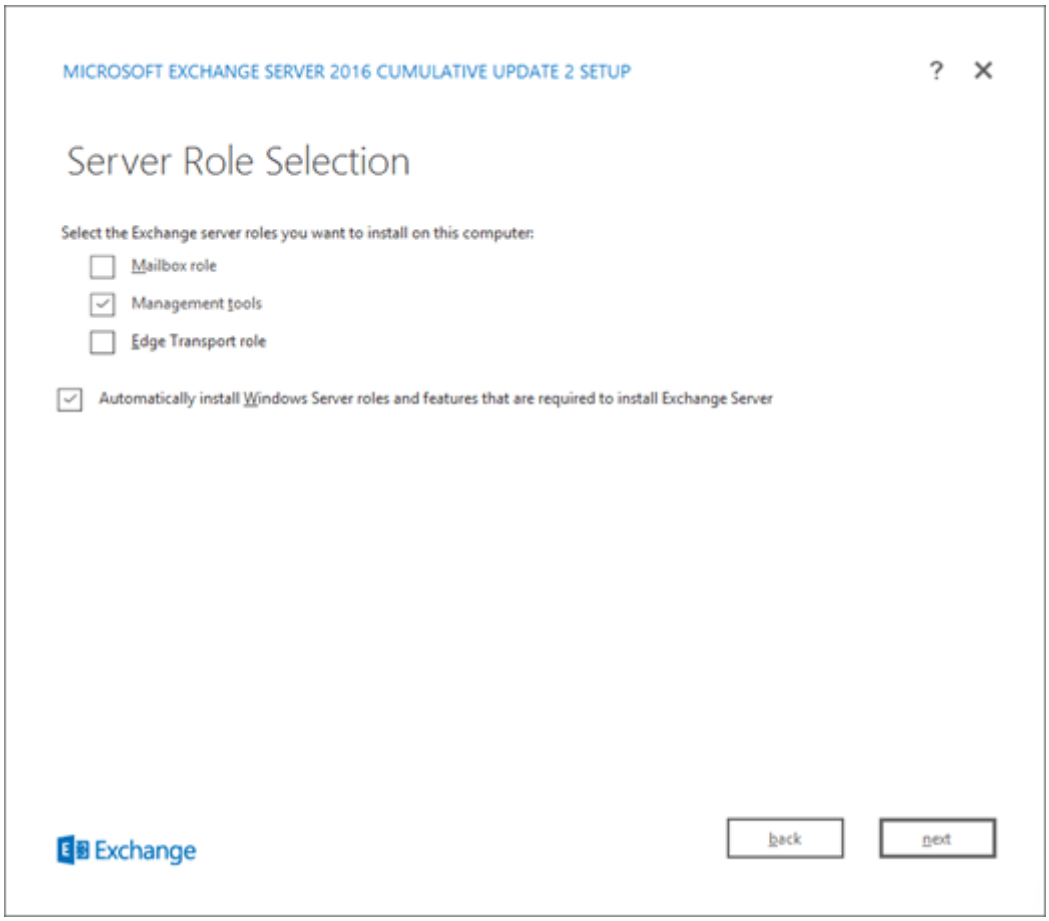


7. На странице **Выбор роли сервера** настройте следующие параметры:

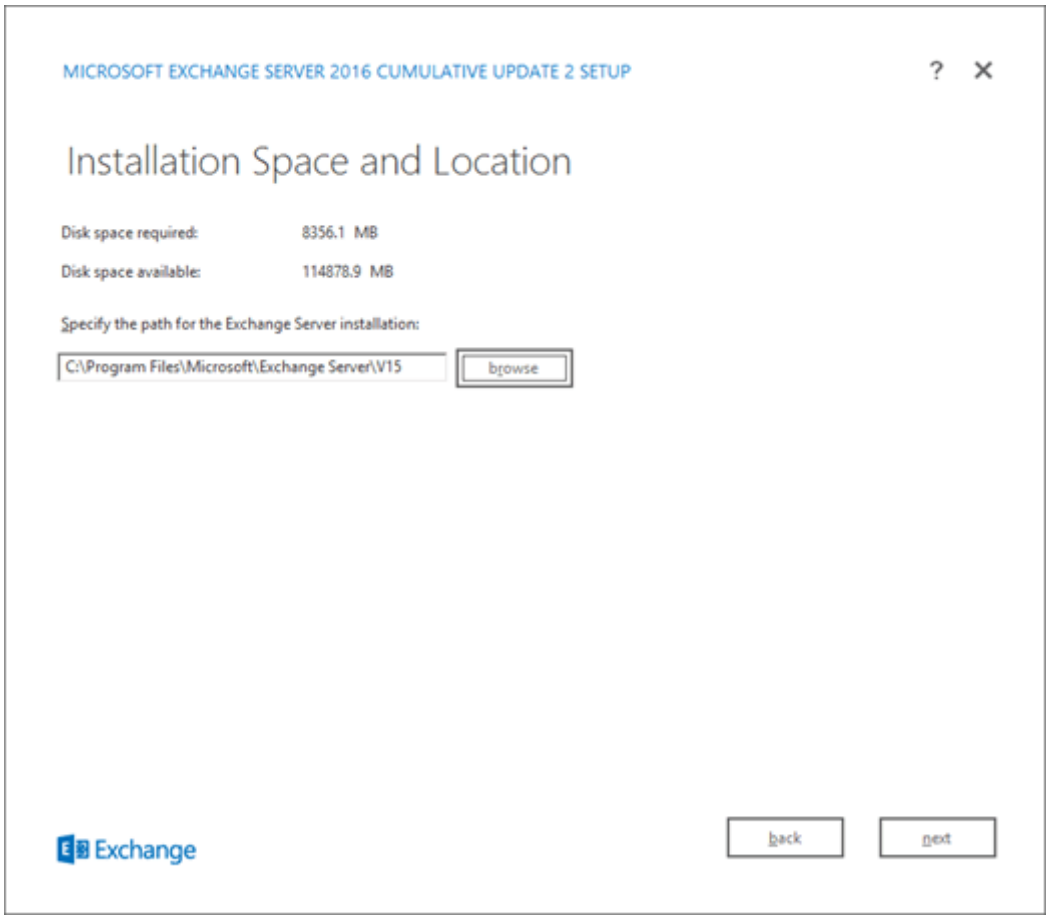
   - Выберите **Средства управления**.
   - **Автоматическая установка ролей и компонентов Windows Server, необходимых для установки Exchange**. Выберите этот параметр, чтобы мастер установки установил необходимые компоненты Windows. Для завершения установки некоторых компонентов Windows может потребоваться перезагрузить компьютер. Если этот параметр не выбран, необходимо установить компоненты Windows вручную.

     Примечание. При выборе этого параметра устанавливаются только *компоненты Windows* , необходимые exchange. Другие необходимые компоненты необходимо установить вручную. Дополнительные сведения см. в разделе предварительные требования Exchange Server.

Для продолжения нажмите кнопку **Далее**.



8. На странице **Место установки и расположение** либо примите расположение установки по умолчанию (`C:\Program Files\Microsoft\Exchange Server\V15`), либо нажмите кнопку **Обзор** , чтобы выбрать новое расположение. Убедитесь, что в этом расположении достаточно дискового пространства для установки средств управления. Для продолжения нажмите кнопку **Далее**.



9. Если это первая установка Exchange в организации (сервера Exchange Server или средств управления), выполнится переход на страницу **Организация Exchange**. На этой странице настройте следующие параметры:

    - **Укажите имя для этой организации Exchange**. Значение по умолчанию — **First Organization**, но для этого значения обычно используется название компании. Название организации используется внутри Exchange — оно, как правило, невидимо для пользователей, не влияет на функциональность Exchange и не определяет доступные адреса электронной почты.

        - Название организации не должно быть длиннее 64 символов и не может быть пустым.

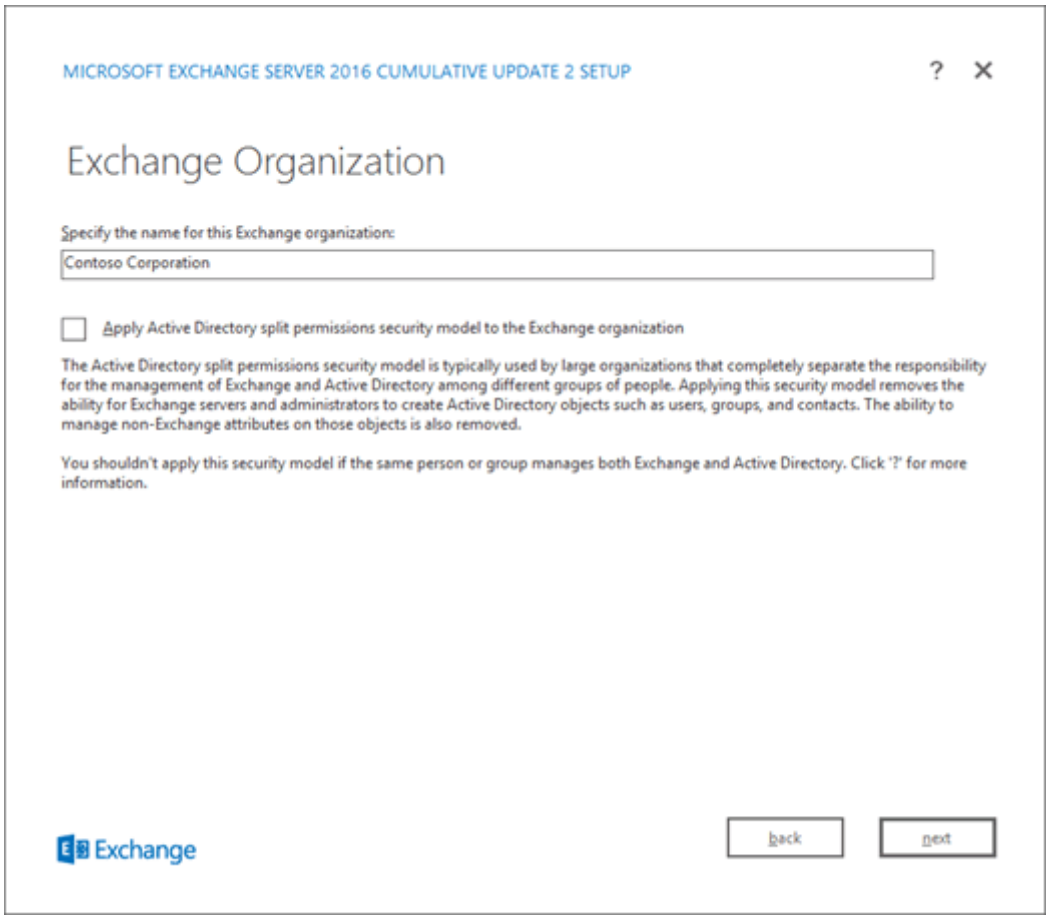
        - Допустимые символы — от A до Z, от a до z, от 0 до 9, дефис или тире (-) и пробел, но пробелов не должно быть в начале и конце названия.

        - Указанное название организации нельзя изменить.

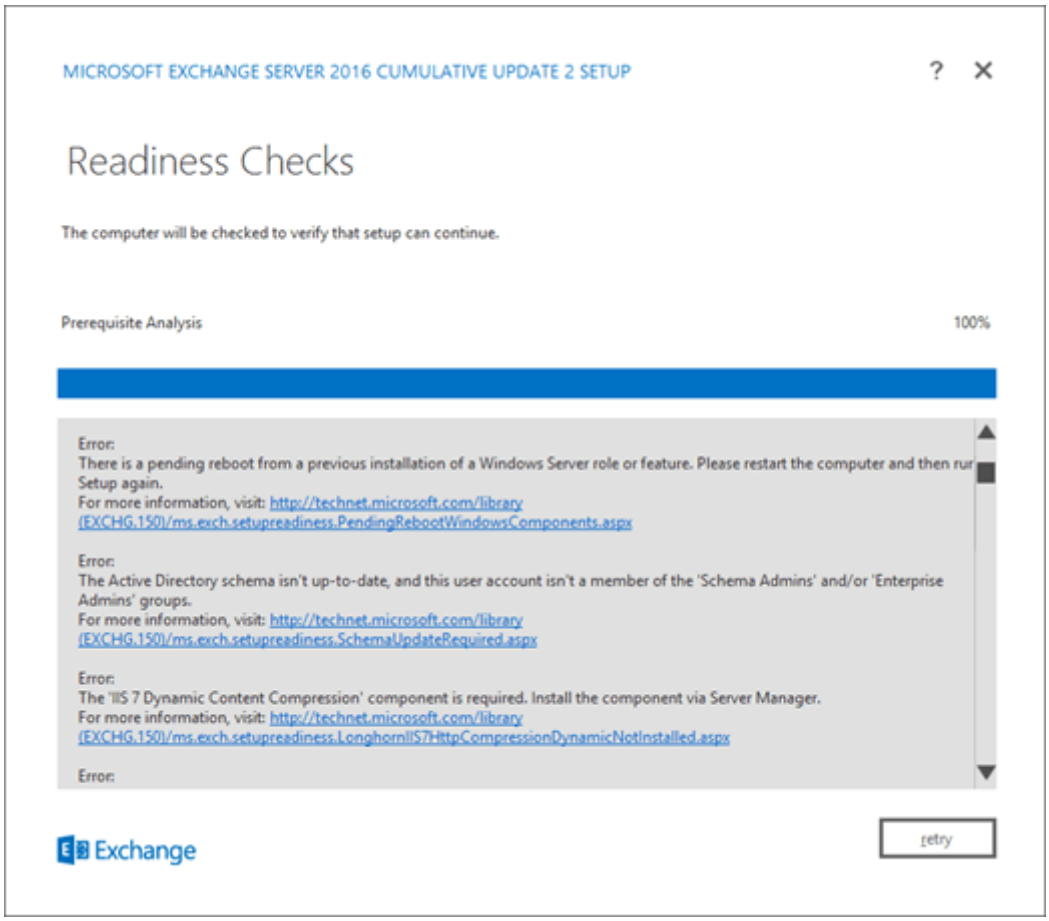
    - **Применение модели безопасности разделенных разрешений Active Directory к организации Exchange**. Большинству организаций не нужно выбирать этот параметр. Если вам нужно разделить управление субъектами безопасности Active Directory и конфигурацию Exchange, вам

могут пригодиться разделенные разрешения. Выберите **?** для получения дополнительных сведений.

Для продолжения нажмите кнопку **Далее**.

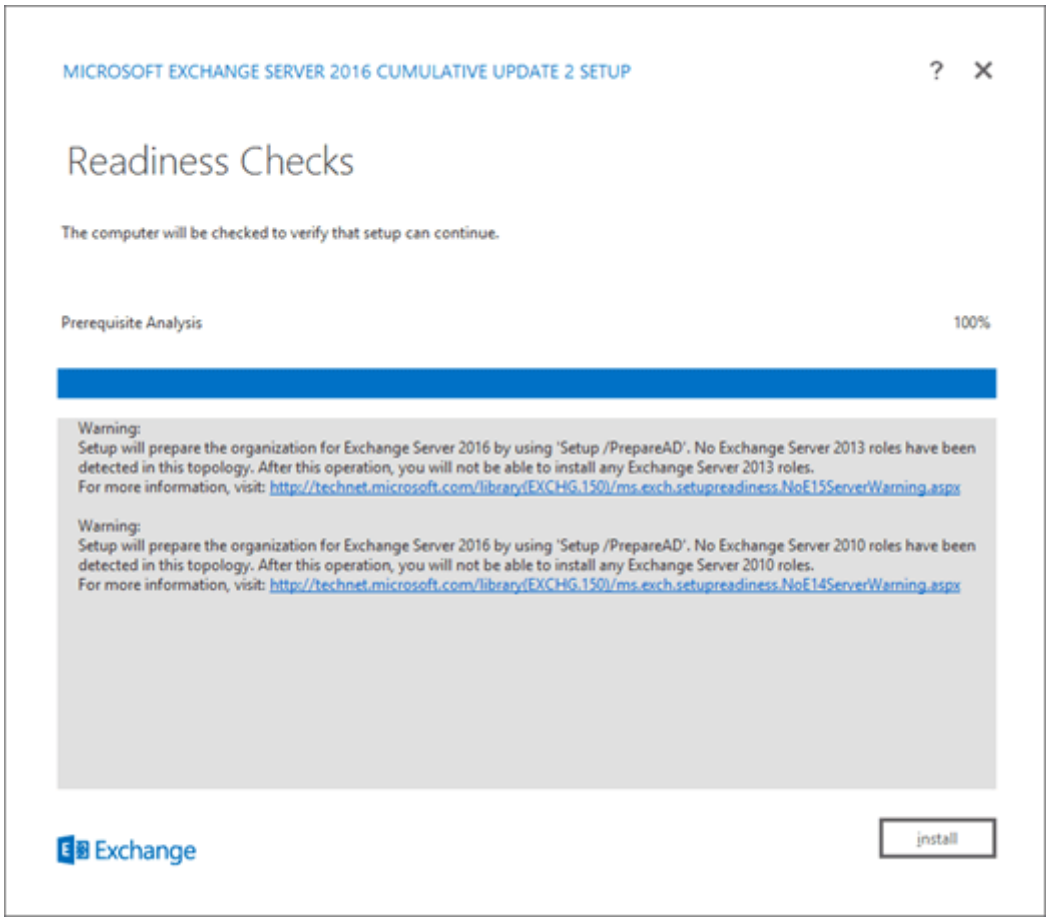


10. На странице **Проверки готовности** убедитесь, что проверки готовности организации и роли сервера выполнены успешно. В противном случае на странице будет отображаться только кнопка **Повторить**.

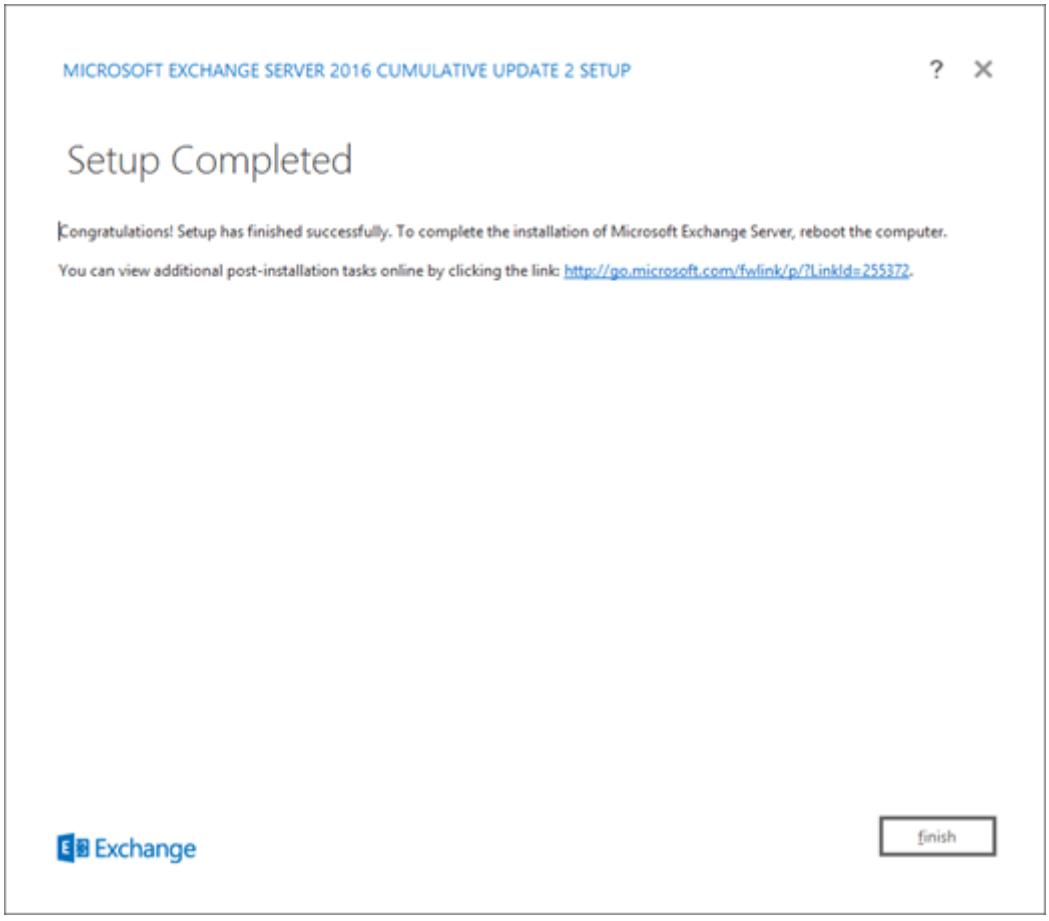


Устранив ошибки, нажмите кнопку **Повторить попытку**, чтобы снова запустить проверки наличия обязательных компонентов. Некоторые ошибки можно устранить, не выходя из программы установки, а для исправления других понадобится перезагрузить компьютер. При перезагрузке компьютера необходимо начать с шага 2.

Если на странице **Проверки готовности** ошибок больше не обнаружено, кнопка **Повторить попытку** заменится кнопкой **Установить**, и тогда вы можете продолжить. Проверьте все предупреждения и нажмите кнопку **Установить** для установки средств управления.



11. На странице **Установка завершена** нажмите **Готово** и перезагрузите компьютер.



Использование режима автоматической установки Exchange для установки средств управления Exchange

1. В проводник на компьютере, на котором требуется установить средства управления Exchange, щелкните правой кнопкой мыши скачанный файл ISO-образа Exchange и выберите **Подключить**.

2. Чтобы установить средства управления Exchange из командной строки, используйте следующий синтаксис в командной строке с повышенными привилегиями (окно командной строки, открытое путем выбора **запуска от имени администратора**):

> ⓘ **Примечание**
>
> - Предыдущий переключатель */IAcceptExchangeServerLicenseTerms* не будет работать начиная с накопительных обновлений (CU) за сентябрь 2021 г. Теперь необходимо использовать */IAcceptExchangeServerLicenseTerms_DiagnosticDataON* или */IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF* для автоматической установки и установки по сценариям.
>
> - В примерах ниже используется переключатель */IAcceptExchangeServerLicenseTerms_DiagnosticDataON*. Вы можете изменить переключатель на */IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF*.

Консоль

```
<Virtual DVD drive letter>:\Setup.exe
/IAcceptExchangeServerLicenseTerms_DiagnosticDataON /Role:ManagementTools
[/EnableErrorReporting] [/CustomerFeedbackEnabled:<True | False>]
[/InstallWindowsComponents] [/TargetDir:<Target folder>] [/OrganizationName:
<Name>]
```

В этом примере файлы установки Exchange на диске E: используются для установки средств управления на локальном сервере.

Консоль

```
E:\Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON
/Role:ManagementTools
```

Дополнительные сведения см. в статье Установка Exchange в автоматическом режиме.

Тестирование функций в Exchange Server

Статья • 11.02.2025

Обзор

Исторически перед установкой обновления Exchange в рабочей среде организации часто развертывают обновления в тестовой среде, чтобы сначала проверить обновление перед его развертыванием в рабочей среде. Это важная задача, но она также занимает много времени и может замедлить развертывание важных обновлений. Кроме того, тестовые среды имеются не во всех организациях.

Тестирование функций предоставляет администраторам дополнительный способ тестирования и развертывания некоторых новых функций в своей Exchange Server организации. Flighting — это необязательная облачная служба для локальных серверов Exchange. Он использует `Office Config Service (OCS)` ту же конечную точку, которая используется службой экстренного устранения рисков и клиентами Microsoft Office, чтобы проверка обновлений от Корпорации Майкрософт, связанных с тестируемыми функциями.

С помощью функции "Тестирование компонентов" администраторы могут немедленно развертывать обновления и контролировать, когда в их среде включена возможность тестирования. Функция "Просмотр компонентов" также позволяет корпорации Майкрософт отключать возможность тестирования в случае обнаружения серьезной проблемы после выпуска обновления, содержащего эту функцию.

Тестирование компонентов не применяется ко всем новым функциям и изменениям в будущих обновлениях. Команда разработчиков Exchange Server определяет, какие функции распространяются через тестирование компонентов, и в этой статье ведется живой подробный список тестируемых функций. Использование функции flighting является необязательным, но оно включено по умолчанию. Его можно настроить или отключить, выполнив описанные ниже действия.

Тестируемые функции

В таблице приведен подробный список всех доступных в настоящее время функций. Эта таблица является живой; Корпорация Майкрософт обновляет таблицу

новыми рейсами и изменениями в затронутом кольце по крайней мере за 7 дней до того, как они станут активными. Корпорация Майкрософт не может объявить об изменениях за несколько дней до этого, если компонент необходимо отключить (отозвать) из-за регрессии или известной проблемы.

Развернуть таблицу

Функция	Описание	Кольца	Утверждение Администратор	Напомнил	Запуск сборки	Завершение сборки
PING.1.0	Проба пульса	0,1,2	Нет	Нет	15.02.1748.005	Недоступно

Как работает тестирование компонентов

Проверка функций — это инновационный метод управления функциями и изменениями в Exchange Server, который позволяет корпорации Майкрософт внедрять новые функции и изменения для Exchange Server в изначально отключенном состоянии. Вот как это работает:

1. **Первоначальное введение**. При вводе функции или изменения в тестовом состоянии они включаются в обновление Exchange Server (CU или SU) в отключенном состоянии. Это гарантирует, что функция не сразу повлияет на работу сервера.
2. **Управляемое включение**. Тестируемые функции и изменения могут быть автоматически включены на всех серверах Exchange в пределах определенного круга. Этот поэтапный подход позволяет корпорации Майкрософт отслеживать производительность компонента и собирать данные телеметрии.
3. **Оценка и развертывание**. На основе собранных данных телеметрии (и любых отзывов, которые мы можем получить в нашем блоге, через обращения в службу поддержки или из других источников), корпорация Майкрософт оценивает стабильность и эффективность функции. Если функция работает хорошо, ее можно постепенно развертывать на серверах Exchange в других кругах.
4. **Механизм Недавнее**. Ключевым преимуществом функции является возможность отзыва функции или изменения при обнаружении каких-либо проблем или регрессий. Это позволяет быстро отключить все проблемные функции для поддержания стабильности и надежности среды Exchange Server.

Примечание

Для пограничных транспортных серверов недоступны функции Flighting.

Это приводит к следующим преимуществам:

- **Расширенный контроль**. Администраторы имеют более детальный контроль над тем, когда и как появляются новые функции.
- **Улучшенная стабильность**. Путем поэтапного развертывания компонентов можно выявить и устранить потенциальные проблемы перед широкомасштабным развертыванием.
- **Гибкость**. Возможность отзыва функций гарантирует быстрое устранение любых регрессий или известных проблем.

Предварительные условия

Новая служба под названием `Microsoft Exchange Flighting service (MSExchangeFlighting)` управляет функцией "Тестирование компонентов". Эта служба ежечасно проверяет и скачивает определения тестов компонентов (FFD) из OCS, а также управляет активацией и деактивацией тестируемых функций на основе настроенного круга.

Функцию flighting нельзя использовать в средах с воздушным зазором или в средах без исходящего подключения к OCS. Службе exchange Flighting требуется исходящее подключение к OCS, чтобы проверка для FFD и скачивания. Вам не нужно предпринимать никаких действий, если ваши серверы не могут связаться с OCS. Кроме того, на пограничных транспортных серверах пока не доступно тестирование компонентов.

Мы рекомендуем регулярно проверять нашу документацию и блог команды Exchange , чтобы оставаться в курсе известных проблем, которые могут временно отключить функцию в качестве меры по устранению рисков.

Развернуть таблицу

Конечная точка	Адрес	Порт	Описание
Служба конфигурации Office	officeclient.microsoft.com/*	443	Конечная точка для тестовой службы Microsoft Exchange для скачивания FFD

Если вы используете сетевой прокси-сервер для разрешения исходящего подключения, убедитесь, что `InternetWebProxy` настроен на каждом из ваших серверов Exchange:

PowerShell

```
Set-ExchangeServer -Identity <ServerName> -InternetWebProxy
<http://proxy.contoso.local:port>
```

Необходимо также настроить параметры прокси-сервера для `WinHTTP`, который является компонентом Windows, обрабатывающим HTTP-запросы для приложений, которые не используют `WinINet API`.

command

```
netsh winhttp set proxy <proxy.contoso.com:port>
```

Помимо исходящего подключения к OCS, службе flighting Также требуется исходящее подключение к различным Certificate Revocation List конечным точкам (CRL). Это необходимо для проверки сертификатов, используемых для подписи FFD. Мы рекомендуем разрешить Windows поддерживать Certificate Trust List (CTL) на вашем компьютере. Чтобы разрешить Windows поддерживать CTL, убедитесь, что следующий URL-адрес доступен с компьютера, на котором установлена Exchange Server:

Развернуть таблицу

Конечная точка	Адрес	Порт	Описание
Скачивание списка доверия сертификатов	ctldl.windowsupdate.com/*	80	Конечная точка для скачивания списка доверия сертификатов

Кольца

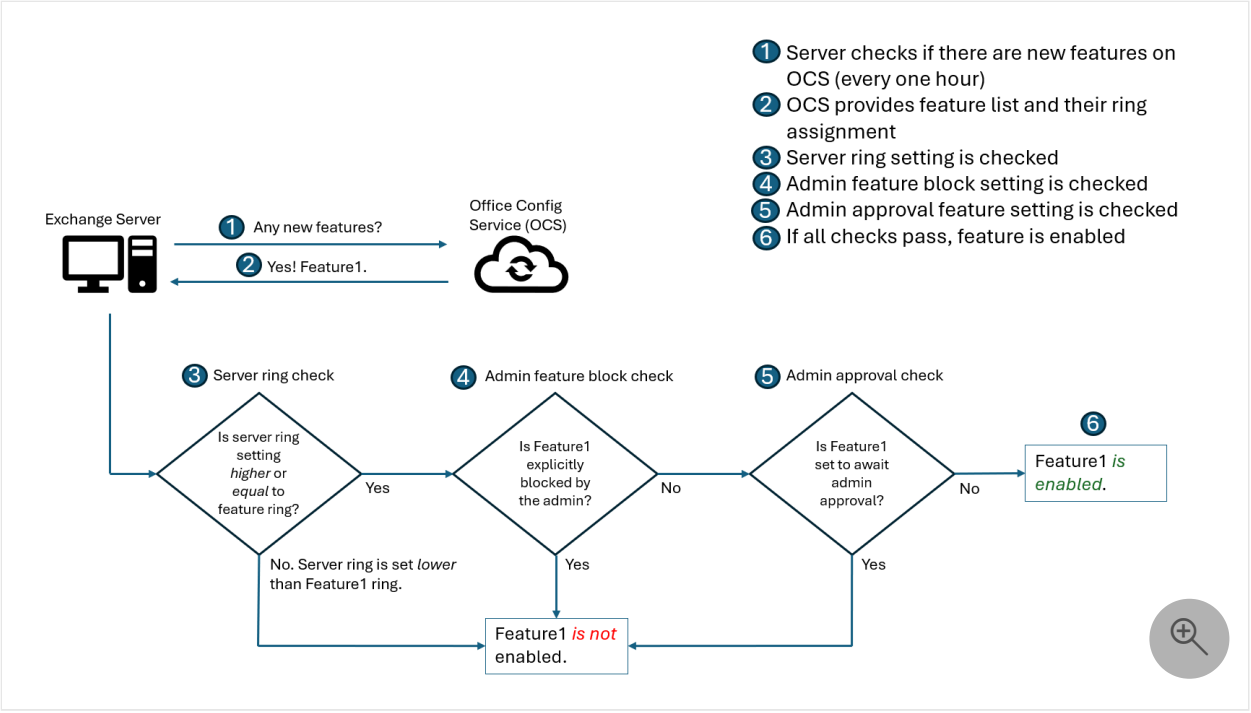
При тестировании компонентов используется механизм развертывания с именем Rings, который определяет, когда или в какой последовательности функция включена на определенном сервере Exchange Server. Каждый сервер Exchange, работающий Exchange Server 2019 CU15 или более поздней версии, автоматически назначается кругу. Назначение по умолчанию может быть изменено администратором в любое время. Доступны следующие круги:

Развернуть таблицу

Круг No.	Имя	Круг по умолчанию	Описание
0	Ранний круг последователей	Нет	Это самое раннее кольцо, которое предназначено для тестирования новых функций. Если этому кольцу назначен сервер Exchange Server, функции, представленные в обновлении, сразу же включаются после установки обновления. Это происходит независимо от классификации признаков.
1	Круг по всему миру	Да	Это круг по умолчанию, назначенный всем серверам Exchange при установке первой сборки, поддерживающей тестирование компонентов (например, CU15). Серверы в этом круге получают новые функции, как только корпорация Майкрософт подтвердит, что эти функции готовы к общедоступной доступности.
2	Круг действий Администратор	Нет	Серверы Exchange в этом круге не позволяют автоматически включить новые возможности, доступные для тестирования. Этот круг позволяет администраторам отменить изменения к предыдущему интерфейсу (например, откат). Тестируемые функции поставляются в отключенном состоянии и должны быть включены администратором с помощью Set-ExchangeFeature, как описано в разделе Состояния компонентов .

> **ⓘ Важно!**
>
> Перемещение сервера между кольцами может привести к включению или отключению определенных функций в зависимости от состояния компонента, определенного в службе тестирования для нового круга.

В следующем рабочем процессе показано, как кольцо определяет, следует ли включать функцию для тестирования.



Для назначения сервера Exchange определенному кольцу можно использовать командную консоль Exchange (EMS). В этом примере серверу Exchange server назначается круг 0:

PowerShell

```
Set-ExchangeServer -Identity <ServerName> -RingLevel 0
```

> **ⓘ Важно!**
>
> Если вы не хотите, чтобы корпорация Майкрософт автоматически включила новые функции или внося изменения в сервер с помощью функции flighting, необходимо назначить серверам Exchange круг 2. Остановка и (или) `Microsoft Exchange Flighting Service (MSExchangeFlighting)` отключение не поддерживается.

В следующем примере сервер назначается кругу 2:

PowerShell

```
Set-ExchangeServer -Identity <ServerName> -RingLevel 2
```

Классификация признаков

Служба тестирования может управлять двумя типами функций: функции с предварительными условиями и компоненты без предварительных требований. Основное различие заключается в том, что некоторые функции зависят от определенных предварительных требований, которые должны быть выполнены:

- Функции с предварительными условиями:
  - Для использования этих функций необходимо выполнить некоторые предварительные условия. Например, на всех серверах Exchange в организации должна выполняться определенная сборка.
  - **Пример**. Подписывание сертификатов полезных данных сериализации PowerShell зависит от допустимого сертификата проверки подлинности, который доступен на всех серверах Exchange.
- Функции без каких-либо предварительных требований:
  - Эти функции работают без зависимостей или предварительных требований. Все, что вам нужно сделать, это установить обновление и включить компонент.
  - **Пример**. Поддержка содержимого, зашифрованного AES256-CBC , не имеет зависимостей или предварительных требований.

Для серверов Exchange Server в кольце 1 функции с предварительными условиями назначаются `FeaturesAwaitingAdminApproval` в состоянии, так как им требуется утверждение администратора, прежде чем они станут активными. В отличие от этого, для серверов Exchange в круге 0 функции с предварительными условиями включены без ожидания утверждения администратора.

Состояния компонентов

Каждому тестируемому компоненту назначается состояние компонента, указывающее текущее состояние компонента. Состояния компонентов являются важным компонентом тестирования компонентов. При запуске функции ей назначается одно или несколько из следующих состояний компонентов:

Развернуть таблицу

Состояние компонента	Функция включена	Описание
FeaturesEnabled	Да	Эта функция включена на сервере.
FeaturesDisabled	Нет	Проверка функций не включила эту функцию на сервере, так как корпорация Майкрософт отозвана ее из-за регрессии или из-за того, что администратор Exchange

Состояние компонента	Функция включена	Описание
		Server заблокировал ее (например, из-за того, что сервер еще не выполнил необходимые предварительные требования).
FeaturesAwaitingAdminApproval	Нет	Эта функция требует явного утверждения администратором Exchange Server.
ФункцииПритвержденные	Да	Администратор Exchange Server явно одобрил эту функцию, и теперь она активна.
FeaturesBlocked	Нет	Эта функция была явно заблокирована администратором Exchange Server и остается в отключенном состоянии.

Например, если компонент ожидает утверждения, ему назначены `FeaturesAwaitingAdminApproval` состояния и `FeaturesDisabled` . Когда администратор утвердит эту функцию, ему назначается `FeaturesApproved` состояние и `FeaturesEnabled` .

> **Совет**
>
> При запуске последней версии скрипта проверки работоспособности Exchange Server отображаются такие сведения, как назначенный сервером круг, а также функции, контролируемые функцией проверки компонентов.

С помощью EMS можно запросить состояния компонентов для определенного сервера Exchange:

PowerShell

```
Get-ExchangeServer -Identity <ServerName> | Format-List Features*
```

Чтобы получить обзор всех доступных функций, используйте командлет Get-ExchangeFeature . Следующая команда возвращает все включенные функции:

PowerShell

```
Get-ExchangeFeature -Status "Enabled"
```

Вы также можете использовать `-FeatureID` параметр вместе с именем компонента, чтобы запросить его состояние и краткое описание:

PowerShell

```
Get-ExchangeFeature -FeatureID "PING.1.0"
```

После выполнения предыдущей команды сервер Exchange server вернет следующий результат:

PowerShell

```
Server              FeatureID   RingLevel  Status                 Description
------              ---------   ---------  ------                 ---------
--
EXCH01              PING.1.0    1          Enabled                Heartbeat
Probe. Validates the Telemetry Channel
```

Эти сведения важны, если вы хотите утвердить новую функцию или изменение, для которого требуется утверждение администратора. Эти сведения также потребуются, если вы хотите запретить включение функции.

Именование компонентов стандартизировано в следующем формате: `<FeatureId>.<SettingId>.<Version>`

Этот формат позволяет компонентам иметь несколько параметров, которые используются для управления им. Предположим, что существует функция `FeatureID=F4` , которой можно управлять с помощью двух переопределений `SettingId=1` параметров и `SettingId=2`, вы увидите следующие записи о тестировании:

- `F4.1.0`
- `F4.2.0`

Чтобы утвердить новую функцию, ожидающую утверждения администратора, используйте Set-ExchangeFeature с параметром `-Approve` . После утверждения или блокировки функции она остается в прерывистом состоянии до следующего цикла тестирования компонентов, который может занять не более часа:

PowerShell

```
Set-ExchangeFeature -Identity <ComputerName> -FeatureID @("F1.1.1") -Approve
```

Кроме того, можно утвердить несколько функций одновременно:

PowerShell

```
Set-ExchangeFeature -Identity <ComputerName> -FeatureID @("F1.1.1",
"F1.2.1", "F2.1.1") -Approve
```

Чтобы запретить включение функции, используйте set-ExchangeFeature с параметром `-Block` . Как показано в предыдущем примере, можно также заблокировать несколько функций одновременно:

PowerShell

```
Set-ExchangeFeature -Identity <ComputerName> -FeatureID @("F1.1.1",
"F1.2.1", "F2.1.1") -Block
```

Пример. Жизненный цикл тестовой функции

В этом разделе показан рабочий процесс и жизненный цикл тестовой функции с именем `Feature1`.

`Contoso` Имеет два сервера Exchange 2019, `EXCHPRD01` `EXCHPRD02` которые входят в группу доступности базы данных (DAG) с именем `DAGPRD01`. У них также есть третий сервер Exchange 2019, `EXCHTST01` который используется для проверки и тестирования новых обновлений и не является членом DAG.

Сначала администратор устанавливает Exchange Server 2019 CU15 на `EXCHTST01` и после успешного завершения всех тестов устанавливает накопительный пакет обновления 15 (CU15) на `EXCHPRD01` и `EXCHPRD02`. Администратор назначает `EXCHTST01` кругу 0, чтобы он получал прокаченные функции и изменения, как только они становятся доступными.

Во-первых, они проверяют текущее назначение круга:

PowerShell

```
Get-ExchangeServer | Format-List Identity,RingLevel

Identity  : EXCHPRD01
RingLevel : 1

Identity  : EXCHPRD02
RingLevel : 1

Identity  : EXCHTST01
RingLevel : 1
```

Затем они назначают `EXCHTST01` кругу 0:

PowerShell

```
Set-ExchangeServer -Identity EXCHTST01 -RingLevel 0

Confirm
Changing the RingLevel of the server will change the flighting of the
features based on the RingLevel selected. Changes will apply once the
flighting service applies these changes. Are you sure you want to continue?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [?] Help (default is "Y"):
```

Несколько месяцев спустя корпорация Майкрософт выпускает SU для CU15. В заметках о выпуске для SU администратор узнает, что su содержит новую функцию для тестирования, `Feature1`. После установки su на всех серверах они хотят убедиться, что `Feature1` включен только на `EXCHTST01` рабочих серверах `EXCHPRD01` `EXCHPRD02`, а не на :

PowerShell

```
Get-ExchangeServer | Get-ExchangeFeature

Server              FeatureID   RingLevel  Status                  Description
------              ---------   ---------  ------                  ---------
EXCHPRD01           PING.1.0    1          Enabled                 Heartbeat
Probe. Validates the Telemetry Channel
EXCHPRD01           F1.1.0      1          Disabled                Feature1
introduces a new functionality
EXCHPRD02           PING.1.0    1          Enabled                 Heartbeat
Probe. Validates the Telemetry Channel
EXCHPRD02           F1.1.0      1          Disabled                Feature1
introduces a new functionality
EXCHTST01           PING.1.0    0          Enabled                 Heartbeat
Probe. Validates the Telemetry Channel
EXCHTST01           F1.1.0      0          Enabled                 Feature1
introduces a new functionality
```

В `EXCHTST01` администратор проверяет, что на их рабочие процессы и сторонние приложения не влияют негативное влияние `Feature1` , и он узнает, что возникла проблема, связанная с `Feature1`. Таким образом, администратор использует следующую команду, чтобы предотвратить `Feature1` включение в круге 1 и отключить ее в круге 0, где он уже активен:

PowerShell

```
Get-ExchangeServer | Set-ExchangeFeature -FeatureID "F1.1.0" -Block

Confirm
Are you sure you want to perform this action?
By running this cmdlet, the features will be updated on server "EXCHTST01".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [?] Help (default is "Y"):
```

Они подтверждают, что `Feature1` успешно заблокирован:

PowerShell

```
Get-ExchangeServer | Get-ExchangeFeature

Server              FeatureID   RingLevel  Status                  ---------
Description
------              ---------   ---------  ------                  ---------
--
EXCHPRD01           PING.1.0    1          Enabled                 Heartbeat
Probe. Validates the Telemetry Channel
EXCHPRD01           F1.1.0      1          Blocked                 Feature1
introduces a new functionality
EXCHPRD02           PING.1.0    1          Enabled                 Heartbeat
Probe. Validates the Telemetry Channel
EXCHPRD02           F1.1.0      1          Blocked                 Feature1
introduces a new functionality
EXCHTST01           PING.1.0    0          Enabled                 Heartbeat
Probe. Validates the Telemetry Channel
EXCHTST01           F1.1.0      0          Blocked                 Feature1
introduces a new functionality
```

Чтобы сообщить о проблеме, служба поддержки Майкрософт контактов Contoso. Корпорация Майкрософт подтверждает проблему и планирует устранить ее в следующем обновлении. После выпуска обновления с исправлением компания Contoso развертывает обновление на своих серверах. Администратор проверяет рабочие процессы и сторонние приложения и подтверждает, что все работает должным образом. Теперь администратор хочет включить на `Feature1` своих рабочих серверах.

Изучив заметки о выпуске с `Feature1` зависимостями, администратор проверяет, требуется ли утверждение администратора:

PowerShell

```
Get-ExchangeServer -Identity EXCHPRD01 | Format-List Features*

FeaturesApproved              : {}
FeaturesAwaitingAdminApproval : {F1.1.0}
FeaturesEnabled               : {PING.1.0}
```

```
FeaturesBlocked               : {}
FeaturesDisabled              : {}
```

Чтобы утвердить и включить `Feature1`, администратор выполняет следующую команду:

PowerShell

```
Get-ExchangeServer -Identity EXCHPRD* | Set-ExchangeFeature -FeatureID
"F1.1.0" -Approve

Confirm
Are you sure you want to perform this action?
By running this cmdlet, the features will be updated on server "EXCHPRD01".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [?] Help (default is "Y"):
```

Затем они проверяют, утверждена ли функция и включена:

PowerShell

```
Get-ExchangeServer -Identity EXCHPRD01 | Format-List Features*

FeaturesApproved              : {F1.1.0}
FeaturesAwaitingAdminApproval : {}
FeaturesEnabled               : {PING.1.0, F1.1.0}
FeaturesBlocked               : {}
FeaturesDisabled              : {}
```

После того как корпорация Майкрософт считает, что все проблемы устранены, она включает эту функцию для всех клиентов по умолчанию. Это произойдет в следующем обновлении, которое включает функцию за пределами тестирования компонентов для всех клиентов.

Диагностические данные

Если общий доступ к данным включен, функция "Проверка компонентов" отправляет диагностические данные в OCS. Эти данные помогают корпорации Майкрософт определить насыщенность тестируемых функций. Дополнительные сведения о том, какие данные собираются и как отключить совместное использование данных, см. в разделе Диагностические данные, собранные для Exchange Server.

Настройка интеграции обмена мгновенными сообщениями с Outlook в Интернете в Exchange

Статья • 04.04.2023

Чтобы настроить интеграцию обмена мгновенными сообщениями между Skype для бизнеса Server и Outlook в Интернете (прежнее название — Outlook Web App) в Exchange 2016 или Exchange 2019, необходимо использовать командную консоль Exchange. В случае предыдущих версий Exchange для этого нужно было изменить файл web.config. Если вы измените файл web.config, а не воспользуетесь рекомендациями из этой статьи, параметры будут проигнорированы и пользователи Outlook в Интернете получат следующее сообщение об ошибке:

```
There's a problem with instant messaging. Please try again later.
```

Кроме того, на сервере Exchange Server будут созданы следующие сообщения о том, что набор средств оценки работоспособности не работает:

- **HealthSet**: `OWA.Protocol.Dep`
- **Тема**: `OWA.Protocol.Dep health set unhealthy (OwaIMInitializationFailedMonitor/OWA.Protocol.Dep) - Owa InstantMessaging provider failed to intialize`
- **Сообщение**: `Owa InstantMessaging provider failed to initialize due to incorrect IM configuration on the server. Signin attempts to OWA IM will fail. Error Message: {Instant Messaging Certificate Thumbprint is null or empty on web.config).`

Используйте процедуры, описанные в этом разделе, чтобы устранить эти ошибки и настроить интеграцию мгновенных сообщений между Skype для бизнеса Server и Exchange 2016 или Exchange 2019. Интеграция обмена мгновенными сообщениями между Lync Server 2013 и Exchange 2016 или более поздней версии не поддерживается. Дополнительные сведения о настройке Skype для бизнеса Server с Outlook в Интернете (ранее — Outlook Web App) см. в статье Настройка интеграции между локальными Skype для бизнеса Server и Outlook Web App

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Для интеграции Exchange и Skype для бизнеса требуются сертификаты сервера, которые являются доверенными для всех участвующих серверов. В этой статье предполагается, что у вас уже есть необходимые сертификаты. Дополнительные сведения см. в статье Планирование интеграции Skype для бизнеса Server 2015 и Exchange. Требуемый отпечаток сертификата для обмена мгновенными сообщениями относится к сертификату Exchange Server, назначенному службе IIS.
- Для выполнения этой процедуры можно использовать только PowerShell. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Параметры виртуального каталога клиентского доступа" в разделе Разрешения клиентов и мобильных устройств .
- В зависимости от топологии Skype для бизнеса Server у вас может быть несколько внешних пулов. Следует выбрать региональную конечную точку (ближайший пул к сайту Exchange AD): `IMServerName=<Skype Server\pool Name>`.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Настройка интеграции IM с Outlook в Интернете при помощи командной консоли Exchange

Шаг 1. Укажите сервер IM и отпечаток сертификата IM

Используйте указанный ниже синтаксис в командной консоли Exchange, чтобы указать сервер IM и отпечаток сертификата IM.

PowerShell

```
New-SettingOverride -Name "<UniqueOverrideName>" -Component OwaServer -
Section IMSettings -Parameters @("IMServerName=<Skype server/pool
name>","IMCertificateThumbprint=<Certificate Thumbprint>") -Reason "
<DescriptiveReason>" [-Server <ServerName>]
```

Примечания:

- Чтобы настроить одинаковые параметры на всех серверах Exchange 2016 и Exchange 2019 в лесу Active Directory, не используйте параметр *Server* .
- Чтобы настроить параметры на определенном сервере Exchange 2016 или Exchange 2019, используйте параметр *Server* и имя сервера (не используйте полное доменное имя или полное доменное имя). Используйте этот метод, чтобы указать различные параметры на различных серверах Exchange Server.

В этом примере указывается отпечаток сервера обмена мгновенными сообщениями и сертификата для обмена мгновенными сообщениями на всех серверах Exchange 2016 и Exchange 2019 в организации.

- **Задание имени переопределения**: "IM Override" (должно быть уникальным)
- **имя сервера Skype для бизнеса**: skype01.contoso.com
- **Отпечаток сертификата**: CDF34A740E9D225A1A06193A9D44B2CE22775308
- **Причина переопределения**: настройка обмена мгновенными сообщениями

PowerShell

```
New-SettingOverride -Name "IM Override"  -Component OwaServer -Section
IMSettings -Parameters
@("IMServerName=skype01.contoso.com","IMCertificateThumbprint=CDF34A740E9D22
5A1A06193A9D44B2CE22775308") -Reason "Configure IM"
```

В этом примере сервер IM и отпечаток сертификата IM указываются только на сервере Mailbox01.

PowerShell

```
New-SettingOverride -Name "Mailbox01 IM Override"  -Component OwaServer -
Section IMSettings -Parameters
@("IMServerName=skype01.contoso.com","IMCertificateThumbprint=CDF34A740E9D22
5A1A06193A9D44B2CE22775308") -Reason "Configure IM" -Server Mailbox01
```

Шаг 2. Обновите параметры обмена мгновенными сообщениями на сервере Exchange Server

Используйте указанный ниже синтаксис в командной консоли Echange, чтобы обновить параметры обмена мгновенными сообщениями на сервере. Это необходимо сделать на каждом сервере Exchange 2016 или Exchange 2019, который используется для Outlook в Интернете.

PowerShell

```
Get-ExchangeDiagnosticInfo -Server <ServerName> -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh
```

В этом примере параметры обмена мгновенными сообщениями обновляются на сервере Mailbox01.

PowerShell

```
Get-ExchangeDiagnosticInfo -Server Mailbox01 -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh
```

Шаг 3. Перезапуск пула Outlook в Интернете на сервере Exchange Server

Выполните указанную ниже команду в командной консоли Exchange или Windows PowerShell на сервере. Это необходимо сделать на каждом сервере Exchange 2016 или Exchange 2019, который используется для Outlook в Интернете.

PowerShell

```
Restart-WebAppPool MSExchangeOWAAppPool
```

Использование командной консоли Exchange для обновления существующей интеграции обмена мгновенными сообщениями с Outlook в Интернете при

обновлении или изменении сертификата IIS Exchange

Шаг 1. Обновление отпечатка сертификата обмена мгновенными сообщениями на существующем переопределении

Используйте следующий синтаксис в командной консоли Exchange, чтобы указать новый отпечаток сертификата обмена мгновенными сообщениями:

PowerShell

```
Set-SettingOverride -Name "<UniqueOverrideName>" -Parameters
@("IMCertificateThumbprint=<Certificate Thumbprint>") -Reason "
<DescriptiveReason>" [-Server <ServerName>]
```

Примечания:

- Чтобы обновить отпечаток на всех серверах Exchange 2016 и Exchange 2019 в лесу Active Directory, не используйте параметр *Server* .
- Чтобы обновить отпечаток на определенном сервере Exchange 2016 или Exchange 2019, используйте параметр *Server* и имя сервера (не используйте полное доменное имя или полное доменное имя). Используйте этот метод, чтобы указать различные параметры на различных серверах Exchange Server.

В этом примере обновляется отпечаток сертификата обмена мгновенными сообщениями на всех серверах Exchange 2016 и Exchange 2019 в организации.

- **Задайте имя переопределения**: "IM Override" (необходимо использовать тот, который уже был на месте из предыдущих шагов, так как мы обновляем, а не создаем новый).
- **имя сервера Skype для бизнеса**: skype01.contoso.com
- **Отпечаток сертификата**: NKT34A740E9D225A1A06193A9D44B2CE22771080
- **Причина переопределения**: настройка обмена мгновенными сообщениями

PowerShell

```
Set-SettingOverride -Name "<UniqueOverrideName>" -Component OwaServer -
Section IMSettings -Parameters @("IMServerName=<Skype server/pool
```

```
name>","IMCertificateThumbprint=<Certificate Thumbprint>") -Reason "
<DescriptiveReason>" [-Server <ServerName>]
```

В этом примере сервер IM и отпечаток сертификата IM указываются только на сервере Mailbox01.

PowerShell

```
Set-SettingOverride -Identity "Mailbox01 IM Override"  -Parameters
@("IMServerName=skype01.contoso.com","IMCertificateThumbprint=NKT34A740E9D22
5A1A06193A9D44B2CE22771080") -Reason "Configure IM" -Server Mailbox01
```

Шаг 2. Обновите параметры обмена мгновенными сообщениями на сервере Exchange Server

Используйте указанный ниже синтаксис в командной консоли Echange, чтобы обновить параметры обмена мгновенными сообщениями на сервере. Это необходимо сделать на каждом сервере Exchange 2016 или Exchange 2019, который используется для Outlook в Интернете.

PowerShell

```
Get-ExchangeDiagnosticInfo -Server <ServerName> -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh
```

В этом примере параметры обмена мгновенными сообщениями обновляются на сервере Mailbox01.

PowerShell

```
Get-ExchangeDiagnosticInfo -Server Mailbox01 -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh
```

Шаг 3. Перезапуск пула Outlook в Интернете на сервере Exchange Server

Выполните указанную ниже команду в командной консоли Exchange или Windows PowerShell на сервере. Это необходимо сделать на каждом сервере Exchange 2016 или Exchange 2019, который используется для Outlook в Интернете.

```
```

PowerShell

```
Restart-WebAppPool MSExchangeOWAAppPool
```

Как проверить, все ли получилось?

Когда интеграция IM с Outlook в Интернете будет настроена, сообщение об ошибке исчезнет и клиенты смогут войти в программу обмена мгновенными сообщениями.

Чтобы проверить значения свойств **IMServerName** и **IMCertificateThumbprint** на сервере Exchange Server, *замените*< *ServerName*> именем сервера (не полным доменным именем) и выполните следующую команду:

PowerShell

```
[xml]$diag=Get-ExchangeDiagnosticInfo -Server <ServerName> -Process
MSExchangeMailboxAssistants -Component VariantConfiguration -Argument
"Config,Component=OwaServer";
$diag.Diagnostics.Components.VariantConfiguration.Configuration.OwaServer.IM
Settings
```

Примечание. В Exchange 2016 с накопительным пакетом обновления 3 (CU3) или более ранней версии для некоторых параметров необходимо использовать разные значения:

- *Процесс*: `Microsoft.Exchange.Directory.TopologyService` (вместо `MSExchangeMailboxAssistants`).
- *Аргумент*: `Config` (вместо `"Config,Component=OwaServer"`).

Изменение расписания создания автономной адресной книги в Exchange

Статья • 04.04.2023

Автономная адресная книга — это копия адресной книги, которая скачивается, чтобы у пользователя Outlook был доступ к сведениям в ней без подключения к серверу. По умолчанию новая автономная адресная адресная область создается каждые 8 часов в Exchange Server 2016 г. и Exchange Server 2019 г., но интервал можно изменить с помощью командной консоли Exchange.

Дополнительные задачи управления, связанные с OAB, см. в разделе Процедуры для автономных адресных книг в Exchange Server.

Что нужно знать перед началом работы

- Предполагаемое время выполнения процедуры: 5 минут.
- Для выполнения этой процедуры можно использовать только PowerShell. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Автономные адресные книги" в разделе разрешения Email адреса и адресной книги.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Изменение графика формирования автономной адресной книги

График формирования автономной адресной книги меняется в два этапа:

1. Изменение графика формирования автономной адресной книги.
2. Применение нового графика формирования автономной адресной книги.

Шаг 1. Изменение графика формирования автономной адресной книги с помощью командной консоли Exchange

Чтобы изменить график формирования автономной адресной книги, используйте следующий синтаксис:

PowerShell

```
New-SettingOverride -Name "<UniqueOverrideName>" -Component
TimeBasedAssistants -Section OABGeneratorAssistant -Parameters @("WorkCycle=
<Timespan>") -Reason "<DescriptiveReason>" [-Server <ServerName>]
```

Примечания:

- Чтобы указать *<значение TimeSpan>* , используйте синтаксис `d.hh:mm:ss`, где *d* = дни, *чч* = часы, *мм* = *минуты и ss* = *секунды* .
- Чтобы настроить расписание создания OAB на всех серверах почтовых ящиков Exchange 2016 и Exchange 2019 в лесу Active Directory, не используйте параметр *Server* .
- Чтобы настроить расписание создания автономной адресной папки на определенном сервере почтовых ящиков Exchange 2016 или Exchange 2019, используйте параметр *Server* и имя сервера (не полное доменное имя или полное доменное имя). Применяйте этот метод, чтобы настроить разные графики на разных серверах Exchange Server.
- В Exchange 2016 с накопительным пакетом обновления 3 (CU3) или более ранней версии значение параметра *Component* имеет значение `MailboxAssistants`.

В этом примере указывается, что автономная адресная запись создается каждые два часа на всех серверах Exchange 2016 и Exchange 2019 в организации, которые отвечают за создание OAB.

- **Задание имени переопределения**: "OAB Generation Override" (должно быть уникальным)
- **WorkCycle**: `02:00:00` (2 часа)

- **Причина переопределения**: создание автономной адресной области каждые 2 часа

```
PowerShell

New-SettingOverride -Name "OAB Generation Override" -Component
TimeBasedAssistants -Section OABGeneratorAssistant -Parameters
@("WorkCycle=02:00:00") -Reason "Generate OAB every 2 hours"
```

Эта команда указывает тот же график формирования автономной адресной книги, но только на сервере Mailbox01.

```
PowerShell

New-SettingOverride -Name "Mailbox01 OAB Generation Override" -Component
TimeBasedAssistants -Section OABGeneratorAssistant -Parameters
@("WorkCycle=02:00:00") -Reason "Generate OAB every 2 hours" -Server
Mailbox01
```

Шаг 2. Применение нового графика формирования автономной адресной книги с помощью командной консоли Exchange

Чтобы применить новый график формирования автономной адресной книги, используйте следующий синтаксис:

```
PowerShell

Get-ExchangeDiagnosticInfo -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh [-Server <ServerName>]
```

Примечания:

- Если вы не использовали параметр *Server* на шаге 1, не используйте его здесь. Если вы использовали параметр *Server* на шаге 1, используйте здесь то же имя сервера.
- Если вы удаляете собственный график формирования автономной адресной книги с помощью командлета **Remove-SettingOverride**, вам все равно нужно выполнить эту команду, чтобы восстановить график формирования по умолчанию (каждые 8 часов).

В этом примере новое расписание создания OAB применяется ко всем серверам почтовых ящиков Exchange 2016 и Exchange 2019 в организации.

PowerShell

```
Get-ExchangeDiagnosticInfo -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh
```

Эта команда применяет новый график формирования автономной адресной книги на сервере Mailbox01.

PowerShell

```
Get-ExchangeDiagnosticInfo -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh -Server Mailbox01
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы настроили расписание создания автономной адресной книги на одном или нескольких серверах Exchange, замените *<serverName>* именем сервера (а не полным доменным именем) и выполните следующую команду, чтобы проверить значение свойства **WorkCycle** :

PowerShell

```
[xml]$diag=Get-ExchangeDiagnosticInfo -Server <ServerName> -Process
MSExchangeMailboxAssistants -Component VariantConfiguration -Argument
"Config,Component=TimeBasedAssistants";
$diag.Diagnostics.Components.VariantConfiguration.Configuration.TimeBasedAss
istants.OABGeneratorAssistant
```

Примечание. В Exchange 2016 CU3 или более ранней версии необходимо выполнить следующую команду: `[xml]$diag=Get-ExchangeDiagnosticInfo -Server <ServerName> -Process Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration -Argument Config; $diag.Diagnostics.Components.VariantConfiguration.Configuration.MailboxAssistants.OABGeneratorAssistant`.

См. также

Процедуры для автономных адресных книг в Exchange Server

Настройка проверки подлинности на основе сертификата в Exchange 2016

Статья • 04.04.2023

Проверка подлинности на основе сертификатов (CBA) в Exchange позволяет Outlook в Интернете (ранее — Outlook Web App) и Exchange ActiveSync клиентам проходить проверку подлинности с помощью сертификатов клиента, а не вводить имя пользователя и пароль.

Прежде чем настраивать Exchange, нужно выдать сертификат клиента каждому пользователю. Так как подобных сертификатов клиентов нужно огромное количество, для их выдачи и управления ими используйте автоматизированную внутреннюю инфраструктуру открытых ключей (PKI), например службы сертификатов Active Directory. Дополнительные сведения об этих службах см. в статье Обзор служб сертификатов Active Directory. Дополнительные сведения о требованиях к сертификатам:

- Для проверки подлинности клиента должен быть выдан сертификат клиента (например, стандартный шаблон сертификата **Пользователь** в службах сертификатов Active Directory).
- В поле **Subject** или **Subject Alternative Name** сертификата должно быть указано имя участника-пользователя (UPN).
- Сертификат клиента должен быть связан с учетной записью пользователя в Active Directory.
- Все серверы и устройства, связанные с доступом к Outlook в Интернете и ActiveSync (в том числе прокси-серверы и клиентские устройства), должны доверять всей цепочке сертификатов клиента (корневому сертификату центра сертификации и возможным сертификатам промежуточных ЦС, которые использовались).

Для CBA в Outlook в Интернете сертификат клиента должен быть установлен на локальном компьютере, устройстве или на смарт-карте. Для CBA в ActiveSync сертификат клиента должен быть установлен на локальном устройстве. Вы можете автоматизировать установку сертификатов на устройствах с помощью решения для управления мобильными устройствами (MDM), например Intune. Дополнительные сведения о Intune см. в статье Обзор Microsoft Intune.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 20 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Диспетчер IIS" в разделе Outlook в Интернете разрешений раздела Разрешения клиентов и мобильных устройств.
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Шаг 1. Установка компонента проверки подлинности с сопоставлением сертификатов клиентов на всех серверах Exchange Server с помощью командной консоли Exchange

Все серверы Exchange Server, использующие общее пространство имен и одинаковые URL-адреса, должны применять одни и те же методы проверки подлинности. Компонент проверки подлинности с сопоставлением сертификатов клиентов необходимо установить на всех серверах Exchange Server.

В командной консоли Exchange выполните следующую команду:

PowerShell

```
Install-WindowsFeature Web-Client-Auth
```

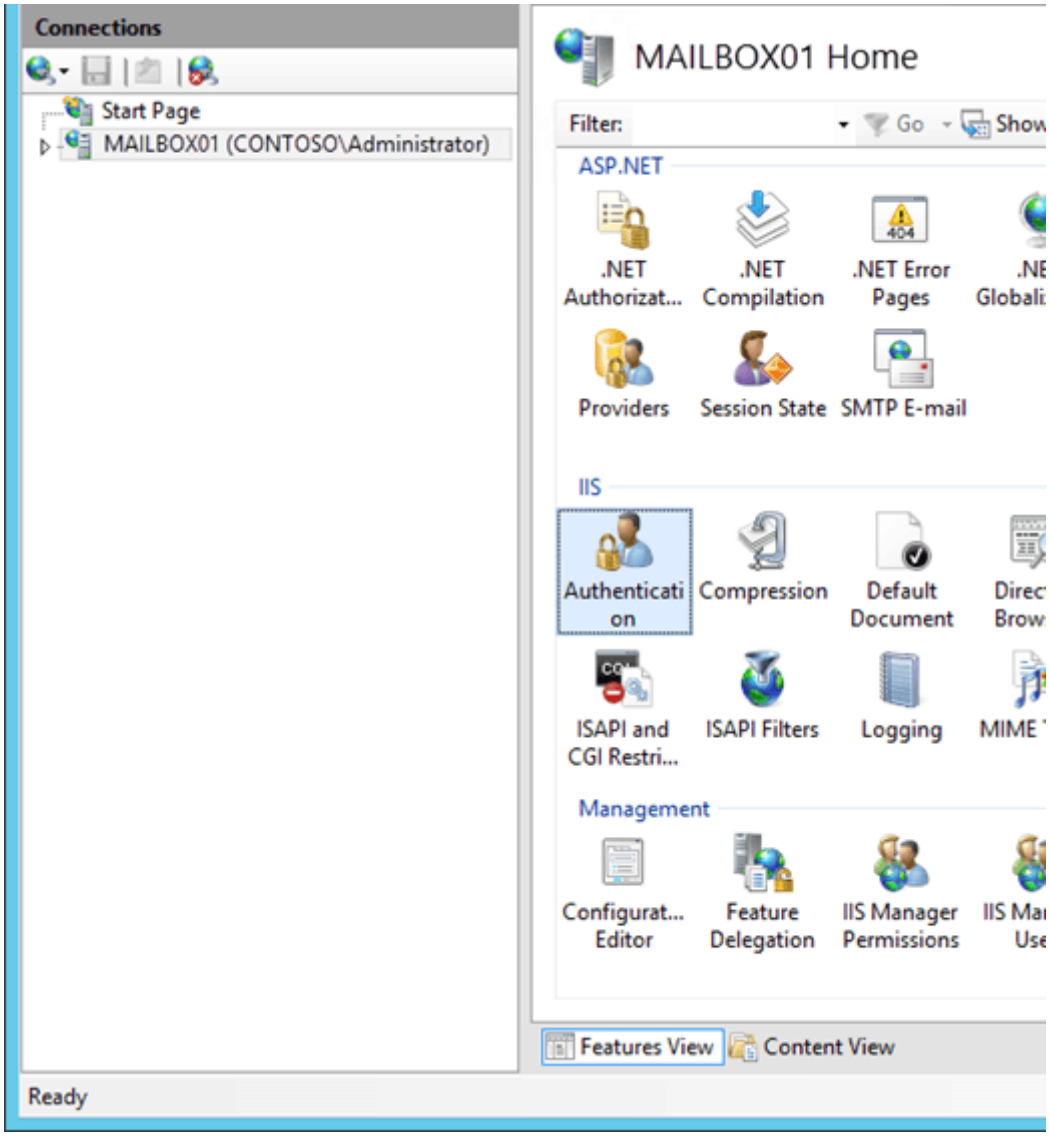
Подробные сведения о синтаксисе и параметрах см. в статье Install-WindowsFeature.

Шаг 2. Включение проверки подлинности на основе сертификата клиента Active Directory для сервера Exchange Server с помощью диспетчера IIS

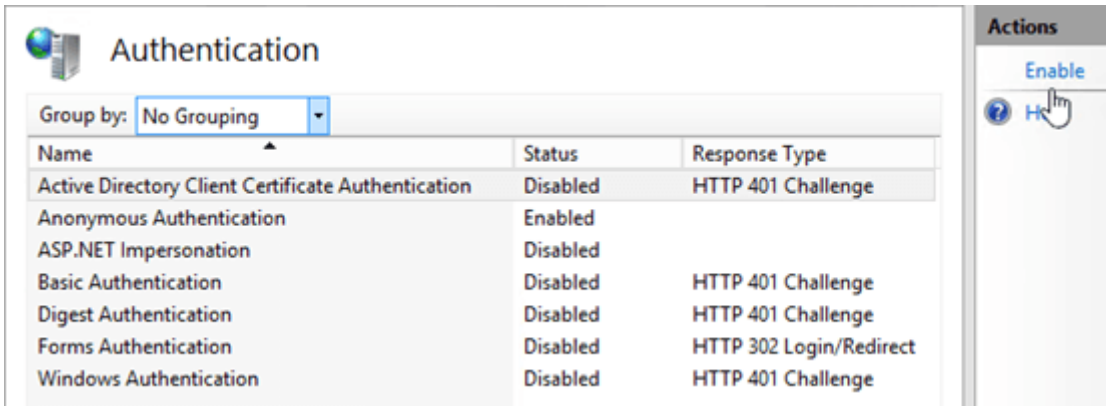
1. Откройте диспетчер IIS на сервере Exchange Server. Простой способ сделать это в Windows Server 2012 или более поздней версии — нажать клавишу Windows + Q, ввести inetmgr и выбрать **Диспетчер служб IIS** в результатах.

2. Выберите сервер, затем в нижней части страницы выберите параметр **Просмотр возможностей**.

3. В разделе **IIS** дважды щелкните элемент **Проверка подлинности**.



4. На странице **Проверка подлинности** выберите из списка пункт **Проверка подлинности клиента Active Directory с помощью сертификата** и щелкните **Включить** в области **Действия**.



Появится предупреждение о том, что для сопоставления сертификатов клиентов в Active Directory необходимо включить SSL.

Шаг 3. Использование диспетчера IIS для настройки Outlook в Интернете, Центра администрирования Exchange и виртуальных каталогов ActiveSync для требования сертификатов клиента

Примечание. Необходимо *требовать* сертификаты клиента, так как *принятие* сертификатов клиента (для поддержки как CBA, так и обычной проверки подлинности имени пользователя и пароля) не работает согласованно на всех типах устройств ActiveSync.

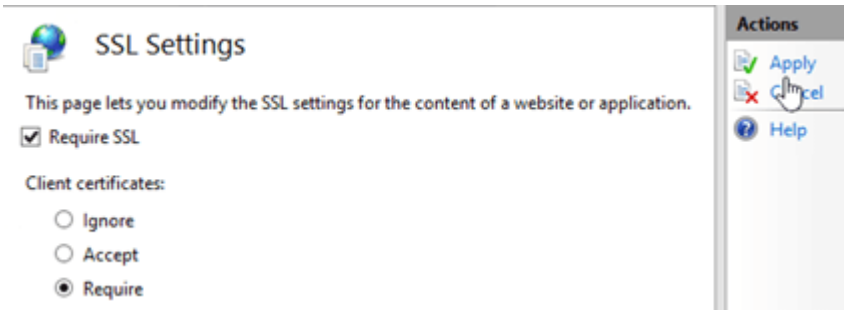
1. In IIS Manager, expand the server, expand **Sites**, and then expand **Default Web Site**.

2. Выберите виртуальный каталог **owa**, затем в нижней части страницы выберите параметр **Просмотр возможностей**.

3. В разделе **IIS** дважды щелкните элемент **Параметры SSL**.

4. На странице **Параметры SSL** установите флажок **Требовать SSL** и выберите значение **Требовать** в разделе **Сертификаты клиентов**.

5. В области **Действия** нажмите кнопку **Применить**.



6. Выберите виртуальный каталог **Microsoft-Server-ActiveSync**.
7. В разделе **IIS** дважды щелкните элемент **Параметры SSL**.
8. На странице **Параметры SSL** установите флажок **Требовать SSL** и выберите значение **Требовать** в разделе **Сертификаты клиентов**.
9. В области **Действия** нажмите кнопку **Применить**.

Примечание. Хотя эти процедуры можно выполнить в командной строке, действия могут не настроить необходимый раздел реестра. Вы можете использовать предыдущие процедуры в диспетчере IIS (который определенно правильно задаст раздел реестра) или убедиться, что для раздела `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters\SslBindingInfo\0.0.0.0:443` реестра задано значение `1` после выполнения процедур в командной строке.

Чтобы выполнить эти процедуры в командной строке, откройте командную строку с повышенными привилегиями на сервере Exchange (открываемое окно командной строки, выбрав **Запуск от имени администратора**) и выполните следующие команды:

Консоль

```
%windir%\system32\inetsrv\appcmd.exe set config "Default Web Site/owa/" -
section:system.webserver/security/access /sslFlags:"Ssl, SslRequireCert"
/commit:apphost
```

Консоль

```
%windir%\system32\inetsrv\appcmd.exe set config "Default Web Site/ecp/" -
section:system.webserver/security/access /sslFlags:"Ssl, SslRequireCert"
/commit:apphost
```

Консоль

```
%windir%\system32\inetsrv\appcmd.exe set config "Default Web Site/Microsoft-Server-ActiveSync/" -section:system.webserver/security/access /sslFlags:"Ssl, SslRequireCert" /commit:apphost
```

Шаг 4. Использование командной консоли Exchange для отключения других методов проверки подлинности в Outlook в Интернете, Центре администрирования Exchange и виртуальных каталогах ActiveSync

После того как для проверки подлинности требуются клиентские сертификаты, необходимо отключить все другие методы проверки подлинности в виртуальных каталогах Outlook в Интернете, Центра администрирования Exchange (EAC) и ActiveSync. По умолчанию включены только обычная проверка подлинности и проверка подлинности на основе форм.

1. В командной консоли Exchange *замените*< *ServerName*> именем сервера Exchange и выполните следующую команду, чтобы отключить все другие методы проверки подлинности в виртуальном каталоге Outlook в Интернете:

   PowerShell

   ```
   Set-OwaVirtualDirectory "<ServerName>\owa (Default Web Site)" -BasicAuthentication $false -WindowsAuthentication $false -DigestAuthentication $false -FormsAuthentication $false -AdfsAuthentication $false -OAuthAuthentication $false
   ```

   Подробные сведения о синтаксисе и параметрах см. в статье Set-OwaVirtualDirectory.

2. В командной консоли Exchange *замените*< *serverName*> именем сервера Exchange и выполните следующую команду, чтобы отключить все другие методы проверки подлинности в виртуальном каталоге EAC:

   PowerShell

   ```
   Set-EcpVirtualDirectory "<ServerName>\ecp (Default Web Site)" -BasicAuthentication $false -WindowsAuthentication $false -DigestAuthentication $false -FormsAuthentication $false -AdfsAuthentication $false
   ```

Подробные сведения о синтаксисе и параметрах см. в разделе Set-EcpVirtualDirectory.

3. Замените <*ServerName*> именем сервера Exchange Server и выполните следующую команду, чтобы отключить все другие методы проверки подлинности в виртуальном каталоге ActiveSync:

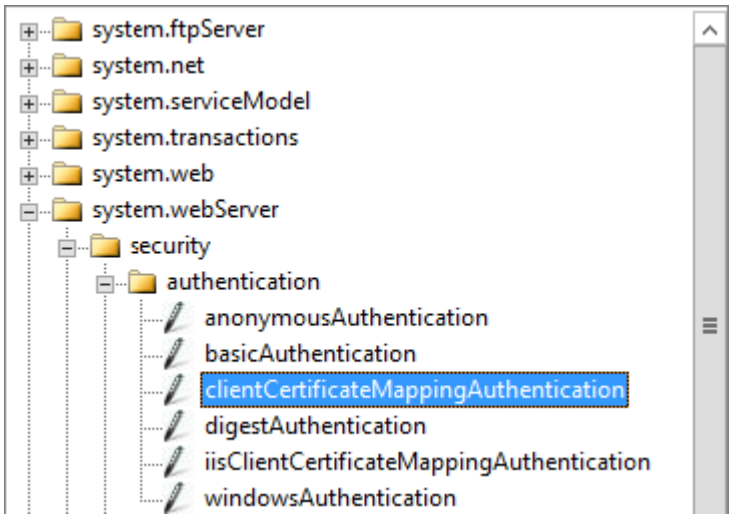
```
PowerShell

Set-ActiveSyncVirtualDirectory "<ServerName>\Microsoft-Server-
ActiveSync (Default Web Site)" -BasicAuthEnabled $false -
WindowsAuthEnabled $false
```

Подробные сведения о синтаксисе и параметрах см. в статье Set-ActiveSyncVirtualDirectory.

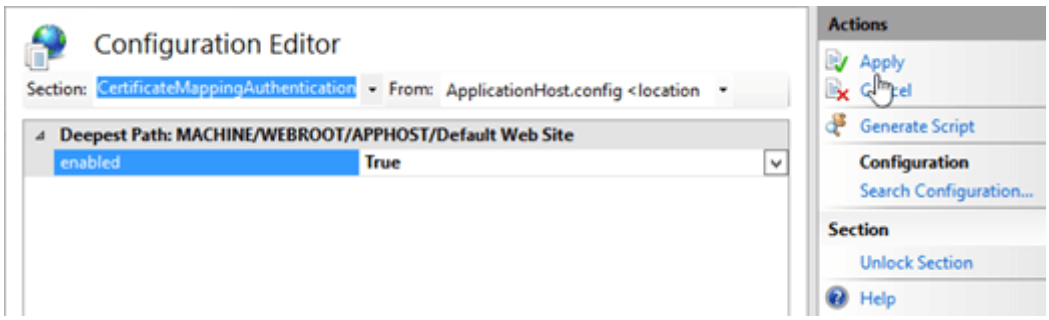
Шаг 5. Использование диспетчера IIS для включения сопоставления сертификатов клиента для Outlook в Интернете, Центра администрирования Exchange и виртуальных каталогов ActiveSync

> ⓘ **Важно!**
>
> После выполнения этого действия выполнение командлета **Set-ActiveSyncVirtualDirectory** может отключить сопоставление сертификатов клиентов для ActiveSync.

1. In IIS Manager, expand the server, expand **Sites**, and then expand **Default Web Site**.
2. Выберите виртуальный каталог **owa**, затем в нижней части страницы выберите параметр **Просмотр возможностей**.
3. В разделе **Управление** дважды щелкните элемент **Редактор конфигураций**.
4. На странице **Редактор конфигурации** щелкните раскрывающийся список **Раздел** и **перейдите к system.webServer>security>authentication>clientCertificateMappingAuthentication**.



5. Установите в строке **enabled** значение **True** и выберите команду **Применить** в области **Действия**.



6. Выберите виртуальный каталог **ECP** .

7. В разделе **Управление** дважды щелкните элемент **Редактор конфигураций**.

8. На странице **Редактор конфигурации** щелкните раскрывающийся список **Раздел** и **перейдите к** **system.webServer>security>authentication>clientCertificateMappingAuthentication**.

9. Установите в строке **enabled** значение **True** и выберите команду **Применить** в области **Действия**.

10. Выберите виртуальный каталог **Microsoft-Server-ActiveSync**.

11. В разделе **Управление** дважды щелкните элемент **Редактор конфигураций**.

12. На странице **Редактор конфигурации** щелкните раскрывающийся список **Раздел** и **перейдите к** **system.webServer>security>authentication>clientCertificateMappingAuthentication**.

13. Установите в строке **enabled** значение **True** и выберите команду **Применить** в области **Действия**.

Примечание. Чтобы выполнить эти процедуры в командной строке, откройте командную строку с повышенными привилегиями на сервере Exchange Server и выполните следующие команды:

Консоль

```
%windir%\system32\inetsrv\appcmd.exe set config "Default Web Site/owa/" -
section:system.webserver/security/authentication/clientCertificateMappingAut
hentication /enabled:"True" /commit:apphost
```

Консоль

```
%windir%\system32\inetsrv\appcmd.exe set config "Default Web Site/ecp/" -
section:system.webserver/security/authentication/clientCertificateMappingAut
hentication /enabled:"True" /commit:apphost
```

Консоль

```
%windir%\system32\inetsrv\appcmd.exe set config "Default Web Site/Microsoft-
Server-ActiveSync/" -
section:system.webserver/security/authentication/clientCertificateMappingAut
hentication /enabled:"True" /commit:apphost
```

Шаг 6 (необязательный). Добавление корневого сертификата стороннего центра сертификации в хранилище Enterprise NTAuth в Active Directory

Выполняйте этот шаг, только если не используете службы сертификатов Active Directory для выдачи сертификатов клиентов. Он необходим для того, чтобы сделать центр сертификации (ЦС) доверенным для выдачи сертификатов клиентов с целью проверки подлинности Active Directory.

1. Экспортируйте корневой сертификат ЦС в CER-файл X.509 с кодировкой Base-64 или двоичной кодировкой DER. В этом примере используется файл C:\Data\CARoot.cer.

2. На любом рядовом сервере домена (например, контроллере домена или сервере Exchange Server) откройте командную строку с повышенными привилегиями и выполните следующую команду:

   Консоль

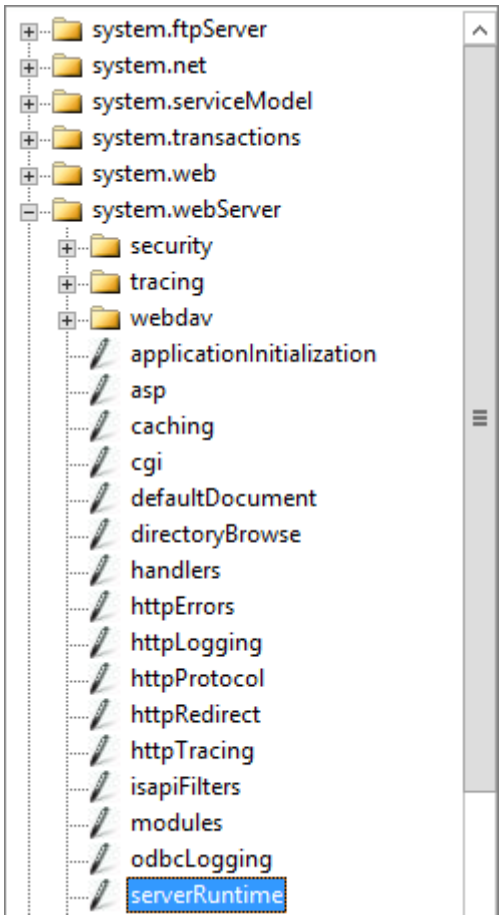
```
%windir%\system32\certutil.exe -enterprise -addstore NTAuth
"C:\Data\CARoot.cer"
```

Обратите внимание на то, что для выполнения этого шага нужно быть членом группы **Администраторы предприятия**.

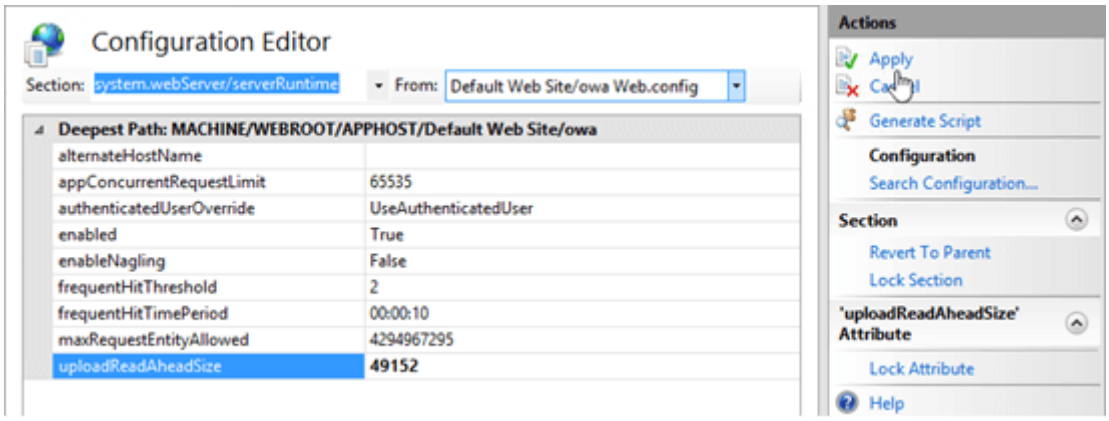
Шаг 7 (необязательный). Увеличение значения UploadReadAheadSize для виртуальных каталогов Outlook в Интернете и ActiveSync с помощью диспетчера IIS

Если клиенты получают ошибки, может потребоваться увеличить значения **uploadReadAheadSize** в метабазе IIS, чтобы разрешить использование заголовков запросов.

1. In IIS Manager, expand the server, expand **Sites**, and then expand **Default Web Site**.
2. Выберите виртуальный каталог **owa**, затем в нижней части страницы выберите параметр **Просмотр возможностей**.
3. В разделе **Управление** дважды щелкните элемент **Редактор конфигураций**.
4. На странице **Редактор конфигурации** щелкните раскрывающийся список **Раздел** и перейдите к **systemwebServer**>**serverRuntime**.



5. Установите значение 49152 в строке **uploadReadAheadSize** и выберите команду **Применить** в области **Действия**.



6. Выберите виртуальный каталог **ECP** .

7. В разделе **Управление** дважды щелкните элемент **Редактор конфигураций**.

8. На странице **Редактор конфигурации** щелкните раскрывающийся список **Раздел** и перейдите к **systemwebServer**>**serverRuntime**.

9. Установите значение 49152 в строке **uploadReadAheadSize** и выберите команду **Применить** в области **Действия**.

10. Выберите виртуальный каталог **Microsoft-Server-ActiveSync**.

11. В разделе **Управление** дважды щелкните элемент **Редактор конфигураций**.
12. На странице **Редактор конфигурации** щелкните раскрывающийся список **Раздел** и перейдите к **systemwebServer**>**serverRuntime**.
13. Установите значение 49152 в строке **uploadReadAheadSize** и выберите команду **Применить** в области **Действия**.

Примечание. Чтобы выполнить эти процедуры в командной строке, откройте командную строку с повышенными привилегиями на сервере Exchange Server и выполните следующие команды:

Консоль

```
%windir%\system32\inetsrv\appcmd.exe set config "Default Web Site/owa/" -
section:system.webserver/serverRuntime /uploadReadAheadSize:49152
```

Консоль

```
%windir%\system32\inetsrv\appcmd.exe set config "Default Web Site/ecp/" -
section:system.webserver/serverRuntime /uploadReadAheadSize:49152
```

Консоль

```
%windir%\system32\inetsrv\appcmd.exe set config "Default Web Site/Microsoft-
Server-ActiveSync/" -section:system.webserver/serverRuntime
/uploadReadAheadSize:49152
```

Включение современной проверки подлинности в локальной среде Exchange

Статья • 23.12.2024

Обзор

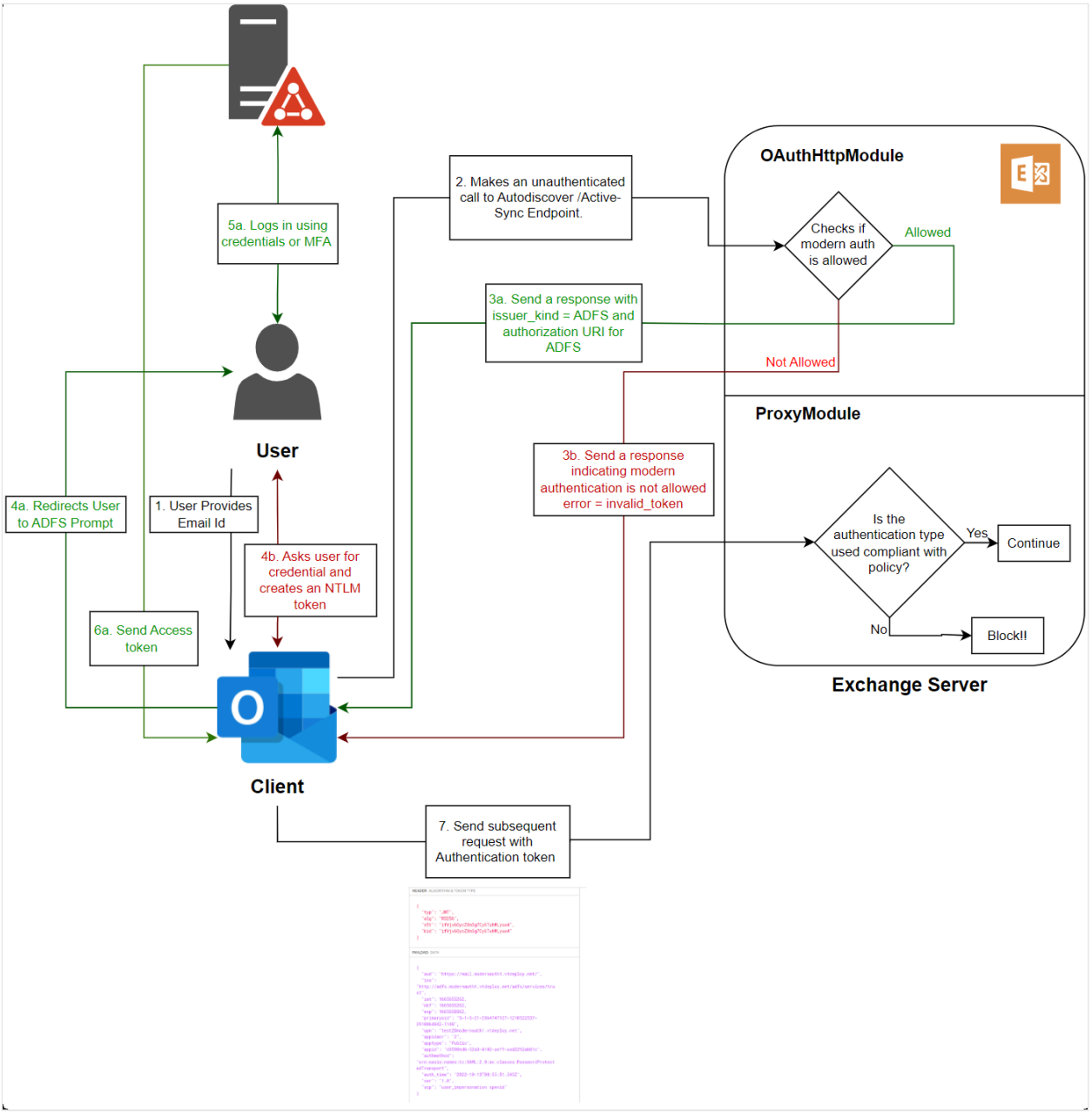
Начиная с **Exchange Server 2019 CU13**, Exchange Server поддерживает `OAuth 2.0` (также называется `Modern Authentication`) для локальных сред, использующих ADFS в качестве службы маркеров безопасности (STS). В этом документе приведены предварительные требования и шаги для включения этой функции.

Современную проверку подлинности в Exchange Server 2019 году не следует путать с гибридной современной проверкой подлинности (HMA), которая использует Microsoft Entra ID для современной проверки подлинности. На самом деле, HMA по-прежнему является рекомендуемым методом для включения современной проверки подлинности для всех локальных и облачных пользователей в гибридной конфигурации Exchange. Эта новая функция позволяет использовать современную проверку подлинности для организаций, которые не имеют Microsoft Entra ID или не находятся в гибридной конфигурации Exchange.

Как будет работать современная проверка подлинности и применима ли эта функция ко мне?

С помощью современной проверки подлинности пользователи могут проходить проверку подлинности в Exchange с помощью ADFS. Если для пользователя включена современная проверка подлинности, клиент Outlook перенаправляется в ADFS. Затем пользователи могут пройти проверку подлинности, предоставив учетные данные или выполнив многофакторную проверку подлинности. После проверки подлинности пользователя ADFS создает маркеры доступа. Exchange Server проверяет эти маркеры доступа для предоставления клиентского доступа к почтовому ящику пользователя.

На следующей схеме показана координация между Exchange Server, ADFS и Outlook для проверки подлинности пользователя с помощью современной проверки подлинности.



На предыдущей диаграмме шаги `3a`, `4a` и `5a` `6a` происходят, когда для конечного пользователя включена современная проверка подлинности. Шаги `3b` выполняются `4b` , когда современная проверка подлинности отключена для пользователя.

Ознакомьтесь со следующей таблицей, чтобы оценить, применима ли эта функция для вас.

Развернуть таблицу

Конфигурация Exchange	Применима ли эта функция?	Замечания
Локальная организация Exchange только с Exchange Server 2019 г.	Да	Н/Д

Конфигурация Exchange	Применима ли эта функция?	Замечания
Локальная организация Exchange с сочетанием Exchange Server 2019, Exchange Server 2016 и Exchange Server 2013	Нет	Exchange Server 2013 не поддерживается.
Локальная организация Exchange с сочетанием Exchange Server 2019 и Exchange Server 2016	Да	В качестве серверов Front-End (клиентский доступ) можно использовать только серверы Exchange 2019.
Гибридная организация Exchange с использованием HMA	Нет	Предпочтительным решением является HMA с использованием Microsoft Entra ID. Ознакомьтесь с руководством по использованию новых политик проверки подлинности.
Гибридная организация Exchange без HMA	Нет	Используйте HMA с Microsoft Entra ID.

Предварительные требования для включения современной проверки подлинности в Exchange

Exchange Server 2019 CU13 или более поздней версии

Чтобы использовать современную проверку подлинности, все серверы, используемые для клиентских подключений, должны иметь Exchange Server 2019 с накопительным пакетом обновления 13 (CU13).

ADFS 2019 или более поздней версии

Чтобы включить современную проверку подлинности в локальной среде Exchange, требуется службы федерации Active Directory (AD FS) (ADFS) в Windows Server 2019 или более поздней версии. Установка и настройка роли ADFS на Exchange Server не поддерживается. Дополнительные сведения см. в статье Планирование топологии развертывания AD FS.

Для включения клиентского доступа извне корпоративной сети также может потребоваться веб-сервер Application Proxy (Windows Server 2019 г. или более поздней версии). Дополнительные сведения см. в разделе Настройка веб-Application Proxy можно настроить для доступа к экстрасети (необязательно).

Предварительные требования для клиента

Для использования современной проверки подлинности пользователям требуются клиентские приложения, такие как Outlook или другие собственные клиенты операционной системы, совместимые с современной проверкой подлинности через ADFS.

Outlook для Windows

Поддержка современной проверки подлинности через ADFS доступна в следующих версиях `Microsoft Outlook for Windows`. Клиент Microsoft Outlook Для Windows, начиная с номера `16.0.17628.10000` сборки, использует последнюю версию `MSAL library` для проверки подлинности. Чтобы убедиться, что используется самый актуальный стек проверки подлинности, рекомендуется установить последнюю версию:

Outlook в Приложения Microsoft 365:

Развернуть таблицу

Канал	Поддерживается	Версия	Сборка (или более поздняя версия)
Канал предварительной оценки	Да	2304	16327.20200
Актуальный канал	Да	2304	16327.20214
Ежемесячный канал (корпоративный)	Да	2304	16327.20324
Полугодовой канал (предварительная корпоративная версия)	Да	2402	17328.20184
Полугодовой канал (корпоративный)	Да	2402	17328.20452

Outlook для Windows (корпоративная лицензия & розничной торговли):

Развернуть таблицу

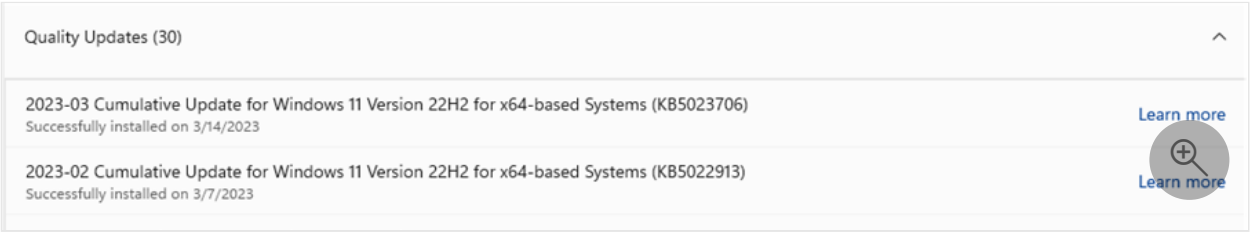
Версия	Поддерживается	Версия	Сборка (или более поздняя версия)
Outlook 2016 (любая версия)	Нет	Н/Д	Н/Д
Outlook 2019 (любая версия)	Нет	Н/Д	Н/Д
Outlook 2021 (розничная версия)	Да	2304	16327.20214
Outlook 2021 (том)	Нет	Н/Д	Н/Д
Outlook 2024 (розничная версия)	Да	2410	18129.20158
Outlook 2024 (том)	Да	2408	17932.20162

Вы можете проверка номер сборки Office, выполнив указанные здесь действия.

ОС Windows

Клиент Windows должен быть `Windows 11 22H2 or later` установлен, и на нем должно быть установлено обновление от 14 марта 2023 г.

Вы можете просмотреть журнал клиентский компонент Центра обновления Windows, чтобы убедиться, что `KB5023706` установлен.



Платформы Apple

Поддержка современной проверки подлинности через ADFS также доступна в `Apple Mail` приложении в `macOS Sequoia` и `iOS 17.6.1` более поздней версии.

Протоколы, работающие с современной проверкой подлинности ADFS

В следующей таблице описаны протоколы, к которым можно получить доступ с помощью маркеров современной проверки подлинности ADFS. Мы постоянно работаем над добавлением поддержки современной проверки подлинности ADFS в более Exchange Server протоколы.

Развернуть таблицу

Протокол	Поддержка современной проверки подлинности ADFS
MAPI через HTTP (MAPI/HTTP)	Да
Outlook Anywhere (RPC/HTTP)	Нет
Exchange Active Sync (EAS)	Да
Веб-службы Exchange (EWS)	Да
Outlook в Интернете (OWA)	Да (проверка подлинности на основе утверждений)
Центр Администратор Exchange (ECP)	Да (проверка подлинности на основе утверждений)
автономная адресная книга (OAB);	Да
IMAP	Нет
POP	Нет

Действия по настройке современной проверки подлинности в Exchange Server с использованием ADFS в качестве службы stS

В этом разделе содержатся сведения о реализации современной проверки подлинности в Exchange Server 2019 с накопительным пакетом обновления 13 (CU13).

Установите Exchange 2019 с накопительным пакетом обновления 13 (CU13) на всех серверах FE (по крайней мере)

Все серверы, используемые для клиентских подключений, должны быть обновлены до Exchange 2019 с накопительным пакетом обновления 13 (CU13). Такой подход

гарантирует, что начальные клиентские подключения к Exchange 2019 используют OAuth, а прокси-подключения для Exchange Server 2016 — Kerberos.

В Exchange 2019 CU13 добавлена поддержка новых политик проверки подлинности, позволяющих разрешить или заблокировать современную проверку подлинности на уровне пользователя. Блокировка современной проверки подлинности используется для обеспечения того, чтобы клиенты, которые не поддерживают современную проверку подлинности, по-прежнему могли подключаться.

Запуск `/PrepareAD` с программой установки требуется для добавления нескольких новых параметров политики проверки подлинности в Exchange Server.

1. `BlockModernAuthActiveSync`
2. `BlockModernAuthAutodiscover`
3. `BlockModernAuthImap`
4. `BlockModernAuthMapi`
5. `BlockModernAuthOfflineAddressBook`
6. `BlockModernAuthPop`
7. `BlockModernAuthRpc`
8. `BlockModernAuthWebServices`

После установки CU13 или более поздней версии все существующие политики проверки подлинности (включая политику проверки подлинности по умолчанию) отключат параметры. Это означает, что если вы уже используете HMA, вам не нужно изменять ранее существующие политики проверки подлинности.

Новая политика проверки подлинности для гибридного развертывания Exchange не требуется

Существующие гибридные конфигурации Exchange **должны использовать гибридную современную проверку подлинности (HMA).** Гибридные установки с использованием HMA могут оставить значения `BlockModernAuth*` параметров на уровне , `0` чтобы продолжить использование HMA. Действия, описанные по настройке современной проверки подлинности с помощью ADFS, актуальны только для организаций, которые не используют гибридную среду Exchange и являются исключительно локальными.

Настройка службы федерации Active Directory (AD FS) (ADFS)

Необходимо установить и настроить ADFS в среде, чтобы разрешить клиентам Exchange использовать проверку подлинности Forms (OAuth) для подключения к Exchange Server. Ознакомьтесь с контрольным списком: настройка сервера федерации , чтобы помочь в настройке ADFS.

Компонент ADFS можно установить, выполнив следующую команду в окне PowerShell с повышенными привилегиями на новом сервере, который становится сервером ADFS:

PowerShell

```
Install-WindowsFeature ADFS-Federation -IncludeManagementTools
```

Требования к сертификатам для конфигурации ADFS в организации Exchange Server

Для ADFS требуются два основных типа сертификатов (подробные сведения см. в этой статье):

1. Обмен данными между службами SSL-сертификатом для зашифрованного трафика веб-служб между сервером ADFS, клиентами, серверами Exchange и необязательным сервером веб-Application Proxy. Рекомендуется использовать сертификат, выданный внутренним или коммерческим центром сертификации (ЦС), так как все клиенты должны доверять этому сертификату.
2. Сертификат подписи маркеров для зашифрованного обмена данными и проверки подлинности между сервером ADFS, контроллерами домена Active Directory и серверами Exchange. Вы можете получить сертификат подписи маркеров, запросив его в ЦС или создав самозаверяющий сертификат.

Дополнительные сведения о создании и импорте SSL-сертификатов в Windows см. в разделе Серверные сертификаты.

Ниже приведена сводка сертификатов, которые мы используем в этом сценарии:

Развернуть таблицу

Общее имя (CN) в сертификате (в поле Тема, Альтернативное имя субъекта или совпадение сертификата с подстановочными знаками)	Тип	Требуется на серверах	Comments
adfs.contoso.com enterpriseregistration.contoso.com	Выдано ЦС	Сервер ADFS, Сервер веб-Application Proxy (необязательно)	Серверы федерации используют SSL-сертификат для защиты трафика веб-служб для связи SSL с клиентами и прокси-серверами федерации. Поскольку сертификат SSL должен быть доверенным для клиентских компьютеров, мы рекомендуем использовать сертификат, подписанный надежным центром сертификации. Все выбранные вами сертификаты должны иметь соответствующий закрытый ключ.
Подписывание маркера ADFS — adfs.contoso.com	Самозаверяющий или проблема в ЦС	Сервер ADFS, Сервер веб-Application Proxy (необязательно)	Сертификат подписи маркера — это сертификат X509. Серверы федерации используют связанные пары открытого и закрытого ключей для цифровой подписи всех создаваемых ими

Общее имя (CN) в сертификате (в поле Тема, Альтернативное имя субъекта или совпадение сертификата с подстановочными знаками)	Тип	Требуется на серверах	Comments
			маркеров безопасности. Этот процесс включает подписывание опубликованных метаданных федерации и запросов на разрешение артефактов. В оснастке "Управление ADFS" можно настроить несколько сертификатов подписи маркеров, чтобы разрешить переключение сертификатов, когда срок действия одного сертификата близок к истечении срока действия. По умолчанию все сертификаты в списке публикуются, но только основной сертификат подписи маркеров используется ADFS для подписывания маркеров. Все выбранные вами сертификаты должны иметь

Общее имя (CN) в сертификате (в поле Тема, Альтернативное имя субъекта или совпадение сертификата с подстановочными знаками)	Тип	Требуется на серверах	Comments
			соответствующий закрытый ключ. Вы можете получить сертификат подписи маркеров, запросив его в корпоративном ЦС или общедоступном ЦС или создав самозаверяющий сертификат.
mail.contoso.com autodiscover.contoso.com	Выдано ЦС	Серверы Exchange, Сервер веб-Application Proxy (необязательно)	Этот сертификат является типичным сертификатом, который используется для шифрования внешних клиентских подключений к Outlook в Интернете (и другим службам Exchange). Дополнительные сведения см. в статье Требования к сертификатам для служб Exchange.

Развертывание и настройка сервера ADFS

Используйте Windows Server 2019 или более поздней версии для развертывания сервера ADFS. Выполните действия, описанные в статьях Развертывание сервера ADFS и Настройка и тестирование сервера ADFS . Убедитесь, что URL-адрес

метаданных федерации можно получить в веб-браузере как с сервера Exchange Server, так и с одного клиентского компьютера.

В URL-адресе используется следующий синтаксис: `https://<FederationServiceName>/federationmetadata/2007-06/federationmetadata.xml`

Пример: `https://adfs.contoso.com/federationmetadata/2007-06/federationmetadata.xml`

Настройка метода проверки подлинности в ADFS

Чтобы использовать современную проверку подлинности в Outlook в Windows, необходимо настроить `Primary Authentication Methods`. Рекомендуется выбрать `Forms Authentication` как для , так `Extranet` и `Intranet` для . Эту настройку можно выполнить, выполнив следующие команды из окна PowerShell на сервере ADFS:

PowerShell

```
Set-AdfsGlobalAuthenticationPolicy -PrimaryIntranetAuthenticationProvider
FormsAuthentication
Set-AdfsGlobalAuthenticationPolicy -PrimaryExtranetAuthenticationProvider
FormsAuthentication
```

Выбор подходящего времени существования единого входа

Выберите подходящее время существования единого Sign-On (SSO), чтобы конечным пользователям не требовалось часто выполнять повторную проверку подлинности. Чтобы проверить текущую конфигурацию времени существования единого входа, откройте новое окно PowerShell на сервере ADFS и выполните следующую команду:

PowerShell

```
Get-AdfsProperties | Format-List SsoLifetime, PersistentSsoLifetimeMins,
KmsiLifetimeMins, DeviceUsageWindowInDays, KmsiEnabled,
PersistentSsoEnabled, BrowserSsoEnabled
```

Используйте командлет Set-AdfsProperties , чтобы настроить соответствующие значения для `SsoLifetime`, `PersistentSsoLifetimeMins`, `KmsiLifetimeMins` и `DeviceUsageWindowInDays`. Эти параметры следует настроить, чтобы включить единый вход и определить срок его действия. В зависимости от режима единого входа, например `Keep Me Signed In (KMSI)` или `Device registration`, также может

потребоваться включить `KsmiEnabled` и `PersistentSsoEnabled`. Дополнительные сведения о едином входе ADFS см. в документации по параметрам AD FS 2016 Единый вход.

Настройка регистрации устройств в ADFS

Рекомендуется включить эту функцию `Device Registration` в ADFS, чтобы воспользоваться улучшенным интерфейсом единого входа. Чтобы включить `Device Registration`, выполните действия, описанные в документации по настройке сервера федерации с помощью службы регистрации устройств .

Затем выполните все действия по настройке `Device Registration Service Discovery` и `Device Registration Discovery Server SSL certificate`, как описано в документации по настройке регистрации устройств .

Чтобы использовать регистрацию устройства, конечные пользователи должны присоединить свое устройство к workplace. Дополнительные сведения см. в следующей документации:

- Пошаговое руководство. Присоединение к рабочему месту с помощью устройства Windows
- Пошаговое руководство. Присоединение к рабочему месту с устройством iOS
- Пошаговое руководство. Присоединение рабочего места к устройству Android

Убедитесь, что регистрация устройства настроена и проверка подлинности устройства включена, проверив `Device Registration Overview`. Этот шаг рекомендуется для сокращения количества запросов на проверку подлинности для пользователей и может помочь применить политики контроль доступа в ADFS.

Настройка KSMI в ADFS

Если вы предпочитаете не использовать `Device Registration` или не можете это сделать, вы можете включить эту функцию `Keep Me Signed In` . Затем ADFS создает постоянный файл cookie сразу после проверки подлинности пользователя, устраняя необходимость повторной проверки подлинности в последующих сеансах при условии, что файл cookie остается действительным.

Срок действия маркера обновления равен времени существования файла cookie постоянного единого входа для `Keep me signed in`. Постоянное время существования файла cookie единого входа по умолчанию составляет один день и не более семи дней. В противном случае время существования маркера

обновления равно времени существования файла cookie единого входа сеанса (по умолчанию 8 часов). Дополнительные сведения о KSMI см. в документации по параметрам единого входа AD FS .

KMSI отключен по умолчанию и может быть включен, задав для свойства `KmsiEnabled` ADFS значение `True`. Обязательно выполните следующие действия в окне PowerShell на сервере ADFS:

```
PowerShell

Set-AdfsProperties -EnableKmsi $true
```

Если ПАРАМЕТР KMSI отключен, период единого входа по умолчанию — `8 hours`. Период единого входа можно настроить с помощью свойства `SsoLifetime`. Свойство измеряется в минутах, поэтому его значение по умолчанию : `480`

```
PowerShell

Set-AdfsProperties -SsoLifetime <LifetimeInMinutes>
```

Если включено KMSI, период единого входа по умолчанию — `24 hours`. Период единого входа с включенным KMSI можно настроить с помощью свойства `KmsiLifetimeMins`. Свойство измеряется в минутах, поэтому его значение по умолчанию : `1440`

```
PowerShell

Set-AdfsProperties -KmsiLifetimeMins <LifetimeInMinutes>
```

Создание группы приложений Outlook ADFS

Если вы впервые настраиваете современную проверку подлинности ADFS в локальной среде Exchange, выполните действия, описанные в этом разделе руководства. Если у вас есть конфигурация современной проверки подлинности ADFS, настроенная до поддержки клиентов, отличных `Microsoft Outlook for Windows` от , см. действия, описанные в разделе Обновление существующей группы приложений Outlook ADFS этой документации. Следующие команды PowerShell должны выполняться из окна PowerShell на сервере ADFS. Если вы не планируете использовать приложения iOS и macOS, например собственное приложение Apple Mail, можно пропустить создание собственного клиентского приложения ADFS для iOS и macOS. Однако мы рекомендуем создавать их ради полноты.

Сначала мы создадим `ADFS Application Group`:

PowerShell

```
New-AdfsApplicationGroup -Name "Outlook" -ApplicationGroupIdentifier
"Outlook" -Disabled:$false
```

Далее мы создадим еще `Scopes` - `EAS.AccessAsUser.All` три и : `EWS.AccessAsUser.All` `offline_access`

PowerShell

```
Add-AdfsScopeDescription -Name "EAS.AccessAsUser.All" -Description "EAS
scope"
Add-AdfsScopeDescription -Name "EWS.AccessAsUser.All" -Description "EWS
scope"
Add-AdfsScopeDescription -Name "offline_access" -Description "Offline
Access"
```

Теперь мы создадим два `Native Client Applications` - `Outlook - Native application` и : `iOS and macOS - Native mail application`

PowerShell

```
Add-AdfsNativeClientApplication -Name "Outlook - Native application" -
ApplicationGroupIdentifier "Outlook" -Identifier "d3590ed6-52b3-4102-aeff-
aad2292ab01c" -RedirectUri @("ms-appx-
web://Microsoft.AAD.BrokerPlugin/d3590ed6-52b3-4102-aeff-
aad2292ab01c","msauth.com.microsoft.Outlook://auth","urn:ietf:wg:oauth:2.0:o
ob")
Add-AdfsNativeClientApplication -Name "iOS and macOS - Native mail
application" -ApplicationGroupIdentifier "Outlook" -Identifier "f8d98a96-
0999-43f5-8af3-69971c7bb423" -RedirectUri @("com.apple.mobilemail://oauth-
redirect","com.apple.preferences.internetaccounts://oauth-
redirect/","com.apple.Preferences://oauth-redirect/")
```

В качестве следующего шага мы создадим `Web Api Applications`. Мы создаем одно приложение для каждого URI, которое используется в среде Exchange Server. Если вы используете, например, `autodiscover.contoso.com` и `mail.contoso.com`, необходимо создать два `Web Api Applications`. Обязательно замените URI в следующем примере на URI, которые используются в настройке. Важно убедиться, что все URI для клиента охвачены. Включите конечный код `/` и убедитесь, что URI начинаются с `https://`:

PowerShell

```
# Replace the URIs with your URIs
$exchangeServerServiceFqdns =
@("https://autodiscover.contoso.com/","https://mail.contoso.com/")

$issuanceTransformRules = @"
@RuleName = "ActiveDirectoryUserSID"
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"]
 => issue(claim = c);

@RuleName = "ActiveDirectoryUPN"
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"]
 => issue(claim = c);

@RuleName = "AppIDACR"
 => issue(Type = "appidacr", Value = "2");

@RuleName = "SCP"
 => issue(Type = "scp", Value = "user_impersonation");

@RuleName = "SCPEAS"
 => issue(Type = "scp", Value = "EAS.AccessAsUser.All");

@RuleName = "SCPEWS"
 => issue(Type = "scp", Value = "EWS.AccessAsUser.All");

@RuleName = "offlineaccess"
 => issue(Type = "scp", Value = "offline_access");
"@
foreach ($fqdn in $exchangeServerServiceFqdns) {
    Add-AdfsWebApiApplication -Name "Outlook - Web API ($((New-
Guid).ToString("N")))" -ApplicationGroupIdentifier "Outlook" -Identifier
$fqdn -IssuanceTransformRules $issuanceTransformRules -
AccessControlPolicyName "Permit Everyone"
}
```

В качестве последнего шага мы добавим разрешения клиента для всех в `Native Client Applications` существующем `Web Api Applications`:

PowerShell

```
$clientRoleIdentifier = @("f8d98a96-0999-43f5-8af3-69971c7bb423","d3590ed6-
52b3-4102-aeff-aad2292ab01c")
(Get-AdfsWebApiApplication -ApplicationGroupIdentifier "Outlook") | ForEach-
Object {
    [string]$serverRoleIdentifier = $_.Identifier
    foreach ($id in $clientRoleIdentifier) {
        Grant-AdfsApplicationPermission -ClientRoleIdentifier $id -
ServerRoleIdentifier $serverRoleIdentifier -ScopeNames
"winhello_cert","email","profile","vpn_cert","logon_cert","user_impersonatio
n","allatclaims","offline_access","EAS.AccessAsUser.All","EWS.AccessAsUser.A
ll","openid","aza"
```

```
    }
}
```

Обновление существующей группы приложений Outlook ADFS

> **ⓘ Важно!**
>
> Пропустите действия, описанные в этом разделе, если у вас нет существующей группы приложений Outlook ADFS, которая была настроена до поддержки клиентов, отличных `Microsoft Outlook for Windows` от появившегося.

Если у вас есть существующая конфигурация группы приложений Outlook ADFS, которая была настроена до поддержки клиентов, отличных `Microsoft Outlook for Windows` от появившегося, выполните приведенные здесь действия, чтобы включить поддержку других платформ. Следующие команды PowerShell должны выполняться из окна PowerShell на сервере ADFS.

Сначала мы создадим три дополнительных `Scopes` - `EAS.AccessAsUser.All` и `offline_access` `EWS.AccessAsUser.All` :

PowerShell

```
Add-AdfsScopeDescription -Name "EAS.AccessAsUser.All" -Description "EAS
scope"
Add-AdfsScopeDescription -Name "EWS.AccessAsUser.All" -Description "EWS
scope"
Add-AdfsScopeDescription -Name "offline_access" -Description "Offline
Access"
```

Теперь мы создадим новый `Native Client Applications` - `iOS and macOS - Native mail application` объект :

PowerShell

```
Add-AdfsNativeClientApplication -Name "iOS and macOS - Native mail
application" -ApplicationGroupIdentifier "Outlook" -Identifier "f8d98a96-
0999-43f5-8af3-69971c7bb423" -RedirectUri @("com.apple.mobilemail://oauth-
redirect","com.apple.preferences.internetaccounts://oauth-
redirect/","com.apple.Preferences://oauth-redirect/")
```

Мы обновляем существующий `Native Client Application` - `Outlook - Native application` объект . Обязательно замените `TargetName` на целевое имя, которое вы

используете в существующей конфигурации:

PowerShell

```
Set-AdfsNativeClientApplication -TargetName "Outlook - Native application" -
RedirectUri @("ms-appx-web://Microsoft.AAD.BrokerPlugin/d3590ed6-52b3-4102-
aeff-
aad2292ab01c","msauth.com.microsoft.Outlook://auth","urn:ietf:wg:oauth:2.0:o
ob")
```

В качестве следующего шага необходимо создать по одному `Web Api Application` для каждого `Identifier` (URI), который используется в среде Exchange Server и существует в текущей конфигурации современной проверки подлинности ADFS:

PowerShell

```
$duplicateFqdnHashSet = New-Object
System.Collections.Generic.HashSet[string]
$issuanceTransformRules = @"
@RuleName = "ActiveDirectoryUserSID"
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"]
 => issue(claim = c);

@RuleName = "ActiveDirectoryUPN"
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"]
 => issue(claim = c);

@RuleName = "AppIDACR"
 => issue(Type = "appidacr", Value = "2");

@RuleName = "SCP"
 => issue(Type = "scp", Value = "user_impersonation");

@RuleName = "SCPEAS"
 => issue(Type = "scp", Value = "EAS.AccessAsUser.All");

@RuleName = "SCPEWS"
 => issue(Type = "scp", Value = "EWS.AccessAsUser.All");

@RuleName = "offlineaccess"
 => issue(Type = "scp", Value = "offline_access");
"@
(Get-AdfsWebApiApplication -ApplicationGroupIdentifier "Outlook") | ForEach-
Object {
    if ($_.Identifier.Count -gt 1) {
        Write-Host "[+] More than one identifier was found in Web Api
Application: $($_.Name)" -ForegroundColor Yellow
        $_.Identifier | Select-Object -Skip 1 | ForEach-Object {
            Write-Host "[+] Identifier $_ must be added to a new Web Api
Application and will now be removed from the existing one" -ForegroundColor
Yellow
```

```
            [void]$duplicateFqdnHashSet.Add($_)
        }

        Set-AdfsWebApiApplication -TargetName $_.Name -Identifier
($_.Identifier)[0] -IssuanceTransformRules $issuanceTransformRules -
AccessControlPolicyName "Permit Everyone"
    }
}

foreach($identifier in $duplicateFqdnHashSet) {
    Write-Host "[+] Creating a new Web Api Application for: $identifier" -
ForegroundColor Yellow
    Add-AdfsWebApiApplication -Name "Outlook - Web API ($((New-
Guid).ToString("N")))" -ApplicationGroupIdentifier "Outlook" -Identifier
$identifier -IssuanceTransformRules $issuanceTransformRules -
AccessControlPolicyName "Permit Everyone"
    Write-Host "[+] Done!`r`n" -ForegroundColor Green
}
```

В качестве последнего шага мы добавим разрешения клиента для всех в `Native Client Applications` существующем `Web Api Applications`:

PowerShell

```
$clientRoleIdentifier = @("f8d98a96-0999-43f5-8af3-69971c7bb423","d3590ed6-
52b3-4102-aeff-aad2292ab01c")
$requiredScopes =
@("winhello_cert","email","profile","vpn_cert","logon_cert","user_impersonat
ion","allatclaims","offline_access","EAS.AccessAsUser.All","EWS.AccessAsUser
.All","openid","aza")

(Get-AdfsWebApiApplication -ApplicationGroupIdentifier "Outlook") | ForEach-
Object {
    [string]$serverRoleIdentifier = $_.Identifier
    Write-Host "[+] Processing Server Role: $serverRoleIdentifier" -
ForegroundColor Yellow
    foreach ($id in $clientRoleIdentifier) {
        Write-Host "[+] Processing Client Role: $id" -ForegroundColor Yellow
        $permissionEntry = Get-AdfsApplicationPermission | Where-Object {
$_.ClientRoleIdentifier -eq $id -and $_.ServerRoleIdentifier -eq
$serverRoleIdentifier }
        if ($null -eq $permissionEntry) {
            Write-Host "[+] No Application Permission found for Client Role:
$id - Server Role: $serverRoleIdentifier" -ForegroundColor Yellow
            Grant-AdfsApplicationPermission -ClientRoleIdentifier $id -
ServerRoleIdentifier $serverRoleIdentifier -ScopeNames $requiredScopes
        } else {
            Write-Host "[+] Application Permission found - validating
Scopes" -ForegroundColor Yellow
            $missingScopesList = New-Object
System.Collections.Generic.List[string]
            $requiredScopes | ForEach-Object {
                if ($_ -in $permissionEntry.ScopeNames) {
```

```
                    Write-Host "[+] Scope: $_ is already set!" -
ForegroundColor Green
                } else {
                    Write-Host "[+] Scope: $_ is missing and must be added"
-ForegroundColor Yellow
                    $missingScopesList.Add($_)
                }
            }

            if ($missingScopesList.Count -ge 1) {
                Write-Host "[+] The following Scopes will be added:
$([string]::Join(", ", $missingScopesList))" -ForegroundColor Yellow
                Set-AdfsApplicationPermission -TargetClientRoleIdentifier
$id -TargetServerRoleIdentifier $serverRoleIdentifier -AddScope
$missingScopesList
                Write-Host "[+] Done!`r`n" -ForegroundColor Green
            } else {
                Write-Host "[+] There is nothing to do!`r`n" -
ForegroundColor Green
            }
        }
    }
}
```

Удаление существующей группы приложений Outlook ADFS

> ⊗ **Внимание!**
>
> Выполнив действия, описанные в этом разделе, удаляется существующая конфигурация группы приложений Outlook ADFS.

Если у вас есть существующая конфигурация группы приложений Outlook ADFS и вы хотите удалить ее, выполните приведенные здесь действия, чтобы удалить существующую конфигурацию. Все следующие команды PowerShell должны выполняться из окна PowerShell на сервере ADFS.

Сначала мы удалим `ADFS Application Group`:

PowerShell

```
Remove-AdfsApplicationGroup -TargetApplicationGroupIdentifier "Outlook"
```

В качестве последнего шага мы удаляем добавленные пользовательские данные `Scopes` :

PowerShell

```
Remove-AdfsScopeDescription -TargetName "EAS.AccessAsUser.All"
Remove-AdfsScopeDescription -TargetName "EWS.AccessAsUser.All"
Remove-AdfsScopeDescription -TargetName "offline_access"
```

(Необязательно) Настроить веб-Application Proxy для доступа к экстрасети

Веб-Application Proxy является частью роли сервера удаленного доступа в Windows Server. Он предоставляет функции обратного прокси-сервера, позволяющие пользователям получать доступ к веб-приложениям за пределами корпоративной сети. Веб-Application Proxy предварительно выполняет проверку подлинности доступа к веб-приложениям с помощью ADFS и работает как прокси-сервер ADFS.

Если вы планируете использовать прокси-сервер веб-приложения, выполните действия, описанные в разделе Установка и настройка сервера веб-Application Proxy, чтобы настроить его. После настройки можно опубликовать правила для `Autodiscover.contoso.com` или и `mail.contoso.com` , выполнив действия, описанные в разделе Публикация приложения, использующего OAuth2.

(Необязательно) Настройка MFA для клиентского доступа

1. Чтобы настроить ADFS с выбранным поставщиком MFA, ознакомьтесь со следующими ссылками.

    - Настройка сторонних поставщиков проверки подлинности в качестве основной проверки подлинности в AD FS 2019
    - Настройка Azure MFA в качестве поставщика проверки подлинности с помощью AD FS

2. Настройте политику контроль доступа, требующую многофакторной проверки подлинности.

    - Политики контроль доступа в Windows Server 2016 AD FS

Создание политик проверки подлинности для конечных пользователей

Возможно, что не все пользователи в вашей организации имеют почтовые клиенты, поддерживающие современную проверку подлинности через ADFS. В этом сценарии рекомендуется включить современную проверку подлинности для

пользователей с поддерживаемыми клиентами и заблокировать ее для пользователей без них.

Чтобы включить современную проверку подлинности для определенного набора пользователей и заблокировать ее для остальных пользователей, необходимо создать по крайней мере две политики проверки подлинности.

> ⓘ **Важно!**
>
> Новые политики проверки подлинности становятся доступными сразу после подготовки Active Directory с помощью носителя Exchange 2019 CU13 или более поздней версии.

- Политика всей организации для блокировки современной проверки подлинности по умолчанию
- Вторичная политика для выборочного разрешения современной проверки подлинности для определенных пользователей

Следующие команды PowerShell должны выполняться из окна командной консоли Exchange (EMS) на сервере Exchange.

Создание политики на уровне организации для блокировки современной проверки подлинности по умолчанию

После включения современной проверки подлинности все клиенты Outlook пытаются использовать маркеры OAuth. Однако некоторые клиенты, несовместимые с современной проверкой подлинности ADFS, могут получать маркеры OAuth только из Microsoft Entra ID. Таким образом, эти клиенты не могут подключиться, если включена современная проверка подлинности.

Чтобы предотвратить этот сценарий, можно реализовать политику для всей организации, чтобы отключить современную проверку подлинности. В этом примере мы создадим новую политику проверки подлинности с именем `Block Modern Auth`.

PowerShell

```
New-AuthenticationPolicy "Block Modern Auth" -BlockModernAuthWebServices -
BlockModernAuthActiveSync -BlockModernAuthAutodiscover -BlockModernAuthImap
-BlockModernAuthMapi -BlockModernAuthOfflineAddressBook -BlockModernAuthPop
-BlockModernAuthRpc
```

Эту политику можно задать на уровне организации с помощью следующей команды.

PowerShell

```
Set-OrganizationConfig -DefaultAuthenticationPolicy "Block Modern Auth"
```

Создание политики проверки подлинности на уровне пользователя для включения современной проверки подлинности

Затем создайте вторую политику проверки подлинности, которая включает современную проверку подлинности. Назначьте эту политику всем пользователям с поддерживаемыми клиентами Outlook, чтобы разрешить их клиентам использовать современную проверку подлинности.

В этом примере мы создадим новую проверку подлинности с именем `Allow Modern Auth` с помощью следующей команды:

PowerShell

```
New-AuthenticationPolicy "Allow Modern Auth"
```

Настройка Exchange Server для использования маркеров OAuth ADFS

1. Проверьте, включен ли `OAuth` параметр в следующих виртуальных каталогах. Если он не включен, включите `OAuth` его для всех этих виртуальных каталогов:

   PowerShell

   ```
   Get-MapiVirtualDirectory | Format-List Server, *auth*
   Get-WebServicesVirtualDirectory | Format-List Server, *auth*
   Get-OabVirtualDirectory | Format-List Server, *auth*
   Get-AutodiscoverVirtualDirectory | Format-List Server, *auth*
   Get-ActiveSyncVirtualDirectory | Format-List Server, *auth*
   ```

   Выходные данные отображаются следующим образом. Основная деталь, на которой следует сосредоточиться, — это `OAuth`, как упоминалось ранее:

   PowerShell

```
Get-MapiVirtualDirectory | Format-List Server, *auth*

Server                          : EX1
IISAuthenticationMethods        : {Ntlm, OAuth, Negotiate}
InternalAuthenticationMethods : {Ntlm, OAuth, Negotiate}
ExternalAuthenticationMethods : {Ntlm, OAuth, Negotiate}
```

Если `OAuth` на любом сервере или в любом из пяти виртуальных каталогов отсутствует, необходимо добавить его с помощью соответствующих команд, прежде чем продолжить: Set-MapiVirtualDirectory, Set-WebServicesVirtualDirectory, Set-OabVirtualDirectory, Set-AutodiscoverVirtualDirectory и Set-ActiveSyncVirtualDirectory.

2. Выполните следующую команду:

PowerShell

```
New-AuthServer -Type ADFS -Name MyADFSServer -AuthMetadataUrl
https://<adfs server FQDN>/FederationMetadata/2007-
06/FederationMetadata.xml
```

Эта команда необходима для создания нового объекта сервера проверки подлинности в Exchange Server для ADFS. Объекты сервера проверки подлинности — это список доверенных издателей. Принимаются только маркеры OAuth от этих издателей.

3. Выполните следующую команду:

PowerShell

```
Set-AuthServer -Identity MyADFSServer -IsDefaultAuthorizationEndpoint
$true
```

Задайте сервер проверки подлинности, который мы только что добавили в `DefaultAuthorizationEndpoint` качестве . При рекламе заголовка Современной проверки подлинности Exchange Server объявляет URL-адрес проверки подлинности `DefaultAuthorizationEndpoint`. Таким образом клиенты узнают, какую конечную точку следует использовать для проверки подлинности.

4. Чтобы включить современную проверку подлинности на уровне организации, необходимо выполнить следующую команду:

PowerShell

```
Set-OrganizationConfig -OAuth2ClientProfileEnabled $true
```

5. Включите современную проверку подлинности для пользователей с поддерживаемыми клиентами, назначив `Allow Modern Auth` политику проверки подлинности:

```
PowerShell
```

```
Set-User -Identity User -AuthenticationPolicy "Allow Modern Auth"
```

Client-Side конфигурация современной проверки подлинности

Перед развертыванием для всех пользователей рекомендуется протестировать современную проверку подлинности с несколькими пользователями. После того как пилотная группа пользователей сможет использовать современную проверку подлинности, можно развернуть больше пользователей. Убедитесь, что клиент поддерживает современную проверку подлинности ADFS. Дополнительные сведения о поддерживаемых клиентах см. в разделе Предварительные требования для клиента .

Microsoft Windows

Включите современную проверку подлинности и добавьте домен ADFS в качестве доверенного домена в Outlook:

1. Создайте следующие разделы реестра, чтобы сделать домен ADFS доверенным доменом. Обязательно добавьте оба ключа с и без в `/` конце домена ADFS:

   - `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\AAD\AuthTrustedDomains\https://your-ADFS-domain/`
   - `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\AAD\AuthTrustedDomains\https://your-ADFS-domain`

   Вы можете использовать PowerShell для создания разделов реестра или их развертывания с помощью групповая политика. Выполните следующие команды из окна PowerShell на каждом клиентском компьютере. Замените `your-ADFS-domain` доменом ADFS.

```
```

PowerShell

```
New-Item -Path
"HKLM:\SOFTWARE\Policies\Microsoft\AAD\AuthTrustedDomains" -Force
(Get-Item
HKLM:).OpenSubKey("SOFTWARE\Policies\Microsoft\AAD\AuthTrustedDomains",
$true).CreateSubKey("https://your-ADFS-domain/")
(Get-Item
HKLM:).OpenSubKey("SOFTWARE\Policies\Microsoft\AAD\AuthTrustedDomains",
$true).CreateSubKey("https://your-ADFS-domain")
```

2. Чтобы включить современную проверку подлинности ADFS, добавьте значение в `Microsoft Outlook for Windows` `EnableExchangeOnPremModernAuth` `REG_DWORD` разделе `.HKCU\SOFTWARE\Microsoft\Office\16.0\Common\Identity\`

   С помощью PowerShell можно создать значение реестра или развернуть его с помощью групповая политика. Выполните следующую команду из окна PowerShell на каждом клиентском компьютере.

   PowerShell

   ```
   Set-ItemProperty -Path
   "HKLM:\SOFTWARE\Microsoft\Office\16.0\Common\Identity\" -Name
   "EnableExchangeOnPremModernAuth" -Value 1 -Type DWord
   ```

Проверка потока современной проверки подлинности

После правильной настройки пользователи получают запрос на вход в ADFS при подключении к серверу Exchange Server.

Влияние на другие клиенты при включенной современной проверке подлинности

Пользователи, включенные для современной проверки подлинности, которые используют несколько клиентов (например, `Outlook on Windows` и `Outlook Mobile`), могут по-разному действовать в каждом клиенте. В приведенной ниже сводке описано поведение клиента при включенной современной проверке подлинности при условии `DefaultAuthenticationPolicy`, что `Block Modern Auth` она применяется в качестве на уровне организации.

Развернуть таблицу

Клиент	Поведение
Outlook для Windows (классическая версия)	По умолчанию использует современную проверку подлинности.
Outlook для Windows (новый)	Пытается использовать современную проверку подлинности, но завершается сбоем.
Outlook для Mac	Пытается использовать современную проверку подлинности, но произойдет сбой; поддержка, пришедшая позже.
Outlook iOS	Возвращается к базовой проверке подлинности.
Outlook Android	Возвращается к базовой проверке подлинности.
Почтовое приложение iOS	Использует современную проверку подлинности.
Почтовое приложение macOS	Использует современную проверку подлинности.
Приложение Gmail	Возвращается к базовой проверке подлинности.
OWA/ECP	Не использует политику проверки подлинности. В зависимости от того, как она настроена, используется современная проверка подлинности или обычная проверка подлинности.
Приложение "Почта Windows"	Не возвращается к базовой проверке подлинности.
Клиент Thunderbird	Не возвращается к базовой проверке подлинности.
PowerShell	Использует обычную проверку подлинности.

Влияние на OWA/ECP при включении современной проверки подлинности для других клиентов

Вы можете использовать проверку подлинности на основе утверждений ADFS для Outlook в Интернете. Указанные действия необходимы для включения OAuth для других клиентов и не влияют на настройку OWA/ECP.

Использование проверки подлинности на основе утверждений AD FS с Outlook в Интернете

Время ожидания после изменения политики проверки подлинности

После изменения политики проверки подлинности, чтобы разрешить современную проверку подлинности или заблокировать устаревшую проверку подлинности:

- Подождите 30 минут, пока новые политики будут считываться внешними серверами

  или

- Выполните сброс IIS на всех внешних серверах.

Переход на гибридную современную проверку подлинности после включения современной проверки подлинности для Exchange Server

Если вы используете современную проверку подлинности с ADFS, а затем решили настроить гибридную проверку подлинности Exchange, следует перейти на гибридную современную проверку подлинности. Подробные действия по миграции будут включены в будущую версию этого документа.

Обновление сертификатов

Оценка текущей конфигурации сертификата

Когда дело доходит до клиентских подключений к Exchange Server, сертификат, который должен быть оценен, является сертификатом, привязанным к интерфейсным сайту IIS. Для сервера ADFS идеально подходит проверка актуальности всех возвращенных `Get-AdfsCertificate` сертификатов.

1. Чтобы определить соответствующий сертификат в Exchange Server, выполните следующие действия в командной консоли Exchange:

   PowerShell

   ```
   Import-Module WebAdministration
   (Get-ChildItem IIS:SSLBindings | Where-Object {($_.Sites -ne $null) -
   and ($_.Port -eq "443")}).Thumbprint | ForEach-Object {Get-
   ExchangeCertificate $_ | Where-Object {$_.Services -Match "IIS"} |
   ```

```
Format-Table Thumbprint, Services, RootCAType, Status, NotAfter, Issuer
-AutoSize -Wrap}
```

2. Чтобы просмотреть активные сертификаты на сервере ADFS, выполните следующие действия в PowerShell:

```PowerShell
Get-AdfsCertificate | Format-Table CertificateType, Thumbprint,
Certificate -AutoSize -Wrap
```

Обновление сертификатов в Exchange Server

Если выяснилось, что сертификат Exchange необходимо обновить для подключения клиента, необходимо выпустить новый сертификат и импортировать его на серверы Exchange. После этого сертификат должен быть как минимум включен для IIS. Оцените, должны ли быть включены другие службы для нового сертификата на основе вашей конфигурации.

Пример создания, завершения, включения и импорта нового сертификата на всех серверах на основе существующего сертификата в командной консоли Exchange:

1. Создайте новый запрос на сертификат в командной консоли Exchange на основе существующего сертификата:

```PowerShell
$txtrequest = Get-ExchangeCertificate <Thumbprint> | New-
ExchangeCertificate -GenerateRequest -PrivateKeyExportable $true
```

2. Создайте переменную, содержащую требуемый выходной путь для нового запроса на сертификат:

```PowerShell
$requestFile = "C:\temp\CertRequest.req"
```

3. Создайте файл запроса сертификата:

```PowerShell
[System.IO.File]::WriteAllBytes($requestFile,
[System.Text.Encoding]::Unicode.GetBytes($txtrequest))
```

> ⓘ **Примечание**
>
> Путь к папке для запроса сертификата уже должен существовать.

4. Предоставление общего доступа к файлу запроса центру сертификации (ЦС). Действия, необходимые для получения завершенного сертификата, зависят от ЦС.

> ⓘ **Примечание**
>
> `.p7b` — предпочтительный формат для завершенного запроса.

5. Создайте переменную, содержащую полный путь к завершенным запросам:

```
PowerShell
$certFile = "C:\temp\ExchangeCert.p7b"
```

6. Импортируйте запрос на сервер, который изначально создал запрос:

```
PowerShell
Import-ExchangeCertificate -FileData
([System.IO.File]::ReadAllBytes($certFile)) -PrivateKeyExportable $true
```

7. Переменная этапа для пароля для защиты завершенного сертификата:

```
PowerShell
$pw = Read-Host "Enter password" -AsSecureString
```

8. Экспортируйте двоичный файл сертификата в переменную:

```
PowerShell
$binCert = Export-ExchangeCertificate <Thumbprint> -BinaryEncoded
```

9. Переменная этапа для требуемого выходного пути завершенного сертификата:

```
PowerShell
```

```
$certificate = "\\$env:computername\c$\temp\CompletedExchangeCert.pfx"
```

10. Экспортируйте выполненный запрос для импорта на другие серверы:

```
PowerShell

[System.IO.File]::WriteAllBytes($certificate, $binCert.FileData)
```

11. Включите службы, которые должны быть привязаны к сертификату:

```
PowerShell

Enable-ExchangeCertificate <Thumbprint> -Services IIS
```

> ⓘ **Примечание**
>
> Возможно, потребуется добавить дополнительные службы в предыдущий пример на основе предыдущей конфигурации сертификатов.

12. Убедитесь, что сертификат работает должным образом, направив клиент на сервер для всех пространств имен клиента с файлом узла.

13. Импортируйте сертификат Exchange на все остальные серверы Exchange:

```
PowerShell

Import-ExchangeCertificate -PrivateKeyExportable $true -FileData
([System.IO.File]::ReadAllBytes($certificate)) -Password $pw -Server
<Server-Name>
```

> ⓘ **Примечание**
>
> `-PrivateKeyExportable` Включение параметра является необязательным при импорте на другие серверы Exchange.

14. Включите сертификат Exchange для необходимых служб Exchange на всех остальных серверах Exchange.

```
PowerShell

Enable-ExchangeCertificate <Thumbprint> -Services IIS -Server <Server-
```

```
Name>
```

> ⓘ **Примечание**
>
> Возможно, потребуется добавить дополнительные службы в предыдущий пример на основе предыдущей конфигурации сертификатов.

Обновление сертификата в ADFS

В зависимости от типа сертификата, который требует обновления в ADFS, определяет, нужно ли выполнять описанные ниже действия.

сертификат Service-Communications

В этом примере представлена оболочка PowerShell, необходимая для импорта сертификата в `.pfx` формате, например, созданном при выполнении действий по Exchange Server сертификату. Убедитесь, что вы вошли на основной сервер ADFS.

1. Этап переменной, содержащей пароль для сертификата:

```PowerShell
$pw = Read-Host "Enter password" -AsSecureString
```

2. Выполните этап переменной, содержащей полный путь к сертификату:

```PowerShell
$certificate = "\\E2k19-1\c$\temp\CompletedExchangeCert.pfx"
```

3. Импортируйте сертификат в личное хранилище LocalMachine:

```PowerShell
Import-PfxCertificate -FilePath $certificate -CertStoreLocation
Cert:\LocalMachine\my -Password $pw
```

4. Обновите сертификат Service-Communications:

```PowerShell
```

```
Set-AdfsSslCertificate -Thumbprint <Thumbprint>
```

сертификаты Token-Signing и Token-Decryption

Выполните действия, описанные в документации по получению и настройке сертификатов TS и TD для AD FS .

> **Примечание**
>
> Использование самозаверяющего сертификата по умолчанию для Token-Signing в проверке подлинности на основе утверждений ADFS для Outlook в Интернете требует установки сертификата на серверах Exchange Server.

Отключение обычной проверки подлинности в виртуальных каталогах Exchange Server

Статья • 16.04.2024

Введение

Обычная проверка подлинности — это метод проверки подлинности клиента, который требует имени пользователя и пароля для доступа к ресурсу. Однако обычная проверка подлинности может представлять угрозу безопасности. Поскольку многие из наших клиентов делают бизнес-решения об устранении обычной проверки подлинности в своих средах, мы предоставляем эту документацию, чтобы помочь в этих усилиях, связанных с Exchange Server.

> ⓘ **Важно!**
>
> Мы не поддерживаем отключение NTLM или Negotiate (встроенная проверка подлинности Windows, которая включает NTLM и Kerberos) в виртуальных каталогах Exchange. Если вы хотите запретить клиентам использовать NTLM или Kerberos при подключении к Exchange Onprem, мы поддерживаем и рекомендуем использовать политики проверки подлинности согласно нашим рекомендациям: **Отключение устаревшей проверки подлинности в Exchange Server 2019** г.

Из этой статьи вы узнаете, как отключить обычную проверку подлинности в каждом виртуальном каталоге, где она включена по умолчанию на Exchange Server.

Если вы ранее включили обычную проверку подлинности для виртуальных каталогов, отличных от перечисленных в этой статье, выполните описанные в документе действия, чтобы отменить внесенные изменения, или используйте статью Параметры по умолчанию для Exchange Server виртуальных каталогов, чтобы задать для метода проверки подлинности параметры по умолчанию.

Предварительные условия

- Outlook в Интернете (OWA) и Exchange Администратор Center (EAC) должны быть настроены с одинаковым методом проверки подлинности.

- По умолчанию OWA и EAC используют проверку подлинности на основе Forms (FBA), которая использует обычную проверку подлинности. Если вы решили отключить обычную проверку подлинности в этих виртуальных каталогах, FBA нельзя использовать и необходимо настроить другой метод проверки подлинности.

- Обычная проверка подлинности — это единственный метод, включенный по умолчанию в виртуальном каталоге Microsoft-Server-ActiveSync. Этот каталог используется мобильными клиентами для подключения Exchange Active Sync (EAS). Перед отключением базовой проверки подлинности для этого виртуального каталога необходимо настроить другой метод. Для этой цели рассмотрите возможность гибридной современной проверки подлинности с помощью Outlook Mobile или проверки подлинности на основе сертификатов.

Отключение обычной проверки подлинности в виртуальном каталоге OWA

Виртуальный каталог OWA используется клиентами, которые обращаются к Outlook в Интернете (OWA) для подключения к серверу Exchange Server. Методы проверки подлинности OWA и ECP должны иметь одинаковую конфигурацию.

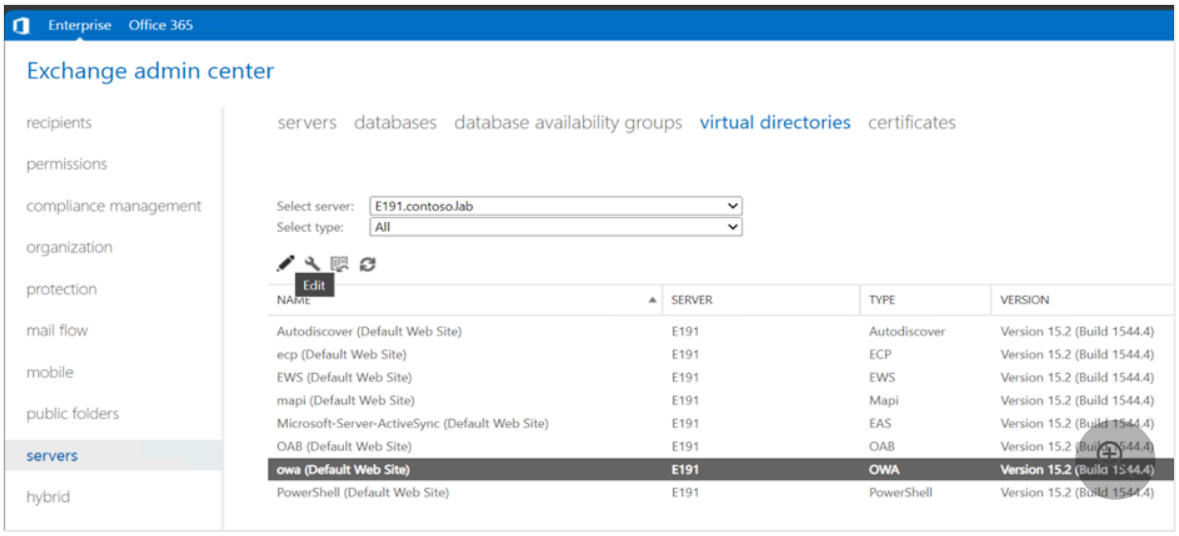
> ⓘ **Важно!**
>
> Перед отключением обычной проверки подлинности для OWA и ECP необходимо настроить другой метод проверки подлинности. Если вы уже настроили другой метод проверки подлинности, например NTLM, Kerberos, ADFS или проверку подлинности на основе сертификатов, для этих виртуальных каталогов, скорее всего, у вас уже отключена обычная проверка подлинности. Если нет, то следующие рекомендации помогут отключить обычную проверку подлинности, если вы больше не требуете FBA и уже используете другой метод.

Чтобы отключить обычную проверку подлинности в виртуальном каталоге OWA, выполните следующие действия.

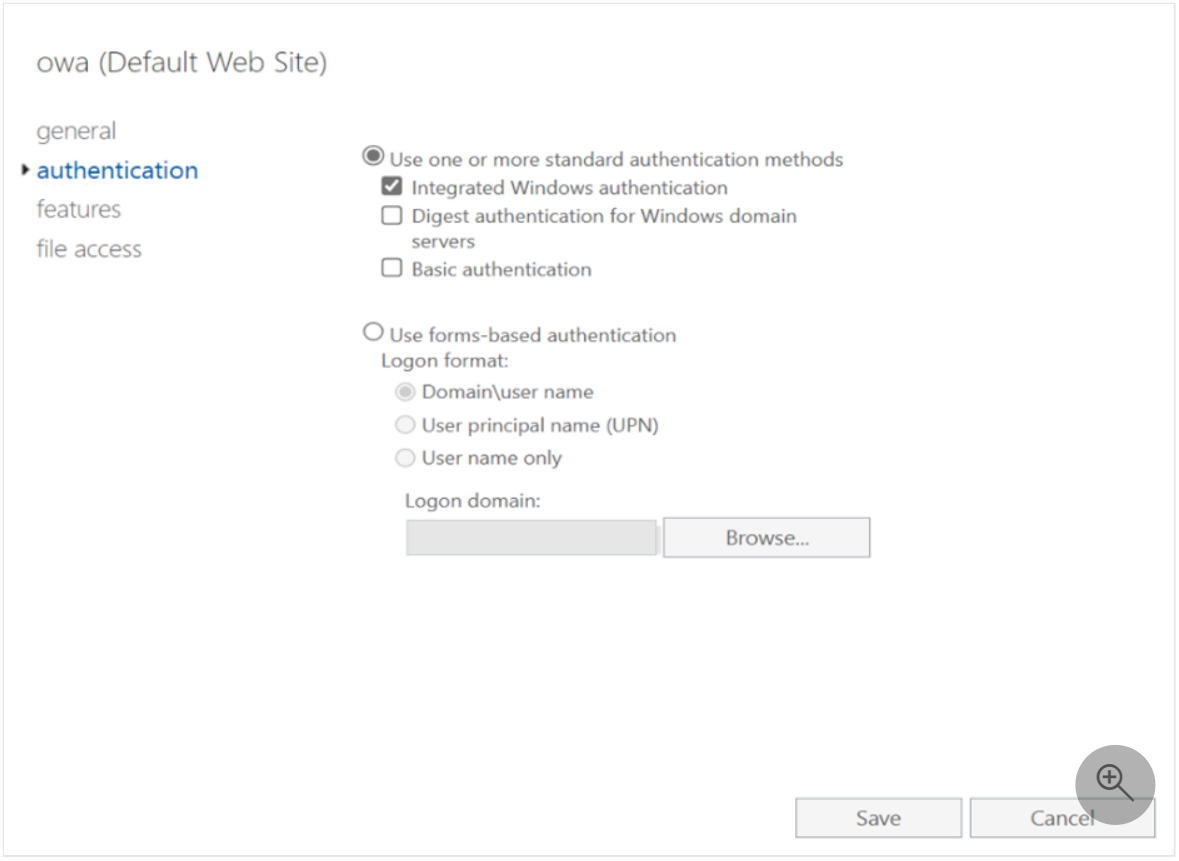
Из Центра Администратор Exchange (EAC)

- Откройте EAC и **перейдите в раздел Серверы** > **Виртуальные каталоги**.

- Выберите сервер, который требуется изменить, в раскрывающемся меню.
- Выберите виртуальный каталог **OWA (веб-сайт по умолчанию)** и нажмите кнопку **Изменить**.



- Выберите **Проверка подлинности**, снимите флажок Обычная проверка подлинности проверка и нажмите кнопку **Сохранить**.



Кроме того, используйте командлет Set-OwaVirtualDirectory в командной консоли Exchange.

Например, следующая команда отключает обычную проверку подлинности в виртуальном каталоге OWA на сервере EX01:

PowerShell

```
Set-OwaVirtualDirectory -Identity "EX01\owa (Default Web Site)" -
BasicAuthentication $False
```

Отключение обычной проверки подлинности в виртуальном каталоге ECP

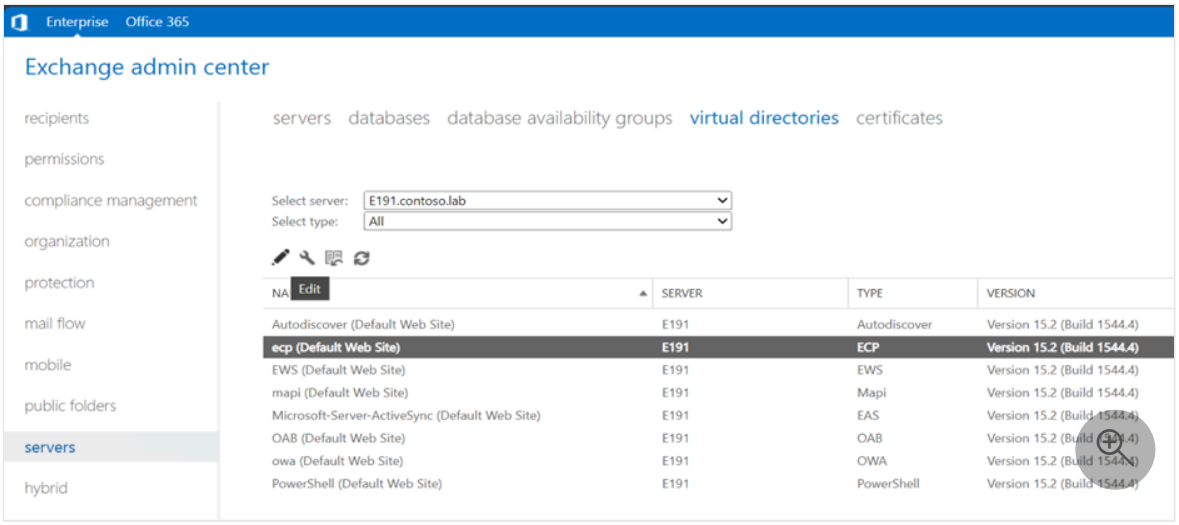
Виртуальный каталог ECP используется клиентами, которые обращаются к Центру Администратор Exchange (EAC) для подключения к серверу Exchange Server. Методы проверки подлинности OWA и ECP должны иметь одинаковую конфигурацию.

> ⓘ **Важно!**
>
> Перед отключением обычной проверки подлинности для OWA и ECP необходимо настроить другой метод проверки подлинности. Если вы уже настроили другой метод проверки подлинности, например NTLM, Kerberos или ADFS или проверку подлинности на основе сертификатов, для этих виртуальных каталогов, скорее всего, вы уже отключили обычную проверку подлинности. Если нет, то следующие рекомендации помогут отключить обычную проверку подлинности, если вы больше не требуете FBA и уже используете другой метод.

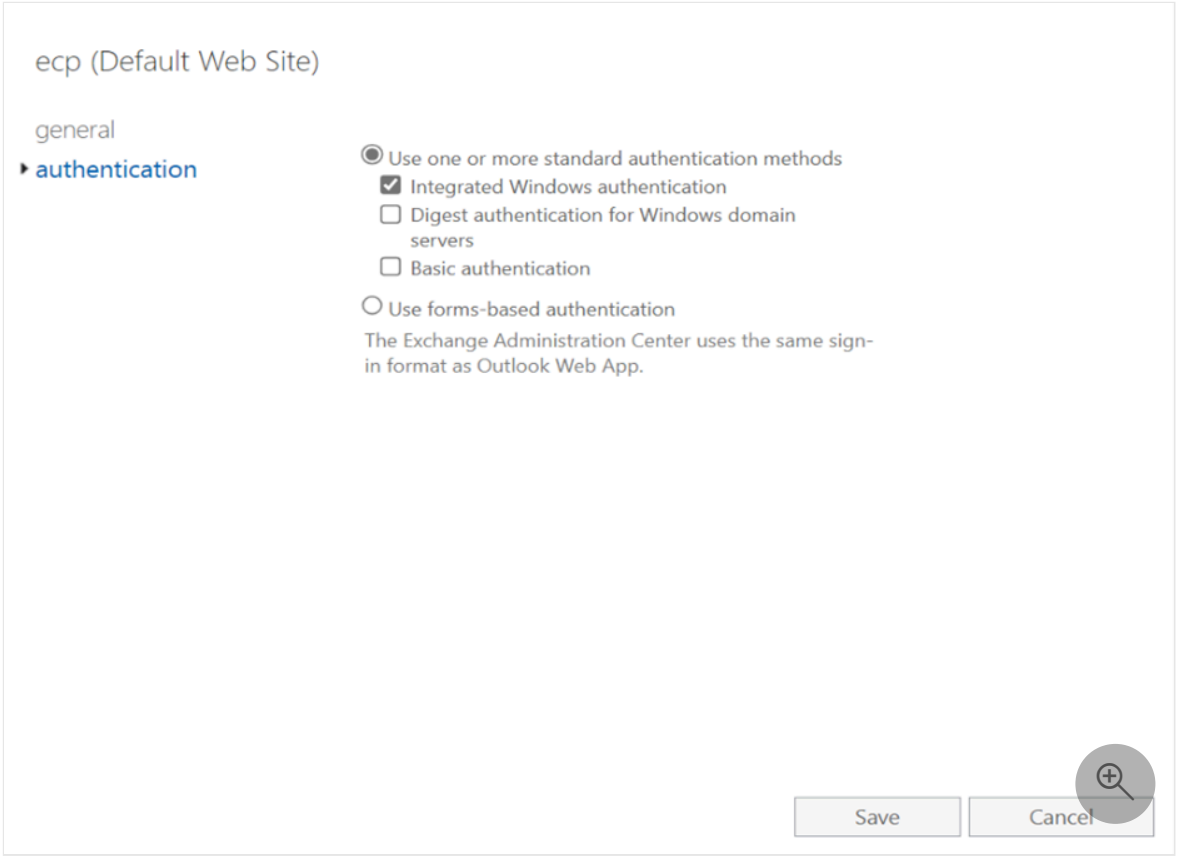
Чтобы отключить обычную проверку подлинности в виртуальном каталоге ECP, выполните следующие действия.

Из Центра Администратор Exchange (EAC)

- Откройте EAC и **перейдите в раздел Серверы** > **Виртуальные каталоги**.
- Выберите сервер, который требуется изменить, в раскрывающемся меню.
- Выберите виртуальный каталог **ECP (веб-сайт по умолчанию)** и нажмите кнопку **Изменить**.



- Выберите **Проверка подлинности**, снимите флажок Обычная проверка подлинности проверка и нажмите кнопку **Сохранить**.



Кроме того, можно использовать командлет Set-EcpVirtualDirectory в командной консоли Exchange.

Например, следующая команда отключает обычную проверку подлинности в виртуальном каталоге ECP на сервере с именем EX01:

PowerShell

```
Set-EcpVirtualDirectory -Identity "EX01\ecp (Default Web Site)" -
```

```
BasicAuthentication $False
```

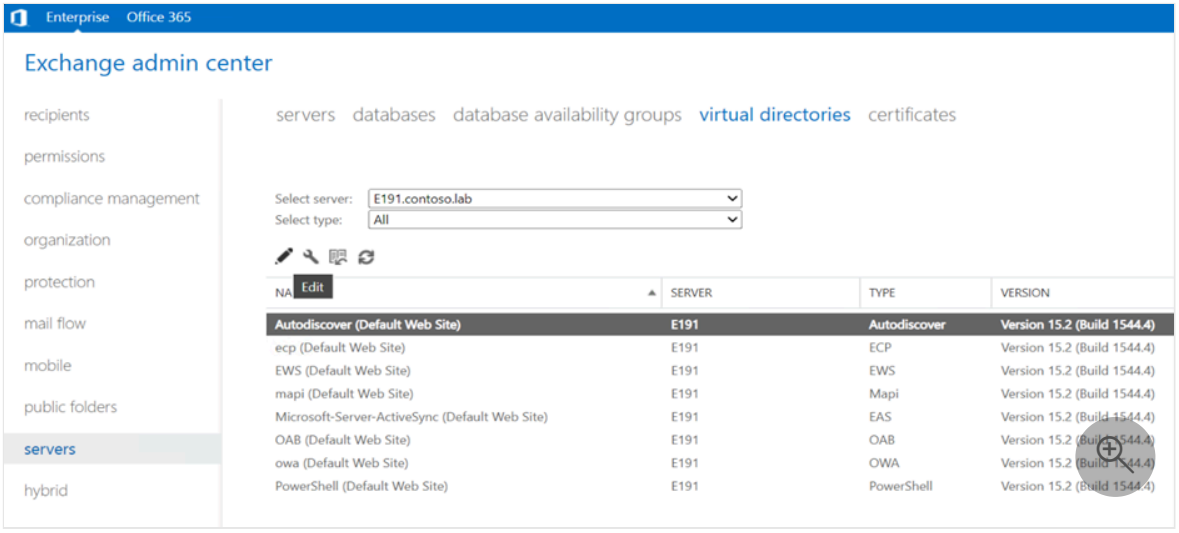
Отключение обычной проверки подлинности в виртуальном каталоге автообнаружения

Виртуальный каталог автообнаружения используется Outlook и мобильными устройствами для автоматической настройки параметров подключения к серверу Exchange Server.

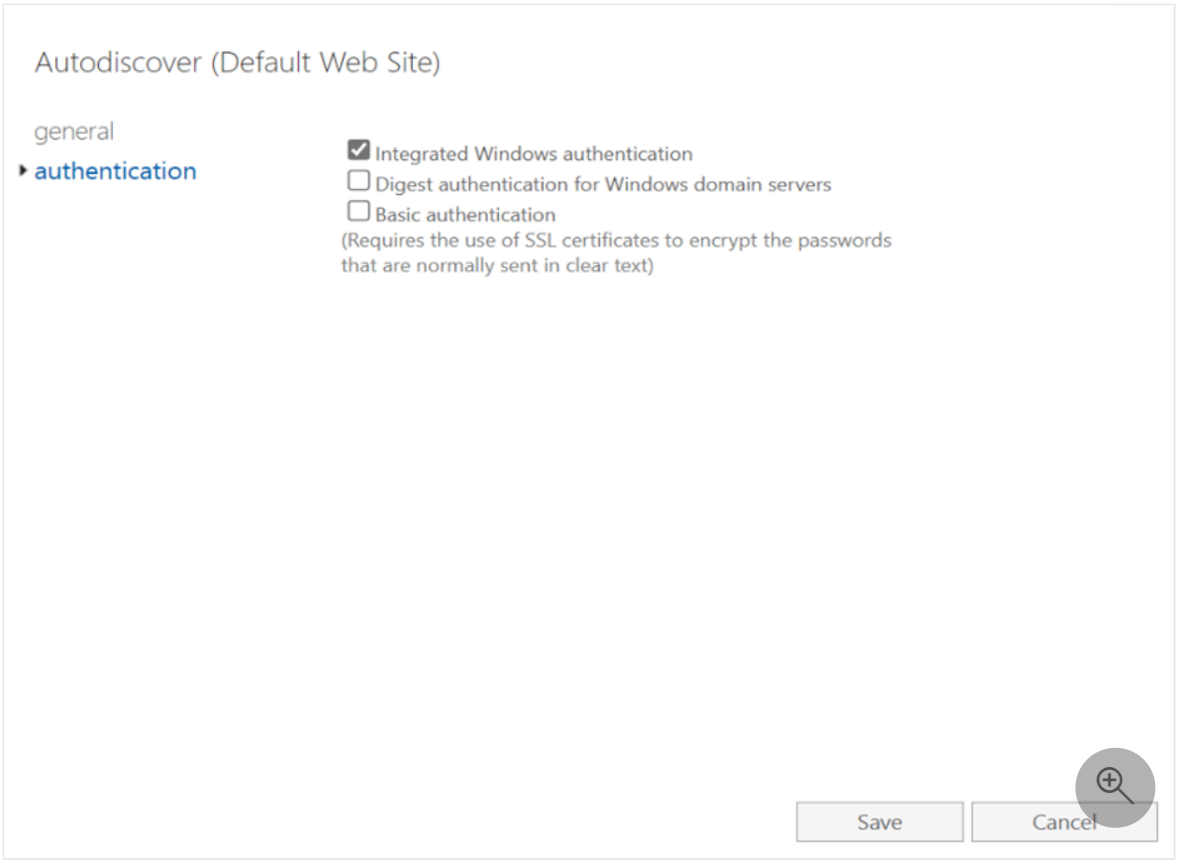
Чтобы отключить обычную проверку подлинности в виртуальном каталоге автообнаружения, выполните следующие действия.

Из Центра Администратор Exchange (EAC)

- Откройте EAC и **перейдите в раздел Серверы** > **Виртуальные каталоги**.
- Выберите сервер, который требуется изменить, в раскрывающемся меню.
- Выберите виртуальный каталог **автообнаружения (веб-сайт по умолчанию)** и нажмите кнопку **Изменить**.



- Выберите **Проверка подлинности**, снимите флажок Обычная проверка подлинности проверка и нажмите кнопку **Сохранить**.



Кроме того, можно использовать командлет Set-AutodiscoverVirtualDirectory в командной консоли Exchange.

Например, следующая команда отключает обычную проверку подлинности в виртуальном каталоге автообнаружения на сервере с именем EX01:

PowerShell

```
Set-AutodiscoverVirtualDirectory -Identity "EX01\Autodiscover (Default Web Site)" -BasicAuthentication $False
```

Отключение обычной проверки подлинности в виртуальном каталоге Microsoft-Server-ActiveSync

Виртуальный каталог Microsoft-Server-ActiveSync (Exchange Active Sync) используется мобильными клиентами для подключения к серверу Exchange Server.

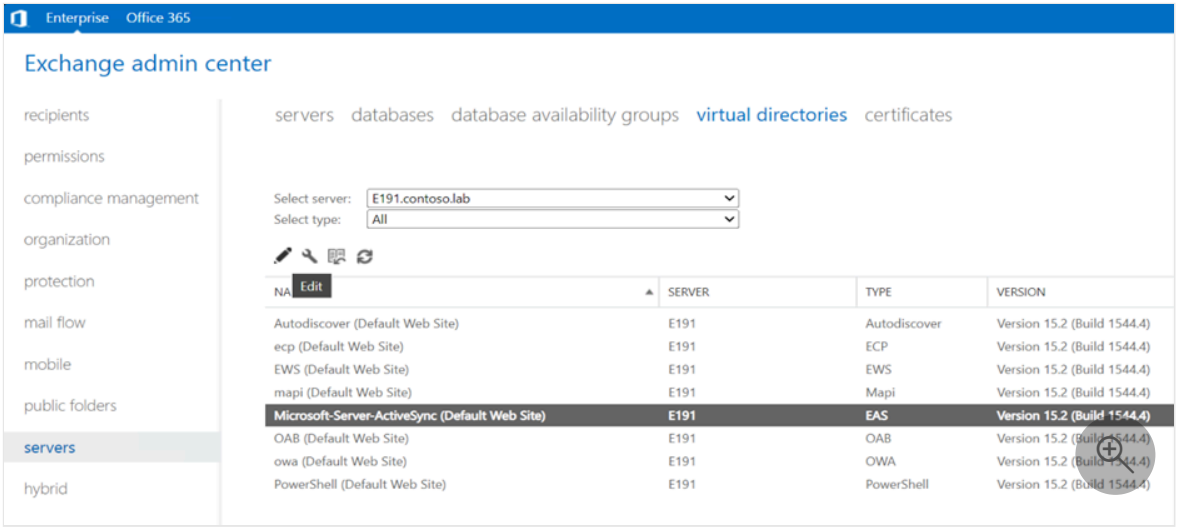
> **ⓘ Важно!**
>
> Вам потребуется настроить другой метод, например гибридная современная проверка подлинности (HMA) или проверка подлинности на основе

сертификатов (CBA), чтобы отключить обычную проверку подлинности для этого виртуального каталога, или клиенты не смогут подключаться с помощью ActiveSync.

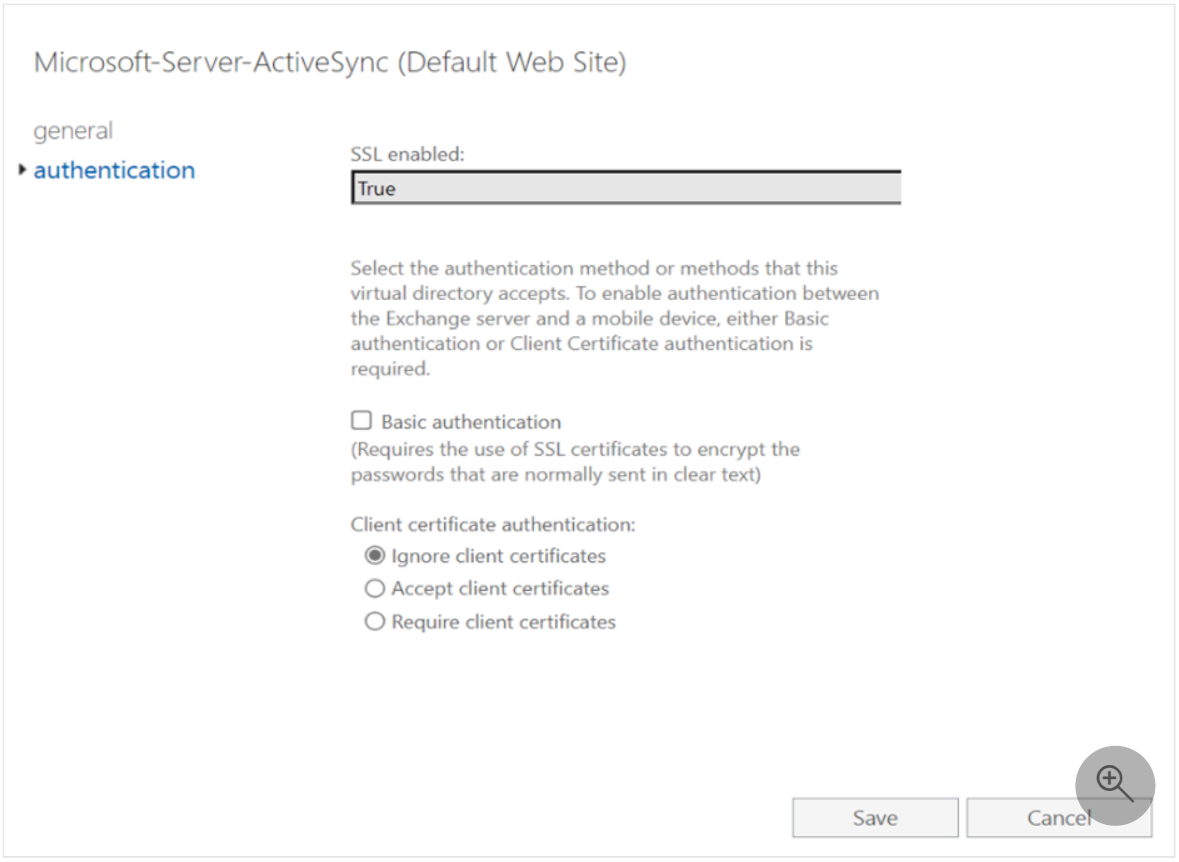
Чтобы отключить обычную проверку подлинности в виртуальном каталоге Microsoft-Server-ActiveSync, выполните следующие действия.

Из Центра Администратор Exchange (EAC)

- Откройте EAC и **перейдите в раздел Серверы** > **Виртуальные каталоги**.
- Выберите сервер, который требуется изменить, в раскрывающемся меню.
- Выберите виртуальный каталог **Microsoft-Server-ActiveSync (веб-сайт по умолчанию)** и нажмите кнопку **Изменить**.



- Выберите **Проверка подлинности**, снимите флажок Обычная проверка подлинности проверка и нажмите кнопку **Сохранить**.



Кроме того, можно использовать командлет Set-ActiveSyncVirtualDirectory в командной консоли Exchange.

Например, следующая команда отключает обычную проверку подлинности в виртуальном каталоге Microsoft-Server-ActiveSync на сервере с именем EX01:

PowerShell

```
Set-ActiveSyncVirtualDirectory -Identity "EX01\ Microsoft-Server-ActiveSync (Default Web Site)" -BasicAuthentication $False
```

Отключение обычной проверки подлинности в виртуальном каталоге RPC (Outlook Anywhere)

Виртуальный каталог Outlook Anywhere используется клиентами Outlook, которые используют устаревший протокол RPC через HTTP для подключения к серверу Exchange Server.

Чтобы отключить обычную проверку подлинности в виртуальном каталоге Outlook Anywhere, выполните следующие действия.

ⓘ Важно!

С помощью EAC можно задать только метод внешней проверки подлинности, поэтому этот метод не рекомендуется.

Для настройки методов внутренней и внешней проверки подлинности необходимо использовать командлет Set-OutlookAnywhere в командной консоли Exchange.

Так как Outlook рекомендует задать как внутренний, так и внешний методы проверки подлинности для подключения к Любому outlook, а Kerberos обычно не может использоваться внешне, рекомендуется использовать параметр DefaultAuthenticationMethod и задать для него значение NTLM. Это позволит одновременно обновить существующие параметры ExternalClientAuthenticationMethod, InternalClientAuthenticationMethod и IISAuthenticationMethods до NTLM.

Большинство организаций больше не используют устаревший протокол RPC через HTTP, и он был в целом заменен MAPI через HTTP, который теперь является протоколом по умолчанию в современных версиях Outlook. Если вы по-прежнему используете RPC через HTTP в организации, но используете только внутренние подключения, использующие этот протокол, рекомендуемый метод проверки подлинности будет Kerberos, если он доступен.

OAuth недоступен для RPC через HTTP.

Следующая команда отключает обычную проверку подлинности в виртуальном каталоге Outlook Anywhere на сервере с именем EX01 и задает метод проверки подлинности NTLM для внутренних и внешних подключений:

PowerShell

```
Set-OutlookAnywhere -Identity "EX01\Rpc (Default Web Site)" -
DefaultAuthenticationMethod NTLM
```

Заключение

В этой статье мы рассказали, как отключить обычную проверку подлинности в каждом соответствующем виртуальном каталоге, где она включена по умолчанию

на Exchange Server. Отключив обычную проверку подлинности, вы можете повысить безопасность среды Exchange.

Связанные статьи

Отключение устаревшей проверки подлинности в Exchange Server 2019 г.

Как настроить локальное развертывание Exchange Server для использования гибридной современной проверки подлинности

Гибридная современная проверка подлинности в случае Outlook для iOS и Android

Настройка проверки подлинности на основе сертификатов в Exchange 2016

Использование проверки подлинности на основе утверждений AD FS с Outlook в Интернете

Рекомендации по обеспечению безопасности для Exchange Server

Статья • 13.11.2024

Обзор

В следующих разделах приведены рекомендации по обеспечению безопасности и рекомендации по безопасной работе Exchange Server. Мы постоянно добавляем новые разделы в этот раздел. Время от времени проверяйте информацию о последних рекомендациях.

Развернуть таблицу

Статья	Описание	Тип
Часто задаваемые вопросы об обновлении Exchange Server	Узнайте, почему важно поддерживать актуальность сервера Exchange Server.	Документация
Exchange Server и SMB версии 1	Узнайте, почему важно отключить небезопасные версии SMB.	Запись блога
Настройка доменов загрузки в Exchange Server	Узнайте, как настроить функцию скачивания домена в Exchange Server.	Документация
Настройка расширенной защиты Windows в Exchange Server	Узнайте, как настроить расширенную защиту в Exchange Server.	Документация
Настройка http Strict Transport Security (HSTS) в Exchange Server	Узнайте, как настроить HSTS в Exchange Server.	Документация
Настройка подписи сертификатов полезных данных сериализации PowerShell в Exchange Server	Узнайте, как настроить подпись сертификата для функции полезных данных сериализации PowerShell в Exchange Server.	Документация
Служба экстренного устранения рисков (EM) для Exchange	Дополнительные сведения о службе устранения чрезвычайных ситуаций Exchange см. в Exchange Server.	Документация
рекомендации по настройке TLS Exchange Server	Дополнительные сведения о правильной настройке TLS в Exchange Server.	Документация
Exchange Server обнаружения заголовков P2 FROM, не	Узнайте больше о функции, которая обнаруживает заголовки P2 FROM, не	Документация

Статья	Описание	Тип
совместимых с RFC	соответствующие RFC, в Exchange Server.	

Настройка доменов загрузки в Exchange Server

Статья • 15.11.2023

Обзор

Эта `Download Domains` функция приводит к загрузке вложений с URL-адреса, отличного от того, который используется пользователем для доступа к Outlook в Интернете (OWA). Этот межсайтовой вызов обеспечивает применение так называемого `SameSite cookies` стандарта браузера, что обеспечивает лучшую защиту от атак CSRF. Эта функция устраняет `Download Domains` уязвимость, например CVE-2021-1730.

Что такое файлы cookie и когда они используются

Файлы cookie — это текстовые строки, отправляемые с веб-сайтов и хранящиеся на компьютере в веб-браузере. Они используются для проверки подлинности и персонализации. Например, файлы cookie используются для отзыва сведений с отслеживанием состояния, сохранения параметров пользователя, записи действий просмотра и отображения соответствующей рекламы. Файлы cookie всегда связаны с определенным доменом и устанавливаются различными сторонами.

Исторически сложилось так, что такие сайты, как `example.com` , делающие `cross-origin` запросы к другим доменам, например, `contoso.com` приводили к тому, что браузер отправлял `example.com` файлы cookie в рамках любого запроса.

В большинстве случаев пользователь может повторно использовать некоторое состояние (например, состояние входа) на сайтах независимо от того, откуда был получен запрос. Тем не менее, это поведение может быть злоупотребление при атаках CSRF. Компонент `SameSite` снизил уязвимость за счет реализации и управления в заголовке `Set-Cookie` .

Как работает стандартный файл cookie SameSite

Определяется `SameSite` как домен верхнего уровня (TLD) и еще одно доменное имя.

Пример:

Развернуть таблицу

Схема	Доменное имя	TLD
https://	Contoso	.Com

Также учитывается схема URL-адреса. Запрос, поступающий от `https://contoso.com` и по которому отправляется `http://contoso.com` (например, щелкнув ссылку), рассматривается как междомовые запросы.

В стандарте `SameSite cookies` сайты или веб-приложения могут задавать `SameSite` атрибут для файлов cookie с помощью заголовка `Set-Cookie` `document.cookie` или с помощью свойства JavaScript, чтобы ограничить, в каких случаях отправляется файл cookie.

Спецификация `SameSite cookies` появилась в Google Chrome версии 51 как необязательный атрибут. Он был представлен с Windows 10 сборки 17672 для Microsoft Edge и Internet Обозреватель.

Поддерживаются три значения:

- `Strict`
  - Браузер не будет отправлять этот файл cookie ни в одном межайтовом запросе
- `Lax`
  - Браузер отправляет этот файл cookie в межсайтовых запросах при определенных условиях (должны применяться все условия):
    - Используется "безопасный" метод HTTP `GET`
    - Запрос поступает из навигации верхнего уровня, которая была выполнена пользователем (например, была щелкнута ссылка).
- `None`
  - Браузер отправляет файл cookie в любом межсайтовом запросе `SameSite` , так как этот параметр отключает ограничение

Стандарт `SameSite cookies` поддерживается всеми основными веб-браузерами, и если `SameSite` атрибут не задан явным образом веб-сайтом или приложением, которое выдает файл cookie, он автоматически предполагается веб-браузером и

обрабатывается по умолчанию для `SameSite=Lax` повышения безопасности от `CSRF` атак.

- Microsoft Edge
- Google Chrome
- Mozilla Firefox

Если взглянуть на `Download Domains` эту функцию, то вызов, `attachments.owa.contoso.com` инициированный из `owa.contoso.com` , считается межстраничного запроса, а файлы cookie отправляются только в том случае, если выполнены условия, описанные для `Lax` значения.

Включить скачивание доменов в организации

Перед включением функции загрузки домена для вашей организации необходимо выполнить несколько действий. Чтобы настроить эту функцию, выполните следующие действия:

1. Создайте новую запись DNS типа CNAME (Псевдоним). Запись должна указывать на домен, используемый для доступа к Outlook в Интернете (OWA).

   Пример:

   Развернуть таблицу

Имя	Тип	Значение
attachments.owa.contoso.com	CNAME	owa.contoso.com

   > **Примечание**
   >
   > Если вы используете разные пространства имен для внутреннего и внешнего доступа OWA, необходимо создать две записи CNAME и задать их соответствующим образом с помощью `InternalDownloadHostName` параметра и `ExternalDownloadHostName` , как описано на шаге 3.

   > **Важно!**
   >
   > Пользователи **не должны использовать домены загрузки** для доступа к Outlook в Интернете, так как это позволит устранить защиту,

предоставляемую функцией загрузки доменов.

2. Обязательно добавьте в сертификат новый поддомен, который используется Exchange Server и привязан к интерфейсу. Дополнительные сведения о запросе сертификата для Exchange Server см. в статье Процедуры сертификации в Exchange Server.

3. Добавьте новый поддомен в конфигурацию Outlook в Интернете, выполнив следующую команду из командной консоли Exchange с повышенными привилегиями (EMS):

```
PowerShell

Set-OwaVirtualDirectory -Identity "Contoso\OWA (Default Web Site)" -
InternalDownloadHostName "attachments.owa.contoso.com" -
ExternalDownloadHostName "attachments.owa.contoso.com"
```

> ⓘ **Примечание**
>
> Убедитесь, что заданы правильные имена узлов, если конфигурация Exchange использует разные пространства имен для доступа к OWA из внутренних и внешних сетей. Использование неправильного пространства имен может привести к ухудшению взаимодействия с пользователем (например, встроенные изображения невидимы и т. д.).

4. После подготовки всех виртуальных каталогов OWA и развертывания нового сертификата на всех серверах Exchange эту функцию можно включить, выполнив следующую команду в командной консоли Exchange с повышенными привилегиями (EMS):

```
PowerShell

Set-OrganizationConfig -EnableDownloadDomains $true
```

5. Для активации `World Wide Web Publishing service` функции необходимо перезапустить и на `Windows Process Activation Service` каждом сервере Exchange Server. Выполните следующую команду в окне PowerShell с повышенными привилегиями или перезапустите сервер:

```
PowerShell
```

```
Restart-Service -Name W3SVC, WAS -Force
```

Убедитесь, что домены загрузки включены

Чтобы убедиться, что функция скачивания домена включена и работает должным образом, выполните следующие действия.

1. Отправьте сообщение электронной почты со встроенным изображением в почтовый ящик. Не имеет значения, было ли сообщение отправлено из внутреннего или внешнего почтового ящика.
2. Войдите в OWA и найдите тестовое сообщение электронной почты, отправленное в почтовый ящик.
3. Убедитесь, что изображение загружено и отображается в области чтения.
4. Щелкните правой кнопкой мыши встроенное изображение и выберите `Copy Image link`
5. Вставьте ссылку в `Notepad.exe` и проверка URL-адрес. Это должен быть настроенный домен загрузки (например, attachments.owa.contoso.com). Этот результат подтверждает, что функция скачивания домена активна и работает должным образом.

Отключить скачивание доменов в организации

Функция загрузки домена настраивается с помощью конфигурации для всей организации и, как следствие, может быть включена или отключена только на всех серверах Exchange server или вообще без нее. Если вы хотите отключить эту функцию, достаточно выполнить следующую команду из командной консоли Exchange с повышенными привилегиями (EMS):

PowerShell

```
Set-OrganizationConfig -EnableDownloadDomains $false
```

Выполните действия, описанные в разделе Подтверждение включения доменов загрузки этой статьи, чтобы убедиться, что эта функция отключена.

Настройка расширенной защиты Windows в Exchange Server

Статья • 15.11.2023

Обзор

Расширенная защита Windows улучшает существующую проверку подлинности в Windows Server и устраняет атаки ретранслятора проверки подлинности или атаки "человек в середине" (MitM). Для устранения рисков используются сведения о безопасности, реализованные с помощью сведений о привязке каналов, указанных в объекте `Channel Binding Token (CBT)` , который в основном используется для подключений TLS.

Расширенная защита включена по умолчанию при установке Exchange Server 2019 CU14 (или более поздней версии). Дополнительные сведения см. в статье Выпущено накопительное обновление H1 2024 для Exchange Server.

В более ранних версиях Exchange Server (например, Exchange Server 2016) расширенную защиту можно включить с помощью сценария ExchangeExtendedProtectionManagement.ps1 на некоторых или всех серверах Exchange.

Терминология, используемая в этой документации

Виртуальный каталог или vDir

Используется Exchange Server для предоставления доступа к веб-приложениям, таким как `Exchange ActiveSync`, `Outlook on the Web` и `AutoDiscover` службе. Администратор может настроить несколько параметров виртуального каталога, включая параметры проверки подлинности, безопасности и отчетов. Расширенная защита является одним из таких параметров проверки подлинности.

Параметр расширенной защиты

Управляет поведением для проверки `Channel Binding Tokens` или `CBT`. Возможные значения для этого параметра перечислены в следующей таблице:

Развернуть таблицу

Значение	Описание
Нет	Указывает, что службы IIS не выполняют проверку CBT.
Разрешить	Указывает, что проверка CBT включена, но не является обязательной. Этот параметр обеспечивает безопасный обмен данными с клиентами, поддерживающими расширенную защиту, и по-прежнему поддерживает клиенты, которые не могут использовать расширенную защиту.
Обязательность	Это значение указывает, что требуется проверка CBT. Этот параметр блокирует клиенты, которые не поддерживают расширенную защиту.

Флаги SSL

Настройка параметров SSL необходима, чтобы клиенты подключались к виртуальным каталогам IIS определенным образом с помощью сертификатов клиента. Чтобы включить расширенную защиту, обязательными флагами SSL являются `SSL` и `SSL128`.

Разгрузка SSL

Завершает подключение на устройстве между клиентом и Exchange Server, а затем использует незашифрованное подключение для подключения к Exchange Server.

Мост SSL

Описывает процесс, в котором устройство, расположенное на границе сети, расшифровывает SSL-трафик, а затем повторно шифрует его перед отправкой на веб-сервер.

Современный гибридный или гибридный агент

Это имя метода настройки гибридной среды Exchange, который устраняет некоторые требования к конфигурации для классической гибридной среды (например, входящие сетевые подключения через брандмауэр) для включения гибридных функций Exchange. Дополнительные сведения об этой функции см. здесь.

Общедоступные папки

Предназначены для общего доступа и упрощают просмотр содержимого в глубокой иерархии. Дополнительные сведения об общедоступных папках см. здесь.

Предварительные требования для включения расширенной защиты в Exchange Server

> **Совет**
>
> Рекомендуется запустить скрипт **средства проверки работоспособности Exchange Server** , чтобы проверить, выполнены ли все предварительные требования на сервере Exchange Server, на котором должна быть активирована расширенная защита.

Версии Exchange Server, поддерживающие расширенную защиту

Расширенная защита поддерживается в Exchange Server 2013, 2016 и 2019, начиная с выпусков обновления для системы безопасности Exchange Server (SU) за август 2022 г .

Если в вашей организации установлен Exchange Server 2016 или Exchange Server 2019, на них **должны** быть установлены ежеквартальные обновления Exchange за сентябрь 2021 г. или накопительное обновление 2022 H1 . Прежде чем продолжить настройку расширенной защиты, **необходимо** установить по крайней мере обновление системы безопасности за август 2022 г. или более поздней версии.

Если в вашей организации установлен Exchange Server 2013, exchange Server должен быть в накопительном пакете обновления 23 (CU23) с установленным обновлением для системы безопасности за август 2022 г. или более поздней версии.

> **⚠ Предупреждение**
>
> **Поддержка Exchange Server 2013закончилась** 11 апреля 2023 г.

Требования к конфигурации Outlook Anywhere

Разгрузка SSL для `Outlook Anywhere` включена по умолчанию и **должна быть отключена** перед включением расширенной защиты. Выполните действия, описанные в примере 3.

> ⓘ **Важно!**
>
> Установщик Exchange Server 2019 CU14 (или более поздней версии) автоматически отключает разгрузку `Outlook Anywhere` SSL. Это часть расширенной защиты, включенной по умолчанию.

Требования к версии NTLM

`NTLMv1` является слабым и не обеспечивает защиту от атак "человек в середине" (MitM). Ее следует рассматривать как уязвимую и больше не использовать.

`NTLMv1` не может использоваться вместе с расширенной защитой. Если принудительно использовать `NTLMv1` клиент вместо `NTLMv2` и на серверах Exchange включена расширенная защита, эта конфигурация приведет к выводу запросов паролей на стороне клиента без способа успешной проверки подлинности на сервере Exchange Server.

> ⓘ **Примечание**
>
> Чтобы повысить безопасность, рекомендуется проверить и настроить этот параметр независимо от того, возникли ли проблемы.

Если после включения расширенной защиты клиенты получают запросы паролей, проверьте следующий раздел реестра и значение на клиенте и на стороне Exchange Server:

Раздел реестра: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa`

Значение реестра: `LmCompatibilityLevel`

Рекомендуется задать для него значение , равное `5 Send NTLMv2 response only. Refuse LM & NTLM`. Ему должно быть присвоено по крайней мере значение , для которого `3` задано значение `Send NTLMv2 response only`.

При удалении значения операционная система применяет системное значение по умолчанию. В Windows Server 2008 R2 и более поздних версиях мы обрабатываем его так, как если бы для него задано значение `3`.

Если вы хотите централизованно управлять параметром, это можно сделать с помощью групповой политики:

Расположение политики: `Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options`

Дополнительные сведения см. в статье Безопасность сети: уровень проверки подлинности LAN Manager

Требования к TLS

Перед включением расширенной защиты необходимо убедиться, что все конфигурации TLS согласованы на всех серверах Exchange. Например, если один из серверов использует `TLS 1.2`, необходимо убедиться, что все серверы в организации настроены с помощью `TLS 1.2`. Любой вариант использования версии TLS на разных серверах может привести к сбою подключений клиента или сервера к серверу.

В дополнение к этому требованию значение `SchUseStrongCrypto` реестра должно иметь значение на всех серверах `1` Exchange в организации.

Если для этого значения явно не задано `1`значение , значение по умолчанию этого ключа можно интерпретировать как `0` или `1` в зависимости от версии .NET, используемой двоичными файлами Exchange Server, и существует вероятность возникновения проблем с подключением при обмене данными между сервером и сервером. Это может произойти, особенно если используются разные версии Exchange Server (например, Exchange Server 2016 и Exchange Server 2019).

То же самое относится и к значению `SystemDefaultTlsVersions` реестра, для которого также должно быть явно задано значение `1`.

Если эти значения реестра не настроены должным образом, эта неправильная настройка может привести к несовпадению TLS в обмене данными между сервером и сервером или клиентом и сервером и, как следствие, может привести к проблемам с подключением.

Сведения о настройке необходимых параметров TLS на серверах Exchange Server см. в этом руководстве по настройке TLS .

Совместимость стороннего программного обеспечения

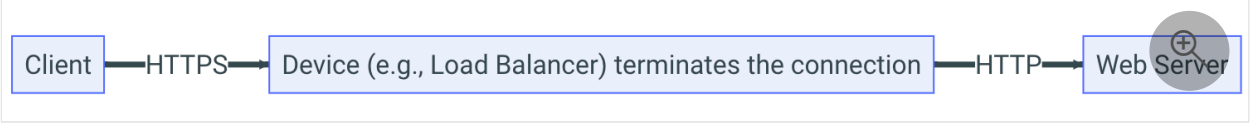
Перед включением расширенной защиты необходимо провести тесты для всех сторонних продуктов в среде Exchange Server, чтобы убедиться, что они работают правильно. Если вы не знаете, поддерживается ли расширенная защита, обратитесь к поставщику за подтверждением.

Мы видели, например, антивирусные решения, которые отправляли подключения через локальный прокси-сервер для защиты клиентского компьютера. Такой сценарий будет препятствовать обмену данными с сервером Exchange Server и должен быть отключен, так как это считается подключением "человек в середине" (MitM), которое будет заблокировано расширенной защитой.

Сценарии, которые могут повлиять на подключение клиента при включенной расширенной защите

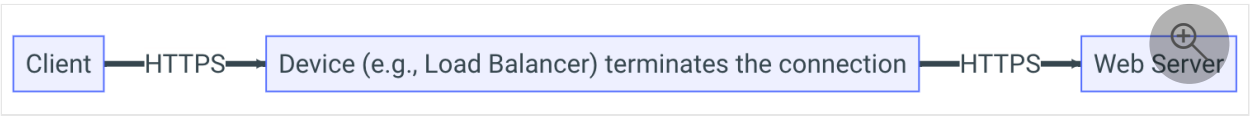
Сценарии разгрузки SSL

Расширенная защита **не поддерживается** в средах, использующих разгрузку SSL. Завершение SSL во время разгрузки SSL приводит к сбою расширенной защиты. Чтобы включить расширенную защиту в среде Exchange, **не следует использовать разгрузку SSL** с подсистемами балансировки нагрузки.



Сценарии мостов SSL

Расширенная защита **поддерживается** в средах, использующих мост ssl при определенных условиях. Чтобы включить расширенную защиту в среде Exchange с помощью МОСТА SSL, **необходимо использовать один и тот же SSL-сертификат в Exchange и load Balancers**. Использование разных сертификатов приводит к сбою проверки маркера привязки канала расширенной защиты и, как следствие, запрету подключения клиентов к серверу Exchange Server.



Сценарии расширенной защиты и общедоступных папок

В следующем разделе рассматриваются сценарии общедоступных папок, которые могут привести к сбоям при включении расширенной защиты.

Расширенная защита не может быть включена на серверах Exchange Server 2013 с общедоступными папками в среде сосуществования

Чтобы включить расширенную защиту в Exchange Server 2013, убедитесь, что у вас нет общедоступных папок, размещенных в Exchange Server 2013. Если у вас есть сосуществование Exchange Server 2013 с Exchange Server 2016 или Exchange Server 2019, **перед включением** расширенной защиты **необходимо** перенести общедоступные папки в Exchange Server 2016 или Exchange Server 2019. После включения расширенной защиты и появления общедоступных папок в Exchange Server 2013 они больше не будут отображаться для конечных пользователей!

> ⚠ **Предупреждение**
>
> Поддержка Exchange Server 2013закончилась 11 апреля 2023 г.

Расширенная защита не может быть включена в Exchange Server 2016 CU22 или Exchange Server 2019 CU11 или более ранней версии, в которых размещена иерархия общедоступных папок.

Если у вас есть среда, содержащая Exchange Server 2016 CU22 или Exchange Server 2019 CU11 или более ранней версии, и вы используете общедоступные папки, перед включением **расширенной защиты необходимо подтвердить версию сервера, на котором размещена иерархия общедоступных папок** .

Убедитесь, что сервер, на котором размещена иерархия общедоступных папок, обновлен до Exchange Server 2016 CU23 или Exchange Server 2019 CU12 (или более поздней версии) с установленными последними обновлениями для системы безопасности . Переместите иерархию общедоступных папок на сервер Exchange Server, на котором выполняется требуемая версия, если не удается обновить сервер Exchange Server до поддерживаемой версии.

Для уточнения можно использовать следующую таблицу:

Развернуть таблицу

Версия Exchange	Установлен накопительный пакет обновления	Установленная единица хранения	Размещает почтовые ящики PF	Поддерживается ли EP?
Exchange 2013	CU23	Август 2022 г. (или более поздняя версия)	Нет	Да
Exchange 2016	CU22	Август 2022 г. (или более поздняя версия)	Нет почтовых ящиков иерархии	Да
Exchange 2016	CU23 (2022 H1) или более поздней версии	Август 2022 г. (или более поздняя версия)	Любой	Да
Exchange 2019	CU11	Август 2022 г. (или более поздняя версия)	Нет почтовых ящиков иерархии	Да
Exchange 2019	CU12 (2022 H1) или более поздней версии	Август 2022 г. (или более поздняя версия)	Любой	Да
Любая другая версия	Любой другой cu	Любой другой su	Любой	Нет

Расширенная защита и современная гибридная конфигурация

В следующем разделе рассматриваются сценарии современной гибридной среды Exchange Server, которые могут привести к сбоям при включении расширенной защиты.

Расширенная защита не может быть полностью настроена на серверах Exchange Server, опубликованных с помощью гибридного агента

В современной гибридной конфигурации серверы Exchange публикуются через гибридный агент, который выполняет прокси-вызовы Exchange Online к серверу Exchange Server.

Включение расширенной защиты на серверах Exchange Server, опубликованных с помощью гибридного агента, может привести к нарушению гибридных функций, таких как перемещение почтовых ящиков и свободные и занятые вызовы, если они выполняются неправильно. Поэтому важно определить все серверы Exchange, опубликованные с помощью гибридного агента, и не включить расширенную защиту в Front-End виртуальном каталоге EWS на них.

Определение серверов Exchange, опубликованных с помощью гибридного агента

Если у вас нет списка серверов, опубликованных через гибридный агент, можно выполнить следующие действия, чтобы определить их. Эти действия не требуются, если вы используете классическое гибридное развертывание Exchange Server.

1. Войдите на компьютер, на котором установлен гибридный агент, и откройте модуль PowerShell гибридного агента. Выполните команду `Get-HybridApplication` , чтобы определить, используемый `TargetUri` гибридным агентом.
2. Параметр `TargetUri` предоставляет полное доменное имя сервера Exchange Server, который настроен для использования гибридным агентом.
    - Выведите удостоверение сервера Exchange с помощью полного доменного имени и запишите имя сервера Exchange.
    - Если вы используете URL-адрес Подсистемы балансировки нагрузки в `TargetUri`, необходимо определить все серверы Exchange, на которых `Client Access` установлена роль и доступ к которым можно получить за URL-адресом Load Balancer.

> ⓘ **Важно!**
>
> Расширенная защита не должна быть включена в виртуальном каталоге Front-End EWS на серверах Exchange Server, опубликованных через гибридный агент.

Для защиты серверов Exchange, опубликованных с помощью гибридного агента, рекомендуется выполнить следующие действия.

> ⓘ **Примечание**

В следующем сценарии гибридный агент устанавливается на сервере, на котором не выполняется Exchange Server. Кроме того, этот сервер находится в сегменте сети, отличном от производственных серверов Exchange.

1. Для серверов Exchange, опубликованных через гибридный агент, входящие подключения должны быть ограничены брандмауэром, чтобы разрешить подключения только с компьютера, на котором установлен гибридный агент. Это не влияет на исходящие подключения с серверов Exchange Server к Exchange Online.
2. Почтовые ящики не должны размещаться на серверах Exchange, опубликованных с помощью гибридного агента. Существующие почтовые ящики следует перенести на другие серверы почтовых ящиков.

Включение расширенной защиты

Расширенная защита автоматически включается во время установки Exchange Server 2019 CU14 (или более поздней версии). В более старых версиях Exchange Server, которые поддерживают расширенную защиту, ее можно включить с помощью сценария, предоставленного корпорацией Майкрософт (рекомендуется) или вручную с помощью диспетчера IIS.

Чтобы правильно настроить расширенную защиту, каждому виртуальному каталогу на всех серверах Exchange в организации (за исключением пограничных транспортных серверов) необходимо задать предписанное значение `Extended Protection` и `sslFlags`.

В следующей таблице перечислены параметры, необходимые для каждого виртуального каталога в поддерживаемых версиях Exchange Server.

Развернуть таблицу

Веб-сайт IIS	Виртуальный каталог	Рекомендуемое значение	Рекомендуемые sslFlags
`Default Website`	`API`	`Required`	`Ssl,Ssl128`
`Default Website`	`AutoDiscover`	`Off`	`Ssl,Ssl128`
`Default Website`	`ECP`	`Required`	`Ssl,Ssl128`

Веб-сайт IIS	Виртуальный каталог	Рекомендуемое значение	Рекомендуемые sslFlags
`Default Website`	`EWS`	`Accept` (Пользовательский интерфейс) / `Allow` (Скрипт)	`Ssl,Ssl128`
`Default Website`	`MAPI`	`Required`	`Ssl,Ssl128`
`Default Website`	`Microsoft-Server-ActiveSync`	`Accept` (Пользовательский интерфейс) / `Allow` (Скрипт)	`Ssl,Ssl128`
`Default Website`	`Microsoft-Server-ActiveSync/Proxy`	`Accept` (Пользовательский интерфейс) / `Allow` (Скрипт)	`Ssl,Ssl128`
`Default Website`	`OAB`	`Accept` (Пользовательский интерфейс) / `Allow` (Скрипт)	`Ssl,Ssl128`
`Default Website`	`OWA`	`Required`	`Ssl,Ssl128`
`Default Website`	`PowerShell`	`Off`	`SslNegotiateCert`
`Default Website`	`RPC`	`Required`	`Ssl,Ssl128`
`Exchange Backend`	`API`	`Required`	`Ssl,Ssl128`
`Exchange Backend`	`AutoDiscover`	`Off`	`Ssl,Ssl128`
`Exchange Backend`	`ECP`	`Required`	`Ssl,Ssl128`
`Exchange Backend`	`EWS`	`Required`	`Ssl,Ssl128`
`Exchange Backend`	`Microsoft-Server-ActiveSync`	`Required`	`Ssl,Ssl128`
`Exchange Backend`	`Microsoft-Server-ActiveSync/Proxy`	`Required`	`Ssl,Ssl128`
`Exchange`	`OAB`	`Required`	`Ssl,Ssl128`

Веб-сайт IIS	Виртуальный каталог	Рекомендуемое значение	Рекомендуемые sslFlags
`Backend`			
`Exchange Backend`	`OWA`	`Required`	`Ssl,Ssl128`
`Exchange Backend`	`PowerShell`	`Required`	`Ssl,SslNegotiateCert,Ssl128`
`Exchange Backend`	`RPC`	`Required`	`Ssl,Ssl128`
`Exchange Backend`	`PushNotifications`	`Required`	`Ssl,Ssl128`
`Exchange Backend`	`RPCWithCert`	`Required`	`Ssl,Ssl128`
`Exchange Backend`	`MAPI/emsmdb`	`Required`	`Ssl,Ssl128`
`Exchange Backend`	`MAPI/nspi`	`Required`	`Ssl,Ssl128`

> ⓘ **Примечание**
>
> После первоначального выпуска мы обновили `Default Website/OAB Accept/Allow Required` значение вместо и `Default Website/PowerShell Off Required` вместо . Изменение в `Default Website/OAB` связано с тем, что клиенты Outlook для Mac больше не могут скачать автономную адресную книгу с параметром `Required` . Изменение заключается `Default Website/PowerShell` в том, что конфигурация Exchange Server по умолчанию не разрешает подключения с использованием проверки подлинности NTLM к PowerShell Front-End виртуальному каталогу, поэтому расширенная защита неприменима.
>
> Внесение изменений в виртуальный `Default Website/PowerShell` каталог не поддерживается за исключением случаев, когда они явно не посоветуются службой поддержки и поддержкой майкрософт (CSS).

Включение расширенной защиты с помощью установщика Exchange Server 2019 CU14 (или более

поздней версии)

При использовании Exchange Server 2019 CU14 и более поздних версий установщик Exchange Server 2019 с накопительным пакетом обновления (CU) автоматически включает расширенную защиту на сервере почтовых ящиков, где выполняется установка. Это происходит при любой новой установке или при обновлении существующей установки Exchange Server до последней версии.

Существуют два новых параметра, которые можно использовать в режиме автоматической установки для управления поведением расширенной защиты, включенной по умолчанию.

Параметры можно использовать, чтобы пропустить автоматическую активацию расширенной защиты (`/DoNotEnableEP`) или не включить расширенную защиту в виртуальном каталоге Front-End EWS (`/DoNotEnableEP_FEEWS`).

> ⚠ **Предупреждение**
>
> Отключение расширенной защиты делает сервер уязвимым для известных уязвимостей Exchange Server и ослабляет защиту от неизвестных угроз. Рекомендуется оставить эту функцию включенной.

Сценарии конфигурации установщика расширенной защиты cu

В этом разделе мы рассмотрим наиболее распространенные сценарии настройки расширенной защиты на Exchange Server с помощью установщика Накопительного пакета обновления 14 (CU) для Exchange Server 2019 (или более поздней версии).

Убедитесь, что сервер Exchange Server настроен правильно и соответствует требованиям, описанным в разделе Предварительные требования для включения расширенной защиты на Сервере Exchange Server .

Сценарий 1. Включение расширенной защиты в Exchange Server 2019

Запустите настройку Exchange Server 2019 CU14 (или более поздней версии) в режиме с репликой или автоматическим. Установщик настроит расширенную защиту при установке сервера, на котором она была запущена.

Сценарий 2. Включение расширенной защиты в Exchange Server 2019, который публикуется с помощью гибридного

агента

Выполните действия, описанные в разделе Определение серверов Exchange, опубликованных с помощью гибридного агента , чтобы определить серверы Exchange, опубликованные с помощью гибридного агента.

Запустите настройку Exchange Server 2019 CU14 (или более поздней версии) в автоматическом режиме с помощью `/DoNotEnableEP_FEEWS` параметра . Он пропускает включение расширенной защиты в виртуальном каталоге Front-End EWS:

Консоль

```
<Virtual DVD drive letter>:\Setup.exe
/IAcceptExchangeServerLicenseTerms_DiagnosticDataON /Mode:Upgrade
/DoNotEnableEP_FEEWS
```

Сценарий 3. Пропуск включения расширенной защиты с помощью установки Exchange Server 2019 CU14 (или более поздней версии)

Запустите настройку Exchange Server 2019 CU14 (или более поздней версии) в автоматическом режиме с помощью `/DoNotEnableEP` параметра . Он пропускает включение расширенной защиты:

Консоль

```
<Virtual DVD drive letter>:\Setup.exe
/IAcceptExchangeServerLicenseTerms_DiagnosticDataON /Mode:Upgrade
/DoNotEnableEP
```

> ⚠ **Предупреждение**
>
> Если не включить расширенную защиту, сервер будет уязвим для известных уязвимостей Exchange и ослабляет защиту от неизвестных угроз. Рекомендуется включить эту функцию.

Включение расширенной защиты с помощью скрипта PowerShell

Вы можете использовать скрипт ExchangeExtendedProtectionManagement.ps1 , чтобы включить расширенную защиту на некоторых или всех серверах Exchange

одновременно.

> **ⓘ Важно!**
>
> Включение расширенной защиты в среде Exchange Server включает внесение большого количества изменений на всех серверах Exchange. Вместо внесения этих изменений вручную с помощью диспетчера IIS рекомендуется использовать скрипт, предоставленный корпорацией Майкрософт.
>
> Перед запуском обязательно скачайте последнюю версию скрипта, чтобы настроить расширенную защиту.

Скрипт можно запустить на любом конкретном сервере Exchange Server в вашей среде, на котором установлена командная консоль Exchange (EMS).

Разрешения на настройку расширенной защиты с помощью скрипта PowerShell

Пользователь, который запускает скрипт, должен быть членом `Organization Management` группы ролей. Скрипт должен выполняться из командной консоли Exchange с повышенными привилегиями (EMS).

Сценарии конфигурации скриптов расширенной защиты

В этом разделе описаны наиболее распространенные сценарии настройки расширенной защиты в Exchange Server с помощью сценария PowerShellExchangeExtendedProtectionManagement.ps1 .

Дополнительные примеры и описание параметров скрипта см. в документации по скрипту .

Сценарий 1. Включение расширенной защиты на всех серверах Exchange Server

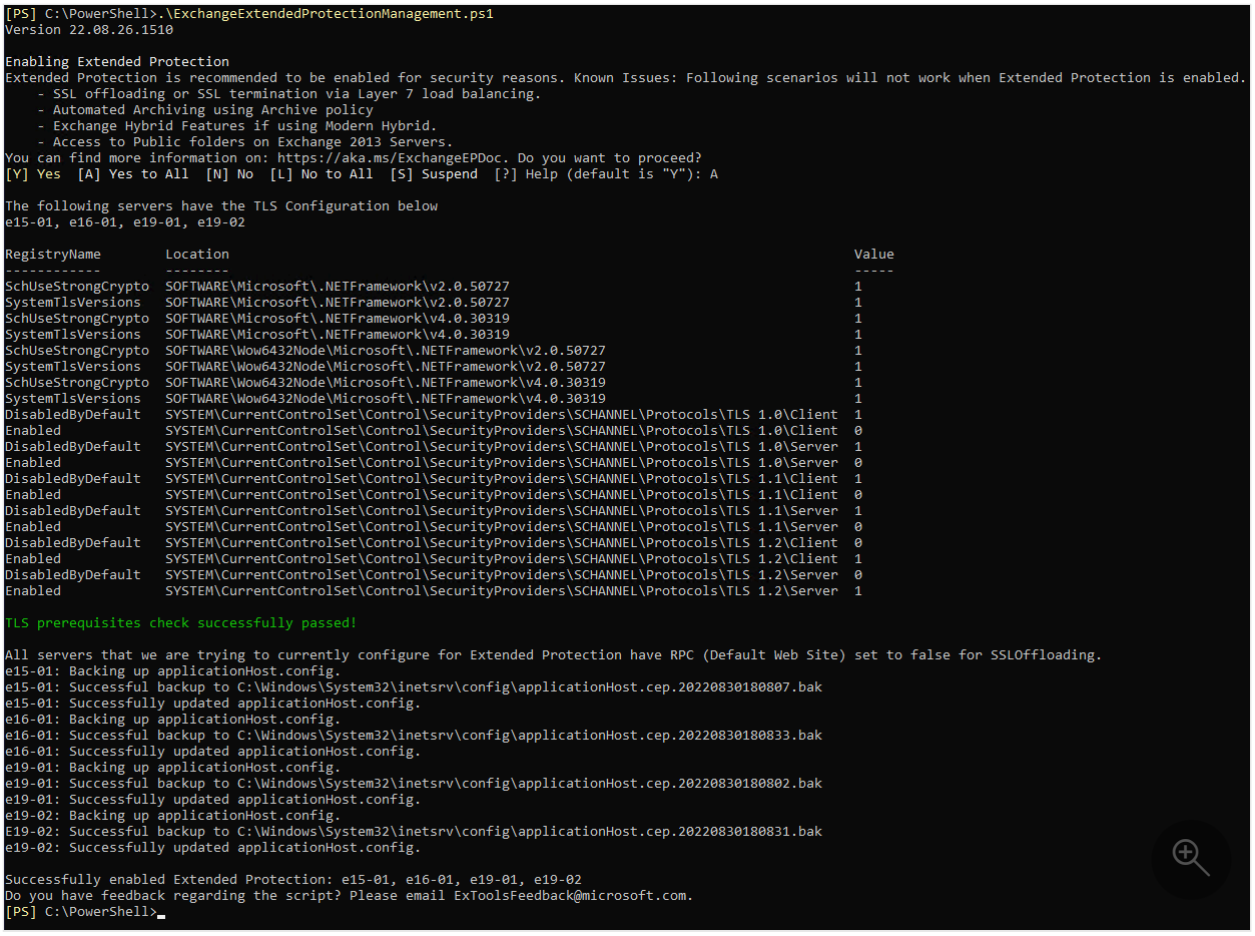
Запустите сценарий следующим образом, чтобы включить расширенную защиту на всех серверах Exchange в организации:

PowerShell

```
.\ExchangeExtendedProtectionManagement.ps1
```

Скрипт выполняет несколько проверок, чтобы убедиться, что все серверы Exchange имеют минимальную требуемую версию CU и SU для включения расширенной защиты. Он также проверяет, используют ли все серверы Exchange одну и ту же конфигурацию TLS.

После прохождения проверок предварительных требований скрипт включает расширенную защиту и добавляет необходимые ssl-флаги во все виртуальные каталоги всех серверов Exchange в области. Он останавливается, если сервер Exchange Server не выполняет требования (например, если обнаружена несогласованная конфигурация TLS).



Сценарий 2. Настройка расширенной защиты при запуске современной гибридной конфигурации

Если у вас есть современная гибридная конфигурация, необходимо пропустить включение расширенной защиты в виртуальном каталоге Front-End EWS на серверах Exchange Server, которые были опубликованы с помощью современного гибридного агента.

Эту настройку можно выполнить с помощью `ExcludeVirtualDirectories` параметра :

PowerShell

```
.\ExchangeExtendedProtectionManagement.ps1 -ExchangeServerNames MHServer1,
MHServer2 -ExcludeVirtualDirectories "EWSFrontEnd"
```

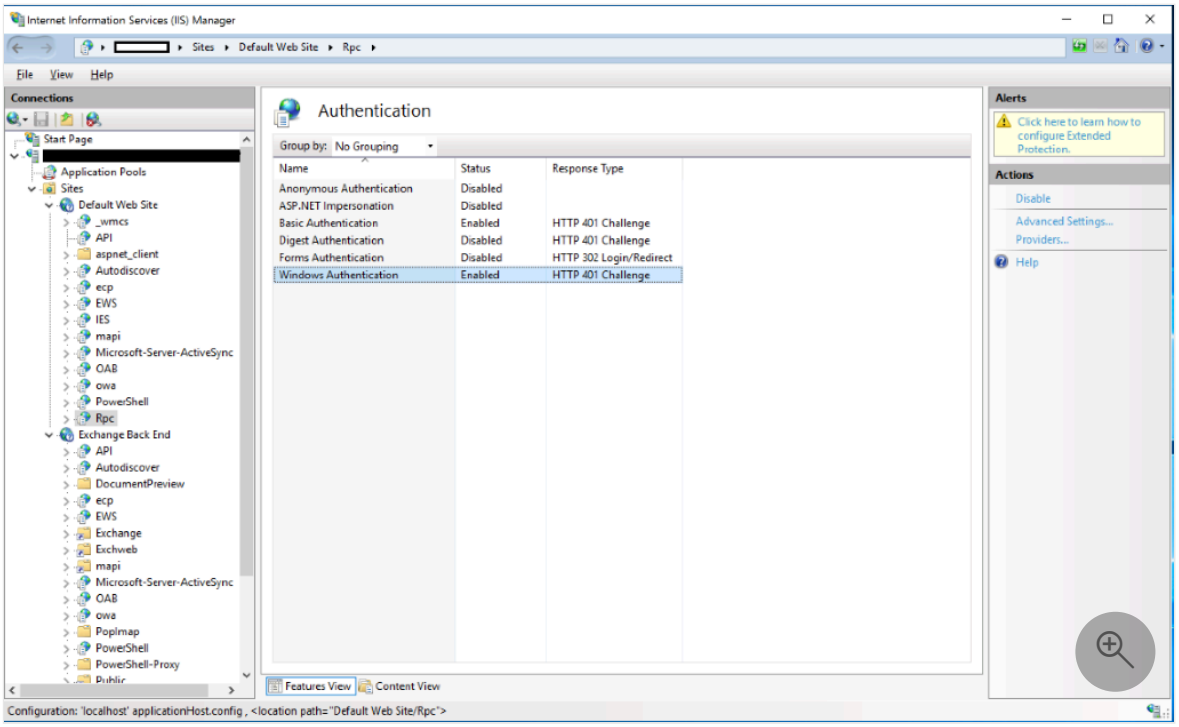
Включение расширенной защиты с помощью диспетчера IIS

Если вы хотите включить расширенную защиту в среде вручную без использования скрипта, выполните следующие действия.

> ⓘ **Примечание**
>
> При включении расширенной защиты вручную убедитесь, что для всех виртуальных каталогов на серверах Exchange настроена расширенная защита, как описано в **таблице выше**.

Установите для параметра Расширенная защита значение Обязательное или принять для в виртуальном каталоге

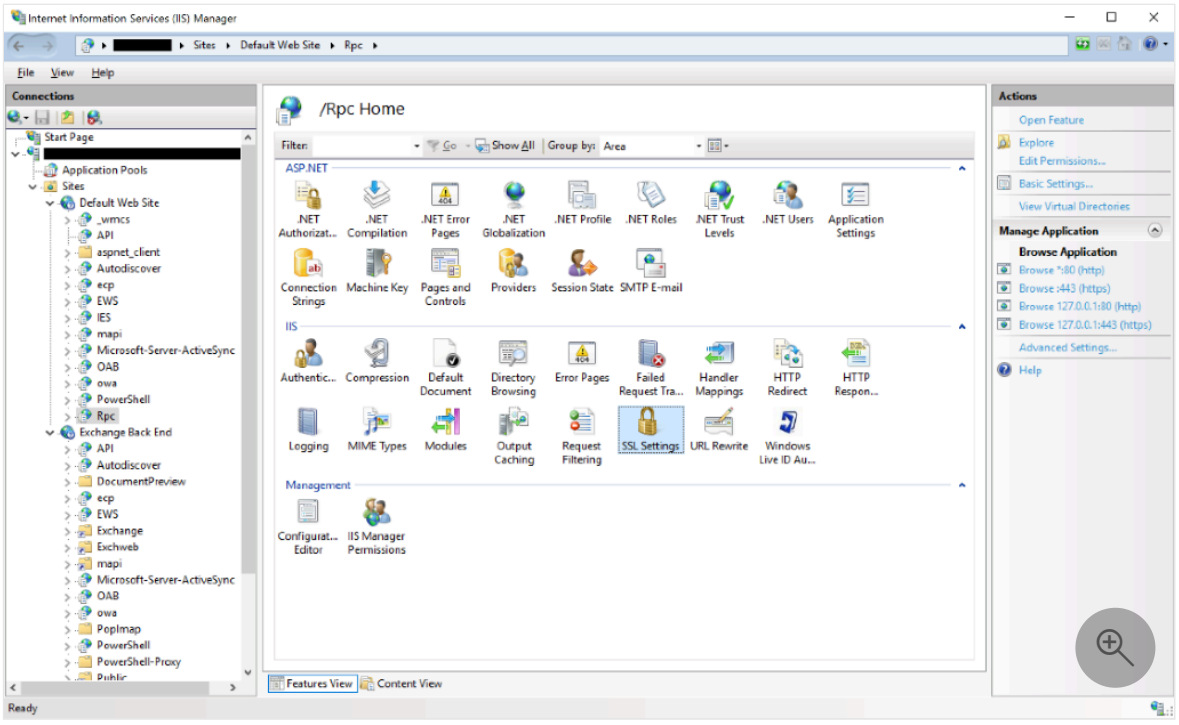
1. Запустите на `IIS Manager (INetMgr.exe)` сервере Exchange Server, на котором требуется настроить расширенную защиту.
2. Перейдите к `Sites` и выберите или `Default Web Site` `Exchange Back End`
3. Выберите виртуальный каталог, который требуется настроить.
4. Выберите `Authentication`
5. Если `Windows Authentication` параметр включен, выберите `Windows Authentication`



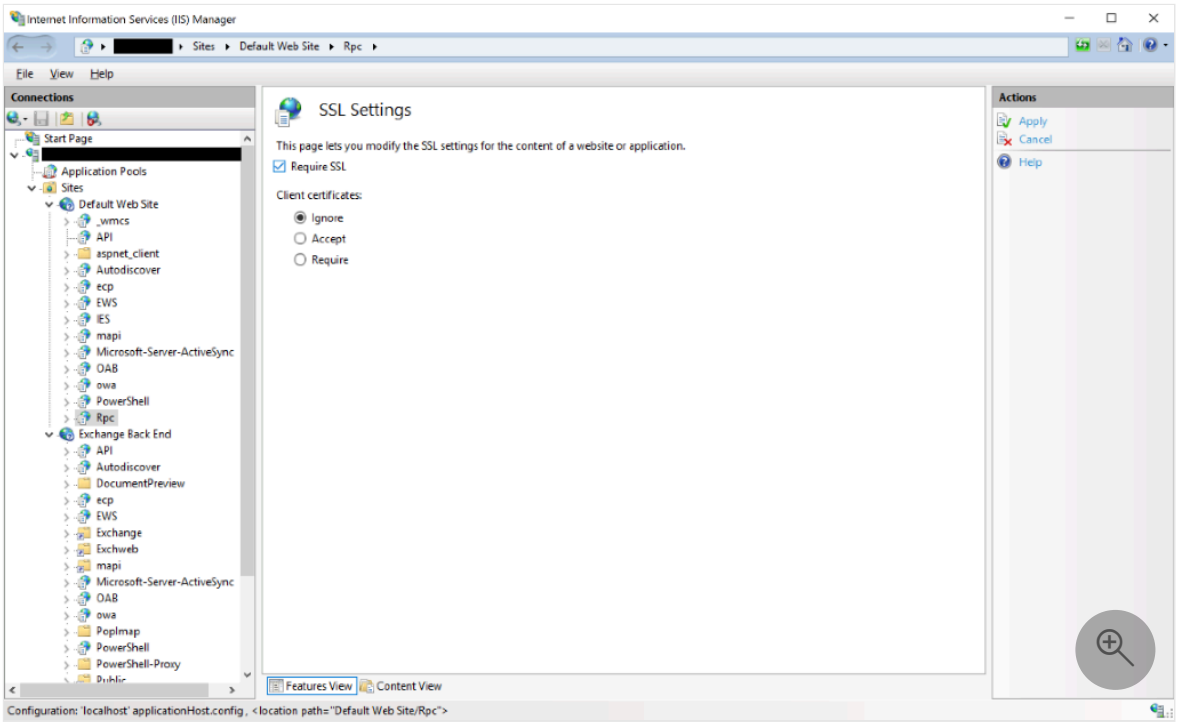
6. Выберите `Advanced Settings` (справа) и в открывающемся окне выберите подходящее значение в раскрывающемся списке Расширенная защита.

Задание параметра Обязательное ssl для виртуального каталога

1. Щелкните виртуальный каталог, чтобы открыть домашнюю страницу.



2. Выберите `SSL Settings`
3. `Require SSL` Проверьте параметры, чтобы убедиться, что `Require SSL` для виртуального каталога включена



4. Щелкните `Apply` , чтобы подтвердить новый параметр

Отключение расширенной защиты

Чтобы отключить расширенную защиту, можно использовать сценарий PowerShellExchangeExtendedProtectionManagement.ps1 .

> ⚠ **Предупреждение**

Отключение расширенной защиты делает сервер уязвимым для известных уязвимостей Exchange и ослабляет защиту от неизвестных угроз. Рекомендуется оставить эту функцию включенной.

Следующая команда отключит конфигурацию расширенной защиты для всех серверов Exchange Server, которые находятся в сети, задав для всех текущих расположений `None` настройки значение :

PowerShell

```
.\ExchangeExtendedProtectionManagement.ps1 -DisableExtendedProtection
```

Можно также указать подмножество серверов, на которых должна быть отключена расширенная защита:

PowerShell

```
.\ExchangeExtendedProtectionManagement.ps1 -DisableExtendedProtection -
ExchangeServerNames ExchServer1, ExchServer2
```

Устранение неполадок

В этом разделе содержатся известные проблемы, которые существуют с расширенной защитой, а также приведены некоторые советы по устранению неполадок для известных сценариев сбоя.

Известные проблемы с расширенной защитой

Совет

Исправлены все ранее сообщаемые проблемы с расширенной защитой на Exchange Server. Мы настоятельно рекомендуем установить **последнее обновление Exchange Server** для версии Exchange, которую вы запускаете в организации, чтобы воспользоваться последними исправлениями и улучшениями.

Проблема. При выполнении /PrepareSchema, /PrepareDomain или /PrepareAllDomains в автоматическом режиме Exchange Server 2019 CU14 программа установки показывает, что расширенная защита активирована.

Это известная проблема с Exchange Server 2019 CU14, которую можно игнорировать. Расширенная защита не включена при запуске `/PrepareSchema` или `/PrepareDomain` `/PrepareAllDomains` для подготовки среды, как описано в документации по подготовке Active Directory и доменов для Exchange Server .

Проблема. Изменение разрешений для общедоступных папок с помощью клиента Outlook завершается сбоем со следующей ошибкой: "Измененные разрешения не могут быть изменены"

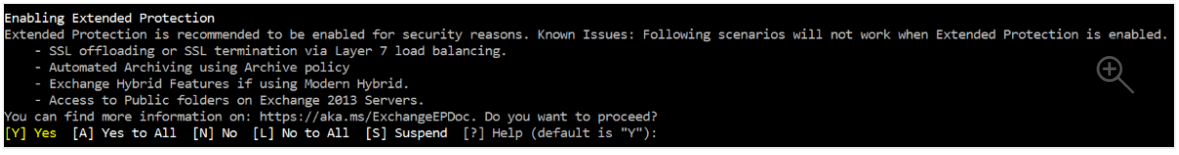
Эта проблема возникает, если общедоступная папка, для которой вы пытаетесь изменить разрешения, размещена в дополнительном почтовом ящике общедоступных папок, а основной почтовый ящик общедоступных папок находится на другом сервере.

Проблема устранена с помощью последнего обновления Exchange Server . Следуйте инструкциям, описанным в этом кб , чтобы включить исправление.

Предупреждения и ошибки при выполнении скрипта конфигурации расширенной защиты

1. Скрипт отображает предупреждение об известных проблемах и запрашивает подтверждение:

   Чтобы предотвратить запуск администраторов в сценариях, в которых существующие функции Exchange Server нарушаются из-за включения расширенной защиты, скрипт предоставляет список сценариев, в которых имеются известные проблемы. Внимательно прочитайте и оцените этот список, прежде чем включать расширенную защиту. Чтобы включить расширенную защиту, нажмите клавишу `Y`.

2. Скрипт не включает расширенную защиту из-за сбоя проверки готовности:

   - Ни на сервере Exchange Server не выполняется сборка, которая поддерживает расширенную защиту:

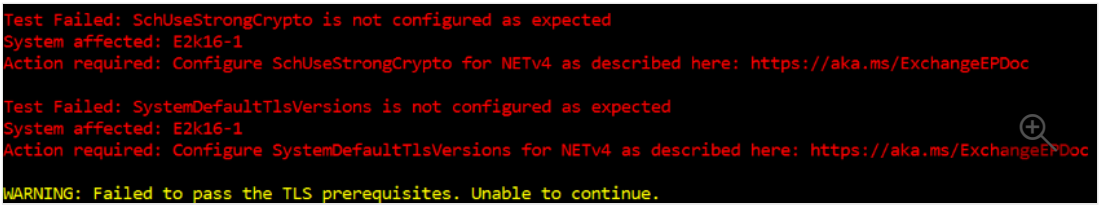
     Если ни на сервере Exchange Server в организации не выполняется сборка, поддерживающая расширенную защиту, скрипт не включает

расширенную защиту на неподдерживаемых серверах, чтобы убедиться, что обмен данными между серверами не завершится сбоем.

Чтобы устранить эту проблему, обновите все серверы Exchange до последней версии CU и SU и запустите скрипт еще раз, чтобы включить расширенную защиту.

- Обнаружено несоответствие TLS:

  На всех серверах Exchange в области требуется допустимая и согласованная конфигурация TLS . Если параметры TLS на всех серверах в области не совпадают, включение расширенной защиты нарушает клиентские подключения к серверам почтовых ящиков.



  Дополнительные сведения см. в рекомендациях по настройке TLS для Exchange Server .

3. Некоторые серверы Exchange недоступны и недоступны:

   Скрипт выполняет несколько тестов для всех серверов Exchange, которые находятся в области. Если один или несколько из этих серверов недоступны, скрипт исключает их, так как он не может выполнить требуемое действие настройки на этих компьютерах.

   Если сервер находится в автономном режиме, следует настроить расширенную защиту, как только он снова будет подключен. Если сервер недоступен по другим причинам, следует запустить скрипт на самом сервере, чтобы включить расширенную защиту.

Пользователи не могут получить доступ к своему почтовому ящику через один или несколько клиентов

Может быть несколько причин, по которым некоторые или все клиенты могут начать предоставлять пользователям ошибки проверки подлинности после включения расширенной защиты.

- Пользователи не могут получить постоянный или периодический доступ к почтовому ящику с помощью Outlook для Windows, Outlook для Mac, Outlook Mobile или собственного почтового клиента iOS:

  - Если конфигурация TLS в организации Exchange не совпадает (например, конфигурация TLS была изменена на одном из серверов Exchange после включения расширенной защиты), эта неправильная настройка может привести к сбою клиентских подключений. Чтобы устранить эту проблему, ознакомьтесь с инструкциями по правильной настройке TLS на всех серверах Exchange, а затем используйте скрипт для повторной настройки расширенной защиты.

  - Проверьте, используется ли разгрузка SSL . Любое завершение SSL приводит к сбою проверки маркера привязки канала расширенной защиты, так как разгрузка SSL считается человеком в середине, что предотвращается расширенной защитой. Чтобы устранить эту проблему, отключите разгрузку SSL и снова включите расширенную защиту с помощью скрипта.

- Пользователи могут получать доступ к электронной почте с помощью Outlook для Windows и OWA, но не через клиенты, отличные от Windows, такие как Outlook для Mac, Outlook Mobile или собственный почтовый клиент iOS. Это может произойти, если параметру расширенной защиты для EWS и (или) Exchange ActiveSync задано значение `Required` на одном или всех Front-End серверах:

  - Чтобы устранить эту проблему, запустите `ExchangeExtendedProtectionManagement.ps1` скрипт с параметром `ExchangeServerNames` и передайте имя сервера Exchange Server с неправильно настроенным параметром расширенной защиты. Вы также можете запустить скрипт без какого-либо параметра, чтобы снова проверить и настроить расширенную защиту для всех серверов.

  - Кроме того, можно также использовать `IIS Manager (INetMgr.exe)` и изменить параметр расширенной защиты для этих виртуальных каталогов на правильное значение, как указано в таблице. Мы настоятельно рекомендуем использовать скрипт, так как он проверяет правильные значения и выполняет перенастройку автоматически, если значения не заданы должным образом.

- Пользователи не могут получить доступ к OWA или ECP с помощью браузера Apple Safari в macOS или iOS, если используется единый вход NTLM и

включена расширенная защита:

- Пользователям на платформе macOS рекомендуется использовать веб-браузер с поддержкой расширенной защиты. Мы рекомендуем использовать Microsoft Edge (Chromium).
- Для пользователей на платформе iOS нет веб-браузера с поддержкой расширенной защиты.
- Решение, которое работает на обеих платформах, заключается в настройке гибридной современной проверки подлинности для OWA и ECP или использовании проверки подлинности на основе утверждений AD FS в Outlook в Интернете.

Если после выполнения описанных выше действий некоторые клиенты по-прежнему не работают должным образом, вы можете временно откатить расширенную защиту и сообщить о проблеме в корпорацию Майкрософт, задав обращение в службу поддержки. Выполните действия, описанные в разделе Отключение расширенной защиты .

Гибридная миграция "свободная/занят" или миграция почтовых ящиков не работает

Если вы используете современную гибридную среду, включение расширенной защиты может привести к тому, что гибридные функции, такие как доступность и миграция почтовых ящиков, перестают работать, если конфигурация не была выполнена, как описано в этой статье. Чтобы устранить эту проблему, определите гибридные серверы, опубликованные с помощью гибридного агента , и отключите расширенную защиту в виртуальном каталоге Front-End EWS на этих серверах.

Общедоступные папки больше не отображаются и недоступны

Существует две проблемы, которые могут повлиять на подключение к общедоступным папкам, если включена расширенная защита. Обязательно следуйте инструкциям, описанным в разделе Расширенная защита и общедоступные папки этой статьи.

Вопросы и ответы

Вопрос: Требуется ли установить обновление для системы безопасности за август 2022 г., если оно уже было установлено в предыдущем накопительном пакете обновления (CU)?

Ответ: Да, при обновлении до более новой сборки CU необходимо снова установить su за август 2022 г. (например, Exchange Server 2019 CU11 до Exchange Server 2019 CU12).

Помните: Если вы планируете выполнить обновление немедленно (означает установку CU + SU), расширенную защиту не нужно выключать. Если вы планируете оставаться в CU без немедленной установки su, необходимо отключить расширенную защиту, так как сборка cu (без установки su) не поддерживает расширенную защиту и, следовательно, у вас могут возникнуть проблемы с подключением клиента.

Вопрос: Безопасно ли включить расширенную защиту в среде, которая использует службы федерации Active Directory (AD FS) для Outlook в Интернете (OWA)?
Ответ: Да, расширенная защита не влияет на проверку подлинности на основе утверждений AD FS с помощью OWA.

Вопрос: Безопасно ли включить расширенную защиту Windows в среде, которая использует гибридную современную проверку подлинности (HMA)?
Ответ: Да, это изменение не повлияет на HMA. Хотя расширенная защита еще больше не улучшает HMA, проверку подлинности Windows по-прежнему можно использовать для приложений, которые не поддерживают гибридную современную проверку подлинности. Учитывая это, включение расширенной защиты рекомендуется в любой среде, в которой по-прежнему есть локальные службы Exchange.

Вопрос: Влияет ли расширенная защита на гибридную современную проверку подлинности или интеграцию с Microsoft Teams?
Ответ: Расширенная защита не влияет на интеграцию Microsoft Teams или гибридную современную проверку подлинности.

Вопрос: Мне не удается получить доступ к OWA/ECP после включения расширенной защиты с кодом состояния HTTP 400, моя OWA/ECP публикуется через прокси приложения Entra, что можно сделать, чтобы устранить эту проблему?
Ответ: Публикация Exchange OWA/ECP через прокси приложения Entra не поддерживается. Вам потребуется опубликовать OWA/ECP через поддерживаемую топологию сети в соответствии с расширенными стандартами защиты.

Вопрос: Хотя мы понимаем, что предотвращение атак MitM важно, можем ли мы иметь собственные устройства в середине с собственными сертификатами?
Ответ: Если устройство использует тот же сертификат, что и сервер Exchange Server, их можно использовать.

Exchange Server обнаружения заголовков P2 FROM, не совместимых с RFC

Статья • 03.01.2025

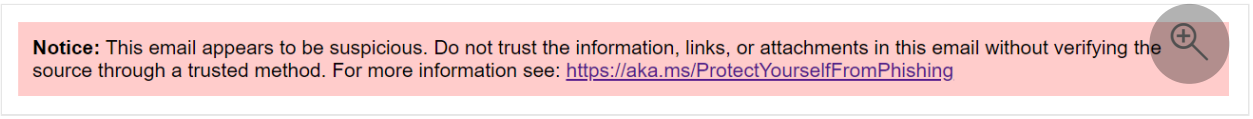
Обзор

Корпорация Майкрософт знает об уязвимости (CVE-2024-49040), которая позволяет злоумышленникам выполнять спуфинговые атаки на Microsoft Exchange Server. Уязвимость вызвана текущей реализацией проверки заголовка `P2 FROM`, которая происходит в транспорте. Текущая реализация позволяет передавать некоторые заголовки P2 FROM, не совместимые с RFC 5322, что может привести к тому, что почтовый клиент (например, Microsoft Outlook) отображает поддельный отправитель, как если бы он был законным.

Начиная с обновления системы безопасности (SU) Exchange Server ноября 2024 г., Exchange Server могут обнаруживать и помечать сообщения электронной почты, содержащие потенциально вредоносные шаблоны, в заголовке P2 FROM.

Как это работает

Если Exchange Server обнаруживает подозрительное сообщение, оно автоматически добавляет следующее заявление об ответственности к тексту сообщения электронной почты:



Exchange Server также добавляет `X-MS-Exchange-P2FromRegexMatch` заголовок во все сообщения электронной почты, обнаруженные этой функцией. Если вы хотите выполнить какие-либо действия с сообщениями электронной почты, обнаруженными функцией, можно использовать правило транспорта Exchange (ETR), чтобы обнаружить заголовок и выполнить определенное действие. В этом примере Exchange Server отклоняет сообщение электронной почты, если оно содержит заголовок:

```
PowerShell
```

```
New-TransportRule -HeaderContainsMessageHeader "X-MS-Exchange-
P2FromRegexMatch" -HeaderContainsWords @("True") -RejectMessageReasonText
"Message not accepted due to a non-RFC compliant P2 FROM header" -Name
"NonCompliantP2FromDetectionRule" -SenderAddressLocation "Header"
```

Дополнительные сведения о правилах потока обработки почты см. в статье Правила потока обработки почты в документации по Exchange Server.

Конфигурация

Новое поведение включено по умолчанию в рамках нашего **подхода защиты по умолчанию** . Хотя можно управлять функцией с помощью New-SettingOverride. В этом разделе объясняется, как можно управлять этой функцией. Обязательно выполните следующие команды из командной консоли Exchange с повышенными привилегиями (EMS).

Если вы предпочитаете, чтобы Exchange автоматически добавлял заявление об отказе к сообщениям, обнаруженным компонентом, можно отключить действие от ответственности, сохраняя при этом настраиваемое действие заголовка включенным. Это позволяет обнаруживать эти сообщения электронной почты с помощью ETR и обрабатывать их по-разному, например путем добавления заявления об отказе от ответственности по вашему выбору. Следующие команды отключают действие отказ от ответственности:

PowerShell

```
New-SettingOverride -Name "DisableP2FromRegexMatchDisclaimer" -Component
"Transport" -Section "NonCompliantSenderSettings" -Parameters
@("AddDisclaimerforRegexMatch=false") -Reason "Disabled For Troubleshooting"
Get-ExchangeDiagnosticInfo -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh
Restart-Service -Name MSExchangeTransport
```

Если вы предпочитаете, чтобы Exchange автоматически добавлял `X-MS-Exchange-P2FromRegexMatch` заголовок в сообщения электронной почты, обнаруженные этой функцией, можно отключить действие заголовка, сохраняя действие от ответственности включенным. Это переопределение параметра появилось в обновлении SUv2 за ноябрь 2024 г. Exchange Server. Чтобы отключить настраиваемое действие заголовка, используйте следующие команды:

PowerShell

```
New-SettingOverride -Name "DisableP2FromRegexMatchHeader" -Component
"Transport" -Section "NonCompliantSenderSettings" -Parameters
@("AddP2FromRegexMatchHeader=false") -Reason "Disabled For Troubleshooting"
Get-ExchangeDiagnosticInfo -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh
Restart-Service -Name MSExchangeTransport
```

Настоятельно рекомендуется оставить эту функцию включенной, так как отключение функции упрощает для злоумышленников фишинговые атаки на вашу организацию. Если вы хотите отключить функцию вообще, используйте следующие команды, чтобы отключить отказ от ответственности и настраиваемое действие заголовка:

PowerShell

```
New-SettingOverride -Name "DisableP2FromRegexMatchDisclaimer" -Component
"Transport" -Section "NonCompliantSenderSettings" -Parameters
@("AddDisclaimerforRegexMatch=false") -Reason "Disabled For Troubleshooting"
New-SettingOverride -Name "DisableP2FromRegexMatchHeader" -Component
"Transport" -Section "NonCompliantSenderSettings" -Parameters
@("AddP2FromRegexMatchHeader=false") -Reason "Disabled For Troubleshooting"
Get-ExchangeDiagnosticInfo -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh
Restart-Service -Name MSExchangeTransport
```

Настройка http Strict Transport Security (HSTS) в Exchange Server

Статья • 15.11.2023

Обзор

Http Strict Transport Security (HSTS) — это широко поддерживаемый стандарт , который помогает защитить посетителей веб-сайта, гарантируя, что их браузер всегда подключается по протоколу HTTPS. HSTS работает путем отправки специального заголовка HTTP-ответа с сервера в браузер с именем `Strict-Transport-Security` (STS). Этот заголовок содержит директиву `max-age` , указывающую продолжительность времени (в секундах), чтобы браузер помнил, что доступ к сайту можно получить только по протоколу HTTPS. Когда браузер получает этот заголовок, он автоматически изменяет все HTTP-запросы для доступа к сайту на HTTPS-запросы.

HSTS не только добавляет защиту от распространенных сценариев атак, но и помогает устранить необходимость в распространенной (и теперь небезопасной) практике перенаправления пользователей с URL-адреса HTTP на URL-адрес HTTPS. HSTS также можно использовать для устранения активных и пассивных сетевых атак. Однако HSTS не устраняет уязвимости вредоносных программ, фишинга или браузеров.

Принцип работы HSTS

Браузеру предписывается принудительно применять HSTS, когда он получает `Strict-Transport-Security` заголовок через HTTPS-подключение. Однако существуют некоторые требования, которые должны быть выполнены, прежде чем браузер применяет HSTS. В частности, сертификат, используемый для шифрования сеанса:

- Должен быть допустимым и доверенным для клиента;
- Срок действия не должен истек; И
- Должен содержать домен или поддомен, который был вызван в браузере.

Дополнительные рекомендации см. в статье Безопасный просмотр веб-страниц с помощью Microsoft Edge .

Когда браузер узнает, что домен включил HSTS, он:

- Всегда используйте `https://` подключение, в том числе при щелчке по ссылке `http://` или после ввода URL-адреса в адресной строке без указания протокола.
- Удаляет возможность для пользователей щелкать предупреждения (например, просроченные или недопустимые сертификаты, несоответствия имен и т. д.).

Существуют некоторые сценарии (например, у пользователя есть новый компьютер, новый профиль, новый браузер или удалены данные и параметры браузера), в которых пользователь уязвим в течение короткого периода времени, так как он посещает сайт в первый раз без принудительного применения HSTS. Для решения этих сценариев проект Chromium поддерживает `HSTS Preload List` (который также используется другими браузерами, такими как Microsoft Edge и Mozilla Firefox). Применяет `Preload List` HSTS даже при первом посещении сайта.

Вы можете отправить свой домен в список HSTS. Веб-сервер (или, в нашем случае, сервер Exchange Server) также должен отправить директиву `preload` как часть заголовка `Strict-Transport-Security` , чтобы сообщить, что предварительная загрузка HSTS должна быть выполнена браузером.

Как Exchange Server обрабатывает HTTP-подключения

По умолчанию Exchange Server не перенаправляет трафик HTTP в HTTPS, так как для веб-сайта по умолчанию требуется ПРОТОКОЛ SSL. Дополнительные сведения см. в разделе Параметры по умолчанию для виртуальных каталогов Exchange .

Однако можно настроить автоматическое перенаправление с HTTP на HTTPS, выполнив действия, описанные в разделе Настройка перенаправления http на https для Outlook в Интернете в Exchange Server, и в результате Exchange Server принимает подключения, установленные через HTTP, и отвечает с `HTTP 302 redirect`помощью .

HSTS может помочь значительно сократить число небезопасных перенаправлений HTTP на HTTPS, так как перезапись на HTTPS выполняется самим браузером, а не сервером `HTTP 302 redirect` в ответе. Использование HSTS также может привести к повышению производительности, хотя это не является основной целью.

Независимо от конфигурации по умолчанию (которая не разрешает незашифрованные подключения), рекомендуется указать `Strict-Transport-Security` заголовок в качестве части заголовка ответа.

Включение HSTS на Exchange Server

Заголовок STS можно настроить в Exchange Server 2019 г. и Exchange Server 2016 г., хотя способ настройки каждой версии отличается.

> ⓘ **Важно!**
>
> HSTS необходимо настроить только в , `Default Web Site` так как это конечная точка, к которой подключаются клиенты. HSTS не следует настраивать в `Exchange Back End`. Также следует рассмотреть возможность настройки HSTS через заголовок ответа на устройствах, работающих перед сервером Exchange Server на уровне 7 (например, подсистемы балансировки нагрузки или обратные прокси-серверы).

Рекомендуется начать с `max-age` конфигурации 300 секунд, что составляет 5 минут. После внесения изменений следует внимательно следить за подключением клиента к серверу Exchange Server и откатить изменения, если возникнет какая-либо проблема.

`max-age` Обновите значение до одной недели (`604800`) или одного месяца (`2592000`) и дождитесь полного `max-age` этапа, прежде чем переходить дальше. Значение `max-age` одного года (`31536000`) должно быть задано как минимальное с точки зрения безопасности, а также по крайней мере обязательно, если вы планируете добавить домен в `HSTS Preload List`. `max-age` Рекомендуется задать значение двух лет (`63072000`).

> ⓘ **Примечание**
>
> В следующих примерах задается `max-age` значение 300 секунд, что является конфигурацией, которая должна использоваться только для проверки функциональности. Обязательно измените значение атрибута на более высокое, когда вы будете готовы к переносу конфигурации в рабочую среду.

Exchange Server 2019

Чтобы настроить Exchange Server 2019 для отправки заголовка `Strict-Transport-Security`, можно использовать Windows PowerShell или пользовательский интерфейс диспетчера IIS. В следующем разделе описаны оба метода.

Конфигурация HSTS является конфигурацией для каждого сервера и поэтому должна выполняться на каждом сервере Exchange Server.

Настройка HSTS с помощью PowerShell

Выполните следующие команды в окне PowerShell с повышенными привилегиями, чтобы настроить и включить HSTS:

> ⓘ **Примечание**
>
> Чтобы настроить более высокое `max-age` значение для Exchange Server 2019 г., можно снова выполнить команды, используя более высокое значение. Нет необходимости удалять существующую конфигурацию заранее.

PowerShell

```
Import-Module IISAdministration
Reset-IISServerManager -Confirm:$false
Start-IISCommitDelay

$sitesCollection = Get-IISConfigSection -SectionPath
"system.applicationHost/sites" | Get-IISConfigCollection
$siteElement = Get-IISConfigCollectionElement -ConfigCollection
$sitesCollection -ConfigAttribute @{"name"="Default Web Site"}
$hstsElement = Get-IISConfigElement -ConfigElement $siteElement -
ChildElementName "hsts"
Set-IISConfigAttributeValue -ConfigElement $hstsElement -AttributeName
"enabled" -AttributeValue $true
Set-IISConfigAttributeValue -ConfigElement $hstsElement -AttributeName "max-
age" -AttributeValue 300
Set-IISConfigAttributeValue -ConfigElement $hstsElement -AttributeName
"includeSubDomains" -AttributeValue $true
```

Если вы планируете добавить домен в `HSTS Preload List`, необходимо убедиться, что директива `preload` также отправляется как часть заголовка `Strict-Transport-Security` . Не следует отправлять директиву, `preload` если вы не планируете отправлять домен в `HSTS Preload List`.

PowerShell

```
Set-IISConfigAttributeValue -ConfigElement $hstsElement -AttributeName
"preload" -AttributeValue $true
```

Наконец, для завершения настройки HSTS необходимо выполнить следующие команды:

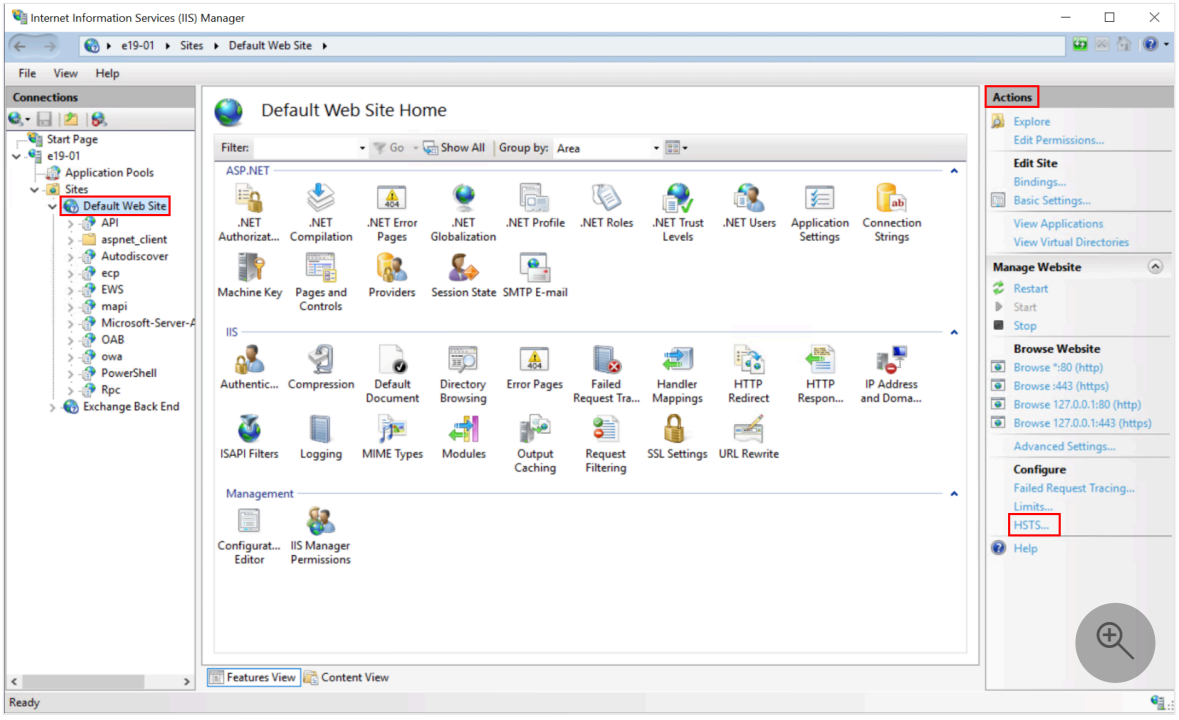
PowerShell

```
Stop-IISCommitDelay
Remove-Module IISAdministration
```

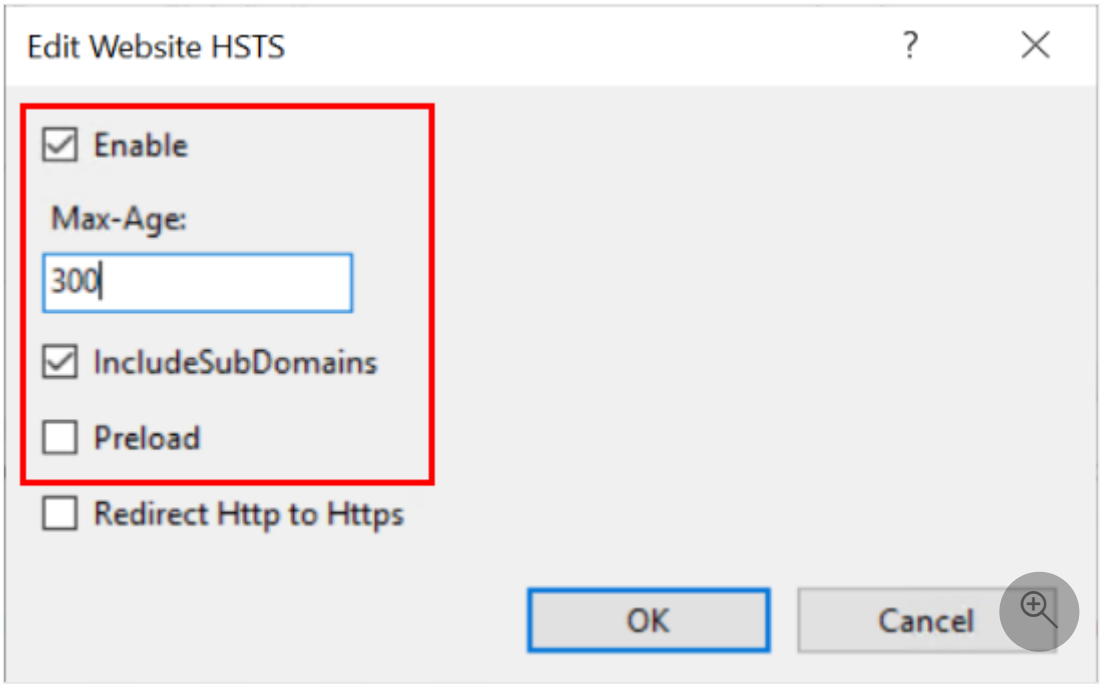
Настройка HSTS с помощью диспетчера IIS

Чтобы настроить и включить HSTS, выполните следующие действия в диспетчере служб IIS.

1. Запуск диспетчера IIS (`InetMgr.exe`)
2. Перейдите к `Sites` и щелкните `Default Web Site`
3. `Actions` В меню выберите `HSTS...`



4. `Enable` Установите флажок, определите `max-age` значение и выберите директивы в соответствии с описанием в этой статье.



> ⓘ **Важно!**
>
> Мы не можем перенаправить HTTP на HTTPS с помощью конфигурации HSTS, так как это нарушает подключение в некоторых сценариях, включая командную консоль Exchange (EMS). Если вы хотите включить перенаправление http to HTTPS, необходимо выполнить действия, описанные в разделе Настройка перенаправления http to https для Outlook в Интернете в Exchange Server.

5. Щелкните `OK` , чтобы завершить и активировать конфигурацию.

Exchange Server 2016

> ⓘ **Примечание**
>
> Хотя настройка HSTS возможна с помощью пользовательского интерфейса в операционных системах, поддерживаемых Exchange Server 2019 г., этот элемент управления изначально недоступен в операционных системах, поддерживаемых Exchange Server 2016 г. Поэтому мы описываем только шаги, которые необходимо выполнить с помощью PowerShell.

Чтобы настроить Exchange Server 2016 для отправки заголовка `Strict-Transport-Security`, выполните следующие команды в окне PowerShell с повышенными привилегиями. Конфигурация HSTS является конфигурацией для каждого сервера и поэтому должна выполняться на каждом сервере Exchange.

> ⓘ **Примечание**
>
> Чтобы настроить более высокое `max-age` значение для Exchange Server 2016, необходимо сначала **удалить заголовок HTTP-ответа**, прежде чем снова выполнять следующие команды.

Windows Server 2012 & 2012 R2

Если вы не планируете добавлять домен в `HSTS Preload List`, необходимо убедиться, что директива `preload` не отправлена в качестве части заголовка `Strict-Transport-Security` . Выполните следующую команду, чтобы настроить HSTS ***без*** отправки директивы `preload` :

PowerShell

```
Import-Module WebAdministration
Add-WebConfigurationProperty -Filter
"system.webServer/httpProtocol/customHeaders" -PSPath "IIS:\Sites\Default
Web Site" -Name . -AtElement @{name="Strict-Transport-Security"} -Value
@{name="Strict-Transport-Security";value="max-age=300; includeSubDomains"}
```

или

Если вы планируете добавить домен в `HSTS Preload List`, необходимо убедиться, что директива `preload` отправлена как часть заголовка `Strict-Transport-Security` . Выполните следующую команду, чтобы настроить Exchange Server отправку `preload` директивы в рамках конфигурации HSTS:

PowerShell

```
Import-Module WebAdministration
Add-WebConfigurationProperty -Filter
"system.webServer/httpProtocol/customHeaders" -PSPath "IIS:\Sites\Default
Web Site" -Name . -AtElement @{name="Strict-Transport-Security"} -Value
@{name="Strict-Transport-Security";value="max-age=300; includeSubDomains;
preload"}
```

Windows Server 2016

PowerShell

```
Import-Module IISAdministration
Reset-IISServerManager -Confirm:$false
```

```
Start-IISCommitDelay

$iisConfig = Get-IISConfigSection -SectionPath
"system.webServer/httpProtocol" -CommitPath "Default Web Site" | Get-
IISConfigCollection -CollectionName "customHeaders"
```

Если вы не планируете добавлять домен в `HSTS Preload List`, необходимо убедиться, что директива `preload` не отправлена в качестве части заголовка `Strict-Transport-Security` . Выполните следующую команду, чтобы настроить HSTS ***без*** отправки директивы `preload` :

PowerShell

```
New-IISConfigCollectionElement -ConfigCollection $iisConfig -ConfigAttribute
@{"name"="Strict-Transport-Security"; "value"="max-age=300;
includeSubDomains";}
```

или

Если вы планируете добавить домен в `HSTS Preload List`, необходимо убедиться, что директива `preload` отправлена как часть заголовка `Strict-Transport-Security` . Выполните следующую команду, чтобы настроить Exchange Server отправку `preload` директивы в рамках конфигурации HSTS:

PowerShell

```
New-IISConfigCollectionElement -ConfigCollection $iisConfig -ConfigAttribute
@{"name"="Strict-Transport-Security"; "value"="max-age=300;
includeSubDomains; preload";}
```

Наконец, для завершения настройки HSTS необходимо выполнить следующие команды:

PowerShell

```
Stop-IISCommitDelay
Remove-Module IISAdministration
```

Отключение HSTS на Exchange Server

Если вы хотите остановить отправку заголовка `Strict-Transport-Security` Exchange Server, можно выполнить откат конфигурации для каждого сервера. Действия по отключению HSTS отличаются в Exchange Server 2016 г. и Exchange Server 2019 г.

> ⓘ **Примечание**
>
> Спецификация HSTS позволяет отправлять директиву `max-age` со значением `0`. Эту конфигурацию можно использовать для перезаписи кэшированных сведений о политике HSTS в браузерах. Если вы планируете удалить конфигурацию Exchange Server HSTS, может быть полезно сначала задать `max-age` значение `0` перед удалением конфигурации заголовка `Strict-Transport-Security`.

Exchange Server 2019

Чтобы Exchange Server 2019 прекратить отправку заголовка `Strict-Transport-Security`, можно использовать Windows PowerShell или пользовательский интерфейс диспетчера IIS. В следующем разделе описаны оба метода.

Настройка HSTS с помощью PowerShell

Выполните следующие команды в окне PowerShell с повышенными привилегиями, чтобы отключить HSTS:

PowerShell

```
Import-Module IISAdministration
Reset-IISServerManager -Confirm:$false
Start-IISCommitDelay

$sitesCollection = Get-IISConfigSection -SectionPath
"system.applicationHost/sites" | Get-IISConfigCollection
$siteElement = Get-IISConfigCollectionElement -ConfigCollection
$sitesCollection -ConfigAttribute @{"name"="Default Web Site"}
$hstsElement = Get-IISConfigElement -ConfigElement $siteElement -
ChildElementName "hsts"
Set-IISConfigAttributeValue -ConfigElement $hstsElement -AttributeName
"enabled" -AttributeValue $false
Set-IISConfigAttributeValue -ConfigElement $hstsElement -AttributeName "max-
age" -AttributeValue 0
Set-IISConfigAttributeValue -ConfigElement $hstsElement -AttributeName
"includeSubDomains" -AttributeValue $false
```

Если предыдущая конфигурация HSTS была для отправки директивы `preload`, убедитесь, что она также отключена:

> ⓘ **Важно!**

Не забудьте [запросить удаление из списка предварительной загрузки HSTS]. Если вы забудете удалить домен из списка предварительной загрузки, браузеры по-прежнему будут пытаться применить HSTS.

PowerShell

```
Set-IISConfigAttributeValue -ConfigElement $hstsElement -AttributeName
"preload" -AttributeValue $false
```

Наконец, для завершения настройки HSTS необходимо выполнить следующие команды:

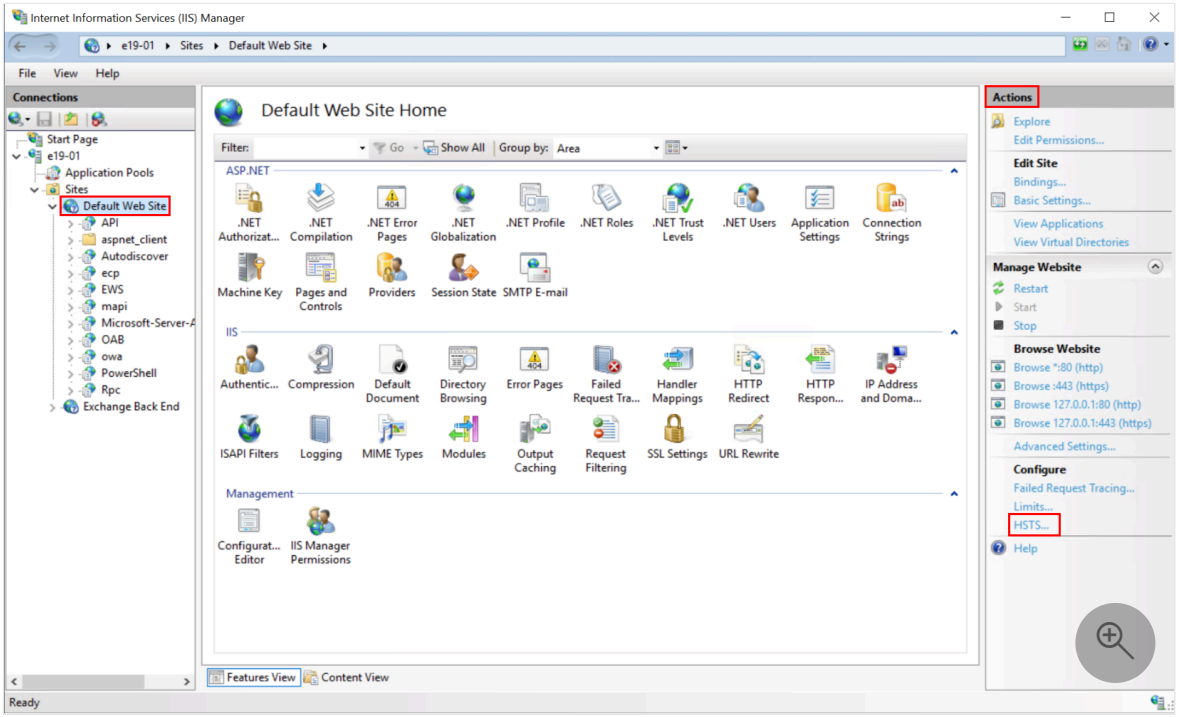
PowerShell

```
Stop-IISCommitDelay
Remove-Module IISAdministration
```

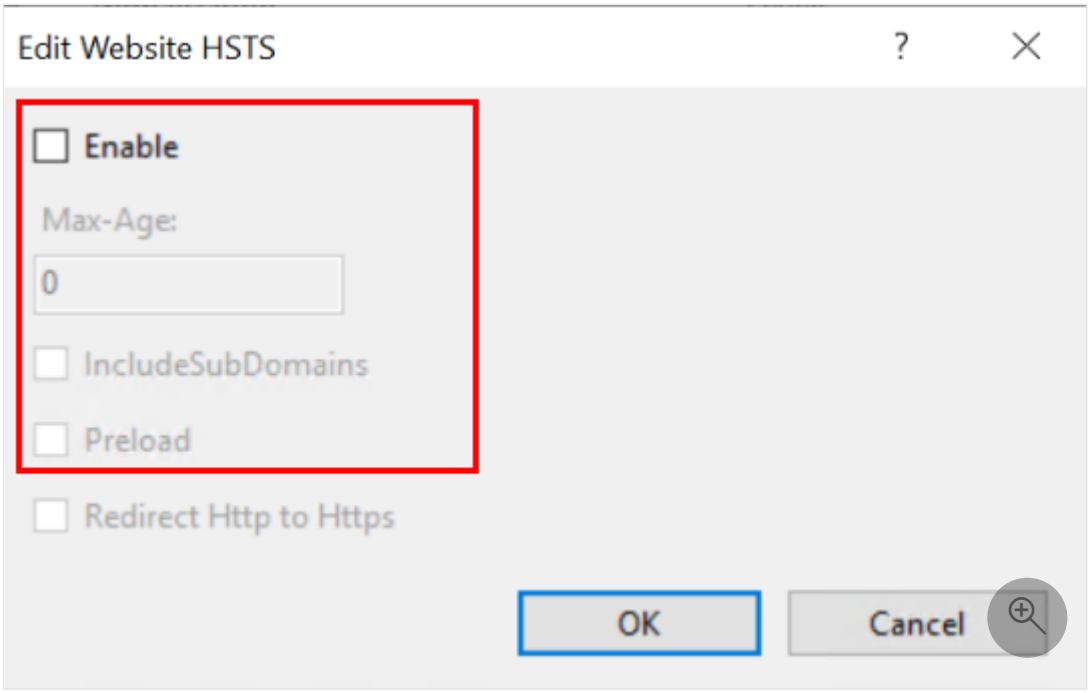
Настройка HSTS с помощью диспетчера IIS

Чтобы отключить HSTS, выполните следующие действия в диспетчере служб IIS.

1. Запуск диспетчера IIS (`InetMgr.exe`)
2. Перейдите к `Sites` и щелкните `Default Web Site`
3. `Actions` В меню выберите `HSTS...`



4. Снимите флажок все директивы, установите `max-age` для директивы значение `0` и, наконец, снимите флажок `Enable`



5. Щелкните `OK` , чтобы завершить настройку.

Exchange Server 2016

> ⓘ **Примечание**
>
> Хотя настройка HSTS возможна с помощью пользовательского интерфейса в операционных системах, поддерживаемых Exchange Server 2019 г., этот элемент управления изначально недоступен в операционных системах, поддерживаемых Exchange Server 2016 г. Поэтому мы описываем только шаги, которые необходимо выполнить с помощью PowerShell.

Чтобы Exchange Server 2016 прекратить отправку `Strict-Transport-Security` заголовка, выполните следующие команды в окне PowerShell с повышенными привилегиями на каждом сервере Exchange.

Windows Server 2012 & 2012 R2

PowerShell

```
Import-Module WebAdministration
Remove-WebConfigurationProperty -PSPath "IIS:\Sites\Default Web Site" -
```

```
Filter "system.webServer/httpProtocol/customHeaders" -Name . -AtElement
@{name="Strict-Transport-Security"}
```

Windows Server 2016

PowerShell

```
Import-Module IISAdministration
Reset-IISServerManager -Confirm:$false
Start-IISCommitDelay

$iisConfig = Get-IISConfigSection -SectionPath
"system.webServer/httpProtocol" -CommitPath "Default Web Site" | Get-
IISConfigCollection -CollectionName "customHeaders"
```

Если предыдущая конфигурация HSTS ***не отправляла*** директиву `preload` , выполните следующую команду:

PowerShell

```
Remove-IISConfigCollectionElement -ConfigCollection $iisConfig -
ConfigAttribute @{"name"="Strict-Transport-Security"; "value"="max-age=300;
includeSubDomains";}
```

или

Если предыдущая конфигурация HSTS была ***для отправки*** `preload` директивы, обязательно выполните следующую команду:

PowerShell

```
Remove-IISConfigCollectionElement -ConfigCollection $iisConfig -
ConfigAttribute @{"name"="Strict-Transport-Security"; "value"="max-age=300;
includeSubDomains; preload";}
```

Наконец, для завершения настройки HSTS необходимо выполнить следующие команды:

PowerShell

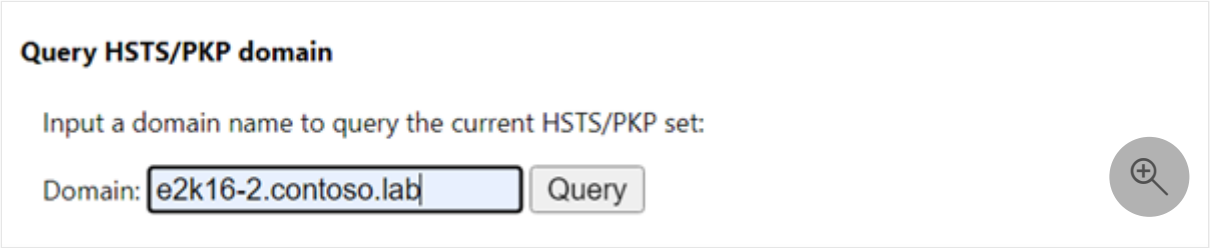
```
Stop-IISCommitDelay
Remove-Module IISAdministration
```

Проверка правильности работы HSTS

Лучший способ убедиться, что защита HSTS работает должным образом, — использовать современный браузер, поддерживающий HSTS (например, Microsoft Edge, Firefox, Chrome, Safari, Opera и т. д.). При использовании браузера Microsoft Edge можно выполнить следующие действия. Если вы используете другой браузер, ознакомьтесь с документацией, чтобы узнать, какие действия по проверке флагов HSTS:

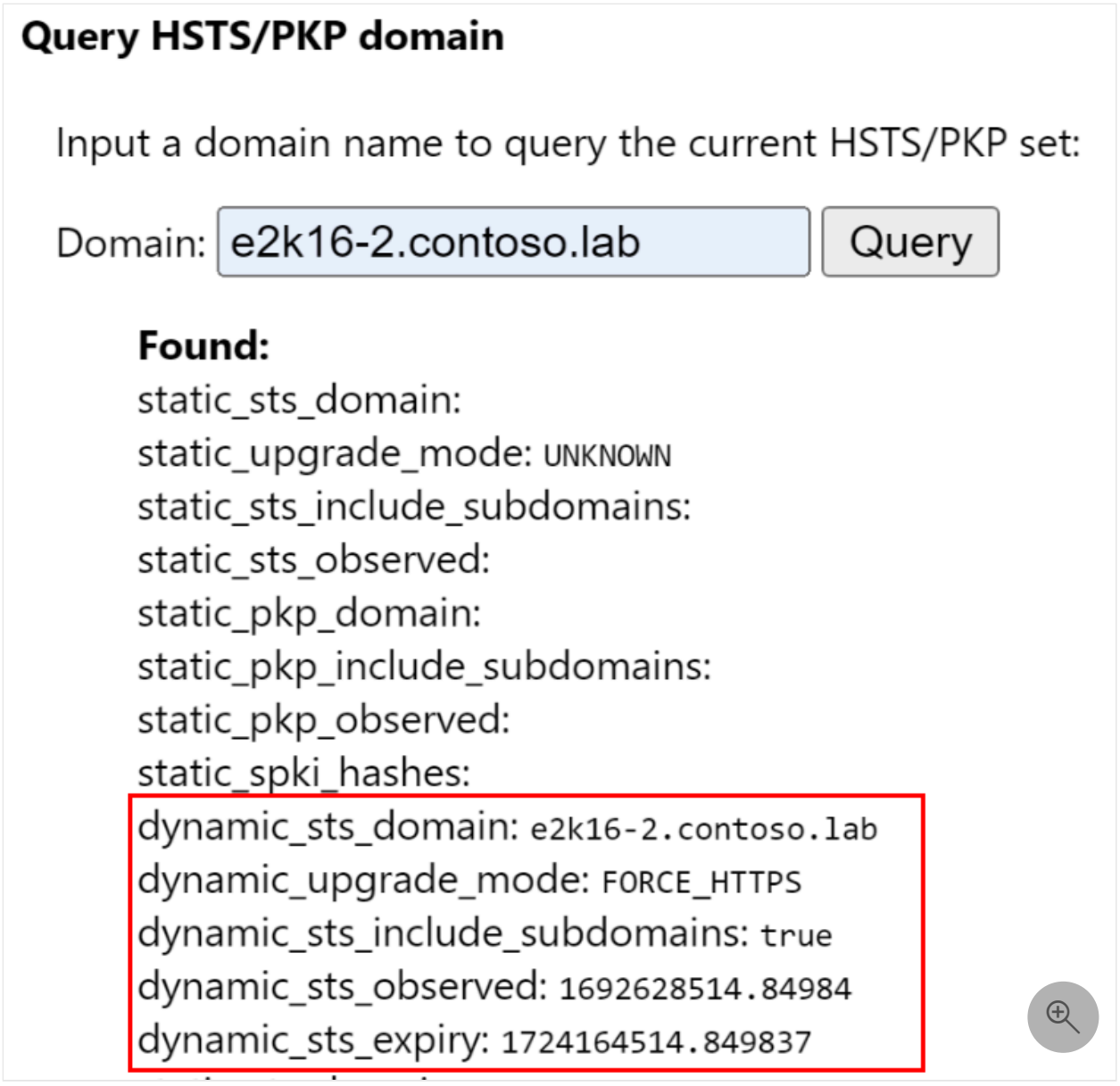
1. Откройте браузер и установите HTTPS-подключение к OWA или ECP. Убедитесь, что сертификат, возвращенный сервером Exchange Server, соответствует используемому домену (например, e2k16-2.contoso.lab) и является доверенным для клиентского компьютера (так как это необходимо для активации защиты HSTS браузера для домена).
2. Введите `edge://net-internals/#hsts` в адресной строке и нажмите клавишу ВВОД.
3. Введите доменное имя, используемое для доступа к OWA или ECP (например, e2k16-2.contoso.lab), `Query HSTS/PKP domain` и нажмите клавишу ВВОД.

Пример.



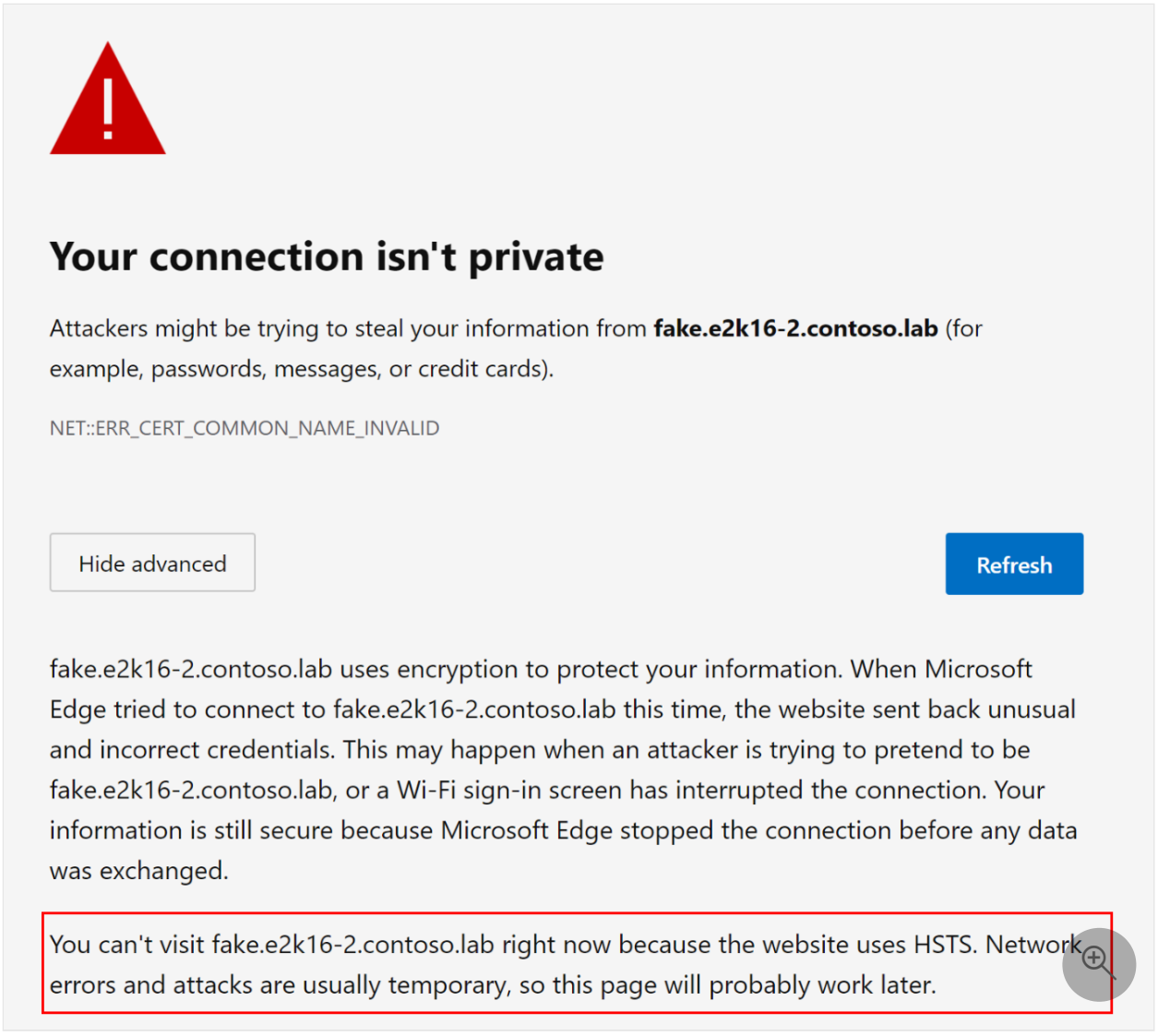
Если результат имеет значение `Not found`, это означает, что HSTS не используется для домена. Причина может быть в том, что URL-адрес ранее не был посещен или срок действия записи с хранилищем политик HSTS истек (он действителен в течение времени, указанного в директиве `max-age`).

Если результат найден, выходные данные выглядят следующим образом:

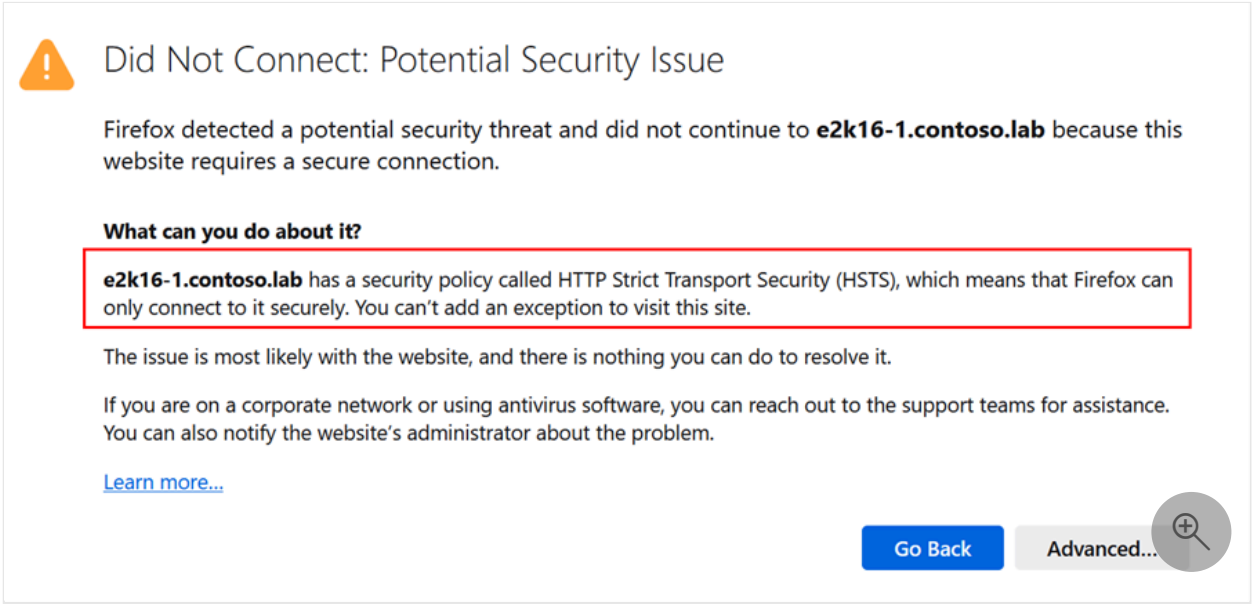


Если используется HSTS и подключение не является доверенным (например, URL-адрес не соответствует домену, для которого выдан сертификат, или сертификат не является доверенным или истек), пользователь видит следующее предупреждение, которое **невозможно обойти**:

Блокирующая страница Microsoft Edge:



Блокировка страницы Mozilla Firefox:



Настройка подписи сертификатов полезных данных сериализации PowerShell в Exchange Server

Статья • 13.11.2024

Обзор

Подписывание полезных данных сериализации PowerShell на основе сертификатов — это функция глубокой защиты для предотвращения вредоносных манипуляций с сериализованными данными, передаваемыми через сеансы командной консоли Exchange (EMS). Он доступен Exchange Server 2013, Exchange Server 2016 и Exchange Server 2019 годах.

Эта функция появилась в обновлении системы безопасности Exchange Server за январь 2023 г. Он был отправлен как отключенный по умолчанию (согласие) и должен быть включен администратором Exchange Server. Его можно включить с помощью переопределения параметра (Exchange Server 2016 и Exchange Server 2019) или с помощью значения реестра (Exchange Server 2013 г.).

При установке обновления безопасности за ноябрь 2023 г. (или более поздней версии) Exchange Server эта функция включается по умолчанию (отказ) для каждого сервера и должна быть отключена администратором Exchange Server, если вы не хотите ее использовать. Перед установкой обновления для системы безопасности за ноябрь 2023 г. (или более поздней версии) Exchange Server убедитесь, что необходимые условия для включения подписи сертификатов сериализованных данных. Чтобы отключить функцию, необходимо создать переопределение параметра, которое явно выключает функцию.

Что такое сериализация данных

Сериализация данных — это процесс преобразования состояния объекта в форму (поток байтов), который можно сохранить или передать в память, базу данных или файл. Например, PowerShell использует сериализацию при передаче объектов .NET между сеансами. После отправки или сохранения объекта его можно восстановить в прежнем формате. Этот процесс называется десериализацией.

Если вы хотите узнать больше о сериализации данных в PowerShell, рекомендуем ознакомиться с записью блога Как объекты отправляются в удаленные сеансы и

из них.

Предварительные требования для включения подписи сертификатов сериализованных данных

Существуют некоторые предварительные требования, которые должны быть выполнены до подписывания сертификатов полезных данных сериализации PowerShell, которые можно включить без нарушения подключения между серверами Exchange Server.

- На всех серверах Exchange в вашей среде должно быть выпущено обновление системы безопасности Exchange Server за январь 2023 г. или более поздняя версия. Если эта функция включена в среде с серверами Exchange, которые не поддерживают подписывание сериализации, могут возникнуть проблемы при обмене данными между серверами или при использовании командной консоли Exchange.
- Все серверы Exchange (кроме пограничных транспортных средств и только серверов средств управления) должны иметь доступ к сертификату проверки подлинности Exchange Server, который должен быть действительным и не должен быть истек.

  > **Совет**
  >
  > Скрипт MonitorExchangeAuthCertificate можно использовать, чтобы проверка, действителен ли сертификат проверки подлинности Exchange Server. Его также можно использовать для автоматического продления сертификата OAuth или для замены сертификата, если срок его действия уже истек.

Проверка использования подписи сертификатов полезных данных сериализации PowerShell

Вы можете проверить, включена ли подпись сертификата для полезных данных сериализации PowerShell, проверив `DataSerialization` файл журнала, который

поддерживается Exchange Server. Файл журнала можно найти в следующем каталоге: `<ExchangeInstallPath>\V15\Logging\Data\Serialization`.

Exchange поддерживает один файл журнала для каждого процесса. При открытии командной консоли Exchange (EMS) создается новый файл журнала. При открытии второго EMS будет записан другой файл журнала. Синтаксис именования файлов журнала — `DataSerialization<yyyyMMdd>-<N>.LOG`. Размер каждого из файлов журнала может быть не более `10 MB` . Максимальный размер каталога журнала сериализации ограничен `1 GB` по умолчанию. Файлы журнала удаляются, если они старше `30 days`.

Столбец `EventData` содержит имя процесса и индикатор, который показывает, используется ли подпись сериализации.

Пример использования входа в сериализацию:

```
"S:MSG=SerializationTypeConverter Initialized, Process Name = w3wp,
SerializationSigningEnabled = True, IsCustomParserEnabled = True"
```

Пример не используется для подписи сериализации:

```
"S:MSG=SerializationTypeConverter Initialized, Process Name = powershell,
SerializationSigningEnabled = False, IsCustomParserEnabled = True"
```

Включение подписи сертификатов полезных данных сериализации PowerShell

> **ⓘ Важно!**
>
> Не нужно создавать переопределение параметра при запуске **обновления для системы безопасности за ноябрь 2023 г. (или более поздней версии) Exchange Server**. Подпись сертификата для функции полезных данных сериализации PowerShell включена по умолчанию при выполнении этой сборки.

Включить при запуске Exchange Server 2016 и Exchange Server 2019

Необходимо создать переопределение параметра, чтобы включить подписывание сертификатов полезных данных сериализации PowerShell.

1. Выполните следующую команду из командной консоли Exchange с повышенными привилегиями (EMS) на сервере, на котором выполняется Exchange Server в вашей среде:

```
PowerShell

New-SettingOverride -Name "EnableSigningVerification" -Component Data -
Section EnableSerializationDataSigning -Parameters @("Enabled=true") -
Reason "Enabling Signing Verification"
```

> ⓘ **Примечание**
>
> Эта команда позволяет всем серверам, работающим Exchange Server 2016 и Exchange Server 2019 в вашей среде, подписывать сертификаты полезных данных сериализации PowerShell. Вам не нужно выполнять команду на каждом сервере Exchange Server.

2. Обновите аргумент VariantConfiguration, выполнив следующую команду:

```
PowerShell

Get-ExchangeDiagnosticInfo -Process
Microsoft.Exchange.Directory.TopologyService -Component
VariantConfiguration -Argument Refresh
```

3. Необходимо перезапустить `World Wide Web Publishing service` и на сервере `Windows Process Activation Service` Exchange Server, на котором было создано переопределение параметра. Выполните следующую команду в окне PowerShell с повышенными привилегиями или перезапустите сервер:

```
PowerShell

Restart-Service -Name W3SVC, WAS -Force
```

Включить при запуске Exchange Server 2013

Если вы запускаете Exchange Server 2013 г., подписывание сертификатов полезных данных сериализации PowerShell должно быть включено путем создания значения реестра для каждого Exchange Server 2013 года.

1. Создайте значение реестра в Exchange Server 2013, выполнив следующую команду:

PowerShell

```
New-ItemProperty -Path
HKLM:\SOFTWARE\Microsoft\ExchangeServer\v15\Diagnostics -Name
"EnableSerializationDataSigning" -Value 1 -Type String
```

2. Необходимо перезапустить `World Wide Web Publishing service` и на каждом сервере `Windows Process Activation Service` Exchange 2013, на котором было создано значение реестра. Выполните следующую команду в окне PowerShell с повышенными привилегиями или перезапустите сервер:

PowerShell

```
Restart-Service -Name W3SVC, WAS -Force
```

Отключение подписи сертификатов полезных данных сериализации PowerShell

Отключить при запуске Exchange Server 2016 и Exchange Server 2019

Чтобы отключить эту функцию в Exchange Server 2016 или Exchange Server 2019 г., необходимо удалить или явно установить значение отключено.

> ⚠ **Предупреждение**
>
> Отключение подписи сертификатов полезных данных сериализации PowerShell делает сервер уязвимым для известных уязвимостей Exchange и ослабляет защиту от неизвестных угроз. Рекомендуется оставить эту функцию включенной.

1. Удалите переопределение параметра или явно задайте для него значение `Enabled=false`:

   При запуске su от января 2023 г. по октябрь 2023 г. exchange SU необходимо удалить переопределение параметра, чтобы отключить эту функцию.

   Выполните следующую команду из командной консоли Exchange с повышенными привилегиями:

PowerShell

```
Get-SettingOverride -Identity "EnableSigningVerification" | Remove-
SettingOverride
```

или

При запуске exchange SU за ноябрь 2023 г. или более поздней версии необходимо создать переопределение параметра, чтобы явно отключить эту функцию.

Выполните следующую команду из командной консоли Exchange с повышенными привилегиями:

PowerShell

```
New-SettingOverride -Name "DisableSigningVerification" -Component Data
-Section EnableSerializationDataSigning -Parameters @("Enabled=false")
-Reason "Disable Signing Verification"
```

2. Обновите аргумент VariantConfiguration, выполнив следующую команду:

PowerShell

```
Get-ExchangeDiagnosticInfo -Process
Microsoft.Exchange.Directory.TopologyService -Component
VariantConfiguration -Argument Refresh
```

3. Необходимо перезапустить `World Wide Web Publishing service` и на сервере `Windows Process Activation Service` Exchange Server, на котором было удалено или обновлено переопределение параметра. Выполните следующую команду в окне PowerShell с повышенными привилегиями или перезапустите сервер:

PowerShell

```
Restart-Service -Name W3SVC, WAS -Force
```

4. Закройте командную консоль Exchange (EMS), которая использовалась для выполнения команд, упомянутых на предыдущих шагах. Это важно для немедленного применения конфигурации.

Отключить при запуске Exchange Server 2013

Чтобы отключить эту функцию Exchange Server 2013, необходимо удалить значение реестра, чтобы явно задать значение `0`.

1. Задайте для параметра реестра значение `0` Exchange Server 2013, выполнив следующую команду:

   PowerShell

   ```
   Set-ItemProperty -Path
   HKLM:\SOFTWARE\Microsoft\ExchangeServer\v15\Diagnostics -Name
   "EnableSerializationDataSigning" -Value 0
   ```

2. Необходимо перезапустить `World Wide Web Publishing service` и на каждом сервере `Windows Process Activation Service` Exchange 2013, на котором было изменено значение реестра. Выполните следующую команду в окне PowerShell с повышенными привилегиями или перезапустите сервер:

   PowerShell

   ```
   Restart-Service -Name W3SVC, WAS -Force
   ```

Известные проблемы с подписью сертификатов сериализованных данных

> ⓘ **Важно!**
>
> Всегда устанавливайте последнее обновление Exchange Server, так как оно устраняет некоторые проблемы, перечисленные в этом разделе. Проблемы, устраненные последним обновлением, помечаются флажком.

- ❌ Если включено подписывание полезных данных сериализации PowerShell, сертификат проверки подлинности с истекшим сроком действия не позволит командлету `Get-ExchangeCertificate` возвращать сведения о сертификате.
- ✅ Если включено подписывание полезных данных сериализации PowerShell, `Get-ExchangeCertificate` командлет не возвращает видимое значение при выполнении на компьютере с установленными только средствами управления Exchange, независимо от допустимости сертификата проверки подлинности.
- ❌Некоторые скрипты, включенные в Exchange Server, например `RedistributeActiveDatabases.ps1`, могут работать неправильно при следующих

условиях:
    - Функция подписывания полезных данных сериализации PowerShell включена.
    - Вы не используете группы безопасности по умолчанию, предоставляемые Exchange RBAC.
    - Скрипт запускается пользователем, который не является членом `Organization Management` группы ролей.

- Приведенные ниже скрипты PowerShell не работают должным образом при выполнении на компьютере, на котором установлены только средства управления Exchange без какой-либо другой роли Exchange Server. Чтобы устранить эту проблему, запустите сценарий на Exchange Server с ролью почтового ящика с помощью командной консоли Exchange с повышенными привилегиями (EMS).
    - ✅ `RedistributeActiveDatabases.ps1`
    - ✅ `StartDagServerMaintenance.ps1`
    - ✅ `Manage-MetaCacheDatabase.ps1`
    - ✅ `Move-PublicFolderBranch.ps1`

- ❌Некоторые командлеты PowerShell, передаваемые по каналу, могут не выполняться на компьютере, на котором установлены только средства управления Exchange и нет других Exchange Server роли. Чтобы устранить эту проблему, используйте `ForEach-Object` , как показано в примерах, или запустите их на сервере Exchange Server с установленной ролью почтового ящика. Это влияет на различные сочетания командлетов, например:
    - `Get-Mailbox | Get-CalendarDiagnosticLog`
    - `Get-Mailbox | Get-MailboxFolderPermission`
    - `Get-Mailbox | Get-MailboxFolderStatistics`
    - `Get-MailboxDatabase | Get-MailboxStatistics`
    - `Get-MailboxDatabase | Get-Mailbox`
    - `Get-MailboxDatabase | Test-ExchangeSearch`
    - `Get-PublicFolderClientPermission | Remove-PublicFolderClientPermission`

      Если вы хотите использовать их на сервере средств управления Exchange (без установленной другой роли Exchange Server), можно обойти эту проблему, как показано ниже:

PowerShell

```
Get-Mailbox | ForEach-Object { Get-CalendarDiagnosticLog -Identity
$_.Name }
Get-Mailbox | ForEach-Object { Get-MailboxFolderPermission -Identity
$_.Name }
Get-Mailbox | ForEach-Object { Get-MailboxFolderStatistics -Identity
$_.Name }
Get-MailboxDatabase | ForEach-Object { Get-MailboxStatistics -
Database $_.Name }
Get-MailboxDatabase | ForEach-Object { Get-Mailbox -Database $_.Name
}
Get-MailboxDatabase | ForEach-Object { Test-ExchangeSearch -
MailboxDatabase $_.Name }
Get-PublicFolderClientPermission \pf1 | ForEach-Object { Remove-
PublicFolderClientPermission -Identity $_.Identity.ToString() -User
$_.User.ToString() }
```

Служба экстренного устранения рисков (EM) для Exchange

Статья • 15.11.2023

Служба экстренного устранения рисков для Exchange (служба EM) помогает защитить безопасность серверов Exchange Server, применяя меры по устранению любых потенциальных угроз для ваших серверов. Она использует облачную службу конфигурации Office (OCS) для проверки и загрузки доступных средств защиты, а также для отправки диагностических данных в корпорацию Майкрософт.

Служба EM работает как служба Windows на сервере почтовых ящиков Exchange. При установке накопительного пакета обновления за сентябрь 2021 г. (или более поздней версии) на Exchange Server 2016 или Exchange Server 2019 служба EM автоматически устанавливается на серверах с ролью почтового ящика. Служба EM не будет установлена на пограничных транспортных серверах.

Использование службы EM является необязательным. Если вы не хотите, чтобы корпорация Майкрософт автоматически применяла меры по устранению рисков к серверам Exchange, эту функцию можно отключить.

Устранение рисков

Устранение рисков — это действие или набор действий, выполняющихся автоматически для защиты сервера Exchange от известной угрозы, которая активно используется. Чтобы защитить организацию и снизить риски, служба EM может автоматически отключать те или иные функции или компоненты сервера Exchange Server.

Служба EM может применять следующие типы мер по устранению рисков:

- **Устранение рисков правила перезаписи URL-адресов IIS** — эта мера по устранению рисков представляет собой правило, блокирующее определенные шаблоны вредоносных HTTP-запросов, которые могут поставить под угрозу сервер Exchange Server.
- **Устранение рисков службы Exchange** — эта мера по устранению рисков отключает уязвимую службу на сервере Exchange Server.
- **Устранение рисков пула приложений** — эта мера по устранению рисков отключает уязвимый пул приложений на сервере Exchange Server.

Вы можете просматривать все примененные меры по устранению рисков и управлять ими с помощью командлетов PowerShell Exchange и сценариев.

Как это работает

Если корпорация Майкрософт узнает об угрозе безопасности, мы можем создать и выпустить меру по устранению рисков. В этом случае мера по устранению рисков будет отправлена из OCS в службу EM в виде подписанного XML-файла, содержащего параметры конфигурации, необходимые для применения этой меры по устранению рисков.

После установки службы EM она каждый час проверяет OCS на наличие доступных мер по устранению рисков. Затем служба EM скачивает XML-файл и проверяет подпись, чтобы убедиться, что XML-файл не был изменен. Служба EM проверяет издателя файла, расширенное использование ключа и цепочку сертификатов. После успешной проверки служба EM применяет меру по устранению рисков.

Каждая мера по устранению рисков является временным решением, пока не будет применено обновление безопасности, устраняющее уязвимость. Служба EM не является заменой для SU Exchange. Тем не менее, это самый быстрый и удобный способ устранить наиболее опасные риски для подключенных к Интернету серверов Exchange Server в локальной среде перед обновлением.

Список выпущенных мер по устранению рисков

В следующей таблице описывается репозиторий для выпущенных мер по устранению рисков.

Развернуть таблицу

Серийный номер	Идентификатор мер по устранению рисков	Описание	Минимальная применимая версия	Максимальная применимая версия	Процедура отката
1	PING1	Проба пульса EEMS. Не изменяет параметры Exchange.	Exchange 2019 г.: CU за сентябрь 2021 г. Exchange 2016 г.: CU за сентябрь 2021 г.	-	Откат не требуется.

Серийный номер	Идентификатор мер по устранению рисков	Описание	Минимальная применимая версия	Максимальная применимая версия	Процедура отката
2	M1	Устранение рисков CVE-2022-41040 с помощью конфигурации перезаписи URL-адресов.	Exchange 2019: RTM Exchange 2016: RTM	Exchange 2019: октябрь 2022 г. Exchange 2016: октябрь 2022 г.	Удалите правило **EEMS M1.1 PowerShell — входящий** вручную из модуля перезаписи URL-адресов IIS на веб-сайте по умолчанию.

Предварительные условия

Если эти предварительные требования еще не установлены на сервере Windows Server, где установлен Exchange, программа установки предложит вам установить следующие предварительные требования во время проверки готовности:

- Модуль перезаписи URL-адресов IIS
- Универсальная среда выполнения C в Windows (KB2999226) для Windows Server 2012 и Windows Server 2012 R2

Соединение

Службе EM требуется исходящее соединение с OCS для проверки и загрузки мер по устранению рисков. Если исходящее подключение к OCS недоступно во время установки Exchange Server, программа установки выдает предупреждение во время проверки готовности.

Хотя служба EM может быть установлена без подключения к OCS, она должна иметь подключение к OCS, чтобы загрузить и применить последние меры по устранению рисков. OCS должен быть доступен с компьютера, на котором установлен Exchange Server, чтобы служба EM работала правильно.

Развернуть таблицу

Конечная точка	Адрес	Порт	Описание
Служба конфигурации Office	`officeclient.microsoft.com/*`	443	Необходимая конечная точка для службы Exchange EM

> **ⓘ Важно!**
>
> Обязательно исключите подключения к `officeclient.microsoft.com` из рабочих процессов проверки SSL, выполняемых брандмауэрами или сторонним программным обеспечением, таким как AntiVirus, так как это может нарушить логику проверки сертификатов, которая встраивается в службу EM.

Если сетевой прокси-сервер развернут для исходящих подключений, администраторам необходимо настроить параметр *InternetWebProxy* на сервере Exchange Server, выполнив следующую команду:

Powershell

```
Set-ExchangeServer -Identity <ServerName> -InternetWebProxy
<http://proxy.contoso.com:port>
```

Необходимо также дополнительно настроить адрес прокси-сервера в параметрах прокси-сервера *WinHTTP* :

Powershell

```
netsh winhttp set proxy <proxy.contoso.com:port>
```

Помимо исходящего подключения к OCS, службе EM требуется исходящее подключение к различным конечным точкам списка отзыва сертификатов (CRL), упомянутым здесь.

Они необходимы для проверки подлинности сертификатов, используемых для подписи XML-файла устранения рисков.

Настоятельно рекомендуется разрешить Windows поддерживать список доверия сертификатов (CTL) на компьютере. В противном случае это необходимо регулярно поддерживать вручную. Чтобы разрешить Windows поддерживать CTL, следующий URL-адрес должен быть доступен с компьютера, на котором установлен Exchange Server.

Развернуть таблицу

Конечная точка	Адрес	Порт	Описание
Скачивание списка доверия сертификатов	`ctldl.windowsupdate.com/*`	80	Скачивание списка доверия сертификатов

Сценарий Test-MitigationServiceConnectivity

Можно убедиться, что сервер Exchange Server подключен к OCS, с помощью сценария **Test-MitigationServiceConnectivity.ps1** в папке `V15\Scripts` в каталоге сервера Exchange Server.

Если у сервера есть подключение, вывод будет следующим:

PowerShell

```
Result: Success.
Message: The Mitigation Service endpoint is accessible from this computer.
```

Если у сервера нет подключения, выходные данные будут такими:

Powershell

```
Result: Failed.
Message: Unable to connect to the Mitigation Service endpoint from this
computer. To learn about connectivity requirements, see
https://aka.ms/HelpConnectivityEEMS.
```

Отключение автоматического применения мер по устранению рисков через службу EM

Одна из функций службы EM — это загрузка мер по устранению рисков от OCS и их автоматическое применение к серверу Exchange Server. Если в организации есть другие способы устранения известных угроз, можно отключить автоматическое устранение рисков. Можно включить или отключить автоматическое устранение рисков на уровне организации или на уровне сервера Exchange Server.

Чтобы отключить автоматическое устранение рисков во всей организации, выполните следующую команду:

PowerShell

```
Set-OrganizationConfig -MitigationsEnabled $false
```

По умолчанию *для mitigationsEnabled задано* значение `$true`. Если задано значение `$false`, служба EM по-прежнему ежечасно проверяет устранение рисков, но не будет автоматически применять их к любому серверу Exchange в организации, независимо от значения параметра *MitigationsEnabled* на уровне сервера.

Чтобы отключить автоматическое устранение рисков на определенном сервере, замените <serverName> именем сервера, а затем выполните следующую команду:

Powershell

```
Set-ExchangeServer -Identity <ServerName> -MitigationsEnabled $false
```

По умолчанию *для mitigationsEnabled задано* значение `$true`. Если задано значение `$false`, служба EM проверяет на устранение рисков ежечасно, но не будет автоматически применять их к указанному серверу.

Сочетание параметров организации и параметров сервера определяет поведение службы EM на каждом сервере Exchange Server. Это поведение описано в следующей таблице:

Развернуть таблицу

Параметр организации	Параметр сервера	Result
Да	Да	Служба EM автоматически применяет меры по устранению рисков для сервера Exchange.
Верно.	Неверно.	Служба EM не будет автоматически применять меры по устранению рисков к определенному серверу Exchange.
Неверно.	Неверно.	Служба EM не будет автоматически применять меры по устранению рисков к любому серверу Exchange Server.

Примечание

Параметр *MitigationsEnabled* автоматически применяется ко всем серверам в организации. Для этого параметра устанавливается значение `$true` сразу же после обновления первого сервера Exchange Server в вашей организации до накопительного пакета обновления за сентябрь 2021 г. (или более поздней

версии). Такое поведение является особенностью данного продукта. Служба EM будет учитывать значение параметра *MitigationsEnabled* только после обновления остальных серверов Exchange Server до накопительного пакета обновления за сентябрь 2021 г. (или более поздней версии).

Просмотр примененных мер по устранению рисков

После применения мер по устранению рисков к серверу можно просмотреть примененные меры по устранению рисков, заменив <ServerName> именем сервера, а затем выполнив следующую команду:

PowerShell

```
Get-ExchangeServer -Identity <ServerName> | Format-List
Name,MitigationsApplied
```

Пример выходных данных:

Powershell

```
Name              :   Server1
MitigationsApplied  :   {M01.1, M01.2, M01.3}
```

Чтобы просмотреть список всех примененных мер по устранению рисков для всех серверов Exchange Server, выполните следующую команду:

PowerShell

```
Get-ExchangeServer | Format-List Name,MitigationsApplied
```

Пример выходных данных:

PowerShell

```
Name              :   Server1
MitigationsApplied  :   {M01.1, M01.2, M01.3}

Name              :   Server2
MitigationsApplied  :   {M01.1, M01.2, M01.3}
```

Повторное применение мер по устранению рисков

Если вы случайно отменили устранение рисков, служба EM повторно применяет его при почасовой проверке новых мер. Чтобы вручную повторно применить любую меру по устранению рисков, перезапустите службу EM на сервере Exchange Server, выполнив следующую команду:

PowerShell

```
Restart-Service MSExchangeMitigation
```

Через 10 минут после перезапуска служба EM запустит проверку и применит все возможные меры.

Блокировка или удаление мер по устранению рисков

Если устранение рисков критически влияет на функциональность сервера Exchange Server, вы можете заблокировать эту меру и вручную отменить ее.

Чтобы заблокировать любые меры по устранению рисков, добавьте идентификатор мер по устранению рисков в параметр *MitigationsBlocked*:

PowerShell

```
Set-ExchangeServer -Identity <ServerName> -MitigationsBlocked @("M1")
```

Предыдущая команда блокирует устранение рисков M1, что гарантирует, что служба EM не будет повторно применить эту меру в следующем ежечасном цикле.

Чтобы заблокировать несколько мер по устранению рисков, используйте следующий синтаксис:

PowerShell

```
Set-ExchangeServer -Identity <ServerName> -MitigationsBlocked @("M1","M2")
```

Блокировка устранения рисков не удаляет его автоматически, но после блокировки устранения рисков вы можете удалить его вручную. Способ устранения рисков зависит от типа устранения рисков. Например, чтобы удалить меру по устранению рисков правил перезаписи IIS, удалите правило в диспетчере IIS. Чтобы удалить

меры по устранению рисков пула служб или приложений, запустите пул службы или приложений вручную.

Также можно удалить одну или несколько мер по устранению рисков из списка заблокированных. Для этого удалите идентификатор меры по устранению рисков в параметре *MitigationsBlocked* в этой же команде.

Например.

PowerShell

```
Set-ExchangeServer -Identity <ServerName> -MitigationsBlocked @()
```

После удаления меры по устранению рисков из списка заблокированных мер по устранению рисков, они будут повторно применены службой EM при следующем запуске. Чтобы вручную повторно применить устранение рисков, остановите и перезапустите службу EM, выполнив следующую команду:

PowerShell

```
Restart-Service MSExchangeMitigation
```

Через 10 минут после перезапуска служба EM запустит проверку и применит все возможные меры.

> ⓘ **Важно!**
>
> Не изменяйте параметр *MitigationsApplied*, поскольку он используется службой EM для хранения и отслеживания состояния устранения рисков.

Просмотр примененных и заблокированных мер по устранению рисков

Вы можете просматривать как примененные, так и заблокированные меры по устранению рисков для всех серверов Exchange в организации с помощью командлета **Get-ExchangeServer**.

Чтобы просмотреть список всех примененных и заблокированных мер по устранению рисков для всех серверов Exchange Server, выполните следующую команду:

PowerShell

```
Get-ExchangeServer | Format-List Name,MitigationsApplied,MitigationsBlocked
```

Пример выходных данных:

PowerShell

```
Name              :   Server1
MitigationsApplied  :   {M01.1, M01.3}
MitigationsBlocked  :   {M01.2}

Name              :   Server2
MitigationsApplied  :   {M01.1, M01.2}
MitigationsBlocked  :   {M01.3}
```

Чтобы просмотреть список примененных и заблокированных мер для каждого сервера, замените <ServerName> именем сервера, а затем выполните следующую команду:

PowerShell

```
Get-ExchangeServer -Identity <ServerName> | fl name, *Mitigations*
```

Пример выходных данных:

PowerShell

```
Name              :   Server1
MitigationsEnabled  :   True
MitigationsApplied  :   {M01.1, M01.3}
MitigationsBlocked  :   {M01.2}
```

Сценарий Get-Mitigation

Вы можете использовать сценарий **Get-Mitigations.ps1** для анализа и отслеживания мер по устранению рисков, предоставляемых корпорацией Майкрософт. Этот сценарий находится в папке `V15\Scripts` в каталоге установки Exchange Server.

Сценарий отображает идентификатор, тип, описание и состояние каждой меры по устранению рисков. Список включает все примененные, заблокированные или неудачные меры по устранению рисков.

Чтобы просмотреть сведения о конкретном сервере, укажите имя сервера в параметре *Identity*. Например, `.\Get-Mitigations.ps1 -Identity <ServerName>`. Чтобы просмотреть состояние всех серверов в организации, опустите параметр *Identity* .

Пример: экспорт списка примененных мер по устранению рисков и их описаний в CSV-файл с помощью параметра ExportCSV:

```
PowerShell

.\Get-Mitigations.ps1 -Identity <ServerName> -ExportCSV
"C:\temp\CSVReport.csv"
```

> **ⓘ Важно!**
>
> Сценарию Get-Mitigations требуется PowerShell версии 4.0.

Удаление мер по устранению рисков после обновления SU или CU

После установки SU или CU администратор должен вручную удалить все меры по устранению рисков, которые больше не нужны. Например, если мера по устранению рисков **M1** больше не актуально после установки SU, служба EM перестанет его применять, и оно будет удалено из списка примененных мер по устранению рисков. В зависимости от типа устранения рисков, при необходимости его можно удалить с сервера.

> **ⓘ Примечание**
>
> Служба аварийного устранения рисков Exchange может добавлять методы устранения рисков для правил перезаписи URL-адресов IIS на уровне каждого сайта или каждого vDir (например, на `Default Web Site` уровне или только на `OWA` vDir в `Default Web Site`), а также на уровне сервера. Устранение рисков на уровне site/vDir добавляется в соответствующий `web.config` файл для site/vDir, тогда как средства устранения рисков на уровне сервера добавляются в `applicationHost.config` файл. Ожидается, что устранение рисков на уровне сайта будет удалено после установки накопительного пакета обновления. Однако средства устранения рисков на уровне сервера остаются на месте и должны быть удалены вручную, если они больше не нужны.

> Если мера защиты применима к только что установленному cu-пакету обновления, оно будет применено em-em.

Может возникнуть задержка между выпуском обновления безопасности Exchange Server (SU) или накопительного обновления (CU) и обновлением XML-файла устранения рисков, за исключением фиксированных номеров сборки безопасности из применяемых мер. Это ожидаемо и не должно вызывать никаких проблем. Если вы хотите удалить и заблокировать применяемый метод устранения рисков, можно выполнить действия, описанные в разделе Блокировка или удаление мер.

Мы обновим таблицу в разделе Список выпущенных мер по устранению рисков процедурой отката для конкретной защиты, как только она больше не будет применена к сборкам Exchange с исправлением безопасности.

Аудит и ведение журнала

Любые меры по устранению рисков, заблокированные администратором, будут регистрироваться в журнале событий приложения Windows. Помимо регистрации заблокированных мер по устранению рисков, служба EM также регистрирует сведения о запуске и завершении работы (как и все службы, работающие в Windows), а также сведения о своих действиях и любых ошибках, которые произошли в службе EM. Например, события 1005 и 1006 с источником "Служба устранения рисков MSExchange" будут регистрироваться для успешных действий, например при применении меры по устранению рисков. Событие 1008 с тем же источником будет регистрироваться для любых возникших ошибок, например, если служба EM не может связаться с OCS.

Вы можете использовать **Search-AdminAuditLog** для просмотра действий, предпринятых вами или другими администраторами, включая включение и отключение автоматических мер по устранению рисков.

Служба EM ведет отдельный файл журнала в папке `\V15\Logging\MitigationService` в каталоге установки Exchange Server. В этом журнале подробно описаны задачи, выполняемые службой EM, включая полученные, проанализированные и примененные меры по устранению рисков, а также сведения об информации, отправляемой в OCS (если отправка диагностических данных включена).

Диагностические данные

Когда доступ к данным включен, служба EM отправляет диагностические данные в OCS. Эти данные используются для выявления и устранения угроз. Дополнительные

сведения о том, какие данные собираются и как отключить совместное использование данных, см. в разделе Диагностические данные, собранные для Exchange Server.

Часто задаваемые вопросы об обновлении Exchange Server

Статья • 15.11.2023

Обзор

Очень важно продолжать обновлять локальные серверы Exchange Server до поддерживаемого состояния. Локальные среды *всегда* должны быть готовы к экстренному обновлению системы безопасности (это относится к Exchange, Windows и другим продуктам, которые вы используете в локальной среде). В условиях быстрого развития ландшафта угроз не следует недооценивать важность поддержания актуальности среды.

Обновляйте серверы Exchange Server. Мы хотим по-прежнему поддерживать безопасность вашей среды, и это означает, что серверы Exchange должны быть обновлены. Это *непрерывный процесс*.

Exchange Server типы обновлений и расписание выпуска

Существует три типа обновлений, которые корпорация Майкрософт может выпускать для Exchange Server:

Развернуть таблицу

Тип обновления	Частота выпуска	Требование к Обмену	Contains
Накопительный пакет обновления (CU)	Два раза в год (без конкретных дат).	Exchange должен находиться в основной поддержке.	Накопительное. Содержит исправления всех ранее выпущенных обновлений.
Обновление для системы безопасности (SU)	При необходимости. Обычно выпускается во вторник исправлений (Майкрософт) — второй вторник каждого месяца	Exchange должен иметь по крайней мере расширенную поддержку. Выпущено только для последнего накопительного пакета обновления (если	Накопительное. Содержит все обновления для системы безопасности с момента выпуска накопительного

Тип обновления	Частота выпуска	Требование к Обмену	Contains
	(если не экстренный выпуск).	Exchange находится в расширенной поддержке) или для последних двух единиц (если Exchange находится в основной поддержке).	пакета обновления, к которому она применяется.
Обновление исправлений (HU)	Выпускается только в том случае, если обновления компонентов требуются быстрее, чем выпуски CU.	Exchange должен находиться в основной поддержке.	Обновление компонентов применяется только к накопительным пакетам обновления, для которые оно выпущено.

Обновление рекомендаций

В этом процессе предполагается, что Exchange Server по-прежнему поддерживается:

- Установите последнюю версию cu. Используйте помощник по обновлению Exchange , чтобы выбрать текущий CU и целевой cu, чтобы получить конкретные маршруты. Дополнительные сведения см. в разделе Обновление Exchange до последнего накопительного обновления.
- Выполните инвентаризацию серверов Exchange Server, чтобы определить необходимые обновления с помощью скрипта проверки работоспособности Exchange Server. При выполнении этого скрипта вы узнаете, есть ли какие-либо серверы Exchange Server за обновлениями (CU, SU или вручную).
- Установите обновление для системы безопасности (SU) по мере их выпуска.
- Повторно запустите средство проверки работоспособности после установки su, чтобы узнать, требуются ли дальнейшие действия. Иногда требуются дополнительные действия.
- Если во время или после установки Exchange Server возникают ошибки, запустите скрипт SetupAssist. Если что-то не работает должным образом после обновлений, см. статью Восстановление неудачных установок накопительных пакетов и обновлений для системы безопасности Exchange.

Вопросы и ответы

Мы подготовили набор вопросов и ответов, которые охватывают то, что мы чаще всего слышим об обновлениях Exchange.

Мы обновили мои серверы Exchange Server несколько месяцев назад! Как же они "не поддерживаются" сегодня?

Для версий Exchange, которые находятся в основной поддержке (см. жизненный цикл продукта), корпорация Майкрософт поддерживает (выпускает соответствующие исправления безопасности для) два последних CU. Иногда последние два CU называются "N и N-1". В качестве текущего примера, если последний выпущенный CU — CU12 ("N"), а версия сервера — Exchange Server 2019, то корпорация Майкрософт в настоящее время поддерживает два Exchange Server 2019 Г., N и N-1 (CU12 и CU11). При выпуске CU13 "поддерживаемое окно cu" будет скользить к недавно выпущенному НАКОПИТЕЛЬному пакету обновления 13 (и то, что раньше было поддерживаемым накопительным пакетом обновления N-1, CU11, станет неподдерживаемой).

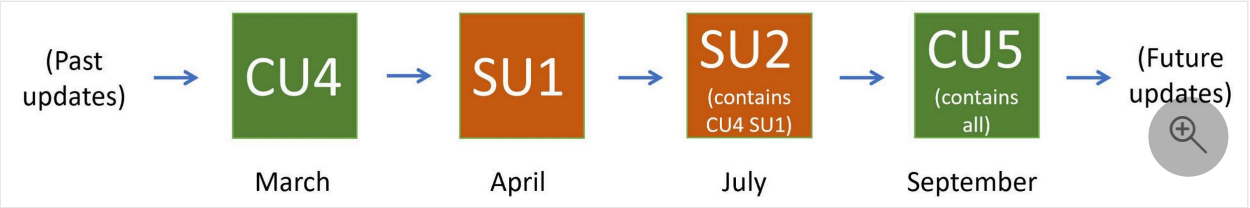
Почему корпорация Майкрософт так часто выпускает обновления?

Хорошо, что обновления выпускаются при обнаружении проблем. Корпорация Майкрософт (и другие издатели программного обеспечения) выпускает обновления только в том случае, если они необходимы. ЦС обычно содержат решения проблем с функциями, о которых нам сообщили наши клиенты (и могут содержать обновления для системы безопасности из предыдущих SU) и выпускаются два раза в год (в H1 и H2). Номера SU выпускаются только при обнаружении и исправлении фактических проблем с безопасностью, и обычно выпускаются в "вторник исправлений". Давайте рассмотрим, как будет выглядеть типичный поток выпуска для двух ЦУ и двух единиц SU, которые мы могли бы выпустить:

- В определенный месяц (скажем, в марте) мы можем выпустить накопительный пакет обновления 4; Накопительный пакет обновления 4 является накопительным и будет включать исправления и обновления, начиная с ранее.
- Месяц спустя мы выпустим CU4 SU1, обновление для системы безопасности для CU4.
- В июле мы выпустим накопительный пакет ОБНОВЛЕНИЯ 4 SU2, дополнительное обновление для системы безопасности для CU4. CU4 SU2

также включает обновления, выпущенные в CU4 SU1.

- В сентябре мы выпустим накопительный пакет обновления 5, который будет содержать все обновления, выпущенные до этого момента.



Наши серверы Exchange Работают должным образом, зачем их обновлять?

Поддержание актуальности Exchange Server позволяет гарантировать, что он будет работать без серьезных перебоев в работе, и поможет обеспечить безопасность данных вашей компании. Вложение времени в Exchange Server обслуживание (в соответствии с запланированным графиком) дает долгосрочное преимущество хорошо работающей системы с кодом, максимально защищенным от уязвимостей.

Как обновить Exchange Server, если (вставьте сюда имя стороннего приложения) не поддерживает последние поддерживаемые Exchange Server CU?

Обратитесь к стороннему поставщику, чтобы своевременно обеспечить актуальное программное обеспечение. Учитывайте, что среда Exchange содержит много ценных корпоративных каталогов и сведений о сообщениях. Приоритетом должно быть обеспечение максимальной безопасности среды.

Как мы можем оставаться в курсе, если мы бизнес 24x7 и не имеем времени, чтобы снять наши серверы для обслуживания?

Многим клиентам требуется Exchange Server для работы 24x7. На самом деле, наш процесс обновления предназначен для этих компаний с высоким спросом. Следует использовать группы доступности баз данных (DAG) и поместить обновляемые серверы в режим обслуживания, чтобы обеспечить корректное и не нарушающее работу процесса обновления для пользователей. Дополнительные сведения см. в разделе Выполнение обслуживания членов DAG .

Если мы находимся в гибридном режиме и не активно используем локальные Exchange Server, нам по-прежнему нужно оставаться в курсе?

Даже если для управления объектами, связанными с Exchange, вы используете только Exchange Server локальной среды, необходимо поддерживать актуальность сервера. `Hybrid Configuration Wizard (HCW)` Не нужно повторно запускать после установки обновлений.

Мы рассмотрели последние выпуски обновлений для системы безопасности, и уровень серьезности распространенных уязвимостей и уязвимостей (CVE) не был высоким; Зачем обновлять?

Корпорация Майкрософт рекомендует применить все доступные обновления для системы безопасности, так как может быть трудно понять, как даже уязвимости с более низкой степенью серьезности, обнаруженные за один месяц, могут взаимодействовать с уязвимостями, раскрытыми и исправленными через месяц. Атака может активировать только определенные функции с низким воздействием на удаленном целевом компьютере и ничего больше, что приводит к низкой оценке cve за один месяц. Например, в следующем месяце может быть обнаружена важная проблема с этой функцией, но она может быть активирована только локально и требовать значительного взаимодействия с пользователем. Это сам по себе также не может быть забито высоко. Но если ваше программное обеспечение отстает от обновлений, эти две проблемы могут объединиться в цепочку атак, что позволит получить оценку на критических уровнях.

Мы применили меры по устранению уязвимости системы безопасности. Зачем устанавливать (позже выпущенные) обновления для тех же уязвимостей?

Устранение рисков — это временная форма защиты, которую следует использовать до тех пор, пока не будет выпущено фактическое исправление кода. Так как меры по устранению рисков не устраняют фактическую уязвимость, которая присутствует в коде, они могут (а иногда и делать) злоумышленниками, атакующими системы, которые по-прежнему уязвимы. Корпорация Майкрософт рекомендует установить исправление кода для любой уязвимости, как только она будет доступна. Устранение рисков не следует рассматривать как долгосрочное решение для уязвимого кода.

Нам трудно обновить, так как расширения схемы Active Directory (AD) и установки Exchange требуют от разных команд действий.

В случаях, когда разным командам необходимо выполнить отдельные действия для подготовки к установке накопительных Обновления Exchange (так как для них может потребоваться расширение схемы AD), рекомендуется запросить изменения схемы при выпуске новых CU, для которых они требуются. Даже если вам не нужно обновлять до последней версии cu (так как последние два CU поддерживаются для версий Exchange, которые по-прежнему находятся в течение времени существования поддержки), тот факт, что схема Active Directory будет обновлена, означает, что если вы обнаружите, что вам нужно установить последнюю накопительную версию, схема AD уже будет обновлена. Мы выпускаем ЦП два раза в год, и не для всех из них требуются обновления схемы AD. Вы можете отслеживать это здесь для Exchange Server 2016 года и здесь для Exchange Server 2019 года.

Мы установили предыдущий CU на нашем сервере, а затем применили доступные номера SU. Мы обновили наш сервер до последней доступной версии cu. Нужно ли применять уже выпущенный su для последней версии CU?

После установки на сервере нового cuu всегда необходимо установить последние номера SU, доступные для этого накопительного пакета обновления. Давайте рассмотрим гипотетический сценарий Exchange Server 2019 года:

- В мае вы установили CU9 (последний доступный cu на тот момент) и все доступные SU для CU9
- В июне мы выпустили CU10 для Exchange Server 2019
- В июле мы выпустили номера SU, которые применяются как к CU9, так и к CU10.
- В июле вы установили июльского su на сервере Exchange 2019 с накопительным пакетом обновления 9 (CU9)
- В августе вы установили накопительный пакет обновления 10 (последний доступный накопительный пакет обновления в июле)
- Теперь необходимо применить последнюю версию su, доступную для Exchange Server 2019 CU10.

В прошлом месяце мы установили su для текущего CU. В этом месяце для того же cu доступен новый SU. Нужно ли удалять su за прошлый месяц перед установкой более новой для того же CU?

Нет, удаление su за прошлый месяц не требуется. Установите su этого месяца по мере его доступности. Более новая версия SU также содержит исправления безопасности единиц безопасности за прошлый месяц.

Номера SU всегда зависят от CU. Иными словами, для установки более поздней версии CU необходимо также установить любой su, доступный для этого накопительного пакета обновления, независимо от того, были ли выпущены в тот же день su для последнего и предыдущего CU. Если для накопительного пакета обновления на сервере есть номера SU, их следует установить. Как правило, при следующем последующем выпуске CU номера единиц будут "сворачены в CU".

Мы пропустили несколько единиц и хотим полностью обновлять Exchange до последней версии SU. Нужно ли установить все номера SU, чтобы получить доступ к последней версии?

Так как номера SU являются накопительными, так как они применимы к накопительным пакетам обновления, необходимо установить только последнюю версию su. Это позволяет получить все исправления безопасности, выпущенные с момента выпуска накопительного пакета обновления.

Изменилась ли корпорация Майкрософт, как часто выпускаются серверы Exchange?

Да, начиная с накопительного Обновления H1 за 2022 г. мы перешли на период выпуска в два CU в год, выпуская в H1 и H2 каждого календарного года, с общими целевыми датами выпуска в марте и сентябре. Но даты выпуска зависят от качества, поэтому мы можем выпустить обновления в апреле, октябре или другом месяце в зависимости от того, что мы поставляем. При таких изменениях модели службы текущее состояние по-прежнему означает запуск последнего cu или непосредственно предшествующего ему (N или N-1), но "валютное окно" теперь продлевается с 6 месяцев до 1 года.

Нужно ли устанавливать SU на всех серверах Exchange в нашей организации? Как насчет компьютеров с параметром "Только средства управления"?

Мы рекомендуем установить Обновления безопасности на всех серверах Exchange Server и серверах или рабочих станциях, на которых работают только средства управления Exchange, что обеспечит отсутствие несовместимости между клиентами и серверами средств управления. Если вы пытаетесь обновить средства управления Exchange в среде без работающих серверов Exchange, см. эту статью.

Мы установили текущие выпуски CU и SU и полностью обновлены. Есть ли еще что-нибудь, что мы должны сделать?

В зависимости от конкретной среды для устранения определенных уязвимостей может потребоваться выполнение дополнительных действий администратором Exchange. Чтобы убедиться, что вы выполнили все необходимые действия после установки соответствующих Обновления безопасности, запустите скрипт проверки работоспособности Exchange Server. Обязательно обновите операционную систему Windows, в котором работает Exchange Server, так как уязвимости в ОС также можно использовать в цепочке атак.

рекомендации по настройке TLS Exchange Server

Статья • 06.11.2024

В этой документации описаны необходимые действия для правильной настройки определенных версий TLS на Microsoft Exchange Server. В нем также описано, как оптимизировать наборы шифров и алгоритмы хэширования, используемые TLS. Неправильная конфигурация TLS может привести к различным проблемам при взаимодействии с Microsoft 365 или другими системами, для которых требуется определенный минимальный стандарт TLS.

Дополнительные сведения о протоколах TLS см. в документации по протоколу безопасности транспортного уровня .

> **Совет**
>
> Скрипт Exchange HealthChecker можно использовать для проверка текущей конфигурации TLS сервера Exchange.

Читайте внимательно, так как некоторые действия можно выполнить только в определенных операционных системах или Exchange Server версиях. Каждый раздел начинается с матрицы, показывающей, поддерживается ли параметр и был ли он предварительно настроен в определенной Exchange Server версии, после чего следуют шаги по включению или отключению определенного протокола ИЛИ функции TLS.

Что следует учитывать перед отключением версии TLS

Убедитесь, что каждое приложение поддерживает версии TLS, которые остаются включенными. Рекомендации, такие как (но не только):

- Поддерживают ли ваши контроллеры домена и серверы глобального каталога, например конфигурацию только TLS 1.2 или TLS 1.3?
- Поддерживают ли партнерские приложения, например конфигурацию только TLS 1.2 или TLS 1.3?
- Поддерживает ли операционная система последнюю версию протокола TLS 1.2 через WinHTTP ?

- Поддерживают ли ваши подсистемы балансировки нагрузки использование TLS 1.2 или TLS 1.3?
- Поддерживают ли классические, мобильные и браузерные приложения TLS 1.2 или TLS 1.3?
- Поддерживают ли устройства, например многофункциональные принтеры, TLS 1.2 или TLS 1.3?
- Поддерживают ли сторонние или пользовательские собственные приложения, которые интегрируются с Exchange Server или Microsoft 356, надежную реализацию TLS?

Поэтому мы настоятельно рекомендуем выполнить все действия, которые вы предпринимаете для перехода на TLS 1.2 или TLS 1.3 и от старых протоколов безопасности, сначала выполнять в лабораториях, которые имитируют рабочие среды, прежде чем вы начнете медленно развертывать их в рабочей среде.

Действия, используемые для отключения определенной версии TLS, как описано ниже, применяются к следующим функциям Exchange Server:

- Протокол SMTP
- Подключение клиента Outlook (Любой Outlook/ MAPI/HTTP)
- Exchange Active Sync (EAS)
- Outlook в Интернете (OWA)
- Центр Администратор Exchange (EAC) и Exchange панель управления (ECP)
- Автообнаружения
- Веб-службы Exchange (EWS)
- REST (Exchange Server 2016/2019)
- Использование PowerShell в Exchange по протоколу HTTPS
- POP и IMAP

Предварительные условия

Поддержка TLS 1.3 появилась с накопительным пакетом обновления 15 Exchange Server 2019 Windows Server 2022 и Windows Server 2025 г., за исключением протокола SMTP. Поддержка этого протокола будет добавлена с последующим обновлением. Поддержка TLS 1.2 появилась в Exchange Server 2013 CU19 и Exchange Server 2016 CU8. Exchange Server 2019 по умолчанию поддерживает TLS 1.2.

Exchange Server не может работать без Windows Server, поэтому важно установить последние обновления операционной системы для запуска стабильной и безопасной реализации TLS.

Кроме того, требуется наличие последней версии платформа .NET Framework и связанных исправлений, поддерживаемых накопительным пакетом обновления.

В зависимости от операционной системы убедитесь, что также установлены следующие обновления (они должны быть установлены, если сервер является текущим в Windows Обновления):

Если ваша операционная система Windows Server 2012 или Windows Server 2012 R2, перед включением TLS 1.2 необходимо установить KB3161949 и KB2973337.

> ⚠ **Предупреждение**
>
> расширенная поддержка Windows Server 2012 и Windows Server 2012 R2 прекращена 10 октября 2023 г. Эти серверы больше не получают Безопасность Windows Обновления без ESU. Мы настоятельно рекомендуем выполнить миграцию на поддерживаемую версию как можно скорее!

Обязательно перезагрузите Exchange Server после применения конфигурации TLS. Он становится активным после перезапуска сервера.

Подготовка платформа .NET Framework к наследованию значений по умолчанию от Schannel

В следующей таблице показаны сочетания Exchange Server/Windows Server с конфигурацией наследования Schannel по умолчанию платформа .NET Framework:

Развернуть таблицу

Exchange Server	Windows Server	Поддерживается	Настроено по умолчанию
Exchange Server 2019 CU14 или более поздней версии	Любой	Да	Да (только для новых установок)
Exchange Server 2019 CU13 или более поздней версии	Любой	Да	Частично (`SchUseStrongCrypto` необходимо настроить вручную)
Exchange Server 2016	Любой	Да	Нет (используются значения по умолчанию для ОС)
Exchange Server 2013	Любой	Да	Нет (используются значения по умолчанию для ОС)

Значение `SystemDefaultTlsVersions` реестра определяет, какие версии протокола безопасности по умолчанию используются платформа .NET Framework 4.x. Если для параметра задано значение `1`, то платформа .NET Framework 4.x наследует значения по умолчанию от значений реестра Windows Secure Channel (Schannel). `DisabledByDefault` Если значение не определено, оно ведет себя так, как если бы для него задано значение `0`.

Надежное шифрование (настроенное по значению `SchUseStrongCrypto` реестра) использует более безопасные сетевые протоколы (TLS 1.3, TLS 1.2 и TLS 1.1) и блокирует небезопасные протоколы. `SchUseStrongCrypto` влияет только на клиентские (исходящие) подключения в приложении. Настроив платформа .NET Framework 4.x для наследования значений от Schannel, мы получаем возможность использовать последние версии TLS, поддерживаемые ОС, включая TLS 1.2 и TLS 1.3.

Включение наследования Schannel платформа .NET Framework 4.x

Выполните следующие команды в окне PowerShell с повышенными привилегиями, чтобы настроить наследование Schannel платформа .NET Framework 4.x:

PowerShell

```
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319" -
Name "SystemDefaultTlsVersions" -Value 1 -Type DWord
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319" -
Name "SchUseStrongCrypto" -Value 1 -Type DWord
Set-ItemProperty -Path
"HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319" -Name
"SystemDefaultTlsVersions" -Value 1 -Type DWord
Set-ItemProperty -Path
"HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319" -Name
"SchUseStrongCrypto" -Value 1 -Type DWord
```

Включение наследования Schannel платформа .NET Framework 3.5

Exchange Server 2013 и более поздних версиях этот параметр не требуется. Однако мы рекомендуем настроить его идентично параметрам .NET 4.x, чтобы обеспечить согласованную конфигурацию.

Выполните следующие команды в окне PowerShell с повышенными привилегиями, чтобы настроить наследование Schannel платформа .NET Framework 3.5:

PowerShell

```
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\.NETFramework\v2.0.50727" -
Name "SystemDefaultTlsVersions" -Value 1 -Type DWord
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\.NETFramework\v2.0.50727" -
Name "SchUseStrongCrypto" -Value 1 -Type DWord
Set-ItemProperty -Path
"HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727" -Name
"SystemDefaultTlsVersions" -Value 1 -Type DWord
Set-ItemProperty -Path
"HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727" -Name
"SchUseStrongCrypto" -Value 1 -Type DWord
```

Действия по настройке TLS 1.3

В следующей таблице показаны сочетания Exchange Server и Windows Server, в которых поддерживается ПРОТОКОЛ TLS 1.3. В таблице также показана конфигурация по умолчанию:

Развернуть таблицу

Exchange Server	Windows Server	Поддерживается	Настроено по умолчанию
Exchange Server 2019 CU15	Windows Server 2022/2025	Да	Да (`enabled`)
Exchange Server 2019 CU15	в Windows Server 2019;	Нет	Н/Д
Exchange Server 2019 CU14 или более поздней версии	Любой	Нет	Н/Д
Exchange Server 2016	Любой	Нет	Н/Д
Exchange Server 2013	Любой	Нет	Н/Д

Включение TLS 1.3

Выполните следующую команду в окне PowerShell с повышенными привилегиями, чтобы включить TLS 1.3 для клиентских и серверных подключений:

PowerShell

```
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
" -Name "TLS 1.3" -ErrorAction SilentlyContinue
New-Item -Path
```

```
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.3" -Name "Client" -ErrorAction SilentlyContinue
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.3" -Name "Server" -ErrorAction SilentlyContinue
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.3\Client" -Name "DisabledByDefault" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.3\Client" -Name "Enabled" -Value 1 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.3\Server" -Name "DisabledByDefault" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.3\Server" -Name "Enabled" -Value 1 -Type DWord
```

Согласно стандарту RFC 8446 TLS 1.3 использует то же пространство набора шифров, что и в предыдущих версиях TLS. Однако наборы шифров TLS 1.3 определяются по-разному, указывая только симметричные шифры, и не могут использоваться для TLS 1.2. Аналогичным образом наборы шифров для TLS 1.2 и более ранних версий не могут использоваться с TLS 1.3.

Выполните следующую команду в окне PowerShell с повышенными привилегиями, чтобы настроить наборы шифров TLS 1.3:

PowerShell

```
Enable-TlsCipherSuite -Name TLS_AES_256_GCM_SHA384 -Position 0
Enable-TlsCipherSuite -Name TLS_AES_128_GCM_SHA256 -Position 1
```

Отключение TLS 1.3

Выполните следующую команду в окне PowerShell с повышенными привилегиями, чтобы явно отключить TLS 1.3 для клиентских и серверных подключений:

PowerShell

```
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
" -Name "TLS 1.3" -ErrorAction SilentlyContinue
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.3" -Name "Client" -ErrorAction SilentlyContinue
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.3" -Name "Server" -ErrorAction SilentlyContinue
```

```
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.3\Client" -Name "DisabledByDefault" -Value 1 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.3\Client" -Name "Enabled" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.3\Server" -Name "DisabledByDefault" -Value 1 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.3\Server" -Name "Enabled" -Value 0 -Type DWord
```

Выполните следующую команду в окне PowerShell с повышенными привилегиями, чтобы удалить наборы шифров TLS 1.3:

PowerShell

```
Remove-TlsCipherSuite -Name TLS_AES_256_GCM_SHA384 -ErrorAction
SilentlyContinue
Remove-TlsCipherSuite -Name TLS_AES_128_GCM_SHA256 -ErrorAction
SilentlyContinue
```

Действия по настройке TLS 1.2

В следующей таблице показаны сочетания Exchange Server и Windows Server, в которых поддерживается ПРОТОКОЛ TLS 1.2. В таблице также показана конфигурация по умолчанию:

Развернуть таблицу

Exchange Server	Windows Server	Поддерживается	Настроено по умолчанию
Exchange Server 2019	Любой	Да	Да (`enabled`)
Exchange Server 2016	Любой	Да	Нет
Exchange Server 2013	Любой	Да	Нет

Включить протокол TLS 1.2

Выполните следующую команду в окне PowerShell с повышенными привилегиями, чтобы включить TLS 1.2 для клиентских и серверных подключений:

PowerShell

```
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
" -Name "TLS 1.2" -ErrorAction SilentlyContinue
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.2" -Name "Client" -ErrorAction SilentlyContinue
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.2" -Name "Server" -ErrorAction SilentlyContinue
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.2\Client" -Name "DisabledByDefault" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.2\Client" -Name "Enabled" -Value 1 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.2\Server" -Name "DisabledByDefault" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.2\Server" -Name "Enabled" -Value 1 -Type DWord
```

Отключение TLS 1.2

Выполните следующую команду в окне PowerShell с повышенными привилегиями, чтобы явно отключить TLS 1.2 для клиентских и серверных подключений:

PowerShell

```
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
" -Name "TLS 1.2" -ErrorAction SilentlyContinue
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.2" -Name "Client" -ErrorAction SilentlyContinue
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.2" -Name "Server" -ErrorAction SilentlyContinue
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.2\Client" -Name "DisabledByDefault" -Value 1 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.2\Client" -Name "Enabled" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.2\Server" -Name "DisabledByDefault" -Value 1 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.2\Server" -Name "Enabled" -Value 0 -Type DWord
```

Действия по настройке TLS 1.1

В следующей таблице показаны сочетания Exchange Server и Windows Server, в которых поддерживается ПРОТОКОЛ TLS 1.1. В таблице также показана конфигурация по умолчанию:

Развернуть таблицу

Exchange Server	Windows Server	Поддерживается	Настроено по умолчанию
Exchange Server 2019	Любой	Да	Да (`disabled`)
Exchange Server 2016	Любой	Да	Нет
Exchange Server 2013	Любой	Да	Нет

Включение TLS 1.1

> **Примечание**
>
> Реализация Microsoft TLS 1.1 не имеет известных уязвимостей системы безопасности. Но из-за возможности будущих атак с понижением уровня протокола и других уязвимостей TLS рекомендуется тщательно спланировать и отключить TLS 1.1. При тщательном планировании клиенты могут потерять подключение.

Выполните следующую команду в окне PowerShell с повышенными привилегиями, чтобы включить TLS 1.1 для клиентских и серверных подключений:

PowerShell

```
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
" -Name "TLS 1.1" -ErrorAction SilentlyContinue
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.1" -Name "Client" -ErrorAction SilentlyContinue
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.1" -Name "Server" -ErrorAction SilentlyContinue
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.1\Client" -Name "DisabledByDefault" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.1\Client" -Name "Enabled" -Value 1 -Type DWord
```

```
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.1\Server" -Name "DisabledByDefault" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.1\Server" -Name "Enabled" -Value 1 -Type DWord
```

Отключение TLS 1.1

Выполните следующую команду в окне PowerShell с повышенными привилегиями, чтобы явно отключить TLS 1.1 для клиентских и серверных подключений:

PowerShell

```
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
" -Name "TLS 1.1" -ErrorAction SilentlyContinue
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.1" -Name "Client" -ErrorAction SilentlyContinue
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.1" -Name "Server" -ErrorAction SilentlyContinue
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.1\Client" -Name "DisabledByDefault" -Value 1 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.1\Client" -Name "Enabled" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.1\Server" -Name "DisabledByDefault" -Value 1 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.1\Server" -Name "Enabled" -Value 0 -Type DWord
```

Действия по настройке TLS 1.0

В следующей таблице показаны сочетания Exchange Server и Windows Server, в которых поддерживается ПРОТОКОЛ TLS 1.0. В таблице также показана конфигурация по умолчанию:

Развернуть таблицу

Exchange Server	Windows Server	Поддерживается	Настроено по умолчанию
Exchange Server 2019	Любой	Да	Да (`disabled`)

Exchange Server	Windows Server	Поддерживается	Настроено по умолчанию
Exchange Server 2016	Любой	Да	Нет
Exchange Server 2013	Любой	Да	Нет

Включение TLS 1.0

> ⓘ **Примечание**
>
> Внедрение Microsoft TLS 1.0 не имеет известных уязвимостей безопасности. Но из-за возможности будущих атак с понижением уровня протокола и других уязвимостей TLS рекомендуется тщательно спланировать и отключить TLS 1.0. При тщательном планировании клиенты могут потерять подключение.

Выполните следующую команду в окне PowerShell с повышенными привилегиями, чтобы включить TLS 1.0 для клиентских и серверных подключений:

PowerShell

```
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
" -Name "TLS 1.0" -ErrorAction SilentlyContinue
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.0" -Name "Client" -ErrorAction SilentlyContinue
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.0" -Name "Server" -ErrorAction SilentlyContinue
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.0\Client" -Name "DisabledByDefault" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.0\Client" -Name "Enabled" -Value 1 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.0\Server" -Name "DisabledByDefault" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.0\Server" -Name "Enabled" -Value 1 -Type DWord
```

Отключение TLS 1.0

Выполните следующую команду в окне PowerShell с повышенными привилегиями, чтобы явно отключить TLS 1.0 для клиентских и серверных подключений:

PowerShell

```
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
" -Name "TLS 1.0" -ErrorAction SilentlyContinue
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.0" -Name "Client" -ErrorAction SilentlyContinue
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.0" -Name "Server" -ErrorAction SilentlyContinue
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.0\Client" -Name "DisabledByDefault" -Value 1 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.0\Client" -Name "Enabled" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.0\Server" -Name "DisabledByDefault" -Value 1 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
\TLS 1.0\Server" -Name "Enabled" -Value 0 -Type DWord
```

Действия по настройке строгого режима повторного согласования TLS

Строгий режим TLS — это функция безопасности, которая гарантирует, что только клиенты с необходимыми обновлениями безопасности могут устанавливать и пересматривать сеансы TLS с сервером.

В следующей таблице показаны сочетания Exchange Server/Windows Server с конфигурацией строгого режима перезаключения TLS по умолчанию.

Развернуть таблицу

Exchange Server	Windows Server	Поддерживается	Настроено по умолчанию
Exchange Server 2019	Любой	Да	Да (`enabled`)
Exchange Server 2016	Любой	Да	Нет
Exchange Server 2013	Любой	Нет	Н/Д

Включение строгого режима повторного согласования TLS

Выполните следующую команду в окне PowerShell с повышенными привилегиями, чтобы включить строгий режим повторного переговоров:

```
PowerShell

Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL" -Name
"AllowInsecureRenegoClients" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL" -Name
"AllowInsecureRenegoServers" -Value 0 -Type DWord
```

Отключение строгого режима повторного согласования TLS

Выполните следующую команду в окне PowerShell с повышенными привилегиями, чтобы явно отключить строгий режим повторного переговоров:

```
PowerShell

Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL" -Name
"AllowInsecureRenegoClients" -Value 1 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL" -Name
"AllowInsecureRenegoServers" -Value 1 -Type DWord
```

Проверка использования TLS 1.2 или TLS 1.3

После включения TLS 1.2 или TLS 1.3 может быть полезно убедиться, что работа выполнена успешно и система сможет согласовать tls 1.2 или TLS 1.3 для входящих (серверных) и исходящих (клиентских) подключений. Существует несколько методов проверки использования TLS, некоторые из которых рассматриваются в следующих разделах.

Многие протоколы, используемые в Exchange Server, основаны на HTTP и, следовательно, проходят процессы IIS на сервере Exchange Server. MAPI/HTTP, Outlook Anywhere, Веб-службы Exchange, Exchange ActiveSync, REST, OWA & EAC, загрузка автономной адресной книги и автообнаружение — это примеры протоколов на основе HTTP, используемых Exchange Server.

Ведение журнала IIS

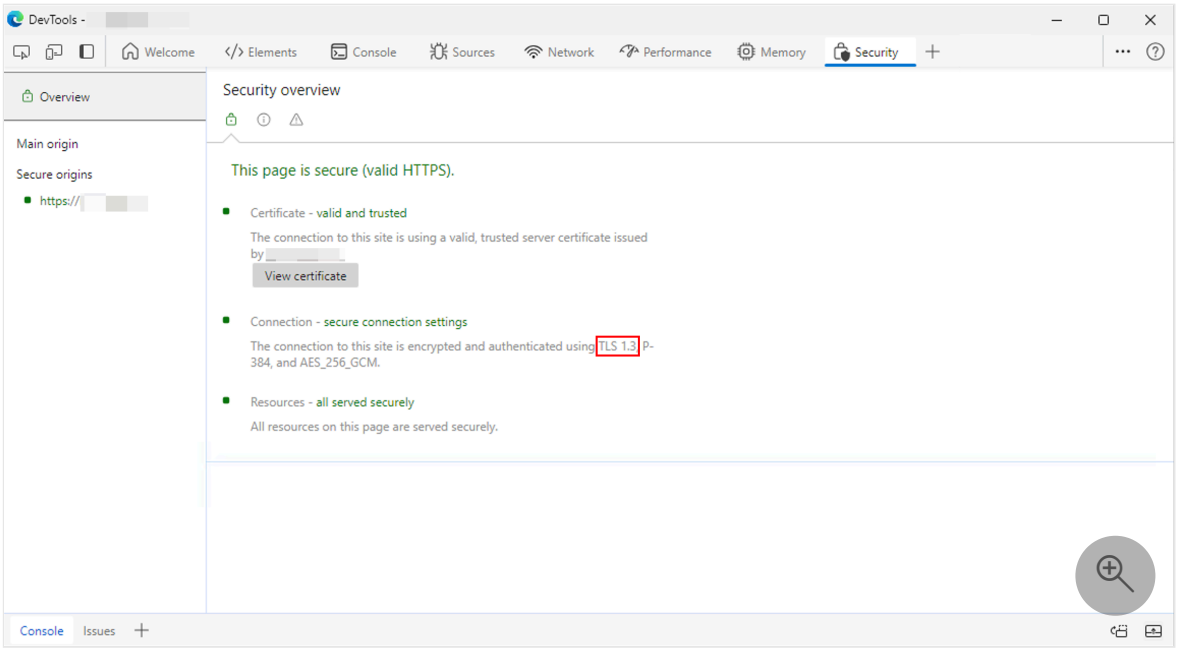
Команда служб IIS добавила возможности для Windows Server 2012 R2 или более поздней версии для регистрации настраиваемых полей, связанных с версиями протокола шифрования и шифрами. Мы рекомендуем просмотреть в блоге документацию о том, как включить эти настраиваемые поля и начать анализ журналов для получения сведений о входящих подключениях в вашей среде, связанных с протоколами на основе HTTP.

Эти настраиваемые поля IIS не существуют для Windows Server версии, предшествующей Windows Server 2012 R2. Эти сведения могут предоставляться в журналах подсистемы балансировки нагрузки или брандмауэра. Запросите рекомендации у поставщиков, чтобы определить, могут ли их журналы предоставлять эту информацию.

Средства разработчика Microsoft Edge

Вы можете использовать `Developer Tools`, доступные в Microsoft Edge, чтобы проверка версию TLS, которая использовалась для установки безопасного подключения, при подключении к Outlook в Интернете (OWA) или Exchange Администратор Center (ECP). Для этого выполните следующие действия:

1. Откройте браузер Microsoft Edge и установите HTTPS-подключение к OWA или ECP.
2. Нажмите , `CTRL + SHIFT + I` чтобы открыть `Developer Tools`.
3. Щелкните символ в `+` правом верхнем углу.
4. `Security` Щелкните в раскрывающемся меню.
5. Проверьте версию TLS в `Connection - secure connection settings` разделе .



Заголовки сообщений

Данные заголовков сообщений в Exchange Server 2016 или более поздней версии предоставляют протокол, согласованный и используемый, когда отправляющий и получающий узел обменивается фрагментом почты. Вы можете использовать анализатор заголовков сообщений , чтобы получить четкий обзор каждого прыжка.

Существует известное исключение из примера заголовков сообщений. Когда клиент отправляет сообщение путем подключения к серверу с использованием протокола SMTP с проверкой подлинности (также известного как протокол отправки клиента SMTP), версия TLS в заголовках сообщений не отображает правильную версию TLS, используемую клиентом. Корпорация Майкрософт изучает возможность добавления этой информации в будущем обновлении.

Ведение журнала SMTP

Журналы SMTP в Exchange Server содержат протокол шифрования и другую информацию, связанную с шифрованием, которая используется при обмене электронной почтой между двумя системами.

Если сервером является `SMTP receiving system`, найдите в журнале `Server value` в зависимости от используемой версии TLS. Если сервером является `SMTP sending system`, найдите в журнале `Client value` в зависимости от используемой версии TLS.

Развернуть таблицу

Версия TLS	Значение сервера	Значение клиента
TLS 1.0	SP_PROT_TLS1_0_SERVER	SP_PROT TLS1_0_CLIENT
TLS 1.1	SP_PROT_TLS1_1_SERVER	SP_PROT-TLS1_1_CLIENT
TLS 1.2	SP_PROT_TLS1_2_SERVER	SP_PROT TLS1_2_CLIENT

> ⓘ **Примечание**
>
> Поддержка ПРОТОКОЛА SMTP TLS 1.3 будет включена в предстоящее обновление Exchange 2019 CU15.

В следующем примере выполняется поиск подключений, выполненных по протоколу TLS 1.0, в файлах журнала на сервере Exchange Server, на котором выполняется роль почтового ящика.

PowerShell

```
Select-String -Path (((Get-TransportService -Identity
$env:COMPUTERNAME).ReceiveProtocolLogPath).PathName.Replace("Hub","FrontEnd"
)+"\*.log") "SP_PROT_TLS1_0"
```

Пример поиска файлов журнала на сервере Exchange Server, на котором выполняется роль пограничного транспорта, для подключений, выполненных по протоколу TLS 1.1:

PowerShell

```
Select-String -Path (((Get-TransportService -Identity
$env:COMPUTERNAME).ReceiveProtocolLogPath).PathName+"\*.log")
"SP_PROT_TLS1_1"
```

POP и IMAP

Не существует ведения журнала, предоставляющего версию протокола шифрования, используемую для клиентов POP и IMAP. Чтобы захватить эти сведения, может потребоваться записать трассировку Netmon с сервера или проверить трафик по мере его прохождения через подсистему балансировки нагрузки или брандмауэр, где выполняется мостовая передача HTTPS.

Рекомендации по алгоритмам шифрования и хэширования

Действия, описанные в этом разделе, можно использовать для настройки Exchange Server 2016 с тем же набором алгоритмов шифра и хэширования, что и Exchange Server 2019. Эти действия не являются обязательными для Exchange Server 2019 г., так как он уже поставляется с предварительно настроенным шифром и хэш-алгоритмом.

В качестве необходимого условия сначала необходимо настроить TLS 1.2, а затем отключить TLS 1.0 и TLS 1.1. Рассмотрите возможность применения следующих параметров отдельно от отключения TLS 1.0 и TLS 1.1 для изоляции проблемных клиентов с конфигурацией.

Включение рекомендуемых наборов шифров

Windows Server 2012 и Windows Server 2012 R2.

Выполните следующие команды в окне PowerShell с повышенными привилегиями, чтобы настроить рекомендуемые наборы шифров:

PowerShell

```
New-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL
\00010002" -Name "Functions" -PropertyType MultiString -Value
"TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384,TLS_ECDHE_RSA_WITH_AES_256_CBC_S
HA384_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,TLS_ECDHE_RSA_WITH_AES
_128_CBC_SHA256_P256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384,TLS_ECDHE_
ECDSA_WITH_AES_256_GCM_SHA384_P256,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P
384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256,TLS_ECDHE_ECDSA_WITH_AES_25
6_CBC_SHA384_P384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P256,TLS_ECDHE_ECD
SA_WITH_AES_128_CBC_SHA256_P384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256
,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_
P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_RSA_WITH_AES_128_CBC_
SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDHE_ECDSA_WITH_AES_
256_CBC_SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_ECDSA_W
ITH_AES_128_CBC_SHA_P256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_12
8_GCM_SHA256" -Force
```

Windows Server 2016

Выполните следующие команды в окне PowerShell с повышенными привилегиями, чтобы настроить рекомендуемые наборы шифров.

> ⓘ **Примечание**
>
> Наборы шифров можно настроить, используя объект групповая политика (GPO). Вы не можете настроить их вручную с помощью командлетов Enable-TlsCipherSuite или Disable-TLSCipherSuite, если они уже настроены с помощью объекта групповой политики или если `Functions` запись реестра уже существует в `HKLM:\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002` пути.

Сначала отключите все наборы шифров:

PowerShell

```
foreach ($suite in (Get-TLSCipherSuite).Name) {
    if (-not([string]::IsNullOrWhiteSpace($suite))) {
        Disable-TlsCipherSuite -Name $suite -ErrorAction SilentlyContinue
    }
}
```

Затем повторно включите только рекомендуемые наборы шифров TLS 1.2:

PowerShell

```
$cipherSuites = @('TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384',
                  'TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256',
                  'TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384',
                  'TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256',
                  'TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384',
                  'TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256',
                  'TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384',
                  'TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256')

$suiteCount = 0
foreach ($suite in $cipherSuites) {
    Enable-TlsCipherSuite -Name $suite -Position $suiteCount
    $suiteCount++
}
```

Отключение устаревших шифров и хэшей

Выполните следующую команду в окне PowerShell с повышенными привилегиями, чтобы явно отключить устаревшие шифры и хэши:

PowerShell

```
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL" -Name
"Hashes" -ErrorAction SilentlyContinue
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL" -Name
"Ciphers" -ErrorAction SilentlyContinue
(Get-Item
HKLM:).OpenSubKey("SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANN
EL\Ciphers", $true).CreateSubKey("DES 56/56")
(Get-Item
HKLM:).OpenSubKey("SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANN
EL\Ciphers", $true).CreateSubKey("NULL")
(Get-Item
HKLM:).OpenSubKey("SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANN
EL\Ciphers", $true).CreateSubKey("RC2 40/128")
(Get-Item
HKLM:).OpenSubKey("SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANN
EL\Ciphers", $true).CreateSubKey("RC2 56/128")
(Get-Item
HKLM:).OpenSubKey("SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANN
EL\Ciphers", $true).CreateSubKey("RC2 56/56")
(Get-Item
HKLM:).OpenSubKey("SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANN
EL\Ciphers", $true).CreateSubKey("RC4 40/128")
(Get-Item
HKLM:).OpenSubKey("SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANN
EL\Ciphers", $true).CreateSubKey("RC4 56/128")
(Get-Item
HKLM:).OpenSubKey("SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANN
EL\Ciphers", $true).CreateSubKey("RC4 64/128")
(Get-Item
HKLM:).OpenSubKey("SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANN
EL\Ciphers", $true).CreateSubKey("RC4 128/128")
(Get-Item
HKLM:).OpenSubKey("SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANN
EL\Ciphers", $true).CreateSubKey("Triple DES 168")
New-Item -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes" -
Name "MD5" -ErrorAction SilentlyContinue
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\D
ES 56/56" -Name "Enabled" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\N
ULL" -Name "Enabled" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\R
C2 40/128" -Name "Enabled" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\R
C2 56/128" -Name "Enabled" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\R
C2 56/56" -Name "Enabled" -Value 0 -Type DWord
```

```
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\R
C4 40/128" -Name "Enabled" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\R
C4 56/128" -Name "Enabled" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\R
C4 64/128" -Name "Enabled" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\R
C4 128/128" -Name "Enabled" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\T
riple DES 168" -Name "Enabled" -Value 0 -Type DWord
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\MD
5" -Name "Enabled" -Value 0 -Type DWord
```

Настройка предпочтения эллиптических кривых

Рекомендуется отключить `curve25519` эллиптическую кривую, так как она недоступна в режиме FIPS. Дополнительные сведения см. в документации по эллиптическим кривым TLS Windows 10 версии 1607 и более поздних версий.

Выполните следующую команду в окне PowerShell с повышенными привилегиями, чтобы настроить параметр эллиптической кривой:

PowerShell

```
Disable-TlsEccCurve -Name "curve25519"
Enable-TlsEccCurve -Name "NistP384" -Position 0
Enable-TlsEccCurve -Name "NistP256" -Position 1
```

Справочник по развертыванию сервера изменений

Статья • 04.04.2023

Exchange Server проверки готовности

выпуски и версии Exchange Server

поддержка языка Exchange Server

параметры конфигурации хранилища Exchange Server

Сетевые порты для клиентов и потока обработки почты в Exchange

Общие сведения о службах Exchange на серверах Exchange

Предпочтительная архитектура Exchange 2019

Exchange Server проверки готовности

Статья • 04.04.2023

В этой статье содержатся сведения о проверках готовности, которые Exchange Server выполняет при установке Exchange. Проверки готовности гарантируют, что лес Active Directory и серверы Exchange готовы к установке версии Exchange. Каждая статья о проверке готовности описывает действия, которые можно предпринять для устранения проблем, обнаруженных при выполнении проверок готовности. Действия, описанные в статье о проверке готовности, следует выполнять только в том случае, если эта проверка готовности была показана во время настройки.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server, Exchange Online или Exchange Online Protection.

Существует каталог AD LDS в местоположении по умолчанию [ADAMDataPathExists]

Статья • 04.04.2023

Не удается продолжить установку Exchange, так как не удалось установить службы Active Directory облегченного каталога (AD LDS).

В папке по умолчанию находится ранее установленная версия AD LDS. Программа установки не может выполнить новую установку AD LDS в существующей структуре каталогов AD LDS.

Чтобы устранить данную проблему, удалите существующий каталог AD LDS, а затем повторно запустите программу установки.

Дополнительные сведения об управлении каталогами AD LDS см. на веб-странице Администрирование разделов каталогов AD LDS.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

В Active Directory существует дубликат контейнера системных объектов Microsoft Exchange [AdInitErrorRule]

Статья • 04.04.2023

Программа установки Exchange не может продолжить работу, так как она обнаружила дубликат контейнера системных объектов Microsoft Exchange в домен Active Directory контексте именования. Когда программа установки находит повторяющийся контейнер системных объектов Microsoft Exchange, перед продолжением установки необходимо удалить его. Обратите внимание, что повторное выполнение **DomainPrep** не устраняет проблему. Необходимо найти и удалить повторяющийся контейнер системных объектов Microsoft Exchange.

Чтобы устранить эту проблему, сделайте следующее:

1. Откройте **Пользователи и компьютеры Active Directory**. Например:
    - Нажмите клавишу Windows + R, введите **dsc.msc** и нажмите кнопку **OK**.
    - В **разделе Администрирование**>**Пользователи и компьютеры Active Directory**.
2. В **Пользователи и компьютеры Active Directory** щелкните **Просмотреть**>**дополнительные функции**.
3. Найдите контейнер повторяющихся **системных объектов Microsoft Exchange** .
4. Убедитесь, что контейнер **повторяющихся системных объектов Microsoft Exchange** не содержит допустимых объектов Active Directory.
5. Щелкните правой кнопкой мыши **повторяющийся контейнер системных объектов Microsoft Exchange**, выберите **команду Удалить**, а затем в диалоговом окне подтверждения выберите **да** .

> **Примечание**
>
> Чтобы немедленно реплицировать изменения, необходимо вручную инициировать репликацию между контроллерами домена.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Компонент Windows 'Командный интерфейс отказоустойчивого кластера' не установлен [RsatClusteringCmdInterfaceInstalled]

Статья • 04.04.2023

Невозможно продолжить установку Microsoft Exchange Server 2016, поскольку на локальном компьютере отсутствует требуемый компонент Windows. Вам необходимо установить этот компонент Windows до продолжения установки Exchange 2016.

Программа установки Exchange 2016 требует установить на компьютере компонент Windows **Командный интерфейс отказоустойчивого кластера**, прежде чем продолжить установку.

Выполните следующие действия, чтобы установить компонент Windows на этом компьютере. Если для завершения установки компонента требуется перезагрузка, вам необходимо закрыть программу установки Exchange 2016, перезагрузить компьютер и запустить программу установки повторно.

> ⓘ **Примечание**
>
> Для продолжения установки Exchange 2016 может потребоваться установить дополнительные компоненты или обновления Windows. Полный список необходимых компонентов и обновлений Windows см. **в Exchange Server предварительных требований**.

1. Откройте Windows PowerShell на локальном компьютере.
2. Запустите следующую команду для установки необходимого компонента Windows.

```
PowerShell

Install-WindowsFeature RSAT-Clustering-CmdInterface
```

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Active Directory не существует или с ним не удается связаться [CanAccessAD]

Статья • 04.04.2023

Программа установки Exchange не может продолжить работу, так как не может связаться с допустимым сайтом Active Directory. Для установки требуется, чтобы целевой сервер мог найти контекст именования конфигурации в Active Directory.

Чтобы устранить эту проблему, убедитесь, что учетная запись Active Directory используется для запуска программы установки, и повторите попытку запуска программы установки. Если проблема не устранена, следуйте указаниям по использованию средств поддержки, приведенным в следующих статьях, для дальнейшей диагностики проблемы.

Дополнительные сведения об устранении неполадок и настройке Active Directory для Exchange см. в следующих статьях:

- Подготовка Active Directory и доменов
- Устранение неполадок доменных служб Active Directory
- Настройка устранения неполадок на компьютере
- Устранение неполадок репликации Active Directory

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Локальный компьютер не присоединен к домену Active Directory [ComputerNotPartofDomain]

Статья • 04.04.2023

Программа установки Exchange не может продолжить работу, так как обнаружила, что целевой сервер не является членом домена Active Directory. Перед установкой роли сервера почтовых ящиков необходимо присоединить целевой сервер к домену Active Directory. Это сообщение также может появиться, если для установки Exchange используется учетная запись локального компьютера вместо учетной записи пользователя домена (с необходимыми разрешениями).

Дополнительные сведения см. в разделе требования к системе Exchange Server.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Установку первого сервера Exchange в организации нельзя делегировать [DelegatedBridgeheadFirstInstall]

Статья • 04.04.2023

Программа установки Exchange не может продолжить работу, так как это первый сервер Exchange Server в организации, и первый сервер Exchange должен быть установлен членом группы безопасности администраторов предприятия (чтобы создать контейнер организации Exchange и настроить в нем объекты).

Примечание. Если вы еще не расширили схему Active Directory для Exchange, необходимо выполнить одно из следующих действий.

- Член группы "Администраторы схемы" может расширить схему Active Directory с помощью другого компьютера в домене перед установкой Exchange.
- Программа установки Exchange может расширить схему, если ваша учетная запись входит в группу администраторов схемы.

Чтобы устранить эту проблему, снова запустите программу установки Exchange, используя учетную запись, которая является членом группы безопасности администраторов предприятия (добавьте текущую учетную запись или используйте другую учетную запись).

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Установку первого сервера Exchange в организации нельзя делегировать [DelegatedCafeFirstInstall]

Статья • 04.04.2023

Программа установки Exchange не может продолжить работу, так как это первый сервер Exchange Server в организации, и первый сервер Exchange должен быть установлен членом группы безопасности администраторов предприятия (чтобы создать контейнер организации Exchange и настроить в нем объекты).

Примечание. Если вы еще не расширили схему Active Directory для Exchange, необходимо выполнить одно из следующих действий.

- Член группы "Администраторы схемы" может расширить схему Active Directory с помощью другого компьютера в домене перед установкой Exchange.
- Программа установки Exchange может расширить схему, если ваша учетная запись входит в группу администраторов схемы.

Чтобы устранить эту проблему, снова запустите программу установки Exchange, используя учетную запись, которая является членом группы безопасности администраторов предприятия (добавьте текущую учетную запись или используйте другую учетную запись).

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Не удается делегировать установку первого сервера Exchange в организации [DelegatedClientAccessFirstInstall]

Статья • 04.04.2023

Программа установки Exchange не может продолжить работу, так как это первый сервер Exchange Server в организации, и первый сервер Exchange должен быть установлен членом группы безопасности администраторов предприятия (чтобы создать контейнер организации Exchange и настроить в нем объекты).

Примечание. Если вы еще не расширили схему Active Directory для Exchange, необходимо выполнить одно из следующих действий.

- Член группы "Администраторы схемы" может расширить схему Active Directory с помощью другого компьютера в домене перед установкой Exchange.
- Программа установки Exchange может расширить схему, если ваша учетная запись входит в группу администраторов схемы.

Чтобы устранить эту проблему, снова запустите программу установки Exchange, используя учетную запись, которая является членом группы безопасности администраторов предприятия (добавьте текущую учетную запись или используйте другую учетную запись).

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Установку первого сервера Exchange в организации нельзя делегировать [DelegatedMailboxFirstInstall]

Статья • 04.04.2023

Программа установки Exchange не может продолжить работу, так как это первый сервер Exchange Server в организации, и первый сервер Exchange должен быть установлен членом группы безопасности администраторов предприятия (чтобы создать контейнер организации Exchange и настроить в нем объекты).

Примечание. Если вы еще не расширили схему Active Directory для Exchange, необходимо выполнить одно из следующих действий.

- Член группы "Администраторы схемы" может расширить схему Active Directory с помощью другого компьютера в домене перед установкой Exchange.
- Программа установки Exchange может расширить схему, если ваша учетная запись входит в группу администраторов схемы.

Чтобы устранить эту проблему, снова запустите программу установки Exchange, используя учетную запись, которая является членом группы безопасности администраторов предприятия (добавьте текущую учетную запись или используйте другую учетную запись).

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Установку первого сервера Exchange Server в организации невозможно делегировать [DelegatedUnifiedMessagingFirstInstall]

Статья • 04.04.2023

Не удается продолжить установку Exchange 2016, так как это первый сервер Exchange Server в организации, и первый сервер Exchange server должен быть установлен членом группы безопасности администраторов предприятия (чтобы создать контейнер организации Exchange и настроить в нем объекты).

Примечание. Если вы еще не расширили схему Active Directory для Exchange, необходимо выполнить одно из следующих действий.

- Член группы "Администраторы схемы" может расширить схему Active Directory с помощью другого компьютера в домене перед установкой Exchange.
- Программа установки Exchange может расширить схему, если ваша учетная запись входит в группу администраторов схемы.

Чтобы устранить эту проблему, снова запустите программу установки Exchange, используя учетную запись, которая является членом группы безопасности администраторов предприятия (добавьте текущую учетную запись или используйте другую учетную запись).

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Чтобы домены могли быть подготовлены для Exchange [DomainPrepWithoutADUpdate]

Статья • 12.01.2024

Программа установки Exchange не может продолжить работу, так как она обнаружила, что приложение PrepareAD не было запущено. Ваша учетная запись должна быть членом группы безопасности "Администраторы предприятия". Компьютер должен находиться на том же сайте и домене Active Directory, что и хозяин схемы, а также должен быть на связи со всеми доменами в лесу через TCP-порт 389. Дополнительные сведения см. в статье Подготовка Active Directory и доменов для Exchange Server.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server .

Не удается выполнить запись в контейнер организации Exchange [GlobalServerInstall]

Статья • 04.04.2023

Программа установки Exchange не может продолжить работу, так как у учетной записи пользователя нет разрешений, необходимых для записи в контейнер организации в службе каталогов Active Directory.

Для установки требуется, чтобы учетная запись, используемая для установки Exchange, была иметь разрешения на создание и изменение объектов в Active Directory:

- Если это первый сервер Exchange Server в вашей организации, ваша учетная запись должна быть членом группы безопасности "Администраторы схемы" (для расширения схемы) и группы безопасности "Администраторы предприятия" (для подготовки Active Directory).
- После подготовки Active Directory к устанавливаемой версии Exchange ваша учетная запись должна быть членом группы ролей "Управление организацией".

Дополнительные сведения см. в статье Подготовка Active Directory и доменов для Exchange.

Чтобы устранить эту проблему, снова запустите настройку Exchange, используя учетную запись с соответствующими разрешениями (предоставьте разрешения текущей учетной записи или используйте другую учетную запись).

> ⓘ **Важно!**
>
> Установка Exchange между лесами не поддерживается. Используйте учетную запись в лесу Active Directory, где устанавливается Exchange.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Требуются глобальные обновления [GlobalUpdateRequired]

Статья • 04.04.2023

Программа установки Exchange не может продолжить работу, так как у учетной записи пользователя нет разрешений, необходимых для записи в контейнер организации в службе каталогов Active Directory.

Для установки требуется, чтобы учетная запись, используемая для установки Exchange, была иметь разрешения на создание и изменение объектов в Active Directory:

- Если это первый сервер Exchange Server в вашей организации, ваша учетная запись должна быть членом группы безопасности "Администраторы схемы" (для расширения схемы) и группы безопасности "Администраторы предприятия" (для подготовки Active Directory).
- После подготовки Active Directory к устанавливаемой версии Exchange ваша учетная запись должна быть членом группы ролей "Управление организацией".

Дополнительные сведения см. в статье Подготовка Active Directory и доменов для Exchange.

Чтобы устранить эту проблему, снова запустите программу установки, используя учетную запись с соответствующими разрешениями (предоставьте разрешения для текущей учетной записи или используйте другую учетную запись).

> ⓘ **Важно!**
>
> Установка Exchange между лесами не поддерживается. Используйте учетную запись в лесу Active Directory, где устанавливается Exchange.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Запись узла для локального компьютера не найдена в базе данных DNS [HostRecordMissing]

Статья • 04.04.2023

Не удается продолжить установку Exchange, так как запись узла (A) для этого компьютера не может быть найдена в зоне DNS для домена. Для установки требуется действительная запись A для сервера, а Exchange использует записи A сервера электронной почты для поиска IP-адреса следующего прыжка для отправки сообщений.

Чтобы устранить эту проблему, выполните следующие действия:

- Убедитесь, что локальная настройка TCP/IP указывает на правильный сервер DNS. Дополнительные сведения см. в разделе Настройка параметров TCP/IP.
- С помощью команды nslookup.exe убедитесь в существовании записи узла (A) на DNS-сервере. Дополнительные сведения см. в статье Проверка наличия записей ресурсов A в DNS.

Сведения о разрешении DNS-имен, устранении неполадок и записи A см. в следующих статьях:

- Устранение неполадок DNS
- Управление записями ресурсов

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Установка на контроллерах домена не поддерживается с разделением разрешений Active Directory [InstallOnDCInADSplitPermissionMode]

Статья • 04.04.2023

Программа установки Exchange обнаружила, что вы устанавливаете Exchange на контроллере домена Active Directory, и выполняется одно из следующих условий:

- В организации Exchange уже настроена служба каталогов Active Directory с разделением разрешений.
- Вы выбрали параметр Разделенные разрешения Active Directory в программе установки Exchange.

Установка Exchange на контроллерах домена не поддерживается, если в организации Exchange настроены разделенные разрешения Active Directory. Чтобы установить Exchange на контроллере домена, необходимо настроить организацию Exchange для разделения разрешений на основе контроль доступа ролей (RBAC) или общих разрешений.

> ⓘ **Важно!**
>
> Не рекомендуется устанавливать Exchange на контроллерах домена Active Directory. Дополнительные сведения см. в разделе **Установка Exchange на контроллере домена не рекомендуется [WarningInstallExchangeRolesOnDomainController]**.

Если вы хотите использовать разделенные разрешения Active Directory, необходимо установить Exchange на рядовом сервере.

Дополнительные сведения о разделенных и общих разрешениях в Exchange 2013 или более поздней версии см. в следующих разделах:

- Understanding Split Permissions
- Configure Exchange 2013 for Split Permissions
- Configure Exchange 2013 for Shared Permissions

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server .

С текущей учетной записи не выполнен вход в домен Active Directory [LoggedOntoDomain]

Статья • 04.04.2023

Не удается продолжить установку Exchange, так как она обнаружила, что текущая учетная запись не входит в домен Active Directory. Необходимо войти с помощью учетной записи Active Directory, которая имеет разрешения, необходимые для установки Exchange.

Для установки требуется, чтобы учетная запись, используемая для установки Exchange, была иметь разрешения на создание и изменение объектов в Active Directory:

- Если это первый сервер Exchange Server в организации, ваша учетная запись должна быть членом группы безопасности "Администраторы схемы" (для расширения схемы) и группы безопасности "Администраторы предприятия" (для подготовки Active Directory).
- После подготовки Active Directory к устанавливаемой версии Exchange ваша учетная запись должна быть членом группы ролей "Управление организацией".

Дополнительные сведения см. в статье Подготовка Active Directory и доменов для Exchange.

Чтобы устранить эту проблему, снова запустите программу установки, используя учетную запись с соответствующими разрешениями (предоставьте разрешения для текущей учетной записи или используйте другую учетную запись).

> ⓘ **Важно!**
>
> Установка Exchange между лесами не поддерживается. Используйте учетную запись в лесу Active Directory, где устанавливается Exchange.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Для продолжения установки необходимо перегрузить компьютер [RebootPending]

Статья • 04.04.2023

Программа установки Exchange не может продолжить работу, так как обнаружена ожидающая перезагрузка для завершения установки других программ или обновлений Windows.

С чем это связано?

При установке программ и обновлений Windows в файлы, которые хранятся на вашем компьютере, вносятся изменения. Некоторые программы или обновления должны изменять или заменять используемые в настоящее время файлы. В этом случае перед установкой других программ необходимо перезагрузить компьютер.

Если установка предыдущей программы или обновления Windows не завершилась успешно, Windows и другие программы могут подумать, что перезагрузка требуется. Эта ошибка будет по-прежнему отображаться при каждом запуске программы установки Exchange , если это происходит (неудачная установка не может исправить условие, указывающее, что требуется перезагрузка).

Как это исправить?

Как правило, для устранения этой ошибки требуется только перезапустить сервер, но эта ошибка может появиться снова после перезапуска (например, для дополнительных обновлений программы или Windows также требуется перезагрузка). Попробуйте перезапустить сервер еще раз.

Если вы видите эту ошибку после перезапуска сервера более двух или трех раз, попробуйте переустановить программы или обновления Windows, которые были установлены недавно. Так вы доведете неудачную установку до конца.

Если эта ошибка *по-прежнему* возникает после нескольких перезапусков и переустановки последних программ или обновлений Windows, рекомендуем обратиться в службу поддержки майкрософт. Там вам помогут узнать, почему Windows и другие программы считают, что компьютер необходимо перезагрузить. Чтобы обратиться в службу поддержки Майкрософт, перейдите в раздел Поддержка для бизнеса и выберите **Серверы**>**Exchange Server**.

⊗ Внимание!

Хотя это заманчиво, настоятельно рекомендуется не пытаться обойти эту проблему, вручную удалив или изменив разделы или значения реестра. Хотя вы можете устранить эту проблему сейчас, изменение реестра вручную может вызвать проблемы позже. Это особенно важно в случае сбоя установки обновления Windows.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Вошедший в систему пользователь не является членом группы администраторов схемы [SchemaUpdateRequired]

Статья • 04.04.2023

Не удается продолжить установку Exchange, так как учетная запись пользователя не входит в группы безопасности "Администраторы схемы" и "Администраторы предприятия".

Для установки требуется, чтобы учетная запись, используемая для установки Exchange, была иметь разрешения на создание и изменение объектов в Active Directory:

- Если это первый сервер Exchange Server в вашей организации, ваша учетная запись должна быть членом группы безопасности "Администраторы схемы" (для расширения схемы) и группы безопасности "Администраторы предприятия" (для подготовки Active Directory).
- После подготовки Active Directory к устанавливаемой версии Exchange ваша учетная запись должна быть членом группы ролей "Управление организацией".

Дополнительные сведения см. в статье Подготовка Active Directory и доменов для Exchange.

Чтобы устранить эту проблему, снова запустите настройку Exchange, используя учетную запись с соответствующими разрешениями (предоставьте разрешения текущей учетной записи или используйте другую учетную запись).

> ⓘ **Важно!**
>
> Установка Exchange между лесами не поддерживается. Используйте учетную запись в лесу Active Directory, где устанавливается Exchange.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

UCMA версии 4.0, ядро времени выполнения не установлено [UcmaRedistMsi]

Статья • 04.04.2023

Для установки Exchange 2016 требуется среда выполнения Unified Communications Managed API 4.0 для служб единой системы обмена сообщениями (UM) в роли сервера почтовых ящиков. Чтобы продолжить установку Exchange 2016, необходимо установить это обновление.

Скачайте и установите 64-разрядное обновление из среды выполнения Unified Communications Managed API 4.0, а затем щелкните **Повторить на** странице **Проверки готовности** в мастере установки Exchange 2016.

> **Примечание**
>
> Если для установки этого обновления требуется перезагрузка, необходимо выйти из программы установки Exchange 2016, перезагрузить ее, а затем снова запустить программу установки.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Невозможно удалить базу данных почтовых ящиков [UnwillingToRemoveMailboxDatabase]

Статья • 04.04.2023

Программа установки Exchange не может продолжить работу, так как она не может удалить базу данных почтовых ящиков пользователя с локального сервера без потенциальной потери данных.

Прежде чем программа установки Exchange удалит роль сервера почтовых ящиков с сервера, программа установки подтверждает, что все базы данных почтовых ящиков удалены с сервера или что почтовые ящики на сервере не содержат активных почтовых ящиков. Однако почтовые ящики пользователей могут остаться на сервере.

Чтобы устранить эту проблему, выполните одно из следующих действий:

- Чтобы сохранить почтовые ящики и их содержимое, переместите их на другой сервер. Инструкции см. в разделе Перемещение почтовых ящиков в Exchange Server.
- Отключите почтовые ящики, если они больше не требуются. Дополнительные сведения см. в разделе Disable-Mailbox.
- Удалите базы данных почтовых ящиков, если они больше не требуются. Инструкции см. в статье Управление базами данных почтовых ящиков в Exchange Server.

После работы с базами данных почтовых ящиков на сервере снова запустите программу установки Exchange.

- Дополнительные сведения об определении почтового ящика в базе данных см. в разделе Get-Mailbox.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Не рекомендуется устанавливать Exchange на контроллере домена [WarningInstallExchangeRolesOnDomainController]

Статья • 04.04.2023

Exchange Server 2016 или Exchange 2019 программа установки обнаружила, что целевой компьютер является контроллером домена Active Directory, и мы не переключили установку Exchange на контроллерах домена.

Если вы устанавливаете Exchange на контроллере домена, обратите внимание на следующие проблемы:

- Настройка разделенных разрешений Exchange для Active Directory не поддерживается. Дополнительные сведения о разделенных разрешениях см. в разделе Общие сведения о разделенных разрешениях.
- Универсальная группа безопасности доверенной подсистемы Exchange (USG) добавляется в группу администраторов домена. Это действие предоставляет всем серверам Exchange Server права администратора домена в домене.
- Как сервер Exchange, так и Active Directory представляют собой ресурсоемкие приложения. Если оба приложения выполняются на одном компьютере, это влияет на производительность.
- Контроллер домена должен быть сервером глобального каталога, но службы Exchange могут неправильно запускаться на сервере глобального каталога.
- Завершение работы системы займет значительно больше времени, если вы не остановите службы Exchange перед завершением работы или перезапуском сервера.
- Понижение уровня контроллера домена до рядового сервера не поддерживается.
- Запуск Exchange на кластеризованном узле, который также является контроллером домена Active Directory, не поддерживается.

Поэтому рекомендуется устанавливать Exchange на рядовом сервере, а не на контроллере домена.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server .

Не установлено обновление KB2619234 [Win7RpcHttpAssocCookieGuidUpdate NotInstalled]

Статья • 04.04.2023

Exchange Server 2016 программа установки не может продолжиться, так как на локальном компьютере требуется обновление программного обеспечения. Вам будет нужно установить это обновление до продолжения установки Exchange 2016.

Для установки Exchange 2016 требуется обновление Windows Server, которое позволяет outlook Anywhere (RPC через HTTP) работать правильно.

Скачайте и установите 64-разрядное обновление из KB2619234, а затем щелкните **Повторить попытку** на странице **Проверки готовности** .

> **Примечание**
>
> Если для завершения установки этого обновления необходимо перезапустить компьютер, вам потребуется выйти из программы установки Exchange 2016, перезапустить компьютер, а затем снова запустить программу установки.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Установку первого сервера Exchange в организации нельзя делегировать [DelegatedFrontendTransportFirstInstall]

Статья • 04.04.2023

Программа установки Exchange не может продолжить работу, так как это первый сервер Exchange Server в организации, и первый сервер Exchange должен быть установлен членом группы безопасности администраторов предприятия (чтобы создать контейнер организации Exchange и настроить в нем объекты).

Примечание. Если вы еще не расширили схему Active Directory для Exchange, необходимо выполнить одно из следующих действий.

- Член группы "Администраторы схемы" может расширить схему Active Directory с помощью другого компьютера в домене перед установкой Exchange.
- Программа установки Exchange может расширить схему, если ваша учетная запись входит в группу администраторов схемы.

Чтобы устранить эту проблему, снова запустите программу установки Exchange, используя учетную запись, которая является членом группы безопасности администраторов предприятия (добавьте текущую учетную запись или используйте другую учетную запись).

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Для продолжения установки необходимо перегрузить компьютер [PendingRebootWindowsComponents]

Статья • 04.04.2023

Программа установки Exchange не может продолжить работу, так как обнаружена ожидающая перезагрузка для завершения установки других программ или обновлений Windows.

С чем это связано?

При установке программ и обновлений Windows в файлы, которые хранятся на вашем компьютере, вносятся изменения. Некоторые программы или обновления должны изменять или заменять используемые в настоящее время файлы. В этом случае перед установкой других программ необходимо перезагрузить компьютер.

Если установка предыдущей программы или обновления Windows не завершилась успешно, Windows и другие программы могут подумать, что перезагрузка требуется. Эта ошибка будет по-прежнему отображаться при каждом запуске программы установки Exchange , если это происходит (неудачная установка не может исправить условие, указывающее, что требуется перезагрузка).

Как это исправить?

Как правило, для устранения этой ошибки требуется только перезапустить сервер, но эта ошибка может появиться снова после перезапуска (например, для дополнительных обновлений программы или Windows также требуется перезагрузка). Попробуйте перезапустить сервер еще раз.

Если вы видите эту ошибку после перезапуска сервера более двух или трех раз, попробуйте переустановить программы или обновления Windows, которые были установлены недавно. Так вы доведете неудачную установку до конца.

Если эта ошибка *по-прежнему* возникает после нескольких перезапусков и переустановки последних программ или обновлений Windows, рекомендуем обратиться в службу поддержки майкрософт. Там вам помогут узнать, почему Windows и другие программы считают, что компьютер необходимо перезагрузить. Чтобы обратиться в службу поддержки Майкрософт, перейдите в раздел Поддержка для бизнеса и выберите **Серверы**>**Exchange Server**.

⊗ Внимание!

Хотя это заманчиво, настоятельно рекомендуется не пытаться обойти эту проблему, вручную удалив или изменив разделы или значения реестра. Хотя вы можете устранить эту проблему сейчас, изменение реестра вручную может вызвать проблемы позже. Это особенно важно в случае сбоя установки обновления Windows.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Невозможно установить Exchange 2016 в лесу, в котором находятся серверы Exchange 2000 или Exchange 2003. [Exchange2000or2003PresentInOrg]

Статья • 04.04.2023

Не удается продолжить установку Exchange, так как версия Exchange, которая слишком старая для сосуществования с устанавливаемой версией была найдена в лесу Active Directory. Прежде чем продолжить, необходимо исключить из леса все неподдерживаемые версии Exchange. Для этого сначала может потребоваться выполнить обновление до промежуточной версии Exchange.

Установка Exchange Server 2016 или более поздних версий не может быть продолжена, так как программа установки обнаружила один или несколько серверов Exchange 2000 или Exchange 2003 в лесу Active Directory. Перед установкой Exchange 2016 или более поздней версии в организации необходимо удалить из леса все серверы Exchange 2000 или Exchange 2003.

Путь обновления, который необходимо выполнить, зависит от текущей версии Exchange. Пути обновления описаны в следующей таблице:

> ⓘ **Примечание**
>
> При необходимости обновления до промежуточной версии Exchange необходимо перенести все почтовые ящики, общедоступные папки и другие компоненты в промежуточную версию Exchange, прежде чем вывести из эксплуатации и удалить предыдущие серверы Exchange.

Текущая версия Exchange	Последняя версия Exchange для сосуществования	Сводка по пути обновления
Exchange 2000	Exchange 2007	Exchange 2000 > Exchange 2007 > Exchange 2013 > Exchange 2019.
Exchange 2003	Exchange 2010	Exchange 2003 > Exchange 2010 > Exchange 2016 > Exchange 2019.

Текущая версия Exchange	Последняя версия Exchange для сосуществования	Сводка по пути обновления
Exchange 2007	Exchange 2013	Exchange 2007 > Exchange 2013 > Exchange 2019.
Exchange 2010	Exchange 2016	Exchange 2010 > Exchange 2016 > Exchange 2019.

При обновлении до Exchange 2013 или более поздней версии можно использовать помощник по развертыванию Exchange, чтобы помочь завершить развертывание. Дополнительные сведения см. в разделе Помощник по развертыванию Exchange.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Найдена несовместимая операционная система [ValidOSVersion]

Статья • 04.04.2023

Программа установки Microsoft Exchange Server 2016 не может продолжать работу, так как обнаружена несовместимая операционная система. Перед установкой Exchange 2016 необходимо установить на этом компьютере совместимую операционную систему. В таблице ниже приведен список операционных систем, совместимых с Exchange 2016.

> **ⓘ Важно!**
>
> Exchange 2016 не поддерживает вариант установки основных серверных компонентов Windows Server.

Поддерживаемые операционные системы для Exchange 2016:

Компонент	Требования
Роли серверов почтовых ящиков и пограничных транспортных серверов	Windows Server 2016 Standard или Datacenter * Windows Server 2012 R2 Standard или Datacenter Windows Server 2012 Standard или Datacenter
Средства управления	Один из следующих продуктов: • Windows Server 2016 Standard или Datacenter * • Windows Server 2012 R2 Standard или Datacenter • Windows Server 2012 Standard или Datacenter • 64-разрядный выпуск Windows 10 • 64-разрядный выпуск Windows 8.1

*Требуется накопительный пакет обновления 3 (или более поздней версии) для Exchange Server 2016.

Дополнительные сведения см. в разделе требования к системе Exchange Server.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server .

Объект групповой политики ExecutionPolicy определен [PowerShellExecutionPolicyCheckSet]

Статья • 04.04.2023

Программа установки Exchange не может продолжить работу, так как обнаружила, что объект **ExecutionPolicy** групповая политика определяет одну или обе из следующих политик:

- **MachinePolicy**
- **UserPolicy**

Не имеет значения, как были определены политики; имеет значение только то, что они были определены.

Программа установки Exchange останавливает и отключает службу инструментария управления Windows (WMI). Если какая-либо из этих политик определена, службу инструментария WMI необходимо включить для выполнения сценария Windows PowerShell. Если эти политики определены, а служба инструментария WMI остановлена, программа установки прекратит работу, а сервер перейдет в несогласованное состояние.

Чтобы продолжить установку, необходимо временно удалить все определения **MachinePolicy** или **UserPolicy** в объекте групповой политики **ExecutionPolicy** :

PowerShell

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell
-Name ExecutionPolicy -Value ""
```

Возникли проблемы? Обратитесь за помощью на форумах Exchange.

Основной суффикс DNS отсутствует [ms.exch.setupreadiness.FqdnMissing]

Статья • 26.02.2024

Не удается продолжить установку Exchange, так как основной DNS-суффикс (например, contoso.com) не настроен на целевом сервере. Как правило, эта ошибка возникает при попытке установить роль пограничного транспортного сервера.

Чтобы устранить эту проблему, добавьте на компьютер основной DNS-суффикс, а затем снова запустите программу установки.

1. Замените <Значение> DNS-суффиксом, который вы хотите использовать (например, contoso.com), и выполните следующую команду в Windows PowerShell на целевом сервере:

PowerShell

```
Set-ItemProperty -Path
HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters -Name 'NV Domain' -
Value <Value>
```

2. Перезагрузите компьютер и снова запустите программу установки.

> ⓘ **Важно!**
>
> Изменение имени компьютера или основного DNS-суффикса после установки Exchange не поддерживается.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Протокол MAPI over HTTP не включен [WarnMapiHttpNotEnabled]

Статья • 04.04.2023

Программа установки Microsoft Exchange Server 2016 отобразила это предупреждение, так как в этой организации запущены серверы под управлением Exchange 2016 или более поздних версий, а протокол MAPI over HTTP не включен.

MAPI over HTTP — это рекомендуемый метод подключения Outlook к серверам под управлением Exchange 2016 или более поздних версий. MAPI через HTTP повышает надежность и стабильность подключений Outlook и Exchange, перемещая транспортный уровень в стандартную отраслевую модель HTTP. Это обеспечивает большую видимость ошибок транспорта и улучшенные возможности восстановления. Дополнительные возможности включают поддержку явной функции приостановки и возобновления. Благодаря этому поддерживаемые клиенты могут менять сети или выходить из режима гибернации, поддерживая тот же контекст сервера.

Программа установки Exchange не выполнит автоматическое включение протокола MAPI over HTTP во избежание внесения нежелательных изменений в клиентские подключения. Однако мы рекомендуем немедленно включить MAPI через HTTP, чтобы получить преимущества, которые он предоставляет.

Дополнительные сведения о MAPI через HTTP и о том, как его включить, см. в разделе MAPI через HTTP в Exchange Server.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Не удается установить Exchange 2016 или более поздней версии в лесу, который содержит Exchange 2007 [E16E12CoexistenceMinVersionRequirement]

Статья • 04.04.2023

Невозможно продолжить установку Exchange Server 2016 или более поздней версии, так как программа установки обнаружила один или несколько серверов Exchange 2007 в лесу Active Directory. Перед установкой Exchange 2016 или более поздней версии в организации необходимо удалить все серверы Exchange 2007 из леса.

Ниже приведены шаги по обновлению exchange 2007.

1. Install Exchange 2013 into your Exchange 2007 organization.
2. Configure Exchange 2013 and Exchange 2007 coexistence.
3. Перенесите почтовые ящики, общие папки и другие компоненты Exchange 2007 в службу Exchange 2013.
4. Спишите и удалите все сервера Exchange 2007.
5. Установите Exchange 2016 или Exchange 2019 в организации Exchange 2013.
6. Настройте сосуществование с Exchange 2013.
7. Перенос почтовых ящиков, общедоступных папок и других компонентов Exchange 2013 в Exchange 2016 или Exchange 2019.
8. Спишите и удалите все сервера Exchange 2013.

Варианты сосуществования (и, следовательно, обновления) для Exchange описаны в следующей таблице:

Текущая версия Exchange	**Последняя версия Exchange для сосуществования**
Exchange 2000	Exchange 2007
Exchange 2003	Exchange 2010

Текущая версия Exchange	Последняя версия Exchange для сосуществования
Exchange 2007	Exchange 2013
Exchange 2010	Exchange 2016
Exchange 2013	Exchange 2019

При обновлении до Exchange 2013 или более поздней версии можно использовать помощник по развертыванию Exchange, чтобы помочь завершить развертывание. Дополнительные сведения см. в разделе Помощник по развертыванию Exchange.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Для сосуществования с Exchange 2016 или более поздней версии требуется Exchange 2013 CU10 или более поздней версии [E16E15CoexistenceMinVersionRequirement]

Статья • 04.04.2023

Установка Exchange Server 2016 или более поздних версий не может быть продолжена, так как программа установки обнаружила один или несколько серверов Exchange 2013, на которых не установлена минимальная требуемая версия Exchange 2013. Перед установкой Exchange 2016 или более поздней версии в организации все серверы Exchange 2013 в лесу должны работать под управлением Exchange 2013 с накопительным пакетом обновления 10 (CU10) или более поздней версии. Это требование включает пограничные транспортные серверы Exchange 2013.

> ⓘ **Важно!**
>
> После обновления пограничных транспортных серверов Exchange 2013 до Exchange 2013 с накопительным пакетом обновления 10 (CU10) или более поздней версии необходимо повторно создать пограничные подписки между **вашей** организацией Exchange и каждым пограничным транспортным сервером (чтобы обновить версию Exchange пограничного транспортного сервера в Active Directory). Дополнительные сведения о повторном создании пограничных подписок в Exchange 2013 см. в статье **Управление пограничными подписками**.

Серверы Exchange 2013 не могут сосуществовать с Exchange Server 2019 CU15 или более поздней версии [E19E15CoexistenceRequirement]

Статья • 24.09.2024

Установка Exchange Server 2019 с накопительным пакетом обновления 15 или более поздней версии не может быть продолжена, так как программа установки обнаружила один или несколько серверов Exchange 2013. Перед установкой Exchange 2019 CU15 или более поздней версии в организации необходимо удалить все серверы Exchange 2013 в лесу.

Дополнительные сведения см. в записи блога Обновление организации с текущих версий до Exchange Server SE .

Компонент Windows Web-Metabase не установлен на этом компьютере [ms-exch-setupreadiness-LonghornIIS6MetabaseNotInstalled]

Статья • 16.01.2025

Microsoft Exchange Server программа установки отображает эту ошибку `Web-Metabase`, так как Компонент Windows не установлен на компьютере.

Прежде чем продолжить Microsoft Exchange Server установку, необходимо установить отсутствующий компонент.

Чтобы установить компонент на Windows Server, выполните следующую команду PowerShell:

PowerShell

```
Install-WindowsFeature Web-Metabase
```

Чтобы установить компонент на клиенте Windows, выполните следующую команду PowerShell:

PowerShell

```
Enable-WindowsOptionalFeature -Online -FeatureName IIS-Metabase -All
```

Полный список необходимых компонентов и обновлений Windows проверка Exchange Server предварительные требования.

Компонент Windows Web-Mgmt-Console не установлен на этом компьютере [ms-exch-setupreadiness-LonghornIIS7ManagementConsoleInstalled]

Статья • 16.01.2025

Microsoft Exchange Server программа установки отображает эту ошибку `Web-Mgmt-Console`, так как Компонент Windows не установлен на компьютере.

Прежде чем продолжить Microsoft Exchange Server установку, необходимо установить отсутствующий компонент.

Чтобы установить компонент на Windows Server, выполните следующую команду PowerShell:

PowerShell

```
Install-WindowsFeature Web-Mgmt-Console
```

Чтобы установить компонент на клиенте Windows, выполните следующую команду PowerShell:

PowerShell

```
Enable-WindowsOptionalFeature -Online -FeatureName IIS-ManagementConsole -All
```

Полный список необходимых компонентов и обновлений Windows проверка Exchange Server предварительные требования.

пакет Распространяемый компонент Visual C++ для Visual Studio 2012 не установлен на этом компьютере [ms-exch-setupreadiness-VC2012RedistDependencyRequirement]

Статья • 16.01.2025

Microsoft Exchange Server программа установки отображает эту ошибку, `Visual C++ Redistributable Package for Visual Studio 2012` так как не установлен на компьютере.

Перед продолжением Microsoft Exchange Server установки необходимо установить отсутствующий компонент.

Скачать пакет Распространяемый компонент Visual C++ для Visual Studio 2012

Полный список необходимых компонентов, обновлений и компонентов Windows проверка Exchange Server предварительные требования.

пакет Распространяемый компонент Visual C++ для Visual Studio 2013 не установлен на этом компьютере [ms-exch-setupreadiness-VC2013RedistDependencyRequirement]

Статья • 16.01.2025

Microsoft Exchange Server программа установки отображает эту ошибку, `Visual C++ Redistributable Package for Visual Studio 2013` так как не установлен на компьютере.

Перед продолжением Microsoft Exchange Server установки необходимо установить отсутствующий компонент.

Скачать пакет Распространяемый компонент Visual C++ для Visual Studio 2013

Полный список необходимых компонентов, обновлений и компонентов Windows проверка Exchange Server предварительные требования.

Компонент Windows NET-Framework-45-Core не установлен на этом компьютере [NETFramework45CoreNotInstalled]

Статья • 15.10.2024

Microsoft Exchange Server программа установки отображает эту ошибку `NET-Framework-45-Core`, так как Компонент Windows не установлен на компьютере.

Прежде чем продолжить Microsoft Exchange Server установку, необходимо установить отсутствующий компонент. Чтобы установить компонент, выполните следующую команду PowerShell:

PowerShell

```
Install-WindowsFeature NET-Framework-45-Core
```

Полный список необходимых компонентов и обновлений Windows проверка Exchange Server предварительные требования.

Компонент Windows NET-Framework-45-ASPNET не установлен на этом компьютере [NETFramework45ASPNETNotInstalled]

Статья • 15.10.2024

Microsoft Exchange Server программа установки отображает эту ошибку `NET-Framework-45-ASPNET`, так как Компонент Windows не установлен на компьютере.

Прежде чем продолжить Microsoft Exchange Server установку, необходимо установить отсутствующий компонент. Чтобы установить компонент, выполните следующую команду PowerShell:

PowerShell

```
Install-WindowsFeature NET-Framework-45-ASPNET
```

Полный список необходимых компонентов и обновлений Windows проверка Exchange Server предварительные требования.

Компонент Windows NET-WCF-HTTP-Activation45 не установлен на этом компьютере [NETWCFHTTPActivation45NotInstalled]

Статья • 15.10.2024

Microsoft Exchange Server программа установки отображает эту ошибку `NET-WCF-HTTP-Activation45`, так как Компонент Windows не установлен на компьютере.

Прежде чем продолжить Microsoft Exchange Server установку, необходимо установить отсутствующий компонент. Чтобы установить компонент, выполните следующую команду PowerShell:

PowerShell

```
Install-WindowsFeature NET-WCF-HTTP-Activation45
```

Полный список необходимых компонентов и обновлений Windows проверка Exchange Server предварительные требования.

Компонент Windows NET-WCF-Pipe-Activation45 не установлен на этом компьютере [NETWCFPipeActivation45NotInstalled]

Статья • 17.09.2024

Microsoft Exchange Server программа установки отображает эту ошибку `NET-WCF-Pipe-Activation45`, так как Компонент Windows не установлен на компьютере.

Прежде чем продолжить Microsoft Exchange Server установку, необходимо установить отсутствующий компонент. Чтобы установить компонент, выполните следующую команду PowerShell:

PowerShell

```
Install-WindowsFeature NET-WCF-Pipe-Activation45
```

Полный список необходимых компонентов и обновлений Windows проверка Exchange Server предварительные требования.

Компонент Windows NET-WCF-TCP-PortSharing45 не установлен на этом компьютере [NETWCFTCPPortSharing45NotInstalled]

Статья • 15.10.2024

Microsoft Exchange Server программа установки отображает эту ошибку `NET-WCF-TCP-PortSharing45`, так как Компонент Windows не установлен на компьютере.

Прежде чем продолжить Microsoft Exchange Server установку, необходимо установить отсутствующий компонент. Чтобы установить компонент, выполните следующую команду PowerShell:

PowerShell

```
Install-WindowsFeature NET-WCF-TCP-PortSharing45
```

Полный список необходимых компонентов и обновлений Windows проверка Exchange Server предварительные требования.

Компонент Windows Web-Net-Ext45 не установлен на этом компьютере [WebNetExt45NotInstalled]

Статья • 15.10.2024

Microsoft Exchange Server программа установки отображает эту ошибку `Web-Net-Ext45`, так как Компонент Windows не установлен на компьютере.

Прежде чем продолжить Microsoft Exchange Server установку, необходимо установить отсутствующий компонент. Чтобы установить компонент, выполните следующую команду PowerShell:

PowerShell

```
Install-WindowsFeature Web-Net-Ext45
```

Полный список необходимых компонентов и обновлений Windows проверка Exchange Server предварительные требования.

Компонент Windows Web-ISAPI-Ext не установлен на этом компьютере [WebISAPIExtNotInstalled]

Статья • 15.10.2024

Microsoft Exchange Server программа установки отображает эту ошибку `Web-ISAPI-Ext`, так как Компонент Windows не установлен на компьютере.

Прежде чем продолжить Microsoft Exchange Server установку, необходимо установить отсутствующий компонент. Чтобы установить компонент, выполните следующую команду PowerShell:

PowerShell

```
Install-WindowsFeature Web-ISAPI-Ext
```

Полный список необходимых компонентов и обновлений Windows проверка Exchange Server предварительные требования.

Компонент Windows Web-ASP-NET45 не установлен на этом компьютере [WebASPNET45NotInstalled]

Статья • 17.09.2024

Microsoft Exchange Server программа установки отображает эту ошибку `Web-ASP-NET45`, так как Компонент Windows не установлен на компьютере.

Прежде чем продолжить Microsoft Exchange Server установку, необходимо установить отсутствующий компонент. Чтобы установить компонент, выполните следующую команду PowerShell:

PowerShell

```
Install-WindowsFeature Web-ASP-NET45
```

Полный список необходимых компонентов и обновлений Windows проверка Exchange Server предварительные требования.

Компонент Windows RPC-over-HTTP-proxy не установлен на этом компьютере [RPCOverHTTPproxyNotInstalled]

Статья • 15.10.2024

Microsoft Exchange Server программа установки отображает эту ошибку `RPC-over-HTTP-proxy`, так как Компонент Windows не установлен на компьютере.

Прежде чем продолжить Microsoft Exchange Server установку, необходимо установить отсутствующий компонент. Чтобы установить компонент, выполните следующую команду PowerShell:

PowerShell

```
Install-WindowsFeature RPC-over-HTTP-proxy
```

Полный список необходимых компонентов и обновлений Windows проверка Exchange Server предварительные требования.

Компонент Windows Server-Gui-Mgmt-Infra не установлен на этом компьютере [ServerGuiMgmtInfraNotInstalled]

Статья • 15.10.2024

Microsoft Exchange Server программа установки отображает эту ошибку `Server-Gui-Mgmt-Infra`, так как Компонент Windows не установлен на компьютере.

Прежде чем продолжить Microsoft Exchange Server установку, необходимо установить отсутствующий компонент. Чтобы установить компонент, выполните следующую команду PowerShell:

PowerShell

```
Install-WindowsFeature Server-Gui-Mgmt-Infra
```

Полный список необходимых компонентов и обновлений Windows проверка Exchange Server предварительные требования.

Компонент Windows RSAT-ADDS-Tools не установлен на этом компьютере [RsatAddsToolsInstalled]

Статья • 15.10.2024

Microsoft Exchange Server программа установки отображает эту ошибку `RSAT-ADDS-Tools`, так как Компонент Windows не установлен на компьютере.

Прежде чем продолжить Microsoft Exchange Server установку, необходимо установить отсутствующий компонент. Чтобы установить компонент, выполните следующую команду PowerShell:

PowerShell

```
Install-WindowsFeature RSAT-ADDS-Tools
```

Полный список необходимых компонентов и обновлений Windows проверка Exchange Server предварительные требования.

Компонент Windows RSAT-Clustering не установлен на этом компьютере [RsatClusteringInstalled]

Статья • 17.09.2024

Microsoft Exchange Server программа установки отображает эту ошибку `RSAT-Clustering`, так как Компонент Windows не установлен на компьютере.

Прежде чем продолжить Microsoft Exchange Server установку, необходимо установить отсутствующий компонент. Чтобы установить компонент, выполните следующую команду PowerShell:

PowerShell

```
Install-WindowsFeature RSAT-Clustering
```

Полный список необходимых компонентов и обновлений Windows проверка Exchange Server предварительные требования.

Компонент Windows RSAT-Clustering-Mgmt не установлен на этом компьютере [RsatClusteringMgmtInstalled]

Статья • 17.09.2024

Microsoft Exchange Server программа установки отображает эту ошибку `RSAT-Clustering-Mgmt`, так как Компонент Windows не установлен на компьютере.

Прежде чем продолжить Microsoft Exchange Server установку, необходимо установить отсутствующий компонент. Чтобы установить компонент, выполните следующую команду PowerShell:

PowerShell

```
Install-WindowsFeature RSAT-Clustering-Mgmt
```

Полный список необходимых компонентов и обновлений Windows проверка Exchange Server предварительные требования.

Компонент Windows RSAT-Clustering-PowerShell не установлен на этом компьютере [RsatClusteringPowerShellInstalled]

Статья • 15.10.2024

Microsoft Exchange Server программа установки отображает эту ошибку `RSAT-Clustering-PowerShell`, так как Компонент Windows не установлен на компьютере.

Прежде чем продолжить Microsoft Exchange Server установку, необходимо установить отсутствующий компонент. Чтобы установить компонент, выполните следующую команду PowerShell:

PowerShell

```
Install-WindowsFeature RSAT-Clustering-PowerShell
```

Полный список необходимых компонентов и обновлений Windows проверка Exchange Server предварительные требования.

Серверы Exchange 2013 не обнаружены [NoE15ServerWarning]

Статья • 04.04.2023

Программа установки Microsoft Exchange Server 2016 отобразила это предупреждение, потому что в организации нет ролей сервера Exchange Server 2013.

> ⊗ **Внимание!**
>
> Если продолжить установку Exchange Server 2016, вы не сможете добавить серверы Exchange 2013 в организации позже.

Прежде чем выполнять развертывание Exchange 2016, рассмотрите указанные ниже факторы, при которых сначала может потребоваться развернуть серверы Exchange 2013.

- **Сторонние или собственные приложения**. Приложения, разработанные для более ранних версий Exchange, могут быть несовместимы с Exchange 2016. Для поддержки этих приложений может потребоваться обслуживание серверов Exchange 2013.
- **Требования для гибридного развертывания или миграции**. Если планируется перенос почтовых ящиков в организации, для некоторых решений могут понадобиться серверы Exchange 2013.

Если необходимо развернуть серверы Exchange 2013, то необходимо сделать это до развертывания Exchange 2016. Необходимо подготовить Active Directory для каждой версии Exchange в следующем порядке:

1. Exchange 2013
2. Exchange 2016

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server, Exchange Online или Exchange Online Protection.

Запуск "dir" на диске в формате ReFS может привести к зависаю компьютера [Win2k12RefsUpdateNotInstalled]

Статья • 26.02.2024

Microsoft Exchange Server 2016 программа установки обнаруживает, что на компьютере, на котором вы пытаетесь установить Exchange 2016, не установлено рекомендуемое обновление Windows. Перед установкой Exchange 2016 настоятельно рекомендуется установить это обновление Windows, чтобы избежать ряда проблем.

Компьютеры под управлением Windows Server 2012 и более поздней версии поддерживают ReFS (Resilient File System). Существует проблема, которая может привести к "зависанию" компьютеров при выполнении команды **dir** для дисков, отформатированных в ReFS.

Скачайте и установите 64-разрядное обновление по следующему URL-адресу, а затем выберите **повторить попытку** на странице **Проверки готовности** .

> ⓘ **Примечание**
>
> Если для завершения установки этого обновления необходимо перезапустить компьютер, вам потребуется выйти из программы установки Exchange 2016, перезапустить компьютер, а затем снова запустить программу установки.

Статья базы знаний Майкрософт KB2894875, компьютер на основе Windows 8 или Windows Server 2012 зависает при выполнении команды "dir" на томе ReFS .

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server .

Накопительный пакет обновления Windows Server 2012 не установлен [Win2k12RollupUpUpDateNotInstalled]

Статья • 26.02.2024

Microsoft Exchange Server 2016 программа установки обнаруживает, что на компьютере, на котором вы пытаетесь установить Exchange 2016, не установлено рекомендуемое обновление Windows. Перед установкой Exchange 2016 настоятельно рекомендуется установить это обновление Windows, чтобы избежать ряда проблем.

Накопительный пакет обновления Windows Server 2012, устраняющий несколько проблем, в том числе проблемы, которые могут привести к ненадежной производительности дисков в формате Отказоустойчивой файловой системы (ReFS).

Загрузите и установите 64-разрядное обновление со следующего URL-адреса, а затем щелкните **Повторить** на странице **проверок готовности**.

> ⓘ **Примечание**
>
> Если для завершения установки этого обновления необходимо перезапустить компьютер, вам потребуется выйти из программы установки Exchange 2016, перезапустить компьютер, а затем снова запустить программу установки.

Статья базы знаний Майкрософт KB2822241, накопительный пакет обновлений Windows 8 и Windows Server 2012: апрель 2013 г.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

Диски, отформатированные в ReFS, могут работать ненадежно [Win2k12UrefsUpdateNotInstalled]

Статья • 04.04.2023

Программа установки Microsoft Exchange Server 2016 обнаружила, что на компьютере, на который вы хотите установить Exchange 2016, нет рекомендованного обновления Windows. Перед установкой Exchange 2016 настоятельно рекомендуется установить это обновление Windows, чтобы избежать ряда проблем.

Компьютеры под управлением Windows Server 2012 и более поздней версии поддерживают ReFS (Resilient File System). Проблема в службе виртуальных дисков может привести к тому, что диски, отформатированные как ReFS, не будут работать надежно. Это может привести к повреждению или потере данных.

Загрузите и установите 64-разрядное обновление со следующего URL-адреса, а затем щелкните **Повторить** на странице **проверок готовности**.

> ⓘ **Примечание**
>
> Если для завершения установки этого обновления необходимо перезапустить компьютер, вам потребуется выйти из программы установки Exchange 2016, перезапустить компьютер, а затем снова запустить программу установки.

Статья базы знаний Майкрософт KB2884597, Служба виртуальных дисков или приложения, использующие службу виртуальных дисков, аварийно завершает работу или зависают в Windows Server 2012 .

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server .

KB3206632 обновление для системы безопасности не установлено [Win2k16LSARollupUpdateNotInstalled]

Статья • 27.02.2024

Невозможно продолжить установку Microsoft Exchange Server 2016, поскольку на локальном компьютере необходимо обновить программное обеспечение. Чтобы продолжить установку Exchange 2016, необходимо установить это обновление.

Для продолжения установки Exchange 2016 на компьютере должно быть установлено обновление для системы безопасности от 13 декабря 2016 г. (KB3206632).

Загрузите и установите 64-разрядное обновление со следующего URL-адреса, а затем щелкните **Повторить** на странице **проверок готовности**.

> **Примечание**
>
> Если для завершения установки этого обновления необходимо перезапустить компьютер, вам потребуется выйти из программы установки Exchange 2016, перезапустить компьютер, а затем снова запустить программу установки.

Обновление для системы безопасности за 13 декабря 2016 г. (KB3206632)

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server.

выпуски и версии Exchange Server

Статья • 04.04.2023

Exchange Server 2016 и Exchange Server 2019 доступны в двух серверных выпусках:

- **выпуск Enterprise**. Можно масштабировать до 100 подключенных баз данных на сервер.
- **Standard Edition**: только пять подключенных баз данных на сервер.

Подключенная база данных — это используемая база данных (активная база данных почтовых ящиков, подключенная для использования клиентами, или пассивная база данных почтовых ящиков, подключенная при восстановлении для репликации и воспроизведения журналов). Хотя можно создать больше баз данных, чем описанные ограничения, можно подключить только максимальное количество баз данных, разрешенных выпуском Exchange. Обратите внимание, что база данных восстановления не учитывается в этих ограничениях.

Выпуски сервера определяются ключом продукта. При вводе допустимого ключа продукта устанавливается поддерживаемый выпуск для сервера. Дополнительные сведения см. в разделе Ввод ключа продукта Exchange Server.

Примечания.

- Допустимый ключ продукта можно использовать для перехода с пробной версии (ознакомительной версии) Exchange на standard edition или выпуск Enterprise. После истечения срока действия пробного выпуска функциональность не будет потеряна, поэтому вы можете поддерживать лабораторию, демонстрацию, учебные и другие нерабочие среды в течение 120 дней без необходимости переустановки пробного выпуска Exchange или ввода ключа продукта.
- Вы можете использовать допустимый ключ продукта для перехода с standard edition на выпуск Enterprise.
- Вы не можете использовать допустимый ключ продукта для перехода с выпуск Enterprise на Standard Edition или возврата к пробной версии. Вы можете выполнить эти типы понижения, только удалив Exchange, переустановив Exchange и введя правильный ключ продукта.

версии Exchange Server

Список Exchange Server версий, а также сведения о том, как скачать и обновить до последней версии Exchange, см. в следующих разделах:

- Номера сборок и даты выпуска Exchange Server
- Установка серверов почтовых ящиков Exchange с помощью мастера
- Обновление Exchange до последнего накопительного пакета обновления

Чтобы просмотреть сведения о версиях и выпусках Exchange для всех серверов Exchange в организации, выполните следующую команду в командной консоли Exchange:

PowerShell

```
Get-ExchangeServer | Format-Table -Auto Name,Edition,AdminDisplayVersion
```

Типы лицензий Exchange Server

Exchange 2013 и все более поздние версии используют модель лицензирования, аналогичную лицензированию Exchange 2010:

- **Серверные лицензии**. Лицензия должна быть назначена для каждого сервера Exchange. Лицензия на сервер продается в двух выпусках сервера: Standard Edition и выпуск Enterprise.
- **Клиентские лицензии (КЛИЕНТСКИЕ лицензии).** Exchange также поставляется в двух выпусках CAL, которые называются клиентскими лицензиями уровня "Стандартный" и "Корпоративный". Вы можете сочетать выпуски Exchange Server с типами CAL и сопоставлять их. Например, можно использовать корпоративные клиентские лицензии с standard edition или стандартные клиентские лицензии с выпуск Enterprise.

Дополнительные сведения о типах лицензий Exchange см. в разделе Часто задаваемые вопросы о лицензировании Exchange.

поддержка языка Exchange Server

Статья • 04.04.2023

Exchange Server 2016 и Exchange Server 2019 годах имеют расширенную языковую поддержку как для серверов, так и для клиентов. В этом разделе перечислены языки, доступные как для серверов, так и для клиентов в Exchange 2016 и Exchange 2019.

Поддерживаемые серверные языки для Exchange 2016 и Exchange 2019

- китайский (упрощенное письмо);
- Китайский (традиционный)
- Английский язык
- Французский язык
- Немецкий язык
- Итальянский язык
- японский;
- Корейский
- Португальский
- Русский
- испанский;

Поддерживаемые клиентские языки для Exchange 2016 и Exchange 2019

- Амхарский
- Арабский
- Баскский (Basque)
- Бенгальский (Индия)

- Болгарский
- Каталонский
- Китайский (упрощенный)
- китайский (традиционный);
- хорватский;
- чешский;
- датский;
- голландский;
- английский;
- Эстонский
- Филиппинский (Филиппины)
- Финский
- Французский
- Галисийский
- Немецкий
- Греческий
- Гуджарати
- Иврит
- хинди;
- Венгерский
- Исландский
- Индонезийский
- итальянский;
- Японский
- Каннада

- Казахский
- Суахили
- Корейский язык
- латышский;
- Литовский
- Малайский (Бруней-Даруссалам)
- Малайский (Малайзия)
- Малаялам
- Маратхи
- Норвежский (букмол)
- Норвежский (нюнорск)
- Ория
- Персидский
- Польский
- португальский (Бразилия);
- португальский (Португалия);
- румынский;
- Русский
- Сербскохорватский (кириллица, Сербия)
- Сербскохорватский (латиница)
- словацкий;
- словенский;
- испанский;
- Шведский
- Тамильский

- Телугу
- Тайский
- турецкий;
- Украинский
- Урду
- Вьетнамский
- Валлийский

параметры конфигурации хранилища Exchange Server

Статья • 04.04.2023

Понимание вариантов хранения и требований к серверам почтовых ящиков в Exchange Server 2016 г. и Exchange Server 2019 г. является важной частью решения по проектированию хранилища сервера почтовых ящиков.

Архитектуры хранилища

В следующей таблице описываются поддерживаемые архитектуры хранилищ и приводятся рекомендации по их выбору.

Поддерживаемые архитектуры хранилища:

Архитектура хранилища	**Описание**	**Рекомендация**
Запоминающее устройство с прямым подключением (DAS)	DAS — это цифровое запоминающее устройство, подключаемое напрямую к серверу или рабочей станции без использования сети хранения в качестве промежуточного звена. Например, к технологиям передачи данных устройств DAS относятся следующие интерфейсы с последовательным подключением: Serial Attached SCSI (SAS) и Serial Attached Advanced Technology Attachment (Serial ATA, SATA).	Недоступно
Сеть хранения данных (SAN): Internet SCSI (iSCSI)	SAN — это архитектура для подключения запоминающих устройств на удаленных компьютерах (например, дисковых массивов и ленточных библиотек) к серверам таким образом, что устройства отображаются как локально подключенные к операционной системе (например, блочное хранилище). В сетях SAN с интерфейсом iSCSI команды SCSI инкапсулируются внутри IP-пакетов, а в качестве технологии передачи данных хранилища используется стандартная сетевая инфраструктура (например, Ethernet).	Не предоставляйте другим приложениям общий доступ к тем физическим дискам, на которых выполняется резервное копирование данных Exchange. Используйте выделенные сети хранения. Применяйте несколько сетевых путей для автономных конфигураций.

Архитектура хранилища	Описание	Рекомендация
SAN: Fibre Channel	San Fibre Channel инкапсулируют команды SCSI в пакетах Fibre Channel и обычно используют специализированные сети Fibre Channel в качестве транспорта хранилища.	Не предоставляйте другим приложениям общий доступ к тем физическим дискам, на которых выполняется резервное копирование данных Exchange. Используйте несколько сетевых путей FC для автономных конфигураций. Следуйте рекомендациям производителей запоминающих устройств для настройки адаптеров шины FC (HBA), например для параметров длины очереди и цели очереди.

Запоминающее устройство, подключаемое к сети (NAS), — это автономный компьютер, подключенный к сети, который предоставляет услуги хранения данных на базе файлов другим устройствам в сети. Операционная система и другое программное обеспечение на устройстве NAS обеспечивают функции хранения данных, файловых систем, доступа к файлам, а также управление этими функциями (например, хранение файлов).

Все хранилища, используемые Exchange для хранения данных Exchange, должны быть хранилищем на уровне блоков, так как Exchange 2016 не поддерживает использование томов NAS, кроме сценария SMB 3.0, описанного в статье Exchange Server виртуализации. Кроме того, в виртуализированной среде не поддерживается запоминающее устройство NAS, представленное для ведомого компьютера через низкоуровневую оболочку как хранилище уровня блоков.

Использовать уровни хранилища не рекомендуется, так как это может негативно повлиять на производительность системы. По этой причине не разрешайте контроллеру хранилища автоматически перемещать наиболее доступные файлы в "более быстрое" хранилище.

Типы физических дисков

В следующей таблице приводится список поддерживаемых типов физических дисков и приводятся рекомендации по их выбору.

Поддерживаемые типы физических дисков:

Тип физического диска	Описание	Поддержка и рекомендации

Тип физического диска	Описание	Поддержка и рекомендации
Serial ATA (SATA)	SATA — это последовательный интерфейс для дисков ATA и IDE (Integrated Device Electronics). Диски SATA доступны в различных форм-факторах, скоростях и емкости. Обычно диски SATA следует выбирать для хранения почтовых ящиков Exchange 2016 при наличии следующих проектных требований: • Большая емкость • Контроль производительности • Контроль энергопотребления	Поддерживаются: диски с секторами по 512 байт для ОС Windows Server 2008 и Windows Server 2008 R2. Кроме того, для версии Windows Server 2008 R2 поддерживаются диски 512e при наличии указанных ниже компонентов. • Исправление, описанное в обновлении KB982018. • Windows Server 2008 R2 с пакетом обновления 1 (SP1) и Exchange Server 2010 SP1. Exchange 2013 и более поздних версий поддерживает собственные диски секторов размером 4 килобайта (КБ) и диски 512e. Поддержка требует размещения всех копий базы данных на физических дисках одного типа. Например, не поддерживается конфигурация размещения одной копии данной базы данных на диске сектора 512 байт, а другая копия той же базы данных на диске 512e или 4K. Рекомендация: Рекомендуется выбирать диски SATA класса Enterprise, которые отличаются более высокими характеристиками нагрева, вибрации и надежности.
Serial Attached SCSI	Serial Attached SCSI — это последовательный интерфейс для дисков SCSI. Диски SCSI с последовательным подключением доступны в различных форм-факторах, скоростях и емкости. Обычно диски Serial Attached SCSI следует выбирать для хранения почтовых ящиков Exchange 2016 при наличии следующих проектных требований: • Контроль емкости • Высокая производительность • Контроль энергопотребления	Поддерживаются: диски с секторами по 512 байт для ОС Windows Server 2008 и Windows Server 2008 R2. Кроме того, для версии Windows Server 2008 R2 поддерживаются диски 512e при наличии указанных ниже компонентов. • Исправление, описанное в обновлении KB982018. • Windows Server 2008 R2 с пакетом обновления 1 (SP1) и Exchange Server 2010 с пакетом обновления 1 (SP1). Exchange 2013 и более поздних версий поддерживает собственные диски секторов размером 4 килобайта (КБ) и диски 512e. Для поддержки требуется, чтобы все копии базы данных были на одном физическом диске типа. Примером неподдерживаемой конфигурации является размещение одной копии данной базы данных на диске с секторами по 512 байт, а другой копии той же базы данных на диске 512e или на диске с секторами по 4 КБ. Рекомендация: кэширование во время записи на физический диск при работе без блока бесперебойного питания (UPS) должно быть отключено.

Тип физического диска	Описание	Поддержка и рекомендации
Fibre Channel	Fibre Channel (FC) — это электрический интерфейс, используемый для подключения дисков к оптоволоконным сетям хранения данных. Диски Fibre Channel доступны с различными скоростями и емкостью. Обычно диски Fibre Channel следует выбирать для хранения почтовых ящиков Exchange 2016 при наличии следующих проектных требований: • Контроль емкости • Высокая производительность • Подключение к сети SAN	Поддерживаются: диски с секторами по 512 байт для ОС Windows Server 2008 и Windows Server 2008 R2. Кроме того, для версии Windows Server 2008 R2 поддерживаются диски 512e при наличии указанных ниже компонентов. • Исправление, описанное в обновлении KB982018. • Windows Server 2008 R2 с пакетом обновления 1 (SP1) и Exchange Server 2010 SP1. Exchange 2013 и более поздних версий поддерживает собственные диски секторов размером 4 килобайта (КБ) и диски 512e. Для поддержки требуется, чтобы все копии базы данных были на одном физическом диске типа. Например, не поддерживается конфигурация размещения одной копии данной базы данных на диске сектора 512 байт, а другая копия той же базы данных на диске 512e или 4K. Рекомендация: кэширование во время записи на физический диск при работе без блока бесперебойного питания (UPS) должно быть отключено.
Твердотельный накопитель (SSD) (флэш-диск)	SSD — это устройство хранения данных, в котором для хранения постоянных данных используется твердотельная память. Устройство SSD эмулирует интерфейс жесткого диска. Диски SSD доступны с различными скоростями (разными возможностями производительности операций ввода-вывода) и емкостью. Обычно диски SSD следует выбирать для хранения почтовых ящиков Exchange 2016 при наличии следующих проектных требований: • Низкая емкость • Высокая производительность	Поддерживаются: диски с секторами по 512 байт для ОС Windows Server 2008 и Windows Server 2008 R2. Кроме того, для версии Windows Server 2008 R2 поддерживаются диски 512e при наличии указанных ниже компонентов. • Исправление, описанное в обновлении KB982018. • Windows Server 2008 R2 с пакетом обновления 1 (SP1) и Exchange Server 2010 с пакетом обновления 1 (SP1). Exchange 2013 и более поздних версий поддерживает собственные диски секторов размером 4 килобайта (КБ) и диски размером 512e, если все копии базы данных находятся на одном физическом диске. Например, не поддерживается конфигурация размещения одной копии данной базы данных на диске сектора 512 байт, а другая копия той же базы данных на диске 512e или 4K. Рекомендация: кэширование во время записи на физический диск при работе без блока бесперебойного питания (UPS) должно быть отключено. Как правило, серверам почтовых ящиков Exchange 2016 не нужны характеристики производительности запоминающих устройств SSD.

Факторы, учитываемые при выборе типов дисков

Существуют некоторые компромиссы при выборе типа диска для хранилища Exchange 2016. Правильно выбранный диск должен быть оптимален по соотношению производительности (как при последовательном, так и при случайном вводе-выводе), емкости, надежности, энергопотребления и капитальных расходов. В следующей таблице поддерживаемых типов физических дисков приводятся сведения по факторам выбора.

С точки зрения производительности использование больших и медленных дисков для хранилища Exchange в порядке при условии, что диски могут поддерживать среднюю задержку чтения и записи в 20

мс или менее при нагрузке.

Факторы выбора типа диска:

Скорость диска (об/мин)	Форм-фактор диска	Интерфейс или передача данных	Емкость	Производительность случайного ввода-вывода	Производительность последовательного ввода-вывода	Энергопотребление
5,400	2,5 дюйма	SATA	Средняя	Низкая	Низкая	Отличная
5,400	3,5 дюйма	SATA	Отличная	Низкая	Низкая	Выше среднего
7,200	2,5 дюйма	SATA	Средняя	Средняя	Средняя	Отличная
7,200	2,5 дюйма	Serial Attached SCSI	Средняя	Средняя	Выше среднего	Отличная
7,200	3,5 дюйма	SATA	Отличная	Средняя	Выше среднего	Выше среднего
7,200	3,5 дюйма	Serial Attached SCSI	Отличная	Средняя	Выше среднего	Выше среднего
7,200	3,5 дюйма	Fibre Channel	Отличная	Средняя	Выше среднего	Средняя
10,000	2,5 дюйма	Serial Attached SCSI	Ниже среднего	Отличная	Выше среднего	Выше среднего
10,000	3,5 дюйма	SATA	Средняя	Средняя	Выше среднего	Выше среднего
10,000	3,5 дюйма	Serial Attached SCSI	Средняя	Выше среднего	Выше среднего	Ниже среднего
10,000	3,5 дюйма	Fibre Channel	Средняя	Выше среднего	Выше среднего	Ниже среднего
15 000	2,5 дюйма	Serial Attached SCSI	Низкая	Отличная	Отличная	Средняя
15 000	3,5 дюйма	Serial Attached SCSI	Средняя	Отличная	Отличная	Ниже среднего
15 000	3,5 дюйма	Fibre Channel	Средняя	Отличная	Отличная	Плохо
SSD: -=	Неприменимо	SATA, Serial Attached SCSI, Fibre Channel	Низкая	Отличная	Отличная	Отличная

Рекомендации для поддерживаемых конфигураций хранилища

В этом разделе приводятся рекомендации для поддерживаемых конфигураций контроллеров дисков и массивов. В дополнение к часто используемому избыточному массиву независимых дисков (RAID), существует также просто куча дисков (или дисков) или JBOD, которая относится к коллекции жестких дисков, которые не были настроены для работы в качестве избыточного массива.

RAID часто используется для улучшения характеристик производительности отдельных дисков (путем чередовки данных между несколькими дисками) и для обеспечения защиты от сбоев отдельных дисков. Благодаря усовершенствованиям в области высокой доступности Exchange 2016 RAID не является обязательным компонентом для проектирования хранилища Exchange 2016. Однако RAID по-прежнему является важным компонентом структуры хранилища Exchange 2016 для автономных серверов и решений, требующих отказоустойчивости хранилища.

Том операционной системы, системы или файла подкачки

Рекомендуемая конфигурация для операционной системы, системы или тома файла подкачки заключается в использовании технологии RAID для защиты данных этого типа. Рекомендуемая конфигурация RAID: RAID-1 или RAID-1/0 (тем не менее, поддерживаются все типы RAID).

Отдельные тома для базы данных почтовых ящиков и для журналов

При развертывании автономной архитектуры роли сервера почтовых ящиков для базы данных почтовых ящиков и томов журналов требуется технология RAID. Рекомендуемая конфигурация RAID для томов почтовых ящиков — RAID-1/0 (особенно при использовании дисков 5,4 или 7,2 КБ); однако поддерживаются все типы RAID. Рекомендуемая конфигурация RAID для томов с журналами: RAID-1 или RAID-1/0.

При использовании конфигурации RAID-5 или RAID-6 для томов с ОС, файлами подкачки или данными Exchange, учитывайте на следующее:

- Конфигурации RAID-5, включая такие варианты, как RAID-50 и RAID-51, должны иметь не более семи дисков на группу массива и высокоприоритетную очистку контроллера массива и сканирование поверхности.
- В конфигурациях RAID-6 должны быть включены функции очистки высокой важности и сканирования поверхности контроллера массива.

Хотя JBOD поддерживается в архитектурах с высоким уровнем доступности с тремя или более высокодоступными копиями базы данных, так как тома базы данных журналов и почтовых ящиков разделены, JBOD не рекомендуется использовать в качестве решения.

Совместное расположение базы данных почтовых ящиков и журналов на одном томе

Совместное размещение базы данных почтовых ящиков и тома журнала не рекомендуется использовать в автономных архитектурах. В архитектуре высокой доступности этот сценарий можно реализовать двумя способами:

1. Одна база данных на том
2. Несколько баз данных на том

Одна база данных на том

В среде Exchange массив JBOD подразумевает хранение базы данных и связанных с ней журналов на одном диске. Чтобы развернуть массив JBOD, необходимо развернуть не менее трех высокодоступных копий базы данных. Использование одного диска является единственной точкой сбоя, так как при сбое диска копия базы данных, размещенная на этом диске, теряется. Наличие не менее трех копий базы данных обеспечивает отказоустойчивость за счет двух дополнительных копий в случае сбоя одной копии (или одного диска). Однако размещение трех высокодоступных копий базы данных и использование отстающего экземпляра базы данных могут повлиять на структуру хранилища. В следующей таблице приводятся указания по выбору технологии RAID или JBOD.

Рекомендации по RAID или JBOD:

Серверы центра обработки данных	**Две высокодоступных копии (всего)**	**Три высокодоступных копии (всего)**	**Две или более высокодоступных копии на каждый центр обработки данных**	**Одна изолированная копия**	**Две или более изолированные копии на каждый центр обработки данных**
Серверы основного центра обработки данных	RAID	RAID или JBOD (2 копии)	RAID или JBOD	RAID	RAID или JBOD
Серверы дополнительного центра обработки данных	RAID	RAID (1 копия)	RAID или JBOD	RAID	RAID или JBOD

Чтобы выполнить развертывание в массиве JBOD с серверами для основного центра обработки данных, необходимо иметь три или более высокодоступных копии базы данных в группе DAG. При смешивании изолированных копий на одном сервере с высокодоступными копиями базы данных (например, когда не используются выделенные серверы для изолированных копий базы данных), следует обеспечить наличие не менее двух изолированных копий базы данных.

Чтобы на серверах для дополнительного центра обработки данных можно было использовать массив JBOD, необходимо иметь не менее двух высокодоступных копий базы данных в дополнительном центре. Потеря копии в дополнительном центре не будет приводить к необходимости повторного заполнения по глобальной сети или возникновению единственной точки сбоя в случае активации дополнительного центра. При смешивании изолированных копий на одном сервере с высокодоступными копиями базы данных (например, когда не используются выделенные серверы для изолированных копий базы данных), следует обеспечить наличие не менее двух изолированных копий базы данных.

Для выделенных серверов с изолированными копиями базы данных необходимо наличие по меньшей мере двух изолированных копий в центре обработки данных, чтобы использовать массив JBOD. В противном случае потеря диска приводит к потере отстающего экземпляра базы данных и потере механизма защиты.

Несколько баз данных на том

Несколько баз данных на том — это новый сценарий JBOD, доступный в Exchange 2016, который позволяет смешивать активные и пассивные копии (включая отстающие копии) на одном диске, что обеспечивает более эффективное использование диска. Тем не менее, для развертывания изолированных копий в таких случаях необходимо включить автоматическое воспроизведение файла журнала

изолированной копии. В следующей таблице перечислены рекомендации для JBOD при размещении нескольких баз данных в одном томе.

Рекомендации по JBOD:

Серверы центра обработки данных	3 или более копий (всего)	Две или более копии на каждый центр обработки данных
Серверы основного центра обработки данных	JBOD	JBOD
Серверы дополнительного центра обработки данных	Недоступно	JBOD

В следующей таблице приведены указания по конфигурациям массива хранения для Exchange 2016.

Поддерживаемые типы RAID для роли сервера почтовых ящиков Exchange 2016:

Тип RAID	Описание	Поддержка и рекомендации
Размер полосы в массиве дисков RAID (КБ)	Размер полосы — это единица распределения данных в наборе RAID. Размер полосы также называется *размером блока*.	Рекомендация: 256 КБ или более. Следуйте рекомендациям поставщика запоминающего устройства.
Параметры кэша для массива хранения	Параметры кэширования предоставляются контроллером массива с кэшированием и резервным питанием от батарей.	Рекомендация: 100 % кэша записи (автономный или с записью во флэш-память) для контроллеров запоминающих устройств DAS в конфигурации RAID или JBOD. 75 % кэша записи и 25 % кэша чтения (автономный или с записью во флэш-память) для других типов систем хранения данных, например SAN. Если рекомендации поставщика SAN по настройке кэша на его платформе отличаются, следуйте им.
Кэширование записи на физический диск	Параметры кэша находятся на каждом отдельном диске.	Поддерживается: кэширование во время записи на физический диск при использовании без блока бесперебойного питания (UPS) должно быть отключено.

В следующей таблице приводятся различные варианты организации файлов базы данных и журналов.

Выбор файлов базы данных и журналов для роли сервера почтовых ящиков Exchange 2016:

Параметры файлов базы данных и журналов	Описание	Автономность: поддержка и рекомендации	Высокая доступность: поддержка и рекомендации
Размещение файлов: изоляция базы данных от журналов	Изоляция базы данных для каждого журнала — это размещение файла базы данных и журналов из одной базы данных почтового ящика в разных томах, поддерживаемых разными физическими дисками.	Рекомендация: для возможности восстановления переместите файл базы данных (EDB) и журналы из одной базы данных в различные тома на различных физических дисках.	Поддерживается: Изоляция журналов от баз данных не требуется.

Параметры файлов базы данных и журналов	Описание	Автономность: поддержка и рекомендации	Высокая доступность: поддержка и рекомендации
Размещение файлов: файлов базы данных на том	Файлы базы данных на том относятся к распределению файлов базы данных в пределах или между томами диска.	Рекомендация: в зависимости от используемого метода резервного копирования.	Поддерживается: При использовании JBOD создайте один том с отдельными каталогами для баз данных и файлов журнала.
Размещение файлов: потоков журналов на том	Потоки журналов на том относятся к распределению файлов журналов базы данных внутри или между томами диска.	Рекомендация: в зависимости от используемого метода резервного копирования.	Поддерживается: При использовании JBOD создайте один том с отдельными каталогами для баз данных и файлов журнала. Рекомендация. При использовании JBOD используйте несколько баз данных на том.
Размер базы данных	Этот параметр относится к размеру файла базы данных (EDB) на диске.	Поддерживается: приблизительно 16 ТБ. Рекомендация: • 200 гигабайт (ГБ) или меньше. • Подготовьте 120 % от рассчитанного максимального размера базы данных.	Поддерживается: приблизительно 16 ТБ. Рекомендация: • 2 ТБ или меньше. • Подготовьте 120 % от рассчитанного максимального размера базы данных.
Метод усечения журнала	Метод усечения журнала — это процесс усечения и удаления старых файлов журнала базы данных. Существует два механизма. • Циклическое ведение журнала, при котором на сервере Exchange удаляются журналы. • Усечение журнала, которое выполняется после успешного полного или добавочного резервного копирования с помощью службы теневого копирования томов (VSS).	Рекомендация: • Используйте резервные копии для усечения журнала (например, циклическое ведение журнала отключено). • Подготовьте место на диске для заполнения журнала на три дня.	Рекомендация: • Включите циклическое ведение журнала для развертываний, использующих собственные функции защиты данных Exchange. • Подготовьте место на диске для заполнения журнала на три дня сверх параметров запаздывания преобразования.

В следующей таблице приведены указания по типам дисков Windows.

Типы дисков Windows для роли сервера почтовых ящиков Exchange 2016:

Тип диска Windows	Описание	Автономность: поддержка и рекомендации	Высокая доступность: поддержка и рекомендации
Базовый диск	Диск, инициализированный для базового хранения данных, называется базовым. Базовый диск содержит базовые тома, такие как основные разделы, дополнительные разделы и логические диски.	Поддерживается. Рекомендация: используйте базовые диски.	Поддерживается. Рекомендация: используйте базовые диски.
Динамический диск	Диски, инициализированный для динамического хранения данных, называется динамическим. Динамический диск содержит динамические тома, такие как простые, составные, чередующиеся, зеркальные тома и тома RAID-5.	Поддерживается.	Поддерживается.

В приведенной ниже таблице содержатся указания по конфигурациям томов.

Конфигурации томов для роли сервера почтовых ящиков Exchange 2016:

Конфигурация тома	Описание	Автономность: поддержка и рекомендации	Высокая доступность: поддержка и рекомендации
Таблица разделов GUID (GPT)	GPT (GUID Partition Table) — это архитектура диска, которая является расширением более старой схемы разделения основной загрузочной записи (MBR). Максимальный размер раздела в формате NTFS — 256 ТБ.	Поддерживается. Рекомендация: используйте разделы GPT.	Поддерживается. Рекомендация: используйте разделы GPT.
MBR	MBR, или сектор раздела, — это загрузочный сектор размером 512 байт, который является первым сектором (Сектор LBA 0) разделенного устройства хранения данных, например жесткого диска. Максимальный размер раздела в формате NTFS — 2 ТБ.	Поддерживается.	Поддерживается.
Выравнивание разделов	Под выравниванием разделов понимается их расположение по границам секторов для обеспечения оптимальной производительности.	Поддерживается. В Windows Server 2008 R2 и Windows Server 2012 значение по умолчанию составляет 1 МБ.	Поддерживается. В Windows Server 2008 R2 и Windows Server 2012 значение по умолчанию составляет 1 МБ.
Путь к тому	Путь к тому определяет способ получения к нему доступа.	Поддерживается: буква диска или точка подключения. Рекомендация: в томе узла с точкой подключения должен быть включен массив RAID.	Поддерживается: буква диска или точка подключения. Рекомендация: в томе узла с точкой подключения должен быть включен массив RAID.
Файловая система	Файловая система — это метод хранения и организации файлов на компьютере и содержащихся в них данных для упрощения их поиска и доступа к ним.	Поддерживается: NTFS и ReFS.	Поддерживается: NTFS и ReFS.

Конфигурация тома	Описание	Автономность: поддержка и рекомендации	Высокая доступность: поддержка и рекомендации
Дефрагментация NTFS	Дефрагментация файловой системы NTFS — это процесс, который понижает степень фрагментации в файловых системах Windows. Это достигается путем физической организации содержимого диска и упорядочения частей каждого файла в единую и непрерывную последовательность.	Поддерживается. Рекомендация: не требуется и не рекомендуется. В Windows Server 2012 также рекомендуется отключить функцию автоматической оптимизации и дефрагментации дисков.	Поддерживается. Рекомендация: не требуется и не рекомендуется. В Windows Server 2012 также рекомендуется отключить функцию автоматической оптимизации и дефрагментации дисков.
Размер кластера NTFS	Размер кластера в файловой системе NTFS определяет минимальный объем дискового пространства, который может быть выделен для хранения файла.	Поддерживается: любой размер кластера. Рекомендация: по 64 КБ для томов с файлами EDB и журналами.	Поддерживается: любой размер кластера. Рекомендация: по 64 КБ для томов с файлами EDB и журналами.
Сжатие NTFS	Сжатие файлов NTFS — это процесс уменьшения фактического размера файлов, хранящихся на жестком диске.	Поддерживается: Не поддерживается для файлов базы данных и журнала Exchange.	Поддерживается: Не поддерживается для файлов базы данных и журнала Exchange.
Шифрующая файловая система (EFS) файловой системы NTFS	Система EFS позволяет пользователям шифровать отдельные файлы, папки или целые диски данных. Так как эта система обеспечивает надежное шифрование благодаря стандартным алгоритмам и шифрованию с открытым ключом, то конфиденциальность зашифрованных файлов сохраняется даже в том случае, если злоумышленник сможет взломать защиту системы.	Поддерживается: Не поддерживается для файлов базы данных и журнала Exchange.	Не поддерживается для файлов базы данных и журнала Exchange.

Конфигурация тома	Описание	Автономность: поддержка и рекомендации	Высокая доступность: поддержка и рекомендации
Windows BitLocker (шифрование тома)	Windows BitLocker — это функция защиты данных в системе Windows Server 2008. BitLocker позволяет предотвратить хищение или раскрытие данных, находившихся на потерянных или украденных компьютерах, и обеспечивает большую безопасность удаления данных с компьютеров при их списании.	Поддерживается: все файлы журнала и базы данных Exchange.	Поддерживается: все файлы журнала и базы данных Exchange. Для отказоустойчивых кластеров Windows требуется Windows Server 2008 R2 или Windows Server 2008 R2 с пакетом обновления 1 (SP1). Тома Exchange с включенным BitLocker не поддерживаются в отказоустойчивых кластерах Windows под управлением более ранних версий Windows. Дополнительные сведения о шифровании с помощью BitLocker в Windows 7 см. в статье Шифрование диска BitLocker в Windows 7: вопросы и ответы.
Server Message Block (SMB) 3.0	Протокол SMB — это сетевой протокол обмена файлами (поверх TCP/IP и других сетевых протоколов), позволяющий приложениям на компьютере получать доступ к файлам и ресурсам на удаленном сервере. Он также позволяет приложениям взаимодействовать с любой серверной программой, настроенной для приема клиентских запросов SMB. В Windows Server 2012 реализована новая версия протокола SMB 3.0 со следующими возможностями: • SMB Transparent failover; • SMB Scaleout; • SMB Multichannel; • SMB Direct; • SMB Encryption; • VSS для общих файловых ресурсов SMB; • SMB Directory Leasing; • SMB PowerShell.	Ограниченная поддержка. Поддерживаемый сценарий является виртуализированным развертыванием оборудования, в котором диски располагаются на виртуальных жестких дисках в общем ресурсе SMB 3.0. Эти виртуальные жесткие диски назначаются главному компьютеру через гипервизор. Дополнительные сведения см. в разделе Exchange Server виртуализации.	Ограниченная поддержка. Поддерживаемый сценарий является виртуализированным развертыванием оборудования, в котором диски располагаются на виртуальных жестких дисках в общем ресурсе SMB 3.0. Эти виртуальные жесткие диски назначаются главному компьютеру через гипервизор. Дополнительные сведения см. в разделе Exchange Server виртуализации.

Конфигурация тома	Описание	Автономность: поддержка и рекомендации	Высокая доступность: поддержка и рекомендации
Дисковые пространства	дисковые пространства — это новое решение для хранения данных, которое предоставляет возможности виртуализации для Windows Server 2012. дисковые пространства позволяет упорядочить физические диски в пулы носителей, которые можно легко расширить путем добавления дисков. Эти диски можно подключить через USB, SATA или SAS. Он также использует виртуальные диски (пробелы), которые ведут себя так же, как физические диски, со связанными мощными возможностями, такими как тонкая подготовка и устойчивость к сбоям базовых физических носителей. Дополнительные сведения о дисковые пространства см. в статье Обзор дисковые пространства.	Поддерживается. Те же ограничения, что и для типов физических дисков, описанных в этой статье.	Поддерживается. Те же ограничения, что и для типов физических дисков, описанных в этой статье.
Resilient File System (ReFS)	ReFS — это новая файловая система для Windows Server 2012, созданная на основе NTFS. ReFS поддерживает высокую степень совместимости с NTFS, обеспечивая расширенные методы проверки данных и автозамены, а также интегрированную комплексную устойчивость к повреждениям, особенно при использовании с функцией дисковых пространств. Дополнительные сведения о ReFS см. в статье Общие сведения об устойчивой файловой системе (ReFS): Поддерживаемые развертывания.	Поддерживается для томов, содержащих файлы базы данных Exchange, файлы журналов и файлы индексирования содержимого, если установлено следующее исправление: Exchange Server 2013 базы данных становятся фрагментированы в Windows Server 2012. Не поддерживается для томов, содержащих двоичные файлы Exchange. Рекомендация: отключите функции обеспечения целостности данных для файлов баз данных Exchange (EDB-файлы) или для тома, в котором они располагаются. Функции целостности можно включить для томов, содержащих каталог индексов содержимого, если том не содержит никаких баз данных или файлов журналов.	Поддерживается для томов, содержащих файлы базы данных Exchange, файлы журналов и файлы индексирования содержимого, если установлено следующее исправление: Exchange Server базы данных 2013 становятся фрагментами в Windows Server 2012. Не поддерживается для томов, содержащих двоичные файлы Exchange. Рекомендация: отключите функции обеспечения целостности данных для файлов баз данных Exchange (EDB-файлы) или для тома, в котором они располагаются. Функции целостности можно включить для томов, содержащих каталог индексов содержимого, если том не содержит никаких баз данных или файлов журналов.
Размер единицы выделения ReFS	Размер единицы выделения ReFS представляет наименьший объем дискового пространства, который можно выделить для хранения файла.	Поддерживается: любой размер кластера. Рекомендация: по 64 КБ для томов с файлами EDB и журналами.	Поддерживается: любой размер кластера. Рекомендация: по 64 КБ для томов с файлами EDB и журналами.

Конфигурация тома	Описание	Автономность: поддержка и рекомендации	Высокая доступность: поддержка и рекомендации
Дедупликация данных	Дедупликация данных — это метод оптимизации использования хранилища. Это метод поиска и удаления дублирования в данных без ущерба для их точности или целостности. Цель заключается в том, чтобы хранить больше данных в меньшем пространстве путем сегментирования файлов на небольшие блоки переменной величины, выявления повторяющихся фрагментов и поддержания одной копии каждого блока. Технологии дедупликации данных обычно реализуются одним из двух способов. на уровне операционной системы или на уровне системы хранения, и операционная система не знает, что она используется.	Уровень ОС: не поддерживается для баз данных почтовых ящиков Exchange, транспортных баз данных или файлов индексов содержимого. Уровень системы хранилища: поддерживается, но входит в политику поддержки сторонних решений для хранения данных Майкрософт. **Примечание.** Дедуп на уровне ОС можно использовать для файлов базы данных Exchange, которые находятся в автономном режиме (используются в качестве резервных копий или архивов).	Уровень ОС: не поддерживается для баз данных почтовых ящиков Exchange, транспортных баз данных или файлов индексов содержимого. Уровень хранилища. Поддерживается, но входит в политику поддержки сторонних решений для хранения данных Майкрософт. **Примечание.** Дедуп на уровне ОС можно использовать для файлов базы данных Exchange, которые находятся в автономном режиме (используются в качестве резервных копий или архивов).

Сетевые порты для клиентов и потока обработки почты в Exchange

Статья • 04.04.2023

В этом разделе содержатся сведения о сетевых портах, используемых Exchange Server 2016 и Exchange Server 2019 для связи с почтовыми клиентами, почтовыми серверами Интернета и другими службами, внешними для вашей локальной организации Exchange. Прежде чем начать, обдумайте следующие основные правила.

- Мы не поддерживаем ограничение или изменение сетевого трафика между внутренними серверами Exchange, между внутренними серверами Exchange и внешними серверами Lync либо Skype для бизнеса или между внутренними серверами Exchange и внутренними контроллерами домена Active Directory в любых типах топологии. Если у вас есть брандмауэры или сетевые устройства, которые могут потенциально ограничить или изменить этот тип внутреннего сетевого трафика, необходимо настроить правила, разрешающие бесплатный и неограниченный обмен данными между этими серверами: правила, разрешающие входящий и исходящий сетевой трафик на любом порту (включая случайные порты RPC), и любой протокол, который никогда не изменяет биты в проводе.

- Пограничные транспортные серверы почти всегда расположены в сети периметра, поэтому ожидается, что вы ограничите сетевой трафик между пограничным транспортным сервером и Интернетом, а также между пограничным транспортным сервером и внутренней организацией Exchange. Эти сетевые порты описаны в данном разделе.

- Ожидается, что вы ограничите сетевой трафик между внешними клиентами и службами и внутренней организацией Exchange. Также можно ограничить трафик между внутренними клиентами и внутренними серверами Exchange. Эти сетевые порты описаны в данном разделе.

Сетевые порты, необходимые для клиентов и служб

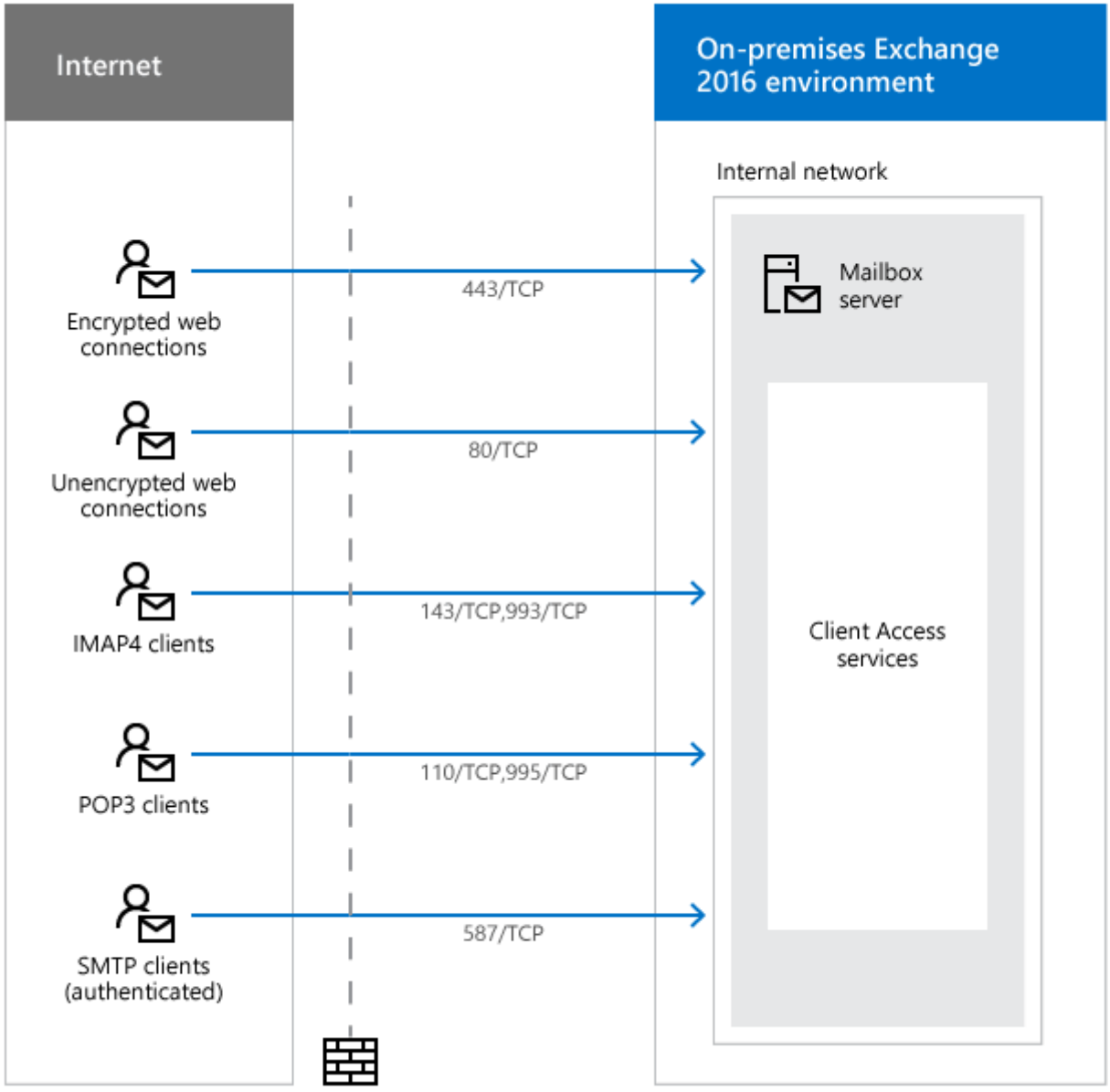
Сетевые порты, которые необходимы почтовым клиентам для доступа к почтовым ящикам и другим службам в организации Exchange, описаны на следующей диаграмме и в таблице.

Примечания:

- Назначением для этих клиентов и служб являются службы клиентского доступа на сервере почтовых ящиков. В Exchange 2016 и Exchange 2019 клиентский доступ (интерфейсная) и серверная службы устанавливаются вместе на одном сервере почтовых ящиков. Дополнительные сведения см. в статье Архитектура протокола клиентского доступа.

- Хотя на схеме показаны клиенты и службы из Интернета, понятия одинаковы для внутренних клиентов (например, клиенты в лесу учетных записей обращаются к серверам Exchange в лесу ресурсов). Аналогичным образом в таблице нет исходного столбца, так как источником может быть любое расположение, которое находится вне организации Exchange (например, Интернет или лес учетных записей).

- Пограничные транспортные серверы не участвуют в сетевом трафике, связанном с этими клиентами и службами.



Назначение	Порты	Comments

Назначение	Порты	Comments
Зашифрованные веб-подключения используются следующими клиентами и службами. • Служба автообнаружения • Exchange ActiveSync • Веб-службы Exchange (EWS) • Распространение автономных адресных книг • Мобильный Outlook (протокол RPC через HTTP) • MAPI Outlook через HTTP • Outlook в Интернете (прежнее название — Outlook Web App)	443/TCP (HTTPS)	Дополнительные сведения об этих клиентах и службах см. в следующих статьях. • Служба автообнаружения в Exchange Server • Exchange ActiveSync • Справка по службам EWS для Exchange • Автономные адресные книги в Exchange Server • Outlook Anywhere • MAPI через HTTP в Exchange Server
Незашифрованные веб-подключения используются следующими клиентами и службами. • Публикация календаря в Интернете • Outlook в Интернете (перенаправление на 443/TCP) • Автообнаружение (откат, когда порт 443/TCP недоступен)	80/TCP (HTTP)	По возможности рекомендуется использовать зашифрованное веб-подключения на TCP-порте 443 для защиты учетных и других данных. Однако вы можете обнаружить, что некоторые службы должны быть настроены для использования незашифрованных веб-подключений по протоколу 80/TCP к службам клиентского доступа на серверах почтовых ящиков. Дополнительные сведения об этих клиентах и службах см. в следующих статьях. • Enable Internet Calendar Publishing • Служба автообнаружения в Exchange Server

Назначение	Порты	Comments
Клиенты IMAP4	143/TCP (IMAP), 993/TCP (безопасный IMAP)	По умолчанию IMAP4 отключен. Дополнительные сведения см. в разделе POP3 и IMAP4 в Exchange Server. Служба IMAP4 в службах клиентского доступа на сервере почтовых ящиков прокси-сервер выполняет подключения к серверной службе IMAP4 на сервере почтовых ящиков.
Клиенты POP3	110/TCP (POP3), 995/TCP (безопасный POP3)	По умолчанию протокол POP3 отключен. Дополнительные сведения см. в разделе POP3 и IMAP4 в Exchange Server. Служба POP3 в службах клиентского доступа на сервере почтовых ящиков выполняет подключения к серверной службе POP3 на сервере почтовых ящиков.
Клиенты SMTP (с проверкой подлинности)	587/TCP (SMTP с проверкой подлинности)	По умолчанию соединитель Received с именем "*Имя> внешнего< сервера* клиента" в транспортной службе переднего плана прослушивает отправку клиента SMTP с проверкой подлинности через порт 587. **Примечание.** Если у вас есть почтовые клиенты, которые могут отправлять только почту SMTP с проверкой подлинности через порт 25, вы можете изменить привязки сетевого адаптера соединителя получения клиента, чтобы также прослушивать отправку почты SMTP с проверкой подлинности через порт 25.

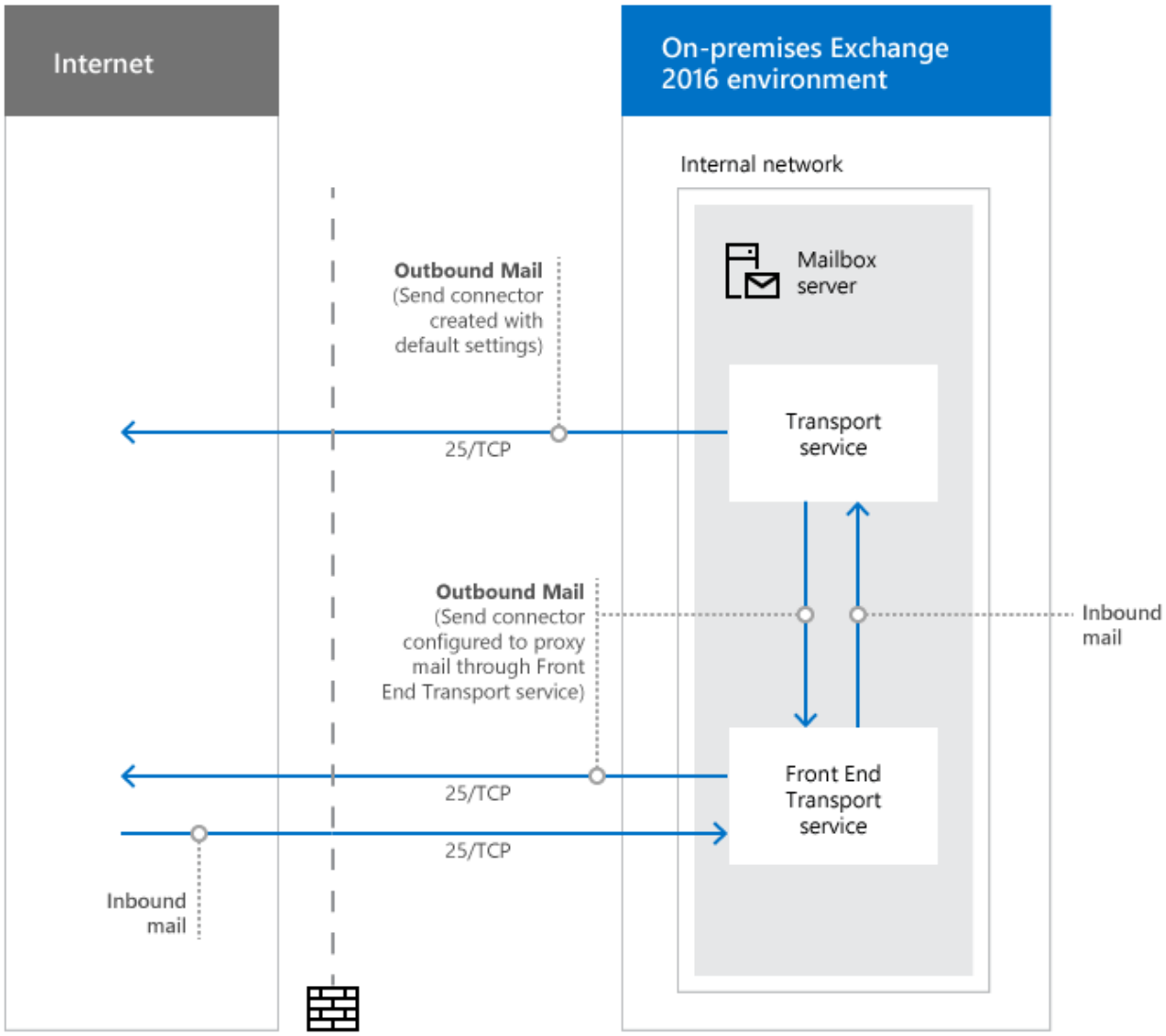
Сетевые порты, необходимые для потока обработки почты

Способ доставки почты в организацию Exchange и из нее зависит от топологии Exchange. Наиболее важный фактор — наличие подписанного пограничного транспортного сервера, развернутого в сети периметра.

Сетевые порты, необходимые для потока обработки почты (без пограничных транспортных серверов)

Сетевые порты, необходимые для потока обработки почты в организации Exchange, которая имеет только серверы почтовых ящиков, описаны на следующей

схеме и в таблице.



Назначение	Порты	Source	Назначение	Comments

Назначение	Порты	Source	Назначение	Comments
Входящая почта	25/TCP (SMTP)	Интернет (все)	Сервер почтовых ящиков	Соединитель получения по умолчанию с именем "*Имя> сервера внешних< почтовых ящиков* по умолчанию" в транспортной службе переднего плана прослушивает анонимную входящую smtp-почту через порт 25. Почта передается из транспортной службы переднего плана в транспортную службу на сервере почтовых ящиков с помощью неявного и невидимого соединителя отправки внутри организации, который автоматически маршрутизирует почту между серверами Exchange в той же организации. Дополнительные сведения см. в разделе Соединители неявной отправки.
Исходящая почта	25/TCP (SMTP)	Сервер почтовых ящиков	Интернет (все)	По умолчанию Exchange не создает соединители отправки, которые позволяют отправлять почту в Интернет. Необходимо создать соединители отправки вручную. Дополнительные сведения см. в статье Создание соединителя отправки для отправки почты в Интернет.

Назначение	Порты	Source	Назначение	Comments
Исходящая почта (при наличии прокси-сервера через транспортную службу переднего плана)	25/TCP (SMTP)	Сервер почтовых ящиков	Интернет (все)	Исходящая почта передается через транспортную службу переднего плана только в том случае, если для соединителя отправки настроен **прокси-сервер через сервер клиентского доступа** в Центре администрирования Exchange или `-FrontEndProxyEnabled $true` в командной консоли Exchange. В этом случае соединитель получения по умолчанию с именем "*Имя> сервера внешнего< почтового ящика* исходящего прокси-сервера" в транспортной службе переднего плана прослушивает исходящую почту от транспортной службы на сервере почтовых ящиков. Дополнительные сведения см. в статье Configure Send connectors to proxy outbound mail.
DNS-сервер для разрешения имен следующего перехода почты (не показан на рисунке)	53/UDP, 53/TCP (DNS)	Сервер почтовых ящиков	DNS-сервер	См. раздел Разрешение имен в этой статье.

Сетевые порты, необходимые для потока обработки почты с пограничными транспортными серверами

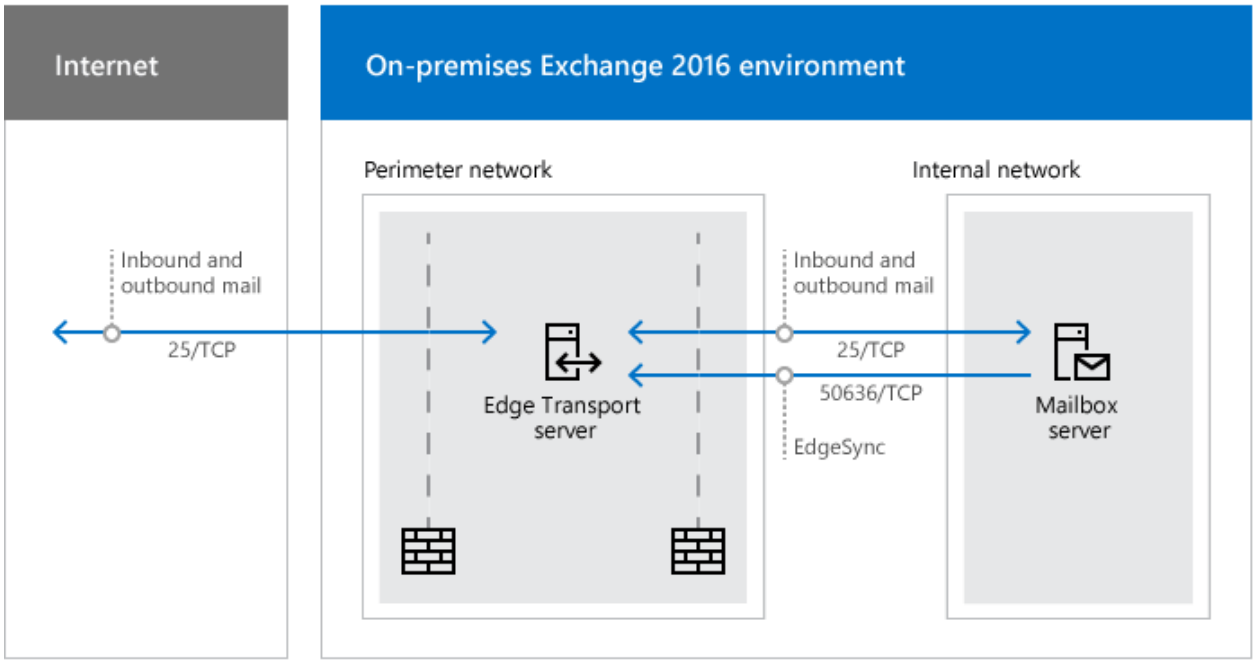
Подписанный пограничный транспортный сервер, установленный в сети периметра, влияет на поток обработки почты следующими способами:

- Исходящая почта из организации Exchange никогда не проходит через интерфейсную транспортную службу на серверах почтовых ящиков. Почта всегда передается из транспортной службы на сервере почтовых ящиков на сайте Active Directory с подпиской на пограничный транспортный сервер (независимо от версии Exchange на пограничном транспортном сервере).

- Входящая почта передается с пограничного транспортного сервера на сервер почтовых ящиков на сайте Active Directory с подпиской. Это означает следующее:
    - Почта с пограничного транспортного сервера Exchange 2013 или более поздней версии сначала поступает в транспортную службу переднего плана, прежде чем она будет отправлена в транспортную службу на сервере почтовых ящиков Exchange 2016 или Exchange 2019.
    - В Exchange 2016 почта с пограничного транспортного сервера Exchange 2010 всегда доставляет почту непосредственно в транспортную службу на сервере почтовых ящиков Exchange 2016. Обратите внимание, что сосуществование с Exchange 2010 не поддерживается в Exchange 2019.

Дополнительные сведения см. в разделе Поток обработки почты и конвейер транспорта.

Сетевые порты, необходимые для потока обработки почты в организациях Exchange с пограничными транспортными серверами, описаны на следующей диаграмме и в таблице.



Назначение	Порты	Source	Назначение	Comments

Назначение	Порты	Source	Назначение	Comments
Входящая почта — из Интернета на пограничный транспортный сервер	25/TCP (SMTP)	Интернет (все)	Пограничный транспортный сервер	Соединитель получения по умолчанию с именем "*Имя> пограничного транспортного сервера внутреннего соединителя<* получения по умолчанию" на пограничном транспортном сервере прослушивает анонимную почту SMTP через порт 25.
Входящая почта — от пограничного транспортного сервера во внутреннюю организацию Exchange	25/TCP (SMTP)	Пограничный транспортный сервер	Серверы почтовых ящиков на подписанном сайте Active Directory	Соединитель отправки по умолчанию с именем "EdgeSync — inbound to *<Active Directory site name>*" ретранслирует входящую почту через порт 25 на любой сервер почтовых ящиков на сайте Active Directory с подпиской. Дополнительные сведения см. в статье Отправка соединителей, автоматически созданных подпиской Edge. Соединитель получения по умолчанию с именем "*Имя> сервера внешнего< почтового ящика* по умолчанию" в транспортной службе переднего плана на сервере почтовых ящиков прослушивает всю входящую почту (включая почту с пограничных транспортных серверов Exchange 2013 или более поздних версий) через порт 25.

Назначение	Порты	Source	Назначение	Comments
Исходящая почта — от внутренней организации Exchange на пограничный транспортный сервера	25/TCP (SMTP)	Серверы почтовых ящиков на подписанном сайте Active Directory	Пограничные транспортные серверы	Исходящая почта всегда обходит службу транспорта переднего плана на серверах почтовых ящиков. Почта ретранслируется из транспортной службы на любом сервере почтовых ящиков на сайте Active Directory с подпиской на пограничный транспортный сервер с помощью неявного и невидимого соединителя отправки внутри организации, который автоматически направляет почту между серверами Exchange в той же организации. Соединитель получения по умолчанию с именем "*Имя> пограничного транспортного сервера внутреннего соединителя<* получения по умолчанию" на пограничном транспортном сервере прослушивает smtp-почту через порт 25 от транспортной службы на любом сервере почтовых ящиков на сайте Active Directory с подпиской.

Назначение	Порты	Source	Назначение	Comments
Исходящая почта — пограничный транспортный сервер в Интернет	25/TCP (SMTP)	Пограничный транспортный сервер	Интернет (все)	Соединитель отправки по умолчанию с именем "EdgeSync — *<имя сайта Active Directory>* в Интернет" ретранслирует исходящую почту через порт 25 с пограничного транспортного сервера в Интернет.
Синхронизация EdgeSync	50636/TCP (безопасный LDAP)	Серверы почтовых ящиков на подписанном сайте Active Directory, которые участвуют в синхронизации EdgeSync	Пограничные транспортные серверы	Когда пограничный транспортный сервер подписан на сайт Active Directory, в синхронизации EdgeSync участвуют все серверы почтовых ящиков, существующие *на* этом сайте. Однако все серверы почтовых ящиков, которые вы добавите позже , *автоматически не* участвуют в синхронизации EdgeSync.
DNS-сервер для разрешения имен следующего перехода почты (не показан на рисунке)	53/UDP, 53/TCP (DNS)	Пограничный транспортный сервер	DNS-сервер	См. раздел Разрешение имен далее в этом разделе.
Обнаружение открытого прокси-сервера в репутации отправителя (не на фото)	см. примечания	Пограничный транспортный сервер	Интернет	По умолчанию репутация отправителя (агент анализа протоколов) использует обнаружение открытого прокси-сервера в качестве одного из критериев для вычисления уровня репутации отправителя (SRL) исходного сервера обмена сообщениями.

Назначение	Порты	Source	Назначение	Comments
				Дополнительные сведения см. в разделе Sender reputation and the Protocol Analysis agent. Обнаружение открытого прокси-сервера использует следующие протоколы и TCP-порты для тестирования исходных серверов обмена сообщениями для открытого прокси-сервера: • SOCKS4, SOCKS5: 1081, 1080 • Wingate, Telnet, Cisco: 23 • HTTP CONNECT, HTTP POST: 6588, 3128, 80 Кроме того, если ваша организация использует прокси-сервер для управления исходящим интернет-трафиком, необходимо определить имя прокси-сервера, тип и TCP-порт, который требуется репутации отправителя для доступа к Интернету для обнаружения открытого прокси-сервера. Кроме того, можно отключить обнаружение открытого прокси-сервера в репутации отправителя. Дополнительные сведения см. в разделе Процедуры репутации отправителя.

Разрешение имен

Разрешение DNS следующего перехода почты является фундаментальной составляющей потока обработки почты в любой организации Exchange. Серверы Exchange, ответственные за получение входящей почты или доставку исходящей, должны иметь возможность разрешать как внутренние, так и внешние имена узлов для правильной маршрутизации почты. Все внутренние серверы Exchange должны иметь возможность разрешать внутренние имена узлов для правильной маршрутизации почты. Существует множество различных способов разработки инфраструктуры DNS, но важный результат — обеспечение правильного разрешения имен для следующего перехода на всех серверах Exchange.

Сетевые порты, необходимые для гибридных развертываний

Сетевые порты, необходимые для организации, которая использует как локальный Exchange, так и Microsoft 365 или Office 365, рассматриваются в статье Протоколы гибридного развертывания, порты и конечные точки.

Сетевые порты, необходимые для единой системы обмена сообщениями в Exchange 2016

Сетевые порты, необходимые для единой системы обмена сообщениями в Exchange 2013 и Exchange 2016, рассматриваются в разделе Протоколы, порты и службы единой системы обмена сообщениями.

Общие сведения о службах Exchange на серверах Exchange

Статья • 04.04.2023

Во время установки Exchange Server 2016 или Exchange Server 2019 программа установки выполняет набор задач, устанавливающих новые службы в Microsoft Windows. Служба — это фоновый процесс, который диспетчер служб Windows может запускать при запуске сервера. Службы — это исполняемые файлы, предназначенные для независимой работы без вмешательства администраторов. Служба может работать в режиме графического пользовательского интерфейса (GUI) или консоли.

Все предыдущие версии Exchange включали компоненты, реализуемые в виде служб. Каждая роль сервера Exchange Server включает службы, которые входят в состав роли сервера (или могут быть ей необходимы), для выполнения своих функций. Обратите внимание, что некоторые службы становятся активны только при использовании определенных функций.

В разделах этого раздела описываются различные службы, установленные Exchange 2016 и Exchange 2016 на серверах почтовых ящиков и пограничных транспортных серверах. Для служб, отмеченных как необязательные, можно отключить службу, если окажется, что вашей организации не требуются предоставляемые ею функции.

Службы Exchange на серверах почтовых ящиков

В приведенной ниже таблице описываются службы Exchange, устанавливаемые на серверах почтовых ящиков.

Имя службы	Короткое имя службы	Описание и зависимости	Тип запуска по умолчанию	Контекст безопасности	Зависимости	Обязательная или необязательна
Microsoft Exchange Топология Active Directory	MSExchangeADTopology	Предоставляет сведения о топологии Active Directory для служб Exchange. Если работа этой службы будет остановлена, большинство служб Exchange не смогут запускаться.	Автоматическая	Локальная система	Служба совместного доступа к портам Net.TCP	Обязательная
Обновление средства защиты от нежелательной почты Microsoft Exchange	MSExchangeAntispamUpdate	Предоставляет обновления определений спама для Exchange SmartScreen. **Примечание.** В ноябре 2016 г. корпорация Майкрософт прекратила выпуск обновлений определений спама для фильтров SmartScreen в Exchange и Outlook. Существующие определения спама SmartScreen остались на месте, но их эффективность, скорее всего, со временем снизится. Дополнительные сведения см. в статье Прекращение поддержки SmartScreen в Outlook и Exchange.	Автоматически	Локальная система	Служба топологии Active DirectoryMicrosoft Exchange	Необязательная
Аудит соответствия требованиям Microsoft Exchange	MSComplianceAudit	Предоставляет функции аудита Exchange.	Автоматически	Локальная система	Служба топологии Active DirectoryMicrosoft Exchange	Обязательная

Имя службы	Короткое имя службы	Описание и зависимости	Тип запуска по умолчанию	Контекст безопасности	Зависимости	Обязательная или необязательна
Служба соответствия требованиям Microsoft Exchange	MSExchangeCompliance	Предоставляет узел для служб соответствия требованиям Exchange.	Автоматически	Локальная система	Служба топологии Active DirectoryMicrosoft Exchange	Обязательная
Служба управления DAG Microsoft Exchange	MSExchangeDagMgmt	Предоставляет возможности управления структурами хранилищ и макетами баз данных для серверов почтовых ящиков в группах обеспечения доступности баз данных.	Автоматически	Локальная система	Microsoft Exchange Active Directory TopologyNet.TCP Port Sharing Service	Обязательный
Служба диагностики Microsoft Exchange	MSExchangeDiagnostics	Предоставляет агент, отслеживающий работоспособность сервера Exchange Server.	Автоматически	Локальная система	Нет	Обязательная
Microsoft Exchange EdgeSync	MSExchangeEdgeSync	Реплицирует данные о конфигурации и получателях, передавая их с сервера почтовых ящиков в службы Active Directory облегченного доступа к каталогам (AD LDS) на подписанных пограничных транспортных серверах по защищенному каналу LDAP, а также наоборот. Если у вас нет подписанных пограничных транспортных серверов, можете отключить эту службу.	Автоматически	Локальная система	Служба топологии Active DirectoryMicrosoft Exchange	Необязательный
Устранение последствий чрезвычайных ситуаций в Microsoft Exchange	Устранение рисков MSExchange	Автоматически применяет важные меры по устранению рисков на Exchange Server для защиты от известных угроз.	Автоматически	Локальная система	Модуль перезаписи URL-адресов IIS	Обязательный
Интерфейсная служба транспорта Microsoft Exchange	MSExchangeFrontEndTransport	Прокси-подключения SMTP от внешних узлов к транспортной службе Microsoft Exchange на серверах почтовых ящиков (локальных или удаленных серверах).	Автоматически	Локальная система	Служба топологии Active DirectoryMicrosoft Exchange	Обязательная

Имя службы	Короткое имя службы	Описание и зависимости	Тип запуска по умолчанию	Контекст безопасности	Зависимости	Обязательная или необязательна
Диспетчер работоспособности Microsoft Exchange	MSExchangeHM	Часть службы управляемой доступности, отслеживающая работоспособность ключевых компонентов на сервере Exchange Server.	Автоматически	Локальная система	Журнал событий WindowsИнструментарий управления Windows (WMI)	Обязательная
Служба восстановления диспетчера работоспособности Microsoft Exchange	MSExchangeHMRecovery	Часть службы управляемой доступности, которая пытается восстановить неработоспособные компоненты на сервере Exchange Server.	Автоматически	Локальная система	• Журнал событий Windows • Инструментарий управления Windows (WMI)	Обязательная
Microsoft Exchange IMAP4	MSExchangeIMAP4	Проксирует клиентские подключения IMAP4 служб клиентского доступа (интерфейсных) к фоновой службе IMAP4 на серверах почтовых ящиков. По умолчанию эта служба не работает, поэтому клиенты IMAP4 не смогут подключаться к серверу Exchange Server, пока она не будет запущена. Если у вас нет клиентов IMAP4, можете отключить эту службу.	Вручную	Локальная система	Служба топологии Active DirectoryMicrosoft Exchange	Необязательная
Внутренняя служба IMAP4 Microsoft Exchange	MSExchangeIMAP4BE	Получает проксированные клиентские подключения IMAP4 от службы клиентского доступа IMAP4 (интерфейсной). По умолчанию эта служба не работает, поэтому клиенты IMAP4 не смогут подключаться к серверу Exchange Server, пока она не будет запущена. Если у вас нет клиентов IMAP4, можете отключить эту службу.	Вручную	Сетевая служба	Служба топологии Active DirectoryMicrosoft Exchange	Необязательная

Имя службы	Короткое имя службы	Описание и зависимости	Тип запуска по умолчанию	Контекст безопасности	Зависимости	Обязательная или необязательна
Банк данных Microsoft Exchange	Msexchangeis	Управляет базами данных почтовых ящиков на сервере. Если эта служба остановлена, базы данных почтовых ящиков на сервере недоступны.	Автоматически	Локальная система	• Служба топологии Active DirectoryMicrosoft Exchange • Удаленный вызов процедур (RPC) • Сервер • Журнал событий Windows • Рабочая станция	Обязательная
Помощники по обслуживанию почтовых ящиков Microsoft Exchange	MSExchangeMailboxAssistants	Выполняет фоновую обработку почтовых ящиков в соответствующих базах данных на сервере.	Автоматически	Локальная система	Служба топологии Active DirectoryMicrosoft Exchange	Обязательная
Служба репликации почтовых ящиков Microsoft Exchange	MSExchangeMailboxReplication	Обрабатывает операции перемещения и запросы на перемещение почтовых ящиков.	Автоматически	Локальная система	Microsoft Exchange Active Directory TopologyNet.TCP Port Sharing Service	Обязательная
Служба доставки транспорта почтовых ящиков Microsoft Exchange	MSExchangeDelivery	Получает сообщения SMTP от службы транспорта Microsoft Exchange (на локальных или удаленных серверах почтовых ящиков) и доставляет их в локальную базу данных почтовых ящиков с помощью RPC.	Автоматически	Сетевая служба	Служба топологии Active DirectoryMicrosoft Exchange	Обязательная
Служба отправки транспорта почтовых ящиков Microsoft Exchange	MSExchangeSubmission	Получает сообщения RPC из локальной базы данных почтовых ящиков и отправляет их по протоколу SMTP в службу транспорта Microsoft Exchange (на локальных или удаленных серверах почтовых ящиков).	Автоматически	Локальная система	Служба топологии Active DirectoryMicrosoft Exchange	Обязательный
Брокер уведомлений Microsoft Exchange (только Exchange 2016)	MSExchangeNotificationsBroker	Предоставляет уведомления Exchange локальным и удаленным процессам Exchange.	Автоматически	Локальная система	• Служба топологии Active DirectoryMicrosoft Exchange • Служба совместного доступа к портам Net.TCP	Обязательная

Имя службы	Короткое имя службы	Описание и зависимости	Тип запуска по умолчанию	Контекст безопасности	Зависимости	Обязательная или необязательна
Microsoft Exchange POP3	MSExchangePOP3	Проксирует клиентские подключения POP3 служб клиентского доступа (интерфейсных) к фоновой службе IMAP4 на серверах почтовых ящиков. По умолчанию эта служба не работает, поэтому клиенты POP3 не смогут подключаться к серверу Exchange Server, пока она не будет запущена.	Вручную	Сетевая служба	Служба топологии Active DirectoryMicrosoft Exchange	Необязательная
Внутренняя служба POP3 Microsoft Exchange	MSExchangePOP3BE	Получает проксированные клиентские подключения POP3 от службы клиентского доступа POP3 (интерфейсной). По умолчанию эта служба не работает, поэтому клиенты POP3 не смогут подключаться к серверу Exchange Server, пока она не будет запущена.	Вручную	Сетевая служба	Служба топологии Active DirectoryMicrosoft Exchange	Необязательная
Служба репликации Microsoft Exchange	MSExchangeRepl	Обеспечивает репликацию баз данных почтовых ящиков в группах обеспечения доступности баз данных.	Автоматически	Локальная система	Служба топологии Active DirectoryMicrosoft Exchange	Обязательная
Клиентский доступ RPC Microsoft Exchange	MSExchangeRPC	Управляет клиентскими подключениями RPC для Exchange.	Автоматически	Сетевая служба	Служба топологии Active DirectoryMicrosoft Exchange	Обязательная
Служба поиска Microsoft Exchange	MSExchangeFastSearch	Обеспечивает индексацию содержимого почтовых ящиков, которая повышает скорость поиска содержимого.	Автоматически	Локальная система	Служба топологии Active DirectoryMicrosoft Exchange	Обязательная
Хост-контроллер поиска Microsoft Exchange	HostControllerService	Предоставляет службы развертывания и управления для приложений на локальном сервере Exchange Server.	Автоматически	Локальная система	HTTP-служба	Обязательная

Имя службы	Короткое имя службы	Описание и зависимости	Тип запуска по умолчанию	Контекст безопасности	Зависимости	Обязательная или необязательна
Расширение сервера Microsoft Exchange для системы архивации данных Windows Server	WSBExchange	Позволяет службе резервного копирования Windows Server копировать и восстанавливать данные сервера Exchange Server.	Вручную	Локальная система	Нет	Необязательная
Microsoft Exchange Service Host	MSExchangeServiceHost	Предоставляет узел службы для компонентов Exchange, у которых нет собственных служб.	Автоматически	Локальная система	Служба топологии Active DirectoryMicrosoft Exchange	Обязательная
Регулирование Microsoft Exchange	MSExchangeThrottling	Предоставляет возможность управления рабочими нагрузками пользователей. Такое управление ограничивает частоту пользовательских операций, оно ранее называлось регулированием пользователей.	Автоматически	Сетевая служба	Служба топологии Active DirectoryMicrosoft Exchange	Обязательная
Транспорт Microsoft Exchange	MSExchangeTransport	Предоставляет SMTP-сервер и транспортный стек.	Автоматически	Сетевая служба	• Служба топологии Active DirectoryMicrosoft Exchange • Служба управления фильтрацией Майкрософт	Обязательная
Поиск журналов транспорта Microsoft Exchange	MSExchangeTransportLogSearch	Предоставляет возможность удаленного поиска для файлов журналов транспорта (например, отслеживание сообщений).	Автоматически	Локальная система	Служба топологии Active DirectoryMicrosoft Exchange	Необязательный

Имя службы	Короткое имя службы	Описание и зависимости	Тип запуска по умолчанию	Контекст безопасности	Зависимости	Обязательная или необязательна
Единая система обмена сообщениями Microsoft Exchange (только Exchange 2016)	MSExchangeUM	Предоставляет функции единой системы обмена сообщениями(UM): позволяет хранить голосовые и факсимильные сообщения в Exchange 2016 и предоставляет пользователям доступ по телефону к электронной почте, голосовой почте, календарю, контактам или автосекретарю. Если служба остановлена, единая система обмена сообщениями недоступна. Если вы не используете UM в Exchange 2016, эту службу можно отключить.	Автоматически	Локальная система	• Изоляция ключей CNG • Служба топологии Active DirectoryMicrosoft Exchange	Необязательный
Маршрутизатор вызовов единой системы обмена сообщениями Microsoft Exchange (только Exchange 2016)	MSExchangeUMCR	Перенаправляет клиентские подключения единой системы обмена сообщениями из служб клиентского доступа (внешний интерфейс) в серверную службу единой системы обмена сообщениями на серверах почтовых ящиков Exchange 2016. Если вы не используете UM в Exchange 2016, эту службу можно отключить.	Автоматически	Локальная система	• Изоляция ключей CNG • Служба топологии Active DirectoryMicrosoft Exchange	Необязательный

Службы Exchange на пограничных транспортных серверах

В приведенной ниже таблице описываются службы Exchange, устанавливаемые на пограничных транспортных серверах.

Имя службы	Короткое имя службы	Описание	Тип запуска по умолчанию	Контекст безопасности	Зависимости	Обязательная или необязательная

Имя службы	Короткое имя службы	Описание	Тип запуска по умолчанию	Контекст безопасности	Зависимости	Обязательная или необязательная
Microsoft Exchange ADAM	ADAM_MSExchange	Хранит сведения о конфигурации и получателях на пограничном транспортном сервере. Эта служба представляет именованный экземпляр служб Active Directory облегченного доступа к каталогам (AD LDS), автоматически создаваемый программой установки Exchange.	Автоматически	Сетевая служба	Система событий COM+	Обязательная
Обновление средства защиты от нежелательной почты Microsoft Exchange	MSExchangeAntispamUpdate	Предоставляет обновления определений спама для Exchange SmartScreen. **Примечание.** В ноябре 2016 г. корпорация Майкрософт прекратила выпуск обновлений определений спама для фильтров SmartScreen в Exchange и Outlook. Существующие определения спама SmartScreen остались на месте, но их эффективность, скорее всего, со временем снизится. Дополнительные сведения см. в статье Прекращение поддержки SmartScreen в Outlook и Exchange.	Автоматически	Локальная система	Microsoft Exchange ADAM	Необязательная
Служба учетных данных Microsoft Exchange	MSExchangeEdgeCredential	Отслеживает изменения учетных данных в службах Active Directory облегченного доступа к каталогам (AD LDS) и применяет изменения на пограничном транспортном сервере.	Автоматически	Локальная система	Microsoft Exchange ADAM	Обязательная
Служба диагностики Microsoft Exchange	MSExchangeDiagnostics	Предоставляет агент, отслеживающий работоспособность сервера Exchange Server.	Автоматически	Локальная система	Нет	Обязательная

Имя службы	Короткое имя службы	Описание	Тип запуска по умолчанию	Контекст безопасности	Зависимости	Обязательная или необязательная
Диспетчер работоспособности Microsoft Exchange	MSExchangeHM	Часть службы управляемой доступности, отслеживающая работоспособность ключевых компонентов на сервере Exchange Server.	Автоматически	Локальная система	• Журнал событий Windows • Инструментарий управления Windows (WMI)	Обязательная
Служба восстановления диспетчера работоспособности Microsoft Exchange	MSExchangeHMRecovery	Часть службы управляемой доступности, которая пытается восстановить неработоспособные компоненты на сервере Exchange Server.	Автоматически	Локальная система	Журнал событий WindowsИнструментарий управления Windows (WMI)	Обязательная
Microsoft Exchange Service Host	MSExchangeServiceHost	Предоставляет узел службы для компонентов Exchange, у которых нет собственных служб.	Автоматически	Локальная система	Microsoft Exchange ADAM	Обязательная
Транспорт Microsoft Exchange	MSExchangeTransport	Предоставляет SMTP-сервер и транспортный стек.	Автоматически	Сетевая служба	Microsoft Exchange ADAM	Обязательная
Поиск журналов транспорта Microsoft Exchange	MSExchangeTransportLogSearch	Предоставляет возможность удаленного поиска для файлов журналов транспорта (например, отслеживание сообщений).	Автоматически	Локальная система	Microsoft Exchange ADAM	Необязательная

Предпочтительная архитектура Exchange 2019

Статья • 04.04.2023

С каждым новым выпуском Exchange Server для наших локальных клиентов мы обновляем предпочитаемую архитектуру и обсуждаем, какие изменения мы хотели бы знать нашим клиентам. Exchange Server 2013 году принес нам первую из предпочитаемых архитектур в современной истории Exchange, а затем обновление для Exchange Server 2016 года, предоставив уточнение изменений, внесенных в выпуск 2016 года. В этом обновлении за Exchange Server 2019 г. мы рассмотрим предыдущий paererr, чтобы воспользоваться преимуществами новых технологий и улучшений.

Предпочтительная архитектура

Pa — это рекомендация команды инженеров Exchange Server, которая, по нашему мнению, является лучшей архитектурой развертывания для Exchange Server 2019 в локальной среде.

Хотя Exchange 2019 предлагает широкий выбор архитектуры для локальных развертываний, рассмотренная здесь архитектура является наиболее тщательной. Хотя существуют и другие поддерживаемые архитектуры развертывания, они не являются рекомендуемой практикой.

После этого клиент становится членом сообщества организаций со схожими Exchange Server развертываниями. Эта стратегия упрощает обмен знаниями и обеспечивает более быстрое реагирование на непредвиденные обстоятельства. Наша организация поддержки знает, как должно выглядеть развертывание Exchange Server PA, и не позволяет им тратить длительные циклы обучения и понимания строго настраиваемой среды клиента, прежде чем работать с ними над решением обращения в службу поддержки.

Pa разработан с учетом нескольких бизнес-требований, таких как требование, чтобы архитектура могла:

- Включите как высокий уровень доступности в центре обработки данных, так и устойчивость сайта между центрами обработки данных.
- Поддержка нескольких копий каждой базы данных, что обеспечивает быструю активацию

- Снижение затрат на инфраструктуру обмена сообщениями
- Повышение доступности за счет оптимизации доменов сбоя и снижения сложности

Конкретный предписывающий характер ра означает, что не каждый клиент сможет развернуть его слово в слово. Например, не у всех наших клиентов есть несколько центров обработки данных. Некоторые из наших клиентов могут иметь разные бизнес-требования или внутренние политики, которым они должны соответствовать, что требует другой архитектуры развертывания. Если вы относитесь к этим категориям и хотите развернуть локальную среду Exchange, вы по-прежнему имеете преимущества в том, чтобы как можно точнее придерживаться ра ра и отклоняться только в том случае, если требования или политики вынуждают вас отличаться. Кроме того, вы всегда можете использовать Microsoft 365 или Office 365, где больше не требуется развертывать большое количество серверов или управлять ими.

Ра устраняет сложность и избыточность, когда это необходимо, чтобы привести архитектуру к прогнозируемой модели восстановления: при сбое активируется другая копия затронутой базы данных.

Основное внимание уделяется следующим четырем областям:

1. Проектирование пространства имен
2. Проектирование пар центров обработки данных, устойчивых к сайту
3. Проектирование сервера
4. Проектирование группы доступности базы данных

Для Exchange Server 2019 г. у нас нет изменений в трех из четырех категорий из предпочтительной архитектуры Exchange Server 2016 года. Области проектирования пространства имен, проектирования центра обработки данных и структуры DAG не получают серьезных изменений. Мы были довольны развертываниями клиентов, которые внимательно следили за Exchange Server 2016 PA, и не видим необходимости отклоняться от рекомендаций в этих областях.

Наиболее заметные изменения в Exchange Server 2019 PA сосредоточены на области проектирования серверов из-за некоторых новых и интересных технологий.

Проектирование пространства имен

В статьях о планировании пространства имен и принципах балансировки нагрузки за Exchange Server 2016 г. Росс Смит IV рассказал о различных вариантах конфигурации, доступных в Exchange 2016, и эти понятия по-прежнему применяются для Exchange Server 2019 г. Для пространства имен можно развернуть привязанное пространство имен (с предпочтением для пользователей работать вне определенного центра обработки данных) или неограниченное пространство имен (пользователи подключаются к любому центру обработки данных без предпочтения).

Рекомендуемый подход — использовать модель без ограничений, развертывая одно пространство имен Exchange для каждого клиентского протокола для пары устойчивых к сайту центров обработки данных (где предполагается, что каждый центр обработки данных представляет свой собственный сайт Active Directory. Дополнительные сведения см. ниже). Например:

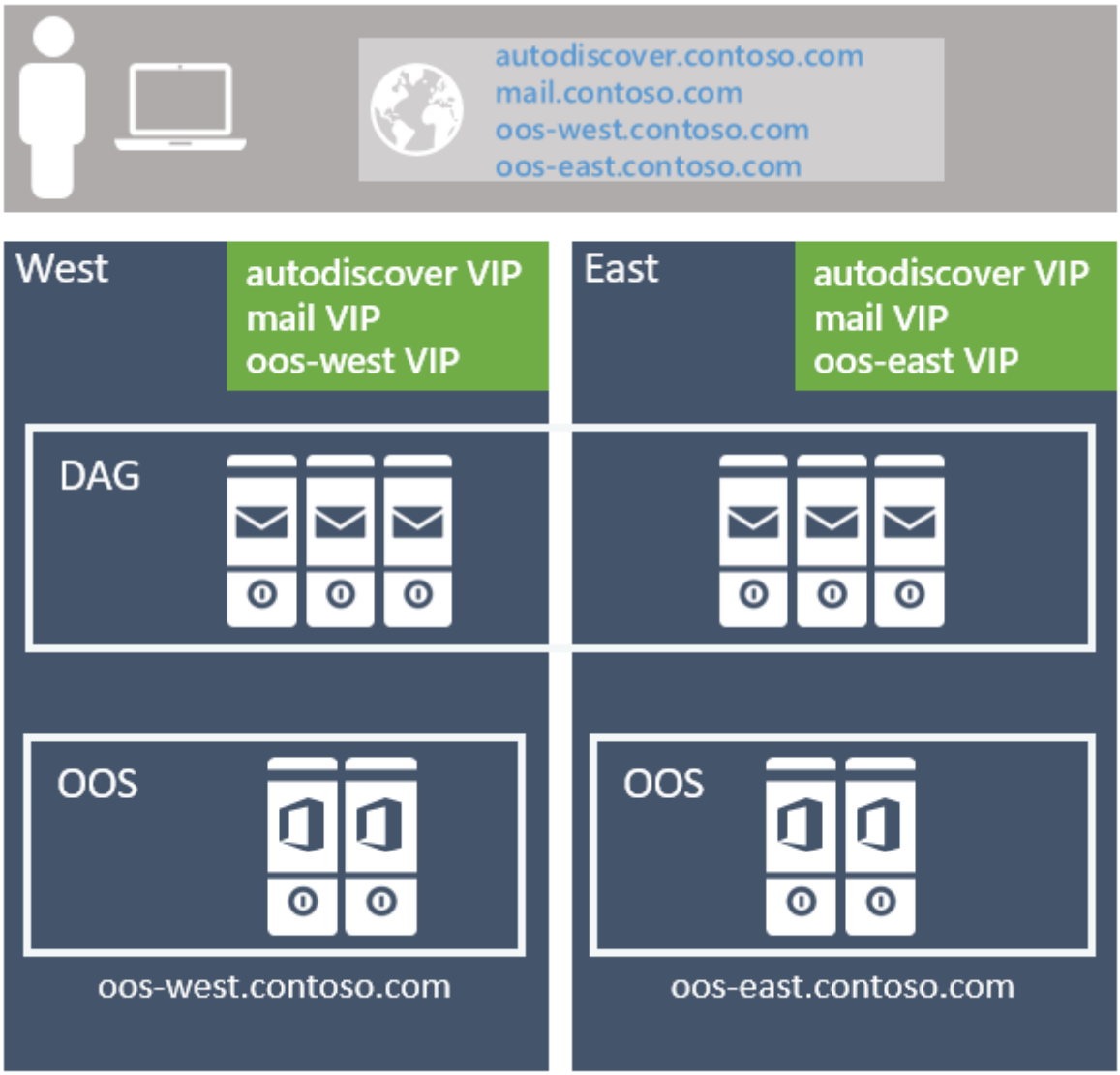
- Для службы автообнаружения: autodiscover.contoso.com
- Для HTTP-клиентов: mail.contoso.com
- Для клиентов IMAP: imap.contoso.com
- Для smtp-клиентов: smtp.contoso.com

Каждое пространство имен Exchange распределяется между обоими центрами обработки данных в конфигурации уровня 7, которая не использует сходство сеансов, что приводит к тому, что 50 процентов трафика перемещается между центрами обработки данных. Трафик равномерно распределяется между центрами обработки данных в паре устойчивых к сайту, через циклический перебор DNS, гео-DNS или другие аналогичные решения. С нашей точки зрения, более простое решение является наименее сложным и простым в управлении, поэтому мы рекомендуем использовать циклический перебор DNS.

Одно из предостережений, которое мы имеем для клиентов, заключается в том, чтобы вы назначали низкое значение срока жизни (время жизни) для любой записи DNS, связанной с вашей архитектурой Exchange. Если при использовании DNS с циклическим перебором происходит полный сбой центра обработки данных, необходимо поддерживать возможность быстрого обновления записей DNS. Вам потребуется удалить IP-адреса из автономного центра обработки данных, чтобы они не возвращались для ЗАПРОСОВ DNS. Например, если ваши записи DNS имеют более длинное значение TTL в 24 часа, для правильного обновления подчиненных кэшей DNS может потребоваться до дня. Если вы не выполните этот шаг, некоторые клиенты не могут правильно перейти на все еще доступные IP-адреса в оставшемся центре обработки данных. Не забудьте добавить IP-адреса

обратно в записи DNS, когда ранее автономный центр обработки данных будет восстановлен и снова готов к размещению служб.

Сходство центров обработки данных требуется для ферм Office Online Server, поэтому пространство имен развертывается для каждого центра обработки данных с подсистемой балансировки нагрузки, использующим уровень 7, и поддерживает сходство сеансов с помощью сохраняемости на основе файлов cookie.



Если в вашей среде есть несколько пар центров обработки данных, устойчивых к сайту, необходимо решить, хотите ли вы иметь одно глобальное пространство имен или вы хотите управлять трафиком к каждому конкретному центру обработки данных с помощью региональных пространств имен. Ваше решение зависит от топологии сети и связанных с ней затрат на использование модели без ограничений. Например, если у вас есть центры обработки данных, расположенные в Северная Америка и Южной Африке, сетевой канал между этими регионами может быть не только дорогостоящим, но также может иметь высокую задержку, что может привести к возникновению проблем пользователей и операционных проблем. В этом случае имеет смысл развернуть привязанную

модель с отдельным пространством имен для каждого региона. Однако такие параметры, как географическая DNS, позволяют развернуть единое единое пространство имен, даже если у вас есть дорогостоящие сетевые каналы. Geo-DNS позволяет направлять пользователей в ближайший центр обработки данных на основе IP-адреса клиента.

Проектирование пар центров обработки данных, устойчивых к сайту

Чтобы обеспечить высокодоступную *и* устойчивую к сайту архитектуру, необходимо иметь два или более хорошо подключенных центров обработки данных (в идеале требуется низкая задержка в сети кругового пути, в противном случае это негативно повлияет на репликацию и взаимодействие с клиентом). Кроме того, центры обработки данных должны быть подключены через избыточные сетевые пути, предоставляемые разными операционными операторами.

Хотя мы поддерживаем растягивание сайта Active Directory между несколькими центрами обработки данных, для ра рекомендуется, чтобы каждый центр обработки данных был собственным сайтом Active Directory. Существует две причины:

1. Обеспечение устойчивости сайта с помощью теневой избыточности в Exchange Server и Safety Net в Exchange Server может быть достигнуто только в том случае, если daG содержит члены, расположенные на нескольких сайтах Active Directory.

2. Active Directory опубликовала руководство , в котором говорится, что подсети должны размещаться на разных сайтах Active Directory, если задержка кругового пути между подсетями превышает 10 мс.

Проектирование сервера

В ра все серверы являются физическими серверами и используют локально подключенное хранилище. Физическое оборудование развертывается вместо виртуализированного оборудования по двум причинам:

1. Серверы масштабируются для использования 80 % ресурсов в режиме наихудшего сбоя.

2. Виртуализация обеспечивает небольшую снижение производительности и добавляет дополнительный уровень управления и сложности, что приводит к добавлению дополнительных режимов восстановления, которые не добавляют ценности, особенно с учетом того, что Exchange Server изначально предоставляет те же функции.

Серверы товаров

Платформы сервера товаров используются в ра. К текущим товарным платформам относятся:

- 2U, серверы с двумя сокетами до 48 физических ядер процессора (увеличение с 24 ядер в Exchange 2016)
- До 256 ГБ памяти (увеличение с 192 ГБ в Exchange 2016)
- Контроллер кэша записи с поддержкой батареи
- 12 или более дисковых отсеков в серверных корпусах
- Возможность смешивать традиционное вращающееся дисковое хранилище (HDD) и твердотельные накопители (SSD) в одном корпусе.

Теория масштабирования

Важно отметить, что несмотря на то, что в Exchange Server 2019 году мы увеличили разрешенную емкость процессора и памяти, Exchange Server PG рекомендуется масштабировать, а не увеличивать. Горизонтальное и вертикальное масштабирование означает, что мы предпочли бы развернуть большее количество серверов с немного меньшим количеством ресурсов на сервер, а не меньшее количество серверов с высокой плотностью, использующих максимальное количество ресурсов и заполненных большим количеством почтовых ящиков. Размещая разумное количество почтовых ящиков на сервере, вы уменьшаете влияние любых запланированных или незапланированных простоев и снижаете риск обнаружения других узких мест системы.

Увеличение системных ресурсов не должно привести к предположению, что в Exchange Server 2019 г. вы увидите линейное повышение производительности с использованием максимально допустимых ресурсов при сравнении с максимально допустимыми ресурсами Exchange 2016. Каждая новая версия Exchange приносит новые процессы и обновления, которые, в свою очередь, затрудняют сравнение текущей версии с предыдущей версией. При определении структуры сервера следуйте всем рекомендациям корпорации Майкрософт по определению размера.

Хранилища

Дополнительные отсеки для дисков могут быть напрямую подключены к каждому серверу в зависимости от количества почтовых ящиков, размера почтовых ящиков и масштабируемости ресурсов сервера.

Каждый сервер содержит одну пару дисков RAID1 для операционной системы, двоичных файлов Exchange, журналов протокола/клиента и транспортной базы данных.

Остальное хранилище настроено как JBOD (всего несколько дисков). Обратите внимание, что некоторые аппаратные контроллеры хранилища могут потребовать, чтобы каждый диск был настроен в качестве группы RAID0 с одним диском для использования кэширования записи. Проконсультируйтесь с производителем оборудования, чтобы подтвердить правильную конфигурацию системы, гарантирующую использование кэша записи.

Впервые в Exchange Server 2019 PA рекомендуется использовать два класса хранилища для всего, что еще не находится в паре дисков RAID1, упомянутой ранее.

Традиционный класс хранения

Этот класс хранения содержит файлы Exchange Server базы данных и Exchange Server файлы журнала транзакций. Эти диски представляют собой диски SCSI большой емкости 7,2 КБ об/мин, последовательно подключенные к SCSI (SAS). Хотя диски SATA также доступны, мы наблюдаем улучшение операций ввода-вывода и более низкую годовую частоту сбоев с использованием эквивалента SAS.

Чтобы обеспечить максимально эффективное использование емкости и операций ввода-вывода каждого диска, на каждом диске развертывается до четырех копий баз данных. Обычный макет копирования во время выполнения гарантирует, что на диск будет не более одной активной копии базы данных.

По крайней мере один диск в традиционном пуле дисков хранилища зарезервирован в качестве горячего резерва. Функция AutoReseed включена и быстро восстанавливает избыточность базы данных после сбоя диска, активируя горячий резерв и инициируя повторное копирование базы данных.

Класс твердотельного хранилища

Этот класс хранения содержит новые файлы Базы данных MetaCache (MCDB) Exchange 2019. Эти твердотельные накопители могут поступать в различных форм-факторах, таких как, помимо прочего, традиционные подключенные sas 2.5"/3.5" или подключенные к M.2 PCIe диски.

Клиенты должны ожидать развертывания примерно 5–10 % дополнительного хранилища в качестве твердотельного хранилища. Например, если ожидается, что один сервер будет хранить 28 ТБ файлов базы данных почтовых ящиков в традиционном хранилище, то в качестве дополнительного хранилища для того же сервера также рекомендуется дополнительное хранилище объемом 1,4–2,8 ТБ.

Традиционные и твердотельные диски должны развертываться в соотношении 3:1, где это возможно. Для каждых трех традиционных дисков на сервере будет развернут один твердотельный диск. Эти твердотельные диски будут содержать mcDB для всех баз данных в трех связанных традиционных дисках. Эта рекомендация ограничивает домен сбоя, который может привести к сбою твердотельного диска в системе. При сбое SSD Exchange 2019 выполнит отработку отказа всех копий базы данных, использующих этот SSD для mcDB, на другой узел DAG с работоспособными ресурсами MCDB для затронутой базы данных. Ограничение числа операций отработки отказа базы данных снижает вероятность влияния на пользователей, если многие другие базы данных совместно использует меньшее число твердотельных дисков.

При сбое твердотельных дисков Служба высокой доступности Exchange попытается подключить затронутые базы данных на разных узлах DAG, где для каждой затронутой базы данных по-прежнему существует работоспособность MCDB. Если по какой-либо причине для одной из затронутых баз данных не существует работоспособных mcDB, службы высокого уровня доступности Exchange оставят локальную затронутую копию базы данных запущенной без преимуществ производительности MCDB.

Например, если клиент должен был развернуть систему, которая может содержать 20 дисков, она может иметь следующий макет.

- 2 жестких диска для зеркального отображения ОС, двоичных файлов Exchange и транспортной базы данных
- 12 жестких дисков для хранилища базы данных Exchange
- 1 жесткий диск в качестве запасного резерва AutoReseed
- 4 накопителя SSD для MCDB Exchange, которые обеспечивают от 5 до 10 % совокупной емкости хранилища базы данных.

- При необходимости клиент может добавить запасной ssd или второй диск с автоматическим удалением.

Эту конфигурацию можно визуализировать на следующей схеме:

10TB HDD	10TB HDD	10TB HDD	10TB HDD	OS Mirror
10TB HDD	10TB HDD	10TB HDD	10TB HDD	OS Mirror
10TB HDD	10TB HDD	10TB HDD	10TB HDD	10TB HDD Spare
1.92TB SSD	1.92TB SSD	1.92TB SSD	1.92TB SSD	Empty

В приведенном выше примере мы имеем 120 ТБ хранилища базы данных Exchange и 7,68 ТБ хранилища MCDB, что составляет примерно 6,4 % традиционного хранилища базы данных. Благодаря такому объему хранилища MCBD мы полностью выровнены в соответствии с рекомендациями 5–10 %. Каждый из дисков емкостью 10 ТБ будет содержать четыре копии базы данных, а каждый диск MCDB будет содержать 12 MCDB.

Общие параметры хранилища

Как традиционные, так и твердотельные, все диски, на которых размещены данные Exchange, форматируются с помощью ReFS (с отключенной функцией целостности), а DAG настраивается таким образом, чтобы автоотбор дисков форматировался с помощью ReFS:

PowerShell

```
Set-DatabaseAvailabilityGroup -Identity <DAGIdentity> -FileSystem ReFS
```

BitLocker используется для шифрования каждого диска, обеспечивая тем самым шифрование неактивных данных и устранение проблем, связанных с кражей данных или заменой диска. Дополнительные сведения см. в разделе Включение BitLocker на серверах Exchange Server.

Проектирование группы доступности базы данных

В каждой паре устойчивых к сайту центров обработки данных у вас будет одна или несколько групп daG. Не рекомендуется растягивать DAG на более чем два центра

обработки данных.

Конфигурация DAG

Как и в случае с моделью пространства имен, каждое daG в паре устойчивых к сайту центров обработки данных работает в модели без ограничений с активными копиями, распределенными поровну между всеми серверами в DAG. Эта модель:

1. Гарантирует, что во время обычных операций проверяется полный стек служб каждого члена DAG (подключение клиента, конвейер репликации, транспорт и т. д.).

2. Распределяет нагрузку между как можно большим количеством серверов во время сценария сбоя, тем самым только постепенно увеличивая использование ресурсов среди остальных членов в DAG.

Каждый центр обработки данных симметричный, с равным числом членов DAG в каждом центре обработки данных. Это означает, что каждое DAG имеет четное число серверов и использует сервер-свидетель для обслуживания кворума.

DaG является основным стандартным блоком в Exchange 2019. Что касается размера DAG, daG с большим количеством участвующих узлов-членов обеспечивает большую избыточность и ресурсы. В ра ра цель состоит в том, чтобы развернуть группы доступности базы данных с большим количеством узлов-членов, обычно начиная с восьми членов DAG и увеличивая количество серверов, необходимых для удовлетворения ваших требований. Создавать новые группы доступности баз данных следует только в том случае, если масштабируемость вызывает проблемы с существующим макетом копии базы данных.

Проектирование сети DAG

Ра использует единый, не объединяемый сетевой интерфейс как для подключения клиента, так и для репликации данных. Единый сетевой интерфейс — это все, что необходимо, так как в конечном итоге наша цель заключается в достижении стандартной модели восстановления независимо от того, происходит ли сбой сервера или происходит сбой сети. Результат тот же: копия базы данных активируется на другом сервере в daG. Это изменение архитектуры упрощает сетевой стек и устраняет необходимость вручную устранять перекрестное взаимодействие с пульсом.

Размещение следящего сервера

Размещение следящего сервера определяет, может ли архитектура предоставлять возможности автоматической отработки отказа центра обработки данных или потребуется активация вручную для включения службы в случае сбоя сайта.

Если в вашей организации есть третье расположение с сетевой инфраструктурой, изолированной от сбоев сети, влияющих на пару устойчивых к сайту центров обработки данных, в которой развернута daG, рекомендуется развернуть следящий сервер DAG в этом третьем расположении. Эта конфигурация дает daG возможность автоматической отработки отказа баз данных в другой центр обработки данных в ответ на событие сбоя на уровне центра обработки данных независимо от того, в каком центре обработки данных произошел сбой.

Если у вашей организации нет третьего расположения, рассмотрите возможность размещения сервера-свидетеля в Azure. Кроме того, поместите следящий сервер в один из центров обработки данных в паре устойчивых к сайту центров обработки данных. Если в паре устойчивых к сайту центров обработки данных имеется несколько групп доступности баз данных, поместите следящий сервер для всех daG в одном центре обработки данных (как правило, в центре обработки данных, где физически расположено большинство пользователей). Кроме того, убедитесь, что основной активный диспетчер (PAM) для каждой группы daG также находится в одном центре обработки данных.

Exchange Server 2019 г. и все более ранние версии не поддерживают использование функции Cloud-свидетеля, впервые представленной в Windows Server 2016 отказоустойчивом кластере.

Устойчивость данных

Устойчивость данных достигается путем развертывания нескольких копий базы данных. В ра копии базы данных распределяются по паре устойчивых к сайту центров обработки данных, обеспечивая тем самым защиту данных почтового ящика от сбоев программного обеспечения, оборудования и даже центра обработки данных.

Каждая база данных имеет четыре копии с двумя копиями в каждом центре обработки данных. Это означает, что для ра ра требуется как минимум четыре сервера. Из этих четырех копий три из них настроены как высокодоступные. Четвертая копия (копия с наибольшим номером предпочтения активации) настраивается как копия базы данных с отстаю. Благодаря структуре сервера каждая копия базы данных изолирована от других копий, тем самым уменьшая домены сбоев и повышая общую доступность решения, как описано в разделе DAG: за пределами "A".

Цель копии базы данных с отстающей базой данных заключается в том, чтобы обеспечить механизм восстановления редких случаев катастрофического логического повреждения в масштабах всей системы. Он не предназначен для восстановления отдельных почтовых ящиков или для восстановления элементов почтового ящика.

Для отстающей копии базы данных настраивается семь дней ReplayLagTime. Кроме того, диспетчер задержки воспроизведения также включается для динамического воспроизведения файлов журнала для отставание копий, когда доступность скомпрометирована из-за потери не отставанных копий.

Используя таким образом отстающую копию базы данных, важно понимать, что отстающая копия базы данных не является гарантированной резервной копией на определенный момент времени. Отстающая копия базы данных будет иметь порог доступности, как правило, около 90 %, из-за периодов, когда диск, содержащий отстающую копию, теряется из-за сбоя диска, отстающая копия становится копией высокого уровня доступности (из-за автоматического воспроизведения) и периодов, когда отстающая копия базы данных перестраивает очередь воспроизведения.

Для защиты от случайного (или вредоносного) удаления элементов используются технологии восстановления одного элемента или хранения на месте , а в окне Хранение удаленных элементов задается значение, соответствующее или превышающее любое определенное соглашение об уровне обслуживания для восстановления на уровне элемента.

При использовании всех этих технологий традиционные резервные копии не нужны; в результате pas использует собственную защиту данных Exchange.

Office Online Server проектирование

Как минимум, вам потребуется развернуть ферму Office Online Server (OOS) с по крайней мере двумя узлами OOS в каждом центре обработки данных, где размещаются серверы Exchange 2019. Каждая Office Online Server должна иметь по крайней мере 8 ядер процессора, 32 ГБ памяти и не менее 40 ГБ пространства, выделенного для файлов журналов. Серверы почтовых ящиков Exchange 2019 должны быть настроены так, чтобы использовать локальную ферму OOS в центре обработки данных, чтобы обеспечить минимальную задержку и максимальную пропускную способность между серверами для отображения содержимого файлов для пользователей.

Аннотация

Exchange Server 2019 году продолжает улучшать инвестиции, представленные в предыдущих версиях Exchange, и вводит дополнительные технологии, первоначально изобретенные для использования в Microsoft 365 и Office 365.

В соответствии с предпочтительной архитектурой вы воспользуетесь преимуществами этих изменений и обеспечите наилучший локальный пользовательский интерфейс. Вы будете продолжать традицию высоконадежного, предсказуемого и устойчивого развертывания Exchange.

разрешения Exchange Server

Статья • 04.04.2023

Microsoft Exchange Server включает в себя большой набор предопределенных разрешений, основанных на модели разрешений на основе ролей контроль доступа (RBAC), которую можно использовать сразу, чтобы легко предоставлять разрешения администраторам и пользователям. Вы можете использовать функции разрешений в Exchange Server, чтобы быстро запустить новую организацию.

Разрешения на основе ролей

В Exchange Server разрешения, предоставляемые администраторам и пользователям, основаны на ролях управления. Роль определяет набор задач, которые может выполнять администратор или пользователь. Например, роль `Mail Recipients` управления определяет задачи, которые кто-то может выполнять в наборе почтовых ящиков, контактов и групп рассылки. Когда роль назначается администратору или пользователю, ему предоставляются разрешения в соответствии с этой ролью.

Существует два типа ролей — административные роли и роли конечных пользователей.

- **Административные роли**. Эти роли содержат разрешения, которые могут быть назначены администраторам или пользователям-специалистам с помощью групп ролей, управляющих частью организации Exchange, например получателями, серверами или базами данных.
- **Роли конечных пользователей**. Эти роли, назначенные с помощью политик назначения ролей, позволяют пользователям управлять аспектами собственных почтовых ящиков и групп рассылки, которыми они владеют. Роли конечных пользователей начинаются с префикса `My`.

Роли дают разрешения администраторам и пользователям на выполнение задач, предоставляя доступ к командлетам лицам с назначенными ролями. Так как Центр администрирования Exchange (EAC) и командная консоль Exchange используют командлеты для управления Exchange, предоставление доступа к командлету дает администратору или пользователю разрешение на выполнение задачи в каждом из интерфейсов управления Exchange.

Группы ролей и политики назначения ролей

Роли предоставляют разрешения на выполнение задач в Exchange Server, но вам нужен простой способ назначить их администраторам и пользователям. Exchange Server предоставляет следующие сведения, которые помогут вам в этом.

- **Группы ролей**. Группы ролей позволяют предоставлять разрешения администраторам и специализированным пользователям.
- **Политики назначения ролей**. Политики назначения ролей позволяют предоставлять конечным пользователям разрешения на изменение параметров в собственных почтовых ящиках или группах рассылки, которыми они владеют.

Дополнительные сведения о группах ролей и политиках назначения ролей см. в следующих разделах:

Группы ролей

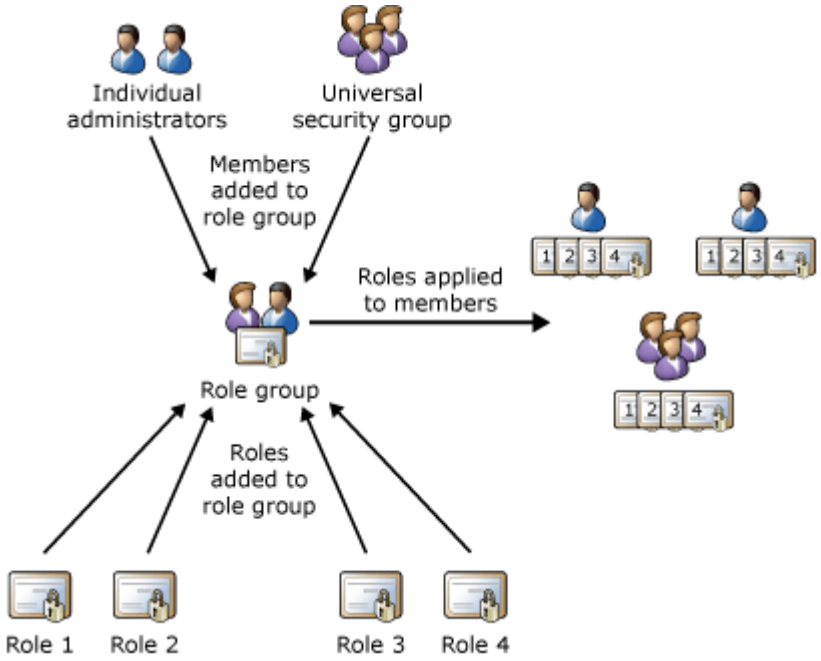
Каждому администратору, управляющего Exchange Server, необходимо назначить по крайней мере одну или несколько ролей. Администраторы могут иметь несколько ролей, так как они могут выполнять функции заданий, охватывающие несколько областей в Exchange. Например, один администратор может управлять как получателями, так и серверами Exchange. В этом случае этому администратору могут быть назначены `Mail Recipients` роли и `Exchange Servers` .

Чтобы упростить назначение администратору нескольких ролей, Exchange Server включает группы ролей. Группы ролей — это специальные универсальные группы безопасности (USG), используемые Exchange Server, которые могут содержать пользователей Active Directory, группы безопасности и другие группы ролей. Когда роль назначается группе ролей, разрешения, соответствующие этой роли, предоставляются всем участникам данной группы. Это позволяет назначить множество ролей сразу нескольким участникам группы ролей. Группы ролей обычно охватывают более широкие области управления, например управление получателями. Они используются только вместе с административными ролями, но не с ролями конечных пользователей.

> ⓘ **Примечание**
>
> Можно назначить роль непосредственно пользователю или группе USG, не используя группу ролей. Однако такой способ назначения ролей относится к расширенным процедурам и не затрагивается в данном разделе. Рекомендуется для управления разрешениями использовать группы ролей.

На приведенном ниже рисунке показана взаимосвязь между пользователями, группами ролей и ролями.

Роли, группы ролей и участники групп ролей



Exchange Server включает несколько встроенных групп ролей, каждая из которых предоставляет разрешения для управления определенными областями в Exchange Server. Некоторые группы ролей могут перекрываться с другими. В приведенной ниже таблице перечислены группы ролей с описанием их использования. Чтобы увидеть роли, назначенные каждой группе ролей, щелкните имя группы ролей в столбце "Группа ролей" и затем откройте раздел "Роли управления, назначенные этой группе ролей".

> ⓘ **Важно!**
>
> Если администратор является членом нескольких групп ролей, Exchange Server предоставляет администратору все разрешения, предоставляемые группами ролей, в которые он входит.

Встроенные группы ролей

Группа ролей	Описание

Группа ролей	Описание
Управление организацией	Администраторы, являющиеся членами группы ролей Управление организацией, имеют административный доступ ко всей Exchange Server организации и могут выполнять практически любую задачу с любым Exchange Server объектом, за некоторыми исключениями, например ролью `Discovery Management`. **Важно!** Так как группа ролей "Управление организацией" является мощной ролью, в нее должны вступить только пользователи или группы безопасности, которые выполняют административные задачи на уровне организации организации, которые могут повлиять на всю организацию Exchange.
View-Only Organization Management	Администраторы, являющиеся участниками группы ролей "Управление организацией" только с правом на просмотр, могут просматривать свойства любого объекта в организации Exchange.
Управление получателями	Администраторы, являющиеся членами группы ролей Управление получателями, имеют административный доступ для создания или изменения Exchange Server получателей в Exchange Server организации.
Управление единой системой обмена сообщениями	Администраторы, которые являются членами группы ролей Управление единой системой обмена сообщениями, могут управлять функциями в организации Exchange, например конфигурацией сервера единой системы обмена сообщениями, свойствами почтовых ящиков единой системы обмена сообщениями, приглашениями единой системы обмена сообщениями и конфигурацией автосекретаря единой системы обмена сообщениями. (**Примечание**. UM недоступна в Exchange 2019.)
Служба поддержки	Группа ролей службы поддержки по умолчанию позволяет участникам просматривать и изменять параметры Outlook в Интернете (прежнее название — Outlook Web App) любого пользователя в организации. В число изменяемых параметров пользователя могут входить отображаемое имя, адрес и номер телефона. К ним не относятся параметры, недоступные в параметрах Outlook в Интернете, такие как изменение размера почтового ящика или настройка базы данных почтовых ящиков, в которой находится почтовый ящик.
Управление санацией	Администраторы, являющиеся членами группы ролей "Управление гигиеной", могут настраивать функции антивирусной программы и защиты от нежелательной почты Exchange Server. Сторонние программы, которые интегрируются с Exchange Server, могут добавлять учетные записи служб в эту группу ролей, чтобы предоставить этим программам доступ к командлетам, необходимым для получения и настройки конфигурации Exchange.
Управление записями	Пользователи, являющиеся членами группы ролей Управление записями, могут настраивать функции соответствия, такие как теги политики хранения, классификации сообщений и правила потока обработки почты (также известные как правила транспорта).

Группа ролей	Описание
Discovery Management	Администраторы или пользователи, являющиеся членами группы ролей "Управление обнаружением", могут выполнять поиск данных в почтовых ящиках в организации Exchange, которые соответствуют определенным критериям, а также могут настроить удержание почтовых ящиков по юридическим причинам.
Управление общими папками	Администраторы, которые являются участниками группы ролей "Управление общедоступными папками", могут управлять общедоступными папками на серверах Exchange Server.
Управление сервером	Администраторы, которые являются участниками группы ролей управления сервером, могут выполнять настройку серверной конфигурации транспорта, единой системы обмена сообщениями, клиентского доступа и компонентов почтовых ящиков, таких как копии базы данных, сертификаты, транспортные запросы и соединители отправки, виртуальные каталоги, а также протоколы клиентского доступа. (**Примечание**. UM недоступна в Exchange 2019.)
Делегированная установка	Администраторы, состоящие в группе ролей "Делегированная установка", могут развертывать серверы Exchange Server, подготовленные участником группы ролей "Управление организацией".
Управление соответствием требованиям	Пользователи, являющиеся участниками группы управления соответствием требованиям, могут настраивать параметры соответствия требованиям Exchange и управлять ими согласно политике организации.

Если в вашей организации всего несколько администраторов, вам может понадобиться только группа ролей "Управление организацией". Если вы работаете в более крупной организации, у вас могут быть администраторы, которые выполняют определенные задачи администрирования Exchange, такие как управление получателями или сервером. В таких случаях можно добавить одного администратора в группу ролей "Управление получателями", а другого администратора в группу ролей "Управление сервером". Затем эти администраторы могут управлять своими конкретными областями Exchange Server но не будут иметь разрешений на управление областями, за которые они не отвечают.

Если вы не можете найти подходящую группу ролей, создайте свою и добавьте в нее роли. Дополнительные сведения см. в разделе Работа с группами ролей далее в этом разделе.

Политики назначения ролей

Exchange Server предоставляет политики назначения ролей, чтобы вы могли управлять параметрами, которые пользователи могут настраивать в своих почтовых ящиках и группах рассылки, которыми они владеют. Эти параметры включают отображаемое имя, контактную информацию, настройки голосовой почты и членство в группах рассылки.

Ваша Exchange Server организация может иметь несколько политик назначения ролей, которые предоставляют различные уровни разрешений для разных типов пользователей в организации. Некоторым пользователям может быть разрешено изменять свой адрес или создавать группы рассылки, а другим — нет. Все зависит от политики назначения ролей, связанной с почтовым ящиком. Политики назначения ролей добавляются непосредственно к почтовым ящикам, и с каждым почтовым ящиком может быть связана только одна политика.

Одна из политик назначения ролей в организации помечается как используемая по умолчанию. Политика назначения ролей по умолчанию связывается с новыми почтовыми ящиками, которым во время создания явным образом не была назначена определенная политика. Политика назначения ролей по умолчанию должна содержать разрешения, применяемые к большинству почтовых ящиков пользователя.

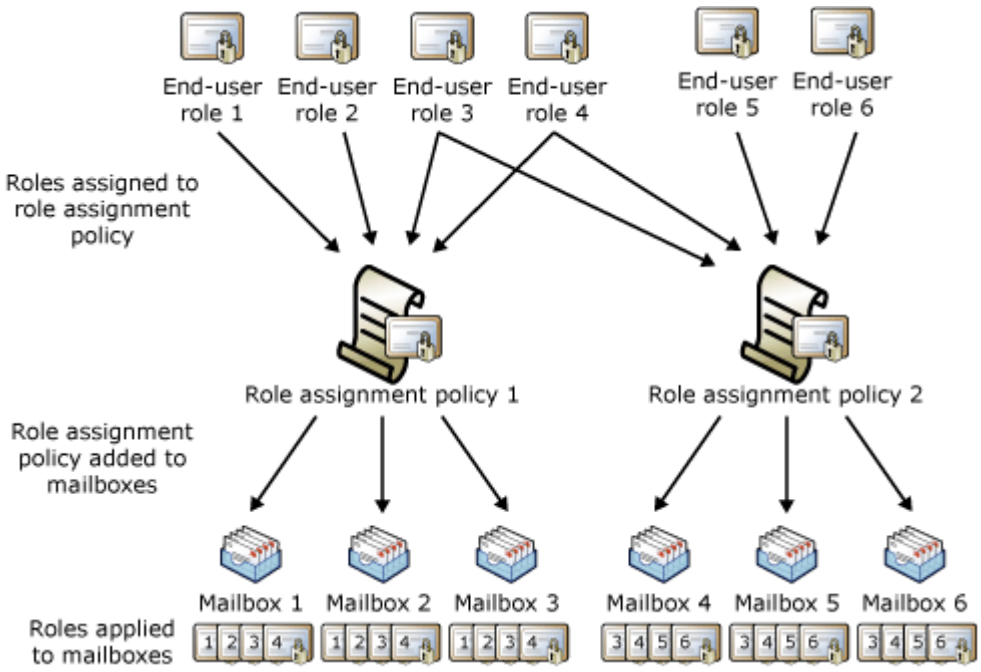
Разрешения добавляются в политики назначения ролей с использованием ролей конечных пользователей. Роли конечных пользователей начинаются с `My` и предоставляют пользователям разрешения на управление только своими почтовыми ящиками или группами рассылки, которыми они владеют. Они не могут использоваться для управления любыми другими почтовыми ящиками. Политикам назначения ролей могут быть назначены только роли конечных пользователей.

Когда роль конечного пользователя назначается политике назначения ролей, все почтовые ящики, связанные с этой политикой, получают разрешения, предусмотренные данной ролью. Это позволяет добавлять и удалять разрешения для групп пользователей без необходимости настройки отдельных почтовых ящиков. На приведенном ниже рисунке показано следующее.

- Роли конечных пользователей назначаются политикам назначения ролей. Политикам назначения ролей могут соответствовать одни и те же роли конечных пользователей.
- Политики назначения ролей связываются с почтовыми ящиками. С каждым почтовым ящиком может быть связана только одна политика назначения ролей.

- После связывания почтового ящика с политикой назначения ролей роли конечных пользователей применяются к этому почтовому ящику. Разрешения, предусмотренные ролями, предоставляются пользователю этого почтового ящика.

Роли, политики назначения ролей и почтовые ящики

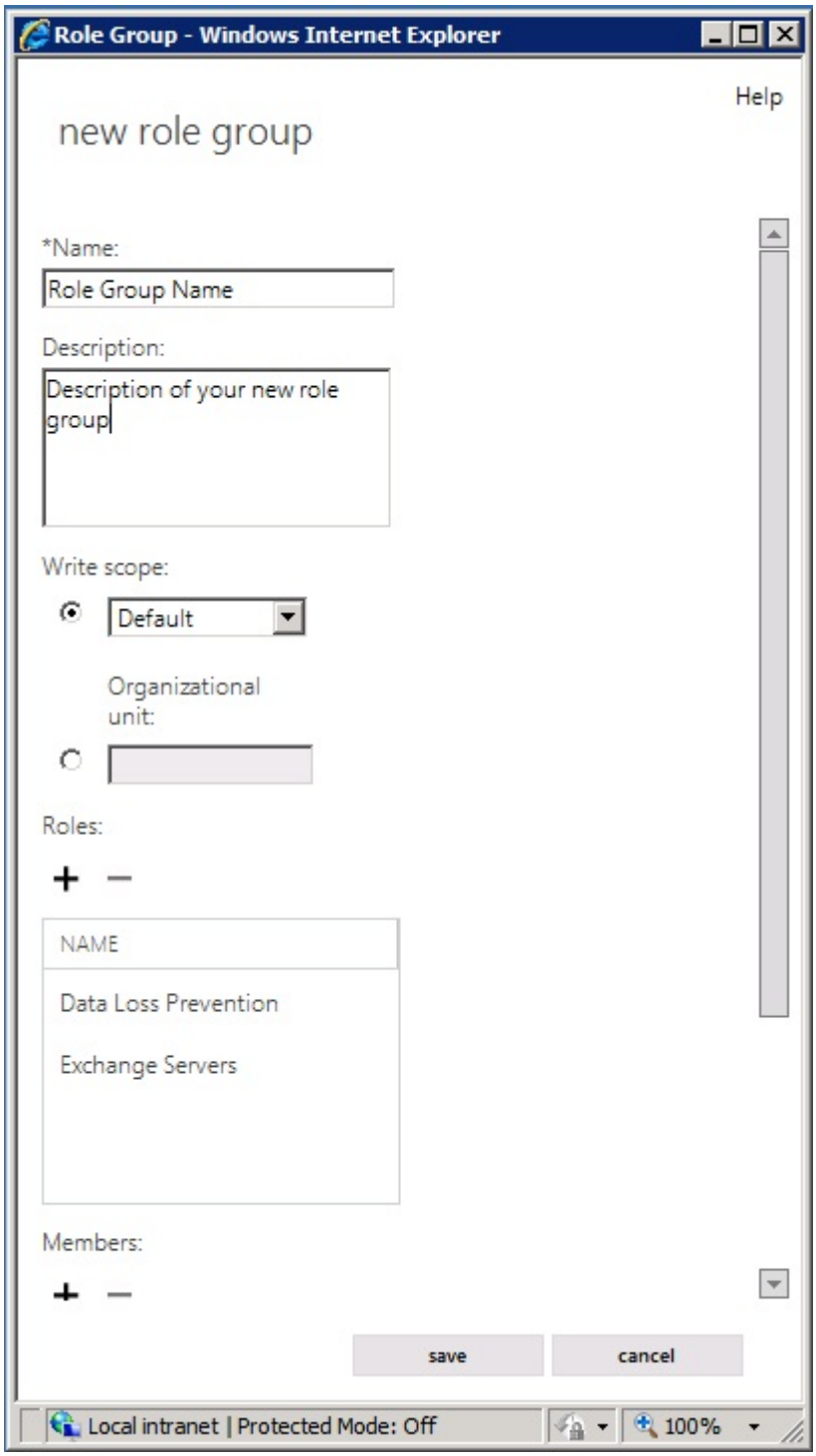


Политика назначения ролей политики назначения ролей по умолчанию включена в Exchange Server. Как и предполагает название, это политика назначения ролей по умолчанию. Если вы хотите изменить разрешения, предоставляемые этой политикой назначения ролей, или хотите создать политики назначения ролей, см. статью Работа с политиками назначения ролей далее в этом разделе.

Работа с группами ролей

Для управления разрешениями с помощью групп ролей в Exchange Server рекомендуется использовать Центр администрирования Exchange (EAC). Используя Центр администрирования Exchange для управления группами ролей, можно добавлять и удалять роли и участников, создавать группы ролей и копировать их с помощью нескольких щелчков кнопкой мыши. Для выполнения этих задач в Центре администрирования Exchange предусмотрены простые диалоговые окна (например, **Создание группы ролей**), показанные на рисунке ниже.

Диалоговое окно создания группы ролей в Центре администрирования Exchange



Если ни одна из групп ролей, входящих в состав Exchange Server, не имеет необходимых разрешений, вы можете использовать EAC для создания группы ролей и добавления ролей с нужными разрешениями. Для создания новой группы ролей выполните следующие действия.

1. Выберите имя для группы ролей.

2. Выберите роли, которые необходимо добавить в группу ролей.

3. Добавьте участников в группу ролей.

4. Сохраните группу ролей.

Создав группу ролей, ею можно управлять аналогично любой другой группе ролей.

Вы можете создать новую группу ролей на основе существующей. Копирование существующей группы ролей позволяет внести в нее изменения, не затрагивая исходную группу. В ходе копирования группы ролей можно добавить новое имя и описание, добавить или удалить роли из новой группы и добавить новых участников. Для создания или копирования группы ролей используется то же диалоговое окно, что показано на предыдущем рисунке.

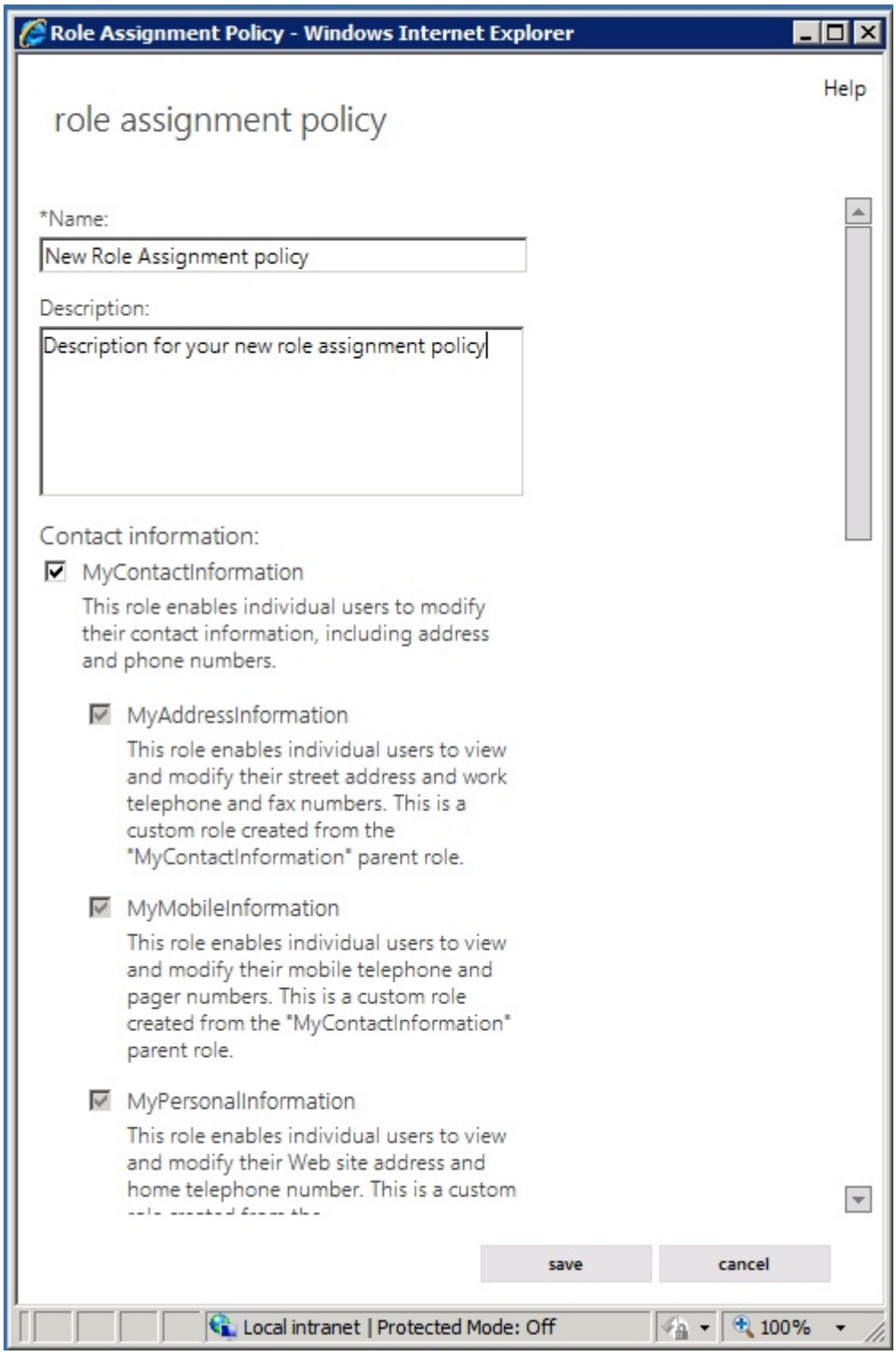
Существующие группы ролей можно также изменять. Можно добавлять и удалять роли из существующих групп ролей, а также одновременно добавлять и удалять из них участников при помощи диалогового окна Центра администрирования Exchange, аналогичного показанному на предыдущем рисунке. Добавляя и удаляя роли из группы ролей, пользователь включает и выключает административные функции для участников этой группы.

> ⓘ **Примечание**
>
> Хотя можно изменять состав ролей, назначаемых встроенным группам ролей, рекомендуется скопировать встроенную группу, изменить копию и затем добавить в нее участников.

Работа с политиками назначения ролей

Чтобы управлять разрешениями, предоставляемыми конечным пользователям для управления собственным почтовым ящиком в Exchange Server, рекомендуется использовать EAC. Используя Центр администрирования Exchange для управления разрешениями конечных пользователей, можно добавлять и удалять роли, а также создавать политики назначения ролей с помощью нескольких щелчков кнопкой мыши. Для выполнения этих задач в Центре администрирования Exchange предусмотрены простые диалоговые окна, такие как диалоговое окно **Политика назначения ролей**, показанное на рисунке ниже.

Диалоговое окно политики назначения ролей в Центре администрирования Exchange



Exchange Server включает политику назначения ролей с именем Политика назначения ролей по умолчанию. Эта политика позволяет пользователям, почтовые ящики которых связаны с ней, выполнять следующие задачи.

- Вступать в группы рассылки, которые позволяют участникам управлять своим членством, или выходить из групп рассылки.
- Просматривать и изменять основные параметры собственного почтового ящика, такие как правила папки "Входящие", поведение средства проверки орфографии, параметры нежелательной почты и устройства Microsoft ActiveSync.

- Изменять свою контактную информацию, такую как рабочий адрес и номер телефона, номер мобильного телефона или пейджера.
- Создавать, изменять и просматривать параметры текстовых сообщений.
- Просматривать и изменять параметры голосовой почты.
- Просматривать и изменять свои программы в marketplace.
- Создавать групповые почтовые ящики и подключать их к спискам Microsoft SharePoint.

Чтобы добавить или удалить разрешения из политики назначения ролей по умолчанию или другой политики назначения ролей, используйте Центр администрирования Exchange. Открыв политику, установите флажки рядом с ролями, которые вы хотите назначить этой политике, и снимите флажки рядом с ролями, которые необходимо удалить. Изменения, внесенные в политику назначения ролей, применяются к каждому связанному с ней почтовому ящику.

Чтобы назначить разные разрешения разным типам пользователей организации, создайте политики назначения ролей. Укажите новое имя для политики, а затем выберите нужные роли. Создав политику назначения ролей, вы можете связать ее с почтовыми ящиками при помощи Центра администрирования Exchange.

Если вы хотите изменить политику назначения ролей по умолчанию, необходимо использовать командную консоль Exchange. После изменения все создаваемые почтовые ящики будут связываться с новой политикой назначения ролей по умолчанию, если таковая не была явно указана. Политика назначения ролей, связанная с существующими почтовыми ящиками, не изменяется при выборе новой политики назначения ролей по умолчанию.

Примечания.

- Если установить флажок для роли, у которой есть дочерние роли, флажки для этих дочерних ролей также устанавливаются. Если снять флажок для роли, у которой есть дочерние роли, флажки для этих дочерних ролей также снимаются.
- Подробные сведения о создании политики назначения ролей, а также о внесении изменений в существующие политики назначения ролей см. в следующих разделах:
  - Управление политиками назначения ролей
  - Изменение политики назначения для почтового ящика

Управление группами ролей в Exchange Server

Статья • 04.04.2023

Группа ролей управления — это универсальная группа безопасности (USG), используемая в модели разрешений на основе ролей контроль доступа (RBAC) в Exchange Server. Группа ролей управления упрощает назначение ролей управления группе пользователей. Для всех участников группы ролей назначается идентичный набор ролей. Дополнительные сведения о группах ролей в Exchange Server см. в разделе Общие сведения о группах ролей управления.

Дополнительные сведения о задачах управления, связанных с группами ролей, см. в разделе Разрешения.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: от 5 до 10 минут
- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Группы ролей" в разделе Разрешения для управления ролями .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Создание группы ролей

Если нужно настроить разрешения, которые можно назначить группе пользователей, создайте новую настраиваемую группу ролей управления.

Использование Центра администрирования Exchange для создания группы ролей

1. В Центре администрирования Exchange перейдите к **разделу Разрешения**>**Администратор Роли**, а затем щелкните **Добавить**+

2. В окне **Новая группа ролей** укажите имя новой группы.

3. Вы можете сразу выбрать роли, которые требуется назначить группе ролей, и членов, которых требуется добавить к группе ролей, или сделать это позднее.

4. Выберите область записи, которую требуется применить к новой группе ролей.

5. Нажмите кнопку **Сохранить**, чтобы создать группу.

Создание группы ролей с помощью командной консоли Exchange

Сведения о создании группы ролей см. в разделе Examples статьи New-RoleGroup.

Как проверить, все ли получилось?

Чтобы убедиться в успешном создании группы ролей, выполните следующие действия.

1. В EAC перейдите в **раздел Разрешения**>**Администратор Роли**.

2. Убедитесь, что новая группа ролей отображается в списке групп ролей, и выберите ее.

3. Убедитесь, что члены, назначенные роли и область, которые вы указали для новой группы ролей, перечислены в области сведений группы ролей.

Копирование группы ролей

Использование Центра администрирования Exchange для копирования группы ролей

Если при предоставлении разрешений группы ролей другим пользователям необходимо применить другую область управления, удалить либо добавить одну

или несколько ролей управления без необходимости добавлять все роли вручную, можно скопировать существующую группу ролей.

> ⓘ **Важно!**
>
> Вы не можете использовать EAC для копирования группы ролей, если вы использовали командную консоль Exchange для настройки нескольких областей ролей управления или монопольных областей в группе ролей. Если вы настроили несколько областей или монопольных областей в группе ролей, необходимо скопировать группу ролей с помощью процедур командной консоли Exchange далее в этом разделе. Дополнительные сведения об областях ролей управления см. в разделе **Understanding Management Role Scopes**.

1. В EAC перейдите в **раздел Разрешения**>**Администратор Роли**.
2. Выберите группу ролей, которую нужно скопировать, и нажмите кнопку
3. В окне **Новая группа ролей** укажите имя новой группы.
4. Просмотрите роли, которые были скопированы в новую группу ролей. Добавьте или удалите роли при необходимости.
5. Просмотрите область записи и при необходимости измените ее.
6. Просмотрите членов, которые были скопированы в новую группу ролей. Добавьте или удалите членов при необходимости.
7. Нажмите кнопку **Сохранить**, чтобы создать группу.

Копирование группы ролей без области применения с помощью командной консоли Exchange

1. Сохраните группу ролей, которую необходимо копировать, в переменной с помощью следующей синтаксической конструкции:

   PowerShell

   ```
   $RoleGroup = Get-RoleGroup <name of role group to copy>
   ```

2. Создайте новую группу ролей, добавьте в нее членов и укажите пользователей, которые могут делегировать новую группу ролей другим пользователям, с помощью следующего синтаксиса.

PowerShell

```
New-RoleGroup <name of new role group> -Roles $RoleGroup.Roles -Members
<member1, member2, member3...> -ManagedBy <user1, user2, user3...>
```

Например, следующие команды копируют группу ролей «Organization Management» и присваивают новой группе ролей имя «Limited Organization Management». В группу добавляются члены Isabelle, Carter и Lukas и назначаются пользователи, которые могут делегировать группу ролей: Jenny и Katie.

PowerShell

```
$RoleGroup = Get-RoleGroup "Organization Management"
New-RoleGroup "Limited Organization Management" -Roles $RoleGroup.Roles
-Members Isabelle, Carter, Lukas -ManagedBy Jenny, Katie
```

После создания группы ролей в нее можно добавлять роли или удалять роли из нее, изменять область назначений ролей и т. д.

Дополнительные сведения о синтаксисе и параметрах см. в разделах Get-RoleGroup и New-RoleGroup.

Копирование группы ролей с пользовательской областью применения с помощью командной консоли Exchange

1. Сохраните группу ролей, которую необходимо копировать, в переменной с помощью следующей синтаксической конструкции:

PowerShell

```
$RoleGroup = Get-RoleGroup <name of role group to copy>
```

2. Создайте новую группу ролей с настраиваемой областью с помощью следующей синтаксической конструкции:

PowerShell

```
New-RoleGroup <name of new role group> -Roles $RoleGroup.Roles -
CustomRecipientWriteScope <recipient scope name> -
CustomConfigWriteScope <configuration scope name>
```

Например, следующие команды копируют группу ролей «Organization Management» и создают новую группу ролей с именем «Vancouver Organization Management» с областью получателей «Vancouver Users» и областью конфигурации «Vancouver Servers».

PowerShell

```
$RoleGroup = Get-RoleGroup "Organization Management"
New-RoleGroup "Vancouver Organization Management" -Roles $RoleGroup.Roles -
CustomRecipientWriteScope "Vancouver Users" -CustomConfigWriteScope
"Vancouver Servers"
```

Вы также можете добавить участников в группу ролей при ее создании с помощью параметра *Members* , как показано в разделе Использование командной консоли Exchange для создания назначения ролей без области , описанной выше в этом разделе. Дополнительные сведения об областях управления см. в разделе Understanding Management Scopes.

После создания группы ролей в нее можно добавлять роли или удалять роли из нее, изменять область назначений ролей и выполнять другие задачи.

Дополнительные сведения о синтаксисе и параметрах см. в разделах Get-RoleGroup и New-RoleGroup.

Копирование группы ролей с областью подразделения с помощью командной консоли Exchange

1. Сохраните группу ролей, которую необходимо копировать, в переменной с помощью следующей синтаксической конструкции:

   PowerShell

   ```
   $RoleGroup = Get-RoleGroup <name of role group to copy>
   ```

2. Создайте новую группу ролей с настраиваемой областью с помощью следующей синтаксической конструкции:

   PowerShell

   ```
   New-RoleGroup <name of new role group> -Roles $RoleGroup.Roles -
   RecipientOrganizationalUnitScope <OU name>
   ```

Например, следующие команды копируют группу ролей «Recipient Management» и создают новую группу ролей с именем «Toronto Recipient Management», которая позволяет управлять только пользователями в подразделении «Toronto Users».

PowerShell

```
$RoleGroup = Get-RoleGroup "Recipient Management"
New-RoleGroup "Toronto Recipient Management" -Roles $RoleGroup.Roles -
RecipientOrganizationalUnitScope "contoso.com/Toronto Users"
```

Вы также можете добавить участников в группу ролей при ее создании с помощью параметра *Members* , как показано в разделе Использование командной консоли Exchange для создания назначения ролей без области , описанной выше в этом разделе. Дополнительные сведения об областях управления см. в разделе Understanding Management Scopes.

После создания группы ролей в нее можно добавлять роли или удалять роли из нее, изменять область назначений ролей и т. д.

Дополнительные сведения о синтаксисе и параметрах см. в разделах Get-RoleGroup и New-RoleGroup.

Как проверить, все ли получилось?

Чтобы убедиться в успешном копировании группы ролей, выполните следующие действия.

1. В EAC перейдите в **раздел Разрешения**>**Администратор Роли**.
2. Убедитесь, что скопированная группа ролей отображается в списке групп ролей, и выберите ее.
3. Убедитесь, что члены, назначенные роли и область, которые вы указали для скопированной группы ролей, перечислены в области сведений группы ролей.

Удаление группы ролей

Если созданная группа ролей больше не нужна, ее можно удалить. При удалении группы ролей также удаляются и назначения управления ролями между группой ролей и ролями управления. Сами роли управления не удаляются. Если доступ пользователя к функции зависел от группы ролей, пользователь не будет иметь доступа к функции. Встроенные группы ролей удалить невозможно.

Использование Центра администрирования Exchange для удаления группы ролей

1. В EAC перейдите в **раздел Разрешения**>**Администратор Роли**.
2. Выберите группу ролей, которую нужно удалить, и нажмите кнопку **Удалить**🗑
3. Убедитесь, что вы хотите удалить выбранную группу ролей, и, если это так, выберите **Да** в качестве ответа на предупреждение.

Удаление группы ролей с помощью командной консоли Exchange

Сведения об удалении группы ролей см. в разделе Examples статьи Remove-RoleGroup.

Просмотр групп ролей

Вы можете просмотреть список групп ролей или подробные сведения о конкретной группе ролей, существующей в организации.

Использование Центра администрирования Exchange для просмотра списка групп ролей и сведений о них

1. В EAC перейдите в **раздел Разрешения**>**Администратор Роли**. Здесь перечислены все группы ролей в организации.
2. Выберите группу ролей для просмотра членов, назначенных ролей и области, настроенных для группы ролей.

Просмотр списка групп ролей и сведений о них с помощью командной консоли Exchange

Сведения о просмотре списка групп ролей см. в разделе Examples статьи Get-RoleGroup.

Добавление роли в группу ролей

Добавление роли управления в группу ролей является самым лучшим и простым способом предоставления разрешений группе администраторов или

пользователей-специалистов. Если следует предоставить пользователям, являющимся членами группы ролей, возможность управлять определенной возможностью, следует добавить в группу ролей роль управления, которая отвечает за управление этой возможностью. После добавления роли членам группы ролей предоставляются разрешения, обеспечиваемые данной ролью.

Использование Центра администрирования Exchange для добавления роли управления в группу ролей

> ⓘ **Важно!**
>
> Вы не можете использовать EAC для добавления ролей в группу ролей, если вы использовали командную консоль Exchange для настройки нескольких областей ролей управления или монопольных областей в группе ролей. Если вы настроили несколько областей или монопольных областей в группе ролей, необходимо использовать процедуры командной консоли Exchange далее в этом разделе, чтобы добавить роли в группу ролей. Дополнительные сведения об областях ролей управления см. в разделе **Understanding Management Role Scopes**.

1. В EAC перейдите в **раздел Разрешения**>**Администратор Роли**.
2. Выберите группу ролей, в которую вы хотите добавить роль, и нажмите кнопку **Изменить**.
3. В разделе **Роли** выберите роли, которые требуется добавить в группу ролей.
4. Когда добавление ролей в группу ролей завершено, нажмите кнопку **Сохранить**.

Создание назначения роли без области с помощью командной консоли Exchange

Можно создать назначение роли без области между ролью и группой ролей. При этом применяются неявные области чтения и записи роли.

Используйте следующий синтаксис для назначения группе ролей роли без области. Если имя назначения роли не задано, оно создается автоматически.

```
PowerShell
```

```
New-ManagementRoleAssignment -SecurityGroup <role group name> -Role <role
name>
```

В этом примере группе ролей Seattle Compliance назначается роль управления Transport Rules.

PowerShell

```
New-ManagementRoleAssignment -SecurityGroup "Seattle Compliance" -Role
"Transport Rules"
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе New-ManagementRoleAssignment.

Создание назначения роли с предварительно определенной областью с помощью командной консоли Exchange

Если предварительно определенная область соответствует потребностям организации, можно применить эту область к назначению роли, а не создавать новую. Список предварительно определенных областей и их описания см. в разделе Understanding Management Role Scopes.

Дополнительные сведения о назначениях ролей см. в разделе Understanding Management Role Assignments.

Используйте следующий синтаксис для назначения группе ролей роли с предварительно определенной областью. Если имя назначения роли не задано, оно создается автоматически.

PowerShell

```
New-ManagementRoleAssignment -SecurityGroup <role group name> -Role <role
name> -RecipientRelativeWriteScope < MyGAL | MyDistributionGroups |
Organization | Self >
```

В этом примере роль Message Tracking назначается группе ролей Enterprise Support, затем применяется предварительно определенная область Organization.

PowerShell

```
New-ManagementRoleAssignment -SecurityGroup "Enterprise Support" -Role
"Message Tracking" -RecipientRelativeWriteScope Organization
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе New-ManagementRoleAssignment.

Создание назначения роли с областью, основанной на фильтре получателей, с помощью командной консоли Exchange

Если вы создали область на основе фильтра получателей, необходимо включить область в команду, используемую для назначения роли группе ролей с помощью параметра *CustomRecipientWriteScope* .

Также можно включить область записи конфигурации при создании назначения роли с областью, основанной на фильтре получателей.

Дополнительные сведения о назначениях ролей и областях см. в следующих разделах:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

Используйте следующий синтаксис для назначения роли группе ролей с областью, основанной на фильтре получателей. Если имя назначения роли не задано, оно создается автоматически.

PowerShell

```
New-ManagementRoleAssignment -SecurityGroup <role group name> -Role <role name> -CustomRecipientWriteScope <role scope name>
```

В этом примере роль Message Tracking назначается группе ролей Seattle Recipient Admins, затем применяется область Seattle Recipients.

PowerShell

```
New-ManagementRoleAssignment -SecurityGroup "Seattle Recipient Admins" -Role "Message Tracking" -CustomRecipientWriteScope "Seattle Recipients"
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе New-ManagementRoleAssignment.

Создание назначения роли с областью конфигурации с помощью командной консоли Exchange

Если вы создали фильтр конфигурации сервера или базы данных или область на основе списка, необходимо включить область в команду, используемую для назначения роли группе ролей с помощью параметра *CustomConfigWriteScope* .

Также можно включить область записи получателей при создании назначения роли с областью, основанной на фильтре конфигураций.

Дополнительные сведения о назначениях ролей и областях управления см. в следующих разделах:

- Understanding Management Role Assignments
- Understanding Management Role Scopes

Используйте следующий синтаксис для назначения группе ролей роли с областью конфигурации. Если имя назначения роли не задано, оно создается автоматически.

PowerShell

```
New-ManagementRoleAssignment -SecurityGroup <role group name> -Role <role name> -CustomConfigWriteScope <role scope name>
```

В этом примере роль Databases назначается группе ролей Seattle Server Admins, затем применяется область Seattle Servers.

PowerShell

```
New-ManagementRoleAssignment -SecurityGroup "Seattle Server Admins" -Role "Databases" -CustomConfigWriteScope "Seattle Servers"
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе New-ManagementRoleAssignment.

Создание назначения роли с областью подразделения с помощью командной консоли Exchange

Если вы хотите ограничить область записи роли подразделением, можно указать подразделение в *параметре RecipientOrganizationalUnitScope* напрямую.

Область записи конфигурации. Определяет объекты сервера и организации, которые участники группы ролей могут изменять в exADNoMk.

- Understanding Management Role Assignments
- Understanding Management Role Scopes

Используйте приведенную ниже команду для назначения роли группе ролей и ограничения области записи роли определенным подразделением. Если имя назначения роли не задано, оно создается автоматически.

PowerShell

```
New-ManagementRoleAssignment -SecurityGroup <role group name> -Role <role name> -RecipientOrganizationalUnitScope <OU>
```

В этом примере роль Mail Recipients назначается группе ролей Seattle Recipient Admins, затем область действия этого назначения сужается до подразделения Sales\Users в домене Contoso.com.

PowerShell

```
New-ManagementRoleAssignment -SecurityGroup "Seattle Recipient Admins" -Role "Mail Recipients" -RecipientOrganizationalUnitScope contoso.com/sales/users
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе New-ManagementRoleAssignment.

Как проверить, все ли получилось?

Чтобы убедиться в успешном добавлении ролей в группу ролей, выполните следующие действия.

1. В EAC перейдите в **раздел Разрешения**>**Администратор Роли**.
2. Выберите группу ролей, в которую вы добавили роли. Убедитесь в наличии добавленных ролей на панели сведений группы ролей.

Удаление роли из группы ролей

Удаление роли из группы ролей управления является самым лучшим и простым способом отзыва разрешений, предоставленных группе администраторов или пользователей-специалистов. Если отсутствует необходимость в предоставлении администраторам или пользователям-специалистам разрешений на управление функцией, следует удалить роль управления из группы ролей управления,

управляющей разрешениями. После удаления роли члены группы ролей больше не имеют допуска к управлению функцией.

> ⓘ **Примечание**
>
> Некоторые группы ролей, например группа ролей "Управление организацией", ограничивают, какие роли можно удалить из группы ролей. Дополнительные сведения см. в статье **Understanding Management Role Groups**. > Если администратор является членом другой группы ролей, содержащей роли управления, предоставляющие разрешения на управление функцией, необходимо либо удалить администратора из других групп ролей, либо роль, предоставляющую разрешения на управление функцией, из других групп ролей.

Использование Центра администрирования Exchange для удаления роли управления из группы ролей

> ⓘ **Важно!**
>
> Вы не можете использовать EAC для удаления ролей из группы ролей, если вы использовали командную консоль Exchange для настройки нескольких областей или монопольных областей в группе ролей. Если вы настроили несколько областей или монопольных областей в группе ролей, необходимо использовать процедуры командной консоли Exchange далее в этом разделе, чтобы удалить роли из группы ролей. Дополнительные сведения об областях ролей управления см. в разделе **Understanding Management Role Scopes**.

1. В EAC перейдите в **раздел Разрешения**>**Администратор Роли**.
2. Выберите группу ролей, из которой нужно удалить роль, и нажмите кнопку **Изменить**.✎
3. В разделе **Роли** выберите роли, которые требуется удалить из группы ролей.
4. Когда удаление ролей из группы ролей завершено, нажмите кнопку **Сохранить**.

Удаление роли из группы ролей с помощью командной консоли Exchange

Можно удалить роли из группы ролей при получении назначения связанной роли управления с использованием командлета **Get-ManagementRoleAssignment** и последующей передачи назначения роли обратно в командлет **Remove-ManagementRoleAssignment**. Если вы не хотите одновременно удалить делегированные и регулярные назначения ролей, укажите параметр *Делегирование* , чтобы указать, нужно ли удалять обычные или делегированные назначения ролей.

Дополнительные сведения о стандартных и делегированных назначениях ролей см. в разделе Understanding Management Role Assignments.

В этой процедуре используется конвейеризация. Дополнительные сведения о конвейерной подготовке см. в разделе about_Pipelines.

Для удаления роли из группы ролей используйте следующий синтаксис.

PowerShell

```
Get-ManagementRoleAssignment -RoleAssignee <role group name> -Role <role
name> -Delegating <$true | $false> | Remove-ManagementRoleAssignment
```

В этом примере роль групп рассылки, позволяющая администраторам управлять группами рассылки, удаляется из группы ролей Seattle Recipient Administrators. Так как мы хотим удалить назначение ролей, предоставляющее разрешения на управление группами рассылки, параметр *Делегации* имеет значение `$False`, который возвращает только обычные назначения ролей.

PowerShell

```
Get-ManagementRoleAssignment -RoleAssignee "Seattle Recipient
Administrators" -Role "Distribution Groups" -Delegating $false | Remove-
ManagementRoleAssignment
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе Remove-ManagementRoleAssignment.

Как проверить, все ли получилось?

Чтобы убедиться в успешном удалении ролей из группы ролей, выполните следующие действия.

1. В EAC перейдите в **раздел Разрешения**>**Администратор Роли**.

2. Выберите группу ролей, из которой вы удалили роли. Убедитесь в отсутствии удаленных ролей на панели сведений группы ролей.

Изменение области группы ролей

Назначения ролей управления между группой ролей и ролью включают в себя области управления, определяющие объекты, которые будут доступны членам этой группы ролей. Можно изменять область записи в группе ролей и указывать, какие объекты разрешено создавать, изменять или удалять членам группы ролей. Невозможно изменить область чтения в группе ролей.

Exchange Server включает области, которые по умолчанию применяются к назначениям ролей, когда пользовательские области не создаются. Чтобы использовать настраиваемую область для назначения роли в группе ролей, необходимо сначала создать такую область. Дополнительные сведения о создании настраиваемых областей, являющемся сложной задачей, см. в разделе Create a Regular or Exclusive Scope.

Дополнительные сведения о областях и назначениях ролей управления в Exchange Server см. в следующих разделах:

- Understanding Management Role Scopes
- Understanding Management Role Assignments

Использование Центра администрирования Exchange для изменения области в группе ролей

При изменении области в группе ролей с помощью Центра администрирования Exchange фактически меняется область всех назначений ролей между этой группой и каждой назначенной для нее ролью управления. Чтобы изменить область определенных назначений ролей, необходимо использовать процедуры с применением командной консоли Exchange, описанные далее в этой статье.

> ⓘ **Важно!**
>
> Вы не можете использовать EAC для управления областями назначения ролей между ролями и группой ролей, если вы использовали командную консоль Exchange для настройки нескольких областей или монопольных областей для этих назначений ролей. Если вы настроили несколько областей или монопольных областей для этих назначений ролей, необходимо использовать

процедуры командной консоли Exchange далее в этом разделе для управления областями. Дополнительные сведения об областях ролей управления см. в разделе **Understanding Management Role Scopes**.

1. В EAC перейдите в **раздел Разрешения**>**Администратор Роли**.
2. Выберите группу ролей, в которой нужно изменить область, и нажмите кнопку **Изменить**.
3. Выберите один из двух следующих параметров для пункта **Область записи**.
   - Область записи из раскрывающегося списка, в котором можно выбрать область записи по умолчанию либо пользовательскую область записи.
   - **Подразделение**. Выберите этот параметр и укажите подразделение, если вы хотите ограничить эту группу ролей подразделением.
4. Нажмите кнопку **Сохранить**, чтобы сохранить изменения в группе ролей.

Изменение областей сразу для всех назначений ролей в группе ролей с помощью командной консоли Exchange

Для назначений ролей между группой ролей и назначенными ей ролями может использоваться неявная область, полученная на основе самих ролей, текущей настраиваемой области или других настраиваемых областей. Дополнительные сведения о назначениях ролей см. в разделе Understanding Management Role Assignments.

Управлять областями назначений ролей можно с помощью командлета **Set-ManagementRoleAssignment**. Невозможно управлять областями с помощью командлета **Set-RoleGroup**.

Чтобы изменить области всех назначений ролей между группой ролей и набором ролей управления одновременно, необходимо получить назначения ролей в группе ролей, а затем установить новую область для каждого назначения. Используйте командлет **Get-ManagementRoleAssignment**, чтобы получить назначения ролей и передать их по конвейеру командлету **Set-ManagementRoleAssignment**.

В этой процедуре используются понятия конвейерной обработки и переключателя *WhatIf* . Дополнительную информацию см. в следующих статьях:

- about_Pipelines
- WhatIf, Confirm, and ValidateOnly Switches

Чтобы установить область для всех назначений ролей в группе ролей одновременно, используйте следующую синтаксическую конструкцию.

PowerShell

```
Get-ManagementRoleAssignment -RoleAssignee <name of role group> | Set-
ManagementRoleAssignment -CustomRecipientWriteScope <recipient scope name> -
CustomConfigWriteScope <configuration scope name> -
RecipientRelativeScopeWriteScope < MyDistributionGroups | Organization |
Self> -ExclusiveRecipientWriteScope <exclusive recipient scope name> -
ExclusiveConfigWriteScope <exclusive configuration scope name> -
RecipientOrganizationalUnitScope <organizational unit>
```

Можно использовать только те параметры, которые требуются для настройки необходимой области. Например, чтобы изменить область получателя для всех назначений ролей в группе ролей «Управление получателями продаж» на «Сотрудники прямых продаж», используйте следующую команду.

PowerShell

```
Get-ManagementRoleAssignment -RoleAssignee "Sales Recipient Management" |
Set-ManagementRoleAssignment -CustomRecipientWriteScope "Direct Sales
Employees"
```

> ⓘ **Примечание**
>
> Вы можете использовать параметр *WhatIf* , чтобы убедиться, что изменяются только назначения ролей, которые вы хотите изменить. Выполните предыдущую команду с параметром *WhatIf* , чтобы проверить результаты, а затем удалите параметр *WhatIf* , чтобы применить изменения.

Дополнительные сведения об изменении назначений ролей управления см. в разделе Change a Role Assignment.

Дополнительные сведения о синтаксисе и параметрах см. в разделе Get-ManagementRoleAssignment.

Изменение области отдельных назначений ролей в группе ролей с помощью командной консоли

Exchange

Для назначений ролей между группой ролей и назначенными ей ролями может использоваться неявная область, полученная на основе самих ролей, текущей настраиваемой области или других настраиваемых областей. Дополнительные сведения о назначениях ролей см. в разделе Understanding Management Role Assignments.

Управлять областями назначений ролей можно с помощью командлета **Set-ManagementRoleAssignment**. Невозможно управлять областями с помощью командлета **Set-RoleGroup**.

В этой процедуре используется концепция конвейерной передачи и командлет **Format-List**. Дополнительную информацию см. в следующих статьях:

- about_Pipelines
- Working with Command Output

Чтобы изменить область назначения роли между группой ролей и ролью управления, необходимо найти имя назначения роли и установить область для назначения роли.

1. Чтобы найти имена всех назначений ролей группы ролей, используйте следующую команду. При передаче по конвейеру назначений ролей управления в командлет **Format-List** отображается полное имя назначения.

   PowerShell

   ```
   Get-ManagementRoleAssignment -RoleAssignee <role group name> | Format-List Name
   ```

2. Поиск имени назначения роли, которое необходимо изменить. Используйте имя назначения роли на следующем шаге.

3. Чтобы задать область отдельного назначения, используйте следующую синтаксическую конструкцию.

   PowerShell

   ```
   Set-ManagementRoleAssignment <role assignment name> -CustomRecipientWriteScope <recipient scope name> -CustomConfigWriteScope <configuration scope name> -RecipientRelativeScopeWriteScope < MyDistributionGroups | Organization | Self> -ExclusiveRecipientWriteScope <exclusive recipient scope name>
   ```

```
-ExclusiveConfigWriteScope <exclusive configuration scope name> -
RecipientOrganizationalUnitScope <organizational unit>
```

Можно использовать только те параметры, которые требуются для настройки необходимой области. Например, чтобы изменить область получателя для назначения роли «Управление получателями почты/продаж» на «Все сотрудники продаж», используйте следующую команду.

PowerShell

```
Set-ManagementRoleAssignment "Mail Recipients_Sales Recipient Management" -
CustomRecipientWriteScope "All Sales Employees"
```

Дополнительные сведения об изменении назначений ролей управления см. в разделе Change a Role Assignment.

Дополнительные сведения о синтаксисе и параметрах см. в разделе Set-ManagementRoleAssignment.

Как проверить, все ли получилось?

Чтобы убедиться в успешном изменении области назначения ролей для группы ролей, выполните следующие действия.

- Если с целью настройки области для группы ролей использовался Центр администрирования Exchange, выполните следующие действия.

    1. В EAC перейдите в **раздел Разрешения**>**Администратор Роли**. Здесь перечислены все группы ролей в организации.

    2. Выберите группу ролей, чтобы просмотреть настроенную для нее область.

- Если вы настраивали область применения группы ролей с помощью командной консоли Exchange, выполните указанные ниже действия.

    1. Выполните в командной консоли Exchange приведенную ниже команду.

        PowerShell

        ```
        Get-ManagementRoleAssignment -RoleAssignee <role group name> |
        Format-Table *WriteScope
        ```

2. Убедитесь, что область записи для назначений ролей была изменена на указанную область.

Добавление или удаление делегата группы ролей

Делегаты группы ролей — это пользователи или универсальные группы безопасности, которые могут добавлять или удалять членов из группы ролей или изменять ее свойства. Добавляя или удаляя делегатов группы ролей, можно управлять разрешениями на управление группой ролей.

> **ⓘ Важно!**
>
> После добавления делегата в группу ролей эта группа может управляться только делегатами группы или пользователями, которым напрямую или косвенно назначена роль управления ролями. > Если пользователю прямо или косвенно назначена роль "Управление ролями" и он не добавляется в качестве делегата группы ролей, он должен использовать параметр *BypassSecurityGroupManagerCheck* для командлетов **Add-RoleGroupMember**, **Remove-RoleGroupMember**, **Update-RoleGroupMember** и **Set-RoleGroup для** управления группой ролей.

> **ⓘ Примечание**
>
> Вы не можете использовать Центр администрирования Exchange для добавления делегата в группу ролей.

Добавление делегата в группу ролей с помощью командной консоли Exchange

Чтобы изменить список делегатов в группе ролей, используйте параметр *ManagedBy* в **командлете Set-RoleGroup** . Параметр *ManagedBy* перезаписывает весь список делегатов в группе ролей. При необходимости добавить делегатов в группу ролей вместо замены всего списка делегатов выполните следующие действия:

1. Сохраните группу ролей в переменной с помощью следующей команды.

```
PowerShell
```

```
$RoleGroup = Get-RoleGroup <role group name>
```

2. Добавьте делегата в группу ролей, сохраненную в переменной, используя следующую команду.

```
PowerShell

$RoleGroup.ManagedBy += (Get-User <user to add>).Identity
```

> ⓘ **Примечание**
>
> При необходимости добавить универсальную группу безопасности используйте командлет **Get-Group**.

3. Повторите шаг 2 для каждого делегата, которого необходимо добавить.

4. Примените новый список делегатов для текущей группы ролей с помощью следующей команды.

```
PowerShell

Set-RoleGroup <role group name> -ManagedBy $RoleGroup.ManagedBy
```

В этом примере в качестве делегата в группу ролей Управление организацией добавляется пользователь Сергей Озеров.

```
PowerShell

$RoleGroup = Get-RoleGroup "Organization Management"
$RoleGroup.ManagedBy += (Get-User "David Strome").Identity
Set-RoleGroup "Organization Management" -ManagedBy $RoleGroup.ManagedBy
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе Set-RoleGroup.

Удаление делегата из группы ролей с помощью командной консоли Exchange

Чтобы изменить список делегатов в группе ролей, используйте параметр *ManagedBy* в **командлете Set-RoleGroup** . Параметр *ManagedBy* перезаписывает весь список делегатов в группе ролей. При необходимости удалить делегатов из

группы ролей вместо замены всего списка делегатов выполните следующие действия:

1. Сохраните группу ролей в переменной с помощью следующей команды.

```
PowerShell

$RoleGroup = Get-RoleGroup <role group name>
```

2. Удалите делегата из группы ролей, сохраненной в переменной, используя следующую команду.

```
PowerShell

$RoleGroup.ManagedBy -= (Get-User <user to remove>).Identity
```

> ⓘ **Примечание**
>
> При необходимости удалить универсальную группу безопасности используйте командлет **Get-Group**.

3. Повторите шаг 2 для каждого делегата, которого необходимо удалить.

4. Примените новый список делегатов для текущей группы ролей с помощью следующей команды.

```
PowerShell

Set-RoleGroup <role group name> -ManagedBy $RoleGroup.ManagedBy
```

В этом примере в качестве делегата из группы ролей Управление организацией удаляется пользователь Сергей Озеров.

```
PowerShell

$RoleGroup = Get-RoleGroup "Organization Management"
$RoleGroup.ManagedBy -= (Get-User "David Strome").Identity
Set-RoleGroup "Organization Management" -ManagedBy $RoleGroup.ManagedBy
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе Set-RoleGroup.

Как проверить, все ли получилось?

Чтобы убедиться в успешном изменении списка делегатов для группы ролей, выполните следующие действия.

1. В командной консоли Exchange выполните приведенную ниже команду.

   PowerShell

   ```
   Get-RoleGroup <role group name> | Format-List ManagedBy
   ```

2. Убедитесь, что делегаты, перечисленные в свойстве *ManagedBy* , включают только делегатов, которые должны иметь возможность управлять группой ролей.

Управление членами группы ролей в Exchange Server

Статья • 30.05.2024

Дополнительные сведения о группах ролей в Exchange Server см. в статье Общие сведения о группах ролей управления.

Дополнительные сведения о задачах управления, связанных с группами ролей, см. в разделе Разрешения.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут
- Сведения об открытии центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Группы ролей" в разделе Разрешения для управления ролями .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Добавление членов в группу ролей

Чтобы предоставить пользователю разрешения, которые имеет группа ролей, необходимо добавить пользователя, универсальную группу безопасности (USG) либо другую группу ролей, к которой относится пользователь, в качестве члена группы ролей.

Использование Центра администрирования Exchange для добавления членов в группу ролей

1. В Центре администрирования Exchange перейдите к**разделу Роли администратораразрешений**>.
2. Выберите группу ролей, в которую нужно добавить участников, и нажмите кнопку **Изменить**.✏️
3. В разделе **Участники** нажмите кнопку **Добавить**➕
4. Выберите пользователей, универсальные группы безопасности или другие группы ролей для добавления в группу ролей, нажмите **Добавить**, а затем нажмите кнопку **OK**.
5. Нажмите кнопку **Сохранить**, чтобы сохранить изменения в группе ролей.

Добавление участников в группу ролей с помощью командной консоли Exchange

To add a role group member, see the Examples section in Add-RoleGroupMember.

To add multiple role group members or to replace the role group membership entirely, see the Examples section in Update-RoleGroupMember.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли добавлен один или несколько членов в группу ролей, выполните следующие действия.

1. В центре администрирования EAC перейдите к**разделу Роли администратораразрешений**>.
2. Выберите группу ролей, в которую добавлены члены.
3. Проверьте, указаны ли добавленные вами члены в области сведений группы ролей.

Удаление членов из группы ролей

Чтобы забрать у пользователя разрешения, предоставленные группой ролей, необходимо удалить пользователя или универсальную группу безопасности, членом которой является пользователь, из состава группы ролей.

Использование Центра администрирования Exchange для удаления членов из группы ролей

1. В центре администрирования EAC перейдите к**разделу Роли администратораразрешений**>.

2. Выберите группу ролей, из которой нужно удалить участников, и нажмите кнопку **Изменить**.✏️

3. В разделе **Участники** выберите участников, которые нужно удалить, щелкните **удалить**➖ а затем нажмите кнопку **Сохранить**.

Удаление участников из группы ролей с помощью командной консоли Exchange

To remove a role group member, see the Examples section in Remove-RoleGroupMember.

To remove multiple role group members or to replace the role group membership entirely, see the Examples section in Update-RoleGroupMember.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли удален один или несколько членов из группы ролей, выполните следующие действия.

1. В центре администрирования EAC перейдите к**разделу Роли администратораразрешений**>.

2. Выберите группу ролей, из которой вы удалили членов.

3. Проверьте, отсутствуют ли удаленные вами члены в области сведений группы ролей.

Просмотр членов группы ролей

Членам группы ролей предоставляются разрешения, обеспечиваемые ролями управления, которые назначены этой группе ролей. Чтобы увидеть, каким пользователям, универсальным группам безопасности или другим группам ролей предоставляет разрешения указанная группа ролей, можно просмотреть участников группы ролей.

Использование Центра администрирования Exchange для просмотра членов группы ролей

1. В центре администрирования EAC перейдите к**разделу Роли администратораразрешений**>.

2. Выберите группу ролей, членов которой нужно просмотреть.

3. Просмотрите членов в области сведений группы ролей.

Использование командной консоли Exchange для просмотра членов группы ролей

To view the members of a role group, see the "Examples" section in Get-RoleGroupMember.

Управление политиками назначения ролей в Exchange Server

Статья • 04.04.2023

Если следует настроить разрешения для группы пользователей, создайте новую пользовательскую политику назначения роли управления. Эта политика назначения может быть настроена для соответствия определенным требованиям пользователей. Дополнительные сведения о политиках назначения в Exchange Server см. в статье Общие сведения о политиках назначения ролей управления.

Ищете другие задачи управления, связанные с управлением разрешениями? См. сведения о разрешениях.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут
- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Политики назначений" в разделе Разрешения управления ролями .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Добавление политики назначения

После создания новой политики назначения можно назначить ей пользователей. Дополнительные сведения см. в разделе Изменение политики назначения для почтового ящика.

Создание политики назначения с помощью Центра администрирования Exchange

> ⓘ **Примечание**
>
> Вы можете создавать явные политики назначения только с помощью центра администрирования Exchange (EAC). Если вы хотите создать новую политику назначения по умолчанию, вы должны использовать командную консоль Exchange. Дополнительные сведения см. в разделе "Использование командной консоли Exchange для создания политики назначения по умолчанию" далее в этом разделе.

1. В EAC перейдите в раздел **Разрешения**>**Роли пользователей** и нажмите кнопку **Добавить**➕
2. В окне политики назначения роли введите имя новой политики назначения.
3. Установите флажок рядом с каждой ролью, которую необходимо добавить в политику назначения. Можно выбрать несколько ролей, в том числе добавленные роли конечных пользователей. При выборе роли с подчиненными ролями последние выбираются автоматически.
4. Нажмите кнопку **Сохранить**, чтобы сохранить изменения политики назначения.

Создание явной политики назначения с помощью командной консоли Exchange

Чтобы создать явную политику назначения, которая может быть вручную назначена почтовым ящикам, используйте следующий синтаксис.

PowerShell

```
New-RoleAssignmentPolicy <assignment policy name> -Roles <roles to assign>
```

В этом примере создается явное назначение политики ограниченного почтового ящика и назначаются `MyBaseOptions` роли , `MyAddressInformation` и `MyDisplayName` .

PowerShell

```
New-RoleAssignmentPolicy "Limited Mailbox Configuration" -Roles
MyBaseOptions, MyAddressInformation, MyDisplayName
```

Подробные сведения о синтаксисе и параметрах см. в разделе New-RoleAssignmentPolicy.

Создание стандартной политики назначения с помощью командной консоли Exchange

Чтобы создать политику назначения по умолчанию для новых ящиков, используйте следующий синтаксис.

PowerShell

```
New-RoleAssignmentPolicy <assignment policy name> -Roles <roles to assign> -IsDefault
```

В этом примере создается политика назначения по умолчанию с ограниченной конфигурацией почтовых `MyBaseOptions` ящиков и назначаются роли , `MyAddressInformation` и `MyDisplayName` .

PowerShell

```
New-RoleAssignmentPolicy "Limited Mailbox Configuration" -Roles
MyBaseOptions, MyAddressInformation, MyDisplayName -IsDefault
```

Подробные сведения о синтаксисе и параметрах см. в разделе New-RoleAssignmentPolicy.

Удаление политики назначения

Если политика назначения ролей управления больше не нужна, ее можно удалить.

Что нужно знать перед началом работы?

- Всем пользователей, которым назначена эта политика назначения, необходимо присвоить другую политику назначения. Дополнительные сведения об изменении политики назначений в почтовом ящике см. в разделе Изменение политики назначения в почтовом ящике.
- Необходимо удалить все назначения ролей управления между политикой назначения и назначенными ролями управления. Дополнительные сведения об удалении назначения роли из политики назначения см. в разделе Удаление роли из политики назначения далее в этом разделе.

- Если вы хотите удалить политику назначения по умолчанию, она должна быть последней политикой назначения в Exchange Server организации.

Удаление политики назначения с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел **Разрешения**>**Роли пользователей**.
2. Выберите политику назначений, которую нужно удалить, и нажмите кнопку **Удалить**🗑

Удаление политики назначения с помощью командной консоли Exchange

Чтобы удалить политику назначения, используйте следующий синтаксис.

```
PowerShell

Remove-RoleAssignmentPolicy <role assignment policy>
```

В данном примере удаляется политика назначения New York Temporary Users.

```
PowerShell

Remove-RoleAssignmentPolicy "New York Temporary Users"
```

Подробные сведения о синтаксисе и параметрах см. в разделе Remove-RoleAssignmentPolicy.

Просмотр списка политик назначения или сведений о политике назначения

Политики назначений ролей управления можно просматривать различными способами в зависимости от того, какие сведения необходимо получить, а также от того, что для этого используется — Центр администрирования Exchange или командная консоль Exchange.

В Центре администрирования Exchange можно просмотреть список политик назначения и роли, назначенные им. В командной консоли Exchange можно просмотреть все политики назначения в организации, список почтовых ящиков, для которых назначена определенная политика, а также другие сведения.

Просмотр списка политик назначения с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел **Разрешения**>**Роли пользователей**. Здесь перечислены все политики назначения в организации.
2. Чтобы просмотреть дополнительные сведения об определенной политике назначения, выберите политику для просмотра. Описание и роли, назначенные этой политике назначения, отобразятся в области сведений.

Просмотр списка политик назначения с помощью командной консоли Exchange

Можно просмотреть список всех политик назначений в организации, не указывая определенные политики назначений при запуске командлета **Get-RoleAssignmentPolicy**.

В этом разделе описывается использование конвейерной передачи и командлета **Format-Table**. Дополнительные сведения об этих понятиях см. в следующих разделах:

- about_Pipelines
- Working with Command Output

Чтобы получить список всех политик назначений в организации, используйте следующую команду.

PowerShell

```
Get-RoleAssignmentPolicy
```

Чтобы получить список с определенными свойствами для всех политик назначений в организации, можно передать конвейерным образом результаты в командлет **Format-Table** и указать свойства, которые будут включены в список результатов. Используйте следующий синтаксис.

PowerShell

```
Get-RoleAssignmentPolicy | Format-Table <property 1>, <property 2...>
```

В этом примере показано возвращение списка всех политик назначений в организации и включение таких свойств, как **Name** и **IsDefault**.

PowerShell

```
Get-RoleAssignmentPolicy | Format-Table Name, IsDefault
```

Дополнительные сведения о синтаксисе и параметрах см. в разделах Get-Mailbox или Get-RoleAssignmentPolicy.

Просмотр сведений об отдельной политике назначения с помощью командной консоли Exchange

Сведения об определенной политике назначения можно просмотреть с помощью конвейерной передачи выходных данных командлета **Get-RoleAssignmentPolicy** в командлет **Format-List**.

В этом разделе описывается использование конвейерной передачи и командлета **Format-List**. Дополнительные сведения об этих понятиях см. в следующих разделах:

- about_Pipelines
- Working with Command Output

Чтобы просмотреть сведения об определенной политике назначения, используйте следующую синтаксическую конструкцию.

PowerShell

```
Get-RoleAssignmentPolicy <assignment policy name> | Format-List
```

В этом примере показан просмотр сведений о политике назначения «Пользователи Редмонда» — нет текстовых сообщений.

PowerShell

```
Get-RoleAssignmentPolicy "Redmond Users - no Text Messaging" | Format-List
```

Дополнительные сведения о синтаксисе и параметрах см. в разделах Get-Mailbox или Get-RoleAssignmentPolicy.

Поиск стандартной политики назначения с помощью командной консоли Exchange

Можно выполнить поиск политики назначения по умолчанию путем конвейерной передачи выходных данных командлета **Get-RoleAssignmentPolicy** в командлет

Where. С помощью командлета **Where** отфильтруйте возвращаемые данные, чтобы отобразить только политику назначений, для которой свойству *IsDefault* присвоено значение `$True`.

В этой процедуре описывается использование конвейерной передачи и командлета **Where**. Дополнительные сведения об этих понятиях см. в следующих разделах:

- about_Pipelines
- Working with Command Output

В этом примере возвращается политика назначения по умолчанию.

PowerShell

```
Get-RoleAssignmentPolicy | Where {$_.IsDefault -eq $True}
```

Дополнительные сведения о синтаксисе и параметрах см. в разделах Get-Mailbox или Get-RoleAssignmentPolicy.

Просмотр почтовых ящиков, для которых назначена определенная политика, с помощью командной консоли Exchange

Можно выполнить поиск всех почтовых ящиков, для которых назначена определенная политика назначения, если передать по конвейеру выходные данные командлета **Get-Mailbox** в командлет **Where**. С помощью командлета **Where** отфильтруйте возвращаемые данные, чтобы отобразить только почтовые ящики, для которых свойству *RoleAssignmentPolicy присвоено* указанное имя политики назначения.

В этой процедуре описывается использование конвейерной передачи и командлета **Where**. Дополнительные сведения об этих понятиях см. в следующих разделах:

- about_Pipelines
- Working with Command Output

Используйте следующий синтаксис.

PowerShell

```
Get-Mailbox | Where {$_.RoleAssignmentPolicy -Eq "<role assignment policy>"}
```

В этом примере выполняется поиск всех почтовых ящиков, для которых назначена политика конечных пользователей Ванкувера.

PowerShell

```
Get-Mailbox | Where {$_.RoleAssignmentPolicy -Eq "Vancouver End Users"}
```

Дополнительные сведения о синтаксисе и параметрах см. в разделах Get-Mailbox или Get-RoleAssignmentPolicy.

Изменение стандартной политики назначения

Политику назначения ролей управления, назначаемую новым почтовым ящикам, можно изменять. Изменение политики назначения ролей по умолчанию не изменяет политику назначения, назначенную существующим почтовым ящикам. Сведения об изменении политики назначений, назначенной существующим почтовым ящикам, см. в статье Изменение политики назначения для почтового ящика.

> ⓘ **Примечание**
>
> Для изменения стандартной политики назначения невозможно использовать Центр администрирования Exchange. Необходимо использовать командную консоль Exchange.

Изменение стандартной политики назначения с помощью командной консоли Exchange

Чтобы изменить политику назначения по умолчанию, используйте следующий синтаксис.

PowerShell

```
Set-RoleAssignmentPolicy <assignment policy name> -IsDefault
```

В этом примере в качестве политики назначения по умолчанию задается политика «Пользователи Ванкувера».

PowerShell

```
Set-RoleAssignmentPolicy "Vancouver End Users" -IsDefault
```

> **ⓘ Важно!**
>
> Для новых почтовых ящиков задается политика назначения по умолчанию, даже если для нее не указаны роли управления. Если заданы политики назначения без указания ролей управления, доступ к функциям настроек почтовых ящиков в Outlook в Интернете невозможен.

Подробные сведения о синтаксисе и параметрах см. в разделе Set-RoleAssignmentPolicy.

Добавление роли к политике назначения

Добавление роли политики назначения с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел **Разрешения**>**Роли пользователей**.
2. Выберите политику назначений, в которую вы хотите добавить одну или несколько ролей, и нажмите кнопку **Изменить**.
3. Установите флажок рядом с каждой ролью, которую необходимо добавить в политику назначения. Можно выбрать несколько ролей, в том числе добавленные роли конечных пользователей. При выборе роли с подчиненными ролями последние выбираются автоматически.
4. Нажмите кнопку **Сохранить**, чтобы сохранить изменения политики назначения.

Добавление роли политики назначения с помощью командной консоли Exchange

Чтобы создать назначение роли управления между ролью и политикой назначения, используйте следующую синтаксическую конструкцию.

PowerShell

```
New-ManagementRoleAssignment -Name <role assignment name> -Role <role name>
-Policy <assignment policy name>
```

This example creates the role assignment Seattle Users - Voicemail between the MyVoicemail role and the Seattle Users assignment policy.

PowerShell

```
New-ManagementRoleAssignment -Name "Seattle Users - Voicemail" -Role
MyVoicemail -Policy "Seattle Users"
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе New-ManagementRoleAssignment.

Удаление роли из политики назначения

Если не нужно, чтобы пользователям предоставлялись разрешения на управление определенными функциями их почтовых ящиков или групп рассылки, можно удалить роль управления, предоставляющую эти разрешения, из политики назначения ролей управления, которая задана для этих пользователей. Если для других пользователей задана эта же политика назначения, они также лишаются возможности управлять этими функциями.

Удаление роли из политики назначения с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел **Разрешения**>**Роли пользователей**.
2. Выберите политику назначений, из которой нужно удалить одну или несколько ролей, а затем щелкните **Изменить**.
3. Снимите флажок рядом с ролями, которые требуется удалить из политики назначения. Если снять флажок для роли, у которой есть дочерние роли, флажки для этих дочерних ролей также снимаются.
4. Нажмите кнопку **Сохранить**, чтобы сохранить изменения политики назначения.

Удаление роли из политики назначения с помощью командной консоли Exchange

Для удаления ролей из политик назначения можно извлечь связанное назначение ролей управления при помощи командлета **Get-ManagementRoleAssignment** и

затем выполнить конвейерную передачу возвращенного назначения роли в командлет **Remove-ManagementRoleAssignment**.

Дополнительные сведения о стандартных и делегированных назначениях ролей см. в разделе Understanding Management Role Assignments.

В этой процедуре используется конвейеризация. Дополнительные сведения о конвейерной подготовке см. в разделе about_Pipelines.

Чтобы удалить роль из политики назначения, используйте указанный ниже синтаксис.

PowerShell

```
Get-ManagementRoleAssignment -RoleAssignee <assignment policy name> -Role
<role name> | Remove-ManagementRoleAssignment
```

Этот пример кода удаляет роль управления MyVoicemail, разрешающую пользователям управлять параметрами их голосовой почты, из политики назначения Seattle Users.

PowerShell

```
Get-ManagementRoleAssignment -RoleAssignee "Seattle Users" -Role MyVoicemail
| Remove-ManagementRoleAssignment
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе Remove-ManagementRoleAssignment.

Exchange Server. Изменение политики назначений в почтовом ящике

Статья • 04.04.2023

При изменении политики назначения роли управления почтового ящика изменения вступают в силу, как только пользователь обновляет соединение, например, при следующем входе в почтовый ящик или при открытии страницы параметров почтового ящика. Дополнительные сведения о политиках назначения в Exchange Server см. в статье Общие сведения о политиках назначения ролей управления.

Ищете другие задачи управления, связанные с разрешениями? См. сведения о разрешениях.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Группы ролей" в разделе Разрешения для управления ролями .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование центра администрирования Exchange для изменения политики назначения для почтового ящика

1. В Центре администрирования Exchange перейдите в раздел **Почтовые ящики получателей**>.

2. Выберите почтовый ящик пользователя или ресурса, в который нужно изменить политику назначений, и нажмите кнопку **Изменить**.

3. Выберите вкладку **Функции почтового ящика**.

4. В списке **Политика назначения ролей** выберите политику назначения ролей, которую необходимо назначить почтовому ящику, и нажмите на кнопку **Сохранить**.

Изменение политики назначения в почтовом ящике с помощью командной консоли Exchange

Для изменения политики назначения для почтового ящика используйте следующую синтаксическую конструкцию.

PowerShell

```
Set-Mailbox <mailbox alias or name> -RoleAssignmentPolicy <assignment
policy>
```

В этом примере задается политика назначения для инженерных пользователей в почтовом ящике Brian.

PowerShell

```
Set-Mailbox Brian -RoleAssignmentPolicy "Engineering Users"
```

Использование командной консоли Exchange для изменения политики назначения для группы почтовых ящиков, назначенных определенной политике назначения

> ⓘ **Примечание**
>
> Нельзя использовать центр администрирования Exchange для одновременного изменения политики назначения для группы почтовых ящиков.

В этой процедуре используется конвейерная передача, командлет **Where** и параметр *WhatIf*. Дополнительные сведения об этих понятиях см. в следующих разделах:

- about_Pipelines
- Working with Command Output
- WhatIf, Confirm, and ValidateOnly Switches

Для изменения политики назначения для группы почтовых ящиков с определенной политикой назначения используйте следующую синтаксическую конструкцию.

PowerShell

```
Get-Mailbox | Where {$_.RoleAssignmentPolicy -Eq "<assignment policy to
find>"} | Set-Mailbox -RoleAssignmentPolicy <assignment policy to set>
```

В данном примере выполняется поиск всех почтовых ящиков с политикой назначения "Пользователи Редмонда — Без голосовой почты" и изменение политики назначения на "Пользователи Редмонда — Голосовая почта включена".

PowerShell

```
Get-Mailbox | Where {$_.RoleAssignmentPolicy -Eq "Redmond Users - No
Voicemail"} | Set-Mailbox -RoleAssignmentPolicy "Redmond Users - Voicemail
Enabled"
```

Этот пример включает параметр *WhatIf* , чтобы можно было просмотреть все почтовые ящики, которые будут изменены без фиксации каких-либо изменений.

PowerShell

```
Get-Mailbox | Where {$_.RoleAssignmentPolicy -Eq "Redmond Users - No
Voicemail"} | Set-Mailbox -RoleAssignmentPolicy "Redmond Users - Voicemail
Enabled" -WhatIf
```

Дополнительные сведения о синтаксисе и параметрах см. в разделах Get-Mailbox или Set-Mailbox.

Разрешения функций в Exchange Server

Статья • 04.04.2023

Разрешения в Microsoft Exchange Server управляются с помощью модели разрешений на основе ролей контроль доступа (RBAC). В следующих разделах определены группы ролей управления, необходимые для администрирования функций, связанных с каждой функциональной областью в Exchange Server.

- Разрешения управления ролями
- Политика обмена сообщениями и соответствие требованиям в Exchange Server
- Разрешения для защиты от нежелательной почты и вредоносных программ
- Разрешения потока обработки почты
- Разрешения получателей
- Разрешения для электронных адресов и адресных книг
- Разрешения на общий доступ и совместную работу
- Разрешения клиентов и мобильных устройств
- Разрешения единой системы обмена сообщениями
- Разрешения высокого уровня доступности и устойчивости сайта
- Инфраструктура Exchange и разрешения PowerShell
- Разрешения работоспособности и производительности сервера

Разрешения управления ролями в Exchange Server

Статья • 04.04.2023

Разрешения, необходимые для выполнения задач по настройке ролей управления, зависят от выполняемой процедуры или запускаемого командлета. Дополнительные сведения о ролях управления см. в разделе Understanding Management Roles.

Для поиска разрешений, необходимых для выполнения процедуры или запуска командлета, выполните следующие действия.

1. Для поиска разрешений, необходимых для выполнения процедуры или запуска командлета, выполните следующие действия.

2. После этого проверьте разрешения, необходимые для функции. Вы должны быть участником одной из этих групп ролей, равнозначной настраиваемой группы ролей или равнозначной роли управления. Вы также можете щелкнуть группу ролей, чтобы просмотреть ее роли управления. Если для функции указано несколько групп ролей, то для ее использования достаточно относиться к одной из этих групп. Дополнительные сведения о группах ролей и ролях управления см. в разделе Understanding Role Based Access Control.

3. Запустите командлет **Get-ManagementRoleAssignment**, чтобы просмотреть назначенные группы ролей или роли управления и проверить наличие необходимых разрешений для управления функцией.

   > ⓘ **Примечание**
   >
   > Для запуска командлета **Get-ManagementRoleAssignment** вам должна быть назначена роль управления "Управление ролями". Если для запуска командлета **Get-ManagementRoleAssignment** отсутствуют необходимые разрешения, попросите администратора Exchange назначить группы ролей или роли управления.

Дополнительные сведения о делегировании возможности управления другим пользователям см. в разделе Назначения роли делегата.

Разрешения на управление ролями

Компоненты, указанные в следующей таблице, можно использовать для управления группами ролей управления, ролями, политиками назначения, назначениями, областями, определяющими разрешения, которые можно назначить администраторам и пользователям. Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Возможность	**Необходимы разрешения**
Роли управления	Управление организацией
Роли управления с незаданной областью	Роль управления Unscoped Role Management
Группы ролей	Управление организацией
Политики назначения	Управление организацией
Назначения ролей	Управление организацией
Области управления	Управление организацией
Записи ролей управления	Управление организацией
Устаревшие разрешения	Управление организацией
Разделенные разрешения Active Directory	Управление организацией **Важно!** Чтобы выполнить `setup.exe` команду с *параметрами PrepareAD* и *ActiveDirectorySplitPermissions* , используемая учетная запись должна быть членом групп "Администраторы схемы" и "Администраторы предприятия".

Политика обмена сообщениями и разрешения на соответствие требованиям в Exchange Server

Статья • 04.04.2023

Разрешения, необходимые для настройки политики обмена сообщениями и соответствия требованиям, отличаются в зависимости от выполняемой процедуры или используемого командлета. Дополнительные сведения о политике обмена сообщениями и соответствии требованиям см. в статье Политика обмена сообщениями и соответствие требованиям в Exchange Server.

Некоторые функции, которыми необходимо управлять, могут находиться на пограничных транспортных серверах. Для управления функциями на пограничных транспортных серверах необходимо стать участником локальной группы администраторов пограничного транспортного сервера, которым требуется управлять. На пограничном транспортном сервере не используется управление доступом на основе ролей (RBAC). Для функций, которыми можно управлять на пограничных транспортных серверах, столбец "Требуемые разрешения" в следующей таблице содержит запись "Локальный администратор пограничного транспортного сервера".

1. Для поиска разрешений, необходимых для выполнения процедуры или запуска командлета, выполните следующие действия.

2. После этого проверьте разрешения, необходимые для функции. Вы должны быть участником одной из этих групп ролей, равнозначной настраиваемой группы ролей или равнозначной роли управления. Вы также можете щелкнуть группу ролей, чтобы просмотреть ее роли управления. Если для функции указано несколько групп ролей, то для ее использования достаточно относиться к одной из этих групп. Дополнительные сведения о группах ролей и ролях управления см. в разделе Understanding Role Based Access Control.

3. Запустите командлет **Get-ManagementRoleAssignment**, чтобы просмотреть назначенные группы ролей или роли управления и проверить наличие необходимых разрешений для управления функцией.

   > ⓘ **Примечание**
   >
   > Для запуска командлета **Get-ManagementRoleAssignment** вам должна быть назначена роль управления "Управление ролями". Если для запуска

> командлета **Get-ManagementRoleAssignment** отсутствуют необходимые разрешения, попросите администратора Exchange назначить группы ролей или роли управления.

Дополнительные сведения о делегировании возможности управления другим пользователям см. в разделе Назначения роли делегата.

Разрешения соответствия требованиям и политики обмена сообщениями

Для настройки политики обмена сообщениями и соответствия требованиям можно использовать компоненты, приведенные в следующей таблице. Также приведен список групп ролей, которые требуются для настройки каждого компонента.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе View-Only Organization Management.

Возможность	**Необходимые разрешения**
Предотвращение потери данных (DLP)	Управление соответствием требованиям
Удаление содержимого почтового ящика (с помощью командлета Search-Mailbox с параметром *DeleteContent*)	Управление обнаружением**и** Mailbox Import Export Role **Примечание.** По умолчанию роль экспорта импорта почтовых ящиков не назначается ни одной группе ролей. Вы можете назначить роль управления встроенной или пользовательской группе ролей, пользователю или универсальной группе безопасности. Рекомендуется назначать роль группе ролей. Подробнее см. в разделе Добавление роли в группу ролей.
Создание почтовых ящиков обнаружения	Управление организацией Управление получателями
Управления правами на доступ к данным, настройка	Управление соответствием требованиям Управление организацией

Возможность	Необходимые разрешения
Архивация на месте	Управление организацией Управление получателями
Архивация на месте — проверка подключения	Управление организацией Управление сервером
Обнаружение электронных данных на месте	Discovery Management **Примечание**. По умолчанию группа ролей "Управление обнаружением" не содержит членов. Ни у каких пользователей, в том числе администраторов, нет необходимых разрешений на поиск в почтовых ящиках. Дополнительные сведения см. в статье Назначение разрешений на обнаружение электронных данных в Exchange Server.
Хранение на месте	Discovery Management Управление организацией **Примечания.** • Чтобы создать удержание на месте на основе запроса, пользователю необходимо назначить роли поиска в почтовых ящиках и удержания по юридическим причинам (напрямую или через членство в группе ролей, которой назначены обе роли). Чтобы создать удержание на месте, не используя запрос, который помещает все элементы почтового ящика на удержание, необходимо назначить роль удержания по юридическим причинам. Группе ролей управления обнаружением назначены обе роли. • Группе ролей "Управление организацией" назначена роль удержания по юридическим причинам. Члены группы ролей управления организацией могут применить удержание на месте для всех элементов в почтовом ящике, но не могут создать удержание на месте на основе запроса.
Ведение журнала	Управление организацией Управление записями
Хранение для судебного разбирательства	Управление организацией
Ведение журнала аудита почтовых ящиков	Управление организацией Управление записями

Возможность	Необходимые разрешения
Классификации сообщений	Управление организацией
Управление записями сообщений	Управление соответствием требованиям Управление организацией Управление записями
Политики хранения — применение	Управление организацией Управление получателями Управление записями
Создание политик хранения	См. раздел, посвященный управлению записями сообщений
Правила потока обработки почты (также известные как правила транспорта)	Управление организацией Управление записями

Разрешения для защиты от нежелательной почты и вредоносных программ

Статья • 04.04.2023

Разрешения, необходимые для выполнения задач, связанных с антиспамом и антивредоносным ПО, зависят от выполняемой процедуры или командлета, который вы хотите запустить. Дополнительные сведения о функциях транспорта см. в разделе Поток обработки почты и конвейер транспорта.

В этом разделе перечислены разрешения, необходимые для управления функциями потока обработки почты в Microsoft Exchange Server.

Некоторые функции, которыми необходимо управлять, могут находиться на пограничных транспортных серверах. Для управления функциями на пограничных транспортных серверах необходимо стать участником локальной группы администраторов пограничного транспортного сервера, которым требуется управлять. На пограничном транспортном сервере не используется управление доступом на основе ролей (RBAC). Для функций, которыми можно управлять на пограничных транспортных серверах, столбец "Требуемые разрешения" в следующей таблице содержит запись "Локальный администратор пограничного транспортного сервера".

1. Для поиска разрешений, необходимых для выполнения процедуры или запуска командлета, выполните следующие действия.

2. После этого проверьте разрешения, необходимые для функции. Вы должны быть участником одной из этих групп ролей, равнозначной настраиваемой группы ролей или равнозначной роли управления. Вы также можете щелкнуть группу ролей, чтобы просмотреть ее роли управления. Если для функции указано несколько групп ролей, то для ее использования достаточно относиться к одной из этих групп. Дополнительные сведения о группах ролей и ролях управления см. в разделе Understanding Role Based Access Control.

3. Запустите командлет **Get-ManagementRoleAssignment**, чтобы просмотреть назначенные группы ролей или роли управления и проверить наличие необходимых разрешений для управления функцией.

   > ⓘ **Примечание**

Для запуска командлета **Get-ManagementRoleAssignment** вам должна быть назначена роль управления "Управление ролями". Если для запуска командлета **Get-ManagementRoleAssignment** отсутствуют необходимые разрешения, попросите администратора Exchange назначить группы ролей или роли управления.

Дополнительные сведения о делегировании возможности управления другим пользователям см. в разделе Назначения роли делегата.

Примечание

Некоторые функции, которыми необходимо управлять, могут находиться на пограничных транспортных серверах. Для управления функциями на пограничных транспортных серверах необходимо стать участником локальной группы администраторов пограничного транспортного сервера, которым требуется управлять. На пограничном транспортном сервере не используется управление доступом на основе ролей (RBAC). Для функций, которыми можно управлять на пограничных транспортных серверах, столбец "Требуемые разрешения" в следующей таблице содержит запись "Локальный администратор пограничного транспортного сервера".

Примечание

Для использования некоторых функций требуются разрешения локального администратора сервера, которым необходимо управлять. Для управления этими функциями необходимо быть участником локальной группы администраторов этого сервера.

Разрешения для защиты от вредоносных программ и защиты от вредоносных программ

Функции, приведенные в следующих таблицах, можно использовать для настройки параметров защиты от нежелательной и вредоносной программы в организации. Также перечислены разрешения, необходимые для настройки каждого компонента.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию компонентов, приведенных в следующей таблице. Дополнительные сведения см. в разделе Управление организацией с правами только на просмотр.

Возможность	**Необходимые разрешения**
Защита от вредоносных программ	Управление организацией Управление санацией
Функции защиты от нежелательной гаммы	Управление организацией Управление санацией
Функции защиты от нежелательной проверки — пограничный транспорт	Локальный администратор на пограничном транспортном сервере

Разрешения потока обработки почты в Exchange Server

Статья • 04.04.2023

Разрешения, необходимые для выполнения задач, связанных с потоком обработки почты, отличаются в зависимости от выполняемой процедуры или командлета, который нужно запустить. Дополнительные сведения о функциях транспорта см. в разделе Поток обработки почты и конвейер транспорта.

В этом разделе перечислены разрешения, необходимые для управления функциями потока обработки почты в Exchange Server 2016 г. и Exchange Server 2019 г. Сведения о том, как разрешения Microsoft 365 или Office 365 связаны с разрешениями Exchange, см. в разделе Сведения о ролях администратора.

Некоторые функции, которыми необходимо управлять, могут находиться на пограничных транспортных серверах. Для управления функциями на пограничных транспортных серверах необходимо стать участником локальной группы администраторов пограничного транспортного сервера, которым требуется управлять. На пограничном транспортном сервере не используется управление доступом на основе ролей (RBAC). Для функций, которыми можно управлять на пограничных транспортных серверах, столбец "Требуемые разрешения" в следующей таблице содержит запись "Локальный администратор пограничного транспортного сервера".

1. Для поиска разрешений, необходимых для выполнения процедуры или запуска командлета, выполните следующие действия.

2. После этого проверьте разрешения, необходимые для функции. Вы должны быть участником одной из этих групп ролей, равнозначной настраиваемой группы ролей или равнозначной роли управления. Вы также можете щелкнуть группу ролей, чтобы просмотреть ее роли управления. Если компонент содержит несколько групп ролей, вам необходимо назначить только одну из групп ролей, чтобы использовать эту функцию. Дополнительные сведения о группах ролей и ролях управления см. в разделе Understanding Role Based Access Control.

3. Запустите командлет **Get-ManagementRoleAssignment**, чтобы просмотреть назначенные группы ролей или роли управления и проверить наличие необходимых разрешений для управления функцией.

> **Примечание**
>
> Для запуска командлета **Get-ManagementRoleAssignment** вам должна быть назначена роль управления "Управление ролями". Если для запуска командлета **Get-ManagementRoleAssignment** отсутствуют необходимые разрешения, попросите администратора Exchange назначить группы ролей или роли управления.

Дополнительные сведения о делегировании возможности управления другим пользователям см. в разделе Назначения роли делегата.

> **Примечание**
>
> Некоторые функции, которыми необходимо управлять, могут находиться на пограничных транспортных серверах. Для управления функциями на пограничных транспортных серверах необходимо стать участником локальной группы администраторов пограничного транспортного сервера, которым требуется управлять. На пограничном транспортном сервере не используется управление доступом на основе ролей (RBAC). Для функций, которыми можно управлять на пограничных транспортных серверах, столбец "Требуемые разрешения" в следующей таблице содержит запись "Локальный администратор пограничного транспортного сервера".

> **Примечание**
>
> Для использования некоторых функций требуются разрешения локального администратора сервера, которым необходимо управлять. Для управления этими функциями необходимо быть участником локальной группы администраторов этого сервера.

Разрешения потока обработки почты

Чтобы настроить параметры потока обработки почты в службах транспорта (в том числе переднего плана и почтовых ящиков) на серверах почтовых ящиков и пограничных транспортных серверах, используйте компоненты, приведенные в таблице ниже. Также перечислены разрешения, необходимые для настройки каждого компонента.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию компонентов, приведенных в следующей таблице. Дополнительные сведения см. в разделе Управление организацией с правами только на просмотр.

Серверы почтовых ящиков

Возможность	**Необходимые разрешения**
Обслуживаемые домены	Управление организацией
Управление сайтом Active Directory и ссылками сайта	Управление организацией
Функции защиты от нежелательной гаммы	Управление организацией Управление санацией
Обновления антиспамов	Управление организацией Управление санацией
Управление сертификатами	Управление организацией
Соединители агента доставки	Управление организацией Управление сервером
Уведомления о доставке	Управление организацией
Edgesync	Управление организацией
Внешние соединители	Управление организацией
Транспортная служба переднего плана	Управление организацией Управление сервером Управление санацией

Возможность	Необходимые разрешения
Ведение журнала	Управление организацией Управление записями
Доступ к почтовому ящику	Управление организацией
Конфигурация нежелательной почты почтовых ящиков	Управление организацией Управление записями Управление получателями Служба поддержки
Транспортная служба почтовых ящиков	Управление организацией Управление сервером Управление санацией
Подсказки	Управление организацией
Классификации сообщений	Управление организацией Управление записями
Отслеживание сообщений	Управление организацией Управление записями Управление получателями
Управляемый транспорт	Управление организацией Управление получателями
Очереди	Управление организацией Управление сервером

Возможность	Необходимые разрешения
Соединители приема	Управление организацией Управление сервером Управление санацией
Удаленные домены	Управление организацией
Объединение списков надежных отправителей	Управление организацией Управление записями
Соединители отправки	Управление организацией
Теневая избыточность	Управление организацией
Проверка потока почты	Управление организацией Управление сервером
Тестирование обработки правила потока обработки (также известного как правило транспорта)	Управление организацией
Агенты транспорта	Управление организацией Управление записями
Конфигурация транспорта	Управление организацией
Журналы транспорта	Управление организацией Управление сервером
Правила потока обработки почты (также известные как правила транспорта)	Управление организацией Управление записями

Возможность	Необходимые разрешения
служба передачи	Управление организацией Управление сервером Управление санацией
Домены X.400	Управление организацией

Пограничные транспортные серверы

Возможность	Необходимые разрешения
Обслуживаемые домены — пограничный транспортный сервер	Локальный администратор на пограничном транспортном сервере
Переопределение адресов — пограничный транспорт	Локальный администратор на пограничном транспортном сервере
Пограничный транспортный сервер	Локальный администратор на пограничном транспортном сервере
EdgeSync — пограничный транспортный сервер	Локальный администратор на пограничном транспортном сервере
Очереди — пограничный транспортный сервер	Локальный администратор на пограничном транспортном сервере
Соединители приема — пограничный транспортный сервер	Локальный администратор на пограничном транспортном сервере
Соединители отправки — пограничный транспортный сервер	Локальный администратор на пограничном транспортном сервере
Конфигурация транспорта — пограничный транспортный сервер	Локальный администратор на пограничном транспортном сервере

Возможность	Необходимые разрешения
Журналы транспорта — пограничный транспортный сервер	Локальный администратор на пограничном транспортном сервере
Правила потока обработки почты (также известные как правила транспорта) — пограничный транспорт	Локальный администратор на пограничном транспортном сервере

Разрешения получателей в Exchange Server

Статья • 14.08.2024

Разрешения, необходимые для выполнения задач по управлению получателями, зависят от выполняемой процедуры или запускаемого командлета.

Для поиска разрешений, необходимых для выполнения процедуры или запуска командлета, выполните следующие действия.

1. Для поиска разрешений, необходимых для выполнения процедуры или запуска командлета, выполните следующие действия.

2. После этого проверьте разрешения, необходимые для функции. Вы должны быть участником одной из этих групп ролей, равнозначной настраиваемой группы ролей или равнозначной роли управления. Вы также можете щелкнуть группу ролей, чтобы просмотреть ее роли управления. Если компонент содержит несколько групп ролей, вам необходимо назначить только одну из групп ролей, чтобы использовать эту функцию. Дополнительные сведения о группах ролей и ролях управления см. в разделе Understanding Role Based Access Control.

3. Запустите командлет **Get-ManagementRoleAssignment**, чтобы просмотреть назначенные группы ролей или роли управления и проверить наличие необходимых разрешений для управления функцией.

   > 7 **Примечание**
   >
   > Для запуска командлета **Get-ManagementRoleAssignment** вам должна быть назначена роль управления "Управление ролями". Если для запуска командлета **Get-ManagementRoleAssignment** отсутствуют необходимые разрешения, попросите администратора Exchange назначить группы ролей или роли управления.

Дополнительные сведения о делегировании возможности управления другим пользователям см. в разделе Назначения роли делегата.

Разрешения для сервера почтовых ящиков

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Развернуть таблицу

Возможность	Необходимые разрешения
Восстановление календаря, конфигурации сервера	Управление организацией Управление сервером
Делегирование серверов почтовых ящиков	Управление организацией
Политики адресов электронной почты	Управление организацией Управление сервером
Служба поиска Exchange	Organization Management View-Only Organization Management Server Management
Служба поиска Exchange — диагностика	Organization Management View-Only Organization Management Роль поддержки диагностики **Примечание.** Роль диагностика поддержки не назначается группе ролей. Подробнее см. в разделе Добавление роли в группу ролей.
Групповые метрики	Управление организацией Управление сервером
Импорт и экспорт	Роль импорта и экспорта почтовых ящиков **Примечание.** Роль экспорта импорта почтовых ящиков не назначается группе ролей. Подробнее см. в разделе Mailbox Import Export Role.
Помощники по обслуживанию почтовых ящиков	Управление организацией Управление сервером
Перемещение почтовых ящиков	Управление организацией Управление получателями
Восстановление почтового ящика	Управление организацией
Запрос на исправление почтового ящика	Управление организацией Управление сервером Управление получателями

Возможность	Необходимые разрешения
Запрос на восстановление почтового ящика	Управление организацией
Конфигурация сервера почтовых ящиков	Управление организацией Управление сервером
Управление службой индексатора поиска Exchange на сервере почтовых ящиков	Локальный администратор на сервере почтовых ящиков
Подключение MAPI	Управление организацией Управление сервером
Виртуальные каталоги автономной адресной книги	Управление организацией Управление сервером
Удаление почтового ящика хранилища	Управление организацией Управление сервером

Разрешения на общий доступ к календарю

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Развернуть таблицу

Возможность	Необходимые разрешения
Конфигурация календаря	Управление организацией Управление получателями Служба поддержки
Диагностика календаря	Управление организацией Управление записями Управление санацией Управление соответствием требованиям Служба поддержки
Обработка календаря	Управление организацией Управление получателями Служба поддержки
Уведомления	Управление организацией Управление получателями

Возможность	Необходимые разрешения
Связи организации	Управление организацией
Политики общего доступа	Управление организацией

Разрешения на изменение настроек почтового ящика ресурса

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Развернуть таблицу

Возможность	Необходимые разрешения
Политики резервирования	Управление организацией Управление получателями Служба поддержки
Делегирование	Управление организацией Управление получателями
Конфигурация схемы почтового ящика ресурса	Управление организацией

Разрешения для базы данных почтовых ящиков

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Развернуть таблицу

Возможность	Необходимые разрешения
Базы данных почтовых ящиков	Управление организацией Управление сервером

Разрешения на подготовку получателей

В этой таблице содержатся различные разрешения, которые требуются для управления получателями.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Развернуть таблицу

Возможность	Необходимые разрешения
Список адресов, глобальный список адресов	Управление организацией
Антиспам	Управление организацией Управление получателями
Приложения для Outlook	Organization Management View-Only Organization Management Help Desk
Применение политик общего доступа	Управление организацией Управление получателями
Арбитраж	Управление организацией
Возможность подключения к архиву	Organization Management View-Only Organization Management Server Management
Назначение автономных адресных книг	Управление организацией Управление получателями
Автоматические ответы	Управление организацией Управление получателями Служба поддержки
Конфигурация календаря	Управление организацией Управление получателями
Восстановление календаря	Управление организацией Управление получателями
Параметры объединения контактов	Управление организацией Recipient Management

Возможность	Необходимые разрешения
	View-Only Organization Management
Преобразование почтовых ящиков	Управление организацией Управление получателями
Отключенные почтовые ящики	Управление организацией Управление получателями Служба поддержки
Группы рассылки	Управление организацией Управление получателями
Динамические группы рассылки	Управление организацией Управление получателями
Адреса электронной почты	Управление организацией Управление получателями Управление единой системой обмена сообщениями
Правила для папки "Входящие"	Управление организацией Управление получателями Служба поддержки
Почтовые контакты	Управление организацией Управление получателями
Советы по использованию электронной почты	Управление организацией Управление получателями
Пользователь почты	Управление организацией Управление получателями
Разрешения для папки почтового ящика	Управление организацией Управление получателями Служба поддержки
Папки почтового ящика	Управление организацией Управление получателями
Подключение MAPI	Управление организацией
Конфигурация сообщения	Управление организацией Управление получателями Служба поддержки
Квоты сообщений	Управление организацией Управление получателями

Возможность	Необходимые разрешения
Контроль	Управление организацией Управление получателями
Разрешения и делегирование	Управление организацией
Архивные почтовые ящики	Управление организацией Управление получателями
Свойства данных получателя	Управление организацией Управление получателями
Удаленные почтовые ящики	Управление организацией Управление получателями
Хранение и юридические удержания	Управление организацией Управление получателями Управление записями
Отправить как	Управление организацией Управление получателями
Конфигурация проверки орфографии	Управление организацией Управление получателями Служба поддержки
Единая система обмена сообщениями (в Exchange 2016; недоступна в Exchange 2019)	Управление организацией Управление единой системой обмена сообщениями
Почтовые ящики пользователей	Управление организацией Управление получателями
Фотографии пользователя	Управление организацией Управление получателями Служба поддержки

Разрешения на перемещение и миграцию почтовых ящиков

Таблица содержит разрешения, которые требуются для переноса локальных почтовых ящиков в разных доменах или лесах, а также для миграции локальных почтовых ящиков в организации на основе облака.

Развернуть таблицу

Возможность	Необходимые разрешения
Перемещение почтовых ящиков (локально или между лесами)	Управление организацией Управление получателями
Перемещение почтовых ящиков (гибридное развертывание)	Управление организацией Управление получателями
Миграция (в облако и из облака)	Управление организацией Управление получателями

Email разрешения на адресную книгу и адресную книгу в Exchange Server

Статья • 04.04.2023

Разрешения, требуемые для настройки адреса электронной почты и адресной книги зависят от выполняемой процедуры или используемого командлета. Дополнительные сведения об адресах электронной почты и адресных книгах см. в разделе Email адреса и адресные книги в Exchange Server.

Некоторые функции, которыми необходимо управлять, могут находиться на пограничных транспортных серверах. Для управления функциями на пограничных транспортных серверах необходимо стать участником локальной группы администраторов пограничного транспортного сервера, которым требуется управлять. На пограничном транспортном сервере не используется управление доступом на основе ролей (RBAC). Для функций, которыми можно управлять на пограничных транспортных серверах, столбец "Требуемые разрешения" в следующей таблице содержит запись "Локальный администратор пограничного транспортного сервера".

1. Для поиска разрешений, необходимых для выполнения процедуры или запуска командлета, выполните следующие действия.

2. После этого проверьте разрешения, необходимые для функции. Вы должны быть участником одной из этих групп ролей, равнозначной настраиваемой группы ролей или равнозначной роли управления. Вы также можете щелкнуть группу ролей, чтобы просмотреть ее роли управления. Если для функции указано несколько групп ролей, то для ее использования достаточно относиться к одной из этих групп. Дополнительные сведения о группах ролей и ролях управления см. в разделе Understanding Role Based Access Control.

3. Запустите командлет **Get-ManagementRoleAssignment**, чтобы просмотреть назначенные группы ролей или роли управления и проверить наличие необходимых разрешений для управления функцией.

   > ⓘ **Примечание**
   >
   > Для запуска командлета **Get-ManagementRoleAssignment** вам должна быть назначена роль управления "Управление ролями". Если для запуска командлета **Get-ManagementRoleAssignment** отсутствуют необходимые

разрешения, попросите администратора Exchange назначить группы ролей или роли управления.

Дополнительные сведения о делегировании возможности управления другим пользователям см. в разделе Назначения роли делегата.

Разрешения адресов электронной почты и адресных книг

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Возможность	**Необходимые разрешения**
Политики адресных книг	Управление организацией
списки адресов,	Управление организацией
Политики адресов электронной почты	Управление организацией
Шаблоны сведений	Управление организацией
Глобальные списки адресов	Управление организацией
автономные адресные книги,	Управление организацией
Подключение к автономной адресной книге	Управление организацией

Разрешения на общий доступ и совместную работу в Exchange Server

Статья • 04.04.2023

Разрешения, необходимые для настройки возможностей общего доступа и взаимодействия, отличаются в зависимости от выполняемой процедуры или используемого командлета. Дополнительные сведения об общем доступе и взаимодействии приведены в разделах Сотрудничество и Совместное использование.

Для поиска разрешений, необходимых для выполнения процедуры или запуска командлета, выполните следующие действия.

1. Для поиска разрешений, необходимых для выполнения процедуры или запуска командлета, выполните следующие действия.

2. После этого проверьте разрешения, необходимые для функции. Вы должны быть участником одной из этих групп ролей, равнозначной настраиваемой группы ролей или равнозначной роли управления. Вы также можете щелкнуть группу ролей, чтобы просмотреть ее роли управления. Если для функции указано несколько групп ролей, то для ее использования достаточно относиться к одной из этих групп. Дополнительные сведения о группах ролей и ролях управления см. в разделе Understanding Role Based Access Control.

3. Запустите командлет **Get-ManagementRoleAssignment**, чтобы просмотреть назначенные группы ролей или роли управления и проверить наличие необходимых разрешений для управления функцией.

   > ⓘ **Примечание**
   >
   > Для запуска командлета **Get-ManagementRoleAssignment** вам должна быть назначена роль управления "Управление ролями". Если для запуска командлета **Get-ManagementRoleAssignment** отсутствуют необходимые разрешения, попросите администратора Exchange назначить группы ролей или роли управления.

Дополнительные сведения о делегировании возможности управления другим пользователям см. в разделе Назначения роли делегата.

Разрешения возможностей общего доступа и взаимодействия

Чтобы настроить возможности общего доступа и взаимодействия, можно использовать компоненты, приведенные в следующей таблице. Также приведен список групп ролей, которые требуются для настройки каждого компонента.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Возможность	**Необходимые разрешения**
Приложения партнеров — настройка	Управление организацией
Общие папки с включенной поддержкой почты	Управление организацией Управление получателями
Общие папки	Управление организацией Управление общими папками
Почтовые ящики сайта	Управление организацией Управление получателями
Политика подготовки почтового ящика сайта	Управление организацией Управление получателями

Разрешения клиентов и мобильных устройств в Exchange Server

Статья • 04.04.2023

Необходимые разрешения на выполнение задач для клиентов и мобильных устройств различаются в зависимости от выполняемой процедуры или запускаемого командлета. Дополнительные сведения о функциях клиентов и мобильных устройств см. в разделе Клиенты и мобильные устройства.

Для поиска разрешений, необходимых для выполнения процедуры или запуска командлета, выполните следующие действия.

1. Для поиска разрешений, необходимых для выполнения процедуры или запуска командлета, выполните следующие действия.

2. После этого проверьте разрешения, необходимые для функции. Вы должны быть участником одной из этих групп ролей, равнозначной настраиваемой группы ролей или равнозначной роли управления. Вы также можете щелкнуть группу ролей, чтобы просмотреть ее роли управления. Если для функции указано несколько групп ролей, то для ее использования достаточно относиться к одной из этих групп. Дополнительные сведения о группах ролей и ролях управления см. в разделе Understanding Role Based Access Control.

3. Запустите командлет **Get-ManagementRoleAssignment**, чтобы просмотреть назначенные группы ролей или роли управления и проверить наличие необходимых разрешений для управления функцией.

   > ⓘ **Примечание**
   >
   > Для запуска командлета **Get-ManagementRoleAssignment** вам должна быть назначена роль управления "Управление ролями". Если для запуска командлета **Get-ManagementRoleAssignment** отсутствуют необходимые разрешения, попросите администратора Exchange назначить группы ролей или роли управления.

Дополнительные сведения о делегировании возможности управления другим пользователям см. в разделе Назначения роли делегата.

> ⓘ **Примечание**

Для использования некоторых функций требуются разрешения локального администратора сервера, которым необходимо управлять. Для управления этими функциями необходимо быть участником локальной группы администраторов этого сервера.

Разрешения службы клиентского доступа

Вы можете настроить любые из указанных ниже функций для службы клиентского доступа.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Возможность	**Необходимые разрешения**
Параметры массива службы клиентского доступа	Управление организацией Управление сервером
Параметры службы клиентского доступа	Управление сервером
Параметры почтового канала службы клиентского доступа	Управление организацией Управление сервером
Параметры пользователя клиентского доступа	Управление сервером
Параметры виртуального каталога клиентского доступа	Управление организацией Управление сервером
Параметры клиентского доступа RPC	Управление организацией Server Management View-Only Organization Management
Параметры прокси-сервера push-уведомлений	Управление организацией Управление получателями
Параметры перенаправления для проверки подлинности OAuth	Управление организацией

Разрешения Exchange ActiveSync

Можно настроить любые из следующих параметров для Exchange ActiveSync.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Возможность	Необходимые разрешения
Параметры автоблокировки Exchange ActiveSync	Управление организацией
Параметры политики почтовых ящиков Exchange ActiveSync	Управление организацией Управление сервером
Параметры сервера Exchange ActiveSync	Управление организацией Управление сервером
Параметры Exchange ActiveSync	Управление организацией Управление сервером
Параметры пользователя Exchange ActiveSync	Управление получателями
Параметры виртуального каталога Exchange ActiveSync	Управление организацией Управление сервером
Параметры политики почтовых ящиков мобильного устройства	Управление организацией Управление сервером
Параметры пользователя мобильного устройства	Управление организацией Управление сервером Управление получателями

Разрешения автообнаружения

Можно настроить следующие параметры для службы автообнаружения.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Возможность	Необходимые разрешения
Параметры конфигурации службы автообнаружения	Управление организацией Server Management View-Only Organization Management Delegated Setup Управление санацией

Возможность	Необходимые разрешения
Параметры виртуального каталога автообнаружения	Управление организацией Управление сервером

Разрешения службы доступности

Можно настроить следующие параметры для службы доступности.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Возможность	Необходимые разрешения
Параметры адресного пространства службы доступности	Organization Management View-Only Organization Management
Параметры конфигурации службы доступности	Управление организацией Server Management View-Only Organization Management

Разрешения регулирования клиентов

Можно настроить следующие параметры для регулирования клиентов.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Возможность	Необходимые разрешения
Параметры регулирования клиентов	Organization Management View-Only Organization Management

Разрешения веб-служб Exchange

Можно настроить следующие параметры для виртуальных каталогов веб-служб.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Возможность	Необходимые разрешения
Параметры виртуального каталога веб-служб Exchange	Управление организацией Управление сервером
Проверка веб-служб Exchange	Управление организацией Управление сервером
Проверка веб-служб Outlook	Управление организацией

Разрешения мобильного Outlook

Можно настроить и управлять следующими параметрами Outlook Мобильный.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Возможность	Необходимые разрешения
Конфигурация Outlook Мобильный (включение, отключение, изменение, просмотр)	Управление организацией Server Management View-Only Organization Management Delegated Setup Управление санацией
Компонент "RPC через HTTP-прокси"	Администратор локального сервера
Проверка подключения Outlook Мобильный	Organization Management View-Only Organization Management Управление сервером

Разрешения Outlook в Интернете

Можно использовать следующие функции для просмотра параметров Outlook в Интернете, управления безопасностью и доступом пользователей к Outlook в Интернете и проверки подключения Outlook в Интернете.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Возможность	**Необходимые разрешения**
Графический редактор	Администратор локального сервера
Диспетчер IIS	Администратор локального сервера
ISA Server 2006	Администратор предприятия ISA Server
Политики почтовых ящиков Outlook в Интернете	Управление организацией Управление получателями
Виртуальные каталоги Outlook в Интернете	Управление организацией Управление сервером
Редактор реестра	Администратор локального сервера
Конфигурация S/MIME	Управление организацией
Текстовый редактор	Администратор локального сервера
Просмотр политик почтовых ящиков Outlook в Интернете	Управление организацией Recipient Management View-Only Organization Management Delegated Setup Управление санацией

Разрешения POP3 и IMAP4

Можно настроить следующие параметры для протоколов POP3 и IMAP4.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Возможность	**Необходимые разрешения**

Возможность	Необходимые разрешения
Параметры IMAP4	Управление организацией Server Management View-Only Organization Management
Параметры POP3	Управление организацией Server Management View-Only Organization Management
Проверка параметров IMAP4	Управление организацией Server Management View-Only Organization Management
Проверка параметров POP3	Управление организацией Server Management View-Only Organization Management

Разрешения виртуальных каталогов Windows PowerShell

Можно настроить следующие параметры для Windows PowerShell.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Возможность	Необходимые разрешения
Тест Windows PowerShell	Управление организацией
Параметры Windows PowerShell	Управление организацией

Разрешения обмена текстовыми сообщениями

Можно настроить следующие параметры для обмена текстовыми сообщениями.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Возможность	Необходимые разрешения
Параметры уведомлений обмена текстовыми сообщениями	Управление получателями
Параметры обмена текстовыми сообщениями	Управление получателями
Параметры пользователя обмена текстовыми сообщениями	Управление получателями

Разрешения единой системы обмена сообщениями в Exchange Server

Статья • 04.04.2023

Разрешения, необходимые для управления службами и функциями единой системы обмена сообщениями на серверах почтовых ящиков Exchange 2016, зависят от выполняемой процедуры или командлета, который вы хотите запустить.

> ⓘ **Примечание**
>
> Единая система обмена сообщениями не доступна в Exchange 2019.

Некоторые функции, которыми необходимо управлять, могут находиться на пограничных транспортных серверах. Для управления функциями на пограничных транспортных серверах необходимо стать участником локальной группы администраторов пограничного транспортного сервера, которым требуется управлять. На пограничном транспортном сервере не используется управление доступом на основе ролей (RBAC). Для функций, которыми можно управлять на пограничных транспортных серверах, столбец "Требуемые разрешения" в следующей таблице содержит запись "Локальный администратор пограничного транспортного сервера".

1. Для поиска разрешений, необходимых для выполнения процедуры или запуска командлета, выполните следующие действия.

2. После этого проверьте разрешения, необходимые для функции. Вы должны быть участником одной из этих групп ролей, равнозначной настраиваемой группы ролей или равнозначной роли управления. Вы также можете щелкнуть группу ролей, чтобы просмотреть ее роли управления. Если для функции указано несколько групп ролей, то для ее использования достаточно относиться к одной из этих групп. Дополнительные сведения о группах ролей и ролях управления см. в разделе Understanding Role Based Access Control.

3. Запустите командлет **Get-ManagementRoleAssignment**, чтобы просмотреть назначенные группы ролей или роли управления и проверить наличие необходимых разрешений для управления функцией.

   > ⓘ **Примечание**

> Для запуска командлета **Get-ManagementRoleAssignment** вам должна быть назначена роль управления "Управление ролями". Если для запуска командлета **Get-ManagementRoleAssignment** отсутствуют необходимые разрешения, попросите администратора Exchange назначить группы ролей или роли управления.

Дополнительные сведения о делегировании возможности управления другим пользователям см. в разделе Назначения роли делегата.

Разрешения для компонентов единой системы обмена сообщениями

Вы можете настраивать параметры для компонентов и функций единой системы обмена сообщениями, приведенных в следующей таблице.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Возможность	**Необходимы разрешения**
Автосекретари единой системы обмена сообщениями	Organization Management Unified Messaging Management
Правила ответа единой системы обмена сообщениями	Organization Management Unified Messaging Management
Отчеты со сводками и данными о вызовах единой системы обмена сообщениями	Organization Management Unified Messaging Management
Служба маршрутизатора звонков единой системы обмена сообщениями (интерфейсная часть)	Organization Management Unified Messaging Management

Возможность	Необходимы разрешения
Абонентские группы единой системы обмена сообщениями	Organization Management Unified Messaging Management
Сервисные группы единой системы обмена сообщениями	Organization Management Unified Messaging Management
Шлюзы IP единой системы обмена сообщениями	Organization Management Unified Messaging Management
Политики почтовых ящиков единой системы обмена сообщениями	Organization Management Unified Messaging Management
Почтовые ящики единой системы обмена сообщениями	Organization Management Unified Messaging Management
Приглашения единой системы обмена сообщениями	Organization Management Unified Messaging Management
Служба единой системы обмена сообщениями (серверная часть)	Управление организацией Управление сервером

Разрешения на высокий уровень доступности и устойчивость сайта в Exchange Server

Статья • 04.04.2023

Разрешения, требуемые для настройки высокого уровня доступности, отличаются в зависимости от выполняемой процедуры или используемого командлета. Дополнительные сведения о высоком уровне доступности см. в статье Высокий уровень доступности и устойчивость сайта.

Для поиска разрешений, необходимых для выполнения процедуры или запуска командлета, выполните следующие действия.

1. Для поиска разрешений, необходимых для выполнения процедуры или запуска командлета, выполните следующие действия.

2. После этого проверьте разрешения, необходимые для функции. Вы должны быть участником одной из этих групп ролей, равнозначной настраиваемой группы ролей или равнозначной роли управления. Вы также можете щелкнуть группу ролей, чтобы просмотреть ее роли управления. Если для функции указано несколько групп ролей, то для ее использования достаточно относиться к одной из этих групп. Дополнительные сведения о группах ролей и ролях управления см. в разделе Understanding Role Based Access Control.

3. Запустите командлет **Get-ManagementRoleAssignment**, чтобы просмотреть назначенные группы ролей или роли управления и проверить наличие необходимых разрешений для управления функцией.

   > ⓘ **Примечание**
   >
   > Для запуска командлета **Get-ManagementRoleAssignment** вам должна быть назначена роль управления "Управление ролями". Если для запуска командлета **Get-ManagementRoleAssignment** отсутствуют необходимые разрешения, попросите администратора Exchange назначить группы ролей или роли управления.

Дополнительные сведения о делегировании возможности управления другим пользователям см. в разделе Назначения роли делегата.

Разрешения группы доступности базы данных

В следующей таблице перечислены функции, которые можно использовать для добавления, удаления и настройки параметров групп доступности баз данных.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Возможность	Необходимые разрешения
Членство в группе доступности базы данных	Organization Management Database Availability Groups
Свойства группы доступности базы данных	Organization Management Database Availability Groups
Группы доступности базы данных	Organization Management Database Availability Groups
Сети доступности базы данных	Organization Management Database Availability Groups

Разрешения на копирование базы данных почтовых ящиков

В таблице ниже перечислены функции, которые можно использовать для добавления, удаления, обновления и активации копий базы данных почтовых ящиков.

Возможность	Необходимые разрешения
Переключение базы данных	Organization Management Database Copies
Копии базы данных почтовых ящиков	Organization Management Database Copies
Переключение сервера	Organization Management Database Copies
Обновление копии базы данных почтовых ящиков	Organization Management Database Copies

Инфраструктура Exchange и разрешения PowerShell

Статья • 04.04.2023

Разрешения, необходимые для выполнения задач для настройки различных компонентов Exchange Server зависят от выполняемой процедуры или командлета, который требуется выполнить. Дополнительные сведения о соответствующих возможностях см. в следующих подразделах.

Для поиска разрешений, необходимых для выполнения процедуры или запуска командлета, выполните следующие действия.

1. Для поиска разрешений, необходимых для выполнения процедуры или запуска командлета, выполните следующие действия.

2. После этого проверьте разрешения, необходимые для функции. Вы должны быть участником одной из этих групп ролей, равнозначной настраиваемой группы ролей или равнозначной роли управления. Вы также можете щелкнуть группу ролей, чтобы просмотреть ее роли управления. Если для функции указано несколько групп ролей, то для ее использования достаточно относиться к одной из этих групп. Дополнительные сведения о группах ролей и ролях управления см. в разделе Understanding Role Based Access Control.

3. Запустите командлет **Get-ManagementRoleAssignment**, чтобы просмотреть назначенные группы ролей или роли управления и проверить наличие необходимых разрешений для управления функцией.

   > ⓘ **Примечание**
   >
   > Для запуска командлета **Get-ManagementRoleAssignment** вам должна быть назначена роль управления "Управление ролями". Если для запуска командлета **Get-ManagementRoleAssignment** отсутствуют необходимые разрешения, попросите администратора Exchange назначить группы ролей или роли управления.

Дополнительные сведения о делегировании возможности управления другим пользователям см. в разделе Назначения роли делегата.

> ⓘ **Примечание**

Для использования некоторых функций требуются разрешения локального администратора сервера, которым необходимо управлять. Для управления этими функциями необходимо быть участником локальной группы администраторов этого сервера.

Разрешения в инфраструктуре Exchange

В следующей таблице перечислены разрешения, необходимые для выполнения задач, которые настраивают общие параметры Exchange.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Возможность	**Необходимые разрешения**
Ведение журнала аудита администратора	Управление организацией Управление записями
Параметры конфигурации Центра администрирования Exchange	View-Only Organization Management
Подключение к Центру администрирования Exchange	Управление организацией Управление сервером
Параметры конфигурации сервера Exchange	Управление организацией Управление сервером
Параметры справки Exchange	Управление организацией
Категории сообщений	Управление организацией Управление санацией Управление получателями Служба поддержки
Ключ продукта	Управление организацией
Проверка работоспособности системы	Управление организацией Управление сервером

Возможность	Необходимые разрешения
Ведение журнала аудита администратора с правом только на просмотр	Управление организацией Управление записями **Примечание.** Вы также можете вручную назначить роль управления View-Only Журналы аудита группе ролей управления. Дополнительные сведения см. в разделе View-Only Audit Logs.
Запись в журнал аудита	Пользователи, являющиеся членами какой-либо группы ролей или которым назначена какая-либо роль управления, могут вносить записи в журнал аудита администратора.

Разрешения инфраструктуры Exchange PowerShell

В следующей таблице перечислены разрешения, которые необходимы для выполнения задач по настройке функций, которые контролируют ход работы командной консоли Exchange.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Возможность	Необходимые разрешения
Параметры сервера служб домена Active Directory	Управление организацией Управление сервером Управление получателями Управление единой системой обмена сообщениями
Агенты расширения командлета	Управление организацией
Виртуальные каталоги PowerShell	Управление организацией Управление сервером
Установка PowerShell и WinRM	Администратор локального сервера
удаленная оболочка PowerShell;	Управление организацией

Разрешения сертификатов и федерации

В таблице ниже перечислены разрешения, необходимые для выполнения задач по доверию федерации, настройке OAuth, управлению сертификатами и настройке

гибридного развертывания.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Возможность	**Необходимые разрешения**
Управление сертификатами	Управление организацией Управление сервером
Доверие федерации, OAuth	Управление организацией
Проверка доверия федерации, OAuth	Organization Management View-Only Organization Management Server Management
Настройка гибридного развертывания	Управление организацией
Соединители Intra-Organization	Управление организацией Управление получателями Управление записями

Разрешения на работоспособность и производительность сервера в Exchange Server

Статья • 14.08.2024

Разрешения, необходимые для выполнения задач для настройки различных компонентов Exchange Server зависят от выполняемой процедуры или командлета, который требуется выполнить. Дополнительные сведения о соответствующих возможностях см. в следующих подразделах.

Для поиска разрешений, необходимых для выполнения процедуры или запуска командлета, выполните следующие действия.

1. Для поиска разрешений, необходимых для выполнения процедуры или запуска командлета, выполните следующие действия.

2. После этого проверьте разрешения, необходимые для функции. Вы должны быть участником одной из этих групп ролей, равнозначной настраиваемой группы ролей или равнозначной роли управления. Вы также можете щелкнуть группу ролей, чтобы просмотреть ее роли управления. Если для функции указано несколько групп ролей, то для ее использования достаточно относиться к одной из этих групп. Дополнительные сведения о группах ролей и ролях управления см. в разделе Understanding Role Based Access Control.

3. Запустите командлет **Get-ManagementRoleAssignment**, чтобы просмотреть назначенные группы ролей или роли управления и проверить наличие необходимых разрешений для управления функцией.

   > 7 **Примечание**
   >
   > Для запуска командлета **Get-ManagementRoleAssignment** вам должна быть назначена роль управления "Управление ролями". Если для запуска командлета **Get-ManagementRoleAssignment** отсутствуют необходимые разрешения, попросите администратора Exchange назначить группы ролей или роли управления.

Дополнительные сведения о делегировании возможности управления другим пользователям см. в разделе Назначения роли делегата.

> **Примечание**
>
> Для использования некоторых функций требуются разрешения локального администратора сервера, которым необходимо управлять. Для управления этими функциями необходимо быть участником локальной группы администраторов этого сервера.

Разрешения управления рабочими нагрузками в Exchange

В следующей таблице перечислены разрешения, необходимые для выполнения задач, которые управляют работоспособностью и производительностью Exchange Server организации. Дополнительные сведения см. в статье Управление рабочими нагрузками пользователей в Exchange Server.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Развернуть таблицу

Возможность	Необходимые разрешения
Регулирование пользователя	Управление организацией Recipient Management View-Only Organization Management
Регулирование нагрузки Exchange	Organization Management View-Only Organization Management

Разрешения Exchange журнала событий

В следующей таблице перечислены разрешения, которые необходимы для выполнения задач по управлению параметрами Exchange журнала событий.

Пользователи, которым назначена группа ролей управления с правами только для просмотра, могут просматривать конфигурацию функций в приведенной ниже таблице. Дополнительные сведения см. в разделе Управление организацией только для просмотра.

Развернуть таблицу

Возможность	Необходимые разрешения
Управление журналом событий Exchange	Управление организацией Server Management View-Only Organization Management UM Management

Разделенные разрешения в Exchange Server

Статья • 07.04.2023

Организации, разделяющие управление Exchange Server 2016 и Exchange Server объектов 2019 года и Объектов Active Directory, используют так называемую модель *разделения разрешений*. Модель разделения разрешений позволяет организациям назначать определенные разрешения и связанные задачи для определенных групп в пределах организации. Такое разделение обязанностей помогает поддерживать соответствие стандартам и объемы рабочих процессов, а также управлять изменениями в организации.

Наивысший уровень разделенных разрешений — это разделение управления Exchange и управления Active Directory. Во многих организациях есть две группы: администраторы, управляющие инфраструктурой Exchange организации, включая серверы и получатели, и администраторы, управляющие инфраструктурой Active Directory. Это важное разделение для многих организаций, так как инфраструктура Active Directory часто охватывает множество расположений, доменов, служб, приложений и даже лесов Active Directory. Администраторы Active Directory должны следить за тем, чтобы изменения, внесенные в Active Directory, не оказывали негативного влияния на другие службы. В результате, как правило, только небольшая группа администраторов может управлять этой инфраструктурой.

В то же время инфраструктура для Exchange, включая серверы и получателей, также может быть сложной и требовать специальных знаний. Кроме того, Exchange хранит крайне конфиденциальную информацию о бизнесе организации. Администраторы Exchange потенциально могут получить доступ к этим сведениям. Ограничивая количество администраторов Exchange, организация ограничивает круг лиц, которые могут вносить изменения в конфигурацию Exchange и доступ к конфиденциальным сведениям.

Разделенные разрешения обычно различаются между созданием субъектов безопасности в Active Directory, таких как пользователи и группы безопасности, и последующей настройкой этих объектов. Это помогает снизить вероятность несанкционированного доступа к сети, контролируя, кто может создавать объекты, предоставляющие доступ к ней. Чаще всего только администраторы Active Directory могут создавать субъекты безопасности, в то время как другие администраторы, например администраторы Exchange, могут управлять определенными атрибутами существующих объектов Active Directory.

Чтобы обеспечить поддержку различных потребностей в разделении управления Exchange и Active Directory, Exchange позволяет выбрать модель общих разрешений или модель разделенных разрешений. Exchange предлагает два типа моделей разделенных разрешений: RBAC и Active Directory. Exchange по умолчанию использует модель общих разрешений.

Объяснение контроль доступа на основе ролей и Active Directory

Чтобы понять разделенные разрешения, необходимо понять, как модель разрешений на основе ролей контроль доступа (RBAC) в Exchange работает с Active Directory. Модель RBAC определяет, кто может выполнять какие действия и на каких объектах могут выполняться эти действия. Дополнительные сведения о различных компонентах RBAC, которые рассматриваются в этом разделе, см. в разделе разрешения Exchange Server.

Все задачи, выполняемые с объектами Exchange, должны выполняться с помощью командной консоли Exchange или интерфейса Центра администрирования Exchange (EAC). Оба этих средства управления используют RBAC для авторизации всех выполняемых задач.

RBAC — это компонент, который существует на каждом сервере Exchange Server. RBAC проверяет, авторизован ли пользователь, выполняющий действие, на это:

- Если пользователь не авторизован на выполнение действия, RBAC не разрешает выполнение действия.
- Если пользователь авторизован на выполнение действия, RBAC проверяет, авторизован ли пользователь на выполнение действия в отношении конкретного запрашиваемого объекта:
- Если пользователь авторизован, RBAC позволяет продолжить действие.
- Если пользователь не авторизован, RBAC не позволяет продолжить действие.

Если RBAC позволяет продолжить действие, действие выполняется в контексте доверенной подсистемы Exchange, а не в контексте пользователя. Доверенная подсистема Exchange — это универсальная группа безопасности с высоким уровнем привилегий(USG), которая имеет доступ на чтение и запись к каждому связанному с Exchange объекту в организации Exchange. Кроме того, он входит в локальную группу безопасности "Администраторы" и группу usG разрешений

Windows для Exchange, которая позволяет Exchange создавать объекты Active Directory и управлять ими.

> ⚠ **Предупреждение**
>
> Не изменяйте членство в группе безопасности доверенной подсистемы Exchange вручную. Кроме того, не добавляйте и не удаляйте его из списков управления доступом к объектам (ACL). Самостоятельно внося изменения в usG доверенной подсистемы Exchange, вы можете нанести непоправимый ущерб вашей организации Exchange.

Важно понимать, что не имеет значения, какие разрешения Active Directory имеются у пользователя при использовании средств управления Exchange. Если пользователь авторизован через RBAC для выполнения действия в средствах управления Exchange, он может выполнить это действие независимо от его разрешений Active Directory. И наоборот, если пользователь является корпоративным Администратор в Active Directory, но не имеет прав на выполнение действия, например создание почтового ящика, в средствах управления Exchange действие не будет выполнено, так как у пользователя нет необходимых разрешений в соответствии с RBAC.

> ⓘ **Важно!**
>
> Хотя модель разрешений RBAC не применяется к средству управления Пользователи и компьютеры Active Directory, Пользователи и компьютеры Active Directory не может управлять конфигурацией Exchange. S, хотя пользователь может иметь доступ к изменению некоторых атрибутов объектов Active Directory, таких как отображаемое имя пользователя, он должен использовать средства управления Exchange и, следовательно, должен быть авторизован RBAC для управления атрибутами Exchange.

общими разрешениями;

Модель общих разрешений является моделью по умолчанию для Exchange. Вам не нужно ничего изменять, если это модель разрешений, которую вы хотите использовать. Эта модель не отделяет управление объектами Exchange и Active Directory от средств управления Exchange. Она позволяет администраторам, использующим средства управления Exchange, создавать субъекты безопасности в Active Directory.

В следующей таблице показаны роли, позволяющие создавать участников безопасности в Exchange, и группы ролей управления, которым они назначены по умолчанию.

Роль управления	Группа ролей
Роль создания получателя электронной почты	Управление организацией Управление получателями
Роль создания и членства в группе безопасности	Управление организацией

Только группы ролей, пользователи или группы usG, которым назначена роль Создания получателей почты, могут создавать субъекты безопасности, такие как пользователи Active Directory. По умолчанию эта роль назначается группам ролей "Управление организацией" и "Управление получателями". Поэтому члены этих групп ролей могут создавать субъекты безопасности.

Создавать группы безопасности или управлять их членством могут только группы ролей, пользователи или группы безопасности, которым назначена роль создания группы безопасности и членства. По умолчанию эта роль назначается только группе ролей Управление организацией. Таким образом, только члены группы ролей "Управление организацией" могут создавать группы безопасности или управлять ими.

Вы можете назначить роль создания получателя почты и роль создания и членства в группе безопасности другим группам ролей, пользователям или группам безопасности, если вы хотите, чтобы другие пользователи могли создавать субъекты безопасности.

Чтобы включить управление существующими субъектами безопасности в Exchange, роль Получатели почты по умолчанию назначается группам ролей "Управление организацией" и "Управление получателями". Только группы ролей, пользователи или группы безопасности, которым назначена роль Получатели почты, могут управлять существующими субъектами безопасности. Если вы хотите, чтобы другие группы ролей, пользователи или группы безопасности могли управлять существующими субъектами безопасности, необходимо назначить им роль Получатели почты.

Дополнительные сведения о добавлении ролей в группы ролей, пользователей или группы безопасности см. в следующих разделах:

- Управление группами ролей
- Добавление роли для пользователя или универсальной группы безопасности

Если вы перешли на модель разделенных разрешений и хотите вернуться к модели общих разрешений, см. раздел Настройка Exchange Server для общих разрешений.

Разделение разрешений

Если ваша организация разделяет управление Exchange и управление Active Directory, необходимо настроить Exchange для поддержки модели разделенных разрешений. При правильной настройке это смогут сделать только администраторы, которым требуется создать субъекты безопасности, например администраторы Active Directory, и только администраторы Exchange смогут изменять атрибуты Exchange для существующих субъектов безопасности. Это разделение разрешений также происходит примерно в соответствии с разделами домена и конфигурации в Active Directory. Секции также называют контекстами именования. В разделе домена хранятся пользователи, группы и другие объекты для определенного домена. В разделе конфигурации хранятся сведения о конфигурации на уровне леса для служб, которые использовали Active Directory, таких как Exchange. Данные, хранящиеся в разделе домена, обычно управляются администраторами Active Directory, хотя объекты могут содержать атрибуты Exchange, которыми могут управлять администраторы Exchange. Данные, хранящиеся в секции конфигурации, управляются администраторами каждой соответствующей службы, которая хранит данные в этом разделе. Для Exchange это обычно администраторы Exchange.

Exchange поддерживает два следующих типа разрешений на разделение:

- **Разрешения на разделение RBAC**. Разрешения на создание субъектов безопасности в разделе домена Active Directory управляются RBAC. Только серверы Exchange, службы и члены соответствующих групп ролей могут создавать субъекты безопасности.

- **Разделенные разрешения Active Directory**. Разрешения на создание субъектов безопасности в разделе домена Active Directory полностью удаляются у любого пользователя, службы или сервера Exchange. В модели RBAC отсутствует возможность создания участников безопасности. Эта процедура должна выполняться в службе Active Directory с помощью средств управления Active Directory.

  > ⓘ **Важно!**
  >
  > В сценариях сосуществования конфигурация разделенных разрешений Active Directory также применяется к любым серверам Exchange 2010 или

более поздних версий в организации.

Если ваша организация решает использовать модель разделенных разрешений вместо общих разрешений, рекомендуется использовать модель разделенных разрешений RBAC. Модель разделенных разрешений RBAC обеспечивает значительно большую гибкость, обеспечивая почти то же разделение администрирования, что и разрешения active Directory, за исключением того, что серверы и службы Exchange могут создавать субъекты безопасности в модели разделенных разрешений RBAC.

Вам будет предложено включить разделенные разрешения Active Directory во время установки. Если вы решили включить разделенные разрешения Active Directory, можно изменить только общие разрешения или разрешения RBAC, повторно запустив программу установки и отключив разделенные разрешения Active Directory. Этот вариант применяется ко всем серверам Exchange 2010 или более поздних версий в организации.

В следующих разделах более подробно описаны разделенные разрешения RBAC и Active Directory.

Разделенные разрешения RBAC

Модель безопасности RBAC изменяет назначения ролей управления по умолчанию, чтобы отделить пользователей, которые могут создавать субъекты безопасности в разделе домена Active Directory, от тех, кто администрирует данные организации Exchange в разделе конфигурации Active Directory. Субъекты безопасности, такие как пользователи с почтовыми ящиками и группами рассылки, могут быть созданы администраторами, которые являются участниками ролей "Создание получателей почты" или "Создание групп безопасности и членство". Эти разрешения остаются отдельными от разрешений, необходимых для создания субъектов безопасности вне средств управления Exchange. Администраторы Exchange, которым не назначены роли "Создание получателей почты" или "Создание групп безопасности и членство", по-прежнему могут изменять атрибуты, связанные с Exchange, в субъектах безопасности. Администраторы Active Directory также могут использовать инструменты управления Exchange для создания участников безопасности Active Directory.

Серверы Exchange и доверенная подсистема Exchange также имеют разрешения на создание субъектов безопасности в Active Directory от имени пользователей и сторонних программ, которые интегрируются с RBAC.

Разделенные разрешения RBAC — это хороший выбор для вашей организации, если верно следующее:

- Ваша организация не требует, чтобы создание субъекта безопасности выполнялось только с помощью средств управления Active Directory и только пользователями, которым назначены определенные разрешения Active Directory.
- Ваша организация позволяет службам, таким как серверы Exchange Server, создавать субъекты безопасности.
- Вы хотите упростить процесс, необходимый для создания почтовых ящиков, пользователей с поддержкой почты, групп рассылки и групп ролей, разрешив их создание из средств управления Exchange.
- Вы хотите управлять членством в группах рассылки и группах ролей в средствах управления Exchange.
- У вас есть сторонние программы, которые требуют, чтобы серверы Exchange могли создавать субъекты безопасности от их имени.

Если вашей организации требуется полное разделение администрирования Exchange и Active Directory, когда администрирование Active Directory не может быть выполнено с помощью средств управления Exchange или служб Exchange, см. раздел Разделенные разрешения Active Directory далее в этом разделе.

Переключение с общих разрешений на разделенные разрешения RBAC выполняется вручную, когда вы удаляете разрешения, необходимые для создания субъектов безопасности, из групп ролей, которым они предоставляются по умолчанию. В следующей таблице показаны роли, позволяющие создавать участников безопасности в Exchange, и группы ролей управления, которым они назначены по умолчанию.

Роль управления	**Группа ролей**
Роль создания получателя электронной почты	Управление организацией Управление получателями
Роль создания и членства в группе безопасности	Управление организацией

По умолчанию участники групп ролей "Управление организацией" и "Управление получателями" могут создавать субъекты безопасности. Необходимо передать возможность создания субъектов безопасности из встроенных групп ролей в новую созданную группу ролей.

Чтобы настроить разделенные разрешения RBAC, необходимо выполнить следующие действия.

1. Отключите разделение разрешений Active Directory, если оно включено.
2. Создайте группу ролей, которая будет содержать администраторов Active Directory, которые смогут создавать субъекты безопасности.
3. Создайте регулярные и делегирующие назначения ролей между ролью создания получателя почты и новой группой ролей.
4. Создайте регулярные и делегирующие назначения ролей между ролью создания и членства в группе безопасности и новой группой ролей.
5. Удалите обычные и делегирующие назначения ролей управления между ролью "Создание получателя почты" и группами ролей "Управление организацией" и "Управление получателями".
6. Удалите обычные и делегирующие назначения ролей между ролью "Создание группы безопасности и членство" и группой ролей "Управление организацией".

После выполнения этих действий только члены создаваемой группы ролей смогут создавать субъекты безопасности, например почтовые ящики. Новая группа сможет только создавать объекты. Он не сможет настроить атрибуты Exchange для нового объекта. Администратору Active Directory, который является членом новой группы, потребуется создать объект, а затем администратору Exchange потребуется настроить атрибуты Exchange для объекта . Администраторы Exchange не смогут использовать следующие командлеты:

- **New-Mailbox**
- **New-MailContact**
- **New-MailUser**
- **New-RemoteMailbox**
- **Remove-Mailbox**
- **Remove-MailContact**
- **Remove-MailUser**
- **Remove-RemoteMailbox**

Однако администраторы Exchange смогут создавать объекты Exchange и управлять ими, такими как правила потока обработки почты (также известные как правила транспорта), группы рассылки и т. д., а также управлять атрибутами, связанными с Exchange, для любого объекта.

Кроме того, связанные функции в EAC и Outlook в Интернете (ранее известные как Outlook Web App), такие как мастер создания почтовых ящиков, также больше не будут доступны или при попытке их использовать будет возникать ошибка.

Если вы хотите, чтобы новая группа ролей также могла управлять атрибутами Exchange для нового объекта, роль Получатели почты также должна быть назначена новой группе ролей.

Дополнительные сведения о настройке модели разделенных разрешений см. в разделе Настройка Exchange 2013 для разделенных разрешений.

Разделенные разрешения Active Directory

При разделенных разрешениях Active Directory создание участников безопасности в разделе домена Active Directory, например почтовых ящиков и групп рассылки, должно выполняться с помощью инструментов управления Active Directory. Несколько изменений внесены в разрешения, предоставленные доверенной подсистеме Exchange и серверам Exchange для ограничения действий администраторов и серверов Exchange. При включении разделенных разрешений Active Directory происходят следующие изменения в функциональности:

- Создание почтовых ящиков, пользователей с включенной поддержкой почты, групп рассылки и других субъектов безопасности удаляется из инструментов управления Exchange.
- Добавление и удаление членов группы рассылки невозможно с помощью инструментов управления Exchange.
- Все разрешения, предоставленные доверенной подсистеме Exchange и серверам Exchange для создания субъектов безопасности, удаляются.
- Серверы Exchange и средства управления Exchange могут изменять только атрибуты Exchange существующих участников безопасности в Active Directory.

Например, чтобы создать почтовый ящик с включенным разделением разрешений Active Directory, сначала необходимо создать пользователя с помощью средств Active Directory пользователем с необходимыми разрешениями Active Directory. Затем пользователь может включить почтовый ящик с помощью средств

управления Exchange. Только атрибуты почтового ящика, связанные с Exchange, могут быть изменены администраторами Exchange с помощью инструментов управления Exchange.

Разделение разрешений Active Directory — хороший выбор для вашей организации, если верно следующее:

- Ваша организация требует, чтобы субъекты безопасности создавались только с помощью средств управления Active Directory или только пользователями, которым предоставлены определенные разрешения в Active Directory.
- Вы хотите полностью отделить возможность создания субъектов безопасности от тех, кто управляет организацией Exchange.
- Вы хотите выполнить все управление группами рассылки, включая создание групп рассылки, а также добавление и удаление членов этих групп с помощью средств управления Active Directory.
- Вы не хотите, чтобы серверы Exchange или сторонние программы, использующие Exchange от их имени, создавали субъекты безопасности.

Примечания.

- Переключение на разделенные разрешения Active Directory — это выбор, который можно сделать при установке Exchange с помощью мастера установки или параметра *командной строки /ActiveDirectorySplitPermissions* с Setup.exe (при этом необходимо всегда указывать параметр */PrepareAD* вместе с параметром */ActiveDirectorySplitPermissions*).
- Вы также можете включить или отключить разделенные разрешения Active Directory **после** установки Exchange, повторно выполнив Setup.exe из командной строки. Чтобы включить разделенные разрешения Active Directory, используйте значение `/ActiveDirectorySplitPermissions:True`. Чтобы отключить его, используйте значение `/ActiveDirectorySplitPermissions:False`.
- При наличии нескольких доменов в одном лесу также необходимо выполнить одно из следующих действий:
  - Укажите параметр */PrepareAllDomains при применении* разделенных разрешений Active Directory.
  - Запустите Setup.exe с параметром */PrepareDomain* в каждом домене. Необходимо подготовить каждый домен, содержащий серверы Exchange,

объекты с поддержкой почты или серверы глобального каталога, доступ к которым может получить сервер Exchange Server.

- Вы не можете включить разделенные разрешения Active Directory, если вы установили Exchange 2010 или более поздней версии на контроллере домена.
- После включения или отключения разделенных разрешений Active Directory рекомендуется перезапустить серверы Exchange в организации, чтобы заставить их получить новый маркер доступа Active Directory с обновленными разрешениями.

Exchange обеспечивает разделение разрешений Active Directory путем удаления разрешений и членства в группе безопасности Exchange Windows Permissions. Этой группе безопасности в общих разрешениях и разделенных разрешениях RBAC предоставляются разрешения для многих объектов и атрибутов, не относящихся к Exchange, в Active Directory. Удалив разрешения и членство в этой группе безопасности, администраторы и службы Exchange не могут создавать или изменять эти объекты Active Directory, отличные от Exchange.

Список изменений, которые происходят в группе безопасности Разрешений Windows Exchange и других компонентах Exchange при включении или отключении разделенных разрешений Active Directory, см. в следующей таблице.

> ⓘ **Примечание**
>
> Назначения ролей группам ролей, которые позволяют администраторам Exchange создавать субъекты безопасности, удаляются при включении разделенных разрешений Active Directory. Это делается для того, чтобы удалить доступ к командлетам, которые в противном случае при их выполнении вызовут ошибку, так как у них нет разрешений на создание связанного объекта Active Directory.

Действие	Изменения, внесенные Exchange

Действие	Изменения, внесенные Exchange
Включение разделенных разрешений Active Directory во время первой Exchange Server установки	При включении разделенных разрешений Active Directory с помощью мастера установки или запуска Setup.exe с параметрами */PrepareAD* и `/ActiveDirectorySplitPermissions:true` командной строки выполняются следующие действия: • Создается подразделение с именем **Защищенные группы Microsoft Exchange** . • Группа безопасности **Разрешений Exchange Windows** создается в подразделении **защищенных групп Microsoft Exchange** . • Группа безопасности **доверенной подсистемы Exchange** не добавляется в группу безопасности **Разрешений Windows Exchange** . • Создание не делегированных назначений ролей управления ролям управления со следующими типами ролей управления пропускается: `MailRecipientCreation` и `SecurityGroupCreationandMembership`. • Записи управления доступом (ACE), которые были бы назначены группе безопасности **Разрешений Windows Exchange** , не добавляются в объект домена Active Directory. При выполнении Setup.exe с параметром */PrepareAllDomains* или */PrepareDomain* в каждом подготовленном дочернем домене выполняются следующие действия: • Все ACE, назначенные группе безопасности **Разрешения Windows Exchange** , удаляются из объекта домена. • ACE задаются в каждом домене, за исключением всех ACE, **назначенных группе безопасности Разрешений Windows Exchange** .

Действие	Изменения, внесенные Exchange
Переключение с общих разрешений или разделенных разрешений RBAC на разрешения Active Directory	При выполнении команды setup.exe с параметрами */PrepareAD* и `/ActiveDirectorySplitPermissions:true` командной строки выполняются следующие действия: • Создается подразделение с именем **Защищенные группы Microsoft Exchange** . • Группа безопасности **"Разрешения Exchange Windows"** перемещается в подразделение **защищенных групп Microsoft Exchange** . • Группа безопасности **доверенной подсистемы Exchange** удаляется из группы безопасности **Разрешения Windows Exchange** . • Удаляются все не делегированные назначения ролей управления со следующими типами ролей: `MailRecipientCreation` и `SecurityGroupCreationandMembership`. • Все ACE, назначенные группе безопасности **Разрешения Windows Exchange** , удаляются из объекта домена. При выполнении Setup.exe с параметром */PrepareAllDomains* или */PrepareDomain* в каждом подготовленном дочернем домене выполняются следующие действия: • Все ACE, назначенные группе безопасности **Разрешения Windows Exchange** , удаляются из объекта домена. • ACE задаются в каждом домене, за исключением всех ACE, **назначенных группе безопасности Разрешений Windows Exchange** .

Действие	Изменения, внесенные Exchange
Переключение с разделенных разрешений Active Directory на общие или разделенные разрешения RBAC	Следующие действия выполняются при выполнении Setup.exe с параметрами */PrepareAD* и `/ActiveDirectorySplitPermissions:false` : • Группа безопасности **"Разрешения Exchange Windows"** перемещается в подразделение **групп безопасности Microsoft Exchange** . • Подразделение **защищенных групп Microsoft Exchange** удалено • Группа безопасности **доверенных подсистем Exchange** добавляется в группу безопасности **Разрешения Exchange Windows** . • ACE добавляются в объект домена для группы безопасности **Разрешений Windows Exchange** . При запуске установки с параметром */PrepareAllDomains* или */PrepareDomain* в каждом подготовленном дочернем домене выполняются следующие действия: • ACE добавляются в объект домена для группы безопасности **Разрешений Windows Exchange** . • ACE задаются в каждом домене, включая ACE, назначенные группе безопасности **Разрешений Windows Exchange** . Назначения ролей для ролей создания получателя почты и создания группы безопасности и членства не создаются автоматически при переключении с разделения Active Directory на общие разрешения. Если делегирование назначений ролей было настроено до включения разделенных разрешений Active Directory, эти настройки остаются без изменений. Сведения о создании назначений ролей между этими ролями и группой ролей Управление организацией см. в статье Настройка Exchange Server для общих разрешений.

После включения разделенных разрешений Active Directory станут недоступны следующие командлеты:

- **New-Mailbox**
- **New-MailContact**
- **New-MailUser**
- **New-RemoteMailbox**
- **Remove-Mailbox**
- **Remove-MailContact**
- **Remove-MailUser**
- **Remove-RemoteMailbox**

После включения разделенных разрешений Active Directory доступны следующие командлеты, но их нельзя использовать для создания групп рассылки или изменения членства в группах рассылки:

- **Добавить DistributionGroupMember**
- **Новая DistributionGroup**
- **Удалить DistributionGroup**
- **Удалить DistributionGroupMember**
- **Обновить DistributionGroupMember**

Некоторые командлеты, хотя они по-прежнему доступны, могут предоставлять только ограниченные функциональные возможности при использовании с разделенными разрешениями Active Directory. Это связано с тем, что они могут позволить настроить объекты получателей, которые находятся в домене раздела Active Directory, и объекты конфигурации Exchange, которые находятся в разделе конфигурации Active Directory. Они также могут позволить настроить атрибуты, связанные с Exchange, для объектов, хранящихся в разделе домена. Попытки использовать командлеты для создания объектов или изменения атрибутов, не связанных с Exchange, в объектах в разделе домена приведут к ошибке. Например, командлет **Add-ADPermission** вернет ошибку при попытке добавить разрешения в почтовый ящик. Однако командлет **Add-ADPermission** будет выполнен успешно, если вы настроите разрешения для соединителя получения. Это связано с тем, что почтовый ящик хранится в разделе домена, а соединители получения — в разделе конфигурации.

Кроме того, связанные функции в EAC и Outlook в Интернете, такие как мастер создания почтовых ящиков, также больше не будут доступны или при попытке их использовать будет возникать ошибка.

Однако администраторы Exchange смогут создавать объекты Exchange и управлять ими, такими как правила потока обработки почты и т. д.

Дополнительные сведения о настройке модели разделенных разрешений Active Directory см. в разделе Настройка Exchange 2013 для разделенных разрешений.

Настройка Exchange Server для разделения разрешений

Статья • 07.04.2023

Разделенные разрешения позволяют двум отдельным группам, таким как администраторы Active Directory и администраторы Exchange, управлять соответствующими службами, объектами и атрибутами. Администраторы Active Directory управляют участниками безопасности, например пользователями, которые предоставляют разрешения на доступ к лесу Active Directory. Администраторы Exchange управляют связанными с Exchange атрибутами объектов Active Directory, а также отвечают за создание и контроль объектов, относящихся к Exchange.

Exchange Server 2016 и Exchange Server 2019 годах предлагают следующие типы моделей разделенных разрешений:

- **Разрешения на разделение RBAC**. Разрешения на создание субъектов безопасности в разделе домена Active Directory управляются контроль доступа на основе ролей (RBAC). Только члены соответствующих групп ролей могут создавать участников безопасности.
- **Разделенные разрешения Active Directory**. Разрешения на создание субъектов безопасности в разделе домена Active Directory полностью удаляются у любого пользователя, службы или сервера Exchange. В модели RBAC отсутствует возможность создания участников безопасности. Эта процедура должна выполняться в службе Active Directory с помощью средств управления Active Directory.

Выбор модели зависит от структуры и потребностей организации. Выберите процедуру, применимую к модели, которую необходимо настроить. Рекомендуется использовать модель разделения разрешений RBAC. Модель разделения разрешений RBAC обеспечивает значительно большую гибкость при сохранении почти такого же разделения администрирования, как при разделении разрешений Active Directory.

Дополнительные сведения о общих и разделенных разрешениях см. в разделе Разделение разрешений в Exchange Server.

Дополнительные сведения о группах ролей управления, ролях управления, регулярных назначениях ролей управления и назначениях делегирования ролей управления см. в следующих разделах:

- Общие сведения об управлении доступом на основе ролей
- Общие сведения о группах ролей управления
- Общие сведения о ролях управления
- Общие сведения о назначениях ролей управления

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Разделенные разрешения Active Directory" в разделе Разрешения управления ролями .
- Выбранная модель разрешений будет применена ко всем серверам Exchange 2010 или более поздних версий в организации.
- Сведения о том, как скачать последнюю версию Exchange, см. в разделе Обновления для Exchange Server.
- Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью на **форумах Exchange Server** .

Переключение на разделение разрешений RBAC

После перехода на разделенные разрешения RBAC только администраторы Active Directory смогут создавать субъекты безопасности Active Directory. Это означает, что администраторы Exchange не смогут использовать следующие командлеты:

- **New-Mailbox**
- **New-MailContact**
- **New-MailUser**
- **New-RemoteMailbox**
- **Remove-Mailbox**
- **Remove-MailContact**
- **Remove-MailUser**

- **Remove-RemoteMailbox**

Администраторы Exchange смогут управлять атрибутами Exchange только в существующих субъектах безопасности Active Directory. Однако они смогут создавать и управлять объектами, зависящими от Exchange, такими как правила потока обработки почты (также известные как правила транспорта) и группы рассылки. Дополнительные сведения см. в разделе "Разделенные разрешения RBAC" статьи Разделение разрешений в Exchange Server.

Чтобы настроить Exchange для разделения разрешений, необходимо назначить роль создания получателя почты и роль создания группы безопасности и членства в группе ролей, содержащей членов, являющихся администраторами Active Directory. После этого необходимо удалить назначения между этими ролями и любой группой ролей или универсальной группой безопасности (USG), содержащей администраторов Exchange.

Чтобы настроить разделенные разрешения RBAC, сделайте следующее:

1. Если в настоящее время в вашей организации настроены разделенные разрешения Active Directory, выполните следующие действия.

   a. На целевом сервере откройте проводник, щелкните правой кнопкой мыши файл ISO-образа Exchange и выберите **Подключить**. Обратите внимание на назначенную букву виртуального DVD-диска.

   b. Откройте окно командной строки Windows. Например:

      - Нажмите клавиши Windows + R, чтобы открыть диалоговое окно **Выполнить**, введите cmd.exe и нажмите кнопку **ОК**.
      - Нажмите кнопку **Пуск**. В поле **Поиск** введите **командная строка**, а затем в списке результатов выберите **Командная строка**.

   c. В окне командной строки выполните следующую команду, чтобы отключить разделенные разрешения Active Directory:

      > ⓘ **Примечание**
      >
      > - Предыдущий параметр */IAcceptExchangeServerLicenseTerms* не будет работать, начиная с Exchange Server 2016 и Exchange Server 2019 за сентябрь 2021 Обновления г. Теперь необходимо использовать */IAcceptExchangeServerLicenseTerms_DiagnosticDataON* или

/IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF для автоматической установки и установки по сценариям.

- В примерах ниже используется переключатель */IAcceptExchangeServerLicenseTerms_DiagnosticDataON*. Вы можете изменить переключатель на */IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF*.

```
DOS

Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON
/PrepareAD /ActiveDirectorySplitPermissions:false
```

d. Перезапустите все серверы Exchange в организации или дождитесь репликации маркера доступа Active Directory на все серверы Exchange.

2. В командной консоли Exchange выполните следующие действия.

a. Создайте группу ролей для администраторов Active Directory. Кроме создания группы ролей, команда создает стандартные назначения ролей между новой группой ролей и ролью создания получателей почты, а также ролью создания и участия в группе безопасности.

```
DOS

New-RoleGroup "Active Directory Administrators" -Roles "Mail
Recipient Creation", "Security Group Creation and Membership"
```

ⓘ Примечание

Если требуется, чтобы члены этой группы ролей могли создавать назначения ролей, включите роль управления ролями. Нет необходимости добавлять эту роль сейчас. Тем не менее, если в какой-либо момент потребуется назначить роль создания получателей почты (Mail Recipient Creation) или роль создания и участия в группе безопасности (Security Group Creation and Membership) другим уполномоченным ролей, то роль управления ролями должна быть назначена этой новой группе ролей. Ниже приводится процедура настройки группы ролей администраторов Active Directory в качестве единственной группы ролей, которая может делегировать эти роли.

b. Создайте делегированные назначения ролей между новой группой ролей и ролью создания получателя почты и ролью создания группы безопасности и членства, выполнив следующие команды:

```
PowerShell

New-ManagementRoleAssignment -Role "Mail Recipient Creation" -
SecurityGroup "Active Directory Administrators" -Delegating
New-ManagementRoleAssignment -Role "Security Group Creation and
Membership" -SecurityGroup "Active Directory Administrators" -
Delegating
```

c. Добавьте участников в новую группу ролей, выполнив следующую команду:

```
PowerShell

Add-RoleGroupMember "Active Directory Administrators" -Member <user
to add>
```

d. Замените список делегатов в новой группе ролей, чтобы только члены группы ролей могли добавлять или удалять участников, выполнив следующую команду:

```
PowerShell

Set-RoleGroup "Active Directory Administrators" -ManagedBy "Active
Directory Administrators"
```

> ⓘ **Важно!**
>
> Члены группы ролей Управление организацией, а также те, которым назначена роль управления ролями напрямую или через другую группу ролей либо универсальную группу безопасности, могут пропускать проверку безопасности делегатов. Чтобы запретить администратору Exchange добавлять себя в новую группу ролей, необходимо удалить назначение роли между ролью управления ролями и любым администратором Exchange, а затем назначить ее другой группе.

e. Найдите все обычные и делегированные назначения ролей роли создания получателя почты, выполнив следующую команду:

```
PowerShell

Get-ManagementRoleAssignment -Role "Mail Recipient Creation" |
Format-Table Name, Role, RoleAssigneeName -Auto
```

f. Удалите все обычные и делегированные назначения ролей роли создания получателя почты, которые не связаны с новой группой ролей или другими группами ролей, группами usg или прямыми назначениями, которые вы хотите сохранить, выполнив следующую команду.

```
PowerShell

Remove-ManagementRoleAssignment <Mail Recipient Creation role
assignment to remove>
```

> ⓘ **Примечание**
>
> Если требуется удалить все назначения обычной роли и роли делегирования для роли создания получателей почты (Mail Recipient Creation) по отношению к уполномоченному роли, не связанному с группой ролей администраторов Active Directory, используйте следующую команду. Параметр *WhatIf* позволяет узнать, какие назначения ролей будут удалены. Удалите параметр *WhatIf* и запустите команду еще раз, чтобы удалить назначения ролей.

```
PowerShell

Get-ManagementRoleAssignment -Role "Mail Recipient Creation" | Where
{ $_.RoleAssigneeName -NE "Active Directory Administrators" } |
Remove-ManagementRoleAssignment -WhatIf
```

g. Найдите все обычные и делегированные назначения ролей роли создания группы безопасности и членства, выполнив следующую команду.

```
PowerShell

Get-ManagementRoleAssignment -Role "Security Group Creation and
Membership" | Format-Table Name, Role, RoleAssigneeName -Auto
```

h. Удалите все обычные и делегированные назначения ролей роли создания и членства в группе безопасности, которые не связаны с новой группой ролей или другими группами ролей, группами usg или прямыми

назначениями, которые вы хотите сохранить, выполнив следующую команду:

```
PowerShell

Remove-ManagementRoleAssignment <Security Group Creation and
Membership role assignment to remove>
```

> **Примечание**
>
> Такую же команду из предыдущего замечания можно использовать с целью удаления всех назначений стандартных ролей и ролей делегирования для роли создания и участия в группе безопасности по отношению к любому уполномоченному роли, не связанному с группой ролей администраторов Active Directory, как показано в этом примере.

```
PowerShell

Get-ManagementRoleAssignment -Role "Security Group Creation and
Membership" | Where { $_.RoleAssigneeName -NE "Active Directory
Administrators" } | Remove-ManagementRoleAssignment -WhatIf
```

Подробные сведения о синтаксисе и параметрах см. в следующих разделах:

- New-RoleGroup
- New-ManagementRoleAssignment
- Add-RoleGroupMember
- Set-RoleGroup
- Get-ManagementRoleAssignment
- Remove-ManagementRoleAssignment

Переключение на разделение разрешений Active Directory

Вы можете настроить организацию Exchange для разделения разрешений Active Directory. При разделении разрешений Active Directory полностью удаляются разрешения, которые позволяют администраторам и серверам Exchange создавать участников безопасности в службе Active Directory или изменять не связанные с системой Exchange атрибуты этих объектов. После завершения настройки только администраторы Active Directory смогут создавать участников безопасности Active

Directory. Это означает, что администраторы Exchange не смогут использовать следующие командлеты:

- **Добавить DistributionGroupMember**
- **Новая DistributionGroup**
- **New-Mailbox**
- **New-MailContact**
- **New-MailUser**
- **New-RemoteMailbox**
- **Удалить DistributionGroup**
- **Удалить DistributionGroupMember**
- **Remove-Mailbox**
- **Remove-MailContact**
- **Remove-MailUser**
- **Remove-RemoteMailbox**
- **Обновить DistributionGroupMember**

Администраторы и серверы Exchange будут управлять только атрибутами Exchange для существующих участников безопасности Active Directory. Однако они смогут создавать объекты, связанные с Exchange, например правила транспорта и абонентские группы единой системы обмена сообщениями, а также управлять этими объектами.

> ⚠ **Предупреждение**
>
> После включения разделенных разрешений Active Directory администраторы и серверы Exchange больше не смогут создавать субъекты безопасности в Active Directory и не смогут управлять членством в группах рассылки. Эти задачи должны выполняться с помощью средств управления Active Directory с необходимыми разрешениями Active Directory. Прежде чем вносить это изменение, следует понять, какое влияние оно окажет на процессы администрирования и сторонние приложения, которые интегрируются с Exchange и моделью разрешений RBAC.
>
> Дополнительные сведения см. в разделе "Разделенные разрешения Active Directory" **статьи Разделение разрешений в Exchange Server**.

Чтобы переключиться с общих разрешений или разрешений RBAC на разрешения Active Directory, сделайте следующее:

1. На целевом сервере откройте проводник, щелкните правой кнопкой мыши файл ISO-образа Exchange и выберите **Подключить**. Обратите внимание на

назначенную букву виртуального DVD-диска.

2. В окне командной строки Windows выполните следующую команду, чтобы включить разделенные разрешения Active Directory:

> ⓘ **Примечание**
>
> - Предыдущий параметр */IAcceptExchangeServerLicenseTerms* не будет работать, начиная с Exchange Server 2016 и Exchange Server 2019 за сентябрь 2021 Обновления г. Теперь необходимо использовать */IAcceptExchangeServerLicenseTerms_DiagnosticDataON* или */IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF* для автоматической установки и установки по сценариям.
> - В примерах ниже используется переключатель */IAcceptExchangeServerLicenseTerms_DiagnosticDataON*. Вы можете изменить переключатель на */IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF*.

```
DOS

Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON
/PrepareAD /ActiveDirectorySplitPermissions:true
```

3. Если в вашей организации несколько доменов Active Directory, необходимо либо запускать `Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON /PrepareDomain` в каждом дочернем домене, содержащем серверы Или объекты Exchange Server, либо с `Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON /PrepareAllDomains` сайта с сервером Active Directory из каждого домена.

4. Перезапустите все серверы Exchange в организации или дождитесь репликации маркера доступа Active Directory на все серверы Exchange.

Настройка Exchange Server для общих разрешений

Статья • 07.04.2023

Если в организации не настраивалось разделение разрешений, выполнять эту процедуру необязательно. Exchange Server 2016 и Exchange Server 2019 по умолчанию настроены для общих разрешений.

Общие разрешения позволяют администратору Exchange создавать субъекты безопасности Active Directory, например пользователей, а затем настраивать их в качестве получателей Exchange. В отличие от модели разделения разрешений, которая разделяет задачи управления между группами администраторов Exchange и Active Directory, в разрешениях общего доступа отсутствует разделение задач.

Дополнительные сведения о общих и разделенных разрешениях см. в разделе Разделение разрешений в Exchange Server.

Вы можете настроить организацию Exchange для общих разрешений, если ранее вы настроили для своей организации разделение разрешений. Процедура переключения на использование разрешений общего доступа различается в зависимости от того, используется ли в текущий момент разделение разрешений управления доступом на основе ролей (RBAC) или разделение разрешений Active Directory. Выберите одну из следующих процедур, которая соответствует текущей конфигурации. При соблюдении следующих условий организация использует разделение разрешений Active Directory.

- Существует подразделение защищенных групп Microsoft Exchange.
- Группа безопасности Разрешений Exchange Windows находится в подразделении защищенных групп Microsoft Exchange.
- Группа безопасности доверенной подсистемы Exchange входит в группу безопасности Разрешений Exchange Windows.
- Отсутствуют назначения обычной роли управления для роли создания получателей почты или роли создания и членства в группе безопасности.

Дополнительные сведения о группах ролей управления, ролях управления, регулярных назначениях ролей управления и назначениях делегирования ролей управления см. в следующих разделах:

- Общие сведения об управлении доступом на основе ролей

- Общие сведения о группах ролей управления
- Общие сведения о ролях управления
- Общие сведения о назначениях ролей управления

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут
- Для процедур, описанных в этом разделе, требуются определенные разрешения. Сведения о разрешениях см. в каждой процедуре.
- В настоящее время организация Exchange должна быть настроена для разделения разрешений RBAC или Active Directory.
- Выбранная модель разрешений будет применена ко всем серверам Exchange 2010 или более поздних версий в организации.
- Необходимо иметь разрешения на делегирование ролей управления "Создание получателей почты" и "Создание и членство в группе безопасности" группе ролей управления Управление организацией или другой группе ролей, которой назначена роль получателей почты.
- Сведения о том, как скачать последнюю версию Exchange на целевом компьютере, см. в разделе Обновления для Exchange Server.
- Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью на **форумах Exchange Server**.

Переключение из режима разделения разрешений RBAC в режим разрешений общего доступа

Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Группы ролей" в разделе Разрешения для управления ролями .

Чтобы переключиться с разделенных разрешений RBAC на общие разрешения Exchange, необходимо назначить роль создания получателей почты и создание и членство в группе безопасности, в которой также назначена роль Получатели почты и администраторы Exchange в качестве участников. В конфигурации разрешений общего доступа по умолчанию группа ролей Управление организацией содержит все эти роли. Поэтому группа ролей Управление организацией включена в эту процедуру.

Настройка разрешений общего доступа

Чтобы настроить общие разрешения в группе ролей "Управление организацией", выполните следующие действия с помощью учетной записи, которая имеет разрешения на делегирование назначений ролей для роли создания получателя почты и роли создания и членства в группе безопасности.

1. Добавьте в группу ролей Управление организацией назначения роли делегирования для ролей "Создание получателей почты" и "Создание и членство в группе безопасности" с помощью следующих команд:

   PowerShell

   ```
   New-ManagementRoleAssignment -Role "Mail Recipient Creation" -
   SecurityGroup "Organization Management" -Delegating
   New-ManagementRoleAssignment -Role "Security Group Creation and
   Membership" -SecurityGroup "Organization Management" -Delegating
   ```

   > ⓘ **Примечание**
   >
   > Группе ролей (в этой процедуре — группа ролей "Администраторы Active Directory"), имеющей назначения роли делегирования для ролей "Создание получателей почты" и "Создание и членство в группе безопасности", необходимо назначить роль "Управление ролями" для запуска командлета **New-ManagementRoleAssignment**. Уполномоченный роли, имеющий разрешение на делегирование роли "Управление ролями", должен назначить эту роль группе ролей "Администраторы Active Directory".

2. Добавьте в группы ролей Управление организацией и Управление получателями назначения обычной роли для роли "Создание получателей почты" с помощью следующих команд:

```
PowerShell

New-ManagementRoleAssignment -Role "Mail Recipient Creation" -
SecurityGroup "Organization Management"
New-ManagementRoleAssignment -Role "Security Group Creation and
Membership" -SecurityGroup "Recipient Management"
```

3. Добавьте группе ролей Управление организацией назначение обычной роли для роли создания и членства в группе безопасности с помощью следующей команды.

```
PowerShell

 New-ManagementRoleAssignment -Role "Security Group Creation and
Membership" -SecurityGroup "Organization Management"
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе New-ManagementRoleAssignment.

Удаление разрешений, предоставленных администраторам Active Directory (необязательно)

Также можно удалить разрешения, предоставленные администраторам Active Directory, чтобы запретить им создавать или управлять объектами Active Directory с помощью средств управления Exchange. Чтобы удалить разрешения, предоставленные администраторам Active Directory, выполните эту процедуру.

> **Примечание**
>
> Хотя вы можете удалить разрешения для администраторов Active Directory на управление объектами Active Directory с помощью средств управления Exchange, администраторы Active Directory могут продолжать управлять объектами Active Directory с помощью средств управления Active Directory, если это разрешено их разрешениями Active Directory. Однако они не смогут управлять атрибутами Exchange в объектах Active Directory. Дополнительные сведения см. **в разделе Разделение разрешений в Exchange Server**.

Чтобы удалить разрешения на разделение, связанные с Exchange, у администраторов Active Directory, выполните следующие действия.

1. Удалите назначения обычной роли и роли делегирования, которые назначают роль "Создание получателей почты" группе ролей или универсальной группе безопасности, членами которой являются администраторы Active Directory, с помощью следующей команды. В этой команде группа ролей "Администраторы Active Directory" используется в качестве примера. Параметр *WhatIf* позволяет узнать, какие назначения ролей будут удалены. Удалите параметр *WhatIf* и запустите команду еще раз, чтобы удалить назначения ролей.

   PowerShell

   ```
   Get-ManagementRoleAssignment -Role "Mail Recipient Creation" | Where {
   $_.RoleAssigneeName -EQ "Active Directory Administrators" } | Remove-
   ManagementRoleAssignment -WhatIf
   ```

2. Удалите назначения обычных ролей и ролей делегирования, которые назначают роль создания и членства в группе безопасности группе ролей или универсальной группе безопасности, содержащей в качестве участников администраторов Active Directory, с помощью следующей команды. В этой команде группа ролей "Администраторы Active Directory" используется в качестве примера. Параметр *WhatIf* позволяет узнать, какие назначения ролей будут удалены. Удалите параметр *WhatIf* и запустите команду еще раз, чтобы удалить назначения ролей.

   PowerShell

   ```
   Get-ManagementRoleAssignment -Role "Security Group Creation and
   Membership" | Where { $_.RoleAssigneeName -EQ "Active Directory
   Administrators" } | Remove-ManagementRoleAssignment -WhatIf
   ```

3. Необязательный параметр. Если вы хотите удалить все разрешения Exchange от администраторов Active Directory, вы можете удалить группу ролей или usg, участниками которой они являются. Дополнительные сведения об удалении группы ролей см. в разделе Управление группами ролей.

Дополнительные сведения о синтаксисе и параметрах см. в разделах Get-ManagementRoleAssignment или Remove-ManagementRoleAssignment.

Переключение из режима разделения разрешений Active Directory в режим разрешений общего доступа

Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Разделенные разрешения Active Directory" в разделе Разрешения управления ролями .

Чтобы переключиться с разделенных разрешений Active Directory на общие разрешения Exchange, необходимо повторно запустить программу установки Exchange, чтобы отключить разделенные разрешения Active Directory в организации Exchange, а затем создать назначения ролей между группой ролей и ролью Создания получателя почты и ролью Создание группы безопасности и членство. В конфигурации разрешений общего доступа по умолчанию группа ролей Управление организацией содержит все эти роли. Поэтому группа ролей Управление организацией включена в эту процедуру.

> ⓘ **Важно!**
>
> Команда Setup.exe в этой процедуре вносит изменения в Active Directory. Необходимо использовать учетную запись с разрешениями, требуемыми для выполнения таких изменений. Такая учетная запись может отличаться от учетной записи с разрешениями на создание назначений ролей с помощью командлета **New-ManagementRoleAssignment**. Используйте такую учетную запись (или записи) с разрешениями, необходимыми для успешного выполнения каждого шага этой процедуры.

Чтобы переключиться с разделенных разрешений Active Directory на общие, выполните следующие действия.

1. На целевом сервере откройте проводник, щелкните правой кнопкой мыши скачанный файл ISO-образа Exchange и выберите **Подключить**. Обратите внимание на назначенную букву виртуального DVD-диска.

2. Откройте окно командной строки Windows. Например:

   - Нажмите клавиши Windows + R, чтобы открыть диалоговое окно **Выполнить**, введите cmd.exe и нажмите кнопку **ОК**.

   - Нажмите кнопку **Пуск**. В поле **Поиск** введите **командная строка**, а затем в списке результатов выберите **Командная строка**.

3. В окне командной строки выполните следующую команду:

> ⓘ **Примечание**

- Предыдущий параметр */IAcceptExchangeServerLicenseTerms* не будет работать, начиная с Exchange Server 2016 и Exchange Server 2019 за сентябрь 2021 Обновления г. Теперь необходимо использовать */IAcceptExchangeServerLicenseTerms_DiagnosticDataON* или */IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF* для автоматической установки и установки по сценариям.

- В примерах ниже используется переключатель */IAcceptExchangeServerLicenseTerms_DiagnosticDataON*. Вы можете изменить переключатель на */IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF*.

PowerShell

```
Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON /PrepareAD
/ActiveDirectorySplitPermissions:false
```

4. В командной консоли Exchange выполните следующие команды, чтобы добавить регулярные назначения ролей между ролью создания получателя почты, ролью создания и управления группой безопасности, а также группами ролей "Управление организацией" и "Управление получателями".

   PowerShell

   ```
   New-ManagementRoleAssignment "Mail Recipient Creation_Organization
   Management" -Role "Mail Recipient Creation" -SecurityGroup
   "Organization Management"
   New-ManagementRoleAssignment "Security Group Creation and
   Membership_Org Management" -Role "Security Group Creation and
   Membership" -SecurityGroup "Organization Management"
   New-ManagementRoleAssignment "Mail Recipient Creation_Recipient
   Management" -Role "Mail Recipient Creation" -SecurityGroup "Recipient
   Management"
   ```

5. Перезапустите все серверы Exchange в организации.

Дополнительные сведения о синтаксисе и параметрах см. в разделе New-ManagementRoleAssignment.

Получатели в Exchange Server

Статья • 04.04.2023

Люди и ресурсы, отправляющие и получающие сообщения, являются ядром любой системы организации совместной работы и обмена сообщениями. В организации Exchange эти люди и ресурсы называются *получателями*. Получатель — это любой объект с включенной поддержкой почты в Active Directory, которому служба Microsoft Exchange может доставлять или маршрутизировать сообщения.

Типы получателей Exchange

В Exchange имеется несколько явных типов получателей. Каждый тип получателя определяется в Центре администрирования Exchange (EAC) и имеет уникальное значение в *свойстве RecipientTypeDetails* в командной консоли Exchange. Использование явных типов получателей имеет следующие преимущества.

- Различные типы получателей теперь можно различить с первого взгляда.
- Вы можете осуществлять поиск и сортировку получателей по их типу.
- Проще выполнять операции массового управления над выбранными типами получателей.
- Проще просматривать свойства получателей, так как типы получателей используются в Центре администрирования Exchange для отображения различных страниц свойств. Например, емкость ресурса отображается для почтового ящика помещения, но не отображается для почтового ящика пользователя.

В следующей таблице приведены доступные типы получателей. Эти типы получателей рассматриваются более подробно далее в этом разделе.

Тип получателя	**Описание**
Динамическая группа рассылки	Группа рассылки с фильтрами получателей и условиями, используемыми для немедленной доставки членам группы отправленных сообщений.
Почтовый ящик оборудования	Почтовый ящик ресурса, назначенный ресурсу, который не зависит от расположения, например переносимому компьютеру, проектору, микрофону или корпоративному автомобилю. Почтовые ящики оборудования можно включать в качестве ресурсов в приглашениях на собрания, обеспечивая простой и эффективный способ использования ресурсов для пользователей.
Связанный почтовый ящик	Почтовый ящик, назначенный отдельному пользователю в отдельном доверенном лесу.

Тип получателя	Описание
Почтовый контакт	Контакт Active Directory с поддержкой почты, содержащий сведения о людях или организациях, которые существуют за пределами организации Exchange. У каждого почтового контакта есть внешний адрес электронной почты. Все сообщения, отправляемые почтовому контакту, направляются на этот внешний адрес электронной почты.
Почтовый контакт леса	Почтовый контакт, представляющий объект получателя из другого леса. Контакты почтового леса обычно создаются с помощью синхронизации сервера интеграции удостоверений Майкрософт (MIIS). **Примечание.** Контакты леса почты — это объекты получателей только для чтения, которые обновляются только с помощью MIIS или аналогичной пользовательской синхронизации. Вы не можете использовать EAC или командную консоль Exchange для удаления или изменения почтового контакта леса.
Пользователь почты	Пользователь Active Directory с поддержкой почты, представляющий пользователя за пределами организации Exchange. Каждый пользователь почты имеет внешний адрес электронной почты. Все сообщения, отправляемые почтовому пользователю, направляются на этот внешний адрес электронной почты. Почтовый пользователь похож на почтовый контакт, за исключением того, что почтовый пользователь имеет учетные данные для входа в Active Directory и может получить доступ к ресурсам.
Неуниверсальная группа с включенной поддержкой почты	Глобальный или локальный объект группы Active Directory с поддержкой почты. Неуниверсальные группы с поддержкой почты были прекращены в Exchange Server 2007 году и могут существовать только в том случае, если они были перенесены из Exchange 2003 или более ранних версий Exchange. Вы не можете использовать Exchange Server 2013 для создания неуниверсационных групп рассылки.
Общая папка с включенной поддержкой почты	Общедоступная папка Exchange, настроенная для получения сообщений.
Группы рассылки	Группа рассылки — это объект группы рассылки Active Directory с поддержкой почты, который можно использовать только для распространения сообщений группе получателей.
Группа безопасности с поддержкой электронной почты	Группа безопасности с поддержкой почты — это объект универсальной группы безопасности Active Directory, который можно использовать для назначения разрешений на доступ к ресурсам в Active Directory, а также для распространения сообщений.

Тип получателя	Описание
Получатель Microsoft Exchange	Особый объект получателя, который предоставляет универсального и хорошо известного отправителя сообщений, позволяющего отличать сообщения, созданные системой, от других сообщений. Он заменяет отправителя системного администратора, используемого для системных сообщений в более ранних версиях Exchange.
Почтовый ящик места	Почтовый ящик ресурса, назначенный месту проведения собрания, такому как конференц-зал, аудитория или учебный класс. Почтовые ящики мест могут быть включены в качестве ресурсов в приглашения на собрания, что обеспечивает простой и эффективный способ организации собраний для пользователей.
Общий почтовый ящик	Почтовый ящик, который не назначен непосредственно одному пользователю и, как правило, настроен на разрешение доступа для нескольких пользователей.
Почтовый ящик сайта	Почтовый ящик, состоящий из почтового ящика Exchange для хранения сообщений электронной почты и сайта SharePoint для хранения документов. Пользователи могут получать доступ к сообщениям и документам, используя один и тот же клиентский интерфейс. Дополнительные сведения см. в разделе Почтовые ящики сайта. **Примечание**. Почтовые ящики сайта удаляются из эксплуатации и будут отключены и (или) удалены. Дополнительные сведения см. в статье Прекращение использования почтовых ящиков сайта.
Почтовый ящик пользователя	Почтовый ящик, назначенный отдельному пользователю в организации Exchange. Этот почтовый ящик обычно содержит сообщения, элементы календаря, контакты, задачи, документы и другие важные деловые данные.
Почтовый ящик Microsoft 365 или Office 365	В гибридных развертываниях почтовый ящик Microsoft 365 или Office 365 состоит из почтового пользователя, существующего в локальной среде Active Directory, и связанного облачного почтового ящика, который существует в Exchange Online.
Связанный пользователь	Связанный пользователь — это пользователь, почтовый ящик которого находится в лесу, отличном от того, в котором находится пользователь.

Почтовые ящики

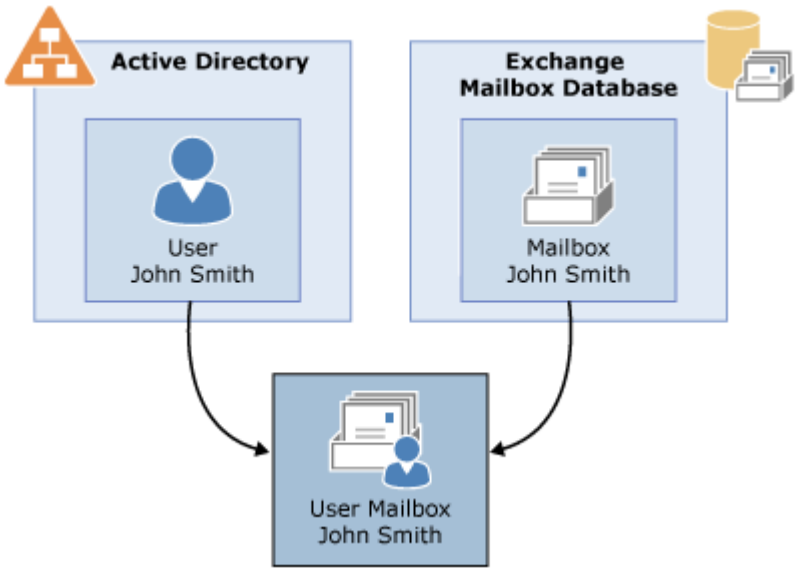
Почтовые ящики — это наиболее распространенный тип получателей, используемый сотрудниками в организации Exchange. Каждый почтовый ящик связан с учетной записью пользователя Active Directory. Пользователь может использовать почтовый ящик для отправки и получения сообщений, а также для хранения сообщений, встреч, задач, заметок и документов. Почтовые ящики — это

основное средство обмена сообщениями и совместной работы для пользователей в организации Exchange.

Компоненты почтового ящика

Каждый почтовый ящик состоит из пользователя Active Directory и данных почтового ящика, хранящихся в базе данных почтовых ящиков Exchange (как показано на следующем рисунке). Все данные конфигурации для почтового ящика хранятся в атрибутах Exchange объекта пользователя Active Directory. В базе данных почтовых ящиков хранятся актуальные данные, находящиеся в почтовом ящике, сопоставленном с учетной записью пользователя.

> ⓘ **Важно!**
>
> При создании почтового ящика для нового или существующего пользователя атрибуты Exchange, необходимые для почтового ящика, добавляются в объект пользователя в Active Directory. Связанные данные почтового ящика не создаются до тех пор, пока почтовый ящик не получит сообщение или пока пользователь не войдет в него.



> ⊗ **Внимание!**
>
> При удалении почтового ящика данные почтового ящика, хранящиеся в базе данных почтовых ящиков Exchange, помечаются для удаления, а связанная учетная запись пользователя также удаляется из Active Directory. Чтобы сохранить учетную запись пользователя и удалить только данные почтового ящика, необходимо отключить почтовый ящик.

Типы почтовых ящиков

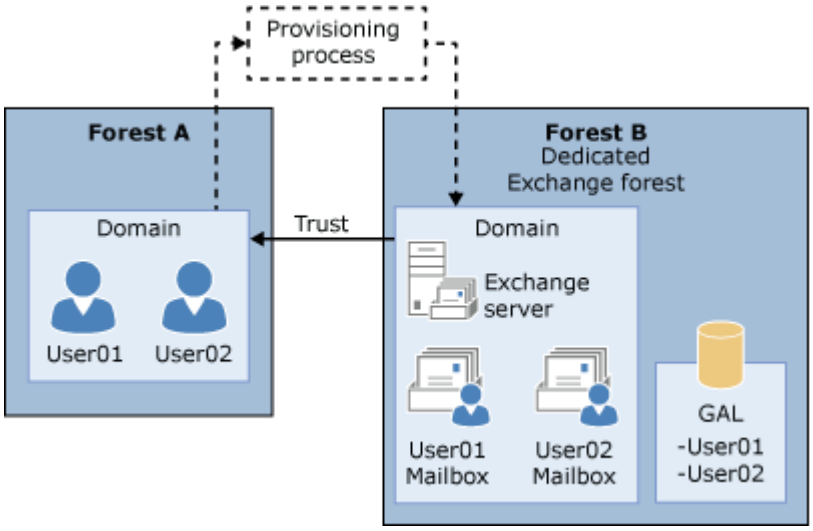
В Exchange поддерживаются следующие типы почтовых ящиков.

- **Почтовые ящики пользователей**. Почтовые ящики пользователей назначаются отдельным пользователям в организации Exchange. Почтовые ящики пользователей предоставляют пользователям обширную платформу для совместной работы. Пользователи могут отправлять и получать сообщения, управлять своими контактами, планировать собрания и вести список задач. Они также могут получать сообщения голосовой почты в свои почтовые ящики. Почтовые ящики пользователей — это наиболее часто используемый тип почтового ящика, который обычно назначается пользователям в вашей организации.

- **Связанные почтовые ящики**. Связанные почтовые ящики — это почтовые ящики, к которым пользователи обращаются в отдельном доверенном лесу. Связанные почтовые ящики могут быть необходимы для организаций, выполнивших развертывание Exchange в лесу ресурсов. Сценарий леса ресурсов позволяет организации централизовать Exchange в одном лесу, одновременно обеспечивая доступ к организации Exchange, в которой учетные записи пользователей находятся в одном или нескольких доверенных лесах.

  Как говорилось ранее, с каждым почтовым ящиком должна быть сопоставлена учетная запись пользователя. Однако учетная запись пользователя, которая обращается к связанному почтовому ящику, не существует в лесу, где развернут Exchange. Таким образом, отключенная учетная запись пользователя, существующая в том же лесу, что и Exchange, связана с каждым связанным почтовым ящиком. На следующем рисунке показана связь между связанной учетной записью пользователя, которая используется для доступа к связанному почтовому ящику, и отключенной учетной записью пользователя в лесу ресурсов Exchange, связанной с этим почтовым ящиком.

  Связанный почтовый ящик



- **Почтовые ящики Microsoft 365 или Office 365**. При создании почтового ящика Microsoft 365 или Office 365 в Exchange Online в гибридном развертывании почтовый пользователь создается в локальной среде Active Directory. Синхронизация каталогов, если она настроена, автоматически синхронизирует этот новый объект пользователя с Microsoft 365 или Office 365, где он преобразуется в облачный почтовый ящик в Exchange Online. Вы можете создавать microsoft 365 или Office 365 почтовые ящики как обычные почтовые ящики пользователей, почтовые ящики ресурсов для конференц-залов и оборудования, а также общие почтовые ящики.

- **Общие почтовые ящики**. Общие почтовые ящики в основном не связаны с отдельными пользователями и обычно настраиваются для разрешения доступа нескольких пользователей.

  Несмотря на то что разрешения на вход в любой почтовый ящик можно предоставить любому количеству дополнительных пользователей, для реализации этой возможности специально предназначены общие почтовые ящики. Пользователь Active Directory, связанный с общим почтовым ящиком, должен быть отключенной учетной записью. После создания общего почтового ящика следует назначить соответствующие разрешения всем пользователям, которым необходим доступ к этому ящику.

- **Почтовые ящики ресурсов**. Почтовые ящики ресурсов — это специальные почтовые ящики, предназначенные для планирования ресурсов. Как и все типы почтовых ящиков, почтовый ящик ресурса имеет связанную учетную запись пользователя Active Directory, но это должна быть отключенная учетная запись. Доступны следующие типы почтовых ящиков ресурсов.

  - **Почтовые ящики комнат**. Эти почтовые ящики назначаются местам проведения собраний, таким как конференц-залы, аудитории и учебные комнаты.

- **Почтовые ящики оборудования**. Эти почтовые ящики назначаются ресурсам, не зависящим от расположения, таким как портативные компьютеры, проекторы, микрофоны или автомобили компании.

  Вы можете включить оба типа почтовых ящиков ресурсов в приглашения на собрания, что обеспечивает простой и эффективный способ использования ресурсов пользователями. Вы можете настроить почтовые ящики ресурсов для автоматической обработки входящих запросов на собрания на основе политик резервирования ресурсов, определенных владельцами ресурсов. Например, можно настроить конференц-зал для автоматического приема входящих запросов на собрания, за исключением повторяющихся собраний, которые могут быть утверждены владельцем ресурса.

Системные почтовые ящики

Системные почтовые ящики создаются Exchange в корневом домене леса Active Directory во время установки. Пользователи и администраторы не могут входить в эти почтовые ящики. Системные почтовые ящики создаются для функций Exchange, таких как единая система обмена сообщениями, миграция, утверждение сообщений и обнаружение электронных данных на месте. В этой таблице перечислены сведения о системных почтовых ящиках, отображаемых в Active Directory.

> ⓘ **Примечание**
>
> Единая система обмена сообщениями недоступна в Exchange 2019

Mailbox	**Имя**
Организация	`SystemMailbox {bb558c35-97f1-4cb9-8ff7-d53741dc928c}`
Утверждение сообщений	`SystemMailbox {1f05a927-xxxx-xxxx-xxxx-xxxxxxxxxxxx_}` где `xxxx-xxxx-xxxx-xxxxxxxxxxxx` — это случайно назначаемый уникальный идентификатор GUID для каждого леса Exchange.
Хранилище данных единой системы обмена сообщениями	`SystemMailbox {e0dc1c29-89c3-4034-b678-e6c29d823ed9}` Этот почтовый ящик существует в Exchange 2016, а не в Exchange 2019
Обнаружение	`DiscoverySearchMailbox {D919BA05-46A6-415f-80AD-7E09334BB852}`

Mailbox	Имя
Федеративная электронная почта	`FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042`
Миграция	`Migration.8f3e7716-2011-43e4-96b1-aba62d229136`

Чтобы списать последний сервер почтовых ящиков в организации Exchange, сначала следует отключить эти системные почтовые ящики с помощью командлета Disable-Mailbox. При списании сервера почтовых ящиков, содержащего эти системные почтовые ящики, следует переместить их на другой сервер почтовых ящиков, чтобы не потерять функциональность.

Планирование почтовых ящиков

Почтовые ящики создаются в базах данных почтовых ящиков на серверах Exchange с установленной ролью сервера почтовых ящиков. Чтобы обеспечить надежную и эффективную платформу для пользователей почтовых ящиков, необходимо тщательное планирование развертывания серверов почтовых ящиков и баз данных. Дополнительные сведения о планировании серверов почтовых ящиков и баз данных см. в статье Планирование и развертывание.

Группы рассылки

Группы рассылки — это объекты групп Active Directory с поддержкой почты, которые в основном используются для распространения сообщений среди нескольких получателей. Членом группы рассылки может быть получатель любого типа.

> ⓘ **Важно!**
>
> Обратите внимание на различия в терминологии между Active Directory и Exchange. В службе каталогов Active Directory группа рассылки означает любую группу, для которой не создан контекст безопасности, независимо от того, была ли включена поддержка почты для этой группы или нет. В Exchange все группы с включенной поддержкой почты считаются группами рассылки независимо от того, был ли создан для них контекст безопасности или нет.

Exchange поддерживает следующие типы групп рассылки:

- **Группы рассылки**. Это объекты универсальной группы рассылки Active Directory с поддержкой почты. Они используются только для рассылки сообщений группе получателей.

- **Группы безопасности с поддержкой почты**. Это объекты универсальной группы безопасности Active Directory с поддержкой почты. Их можно использовать для назначения разрешений на доступ к ресурсам в Active Directory, а также для распространения сообщений.

- **Неуниверсационные группы с поддержкой почты**. Это глобальные или локальные объекты Active Directory с поддержкой почты. Можно создавать только универсальные группы рассылки или включать поддержку почты только для этих групп. У вас могут быть группы с поддержкой почты, перенесенные из предыдущих версий Exchange, которые не являются универсальными группами. Этими группами по-прежнему можно управлять с помощью EAC или командной консоли Exchange.

  > ⓘ **Примечание**
  >
  > Чтобы преобразовать локальную или глобальную группу домена в универсальную группу, можно использовать командлет **Set-Group** в командной консоли Exchange.

Динамические группы рассылки

Динамические группы рассылки — это группы рассылки, членство в которых основано на заданных фильтрах получателей, а не на определенном списке получателей.

В отличие от обычных групп рассылки, список членов для динамических групп рассылки рассчитывается каждый раз при отправке сообщения в такую группу в соответствии с задаваемыми фильтрами и условиями. Когда сообщение электронной почты отправляется в динамическую группу рассылки, оно доставляется всем получателям в организации, подходящим под заданные для группы критерии.

> ⓘ **Важно!**
>
> Динамическая группа рассылки включает любого получателя в Active Directory, который имеет атрибуты, соответствующие фильтру группы на момент отправки сообщения. Если после изменения свойств получателя они начинают

отвечать критериям фильтра группы, такой получатель может непреднамеренно стать членом группы и начать получать сообщения, отправляемые в динамическую группу рассылки. Строгий и последовательный процесс подготовки учетной записи позволяет снизить вероятность возникновения такой ситуации.

Для облегчения создания фильтров получателей для динамических групп рассылки можно использовать предустановленные фильтры. *Предустановленный фильтр* — это часто используемый фильтр, который учитывает различные критерии фильтрации получателей. Эти фильтры можно использовать, чтобы указать типы получателей, которые необходимо включить в динамическую группу рассылки. Кроме того, можно также указать список условий, которым должны соответствовать получатели. Можно создавать предустановленные условия на основе следующих свойств:

- Настраиваемые атрибуты 1–15
- Область, край;
- Организация
- Отдел
- Контейнер получателей

Можно также указать условия на основе свойств получателей, которые отличаются от вышеуказанных. Чтобы создать настраиваемый запрос для динамической группы рассылки, необходимо использовать командную консоль Exchange. Помните, что параметрами фильтра и условий для динамических групп рассылки с настраиваемыми фильтрами получателей можно управлять только с помощью командной консоли Exchange. Пример создания динамической группы рассылки с помощью пользовательского запроса см. в разделе Управление динамическими группами рассылки.

Почтовые контакты

Почтовые контакты обычно содержат сведения о людях или организациях, которые существуют за пределами вашей организации Exchange. Почтовые контакты могут отображаться в общей адресной книге вашей организации (также называемой глобальным списком адресов или gal) и другими списками адресов, а также могут быть добавлены в качестве участников в группы рассылки. У каждого контакта есть внешний адрес электронной почты, и все сообщения электронной почты, отправляемые контакту, автоматически пересылаются на этот адрес. Контакты идеально подходят для представления людей за пределами организации

Exchange (в общей адресной книге), которым не нужен доступ к внутренним ресурсам. Ниже перечислены типы почтовых контактов.

- **Почтовые контакты**. Это контакты Active Directory с поддержкой почты, которые содержат сведения о людях или организациях, которые существуют за пределами вашей организации Exchange.
- **Контакты почтового леса**. Они представляют объекты получателей из другого леса. Эти контакты обычно создаются при синхронизации службы каталогов. Почтовые контакты леса — это предназначенные только для чтения объекты получателей, поддерживающие обновление и удаление только с помощью синхронизации. Вы не можете использовать интерфейсы управления Exchange для изменения или удаления почтового контакта леса.

Почтовые пользователи

Пользователи почты сходны с почтовыми контактами. Оба имеют внешние адреса электронной почты, оба содержат сведения о людях за пределами вашей организации Exchange, и оба могут отображаться в общей адресной книге и других списках адресов. Однако, в отличие от почтового контакта, пользователи почты имеют учетные данные для входа в Active Directory и могут обращаться к ресурсам, которым им назначены разрешения.

Если лицу, находящемуся за пределами организации, необходим доступ к ресурсам во внутренней сети, для него следует создать пользователя почты, а не почтовый контакт. Например, для временных консультантов, которым требуется доступ к серверной инфраструктуре организации, но которые при этом будут пользоваться своими внешними адресами, можно создать почтовых пользователей.

Другой сценарий — создание пользователей почты в организации для пользователей, которые не хотят обслуживать почтовый ящик Exchange. Например, после приобретения приобретенная компания может поддерживать отдельную инфраструктуру обмена сообщениями, но также может потребоваться доступ к ресурсам в вашей сети. Для этих пользователей может потребоваться создать пользователей почты вместо пользователей почтовых ящиков.

> ⓘ **Примечание**
>
> В EAC вы используете страницу **Контакты получателей**для создания пользователей почты > и управления ими. Отдельная страница для почтовых пользователей отсутствует.

Общедоступные папки с включенной поддержкой почты

Общие папки служат хранилищем общих данных для большого количества пользователей. Включение поддержки почты для общих папок представляет собой введение дополнительного уровня возможностей для пользователей. Пользователи могут не только помещать в папку сообщения, но также отправлять в общедоступную папку сообщения электронной почты, а иногда и получать их от нее. Каждая папка с поддержкой почты содержит объект в Active Directory, который хранит свой адрес электронной почты, имя адресной книги и другие атрибуты, связанные с почтой.

Вы можете управлять общедоступными папками с помощью EAC или командной консоли Exchange. Дополнительные сведения об управлении общедоступными папками см. в разделе Общедоступные папки.

Получатель Microsoft Exchange

Получатель Microsoft Exchange — это специальный объект получателя, предоставляющий унифицированный и хорошо известный отправитель сообщений, который отличает созданные системой сообщения от других сообщений. Он заменяет отправителя системного администратора, который использовался для системных сообщений в более ранних версиях Exchange.

Получатель Microsoft Exchange не является типичным объектом получателя, например почтовым ящиком, почтовым пользователем или почтовым контактом, и он не управляется с помощью стандартных средств получателя. Однако для настройки получателя Microsoft Exchange можно использовать командлет Set-OrganizationConfig в командной консоли Exchange.

> ⓘ **Примечание**
>
> При отправке системных сообщений внешнему отправителю получатель Microsoft Exchange не используется в качестве отправителя сообщения. Вместо этого используется адрес электронной почты, заданный параметром *ExternalPostmasterAddress* командлета **Set-TransportConfig**.

Документация о получателях

В следующей таблице приведены ссылки на разделы, в которых можно узнать больше о получателях в Exchange и управлении ими.

Статья	Описание
Создание почтовых ящиков пользователей в Exchange Server	Узнайте, как создавать почтовые ящики пользователей с помощью Центра администрирования Exchange или командной консоли Exchange.
Управление почтовыми ящиками пользователей	Узнайте, как создавать почтовые ящики пользователей, изменять их свойства и выполнять групповую настройку выбранных свойств для нескольких почтовых ящиков.
Управление группами рассылки	Узнайте о том, как создавать группы рассылки, настраивать их, а также о том, как создать политику именования групп для организации.
Управление динамическими группами рассылки	Узнайте, как создавать динамические группы рассылки и управлять их свойствами, в том числе использовать настраиваемые атрибуты и другие свойства для определения членства в группе.
Управление почтовыми контактами	Узнайте, как создавать почтовые контакты и управлять ими.
Управление пользователями почты	Узнайте, как создавать почтовых пользователей и управлять ими.
Создание почтовых ящиков помещений и управление ими	Узнайте, как создавать почтовые ящики помещений и управлять их свойствами, в том числе включать повторяющиеся собрания и настраивать параметры резервирования и планирования.
Управление почтовыми ящиками оборудования	Узнайте, как создавать почтовые ящики оборудования, управлять их свойствами, а также настраивать параметры резервирования и планирования.
Отключенные почтовые ящики	Узнайте о двух типах отключенных почтовых ящиков и способах работы с ними.
Настраиваемые атрибуты.	Узнайте, как добавлять информацию о получателе с помощью настраиваемых атрибутов.
Фильтры в командах получателей для командной консоли	Узнайте, как использовать предустановленные или настраиваемые фильтры с командами, чтобы фильтровать список получателей.
Управление разрешениями для получателей	Узнайте, как использовать EAC или командную консоль Exchange для назначения разрешений пользователям и группам.

Статья	Описание
Автоматическое распределение почтовых ящиков	Узнайте о том, как работает автоматическое распространение почтовых ящиков, и как управлять выбором баз данных почтовых ящиков для новых и перемещенных почтовых ящиков.

Создание почтовых ящиков пользователей в Exchange Server

Статья • 04.04.2023

Почтовые ящики пользователя — это почтовые ящики Exchange, сопоставленные с пользователями (обычно один почтовый ящик на пользователя). Каждый почтовый ящик пользователя сопоставлен с учетной записью Active Directory, с помощью которой пользователь может входить в почтовый ящик для отправки и получения электронных сообщений, создания собраний и встреч.

При создании почтового ящика в Exchange можно также сразу создать соответствующего пользователя Active Directory. Можно также создать почтовый ящик для существующей учетной записи Active Directory, которая не сопоставлена с почтовым ящиком. Это называется *включением поддержки почтовых ящиков* для существующих пользователей.

Почтовые ящики пользователей можно создавать в Exchange Server с помощью Центра администрирования Exchange (EAC) или командной консоли Exchange. В приведенной ниже таблице описаны некоторые важные свойства для почтовых ящиков пользователей.

Свойство	**Обязательное или необязательное**	**Описание**
Alias (Псевдоним)	Необязательный	Псевдоним Exchange (также известный как *почтовый псевдоним*) для почтового ящика. Максимальная длина: 64 символа. Допустимые символы: буквы, числа и текстовые символы ASCII, разрешенные в электронных адресах. Например, точки разрешены, но каждая точка должна быть окружена другими допустимыми символами (например, pilar.pinilla). Значение псевдонима используется для создания основного адреса электронной *почты (<домена псевдонима>@ <).*> Если не указать значение псевдонима, используется часть имени учетной записи (имя участника-пользователя). Значение псевдонима должно быть уникальным. **Примечание**. Не используйте апострофы (') или кавычки (") в псевдониме. Хотя эти символы разрешены, они могут вызывать проблемы позже.

Свойство	Обязательное или необязательное	Описание
Отображаемое имя	Для Центра администрирования Exchange: обязательное Для командной консоли Exchange: необязательное	Определяет почтовый ящик в Центре администрирования Exchange, а также в списках адресов в Outlook и Outlook в Интернете (предыдущее имя — Outlook Web App). Максимальная длина: 256 символов. Допускаются пробелы и другие символы. В Центре администрирования Exchange отображаемое имя заполняется значениями, введенными для имени, отчества и фамилии, но можно указать пользовательское значение. В командной консоли Exchange используется значение свойства **Имя**, если не указать значение для отображаемого имени. Значение отображаемого имени не должно быть уникальным, но использование нескольких почтовых ящиков с одинаковым отображаемым именем вызовет путаницу.
Имя	Обязательный	Указывает имя объекта в Active Directory. Только администраторы могут видеть это значение в средствах управления в Exchange или Active Directory. Максимальная длина: 64 символа. Допускаются пробелы и другие символы. Значение имени должно быть уникальным.

Что нужно знать перед началом работы

- Предполагаемое время выполнения каждой задачи для почтового ящика пользователя: от 2 до 5 минут.
- Дополнительные сведения о EAC см. в разделе Центр администрирования Exchange в Exchange Server. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения подготовки получателей" раздела Разрешения получателей .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

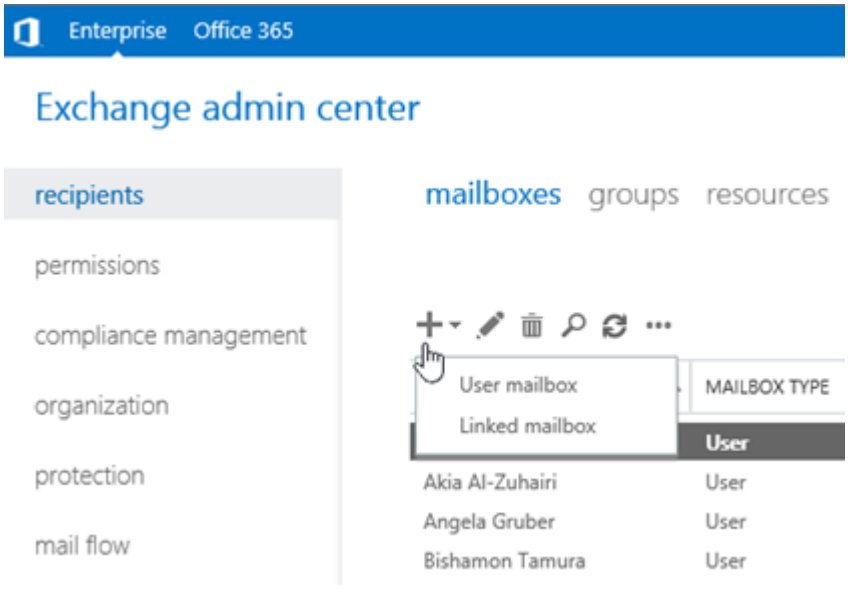
> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Создание почтовых ящиков пользователей

В этом разделе показано, как создать почтовый ящик и сопоставленную учетную запись пользователя в Active Directory.

Создание почтовых ящиков пользователей в Центре администрирования Exchange

1. В EAC перейдите в раздел **Почтовые ящики получателей**>.
2. Нажмите кнопку **Создать** (+ А затем выберите **Почтовый ящик пользователя**.



Примечание. Связанный почтовый ящик — это локальный почтовый ящик, связанный с учетной записью пользователя в другом (доверенном) лесу Active Directory. Дополнительные сведения см. в разделе Управление связанными почтовыми ящиками.

3. На странице **Новый почтовый ящик пользователя** настройте указанные ниже параметры. Обязательные параметры отмечены звездочкой (*).

   - **Alias**

- **Существующий пользователь** или **Новый пользователь**. Выберите **Новый пользователь**.
- **Имя**
- **Инициалы**
- **Фамилия**
- * **Отображаемое имя**. По умолчанию это поле заполняется именами, которые вы вводите в **полях Имя**, **Инициалы** и **Фамилия** , но его можно переопределить. Максимальная длина имени составляет 256 символов.
- * **Имя**. По умолчанию это поле заполняется именами, которые вы вводите в поля **Имя**, **Инициалы** и **Фамилия** , но вы можете переопределить его. Максимальная длина — 64 символа, и значение должно быть уникальным в вашей организации.
- **Подразделение**. Обычно по умолчанию для учетной записи пользователя используется контейнер "Пользователи". Чтобы изменить его, нажмите кнопку **Обзор** и укажите подразделение или контейнер, в котором хотите создать учетную запись.
- * **Имя входа пользователя**. Это учетная запись пользователя Active Directory, созданная и связанная с почтовым ящиком.

Примечания.

- Не используйте апострофы (') или кавычки ("). Хотя эти символы разрешены, они могут вызывать проблемы позже (например, при назначении прав доступа к почтовому ящику).
- Если это значение отличается от значения параметра **Псевдоним**, электронный адрес и имя учетной записи пользователя будут отличаться (это важно, если домен электронной почты и домен Active Directory совпадают).
- * **Новый пароль**: убедитесь, что значение соответствует требованиям к длине пароля, сложности и журналу вашей организации.
- * **Подтвердите пароль**.
- **Требовать изменения пароля при следующем входе**. Установите этот флажок, чтобы заставить пользователя изменить первоначальный пароль при первом входе в почтовый ящик.

4. Можно нажать кнопку **Сохранить**, чтобы создать почтовый ящик и сопоставленную учетную запись пользователя в Active Directory, либо выбрать элемент **Дополнительные параметры**, чтобы настроить указанные ниже дополнительные параметры.

    - **База данных почтовых ящиков**. Нажмите кнопку **Обзор** , чтобы выбрать базу данных почтовых ящиков, в которой хранится почтовый ящик.

    - **Создание локального архивного почтового ящика для этого пользователя**. Установите этот флажок, чтобы создать архивный почтовый ящик для почтового ящика, а затем нажмите кнопку **Обзор** , чтобы выбрать базу данных почтовых ящиков, в которой хранится архивный почтовый ящик. Элементы автоматически перемещаются из основного почтового ящика в архив, при этом учитываются параметры политики хранения. Дополнительные сведения см. в статье Архивация на месте в Exchange Server.

    - **Политика адресной книги**: ASP определяют глобальный список адресов (GAL), автономную адресную книгу (OAB), список помещений и набор списков адресов. ABP предоставляет пользователю доступ к настраиваемой глобальной записи в Outlook и Outlook в Интернете. Дополнительные сведения см. в разделе Политики адресных книг в Exchange Server.

    По завершении нажмите кнопку **Сохранить**.

Создание почтовых ящиков пользователей с помощью командной консоли Exchange

Чтобы создать почтовый ящик пользователя в командной консоли Exchange, используйте следующий синтаксис:

PowerShell

```
New-Mailbox -Name <Name> -UserPrincipalName <UPN> -Password (ConvertTo-SecureString -String '<Password>' -AsPlainText -Force) [-Alias <Alias>] [-FirstName <FirstName>] [-LastName <LastName>] [-DisplayName <DisplayName>] -[OrganizationalUnit <OU>]
```

Приведенный ниже пример кода создает почтовый ящик и учетную запись Active Directory для пользователя Pilar Pinilla со следующими параметрами:

- **Обязательные параметры:**

- *Имя*: Пилар Пинилья. Это значение также используется для отображаемого имени, так как мы не используем параметр *DisplayName* .
- *UserPrincipalName*: имя учетной записи Active Directory — `pilarp@contoso.com`.
- *Пароль*: `Pa$$word1`

- **Необязательные параметры:**
  - *FirstName*: Pilar
  - *LastName*: Pinilla
  - Значение псевдонима связано `pilarp` с тем, что мы не используем параметр *Alias* и `pilarp` берется из значения параметра *UserPrincipalName* .

PowerShell

```
New-Mailbox -Name "Pilar Pinilla" -UserPrincipalName pilarp@contoso.com -
Password (ConvertTo-SecureString -String 'Pa$$word1' -AsPlainText -Force) -
FirstName Pilar -LastName Pinilla
```

Дополнительные сведения о синтаксисе и параметрах см. в статье New-Mailbox.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли создан почтовый ящик пользователя, выполните одно из указанных ниже действий.

- В EAC перейдите в раздел **Почтовые ящики получателей**> и убедитесь, что почтовый ящик отображается в списке.
- В командной консоли Exchange замените <*Name*> используемым значением параметра *Name* и выполните следующую команду:

  PowerShell

  ```
  Get-Mailbox -Identity <Name> | Format-List
  Name,DisplayName,Alias,PrimarySmtpAddress,Database
  ```

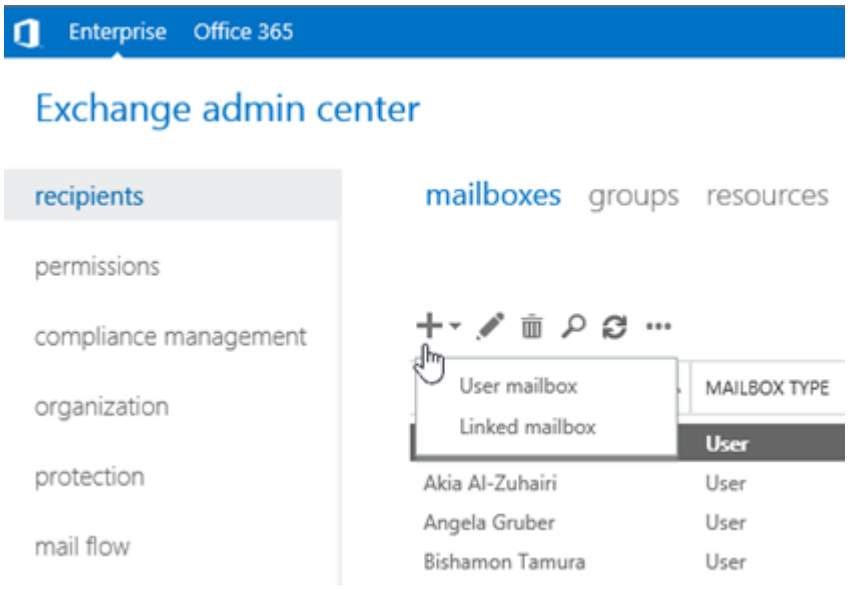
Создание почтовых ящиков для существующих учетных записей

пользователей

При включении поддержки почтовых ящиков для учетных записей пользователей можно выбирать только существующих пользователей Active Directory, для которых еще не включена поддержка почты (то есть почтовых пользователей или учетные записи, с которыми не сопоставлены почтовые ящики).

Создание почтовых ящиков для существующих учетных записей пользователей с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел **Почтовые ящики получателей**>.
2. Нажмите кнопку **Создать** (+ А затем выберите **Почтовый ящик пользователя**.



3. На странице **Новый почтовый ящик пользователя** настройте указанные ниже параметры.

   - **Псевдоним**. Этот параметр является необязательным.

     Примечания.

     - Не используйте апострофы (') или кавычки ("). Хотя эти символы разрешены, они могут вызывать проблемы позже.
     - Если это значение отличается от имени имени участника-пользователя, адрес электронной почты и имя учетной записи пользователя будут отличаться (важно, если домен электронной почты и домен Active Directory совпадают).

- **Существующий пользователь** или **Новый пользователь**. Убедитесь, что выбран **существующий пользователь** , а затем нажмите кнопку **Обзор** , чтобы выбрать доступную учетную запись.

4. Можно нажать кнопку **Сохранить**, чтобы создать почтовый ящик, либо выбрать **Дополнительные параметры**, чтобы настроить указанные ниже дополнительные параметры.

   - **База данных почтовых ящиков**. Нажмите кнопку **Обзор** , чтобы выбрать базу данных почтовых ящиков, в которой хранится почтовый ящик.

   - **Создание локального архивного почтового ящика для этого пользователя**. Установите этот флажок, чтобы создать архивный почтовый ящик для почтового ящика, а затем нажмите кнопку **Обзор** , чтобы выбрать базу данных почтовых ящиков, в которой хранится архивный почтовый ящик. Элементы автоматически перемещаются из основного почтового ящика в архив, при этом учитываются параметры политики хранения. Дополнительные сведения см. в статье Архивация на месте в Exchange Server.

   - **Политика адресной книги**: ASP определяют глобальный список адресов (GAL), автономную адресную книгу (OAB), список помещений и набор списков адресов. ABP предоставляет пользователю доступ к настраиваемой глобальной записи в Outlook и Outlook в Интернете. Дополнительные сведения см. в разделе Политики адресных книг в Exchange Server.

   По завершении нажмите кнопку **Сохранить**.

Создание почтовых ящиков для существующих учетных записей пользователей с помощью командной консоли Exchange

Чтобы создать почтовый ящик для существующей учетной записи пользователя, используйте следующий синтаксис:

PowerShell

```
Enable-Mailbox -Identity <Account> [-Alias <Alias>] [-DisplayName
<DisplayName>] [-Database <Database>]
```

В этом примере создается почтовый ящик в базе данных почтовых ящиков с именем UsersMailboxDatabase для существующего пользователя Kathleen Reiter,

имя учетной записи которого (имя участника-пользователя) имеет значение kreiter@contoso.com.

- Так как мы не используем параметр *Alias* , значение псевдонима — `kreiter`.
- Так как мы не используем параметр *DisplayName* , значение атрибута **name** в Active Directory используется в качестве отображаемого имени.

PowerShell

```
Enable-Mailbox -Identity kreiter@contoso.com -Database UsersMailboxDatabase
```

Этот пример кода находит все учетные записи пользователей, для которых не включена поддержка почты и которые не системные (атрибут **userPrincipalName** не пустой), а затем создает почтовые ящики для таких учетных записей.

PowerShell

```
Get-User -RecipientTypeDetails User -Filter "UserPrincipalName -ne `$null" -
ResultSize unlimited | Enable-Mailbox
```

Дополнительные сведения о синтаксисе и параметрах см. в статьях Enable-Mailbox и Get-User.

Как проверить, все ли получилось?

Чтобы убедиться в том, что почтовый ящик для существующего пользователя успешно создан, выполните одно из указанных ниже действий.

- В EAC перейдите в раздел **Почтовые ящики получателей**> и убедитесь, что почтовый ящик отображается в списке.
- В командной консоли Exchange замените <*Name*> атрибутом name пользователя и выполните следующую команду:

  PowerShell

  ```
  Get-Mailbox -Identity <Name> | Format-List
  Name,DisplayName,Alias,PrimarySmtpAddress,Database
  ```

Управление почтовыми ящиками пользователей

Статья • 04.04.2023

После создания почтового ящика пользователя можно внести изменения и задать дополнительные свойства с помощью EAC или командной консоли Exchange.

Также можно одновременно менять свойства нескольких почтовых ящиков пользователей. Дополнительные сведения см . в статье Использование EAC для массового изменения почтовых ящиков пользователей.

Что нужно знать перед началом работы

- Предполагаемое время выполнения каждой задачи для почтового ящика пользователя: от 2 до 5 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения подготовки получателей" раздела Разрешения получателей .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Изменение свойств почтового ящика пользователя

Использование Центра администрирования Exchange для настройки свойств почтового ящика пользователя

1. В Центре администрирования Exchange (EAC) выберите **Получатели**>**Почтовые ящики**.

2. В списке почтовых ящиков пользователей щелкните почтовый ящик, для которого требуется изменить свойства, а затем щелкните **Изменить**.✎

3. На странице свойств почтового ящика щелкните один из следующих разделов, чтобы просмотреть или изменить свойства.

    - Общие
    - Заполнение почтового ящика
    - Контактные данные
    - Организация
    - Адрес электронной почты
    - Функции почтового ящика
    - Участник
    - Подсказка
    - Mailbox Delegation

Общие

В разделе **Общие** можно просматривать и изменять основные сведения о пользователе.

- **Имя**, **Отчество**, **Фамилия**
- * **Имя**: это имя, указанное в Active Directory. Если вы решите изменить это имя, помните, что оно не может превышать 64 символа.
- * **Отображаемое имя**: это имя отображается в адресной книге вашей организации, в строках "По" и "От": в сообщении электронной почты, а также в списке почтовых ящиков. Это имя не может содержать пробелы до или после отображаемого имени.
- * **Псевдоним**: указывает псевдоним электронной почты для пользователя. Псевдоним пользователя — это часть адреса электронной почты слева от символа (@). Псевдоним должен быть уникальным в пределах леса.
- * **Имя входа пользователя**. Это имя, которое пользователь использует для входа в свой почтовый ящик и для входа в домен. Обычно имя пользователя для входа состоит из псевдонима пользователя в левой части символа @, а

доменное имя, в котором находится учетная запись пользователя, в правой части символа @.

- **Требовать изменение пароля при следующем входе**. Установите этот флажок, если вы хотите, чтобы пользователь сбросил пароль при следующем входе в почтовый ящик.

- **Скрыть из списков адресов**. Установите этот флажок, чтобы предотвратить отображение получателя в адресной книге и других списках адресов, определенных в организации Exchange. После установки этого флажка пользователи все еще могут отправлять сообщения этому получателю на его адрес электронной почты.

Щелкните **Дополнительные параметры**, чтобы просмотреть или изменить дополнительные свойства:

- **Подразделение**. В этом поле только для чтения отображается подразделение, содержащее учетную запись пользователя. Чтобы переместить учетную запись пользователя в другое подразделение, необходимо использовать средство "Пользователи и компьютеры Active Directory".

- **База данных почтовых ящиков**. В этом поле только для чтения отображается имя базы данных почтовых ящиков, в котором размещается почтовый ящик. Чтобы переместить почтовый ящик в другую базу данных, выберите его в списке почтовых ящиков, а затем щелкните **Переместить почтовый ящик в другую базу данных** в области Сведения.

- **Настраиваемые атрибуты**. В этом разделе отображаются настраиваемые атрибуты, определенные для почтового ящика пользователя. Чтобы указать собственные значения атрибутов, нажмите **Изменить**. Для получателя можно указать до 15 настраиваемых атрибутов.

Заполнение почтового ящика

Используйте раздел **Заполнение почтового ящика** для просмотра и изменения квот хранения и параметров хранения удаленных элементов для почтового ящика. Эти параметры настраиваются по умолчанию при создании почтового ящика. Они используют значения, настроенные для базы данных почтовых ящиков и применяемые ко всем почтовым ящикам в этой базе данных. Можно настроить эти параметры для каждого почтового ящика, а не использовать установленные по умолчанию настройки базы данных почтовых ящиков.

- **Последний вход**. В этом поле только для чтения отображается время последнего входа пользователя в почтовый ящик.
- **Использование почтового ящика**. В этой области отображается общий размер почтового ящика и процент использованной общей квоты почтового ящика.

> ⓘ **Примечание**
>
> Чтобы получить отображаемые в предыдущих двух полях сведения, центр администрирования Exchange отправляет запрос в базу данных почтовых ящиков, в которой размещен этот почтовый ящик. Если вам не удалось выполнить в EAC подключение к хранилищу Exchange, где находится база данных почтовых ящиков, это поле остается пустым. Если пользователь не вошел в почтовый ящик в первый раз, отображается предупреждающее сообщение.

Нажмите кнопку **Дополнительные параметры**, если нужно просмотреть или изменить квоту хранилища почтового ящика и параметры хранения удаленных элементов для почтового ящика.

- **Параметры квоты хранилища**. Чтобы настроить эти параметры для почтового ящика и не использовать значения по умолчанию базы данных почтовых ящиков, щелкните **Настроить параметры для этого почтового ящика**, введите новое значение и нажмите кнопку **Сохранить**.

  Диапазон значений для каждого из параметров квоты хранилища составляет от 0 до 2 047 гигабайт (ГБ).

  - **Выдача предупреждения в (ГБ):** в этом поле отображается максимальный объем хранилища, прежде чем пользователю будет выдано предупреждение. Если размер почтового ящика равен указанному значению или превышает его, пользователю этого ящика на сервере Exchange отправляется предупреждающее сообщение.
  - **Запретить отправку в (ГБ):** в этом поле отображается ограничение *запрета отправки* для почтового ящика. Если размер почтового ящика достигнет указанного значения или превысит его, пользователь не сможет отправлять новые сообщения — появится сообщение об ошибке.
  - **Запретить отправку и получение в (ГБ).** В этом поле отображается ограничение *запрета на отправку и получение* для почтового ящика. Если размер почтового ящика достигнет указанного значения или превысит его,

пользователь почтового ящика не сможет отправлять и получать новые сообщения. Сообщения, отправляемые в почтовый ящик, будут возвращаться отправителю с сообщением об ошибке.

- **Параметры хранения удаленных элементов**. Чтобы настроить эти параметры для почтового ящика и не использовать значения по умолчанию базы данных почтовых ящиков, щелкните **Настройка параметров для этого почтового ящика**, введите новое значение и нажмите кнопку **Сохранить**.
    - **Хранить удаленные элементы в течение (дней)**: в этом поле отображается время хранения удаленных элементов, прежде чем они будут окончательно удалены и не могут быть восстановлены пользователем. По окончании этого срока удаленные элементы удаляются без возможности восстановления. По умолчанию для базы данных почтовых ящиков настроено хранение удаленных элементов в течение 14 дней. Диапазон значений этого свойства находится в пределах от 0 до 24 855 дней.
    - **Не удаляйте элементы без возможности восстановления до создания резервной копии базы данных**. Установите этот флажок, чтобы запретить удаление почтовых ящиков и сообщений электронной почты до тех пор, пока не будет создана резервная копия базы данных почтовых ящиков, в которой находится почтовый ящик.

Контактные данные

В разделе **Сведения о контактах** можно просмотреть или изменить контактные данные пользователя. Информация на этой странице отображается в адресной книге. Нажмите кнопку **Дополнительные сведения** для отображения дополнительных полей.

> **Совет**
>
> Поле **Область/Край** можно использовать, чтобы создать условия получателей для образования динамической группы рассылки, политики адресов электронной почты или списка адресов.

Пользователи почтовых ящиков могут использовать Outlook или Outlook в Интернете (прежнее название — Outlook Web App) для просмотра и изменения своих контактных данных. Однако они не могут изменять данные в полях **Заметки** и **Веб-страница**.

Организация

В разделе **Организация** можно указать подробные сведения о роли пользователя в организации. Эти данные отображаются в адресной книге. Кроме того, можно создать виртуальную организационную диаграмму, доступную для таких почтовых клиентов, как Outlook.

- Вкладка **Организация** используется для просмотра и изменения сведений о роли получателя в организации.
- **Отдел**. Используйте это поле для просмотра или изменения отдела, в котором работает пользователь. Это поле можно использовать, чтобы создавать условия получателей для динамических групп рассылки, политик адресов электронной почты или списков адресов.
- **Компания**. Используйте это поле для просмотра или изменения компании, в которой работает пользователь. Это поле можно использовать, чтобы создавать условия получателей для динамических групп рассылки, политик адресов электронной почты или списков адресов.
- **Диспетчер**. Чтобы добавить руководителя, нажмите кнопку **Обзор**. В окне **Выбор руководителя** выберите соответствующего человека и нажмите кнопку **ОК**.
- **Прямые отчеты**. Изменить это поле нельзя. *Подчиненный* — это пользователь, подотчетный определенному руководителю. Если вы указали руководителя для пользователя, он отображается как прямой отчет в сведениях о почтовом ящике руководителя. Например, Кари управляет Крисом и Кейт, поэтому почтовый ящик Кари указан в поле **Менеджер** почтового ящика Криса и Кейт, а Крис и Кейт отображаются в поле **Прямые отчеты** в свойствах почтового ящика Кари.

Адрес электронной почты

Используйте раздел **Адрес электронной почты** для просмотра и изменения адресов электронной почты, связанных с почтовым ящиком пользователя. Сюда относится SMTP-адрес основного почтового ящика и все связанные прокси-адреса. Основной адрес SMTP (также называется *адрес ответа по умолчанию*) отображается жирным шрифтом в списке адресов со значением **SMTP** (прописными буквами) в столбце **Тип**.

- **Добавить: щелкните**+ чтобы добавить новый адрес электронной почты для этого почтового ящика. Выберите один из следующих типов адресов:

- **SMTP**. Это тип адреса по умолчанию. Нажмите эту кнопку, а затем введите новый адрес SMTP в поле ***Адрес электронной почты**.
- **EUM**. Адрес единой системы обмена сообщениями (Exchange) используется службой единой системы обмена сообщениями Microsoft Exchange в Exchange 2016 для поиска пользователей с поддержкой единой системы обмена сообщениями в организации Exchange. Адреса единой системы обмена сообщениями Exchange содержат добавочный номер и абонентскую группу единой системы обмена сообщениями для пользователя с включенной поддержкой единой системы обмена сообщениями. Нажмите эту кнопки и введите добавочный номер в поле **Адрес/добавочный номер**. После этого нажмите **Обзор** и выберите абонентскую группу для пользователя. (**Примечание**. Единая система обмена сообщениями недоступна в Exchange 2019.)
- **Пользовательский тип адреса**. Нажмите эту кнопку и введите один из поддерживаемых типов адресов электронной почты, **отличных от** SMTP, в поле *Email адрес.

  > ⓘ **Примечание**
  >
  > Настраиваемый адрес. Чтобы добавить настраиваемый адрес (например, факс или X.400), нажмите эту кнопку и используйте соответствующее диалоговое окно.

- **Укажите адрес ответа**. В Exchange Online можно установить этот флажок, чтобы сделать новый адрес электронной почты основным SMTP-адресом почтового ящика. Этот флажок недоступен в EAC в Exchange Server.

- **Автоматически обновлять адреса электронной почты на основе политики адресов электронной почты, которая применяется к этому получателю**. Установите этот флажок, чтобы адреса электронной почты получателей автоматически обновлялись на основе изменений политики адресов электронной почты организации. По умолчанию этот флажок установлен.

Функции почтового ящика

В разделе **Функции почтового ящика** можно просматривать и изменять следующие функции и параметры почтовых ящиков:

- **Политика общего доступа**. В этом поле показана политика общего доступа, применяемая к почтовому ящику. Она определяет правила предоставления

общего доступа к календарю и контактной информация для внешних пользователей. При создании почтовым ящикам назначается политика общего доступа по умолчанию. Чтобы изменить назначенную пользователю политику общего доступа, выберите другую политику из раскрывающегося списка.

- **Политика назначения ролей**. В этом поле отображается политика назначения ролей, назначенная почтовому ящику. Политика назначения ролей определяет роли управления доступом на основе ролей (RBAC), назначенные пользователю, и управляет параметрами конфигурации конкретных почтовых ящиков и групп рассылки, которые пользователи могут изменять. Чтобы изменить выбранную для пользователя политику назначения ролей, выберите другую политику из раскрывающегося списка.

- **Политика хранения**. В этом поле отображается политика хранения, назначенная почтовому ящику. Политика хранения представляет собой группу тегов хранения, которые применяются к почтовому ящику пользователя. Возможность управлять сроками хранения элементов почтовых ящиков пользователей и указывать действия, применяемые к элементам, которые достигли определенного возраста. Политика хранения не назначается почтовым ящикам во время их создания. Чтобы назначить пользователю политику хранения, выберите ее из раскрывающегося списка.

- **Политика адресной книги**. В этом поле отображается политика адресной книги, применяемая к почтовому ящику. Политика адресных книг позволяет делить пользователей на определенные группы для обеспечения настраиваемых представлений адресной книги. Чтобы применить или изменить политику адресной книги, примененную к почтовому ящику, выберите ее из раскрывающегося списка.

- **Единая система обмена сообщениями (недоступная в Exchange 2019):** эта функция отключена по умолчанию. При включении единой системы обмена сообщениями (UM) в Exchange 2016 пользователь сможет использовать функции единой системы обмена сообщениями вашей организации, а набор свойств единой системы обмена сообщениями по умолчанию применяется к пользователю. Нажмите кнопку **Включить**, чтобы включить единую систему обмена сообщениями для почтового ящика. Сведения о включении единой системы обмена сообщениями см. в разделе Enable a User for Unified Messaging.

  > ⓘ **Примечание**

Для включения единой системы обмена сообщениями необходимо сначала создать абонентскую группу единой системы обмена сообщениями и политику почтовых ящиков единой системы обмена сообщениями.

- **Мобильные устройства**. Используйте этот раздел для просмотра и изменения параметров для Exchange ActiveSync, которые включены по умолчанию. Exchange ActiveSync обеспечивает доступ к почтовому ящику Exchange с мобильного устройства. Чтобы отключить эту функцию для почтового ящика, нажмите **Отключить Exchange ActiveSync**.

- **Outlook Web App**. Эта функция включена по умолчанию. Outlook в Интернете обеспечивает доступ к почтовому ящику Exchange из веб-браузера. Нажмите **Отключить**, чтобы отключить Outlook в Интернете для почтового ящика. Нажмите **Изменить сведения**, чтобы добавить или изменить политику почтовых ящиков Outlook в Интернете для почтового ящика.

- **IMAP**: эта функция включена по умолчанию. Чтобы отключить функцию IMAP для почтового ящика, щелкните **Отключить**.

- **POP3**: эта функция включена по умолчанию. Чтобы отключить функцию POP3 для почтового ящика, щелкните **Отключить**.

- **MAPI**: эта функция включена по умолчанию. MAPI обеспечивает доступ к почтовому ящику Exchange из клиента MAPI, такого как Outlook. Чтобы отключить MAPI для почтового ящика, нажмите **Отключить**.

- **Удержание для судебного разбирательства**. Эта функция отключена по умолчанию. Судебное удержание позволяет сохранять удаленные элементы почтовых ящиков и записывать изменения в элементах. Удаленные элементы и все экземпляры измененных элементов возвращаются при поиске на обнаружение. Нажмите кнопку **Включить**, чтобы поместить почтовый ящик на хранение для судебного разбирательства. Если почтовый ящик помещен на хранение для судебного разбирательства, нажмите кнопку **Отключить**, чтобы отменить хранение для судебного разбирательства. Почтовые ящики, удерживаемые в судебном порядке, являются неактивными и не могут быть удалены. Чтобы удалить почтовый ящик, удалите удержание для судебного разбирательства. Если почтовый ящик помещен на хранение для судебного разбирательства, нажмите кнопку **Изменить сведения**, чтобы просмотреть и изменить следующие параметры хранения для судебного разбирательства:

- **Дата удержания**. Это поле только для чтения указывает дату и время, когда почтовый ящик был помещен на удержание в судебном порядке.
- **Поставить на удержание**: это поле только для чтения указывает пользователя, который поставил почтовый ящик на удержание для судебного разбирательства.
- **Примечание.** Используйте это поле, чтобы уведомить пользователя о удержании в судебном порядке, объяснить, почему почтовый ящик находится на удержании в судебном порядке, или предоставить пользователю дополнительные инструкции, такие как информирование пользователя о том, что удержание в судебном порядке не повлияет на его повседневное использование электронной почты.
- **URL-адрес**. Используйте это поле для предоставления URL-адреса веб-сайта, который предоставляет сведения или рекомендации по удержанию судебного разбирательства в почтовом ящике.

  > ⓘ **Примечание**
  >
  > Текст из этих полей отображается в почтовом ящике пользователя, только если он использует Outlook 2010 или более поздних версий. Он отсутствует в Outlook в Интернете и других почтовых клиентах. Чтобы просмотреть текст в полях Заметка и URL-адрес в Outlook, откройте вкладку **Файл** и на странице **Сведения** в разделе **Параметры учетной записи** вы увидите комментарий удержания судебного разбирательства.

- **Архивация**. Если архивный почтовый ящик не существует для пользователя, эта функция отключена. Чтобы включить архивный почтовый ящик, щелкните **Включить**. Если у пользователя есть архивный почтовый ящик, отображаются его размер и статистика использования. Нажмите кнопку **Изменить сведения**, чтобы просмотреть и изменить следующие параметры архивного почтового ящика:
  - **Состояние**. Это поле только для чтения указывает, существует ли архивный почтовый ящик.
  - **База данных**. В этом поле только для чтения отображается имя базы данных почтового ящика, в котором размещается архивный почтовый ящик.

- **Имя**. Введите имя архивного почтового ящика в этом поле. Это имя отображается под списком папок в Outlook или Outlook в Интернете.
- **Архивная квота (ГБ):** в этом поле отображается общий размер архивного почтового ящика. Чтобы изменить размер, введите в этом поле новое значение или выберите его в раскрывающемся списке.
- **Предупреждение о проблеме в (ГБ):** в этом поле отображается максимальный объем хранилища для архивного почтового ящика, прежде чем пользователю будет выдано предупреждение. Если размер архивного почтового ящика достигает указанного значения или превышает его, Exchange отправляет пользователю предупреждающее сообщение. Чтобы изменить это ограничение, введите новое значение в поле или выберите значение из раскрывающегося списка.

- **Параметры доставки**. Используйте для пересылки сообщений электронной почты, отправленных пользователю, другому получателю и для задания максимального числа получателей, которым пользователь может отправить сообщение. Щелкните **Подробнее**, чтобы просмотреть и изменить эти настройки.
  - **Адрес пересылки**. Установите флажок **Включить пересылку** и нажмите кнопку **Обзор** , чтобы отобразить страницу **Выбор почтового пользователя и почтового ящика** . Эта страница используется, чтобы выбрать получателя, которому нужно переадресовывать все сообщения электронной почты, отправляемые в этот почтовый ящик.
  - **Доставка сообщения на адрес пересылки и почтовый ящик**. Установите этот флажок, чтобы сообщения доставлялись как по адресу пересылки, так и в почтовый ящик пользователя.
  - **Ограничение получателей**. Этот параметр определяет максимальное число получателей, в которые пользователь может отправить сообщение. Установите флажок **Максимальное число получателей** , чтобы ограничить число получателей, разрешенное в полях Кому:, Копия и СК: сообщения электронной почты, а затем укажите максимальное число получателей. Для локальной организации Exchange число получателей не ограничено.

- **Ограничения размера сообщений**. Эти параметры определяют размер сообщений, которые пользователь может отправлять и получать. Щелкните **Подробнее**, чтобы просмотреть и изменить максимальный размер отправленных и полученных сообщений.

- **Отправленные сообщения**. Чтобы указать максимальный размер сообщений, отправленных этим пользователем, установите флажок **Максимальный размер сообщения (КБ)** и введите в поле значение. Размер сообщений должен находиться в диапазоне от 0 до 2 097 151 КБ. Если размер отправляемого пользователем сообщения превышает указанный размер, оно будет возвращено отправителю с соответствующим сообщением об ошибке.

- **Полученные сообщения**. Чтобы указать максимальный размер сообщений, полученных этим пользователем, установите флажок **Максимальный размер сообщения (КБ)** и введите значение в поле . Размер сообщений должен находиться в диапазоне от 0 до 2 097 151 КБ. Если пользователь получает сообщение, размер которого превышает установленное значение, это сообщение будет возвращено отправителю с описательным сообщением об ошибке.

- **Ограничения доставки сообщений**. Эти параметры определяют, кто может отправлять сообщения электронной почты этому пользователю. Щелкните **Подробнее**, чтобы просмотреть и изменить эти ограничения.

  - **Принять сообщения из**: используйте этот раздел, чтобы указать, кто может отправлять сообщения этому пользователю.

  - **Все отправители**. Выберите этот параметр, чтобы указать, что пользователь может принимать сообщения от всех отправителей. Сюда относятся отправители из вашей организации Exchange и внешние отправители. Этот вариант выбран по умолчанию. Этот параметр включает внешних пользователей, только если снят флажок **Требовать проверку подлинности всех отправителей**. Если этот флажок установлен, сообщения от внешних пользователей будут отклоняться.

  - **Только отправители в следующем списке**. Выберите этот параметр, чтобы указать, что пользователь может принимать сообщения только от указанного набора отправителей в организации Exchange. **Щелкните**+ Чтобы открыть страницу **Выбор получателей**, на которой отображается список всех получателей в организации Exchange. Выберите нужных получателей, добавьте их в список и нажмите **ОК**. Вы также можете выполнить поиск определенного получателя, введя имя получателя в поле поиска и щелкнув 🔎.

  - **Требовать проверку подлинности всех отправителей**. Выберите этот параметр, чтобы запретить анонимным пользователям отправлять сообщения пользователю.

- **Отклонить сообщения из**: используйте этот раздел, чтобы запретить пользователям отправлять сообщения этому пользователю.
- **Нет отправителей**. Выберите этот параметр, чтобы указать, что почтовый ящик не будет отклонять сообщения от отправителей в организации Exchange. Этот вариант выбран по умолчанию.
- **Отправители в следующем списке**. Выберите этот параметр, чтобы указать, что почтовый ящик будет отклонять сообщения от указанного набора отправителей в организации Exchange. **Щелкните**➕ Чтобы открыть страницу **Выбор получателей**, на которой отображается список всех получателей в организации Exchange. Выберите нужных получателей, добавьте их в список и нажмите **OK**. Вы также можете выполнить поиск определенного получателя, введя имя получателя в поле поиска и щелкнув 🔎.

Участник

Используйте раздел **Member Of** для просмотра списка групп рассылки или групп безопасности, к которым принадлежит этот пользователь. На этой странице нельзя изменять сведения о членстве. Обратите внимание, что пользователь может соответствовать критериям для одной или нескольких динамических групп рассылки в вашей организации. Однако динамические группы рассылки не отображаются на этой странице, так как их членство вычисляется каждый раз, когда они используются.

Подсказка

Используйте раздел **Подсказка** для добавления подсказок, предупреждающих пользователей о возможных проблемах при отправке сообщения данному получателю. Подсказка — это текст, который отображается в информационной строке при добавлении этого получателя в поля "Кому", "Копия" и "СК" нового сообщения электронной почты.

> ⓘ **Примечание**
>
> Подсказки могут содержать HTML-теги, но сценарии не допускаются. Длина пользовательской подсказки не должна превышать 175 отображаемых символов. HTML-теги при этом не учитываются.

Делегация почтовых ящиков

Используйте раздел **Делегирование почтовых ящиков** , чтобы назначить разрешения другим пользователям (также *называемым делегатам*), чтобы разрешить им входить в почтовый ящик пользователя или отправлять сообщения от имени пользователя. Можно назначать следующие разрешения:

- **Отправить как**. Это разрешение позволяет пользователям, кроме владельца почтового ящика, использовать почтовый ящик для отправки сообщений. После назначения этого разрешения делегату все сообщения, которые делегат отправляет через этот почтовый ящик, будут отображаться так, как если бы их отправил владелец почтового ящика. Тем не менее это разрешение не позволяет делегату входить в почтовый ящик этого пользователя.

- **Отправить от имени:** это разрешение также позволяет делегату использовать этот почтовый ящик для отправки сообщений. Тем не менее, когда это разрешение назначается делегату, адрес **От:** в сообщениях, отправляемых делегатом, будет указывать, что сообщение отправлено именно делегатом от лица владельца почтового ящика.

- **Полный доступ**. Это разрешение позволяет делегату входить в почтовый ящик пользователя и просматривать содержимое почтового ящика. Однако после назначения этого разрешения делегату он не сможет отправлять сообщения из почтового ящика. Чтобы разрешить делегату отправлять сообщения электронной почты из почтового ящика пользователя, по-прежнему необходимо назначить делегату разрешение Отправить как или Отправить от имени.

Чтобы назначить разрешения делегатам **, щелкните**+ Под соответствующим разрешением отобразится страница со списком всех получателей в организации Exchange, которым можно назначить разрешение. Выберите нужных получателей, добавьте их в список и нажмите **OK**. Вы также можете выполнить поиск определенного получателя, введя имя получателя в поле поиска и щелкнув 🔎.

Изменение свойств почтового ящика пользователя с помощью командной консоли Exchange

Используйте командлеты **Get-Mailbox** и **Set-Mailbox** для просмотра и изменения свойств почтовых ящиков пользователей. Одним из преимуществ использования командной консоли Exchange является возможность изменять свойства для нескольких почтовых ящиков. Сведения о том, какие параметры соответствуют свойствам почтового ящика, см. в следующих разделах:

- Get-Mailbox
- Set-Mailbox

Ниже приведены некоторые примеры использования командной консоли Exchange для изменения свойств почтового ящика пользователя.

В этом примере показано, как пересылать сообщения электронной почты Пэта Коулмана в почтовый ящик Sunil Koduri (sunilk@contoso.com).

PowerShell

```
Set-Mailbox -Identity patc -DeliverToMailboxAndForward $true -
ForwardingAddress sunilk@contoso.com
```

В этом примере командлет **Get-Mailbox** используется для поиска всех пользователей почтовых ящиков в организации, а затем применяется командлет **Set-Mailbox**, чтобы установить предел в 500 получателей в полях "Кому:", "Копия:" и "СК:" полях сообщения электронной почты.

PowerShell

```
Get-Mailbox -ResultSize unlimited -Filter "RecipientTypeDetails -eq
'UserMailbox'" | Set-Mailbox -RecipientLimits 500
```

В этом примере используется команда **Get-Mailbox** для поиска почтовых ящиков в маркетинговом подразделении, а затем — команда **Set-Mailbox** для настройки этих ящиков. Ограничения настраиваемого предупреждения, запрещения отправки, а также запрещения отправки и получения определяются как 200 мегабайт (МБ), 250 МБ и 280 МБ соответственно, а установленные по умолчанию ограничения базы данных почтовых ящиков игнорируются. Эта команда может быть использована, чтобы настроить для конкретного набора почтовых ящиков ограничения, большие или меньшие ограничений для других почтовых ящиков в организации.

PowerShell

```
Get-Mailbox -OrganizationalUnit "Marketing" | Set-Mailbox -IssueWarningQuota
209715200 -ProhibitSendQuota 262144000 -ProhibitSendReceiveQuota 293601280 -
UseDatabaseQuotaDefaults $false
```

В этом примере используется командлет **Get-Mailbox** для поиска всех пользователей в отделе обслуживания клиентов, а затем — командлет **Set-Mailbox** для изменения максимального размера отправляемых сообщений на значение 2 МБ.

PowerShell

```
Get-Mailbox -Filter "Department -eq 'Customer Service'" | Set-Mailbox -
MaxSendSize 2097152
```

В этом примере задается перевод MailTip на французский и китайский языки.

PowerShell

```
Set-Mailbox john@contoso.com -MailTipTranslations ("FR: C'est la langue
française", "CHT: 這是漢語語言")
```

Как проверить, все ли получилось?

Чтобы убедиться в том, что свойства почтового ящика пользователя успешно изменены, выполните следующие действия:

- В EAC выберите почтовый ящик и щелкните ✎ чтобы просмотреть измененное свойство или функцию. В зависимости от измененного свойства оно может отображаться в области "Сведения" выбранного почтового ящика.
- В командной консоли Exchange для проверки изменений используется командлет **Get-Mailbox**. С помощью командной консоли Exchange можно просмотреть несколько свойств нескольких почтовых ящиков. В примере выше, где изменялся предел для получателей, выполните следующую команду, чтобы проверить, изменилось ли значение.

  PowerShell

  ```
  Get-Mailbox -ResultSize unlimited -Filter "RecipientTypeDetails -eq
  'UserMailbox'" | Format-List Name,RecipientLimits
  ```

  Чтобы увидеть указанный выше пример, в котором изменяются пределы сообщения, выполните эту команду.

  PowerShell

  ```
  Get-Mailbox -OrganizationalUnit "Marketing" | Format-List
  Name,IssueWarningQuota,ProhibitSendQuota,ProhibitSendReceiveQuota,UseDa
  tabaseQuotaDefaults
  ```

Массовое изменение почтовых ящиков пользователей

С помощью Центра администрирования Exchange (EAC) можно также изменять выбранные свойства для нескольких почтовых ящиков пользователей. Если вы выберете несколько почтовых ящиков в списке в EAC, свойства, для которых возможно массовое изменение, отображаются в области сведений. Изменение одного из этих свойств применяется ко всем выбранным почтовым ящикам.

Ниже представлен список функций и свойств почтовых ящиков пользователей, для которых возможно массовое изменение. Обратите внимание, что не все свойства могут быть изменены.

- **Контактные сведения**: В этом поле можно изменить общие свойства, такие как название улицы, почтовый индекс и название города.
- **Организация**. Измените общие свойства, такие как название отдела, название компании и руководителя, которому сообщают выбранные пользователи.
- **Настраиваемые атрибуты**: изменение или добавление значений для настраиваемых атрибутов 1–15.
- **Квота почтового ящика**. Измените значения квоты почтового ящика и срок хранения удаленных элементов.
- **подключение Email**: включение или отключение Outlook в Интернете, POP3, IMAP, MAPI и Exchange ActiveSync.
- **Архивирование**: включение или отключение архивного почтового ящика.
- **Политика хранения, политика назначения ролей и политика общего доступа**. Обновите параметры для каждой из этих функций почтового ящика.
- **Перемещение почтовых ящиков в другую базу данных**. Переместите выбранные почтовые ящики в другую базу данных.
- **Делегирование разрешений**. Назначьте разрешения пользователям или группам, которые позволяют им открывать или отправлять сообщения из других почтовых ящиков. Пользователям или группам можно назначать разрешения "Полный", "Отправить как" и "Отправить от имени". Дополнительные сведения см. в статье Управление разрешениями для получателей .

Примечание

Предполагаемое время выполнения этой задачи — 2 минуты, но она может потребовать больше при изменении нескольких свойств или функций.

Использование Центра администрирования Exchange для операции массового редактирования почтовых ящиков пользователей

1. В Центре администрирования Exchange (EAC) выберите **Получатели**>**Почтовые ящики**.
2. В списке почтовых ящиков выберите не менее двух почтовых ящиков.

   Совет

   Можно выбрать несколько смежных ящиков, удерживая клавишу SHIFT и щелкнув первый почтовый ящик, а затем щелкнув последний ящик, который требуется изменить. Также можно выбрать несколько отдельных ящиков, удерживая клавишу CTRL и щелкая каждый ящик, который требуется изменить.

3. В области сведений в разделе **Массовое редактирование** нужно выбрать свойства или функции почтового ящика, которые требуется изменить.
4. Внесите необходимые изменения на странице свойств, а затем сохраните изменения.

Как проверить, все ли получилось?

Чтобы убедиться в том, что массовое изменение почтовых ящиков успешно, выполните одно из следующих действий:

- В EAC выберите каждый из почтовых ящиков, которые вы массово редактировали, и нажмите кнопку **Изменить** чтобы просмотреть измененное свойство или функцию.
- В командной консоли Exchange для проверки изменений используется командлет **Get-Mailbox**. С помощью командной консоли Exchange можно просмотреть несколько свойств нескольких почтовых ящиков. Например, вы

использовали функцию массового редактирования в EAC, чтобы включить архивный почтовый ящик и назначить политику хранения для всех пользователей организации. Для проверки этих изменений можно выполнить следующую команду:

PowerShell

```
Get-Mailbox -ResultSize unlimited -Filter "RecipientTypeDetails -eq
'UserMailbox'" | Format-List Name,ArchiveDatabase,RetentionPolicy
```

Дополнительные сведения о доступных параметрах **Get-Mailbox** см. в разделе Get-Mailbox.

Добавление и удаление адресов электронной почты для почтового ящика

Статья • 04.04.2023

Добавить или удалить адрес электронной почты для почтового ящика пользователя можно в Центре администрирования Exchange или командной консоли Exchange. Для одного почтового ящика можно настроить несколько адресов электронной почты. Дополнительные адреса называются *прокси-адресами*. Прокси-адреса позволяют пользователям получать электронную почту, отправляемую на другой адрес электронной почты. Любое сообщение электронной почты, отправленное на прокси-адрес пользователя, доставляется на основной адрес электронной почты, который также называется *основным SMTP-адресом* или *адресом ответа по умолчанию*.

> ⓘ **Примечание**
>
> Процедуры, описанные в данном разделе, показывают, как добавлять и удалять адреса электронной почты для почтового ящика пользователя. Можно использовать сходные процедуры для добавления или удаления адресов электронной почты у других типов получателей.

Дополнительные задачи, связанные с управлением получателями, см. в таблице "Документация о получателях" в статье Получатели.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 2 минут.
- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения подготовки получателей" раздела Разрешения получателей .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Добавление адреса электронной почты в почтовый ящик пользователя

Использование EAC для добавления адреса электронной почты

1. В Центре администрирования Exchange (EAC) выберите **Получатели**>**Почтовые ящики**.
2. В списке почтовых ящиков пользователей щелкните почтовый ящик, в который нужно добавить адрес электронной почты, а затем щелкните **Изменить**.
3. На странице свойств почтового ящика нажмите кнопку **Адрес электронной почты**.

   > **Примечание**
   >
   > На странице **Адрес электронной почты** основной SMTP-адрес отображается жирным шрифтом в списке адресов и прописными буквами **SMTP** в столбце **Тип**.

4. Нажмите ➕ а затем щелкните **SMTP**, чтобы добавить SMTP-адрес электронной почты в этот почтовый ящик.

   > **Примечание**
   >
   > Тип SMTP используется для адреса электронной почты по умолчанию. Вы также можете добавить адреса единой системы обмена сообщениями Exchange (EUM) или пользовательские адреса в почтовый ящик в Exchange 2016. Дополнительные сведения см. в подразделе «Изменение свойств почтового ящика пользователя» в разделе Manage user

mailboxes. (**Примечание**. Единая система обмена сообщениями недоступна в Exchange 2019.)

5. Введите новый SMTP-адрес в поле **Адрес электронной почты**, а затем нажмите кнопку **OK**.

   Новый адрес выводится в списке адресов электронной почты для выбранного почтового ящика.

6. Чтобы сохранить изменения, нажмите кнопку **Сохранить**.

Добавление адреса электронной почты в командной консоли Exchange

Адреса электронной почты, связанные с почтовым ящиком, содержатся в свойстве *EmailAddresses* для почтового ящика. Так как он может содержать несколько адресов электронной *почты, свойство EmailAddresses* называется *многозначным* . Следующие примеры показывают различные способы изменения многозначного свойства.

В этом примере показывается добавление SMTP-адреса к почтовому ящику Dan Jump.

PowerShell

```
Set-Mailbox "Dan Jump" -EmailAddresses
@{add="dan.jump@northamerica.contoso.com"}
```

В этом примере показано, как добавить несколько SMTP-адресов в почтовый ящик.

PowerShell

```
Set-Mailbox "Dan Jump" -EmailAddresses
@{add="dan.jump@northamerica.contoso.com","danj@tailspintoys.com"}
```

Дополнительные сведения об использовании этого способа для добавления и удаления значений многозначных свойств см. в разделе Modifying Multivalued Properties.

Здесь показан другой способ добавления адреса электронной почты для почтового ящика путем указания всех адресов, связанных с этим почтовым ящиком. В этом примере — это новый адрес электронной почты, danj@tailspintoys.com который требуется добавить. Остальные два адреса электронной почты уже существуют.

Адрес с квалификатором с учетом регистра `SMTP` является основным SMTP-адресом. В этой команде необходимо указать все адреса электронной почты для почтового ящика. Иначе адрес в команде перезапишет существующие адреса.

PowerShell

```
Set-Mailbox "Dan Jump" -EmailAddresses
"SMTP:dan.jump@contoso.com","dan.jump@northamerica.contoso.com","danj@tailsp
intoys.com"
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе Set-Mailbox.

Как проверить, все ли получилось?

Чтобы убедиться в том, что вы успешно добавили адрес электронной почты для почтового ящика, выполните одно из следующих действий:

- В EAC перейдите в раздел **Почтовые ящики получателей**>, щелкните почтовый ящик, а затем щелкните**изменить**.

- На странице свойств почтового ящика нажмите кнопку **Адрес электронной почты**.

- В списке адресов электронной почты для почтового ящика убедитесь, что новый адрес электронной почты указан.

Или

- Выполните указанную ниже команду в командной консоли Exchange.

  PowerShell

  ```
  Get-Mailbox <identity> | Format-List EmailAddresses
  ```

- Убедитесь, что новый адрес электронной почты входит в результаты.

Удаление адреса электронной почты из почтового ящика пользователя

Использование EAC для удаления адреса электронной почты

1. В Центре администрирования Exchange (EAC) выберите **Получатели**>**Почтовые ящики**.
2. В списке почтовых ящиков пользователей щелкните почтовый ящик, из которого нужно удалить адрес электронной почты, а затем щелкните **Изменить**.
3. На странице свойств почтового ящика нажмите кнопку **Адрес электронной почты**.
4. В списке адресов электронной почты выберите адрес, который нужно удалить, и нажмите кнопку **Удалить**.
5. Чтобы сохранить изменения, нажмите кнопку **Сохранить**.

Удаление адреса электронной почты в командной консоли Exchange

В этом примере показано, как удалить адрес электронной почты из почтового ящика Janet Schorr.

PowerShell

```
Set-Mailbox "Janet Schorr" -EmailAddresses
@{remove="janets@corp.contoso.com"}
```

В этом примере показано, как удалить несколько адресов из почтового ящика.

PowerShell

```
Set-Mailbox "Janet Schorr" -EmailAddresses
@{remove="janet.schorr@corp.contoso.com","janets@tailspintoys.com"}
```

Дополнительные сведения об использовании этого способа для добавления и удаления значений многозначных свойств см. в разделе Modifying Multivalued Properties.

Кроме того, можно удалить адрес электронной почты, пропустив его в команде для задания всех адресов электронной почты для почтового ящика. Например, предположим, что почтовый ящик Джанет Шорр содержит три адреса электронной почты: janets@contoso.com (основной SMTP-адрес), janets@corp.contoso.comи janets@tailspintoys.com. Чтобы удалить адрес janets@corp.contoso.com, выполните следующую команду.

PowerShell

```
Set-Mailbox "Janet Schorr" -EmailAddresses
"SMTP:janets@contoso.com","janets@tailspintoys.com"
```

Так как janets@corp.contoso.com эта команда была опущена в предыдущей команде, она удаляется из почтового ящика.

Подробные сведения о синтаксисе и параметрах см. в разделе Set-Mailbox.

Как проверить, все ли получилось?

Чтобы убедиться в том, что вы успешно удалили адрес электронной почты для почтового ящика, выполните одно из следующих действий:

- В EAC перейдите в раздел **Почтовые ящики получателей**>, щелкните почтовый ящик, а затем щелкните**изменить**.

- На странице свойств почтового ящика нажмите кнопку **Адрес электронной почты**.

- В списке адресов электронной почты для почтового ящика убедитесь, что новый адрес электронной почты не указан.

Или

- Выполните указанную ниже команду в командной консоли Exchange.

  PowerShell

  ```
  Get-Mailbox <identity> | Format-List EmailAddresses
  ```

- Убедитесь, что новый адрес электронной почты не входит в результаты.

Добавление адресов электронной почты для нескольких почтовых ящиков в командной консоли Exchange

Вы можете добавить новый адрес электронной почты сразу для нескольких почтовых ящиков, используя командную консоль Exchange и CSV-файл.

Этот пример импортирует данные из C:\Users\Administrator\Desktop\AddEmailAddress.csv, который имеет следующий

формат.

CSV

```
Mailbox,NewEmailAddress
Dan Jump,danj@northamerica.contoso.com
David Pelton,davidp@northamerica.contoso.com
Kim Akers,kima@northamerica.contoso.com
Janet Schorr,janets@northamerica.contoso.com
Jeffrey Zeng,jeffreyz@northamerica.contoso.com
Spencer Low,spencerl@northamerica.contoso.com
Toni Poe,tonip@northamerica.contoso.com
...
```

Выполните следующую команду, чтобы использовать данные в CSV-файле для добавления адреса электронной почты для каждого почтового ящика, указанного в CSV-файле.

PowerShell

```
Import-CSV "C:\Users\Administrator\Desktop\AddEmailAddress.csv" | foreach
{Set-Mailbox $_.Mailbox -EmailAddresses @{add=$_.NewEmailAddress}}
```

> ⓘ **Примечание**
>
> Имена столбцов в первой строке этого CSV-файла (`Mailbox,NewEmailAddress`) являются произвольными. В команде командной консоли Exchange необходимо использовать те же имена столбов, что и в этом файле.

Как проверить, все ли получилось?

Чтобы убедиться в том, что вы успешно добавили адрес электронной почты для нескольких почтовых ящиков, выполните одно из следующих действий:

- В EAC перейдите в раздел **Почтовые ящики получателей**>, щелкните почтовый ящик, в который вы добавили адрес, а затем щелкните**Изменить**.✏

- На странице свойств почтового ящика нажмите кнопку **Адрес электронной почты**.

- В списке адресов электронной почты для почтового ящика убедитесь, что новый адрес электронной почты указан.

Или

- Выполните следующую команду в командной консоли Exchange, используя тот же CSV-файл, с помощью которого вы добавляли новый адрес электронной почты.

```
PowerShell
```

```
Import-CSV "C:\Users\Administrator\Desktop\AddEmailAddress.csv" |
foreach {Get-Mailbox $_.Mailbox | Format-List Name,EmailAddresses}
```

- Убедитесь, что новый адрес электронной почты входит в результаты для каждого ящика.

Настройка переадресации электронной почты для почтового ящика

Статья • 04.04.2023

Функция переадресации писем позволяет настроить почтовый ящик на пересылку сообщений, отправленных одному пользователю, в почтовый ящик другого пользователя в вашей организации или за ее пределами.

Использование Центра администрирования Exchange и командной консоли Exchange

Для настройки переадресации электронной почты можно использовать Центр администрирования Exchange (EAC) или командную консоль Exchange.

Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Разрешения подготовки получателей" в разделе Разрешения получателей .

Настройка переадресации электронной почты с помощью Центра администрирования Exchange

1. В Центре администрирования Exchange перейдите в раздел **Почтовые ящики получателей**>.
2. В списке почтовых ящиков пользователей щелкните или коснитесь почтового ящика, для которого требуется настроить пересылку почты, а затем щелкните ✎
3. На странице свойств почтового ящика нажмите кнопку **Функции почтового ящика**.
4. В разделе **Поток обработки почты** выберите **Подробные сведения**, чтобы просмотреть или изменить настройки пересылки сообщений электронной почты.

   На этой странице вы можете указать максимальное количество получателей, которым пользователь сможет отправить сообщение. По умолчанию количество получателей не ограничено. Если вы хотите задать ограничение,

установите флажок **Максимальное число получателей**, а в текстовом поле под ним введите ограничение.

5. Установите флажок **Включить переадресацию** и нажмите или выберите кнопку **Обзор**.

6. На странице **Выбор получателя** выберите пользователя, которому вы хотите переслать все сообщения. Установите флажок **Доставить сообщение на адрес пересылки и в почтовый ящик**, чтобы копии отправляемых сообщений поступали получателю и на адрес пересылки. Последовательно нажмите или выберите кнопки **ОК** и **Сохранить**.

> ⓘ **Примечание**
>
> Что делать, если вы хотите пересылать сообщения электронной почты на адрес электронной почты за пределами организации? Для этого можно использовать командную консоль Exchange. См. следующий пример в разделе "Настройка пересылки почты с помощью командной консоли Exchange".

Настройка пересылки писем с помощью командной консоли Exchange

Не используете командную консоль Exchange? Дополнительные сведения см. в статье Оболочка управления Exchange . Дополнительные сведения о командлетах, используемых здесь, см. в разделах Get-Mailbox и Set-Mailbox .

В этом примере электронная почта доставляется в почтовый ящик Дугласа Кона, а также пересылается все сообщения, отправленные Дугласу Кону, на внешний адрес электронной почты . douglaskohn.parents@fineartschool.net

PowerShell

```
Set-Mailbox -Identity "Douglas Kohn" -DeliverToMailboxAndForward $true -
ForwardingSMTPAddress "douglaskohn.parents@fineartschool.net"
```

В этом примере пересылается все сообщения электронной почты, отправленные в почтовый ящик Кена Санчеса, сотрудника Contoso Suites, одному из его коллег, pilarp@contoso.com.

PowerShell

```
Set-Mailbox -Identity "Ken Sanchez" -ForwardingAddress "pilarp@contoso.com"
```

Подробные сведения о синтаксисе и параметрах см. в разделе Set-Mailbox.

Как проверить, все ли получилось?

Убедиться, что переадресация почты настроена успешно, можно двумя способами. Первый вариант:

1. В Центре администрирования Exchange перейдите в раздел **Почтовые ящики получателей**>.
2. В списке почтовых ящиков пользователей щелкните или коснитесь почтового ящика, для который настроена пересылка электронной почты, а затем щелкните **Изменить**.
3. На странице свойств почтового ящика нажмите кнопку **Функции почтового ящика**.
4. В разделе **Поток обработки почты** щелкните **Подробности**, чтобы просмотреть настройки переадресации почты.

Второй вариант:

Выполните указанную ниже команду в командной консоли Exchange.

```
PowerShell

Get-Mailbox <identity> | Format-List
ForwardingSMTPAddress,DeliverToMailboxandForward
```

Убедитесь, что адрес пересылки указан в параметре *ForwardingSMTPAddress* . Кроме того, если параметр *DeliverToMailboxAndForward* имеет значение `$true`, сообщения будут доставлены в почтовый ящик и на адрес переадресации. Если параметр имеет значение `$false`, сообщения доставляются только по адресу переадресации.

Пользователи

Чтобы узнать о переадресации почты на другой адрес электронной почты с использованием программы Outlook и приложения Outlook Web App, ознакомьтесь со статьями ниже.

- Переадресация электронной почты на другую учетную запись электронной почты

- Управление сообщениями электронной почты с помощью правил

Дополнительные сведения

Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server, Exchange Online или Exchange Online Protection.

Настройка ограничений на доставку сообщений для почтового ящика

Статья • 04.04.2023

Вы можете использовать Центр администрирования Exchange или командную консоль Exchange, чтобы установить ограничения на доставку сообщений отдельным получателям. Используйте их, чтобы контролировать, кто может отправлять сообщения сотрудникам вашей организации. Например, вы можете настроить почтовый ящик так, чтобы он принимал или отклонял сообщения от отдельных отправителей или принимал сообщения только от сотрудников вашей организации Exchange.

Ограничения доставки сообщений, рассматриваемые в этом разделе, применяются ко всем типам получателей. Дополнительные сведения о типах получателей см. в разделе Recipients.

Дополнительные задачи управления, связанные с получателями, содержатся в следующих разделах:

- Управление почтовыми ящиками пользователей
- Управление группами рассылки
- Управление динамическими группами рассылки
- Manage mail users
- Управление почтовыми контактами

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения подготовки получателей" раздела Разрешения получателей .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Установка ограничений на доставку сообщений в Центре администрирования Exchange

1. В Центре администрирования Exchange (EAC) выберите **Получатели**>**Почтовые ящики**.

2. В списке почтовых ящиков пользователей щелкните почтовый ящик, для которого нужно настроить ограничения на доставку сообщений, а затем щелкните **Изменить**.

3. На странице свойств почтового ящика нажмите кнопку **Функции почтового ящика**.

4. В разделе **Ограничения доставки сообщений** щелкните **Подробности**, чтобы просмотреть и изменить следующие ограничения доставки:

    - **Принять сообщения из**: используйте этот раздел, чтобы указать, кто может отправлять сообщения этому пользователю.

    - **Все отправители**. Этот параметр указывает, что пользователь может принимать сообщения от всех отправителей. Сюда относятся отправители из вашей организации Exchange и внешние отправители. Это значение используется по умолчанию. Этот параметр включает внешних пользователей, только если снят флажок **Требовать проверку подлинности всех отправителей**. Если этот флажок установлен, сообщения от внешних пользователей будут отклоняться.

    - **Только отправители в следующем списке**. Этот параметр указывает, что пользователь может принимать сообщения только от указанного набора отправителей в организации Exchange. Щелкните **добавить** Чтобы отобразить список всех получателей в организации Exchange. Выберите нужных получателей, добавьте их в список и нажмите **OK**. Вы также можете выполнить поиск определенного получателя, введя имя получателя в поле поиска и щелкнув .

- **Требовать проверку подлинности всех отправителей**. Этот параметр запрещает анонимным пользователям отправлять сообщения пользователю. Это включает внешних пользователей, которые находятся за пределами вашей организации Exchange.
- **Отклонить сообщения из**: используйте этот раздел, чтобы запретить пользователям отправлять сообщения этому пользователю.
- **Нет отправителей**. Этот параметр указывает, что почтовый ящик не будет отклонять сообщения от отправителей в организации Exchange. Этот параметр установлен по умолчанию.
- **Отправители в следующем списке**. Этот параметр указывает, что почтовый ящик будет отклонять сообщения от указанного набора отправителей в организации Exchange. Щелкните **добавить**➕ Чтобы отобразить список всех получателей в организации Exchange. Выберите нужных получателей, добавьте их в список и нажмите **OK**. Вы также можете выполнить поиск определенного получателя, введя имя получателя в поле поиска и щелкнув 🔎.

5. Щелкните **OK**, чтобы закрыть страницу **Ограничения доставки сообщений**, а затем нажмите **Сохранить** для сохранения изменений.

Установка ограничений на доставку сообщений с помощью командной консоли Exchange

В приведенных ниже примерах показано, как установить ограничения на доставку сообщений для почтового ящика с помощью командной консоли Exchange. Для других типов получателей используйте соответствующий командлет **Set-** с теми же параметрами.

В этом примере показано, как настроить почтовый ящик Robin Wood на получение сообщений только от Lori Penor, Jeff Phillips и членов группы рассылки Legal Team 1.

PowerShell

```
Set-Mailbox -Identity "Robin Wood" -AcceptMessagesOnlyFrom "Lori
Penor","Jeff Phillips" -AcceptMessagesOnlyFromDLMembers "Legal Team 1"
```

ⓘ **Примечание**

Если вы настраиваете почтовый ящик для приема сообщений только от отдельных отправителей, необходимо использовать параметр *AcceptMessagesOnlyFrom* . Если вы настраиваете почтовый ящик для приема сообщений только от отправителей, входящих в определенную группу рассылки, используйте параметр *AcceptMessagesOnlyFromDLMembers* .

Этот пример добавляет пользователя с именем David Pelton в список пользователей, чьи сообщения будут приниматься ящиком Robin Wood.

PowerShell

```
Set-Mailbox -Identity "Robin Wood" -AcceptMessagesOnlyFrom @{add="David Pelton"}
```

В этом примере показано, как настроить почтовый ящик Robin Wood с обязательной проверкой подлинности всех отправителей. Это означает, что почтовый ящик будет принимать только сообщения, отправленные другим пользователям в организации Exchange.

PowerShell

```
Set-Mailbox -Identity "Robin Wood" -RequireSenderAuthenticationEnabled $true
```

В этом примере показана настройка почтового ящика Robin Wood с отклонением сообщений от пользователей Joe Healy, Terry Adams и членов группы рассылки Legal Team 2.

PowerShell

```
Set-Mailbox -Identity "Robin Wood" -RejectMessagesFrom "Joe Healy","Terry Adams" -RejectMessagesFromDLMembers "Legal Team 2"
```

В этом примере показано, как настроить почтовый ящик Robin Wood для отклонения сообщений, созданных членами группы рассылки Legal Team 3.

PowerShell

```
Set-Mailbox -Identity "Robin Wood" -RejectMessagesFromDLMembers @{add="Legal Team 3"}
```

ⓘ Примечание

Если вы настраиваете почтовый ящик для отклонения сообщений от отдельных отправителей, необходимо использовать параметр *RejectMessagesFrom* . Если вы настраиваете почтовый ящик для отклонения сообщений от отправителей, входящих в определенную группу рассылки, используйте параметр *RejectMessagesFromDLMembers* .

Подробные сведения о синтаксисе и параметрах, связанные с установкой ограничений на доставку для различных типов получателей, см. в следующих статьях:

- Настроить DistributionGroup
- Настроить DynamicDistributionGroup
- Set-Mailbox
- Set-MailContact
- Set-MailUser

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно установили ограничения на доставку сообщений для почтового ящика пользователя, выполните одно из следующих действий:

1. В Центре администрирования Exchange (EAC) выберите **Получатели**>**Почтовые ящики**.
2. В списке почтовых ящиков пользователей щелкните почтовый ящик, для которого нужно проверить ограничения доставки сообщений, а затем щелкните **Изменить**.
3. На странице свойств почтового ящика нажмите кнопку **Функции почтового ящика**.
4. В разделе **Ограничения доставки сообщений** щелкните **Подробности** для просмотра ограничений доставки для почтового ящика.

Или

Выполните указанную ниже команду в командной консоли Exchange.

```
PowerShell
```

```
Get-Mailbox <identity> | Format-List
AcceptMessagesOnlyFrom,AcceptMessagesOnlyFromDLMembers,RejectMessagesFrom,Re
jectMessagesFromDLMembers,RequireSenderAuthenticationEnabled
```

Настройка ограничений на размер сообщений для почтового ящика в Exchange Server

Статья • 04.04.2023

Эти ограничения определяют размер сообщений, которые может отправлять и получать пользователь. По умолчанию при создании почтового ящика эти ограничения не задаются.

Следует иметь в виду, что существуют другие параметры организации Exchange, определяющие максимальный размер сообщения, которое можно принять или отправить из почтового ящика (например, максимальный размер сообщения, указанный на сервере почтовых ящиков). Дополнительные сведения об ограничениях размера сообщений в Exchange, включая типы ограничений на размер сообщений, их область и порядок приоритета, см. в статье Ограничения размера сообщений и получателей в Exchange Server.

Сведения о дополнительных задачах по управлению почтовыми ящиками пользователей см. в разделе Управление почтовыми ящиками пользователей.

> ⓘ **Примечание**
>
> Можно также контролировать размер сообщений, отправляемых и получаемых пользователей почты в общих почтовых ящиках.

Что нужно знать перед началом работы?

- Предполагаемое время для завершения: 2 минуты.
- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения подготовки получателей" раздела Разрешения получателей .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Настройка ограничений на размер сообщений в Центре администрирования Exchange

1. В Центре администрирования Exchange (EAC) выберите **Получатели** > **Почтовые ящики**.

2. В списке почтовых ящиков пользователей щелкните почтовый ящик, для которого требуется изменить ограничения на размер сообщений, а затем щелкните **Изменить**.

3. На странице свойств почтового ящика нажмите кнопку **Функции почтового ящика**.

4. В разделе **Ограничения размера сообщений** щелкните **Подробности**, чтобы просмотреть и изменить следующие ограничения размера:

   - **Отправленные сообщения**. Чтобы задать максимальный размер сообщений, отправленных этим пользователем, установите флажок **Максимальный размер сообщения (КБ)** и введите значение в поле. Размер сообщений должен находиться в диапазоне от 0 до 2 097 151 КБ. Если размер отправляемого пользователем сообщения превышает указанный размер, оно будет возвращено отправителю с соответствующим сообщением об ошибке.

   - **Полученные сообщения**. Чтобы задать максимальный размер сообщений, полученных этим пользователем, установите флажок **Максимальный размер сообщения (КБ)** и введите в поле значение. Размер сообщений должен находиться в диапазоне от 0 до 2 097 151 КБ. Если размер полученного сообщения превышает указанное значение, оно будет возвращено отправителю с сообщением об ошибке.

5. Нажмите кнопку **ОК**, а затем кнопку **Сохранить**, чтобы сохранить изменения.

Настройка ограничений на размер сообщений с помощью командной консоли Exchange

В этом примере показано, как установить максимальный размер отправляемых сообщений в 25 МБ и максимальный размер получаемых сообщений в 35 МБ для почтового ящика Debra Garcia.

PowerShell

```
Set-Mailbox -Identity "Debra Garcia" -MaxSendSize 25mb -MaxReceiveSize 35mb
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе Set-Mailbox.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно настроили ограничения на размер сообщений для почтового ящика, выполните одно из следующих действий:

1. В Центре администрирования Exchange (EAC) выберите **Получатели**>**Почтовые ящики**.
2. В списке почтовых ящиков пользователей щелкните почтовый ящик, для которого нужно проверить ограничения на размер сообщений, а затем щелкните **Изменить**.
3. На странице свойств почтового ящика нажмите кнопку **Функции почтового ящика**.
4. В разделе **Ограничения доставки сообщений** щелкните **Подробности** для просмотра ограничений на размер сообщений для почтового ящика.

   Или

   Выполните указанную ниже команду в командной консоли Exchange.

   PowerShell

   ```
   Get-Mailbox -Identity <Identity> | Format-List
   MaxSendSize,MaxReceiveSize
   ```

Настройка квот хранилища для почтового ящика в Exchange Server

Статья • 25.10.2023 • Применяется к: Exchange Server 2013, Exchange Server 2016

Вы можете использовать Центр администрирования Exchange или командную консоль Exchange, чтобы настроить квоты хранилища для почтовых ящиков. Квоты хранилища позволяют контролировать размер почтовых ящиков и управлять базами данных почтовых ящиков. Когда размер почтового ящика достигает указанной квоты хранилища или превышает ее, Exchange отправляет владельцу почтового ящика соответствующее уведомление.

Квоты хранилища обычно настраиваются отдельно для каждой базы данных. Это значит, что квоты, настроенные для базы данных почтовых ящиков, применяются ко всем почтовым ящикам в этой базе данных. Дополнительные сведения об управлении параметрами почтовых ящиков для каждой базы данных см. в статье Управление базами данных почтовых ящиков в Exchange Server.

В этом разделе показано, как настроить параметры хранения для определенного почтового ящика вместо того, чтобы использовать параметры хранения для базы данных почтовых ящиков. Сведения о дополнительных задачах по управлению почтовыми ящиками пользователей см. в разделе Управление почтовыми ящиками пользователей.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 2 минуты.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения подготовки получателей" раздела Разрешения получателей .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Настройка квот хранилища для почтового ящика в Центре администрирования Exchange

1. В Центре администрирования Exchange (EAC) выберите **Получатели**>**Почтовые ящики**.

2. В списке почтовых ящиков пользователей щелкните почтовый ящик, для которого требуется изменить квоты хранилища, а затем щелкните ✎.

3. На странице свойств почтового ящика последовательно щелкните **Использование почтового ящика** и **Дополнительные параметры**.

4. Щелкните **Настроить параметры для этого почтового ящика**, а затем укажите необходимые значения в следующих полях. Диапазон значений для каждого из параметров квоты хранилища составляет от 0 до 2047 ГБ.

    - **Выдача предупреждения в (ГБ):** в этом поле отображается максимальный объем хранилища, прежде чем пользователю будет выдано предупреждение. Если размер почтового ящика равен указанному значению или превышает его, пользователю этого ящика на сервере Exchange отправляется предупреждающее сообщение.

      > ⓘ **Важно!**
      >
      > Сообщение, сопоставленное с квотой **Выводить предупреждение**, не отправляется пользователю, если только значение этого параметра не превышает 50 % значения, заданного в квоте **Запретить отправку**. Например, если вы устанавливаете для квоты **Запретить отправку** значение 8 МБ, необходимо задать для квоты **Выводить предупреждение** значение не ниже 4 МБ. В противном случае сообщение квоты **Выводить предупреждение** не отправляется.

    - **Запретить отправку в (ГБ):** если размер почтового ящика достигает или превышает указанное ограничение, Exchange запрещает пользователю отправлять новые сообщения и отображает описательное сообщение об ошибке.

    - **Запретить отправку и получение в (ГБ).** Если размер почтового ящика достигает или превышает указанное ограничение, Exchange запрещает

пользователю почтового ящика отправлять новые сообщения и не будет доставлять в почтовый ящик новые сообщения. Сообщения, отправляемые в почтовый ящик, будут возвращаться отправителю с сообщением об ошибке.

5. Нажмите кнопку **Сохранить**, чтобы сохранить изменения.

Настройка квот хранилища для почтового ящика с помощью командной консоли Exchange

В этом примере показано, как задать квоты для предупреждения, запрета на отправку, запрета на отправку и получение для почтового ящика пользователя Joe Healy, равные 24,5 ГБ, 24,75 ГБ и 25 ГБ соответственно.

> ⓘ **Примечание**
>
> Чтобы обеспечить использование пользовательских параметров почтового ящика, а не базы данных почтовых ящиков по умолчанию, необходимо задать для параметра *UseDatabaseQuotaDefaults* значение `$false`.

PowerShell

```
Set-Mailbox -Identity "Joe Healy" -IssueWarningQuota 24.5gb -
ProhibitSendQuota 24.75gb -ProhibitSendReceiveQuota 25gb -
UseDatabaseQuotaDefaults $false
```

В этом примере показано, как задать квоты для предупреждения, запрета на отправку, запрета на отправку и получение для почтового ящика пользователя Ayla Kol, равные 900 МБ, 950 МБ и 1 ГБ соответственно, а также настроить почтовый ящик на использование настраиваемых параметров.

PowerShell

```
Set-Mailbox -Identity "Ayla Kol" -IssueWarningQuota 900mb -ProhibitSendQuota
950mb -ProhibitSendReceiveQuota 1gb -UseDatabaseQuotaDefaults $false
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе Set-Mailbox.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли заданы квоты хранилища для почтового ящика, выполните одно из следующих действий.

1. В Центре администрирования Exchange (EAC) выберите **Получатели**>**Почтовые ящики**.
2. В списке почтовых ящиков пользователей щелкните почтовый ящик, для которого требуется проверить квоты хранилища, а затем щелкните ✎.
3. На странице свойств почтового ящика последовательно щелкните **Использование почтового ящика** и **Дополнительные параметры**.
4. Убедитесь, что выбран пункт **Настроить параметры для данного почтового ящика**.
5. Проверьте параметры квоты хранилища.

или

В командной консоли Exchange замените <Identity> именем, адресом электронной почты или псевдонимом почтового ящика и выполните следующую команду:

PowerShell

```
Get-Mailbox <Identity> | Format-List
IssueWarningQuota,ProhibitSendQuota,ProhibitSendReceiveQuota,UseDatabaseQuot
aDefaults
```

Настройка квот хранения удаленных элементов и элементов с возможностью восстановления в Exchange Server

Статья • 04.04.2023

Когда пользователь удаляет элементы из используемой по умолчанию папки «Удаленные» с помощью кнопки Delete, сочетания кнопок Shift+Delete или действия **Очистить папку «Удаленные»**, эти элементы перемещаются в папку **Элементы с возможностью восстановления\удаления**. Длительность нахождения удаленных элементов в данной папке зависит от параметров хранения удаленных элементов, заданных для базы данных почтовых ящиков или отдельного почтового ящика. По умолчанию база данных почтовых ящиков настроена на хранение удаленных элементов в течение 14 дней, а для квоты предупреждения элементов для восстановления и квоты элементов для восстановления устанавливаются значения 20 гигабайт (ГБ) и 30 ГБ соответственно.

> ⓘ **Примечание**
>
> До истечения срока хранения удаленных элементов пользователи Outlook и Outlook в Интернете смогут восстановить удаленные элементы с помощью функции Восстановить удаленные элементы. Дополнительные сведения об этих функциях см. в разделе "Восстановление удаленных элементов" для **Outlook для Windows** или **Outlook в Интернете**.

Настроить хранение удаленных элементов и квоты элементов с возможностью восстановления для почтового ящика или базы данных почтовых ящиков можно с помощью командной консоли Exchange. Настройки хранения удаленных элементов игнорируются, когда почтовому ящику назначено удержание на месте или хранении для судебного разбирательства.

Дополнительные сведения о хранении удаленных элементов, папке "Элементы с возможностью восстановления", In-Place удержании и удержании для судебного разбирательства см. в статье Папка "Элементы с возможностью восстановления" в Exchange Server.

Что нужно знать перед началом работы

- Предполагаемое время выполнения: 5 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Управление записями обмена сообщениями" в разделе Политика обмена сообщениями и разрешения на соответствие требованиям Exchange Server.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

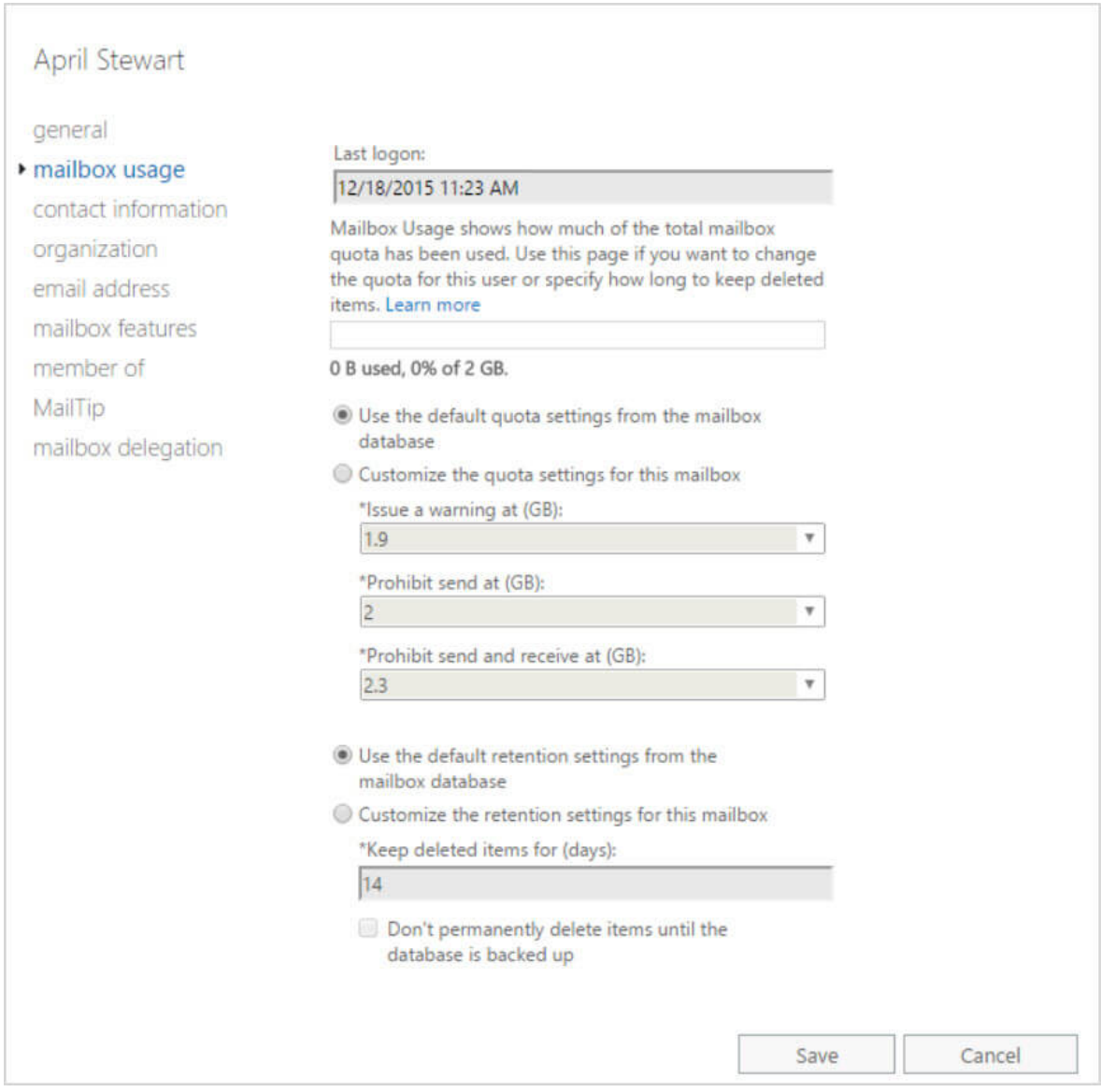
Настроить хранение удаленных элементов для почтового ящика

Настройка хранения удаленных элементов для почтового ящика с помощью Центра администрирования Exchange (EAC)

1. Перейдите в раздел **Почтовые ящики**>**получателей**.
2. В представлении списка выберите почтовый ящик и нажмите кнопку **Изменить**.
3. На странице свойств почтового ящика щелкните **Использование почтового ящика**, щелкните **Дополнительно**, а затем выберите один из следующих вариантов:
   - **Использование параметров хранения по умолчанию из базы данных почтовых ящиков**. Используйте параметр хранения удаленных элементов, настроенный для базы данных почтовых ящиков.
   - **Настройка параметров для этого почтового ящика**. Настройка параметров хранения удаленных элементов для почтового ящика.
   - ***Хранить удаленные элементы в течение (дней)**: отображает время хранения удаленных элементов, прежде чем они будут окончательно удалены и не могут быть восстановлены пользователем. По окончании этого срока удаленные элементы удаляются без возможности

восстановления. При создании почтового ящика это значение зависит от настроек хранения удаленных элементов для базы данных почтовых ящиков. По умолчанию удаленные элементы хранятся в течение 14 дней, но можно выбрать значение от 0 до 24 855 дней.

- **Не удаляйте элементы без возможности восстановления до создания резервной копии базы данных**. Установите этот флажок, чтобы предотвратить удаление почтовых ящиков и сообщений электронной почты до тех пор, пока не будет создана резервная копия базы данных почтовых ящиков, в которой находится почтовый ящик.



Настройка хранения удаленных элементов для базы данных почтовых ящиков

Настройка хранения удаленных элементов для базы данных почтовых ящиков с помощью Центра администрирования Exchange (EAC)

1. Перейдите в раздел **Серверы**>**Базы данных**.

2. В представлении списка выберите базу данных почтовых ящиков и нажмите кнопку **Изменить**.

3. На странице свойств базы данных почтовых ящиков щелкните **Ограничения**, а затем выберите один из следующих вариантов:

    - ***Хранить удаленные элементы в течение (дней)**: отображает время хранения удаленных элементов, прежде чем они будут окончательно удалены и не могут быть восстановлены пользователем. При создании почтового ящика это значение основано на параметрах хранения удаленных элементов, настроенных для базы данных почтовых ящиков. При создании почтового ящика это значение зависит от настроек хранения удаленных элементов для базы данных почтовых ящиков. По умолчанию удаленные элементы хранятся в течение 14 дней, но можно выбрать значение от 0 до 24 855 дней.

    - **Не удаляйте элементы без возможности восстановления до создания резервной копии базы данных**. Установите этот флажок, чтобы предотвратить удаление почтовых ящиков и сообщений электронной почты до тех пор, пока не будет создана резервная копия базы данных почтовых ящиков, в которой находится почтовый ящик.

Настройка хранения удаленных элементов для почтового ящика с помощью командной консоли Exchange

В этом примере почтовый ящик Эйприл Стюарт настраивается для хранения удаленных элементов в течение 30 дней до тех пор, пока не будет создана резервная копия базы данных почтовых ящиков, в которой находится почтовый ящик.

PowerShell

```
Set-Mailbox -Identity - "April Stewart" -RetainDeletedItemsFor 30 -
RetainDeletedItemsUntilBackup $true
```

Подробные сведения о синтаксисе и параметрах см. в разделе Set-Mailbox.

Настроить квоты элементов с возможностью восстановления для почтового ящика с помощью командной консоли Exchange

> **Примечание**
>
> Нельзя использовать EAC, чтобы настроить квоты восстанавливаемых элементов для почтового ящика.

В данном примере описывается настройка квоты предупреждения элементов для восстановления в размере 12 ГБ и квоты элементов для восстановления в размере 15 ГБ для почтового ящика April Stewart.

PowerShell

```
Set-Mailbox -Identity "April Stewart" -RecoverableItemsWarningQuota 12GB -
RecoverableItemsQuota 15GB -UseDatabaseQuotaDefaults $false
```

> **Примечание**
>
> Чтобы настроить для почтового ящика другие квоты восстанавливаемых элементов, чем для базы данных почтовых ящиков, в которой он находится, необходимо задать для параметра *UseDatabaseQuotaDefaults* значение `$false`.

Подробные сведения о синтаксисе и параметрах см. в разделе Set-Mailbox.

Настроить хранение удаленных элементов для базы данных почтовых ящиков с помощью командной консоли Exchange

> **Примечание**
>
> Нельзя использовать EAC, чтобы настроить хранение удаленных элементов для базы данных почтовых ящиков.

В этом примере настраивается период хранения удаленных элементов в 10 дней для базы данных почтовых ящиков MDB2 и параметр для хранения удаленных

элементов до создания резервной копии базы данных почтовых ящиков.

PowerShell

```
Set-MailboxDatabase -Identity MDB2 -DeletedItemRetention 10 -
RetainDeletedItemsUntilBackup $true
```

Подробные сведения о синтаксисе и параметрах см. в разделе Set-MailboxDatabase.

Настроить квоты элементов с возможностью восстановления для базы данных почтовых ящиков с помощью командной консоли Exchange

> **Примечание**
>
> Нельзя использовать EAC, чтобы настроить квоты восстанавливаемых элементов для базы данных почтовых ящиков.

В данном примере описывается настройка квоты предупреждения элементов для восстановления в размере 15 ГБ и квоты элементов для восстановления в размере 20 ГБ для базы данных почтовых ящиков MDB2.

PowerShell

```
Set-MailboxDatabase -Identity MDB2 -RecoverableItemsWarningQuota 15GB -
RecoverableItemsQuota 20GB
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе Set-MailboxDatabase.

Преобразование почтового ящика в Exchange Server

Статья • 04.04.2023

В Exchange Server 2013 или более поздней версии преобразование почтового ящика из одного типа в другой в основном не изменилось по сравнению с exchange 2010. Чтобы выполнить преобразование, вам по-прежнему необходимо использовать командлет **Set-Mailbox** в Командная консоль Exchange.

Преобразовать можно:

- почтовый ящик пользователя в почтовый ящик помещения или оборудования;
- почтовый ящик пользователя в общий почтовый ящик;
- общий почтовый ящик в почтовый ящик пользователя;
- общий почтовый ящик в почтовый ящик помещения или оборудования;
- почтовый ящик помещения или оборудования в почтовый ящик пользователя;
- почтовый ящик помещения или оборудования в общий почтовый ящик.

> ⓘ **Примечание**
>
> Если в вашей организации используется гибридная среда Exchange, необходимо управлять почтовыми ящиками с помощью локальных средств управления Exchange. Чтобы преобразовать почтовый ящик в гибридной среде, может потребоваться переместить его обратно в локальную среду Exchange, преобразовать тип почтового ящика, а затем вернуть его обратно в Microsoft 365 или Office 365.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Почтовые ящики помещений и оборудования, а также общие почтовые ящики имеют связанные учетные записи пользователей в Active Directory, однако эти учетные записи отключены. При преобразовании почтового

ящика одного из этих типов в обычный (почтовый ящик пользователя) необходимо ввести пароль, длина и сложность которого соответствуют требованиям вашей организации.

Для перезаписи существующего пароля требуется роль сброса пароля, которая не назначается по умолчанию группам ролей. О том, как назначить роль вашей группе ролей, см. в разделе Добавление роли в группу ролей. Обратите внимание: чтобы изменения разрешений вступили в силу, необходимо выйти из системы и повторить вход.

- Связанная учетная запись будет отключена при преобразовании обычного почтового ящика (ящика пользователя) в почтовый ящик помещения, оборудования или общий.

  Вы можете включить связанные учетные записи пользователей для почтовых ящиков помещений, но при этом вам опять необходимо будет ввести пароль (для чего требуется роль смены пароля). Включенные учетные записи пользователей для почтовых ящиков помещений необходимы для доступа к таким функциям, как Skype для бизнеса с системой комнат.

- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения подготовки получателей" раздела Разрешения получателей .

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Преобразование почтового ящика с помощью командной консоли Exchange

Чтобы преобразовать почтовый ящик, используйте следующий синтаксис:

```
PowerShell
```

```
Set-Mailbox -Identity <MailboxIdentity> -Type <Regular | Room | Equipment |
Shared> [-Password (ConvertTo-SecureString -String '<Password>' -AsPlainText
-Force)] [-EnableRoomMailboxAccount <$true | $false>] [-RoomMailboxPassword
(ConvertTo-SecureString -String '<Password>' -AsPlainText -Force)] [-
ResetPasswordOnNextLogon <$true | $false>]
```

В этом примере общий почтовый ящик с названием Marketing Dept 01 преобразуется в почтовый ящик пользователя с новым паролем P@ssw0rd25 и требованием сменить пароль при следующем входе пользователя в почтовый ящик.

PowerShell

```
Set-Mailbox -Identity "Marketing Dept 01" -Type Regular -Password
(ConvertTo-SecureString -String 'P@ssw0rd25' -AsPlainText -Force) -
ResetPasswordOnNextLogon $true
```

В этом примере почтовый ящик пользователя с названием Conference Room 01 преобразуется в почтовый ящик помещения.

PowerShell

```
Set-Mailbox -Identity "Conference Room 01" -Type Room
```

Это тот же пример, но с включенной учетной записью пользователя для почтового ящика помещения и паролем P@ssw0rd25

PowerShell

```
Set-Mailbox -Identity "Conference Room 01" -Type Room -
EnableRoomMailboxAccount $true -RoomMailboxPassword (ConvertTo-SecureString
-String 'P@ssw0rd25' -AsPlainText -Force)
```

Примечание. Даже при преобразовании почтового ящика пользователя с известным паролем в почтовый ящик комнаты все равно необходимо использовать параметр *RoomMailboxPassword* для указания пароля.

Подробные сведения о синтаксисе и параметрах см. в разделе Set-Mailbox.

Как проверить, все ли получилось?

Чтобы убедиться, что почтовый ящик успешно преобразован, *замените*< *MailboxIdentity*> именем, псевдонимом или адресом электронной почты почтового

ящика и выполните следующую команду в командной консоли Exchange, чтобы проверить значения свойств:

PowerShell

```
Get-Mailbox -Identity <MailboxIdentity> | Format-List
Name,RecipientTypeDetails,UserPrincipalName,AccountDisabled
```

Подробные сведения о синтаксисе и параметрах см. в разделе Get-Mailbox.

Включение или отключение восстановления отдельного элемента в почтовом ящике

Статья • 04.04.2023

С помощью командной консоли Exchange можно включить или отключить восстановление одного элемента в почтовом ящике. В Exchange Server восстановление одного элемента отключено при создании почтового ящика. Если включено восстановление одного элемента, сообщения, очищенные (жестко удаленные) пользователем, хранятся в папке "Элементы с возможностью восстановления" почтового ящика до истечения срока хранения удаленных элементов. Это позволяет администратору восстанавливать сообщения, очищенные пользователем до истечения срока хранения удаленных элементов.

Что нужно знать перед началом работы

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Хранение и удержание по юридическим причинам" в разделе Разрешения получателей .
- Включить или отключить восстановление отдельных элементов с помощью Центра администрирования Exchange (EAC) невозможно.
- В Exchange Server почтовый ящик по умолчанию использует параметры хранения удаленных элементов базы данных почтовых ящиков. Срок хранения удаленных элементов для базы данных почтового ящика составляет 14 дней, но значение по умолчанию можно переопределить, настроив эти параметры для каждого почтового ящика отдельно. Дополнительные сведения см. в разделе Настройка квот на хранение удаленных элементов и восстанавливаемых элементов.

Включение восстановления отдельных элементов

В данном примере показывается включение восстановления отдельных элементов для почтового ящика пользователя April Summers.

PowerShell

```
Set-Mailbox -Identity "April Summers" -SingleItemRecoveryEnabled $true
```

В данном примере показывается включение восстановления отдельных элементов для почтового ящика пользователя Pilar Pinilla и установка количества дней для сохранения удаленных элементов, равное 30.

PowerShell

```
Set-Mailbox -Identity "Pilar Pinilla" -SingleItemRecoveryEnabled $true -
RetainDeletedItemsFor 30
```

В данном примере показывается, как включить восстановление отдельных элементов для всех почтовых ящиков пользователей в организации.

PowerShell

```
Get-Mailbox -ResultSize unlimited -Filter "RecipientTypeDetails -eq
'UserMailbox'" | Set-Mailbox -SingleItemRecoveryEnabled $true
```

В этом примере показано, как включить восстановление отдельного элемента для всех почтовых ящиков пользователей в организации и установить период хранения удаленных элементов в 30 дней.

PowerShell

```
Get-Mailbox -ResultSize unlimited -Filter "RecipientTypeDetails -eq
'UserMailbox'" | Set-Mailbox -SingleItemRecoveryEnabled $true -
RetainDeletedItemsFor 30
```

Подробные сведения о синтаксисе и параметрах см. в разделе Set-Mailbox.

Отключение функции восстановления отдельного элемента

Может потребоваться отключить восстановление одного элемента для почтового ящика пользователя. Например, прежде чем использовать **Search-Mailbox -DeleteContent** для окончательного удаления содержимого из почтового ящика, необходимо отключить восстановление одного элемента. Дополнительные сведения см. в разделе Поиск и удаление сообщений в Exchange Server.

В этом примере отключается восстановление отдельных элементов для почтового ящика пользователя Ayla Kol.

PowerShell

```
Set-Mailbox -Identity "Ayla Kol" -SingleItemRecoveryEnabled $false
```

Как проверить, все ли получилось?

Чтобы проверить, включено ли восстановление отдельных элементов для почтового ящика и отображается ли значение срока хранения удаленных элементов (в днях), выполните следующую команду.

PowerShell

```
Get-Mailbox <Name> | Format-List
SingleItemRecoveryEnabled,RetainDeletedItemsFor
```

Вы также можете использовать эту команду, чтобы проверять, отключено ли восстановление отдельных элементов в почтовом ящике.

Дополнительные сведения

- Дополнительные сведения о восстановлении одного элемента см. в статье Папка "Элементы с возможностью восстановления" в Exchange Server. Сведения о восстановлении удаленных пользователем сообщений до окончания срока хранения см. в статье Recover deleted messages in a user's mailbox.
- Если почтовый ящик помещается на хранение для судебного разбирательства или хранение на месте, сообщения в папке "Элементы для восстановления" сохраняются в течение всего периода хранения. Если период хранения не ограничен, элементы сохраняются до прекращения хранения или изменения периода хранения.

Восстановление удаленных сообщений в почтовом ящике пользователя в Exchange Server

Статья • 04.04.2023

Администраторы могут искать элементы, которые были очищены (удалены пользователем) с помощью функции Восстановить удаленные элементы в Outlook или Outlook в Интернете. Они также могут искать элементы, удаленные автоматическим процессом, например политику хранения, назначенную почтовым ящикам пользователей. В таких ситуациях очищенные элементы не могут быть восстановлены пользователем. Но администраторы могут восстановить очищенные сообщения, если срок хранения удаленного элемента не истек.

> ⓘ **Примечание**
>
> Кроме поиска и восстановления удаленных элементов, эту функцию также можно использовать для поиска элементов в других папках и удаления элементов из исходного почтового ящика (*поиск и удаление*).

Что нужно знать перед началом работы?

- Для процедур, описанных в этом разделе, требуются определенные разрешения. Сведения о разрешениях см. в каждой процедуре.
- Для почтового ящика должно быть включено восстановление отдельных элементов перед удалением нужного элемента. В Exchange Server восстановление одного элемента отключено при создании почтового ящика. Дополнительные сведения см. в статье Enable or disable single item recovery for a mailbox.
- Для поиска и восстановления элементов нужны следующие сведения:
  - **Исходный почтовый ящик**: почтовый ящик, в который выполняется поиск.
  - **Целевой почтовый ящик**: почтовый ящик обнаружения, в котором будут восстанавливаться сообщения. Exchange Server программа установки создает почтовый ящик обнаружения по умолчанию. По умолчанию этот почтовый ящик также создается в Exchange Online. При необходимости

можно создать дополнительные почтовые ящики обнаружения. в разделе Create a Discovery Mailbox.

> ⓘ **Примечание**
>
> С помощью командлета **Search-Mailbox** можно также указать другой целевой почтовый ящик вместо ящика найденных сообщений. Однако невозможно указать один ящик в качестве исходного и целевого одновременно.

- **Критерии поиска**. Критерии включают отправителя или получателя или ключевые слова (слова или фразы) в сообщении.

Действие 1. Поиск и восстановление отсутствующих элементов

Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Обнаружение электронных данных на месте" в разделе Политика обмена сообщениями и разрешения на соответствие требованиям Exchange Server.

> ⓘ **Примечание**
>
> Вы можете использовать In-Place eDiscovery в Центре администрирования Exchange (EAC) для поиска отсутствующих элементов. Однако при использовании EAC нельзя ограничить поиск папкой "Элементы с возможностью восстановления". Все сообщения, соответствующие параметрам поиска, будут возвращены, даже если они не удалены. После их восстановления в указанный почтовый ящик обнаружения может потребоваться просмотреть результаты поиска и удалить ненужные сообщения, прежде чем восстановить оставшиеся сообщения в почтовый ящик пользователя или экспортировать их в PST-файл. Дополнительные сведения о том, как использовать EAC для выполнения поиска In-Place eDiscovery, см. **в разделе Создание поиска In-Place eDiscovery в Exchange Server**.

Первым шагом процесса восстановления является поиск сообщений в исходном почтовом ящике. Используйте один из следующих способов поиска в почтовом

ящике пользователя и копирования сообщений в почтовый ящик найденных сообщений.

Поиск сообщений с помощью командной консоли Exchange

PowerShell

```
Get-RecoverableItems -Identity laura@contoso.com -SubjectContains "FY17 Accounting" -FilterItemType IPM.Note -FilterStartTime "2/1/2018 12:00:00 AM" -FilterEndTime "2/5/2018 11:59:59 PM"
```

В этом примере возвращаются все доступные для восстановления удаленные сообщения с указанной темой в почтовом ящике laura@contoso.com для указанного диапазона даты и времени.

> **Совет**
>
> Используйте командлет **Get-RecoverableItems** , чтобы создать поисковый запрос для поиска элемента Outlook. Получив список результатов, можно использовать такие свойства, как дата последнего изменения, тип элемента и т. д., чтобы сузить количество восстановленных элементов или восстановить определенный элемент.

Подробные сведения о синтаксисе и параметрах см. в разделе Get-RecoverableItems.

Как проверить, все ли получилось?

Чтобы убедиться в том, что вы успешно нашли сообщения, которые вы хотите восстановить, войдите в почтовый ящик обнаружения, выбранный в качестве целевого почтового ящика, и ознакомьтесь с результатами поиска.

Действие 2. Восстановление элементов из папки «Восстановленные»

Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Обнаружение электронных данных на месте" в разделе Политика обмена сообщениями и разрешения на соответствие требованиям Exchange Server.

> ⓘ **Примечание**
>
> Невозможно использовать EAC для восстановления элементов из папки «Восстановленные».

После восстановления сообщений в почтовый ящик найденных сообщений можно восстановить их в почтовый ящик пользователя с помощью командлета **Search-Mailbox**. В Exchange Server можно также использовать командлеты **New-MailboxExportRequest** и **New-MailboxImportRequest** для экспорта сообщений в PST-файл или их импорта.

Восстановление сообщений с помощью командной консоли Exchange

PowerShell

```
$mailboxes = Import-CSV "C:\My Documents\RestoreMessage.csv"; $mailboxes |
foreach {Restore-RecoverableItems -Identity $_.SMTPAddress -SubjectContains
Project X" -SourceFolder DeletedItems -FilterItemType IPM.Note}
```

В этом примере восстанавливается удаленное сообщение электронной почты "Project X" для почтовых ящиков, указанных в csv-файле C:\My Documents\RestoreMessage.csv. CSV-файл использует значение заголовка SMTPAddress и содержит адреса электронной почты каждого почтового ящика в отдельной строке следующим образом:

SMTPAddress

chris@contoso.com

michelle@contoso.com

laura@contoso.com

julia@contoso.com

Первая команда считывает CSV-файл в переменную с именем $mailboxes. Вторая команда восстанавливает указанное сообщение из папки "Удаленные" в этих почтовых ящиках.

Подробные сведения о синтаксисе и параметрах см. в разделе Restore-RecoverableItems.

Как проверить, что все получилось?

Для проверки успешного восстановления сообщений в почтовом ящике пользователя пользователю необходимо просмотреть сообщения в целевой папке, указанной в команде, приведенной выше.

Экспорт сообщений в файл PST и импорт сообщений из него с помощью командной консоли Exchange

В Exchange Server можно экспортировать содержимое из почтового ящика в PST-файл и импортировать содержимое PST-файла в почтовый ящик. Дополнительные сведения об импорте и экспорте почтовых ящиков см. в статье Импорт и экспорт почтовых ящиков в Exchange Server. Эту задачу нельзя выполнить в Exchange Online.

В этом примере для экспорта сообщений из папки "April Stewart Recovery" почтового ящика найденных сообщений в PST-файл используются следующие параметры.

- **Почтовый ящик: почтовый** ящик поиска обнаружения
- **Исходная папка**: April Stewart Recovery
- **ContentFilter**: апрельские планы поездок
- **Путь к PST-файлу**: \MYSERVER\HelpDeskPst\AprilStewartRecovery.pst

PowerShell

```
New-MailboxExportRequest -Mailbox "Discovery Search Mailbox" -
SourceRootFolder "April Stewart Recovery" -ContentFilter "Subject -eq 'April
travel plans'" -FilePath \\MYSERVER\HelpDeskPst\AprilStewartRecovery.pst
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе New-MailboxExportRequest.

В этом примере для импорта сообщений из файла PST в папку «Восстановленные службой технической поддержки» в почтовом ящике пользователя April Stewart используются следующие параметры.

- **Почтовый ящик**: Эйприл Стюарт
- **Целевая папка**: восстановлена службой поддержки
- **Путь к PST-файлу**: \MYSERVER\HelpDeskPst\AprilStewartRecovery.pst

PowerShell

```
New-MailboxImportRequest -Mailbox "April Stewart" -TargetRootFolder
"Recovered By Helpdesk" -FilePath
\\MYSERVER\HelpDeskPst\AprilStewartRecovery.pst
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе New-MailboxImportRequest.

Как проверить, что все получилось?

Чтобы убедиться в том, что вы успешно экспортировали сообщения в PST-файл используйте Outlook для открытия PST-файла и проверьте его содержимое. Чтобы убедиться в том, что вы успешно импортировали сообщения из PST-файла, пользователю необходимо осмотреть содержимое указанной папки назначения в команде, приведенной выше.

Дополнительные сведения

- Если включено *восстановление отдельных элементов*, администратор может восстановить сообщения, удаленные пользователем или политикой хранения, если еще не истек их срок хранения. Дополнительные сведения о восстановлении одного элемента см. в статье Папка "Элементы с возможностью восстановления" в Exchange Server.
- В Exchange Server база данных почтовых ящиков по умолчанию настроена на хранение удаленных элементов в течение 14 дней. Вы можете настроить хранение удаленных элементов для почтового ящика или базы данных почтовых ящиков. Дополнительные сведения см. в разделе:
  - Настройка хранения удаленных элементов и квот элементов для восстановления
- Пользователи могут восстановить удаленный элемент, если он не был окончательно удален, и если срок хранения удаленных элементов для этого элемента не истек. Если пользователям требуется восстановить удаленные элементы из папки "Элементы с возможностью восстановления", рекомендуем ознакомиться со следующими статьями:
  - Восстановление удаленных элементов в Outlook для Windows
  - Восстановление удаленных элементов или электронной почты в Outlook в Интернете

- В этой статье описано, как использовать командлет **Search-Mailbox** для поиска и восстановления элементов. С его помощью можно выполнять поиск только в одном почтовом ящике. Если вы хотите выполнить поиск в нескольких почтовых ящиках одновременно, можно использовать обнаружение электронных данных на месте в Exchange Server в Центре администрирования Exchange (EAC) или командлет New-ComplianceSearch в Windows PowerShell.

- Кроме поиска и восстановления удаленных элементов, похожую процедуру можно использовать для поиска элементов в почтовых ящиках пользователей и удаления найденных элементов из исходного почтового ящика. Дополнительные сведения см. в разделе Поиск и удаление сообщений в Exchange Server.

Связанная статья

Вы используете Exchange Online? См. статью Восстановление удаленных сообщений в почтовом ящике пользователя в Exchange Online.

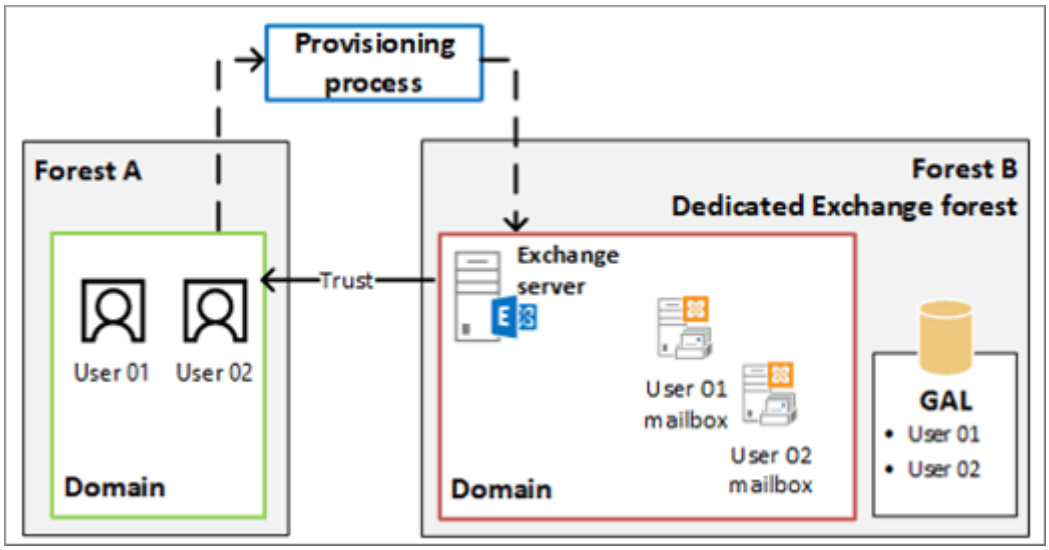
Управление связанными почтовыми ящиками в Exchange Server

Статья • 04.04.2023

Связанные почтовые ящики могут потребоваться организациям, которые развертывают Exchange в *лесу ресурсов*. Сценарий леса ресурсов позволяет организации централизовать Exchange в одном лесу, в то же время предоставляя доступ к организации Exchange с учетными записями пользователей, расположенными в одном или нескольких доверенных лесах (называемых *лесами учетных записей*). Учетная запись пользователя, которая получает доступ к связанному почтовому ящику, не существует в лесу, в котором развернут Exchange. Поэтому в этом лесу создается отключенная учетная запись пользователя, которая связывается с соответствующим почтовым ящиком.

На следующем рисунке показана связь между связанной учетной записью пользователя, которая используется для доступа к связанному почтовому ящику, и отключенной учетной записью пользователя в лесу ресурсов Exchange, связанной с этим почтовым ящиком.

Связанные почтовые ящики



> ⓘ **Примечание**
>
> Прежде чем можно будет создавать связанные почтовые ящики, необходимо настроить отношения доверия между лесом Exchange и хотя бы одним лесом учетных записей. Как минимум, необходимо настроить односторонное исходящее доверие, чтобы лес Exchange доверял лесу учетной записи.

Дополнительные сведения см. в статье **Learn more about setting up a forest trust to support linked mailboxes.**

Что нужно знать перед началом работы

- Осталось времени до завершения: от 2 до 5 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения подготовки получателей" раздела Разрешения получателей .
- Учетная запись пользователя (называемая *связанной главной учетной записью*) должна существовать в лесу учетных записей, чтобы можно было создать новый связанный почтовый ящик. Это вызвано тем, что связанный почтовый ящик связывается с пользователем в лесу учетных записей.
- Если вы настроите одностороннее исходящее доверие, в котором лес Exchange доверяет лесу учетных записей, для создания связанного почтового ящика потребуются учетные данные администратора в лесу учетных записей.

  Чтобы создать связанный почтовый ящик, не указывая учетные данные администратора в лесу учетных записей, необходимо создать двустороннее доверие или еще одно одностороннее исходящее доверие, в котором лес учетных записей также доверяет лесу Exchange. На этом шаге также требуется ввести учетные данные администратора в лесу учетных записей.
- Эту процедуру можно выполнить в Центре администрирования Exchange или командной консоли Exchange.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Создание связанного почтового ящика

Использование EAC для создания связанного почтового ящика

1. В Центре администрирования Exchange (EAC) выберите **Получатели**>**Почтовые ящики**.

2. Щелкните **Создать**>**связанный почтовый ящик**.

3. На странице **Новый связанный почтовый ящик** в поле **Доверенный лес или домен** выберите имя леса учетных записей, который содержит нужную учетную запись пользователя, для которой создается связанный почтовый ящик. Нажмите кнопку **"Далее"**.

4. Если в организации настроено одностороннее исходящее доверие, в котором лес Exchange доверяет лесу учетных записей, чтобы получить доступ к контроллеру домена в доверенном лесу, потребуется ввести учетные данные администратора в лесу учетных записей. Введите имя пользователя и пароль для учетной записи администратора в лесу учетных записей, а затем нажмите кнопку **Далее**.

   > ⓘ **Примечание**
   >
   > Учетные данные администратора не будут запрашиваться, если вы создали двустороннее доверие или другое одностороннее исходящее доверие, в котором лес учетных записей доверяет лесу Exchange.

5. Заполните следующие поля на странице **Выбор связанной главной учетной записи**.

   - **Связанный контроллер домена**. Выберите контроллер домена в лесу учетных записей. Exchange подключится к этому контроллеру домена, чтобы получить список учетных записей пользователей в лесу учетных записей, чтобы можно было выбрать связанную главную учетную запись.

   - **Связанная главная учетная запись**. Нажмите кнопку **Обзор**, выберите учетную запись пользователя в лесу учетных записей и нажмите кнопку **ОК**. Новый связанный почтовый ящик будет связан с этой учетной записью.

6. Щелкните **Далее** и заполните следующие поля на странице **Введите общие сведения**.

- * **Имя**: используйте это поле, чтобы ввести имя пользователя. Это имя используется в качестве отображаемого имени в EAC и адресной книге организации, а также в Active Directory. Имя вводить обязательно.

- **Подразделение**. Вы можете выбрать подразделение, отличное от стандартного (который является областью получателя). Если область получателей установлена на уровне леса, будет установлено значение по умолчанию для контейнера "Пользователи" домена Active Directory, в котором находится компьютер с запущенным центром администрирования Exchange. Если область получателей настроена на определенный домен, то контейнер пользователей в этом домене выбирается по умолчанию. Если в качестве области получателей задано определенное подразделение организации, то оно выбирается по умолчанию.

  Нажмите **Обзор**, чтобы выбрать другое подразделение. В этом диалоговом окне отображаются все подразделения в лесу Exchange, которые находятся в указанной области. Выберите нужное подразделение и нажмите **ОК**.

- * **Имя входа пользователя**. Используйте это поле, чтобы ввести имя пользователя, необходимое для создания связанного почтового ящика. Введите имя пользователя здесь. Это имя будет использовано в левой части адреса электронной почты для связанного почтового ящика, если вы не укажете псевдоним.

  > ⓘ **Примечание**
  >
  > Так как учетная запись пользователя, созданная в лесу Exchange, отключена при создании связанного почтового ящика, пользователь не использует имя пользователя для входа в связанный почтовый ящик. Они выполняют вход, используя свои учетные данные из леса учетных записей.

7. Чтобы настроить следующие поля, нажмите кнопку **Дополнительные параметры**. В противном случае перейдите к шагу 8, чтобы сохранить новый связанный почтовый ящик.

   - **Псевдоним**. Введите псевдоним, указывающий псевдоним электронной почты для связанного почтового ящика. Псевдоним пользователя — это часть адреса электронной почты слева от символа (@). Псевдоним должен быть уникальным в пределах леса.

> ⓘ **Примечание**
>
> Если оставить это поле пустым, для псевдонима электронной почты будет использоваться значение из части имени пользователя .

- **Имя**, **Отчество**, **Фамилия**

- **База данных почтовых ящиков**. Используйте этот параметр, чтобы указать базу данных почтовых ящиков вместо того, чтобы разрешить Exchange выбрать базу данных. Нажмите **Обзор**, чтобы открыть диалоговое окно **Выбор базы данных почтовых ящиков**. В этом диалоговом окне указаны все базы данных почтовых ящиков в организации Exchange. По умолчанию они отсортированы по имени. Чтобы отсортировать базы данных по имени или версии сервера, щелкните заголовок соответствующего столбца. Выберите необходимую базу данных почтовых ящиков и нажмите **OK**.

- **Политика адресной книги**. Используйте этот параметр, чтобы указать политику адресной книги (ABP) для связанного почтового ящика. Политика адресных книг содержит глобальный список адресов, автономную адресную книгу, список помещений и набор списков адресов. При назначении пользователям ABP предоставляет им доступ к настраиваемому глобальному списку в Outlook и Outlook в Интернете (ранее — Outlook Web App). Дополнительные сведения см. в разделе Политики адресных книг в Exchange Server.

  Из раскрывающегося списка выберите политику, которую нужно сопоставить с этим почтовым ящиком.

8. По завершении нажмите кнопку **Сохранить**, чтобы создать связанный почтовый ящик.

Создание связанного почтового ящика в командной консоли Exchange

В этом примере показано, как создать связанный почтовый ящик для пользователя Ayla Kol в лесе ресурсов Exchange CONTOSO. Домен FABRIKAM находится в лесу учетных записей. Учетная запись администратора FABRIKAM\administrator используется для доступа к связанному контроллеру домена.

```
PowerShell
```

```
New-Mailbox -Name "Ayla Kol" -LinkedDomainController "DC1_FABRIKAM" -
LinkedMasterAccount " FABRIKAM\aylak" -OrganizationalUnit Users -
UserPrincipalName aylak@contoso.com -LinkedCredential:(Get-Credential
FABRIKAM\administrator)
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе New-Mailbox.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли создан связанный почтовый ящик, выполните одно из следующих действий.

- В Центре администрирования Exchange (EAC) выберите **Получатели**>**Почтовые ящики**. Новый почтовый ящик отображается в списке почтовых ящиков. В разделе **Тип почтового ящика** указан тип **Связанный**.
- В командной консоли Exchange выполните следующую команду для вывода информации о новом почтовом ящике.

  PowerShell

  ```
  Get-Mailbox <Name> | Format-List
  Name,RecipientTypeDetails,IsLinked,LinkedMasterAccount
  ```

Изменение свойств связанного почтового ящика

После создания почтового ящика пользователя вы можете изменять и добавлять свойства с помощью Центра администрирования Exchange или командной консоли Exchange.

Также можно одновременно менять свойства нескольких связанных почтовых ящиков. Дополнительные сведения см. в разделе Массовое изменение почтовых ящиков пользователей.

> ⓘ **Важно!**
>
> Время выполнения этой задачи зависит от количества свойств, которые нужно просмотреть или изменить.

Использование EAC для изменения свойств связанного почтового ящика

1. В Центре администрирования Exchange (EAC) выберите **Получатели**>**Почтовые ящики**.
2. В списке почтовых ящиков щелкните связанный почтовый ящик, свойства которого требуется изменить, а затем щелкните **Изменить**.
3. На странице свойств почтового ящика щелкните один из следующих разделов, чтобы просмотреть или изменить свойства.
   - Общие
   - Заполнение почтового ящика
   - Адрес электронной почты
   - Функции почтового ящика
   - Участник
   - Подсказка

Общие сведения

В разделе **Общие** можно просматривать и изменять основные сведения о пользователе.

- * **Имя связанного почтового ящика**: это имя, указанное в Active Directory. Если вы решите изменить это имя, помните, что оно не может превышать 64 символа.
- * **Отображаемое имя**: это имя отображается в адресной книге вашей организации, в строках "По" и "От": в сообщении электронной почты, а также в списке Почтовые ящики в EAC. Это имя не может содержать пробелы до или после отображаемого имени.
- * **Имя входа пользователя**. Для почтовых ящиков пользователей это имя, которое пользователь использует для входа в свой почтовый ящик и для входа в домен. Для связанных почтовых ящиков соответствующая учетная запись пользователя, которая создается в лесу Exchange при создании связанного почтового ящика, отключена. Пользователь использует для входа в связанный почтовый ящик учетные данные из леса учетных записей.

Если вы измените это имя, оно должно быть уникальным в пределах организации.

- **Связанная главная учетная запись**. В этом поле только для чтения отображается пользователь (в формате домен\имя пользователя) из леса учетных записей, связанного со связанным почтовым ящиком. Чтобы изменить связанную главную учетную запись, связанную со связанным почтовым ящиком, необходимо использовать командлет **Set-Mailbox** в командной консоли Exchange. При изменении связанной главной учетной записи пользователю потребуется использовать учетные данные для новой связанной главной учетной записи для входа в связанный почтовый ящик. Синтаксис команды для изменения связанной главной учетной записи см. в статье Изменение свойств связанного почтового ящика с помощью командной консоли Exchange.

- **Скрыть из списков адресов**. Установите этот флажок, чтобы предотвратить появление связанного почтового ящика в адресной книге и других списках адресов, определенных в организации Exchange. Пользователи все равно смогут отправлять сообщения этому пользователю, используя адрес электронной почты.

Щелкните **Дополнительные параметры**, чтобы просмотреть или изменить дополнительные свойства:

- **Подразделение**. В этом поле только для чтения отображается подразделение, содержащее учетную запись пользователя. Чтобы переместить учетную запись пользователя в другое подразделение, необходимо использовать средство "Пользователи и компьютеры Active Directory".

- **База данных почтовых ящиков**. В этом поле только для чтения отображается имя базы данных почтовых ящиков, в котором размещается почтовый ящик. Чтобы переместить почтовый ящик в другую базу данных, выберите его в списке почтовых ящиков, а затем щелкните **Переместить почтовый ящик в другую базу данных** в области сведений.

- ***Псевдоним** Это указывает псевдоним электронной почты для связанного почтового ящика. Псевдоним — это часть адреса электронной почты слева от знака "@". Псевдоним должен быть уникальным в пределах леса.

- **Имя**, **Отчество**, **Фамилия**

- **Настраиваемые атрибуты**. В этом разделе отображаются настраиваемые атрибуты, определенные для связанного почтового ящика. Чтобы указать

значения настраиваемых атрибутов, нажмите кнопку **Изменить**✏️ Для получателя можно указать до 15 настраиваемых атрибутов.

Заполнение почтового ящика

Используйте раздел **Заполнение почтового ящика** для просмотра и изменения квот хранения и параметров хранения удаленных элементов для почтового ящика. Эти параметры настраиваются по умолчанию при создании почтового ящика. Они используют значения, настроенные для базы данных почтовых ящиков и применяемые ко всем почтовым ящикам в этой базе данных. Можно настроить эти параметры для каждого почтового ящика, а не использовать установленные по умолчанию настройки базы данных почтовых ящиков.

- **Последний вход**. В этом поле только для чтения отображается время последнего входа пользователя в почтовый ящик.
- **Использование почтового ящика**. В этой области отображается общий размер почтового ящика и процент использованной общей квоты почтового ящика.

> ⓘ **Примечание**
>
> Чтобы получить отображаемые в предыдущих двух полях сведения, Центр администрирования Exchange отправляет запрос в базу данных почтовых ящиков. Если он не может связаться с хранилищем базы данных, эти поля остаются пустыми. Если пользователь не вошел в почтовый ящик в первый раз, отображается предупреждение.

Нажмите кнопку **Дополнительные параметры**, если нужно просмотреть или изменить квоту хранилища почтового ящика и параметры хранения удаленных элементов для почтового ящика.

- **Параметры квоты хранилища**. Чтобы настроить эти параметры для почтового ящика и не использовать значения по умолчанию базы данных почтовых ящиков, щелкните **Настроить параметры для этого почтового ящика**, введите новое значение и нажмите кнопку **Сохранить**.

  Диапазон значений для каждого из параметров квоты хранилища составляет от 0 до 2 047 гигабайт (ГБ).

  - **Выдача предупреждения в (ГБ):** в этом поле отображается максимальный объем хранилища, прежде чем пользователю будет выдано

предупреждение. Если размер почтового ящика равен указанному значению или превышает его, пользователю этого ящика на сервере Exchange отправляется предупреждающее сообщение.

  - **Запретить отправку в (ГБ):** в этом поле отображается ограничение *запрета отправки* для почтового ящика. Если размер почтового ящика достигнет указанного значения или превысит его, пользователь не сможет отправлять новые сообщения — появится сообщение об ошибке.

  - **Запретить отправку и получение в (ГБ).** В этом поле отображается ограничение *запрета на отправку и получение* для почтового ящика. Если размер почтового ящика достигнет указанного значения или превысит его, пользователь почтового ящика не сможет отправлять и получать новые сообщения. Сообщения, отправляемые в почтовый ящик, будут возвращаться отправителю с сообщением об ошибке.

- **Параметры хранения удаленных элементов**. Чтобы настроить эти параметры для почтового ящика и не использовать значения по умолчанию базы данных почтовых ящиков, щелкните **Настройка параметров для этого почтового ящика**, введите новое значение и нажмите кнопку **Сохранить**.

  - **Хранить удаленные элементы в течение (дней)**: в этом поле отображается время хранения удаленных элементов до их окончательного удаления и не может быть восстановлено пользователем. При создании почтового ящика это время зависит от параметров хранения удаленных элементов, заданных в базе данных почтовых ящиков. По умолчанию для базы данных почтовых ящиков настроено хранение удаленных элементов в течение 14 дней. Диапазон значений этого свойства находится в пределах от 0 до 24 855 дней.

  - **Не удаляйте элементы без возможности восстановления до создания резервной копии базы данных**. Установите этот флажок, чтобы запретить удаление почтовых ящиков и сообщений электронной почты до тех пор, пока не будет создана резервная копия базы данных почтовых ящиков, в которой находится почтовый ящик.

Адрес электронной почты

Используйте раздел **Адрес электронной почты** для просмотра и изменения адресов электронной почты, связанных с почтовым ящиком. Он включает основные адреса SMTP пользователя и любые связанные прокси-адреса. Основной адрес SMTP (также называется *адрес ответа по умолчанию*) отображается

жирным шрифтом в списке адресов со значением **SMTP** (прописными буквами) в столбце **Тип**.

- **Добавить: щелкните**+ чтобы добавить новый адрес электронной почты для этого почтового ящика. Выберите один из следующих типов адресов:
  - **SMTP**. Это тип адреса по умолчанию. Нажмите эту кнопку, а затем введите новый адрес SMTP в поле *** Адрес электронной почты**.
  - **EUM**. Адрес EUM (Единая система обмена сообщениями Exchange) используется службой единой системы обмена сообщениями Exchange в Exchange 2016 для поиска пользователей с поддержкой единой системы обмена сообщениями в организации Exchange. Адреса единой системы обмена сообщениями Exchange содержат добавочный номер и абонентскую группу единой системы обмена сообщениями для пользователя с включенной поддержкой единой системы обмена сообщениями. Нажмите эту кнопку и введите добавочный номер в поле **Адрес/добавочный номер**. После этого нажмите **Обзор** и выберите абонентскую группу для пользователя. (**Примечание**. Единая система обмена сообщениями недоступна в Exchange 2019.)
  - **Пользовательский тип адреса**. Нажмите эту кнопку и введите один из поддерживаемых типов адресов электронной почты, **отличных от** SMTP, в поле *Email адрес.

    > ⓘ **Примечание**
    >
    > Настраиваемый адрес. Чтобы добавить настраиваемый адрес (например, факс или X.400), нажмите эту кнопку и используйте соответствующее диалоговое окно.

- **Автоматически обновлять адреса электронной почты на основе политики адресов электронной почты, применяемой к этому получателю**. Установите этот флажок, если вы хотите, чтобы адреса электронной почты получателя обновлялись автоматически при внесении изменений в политики адресов электронной почты в вашей организации. По умолчанию этот флажок установлен.

Функции почтового ящика

В разделе **Функции почтового ящика** можно просматривать и изменять следующие функции и параметры почтовых ящиков:

- **Политика общего доступа**. В этом поле показана политика общего доступа, применяемая к почтовому ящику. Она определяет правила предоставления общего доступа к календарю и контактной информация для внешних пользователей. При создании почтовым ящикам назначается политика общего доступа по умолчанию. Чтобы изменить назначенную пользователю политику общего доступа, выберите другую политику из раскрывающегося списка.

- **Политика назначения ролей**. В этом поле отображается политика назначения ролей, назначенная почтовому ящику. Политика назначения ролей определяет роли управления доступом на основе ролей, назначенные пользователю, и определяет, какие параметры конфигурации почтового ящика и групп рассылки он может изменять. Чтобы изменить выбранную для пользователя политику назначения ролей, выберите другую политику из раскрывающегося списка.

- **Политика хранения**. В этом поле отображается политика хранения, назначенная почтовому ящику. Политика хранения представляет собой группу тегов хранения, которые применяются к почтовому ящику пользователя. Теги позволяют управлять сроками хранения элементов почтовых ящиков пользователей и указывать действия, применяемые к элементам, достигшим определенного возраста. Политика хранения не назначается почтовым ящикам во время их создания. Чтобы назначить пользователю политику хранения, выберите ее из раскрывающегося списка.

- **Политика адресной книги**. В этом поле отображается политика адресной книги, примененная к почтовому ящику. Политика адресных книг позволяет делить пользователей на определенные группы для обеспечения настраиваемых представлений адресной книги. Для применения или изменения политики адресной книги почтового ящика выберите ее из раскрывающегося списка.

- **Единая система обмена сообщениями**. Эта функция отключена по умолчанию. При включении единой системы обмена сообщениями (UM) в Exchange 2016 пользователь сможет использовать функции единой системы обмена сообщениями вашей организации, а набор свойств единой системы обмена сообщениями по умолчанию применяется к пользователю. Нажмите кнопку **Включить**, чтобы включить единую систему обмена сообщениями для почтового ящика. Сведения о включении единой системы обмена сообщениями см. в разделе Enable a User for Unified Messaging. (**Примечание**. Единая система обмена сообщениями недоступна в Exchange 2019.)

> ⓘ **Примечание**
>
> Для включения единой системы обмена сообщениями необходимо сначала создать абонентскую группу единой системы обмена сообщениями и политику почтовых ящиков единой системы обмена сообщениями.

- **Мобильные устройства**. Используйте этот раздел для просмотра и изменения параметров для Exchange ActiveSync, которые включены по умолчанию. Exchange ActiveSync обеспечивает доступ к почтовому ящику Exchange с мобильного устройства. Чтобы отключить эту функцию для почтового ящика, нажмите **Отключить Exchange ActiveSync**.

- **Outlook Web App**. Эта функция включена по умолчанию. Outlook в Интернете обеспечивает доступ к почтовому ящику Exchange через веб-браузер. Нажмите **Отключить**, чтобы отключить Outlook в Интернете для почтового ящика. Нажмите **Изменить сведения**, чтобы добавить или изменить политику почтовых ящиков Outlook в Интернете для почтового ящика.

- **IMAP**: эта функция включена по умолчанию. Чтобы отключить функцию IMAP для почтового ящика, щелкните **Отключить**.

- **POP3**: эта функция включена по умолчанию. Чтобы отключить функцию POP3 для почтового ящика, щелкните **Отключить**.

- **MAPI**: эта функция включена по умолчанию. MAPI обеспечивает доступ к почтовому ящику Exchange из клиента MAPI, такого как Outlook. Чтобы отключить MAPI для почтового ящика, нажмите **Отключить**.

- **Удержание для судебного разбирательства**. Эта функция отключена по умолчанию. Судебное удержание позволяет сохранять удаленные элементы почтовых ящиков и записывать изменения в элементах. Удаленные элементы и все экземпляры измененных элементов возвращаются при поиске на обнаружение. Нажмите кнопку **Включить**, чтобы поместить почтовый ящик на хранение для судебного разбирательства. Если почтовый ящик помещен на хранение для судебного разбирательства, нажмите кнопку **Отключить**, чтобы отменить хранение для судебного разбирательства. Если почтовый ящик помещен на хранение для судебного разбирательства, нажмите кнопку **Изменить сведения**, чтобы просмотреть и изменить следующие параметры хранения для судебного разбирательства:

- **Дата удержания**. Это поле только для чтения указывает дату и время, когда почтовый ящик был помещен на удержание по делу.
- **Поставить на удержание**: это поле только для чтения указывает пользователя, который поставил почтовый ящик на удержание для судебного разбирательства.
- **Примечание.** Используйте это поле, чтобы уведомить пользователя о удержании в судебном порядке, объяснить, почему почтовый ящик находится на удержании в судебном порядке, или предоставить пользователю дополнительные инструкции, такие как информирование пользователя о том, что удержание в судебном порядке не повлияет на его повседневное использование электронной почты.
- **URL-адрес**. Используйте это поле для предоставления URL-адреса веб-сайта, который предоставляет сведения или рекомендации по удержанию судебного разбирательства в почтовом ящике.

  > ⓘ **Примечание**
  >
  > Текст из этих полей отображается в почтовом ящике, только если пользователь использует Outlook 2010 или более поздней версии. Он отсутствует в Outlook в Интернете и других почтовых клиентах. Чтобы просмотреть текст из полей "Заметка" и "URL-адрес" в Outlook, щелкните вкладку **Файл** и на странице **Сведения**, в разделе **Настройки учетной записи**, вы увидите комментарий по поводу хранения для судебного разбирательства.

- **Архивация**. Если архивный почтовый ящик не существует для пользователя, эта функция отключена. Чтобы включить архивный почтовый ящик, щелкните **Включить**. Если у пользователя есть архивный почтовый ящик, отображаются его размер и статистика использования. Нажмите кнопку **Изменить сведения**, чтобы просмотреть и изменить следующие параметры архивного почтового ящика:
  - **Состояние**. Это поле только для чтения указывает, существует ли архивный почтовый ящик.
  - **База данных**. В этом поле только для чтения отображается имя базы данных почтового ящика, в котором размещается архивный почтовый ящик.

- **Имя**. Введите имя архивного почтового ящика в этом поле. Это имя отображается под списком папок в Outlook или Outlook в Интернете.
- **Использование квоты**. В этой области, доступной только для чтения, отображается общий размер архивного почтового ящика и процент использованной общей квоты архивного почтового ящика.
- **Значение квоты (ГБ):** в этом поле отображается общий размер архивного почтового ящика. Чтобы изменить размер, введите в этом поле новое значение или выберите его в раскрывающемся списке.
- **Предупреждение о проблеме в (ГБ):** в этом поле отображается максимальный объем хранилища для архивного почтового ящика, прежде чем пользователю будет выдано предупреждение. Если размер архивного почтового ящика достигает указанного значения или превышает его, Exchange отправляет пользователю предупреждающее сообщение. Чтобы изменить это ограничение, введите новое значение в поле или выберите значение из раскрывающегося списка.

- **Параметры доставки**. Используйте параметры доставки, чтобы пересылать сообщения электронной почты, отправленные пользователю, другому получателю и задать максимальное число получателей, которым пользователь может отправить сообщение. Нажмите кнопку **Изменить сведения**, чтобы открыть и изменить параметры.
  - **Адрес пересылки**. Установите флажок **Включить пересылку** и нажмите кнопку **Обзор** , чтобы отобразить страницу **Выбор почтового пользователя и почтового ящика** . Эта страница используется, чтобы выбрать получателя, которому нужно переадресовывать все сообщения электронной почты, отправляемые в этот почтовый ящик. Сообщения будут доставляться в связанный почтовый ящик и на адрес переадресации.
  - **Ограничение получателей**. Этот параметр определяет максимальное число получателей, в которые пользователь может отправить сообщение. Установите флажок **Максимальное количество получателей**, чтобы ограничить число получателей в полях "Кому:", "Копия:" и "СК:" в сообщениях электронной почты, а затем укажите максимальное количество получателей.

    > ⓘ **Примечание**
    >
    > В локальных организациях Exchange количество получателей не ограничено. В организациях Exchange Online можно указать не более

500 получателей.

- **Ограничения размера сообщений**. Эти параметры определяют размер сообщений, которые пользователь может отправлять и получать. Нажмите кнопку **Изменить сведения**, чтобы открыть и изменить параметры.

  - **Отправленные сообщения**. Чтобы указать максимальный размер сообщений, отправленных этим пользователем, установите флажок **Максимальный размер сообщения (КБ)** и введите в поле значение. Размер сообщений должен находиться в диапазоне от 0 до 2 097 151 КБ. Если размер отправляемого пользователем сообщения превышает указанный размер, оно будет возвращено отправителю с соответствующим сообщением об ошибке.

  - **Полученные сообщения**. Чтобы указать максимальный размер сообщений, полученных этим пользователем, установите флажок **Максимальный размер сообщения (КБ)** и введите значение в поле . Размер сообщений должен находиться в диапазоне от 0 до 2 097 151 КБ. Если пользователь получает сообщение, размер которого превышает установленное значение, это сообщение будет возвращено отправителю с описательным сообщением об ошибке.

- **Ограничения доставки сообщений**. Эти параметры определяют, кто может отправлять сообщения электронной почты этому пользователю. Нажмите кнопку **Изменить сведения**, чтобы открыть и изменить параметры.

  - **Принять сообщения из**: используйте этот раздел, чтобы указать, кто может отправлять сообщения этому пользователю.

  - **Все отправители**. Выберите этот параметр, чтобы указать, что пользователь может принимать сообщения от всех отправителей. Сюда относятся отправители из вашей организации Exchange и внешние отправители. Этот вариант выбран по умолчанию. Этот параметр включает внешних пользователей, только если снят флажок **Требовать проверку подлинности всех отправителей**. Если этот флажок установлен, сообщения от внешних пользователей будут отклоняться.

  - **Только отправители в следующем списке**. Выберите этот параметр, чтобы указать, что пользователь может принимать сообщения только от указанного набора отправителей в организации Exchange. Нажмите кнопку **Добавить**, чтобы открыть страницу **Выбор получателей** со списком всех получателей в вашей организации Exchange. Выберите нужных

получателей, добавьте их в список и нажмите **ОК**. Чтобы найти конкретного получателя, введите его имя в поле поиска и нажмите **Поиск**.

- **Требовать проверку подлинности всех отправителей**. Выберите этот параметр, чтобы запретить анонимным пользователям отправлять сообщения пользователю.
- **Отклонить сообщения из**: используйте этот раздел, чтобы запретить пользователям отправлять сообщения этому пользователю.
- **Нет отправителей**. Выберите этот параметр, чтобы указать, что почтовый ящик не будет отклонять сообщения от отправителей в организации Exchange. Этот вариант выбран по умолчанию.
- **Отправители в следующем списке**. Выберите этот параметр, чтобы указать, что почтовый ящик будет отклонять сообщения от указанного набора отправителей в организации Exchange. Нажмите **Добавить**, чтобы открыть страницу **Выбор получателей** со списком всех получателей в вашей организации Exchange. Выберите нужных получателей, добавьте их в список, а затем нажмите **ОК**. Чтобы найти определенного получателя, введите его имя в поле поиска и нажмите **Поиск**.

Участник

Используйте раздел **Member Of** для просмотра списка групп рассылки или групп безопасности, к которым принадлежит этот пользователь. На этой странице нельзя изменять сведения о членстве. Обратите внимание, что пользователь может соответствовать критериям для одной или нескольких динамических групп рассылки в вашей организации. Однако динамические группы рассылки не отображаются на этой странице, так как их членство вычисляется при каждом использовании.

Подсказка

Используйте раздел **Подсказка** для добавления подсказок, предупреждающих пользователей о возможных проблемах при отправке сообщения данному получателю. Подсказка — это текст, который отображается на панели информации при добавлении получателя в строки "Кому", "Копия" и "СК" нового сообщения электронной почты.

> ⓘ **Примечание**

Подсказки могут содержать HTML-теги, но сценарии не допускаются. Длина пользовательской подсказки не должна превышать 175 отображаемых символов. HTML-теги при этом не учитываются.

Делегация почтовых ящиков

Используйте раздел **Делегирование почтовых ящиков** , чтобы назначить разрешения другим пользователям (также *называемым делегатам*), чтобы разрешить им входить в почтовый ящик пользователя или отправлять сообщения от имени пользователя. Можно назначать следующие разрешения:

- **Отправить как**. Это разрешение позволяет пользователям, кроме владельца почтового ящика, использовать почтовый ящик для отправки сообщений. После назначения этого разрешения делегату все сообщения, которые делегат отправляет через этот почтовый ящик, будут отображаться так, как если бы их отправил владелец почтового ящика. Тем не менее это разрешение не позволяет делегату входить в почтовый ящик этого пользователя.

- **Отправить от имени:** это разрешение также позволяет делегату использовать этот почтовый ящик для отправки сообщений. Тем не менее, когда это разрешение назначается делегату, адрес **От:** в сообщениях, отправляемых делегатом, будет указывать, что сообщение отправлено именно делегатом от лица владельца почтового ящика.

- **Полный доступ**. Это разрешение позволяет делегату входить в почтовый ящик пользователя и просматривать содержимое почтового ящика. Однако после назначения этого разрешения делегату он не сможет отправлять сообщения из почтового ящика. Чтобы разрешить делегату отправлять сообщения электронной почты из почтового ящика пользователя, по-прежнему необходимо назначить делегату разрешение Отправить как или Отправить от имени.

Для назначения разрешений представителям нажмите кнопку **Добавить** под соответствующим разрешением, чтобы открыть страницу **Выбрать получателя**, в которой отображается список всех получателей в организации Exchange, которым можно назначить разрешение. Выберите получателей, которым нужно назначить разрешения делегата, добавьте их в список и нажмите кнопку **ОК**. Чтобы найти определенного получателя, введите его имя в поле поиска и нажмите **Поиск**.

Изменение свойств связанных почтовых ящиков с помощью командной консоли Exchange

Используйте командлеты **Get-Mailbox** и **Set-Mailbox** для просмотра и изменения свойств связанных почтовых ящиков. Одним из преимуществ использования командной консоли Exchange является возможность изменять свойства для нескольких связанных почтовых ящиков. Сведения о том, какие параметры соответствуют свойствам почтового ящика, см. в следующих разделах:

- Get-Mailbox
- Set-Mailbox

Ниже приведены примеры изменения свойств связанного почтового ящика с помощью командной консоли Exchange.

В этом примере с помощью команды **Get-Mailbox** ведется поиск всех связанных почтовых ящиков в организации.

PowerShell

```
Get-Mailbox -ResultSize unlimited -Filter "RecipientTypeDetails -eq
'LinkedMailbox'"
```

В этом примере с помощью команды **Set-Mailbox** ограничивается количество получателей в полях "Кому", "Копия" и "СК" сообщений электронной почты до 500. Это ограничение применяется ко всем связанным почтовым ящикам в организации.

PowerShell

```
Get-Mailbox -ResultSize unlimited -Filter "RecipientTypeDetails -eq
'LinkedMailbox'" | Set-Mailbox -RecipientLimits 500
```

В этом примере изменяется главная учетная запись в лесу учетных записей fabrikam.com, сопоставленная со связанным почтовым ящиком в лесу Exchange.

PowerShell

```
Set-Mailbox -Identity "Ayla Kol" -LinkedDomainController DC1.fabrikam.com -
LinkedMasterAccount "fabrikam\robinw" -LinkedCredential:(Get-Credential
fabrikam\administrator)
```

Как проверить, все ли получилось?

Чтобы убедиться в том, что свойства почтового ящика успешно изменены, выполните следующие действия:

- В центре администрирования Exchange выберите почтовый ящик и нажмите кнопку **Изменить**, чтобы открыть измененное свойство или компонент. В зависимости от измененного свойства оно может отображаться в области "Сведения" выбранного почтового ящика.

- В командной консоли Exchange для проверки изменений используется командлет **Get-Mailbox**. С помощью командной консоли Exchange можно просмотреть несколько свойств нескольких почтовых ящиков. Выполните следующую команду, чтобы проверить, изменилось ли максимальное количество получателей в примере выше.

  PowerShell

  ```
  Get-Mailbox -ResultSize unlimited -Filter "RecipientTypeDetails -eq
  'LinkedMailbox'" | Format-List Name,RecipientLimits
  ```

  В примере выше, где изменялась связанная учетная запись, выполните следующую команду, чтобы проверить, изменилось ли значение.

  PowerShell

  ```
  Get-Mailbox "Ayla Kol" | Format-List LinkedMasterAccount
  ```

Управление группами рассылки

Статья • 04.04.2023

Используйте Центр администрирования Exchange (EAC) или командную консоль Exchange, чтобы создать новую группу рассылки в организации Exchange или включить существующую группу в Active Directory по почте.

Существует два типа групп, которые можно использовать для рассылки сообщений:

- *Универсальные группы рассылки с включенной поддержкой почты* (также известные как *группы рассылки*) можно использовать только для распространения сообщений.
- *Универсальные группы безопасности с поддержкой почты* (также называемые *группами безопасности*) можно использовать для распространения сообщений, а также для предоставления разрешений на доступ к ресурсам в Active Directory. Дополнительные сведения см. в статье Управление группами безопасности с поддержкой почты в Exchange Server.

Необходимо учитывать различия в терминологии для службы каталогов Active Directory и Exchange. В службе каталогов Active Directory группа рассылки означает любую группу, для которой не создан контекст безопасности, независимо от того, была ли включена поддержка почты для этой группы или нет. В противоположность этому, в Exchange все группы с включенной поддержкой почты считаются группами рассылки независимо от того, был ли создан для них контекст безопасности или нет.

> ⓘ **Примечание**
>
> Можно создавать только универсальные группы рассылки или включать поддержку почты только для этих групп. Чтобы преобразовать локальную или глобальную группу домена в универсальную группу, можно использовать командлет **Set-Group** с помощью командной консоли Exchange. В организации могут существовать группы с включенной поддержкой почты, перемещенные с серверов Exchange предыдущих версий и не являющиеся универсальными группами. Для управления этими группами можно использовать EAC или командную консоль Exchange.

Что нужно знать перед началом работы

- Осталось времени до завершения: от 2 до 5 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Группы рассылки" в разделе Разрешения получателей .
- Если для организации настроена политика именования групп, она применяется только к группам, созданным пользователями. Если вы или другие администраторы используют EAC для создания групп рассылки, политика именования групп игнорируется и не применяется к имени группы. Однако если для создания или переименования группы рассылки используется командная консоль Exchange, политика применяется, если для переопределения политики именования групп не используется параметр *IgnoreNamingPolicy* . Дополнительные сведения см. в разделе:
  - Создание политики именования групп рассылки
  - Переопределение политики именования групп рассылки
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Создание группы рассылки

Как использовать Центр администрирования Exchange для создания группы рассылки

1. В Центре администрирования Exchange (EAC) выберите **Получатели**>**Группы**.
2. Щелкните **Значок "Создать**+>**Группа рассылки**.
3. На странице **Создание группы рассылки** заполните следующие поля:
   - * **Отображаемое имя**: используйте это поле для ввода отображаемого имени. Это имя отображается в адресной книге вашей организации в строке Кому: при отправке электронной почты в эту группу, а также в

списке Группы в EAC. Отображаемое имя обязательно и должно быть понятным, чтобы пользователи могли понять его назначение. Это имя также должно быть уникальным в лесу.

- * **Псевдоним**. Используйте это поле, чтобы ввести имя псевдонима для группы. Псевдоним не может превышать 64 символов и должен быть уникальным в лесу. Когда пользователь вводит псевдоним в строку "Кому" электронного сообщения, он сопоставляется с кратким именем группы.

- **Описание**. Используйте это поле, чтобы описать группу, чтобы пользователи знали, каково назначение группы. Это описание отображается в адресной книге.

- **Подразделение**. Вы можете выбрать подразделение, отличное от стандартного (который является областью получателя). Если область получателей установлена на уровне леса, будет установлено значение по умолчанию для контейнера "Пользователи" домена Active Directory, в котором находится компьютер с запущенным центром администрирования Exchange. Если область получателей настроена на определенный домен, то контейнер пользователей в этом домене выбирается по умолчанию. Если в качестве области получателей задано определенное подразделение организации, то оно выбирается по умолчанию.

  Нажмите кнопку **Обзор**, чтобы выбрать другое подразделение. В этом диалоговом окне отображаются все подразделения в лесу, которые находятся внутри определенной области. Выберите нужное подразделение и нажмите кнопку **ОК**.

- * **Владельцы**. По умолчанию владелец группы создает группу. Для каждой группы должен существовать по крайней мере один владелец. Вы можете добавить владельцев, щелкнув ✚

- **Участники**. Используйте этот раздел, чтобы добавить участников и указать, требуется ли утверждение для присоединения пользователей к группе или выхода из нее.

  Владельцы группы не обязательно должны быть ее членами. Используйте флажок **Добавлять владельцев группы как участников**, чтобы добавить или удалить владельцев в качестве участников.

Чтобы добавить участников в группу, щелкните **Добавить**➕ После добавления участников нажмите кнопку **OK**, чтобы вернуться на страницу **Создать группу рассылки**.

В разделе **Укажите, требуется ли подтверждение владельца для присоединения к группе** укажите, требуется ли подтверждение для пользователей, желающих присоединиться к группе. Выберите один из приведенных ниже параметров.

- **Открыть. Любой пользователь может присоединиться к этой группе без утверждения ее владельцами**. Это параметр по умолчанию.
- **Закрыто: участники могут добавляться только владельцами группы. Все запросы на присоединение будут отклонены автоматически**

- **Утверждение владельца. Все запросы вручную утверждаются или отклоняются владельцами группы**. Если выбрать этот параметр, владелец группы или владельцы получат сообщение электронной почты с просьбой утвердить присоединение к группе.

  В разделе **Выберите, будет ли эта группа открыта для выхода** укажите, требуется ли для пользователей утверждение владельца группы, чтобы ее покинуть. Выберите один из приведенных ниже параметров.

- **Открыть. Любой пользователь может покинуть эту группу без утверждения ее владельцами**. Это параметр по умолчанию.
- **Закрытая группа: членов группы удаляют только владельцы группы. Все запросы на выход из группы будут автоматически отклонены.**

4. По завершении нажмите кнопку **Сохранить**, чтобы создать группу рассылки.

> ⓘ **Примечание**
>
> По умолчанию новые группы рассылки требуют проверки подлинности всех отправителей. Это запрещает внешним отправителям отправлять сообщения в группы рассылки. Чтобы настроить группу рассылки на прием сообщений от всех отправителей, необходимо изменить параметры ограничения доставки сообщений для данной группы рассылки.

Создание группы рассылки с помощью командной консоли Exchange

В этом примере создается группа рассылки с псевдонимом **itadmin** и именем **ИТ-администраторы**. Группа рассылки создается в подразделении по умолчанию, и любой пользователь может присоединиться к этой группе без утверждения владельцев.

PowerShell

```
New-DistributionGroup -Name "IT Administrators" -Alias itadmin -
MemberJoinRestriction open
```

Дополнительные сведения об использовании командной консоли Exchange для создания групп рассылки см. в разделе New-DistributionGroup.

Как проверить, все ли получилось?

Чтобы убедиться, что группа рассылки успешно создана, выполните одно из следующих действий:

- В Центре администрирования Exchange (EAC) выберите **Получатели**>**Группы**. Новая группа рассылки отобразится в списке групп. В разделе **Тип группы** указан тип **Группа рассылки**.
- В командной консоли Exchange выполните следующую команду, чтобы отобразить сведения о новой группе рассылки.

  PowerShell

  ```
  Get-DistributionGroup <Name> | Format-List
  Name,RecipientTypeDetails,PrimarySmtpAddress
  ```

Изменение свойств группы рассылки

Использование Центра администрирования Exchange для изменения свойств группы рассылки

1. В Центре администрирования Exchange (EAC) выберите **Получатели**>**Группы**.
2. В списке групп щелкните группу рассылки, которую вы хотите просмотреть или изменить, а затем щелкните **Изменить**.
3. На странице свойств группы щелкните один из следующих разделов, чтобы просмотреть или изменить свойства.

- Общие
- Владение.
- Членство.
- Утверждение членства.
- Управление доставкой.
- Утверждение сообщений.
- Параметры электронной почты.
- Подсказка
- Делегирование группы

Общие

Этот раздел используется для просмотра или изменения базовых сведений о группе.

- * **Отображаемое имя**: это имя отображается в адресной книге, в строке Кому: при отправке сообщения электронной почты в эту группу, а также в списке Группы. Отображаемое имя обязательно и должно быть понятным, чтобы пользователи могли понять его назначение. Кроме того, оно должно быть уникальным в пределах домена.

  Если используется политика именования групп, отображаемое имя должно соответствовать заданному в ней формату именования.

- * **Псевдоним**: это часть адреса электронной почты, которая отображается слева от символа (@). Если изменить псевдоним, основной адрес SMTP группы также изменится и будет содержать новый псевдоним. Кроме того, адрес электронной почты с предыдущим псевдонимом сохранится в качестве прокси-адреса группы.

- **Описание**. Используйте это поле, чтобы описать группу, чтобы пользователи знали, каково назначение группы. Это описание отображается в адресной книге на панели подробностей в центре администрирования Exchange.

- **Скрыть эту группу из списков адресов**. Установите этот флажок, если вы не хотите, чтобы пользователи видели эту группу в адресной книге. Чтобы отправить электронное сообщение этой группе, отправитель должен ввести

псевдоним группы или адрес электронной почты в строки "Кому" или "Копия"
.

> **Совет**
>
> Рекомендуется скрывать группы безопасности, так как они обычно используются для назначения разрешений членам группы, а не для отправки электронной почты.

- **Подразделение**. В этом поле только для чтения отображается подразделение, содержащее группу рассылки. Необходимо использовать оснастку "Пользователи и компьютеры Active Directory", чтобы переместить группу в другое подразделение.

Собственность

Этот раздел используется для назначения владельцев группы. Владелец группы может добавлять новых членов, утверждать или отклонять запросы о присоединении и выходе из группы, а также утверждать и отклонять отдельные сообщения, рассылаемые группе. По умолчанию владельцем группы становится пользователь, создавший ее. Для каждой группы должен существовать по крайней мере один владелец.

Вы можете добавить владельцев, щелкнув ✚ Вы можете удалить владельца, выбрав владельца и нажав кнопку **Удалить**━

Участие

В этом разделе добавляются и удаляются члены. Владельцы группы не обязательно должны быть ее членами. В разделе **Участники** можно добавить участников, щелкнув ✚ Вы можете удалить участника, выбрав пользователя в списке участников, а затем щелкнув ━

Утверждение членства

В этом разделе можно указать, требуется ли утверждение для пользователей, желающих присоединиться к группе или покинуть ее.

- **Выберите, требуется ли утверждение владельца для присоединения к группе**. Выберите один из следующих параметров:

- **Открытая группа. К ней может присоединиться любой пользователь. Утверждение владельцев группы не требуется.**
- **Закрыто: участники могут добавляться только владельцами группы. Все запросы на присоединение будут отклонены автоматически**
- **Утверждение владельца. Все запросы утверждаются или отклоняются владельцами группы**. Если выбран этот параметр, владелец группы или владельцы получат электронное письмо с просьбой утвердить присоединение к группе.

- **Выберите, открыта ли группа для выхода**: выберите один из следующих параметров:
  - **Открыто: любой пользователь может покинуть эту группу без утверждения ее владельцами.**
  - **Закрытая группа: членов группы удаляют только владельцы группы. Все запросы на выход из группы будут автоматически отклонены.**

Управление доставкой

В этом разделе можно определить, кто может отправлять почту в эту группу.

- **Только отправители внутри моей организации**. Выберите этот параметр, чтобы разрешить только отправителям в вашей организации отправлять сообщения в группу. Это означает, что будут отклоняться сообщения электронной почты, отправленные в эту группу от пользователей за пределами организации. Это параметр по умолчанию.
- **Отправители внутри и за пределами моей организации**. Выберите этот параметр, чтобы разрешить всем пользователям отправлять сообщения в группу.

  Можно дополнительно ограничить круг пользователей, имеющих право отправлять сообщения в эту группу, указав только определенных отправителей. Щелкните **Добавить**➕ а затем выберите одного или нескольких получателей. Если в этот список будут добавлены отправители, они станут единственными пользователями, которые будут иметь право на отправку сообщений в эту группу. Сообщения электронной почты, отправленные кем-либо, не содержащимся в этом списке, будут отклоняться.

  Чтобы удалить пользователя или группу из списка, выберите их в списке и нажмите кнопку **Удалить**➖.

> ⓘ **Важно!**
>
> Если в группу могут отправлять сообщения только отправители внутри организации, то сообщения, отправленные почтовыми контактами, будут отклоняться, даже если эти контакты включены в рассматриваемый список.

Утверждение сообщений

В этом разделе можно установить параметры изменения группы. Модераторы утверждают или отклоняют отправленные в группу сообщения перед их доставкой членам группы.

- **Сообщения, отправленные в эту группу, должны быть утверждены модератором**. Этот флажок не установлен по умолчанию. Если установить этот флажок, входящие сообщения перед доставкой будут проверяться модераторами группы. Модераторы группы могут утвердить или отклонить входящее сообщение.

- **Модераторы групп**. Чтобы добавить модераторов групп, нажмите кнопку **Добавить**➕ Чтобы удалить модератора, выберите его и нажмите кнопку **Удалить**➖. Если вы выбрали "Сообщения, отправленные в эту группу, должны быть утверждены модератором" и не выбираете модератора, сообщения в группу отправляются владельцам групп для утверждения.

- **Отправители, которым не требуется утверждение сообщений**. Чтобы добавить людей или группы, которые могут обойти модерацию для этой группы, щелкните **Добавить**➕ Чтобы удалить пользователя или группу, выберите элемент и нажмите кнопку **Удалить**➖.

- **Выбор уведомлений о модерации**. Используйте этот раздел, чтобы задать способ уведомления пользователей об утверждении сообщений.

    - **Уведомление всех отправителей о том, что их сообщения не утверждены**. Это параметр по умолчанию. Все отправители, которые находятся внутри и вне организации, будут уведомляться в том случае, если их сообщения не были утверждены.

    - **Уведомлять отправителей в вашей организации о том, что их сообщения не утверждены**. При выборе этого параметра только пользователи или группы в вашей организации получают уведомления, если сообщение, отправленное ими группе, не утверждено модератором.

- **Не уведомляйте никого о том, что сообщение не утверждено**. При выборе этого параметра уведомления не отправляются отправителям сообщений, сообщения которых не утверждены модераторами групп.

Параметры электронной почты

Этот раздел используется для просмотра и изменения адресов электронной почты, связанных с группой. Он включает основные адреса SMTP группы и любые связанные прокси-адреса. Основной адрес SMTP (также известный как *адрес ответа*) отображается жирным шрифтом в списке адресов и прописными буквами **SMTP** в столбце **Тип**.

- **Добавить: щелкните**➕ чтобы добавить новый адрес электронной почты для этого почтового ящика. Выберите один из следующих типов адресов:
  - **SMTP**. Это тип адреса по умолчанию. Нажмите эту кнопку, а затем введите новый адрес SMTP в поле ***Адрес электронной почты**.
  - **Пользовательский тип адреса**. Нажмите эту кнопку и введите один из поддерживаемых типов адресов электронной почты, **отличных от** SMTP, в поле *Email адрес.

    > ⓘ **Примечание**
    >
    > В Exchange не выполняется проверка правильности формата настраиваемых адресов (за исключением адресов X.400). Чтобы добавить настраиваемый адрес (например, факс или X.400), нажмите эту кнопку и используйте соответствующее диалоговое окно.

- **Изменить**. Чтобы изменить адрес электронной почты, связанный с группой, выберите его в списке и нажмите кнопку **Изменить**.✏️
- **Удалить**. Чтобы удалить адрес электронной почты, связанный с группой, выберите его в списке и нажмите кнопку **Удалить**➖.
- **Автоматически обновлять адреса электронной почты на основе политики адресов электронной почты, которая применяется к этому получателю**. Установите этот флажок, чтобы адреса электронной почты получателей автоматически обновлялись на основе изменений политики адресов электронной почты организации. По умолчанию этот флажок установлен.

Подсказка

Используйте этот раздел для добавления подсказок, предупреждающих пользователей о возможных проблемах при отправке сообщения определенной группе. Подсказка — это текст, который отображается на панели информации при добавлении этой группы в строки "Кому", "Копия" и "СК" нового сообщения электронной почты. Например, можно добавить подсказку для больших аудиторий, чтобы предупредить возможных отправителей о том, что сообщение отправится большому числу получателей.

> ⓘ **Примечание**
>
> Подсказки могут содержать HTML-теги, но сценарии не допускаются. Длина пользовательской подсказки не должна превышать 175 отображаемых символов. HTML-теги при этом не учитываются.

Делегирование группы

Этот раздел используется для назначения разрешений пользователю (известному как *представитель*), чтобы разрешить ему отправлять сообщения в качестве группы или от ее имени. Можно назначать следующие разрешения:

- **Отправить как**. Это разрешение позволяет делегату отправлять сообщения в качестве группы. После того, как разрешение будет назначено, представитель сможет добавить группу в строку **От**, чтобы указать, что сообщение было отправлено группой.
- **Отправить от имени:** это разрешение также позволяет делегату отправлять сообщения от имени группы. После назначения этого разрешения делегат может добавить группу в строку **От**. Это сообщение отобразится как отправленное группой, и в нем будет сообщаться, что оно было отправлено представителем от имени группы.

Для назначения разрешений представителям нажмите кнопку **Добавить** под соответствующим разрешением, чтобы открыть страницу **Выбрать получателя**, в которой отображается список всех получателей в организации Exchange, которым можно назначить разрешение. Выберите нужных получателей, добавьте их в список и нажмите кнопку **ОК**. Чтобы найти конкретного получателя, введите его имя в поле поиска и нажмите **Поиск**.

Изменение свойств группы рассылки с помощью командной консоли Exchange

Используйте командлеты **Get-DistributionGroup** и **Set-DistributionGroup** для просмотра и изменения свойств группы рассылки. Преимущества использования командной консоли Exchange — это возможность изменять свойства, недоступные в EAC, и изменять свойства для нескольких групп. Сведения о том, какие параметры соответствуют свойствам групп рассылки, см. в следующих разделах:

- Получить DistributionGroup
- Настроить DistributionGroup

Ниже приведены некоторые примеры использования командной консоли Exchange для изменения свойств группы рассылки.

В этом примере основной SMTP-адрес (также называемый адресом ответа) для группы рассылки Seattle Employees изменяется с employees@contoso.com на sea.employees@contoso.com. Кроме того, предыдущий адрес ответа сохраняется в качестве прокси-адреса.

PowerShell

```
Set-DistributionGroup "Seattle Employees" -EmailAddresses
SMTP:sea.employees@contoso.com,smtp:employees@contoso.com
```

В этом примере ограничивается максимальный размер сообщений, которые могут быть отправлены во все группы рассылки в организации, до 10 мегабайт (МБ).

PowerShell

```
Get-DistributionGroup -ResultSize unlimited -Filter "RecipientTypeDetails -
eq 'MailUniversalDistributionGroup'" | Set-DistributionGroup -MaxReceiveSize
10MB
```

В этом примере разрешается управление для группы рассылки Customer Support, а модератором назначается Amy. Кроме того, в соответствии с настройками этой группы рассылки отправители сообщений из организации будут получать уведомления при отсутствии утверждения для этих сообщений.

PowerShell

```
Set-DistributionGroup -Identity "Customer Support" -ModeratedBy "Amy" -
ModerationEnabled $true -SendModerationNotifications 'Internal'
```

В этом примере изменяется пользовательская группа рассылки Dog Lovers, чтобы диспетчер группы утверждал запросы пользователей на присоединение к группе.

Кроме того, если устанавливается параметр *BypassSecurityGroupManagerCheck*, диспетчер группы не будет уведомляться об изменении параметров группы рассылки.

PowerShell

```
Set-DistributionGroup -Identity "Dog Lovers" -MemberJoinRestriction
'ApprovalRequired' -BypassSecurityGroupManagerCheck
```

Как проверить, все ли получилось?

Чтобы убедиться, что свойства группы рассылки успешно изменены, выполните следующие действия:

- В EAC выберите группу и нажмите кнопку **Изменить** чтобы просмотреть измененное свойство или функцию. В зависимости от свойства, которое было изменено, оно может отображаться в панели подробностей выбранной группы.
- В командной консоли Exchange используйте командлет **Get-DistributionGroup** для проверки изменений. Одним из преимуществ использования командной консоли Exchange является возможность просмотра нескольких свойств для нескольких групп. В примере выше, где изменялся предел для получателей, выполните следующую команду, чтобы проверить, изменилось ли значение.

  PowerShell

  ```
  Get-Mailbox -ResultSize unlimited -Filter "RecipientTypeDetails -eq
  'UserMailbox'" | Format-List Name,RecipientLimits
  ```

  Чтобы увидеть указанный выше пример, в котором изменяются пределы сообщения, выполните эту команду.

  PowerShell

  ```
  Get-Mailbox -OrganizationalUnit "Marketing" | Format-List
  Name,IssueWarningQuota,ProhibitSendQuota,ProhibitSendReceiveQuota,UseDa
  tabaseQuotaDefaults
  ```

Управление группами безопасности с поддержкой почты в Exchange Server

Статья • 04.04.2023

Группы безопасности с поддержкой почты можно использовать для распространения сообщений, а также предоставления разрешений на доступ к ресурсам в Exchange и Active Directory. Вы можете создавать, изменять и удалять группы безопасности с поддержкой почты в Центре администрирования Exchange (EAC) или в командной консоли Exchange. Дополнительные сведения о группах безопасности с поддержкой почты см. в разделе Получатели.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Группы рассылки" в разделе Разрешения получателей .
- Дополнительные сведения о доступе и использовании Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server.
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Если вы добавляете пользователей в группу безопасности с поддержкой электронной почты или удаляете их из нее, пользователям необходимо выйти, а затем войти еще раз, чтобы изменения разрешений вступили в силу.
- Что касается групп безопасности с поддержкой электронной почты, пользователи не могут самостоятельно добавляться в группу или удаляться из нее, равно как и отправлять владельцам группы соответствующие запросы. Владельцу группы необходимо вручную добавлять членов в группу безопасности с поддержкой электронной почты и удалять их из нее.
- Если группа безопасности с поддержкой почты содержит участников, которые не поддерживают почту, при отправке сообщения группе возвращается отчет о недоставке (также известном как сообщение о недоставке или отказе от почты). Чтобы предотвратить NDR, перед отправкой сообщения можно

развернуть участников группы в поле **Кому** (будут отображаться только члены группы с поддержкой почты).

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**.

Создание групп безопасности с поддержкой электронной почты

- При создании групп в Центре администрирования Exchange значение свойства **Отображаемое имя** используется в качестве значения невидимого свойства **Name** (уникального идентификатора объекта группы в лесу). Так как максимальная длина для значения **Name** составляет 64 символа, значение свойства **Отображаемое имя** также не должно содержать более 64 символов при создании групп в Центре администрирования Exchange.

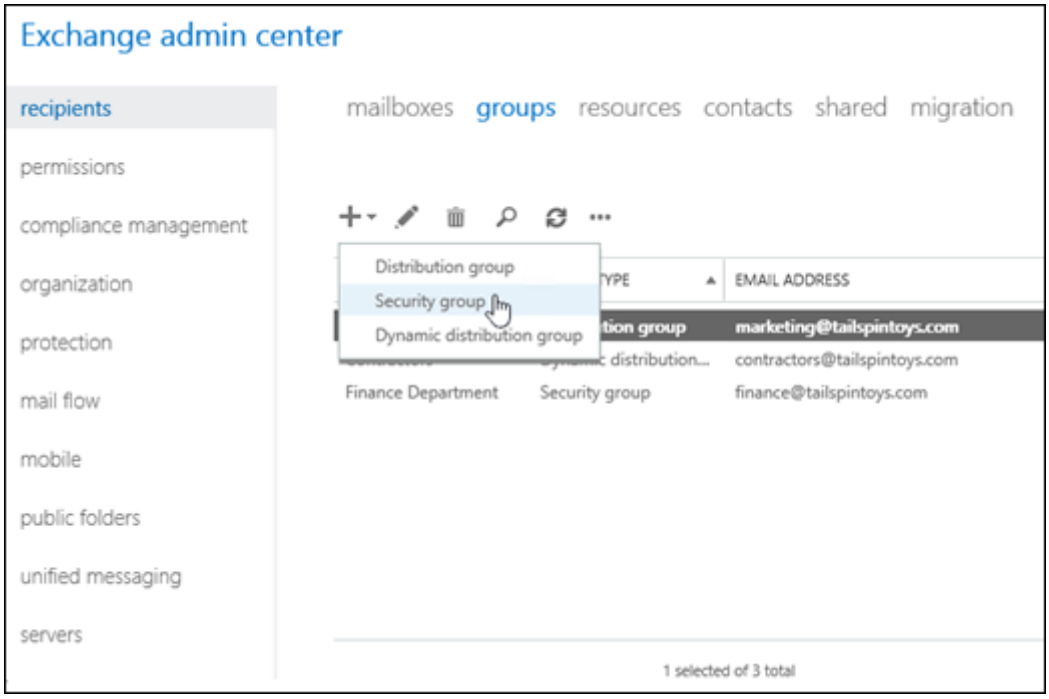
- При создании групп в командной консоли Exchange параметр *Name* является обязательным, значение должно быть уникальным, а максимальная длина значения — 64 символа. Параметр *DisplayName* необязателен (значение *Name* используется, если вы его не используете), значение не обязательно должно быть уникальным, а максимальная длина значения — 256 символов.

- Когда вы создаете группы в Центре администрирования Exchange, они автоматически настраиваются на принятие сообщений только от внутренних отправителей, то есть от таких, которые прошли проверку подлинности. При создании групп в командной консоли Exchange можно использовать параметр *RequireSenderAuthenticationEnabled со значением* `$false`, чтобы группа могла принимать сообщения от прошедших проверку подлинности отправителей (внутренних и внешних) с проверкой подлинности. После создания группы этот параметр можно изменить в Центре администрирования Exchange или командной консоли Exchange.

Создание группы безопасности с поддержкой электронной почты при помощи Центра

администрирования Exchange

1. В EAC перейдите в раздел **Группы получателей**>.
2. Щелкните **Новый**+ Затем в появившемся раскрывающемся списке выберите **Группа безопасности** .



3. На открывшейся странице **Новая группа безопасности** настройте указанные ниже параметры (значения, отмеченные символом *, обязательны).

   - * **Отображаемое имя**: это значение должно помочь пользователям сразу распознать, для чего используется группа. Это имя отображается в глобальном списке адресов, в строке "Кому" отправляемого группе сообщения, а также в списке **Группы** Центра администрирования Exchange. Значение в Центре администрирования Exchange должно содержать не более 64 символов и быть уникальным.

     > ⓘ **Примечание**
     >
     > Если применяется политика именования групп, необходимо соблюдать ограничения именования, принятые для организации. Дополнительные сведения см. в статье **Create a Distribution Group Naming Policy**. Если требуется переопределить политику именования групп в организации, см. статью **Override a Distribution Group Naming Policy**.

- * **Псевдоним**: это значение используется для создания основного адреса электронной *почты (<домена псевдонима>@ <).>* Это значение может содержать буквы, цифры и символы !, #, $, %, &, ', *, +, -, /, =, ?, ^, _, ', {, |, } и ~. Точки (.) можно использовать, но каждая точка должна быть окружена другими допустимыми символами (например, help.desk). Символы Юникода от U+00A1 до U+00FF также разрешены, но сопоставляются с текстовыми символами US-ASCII на основном адресе электронной почты (например, U+00F6 (ö) изменен на oe). Псевдоним не может превышать 64 символов и должен быть уникальным в лесу. Когда пользователь вводит псевдоним в строке Кому: сообщения электронной почты, он разрешается в отображаемое имя группы.

- **Примечания**. Используйте это поле для описания назначения группы. Такое описание отображается в глобальном списке адресов и области сведений в Центре администрирования Exchange.

- **Подразделение**. Расположение по умолчанию в Active Directory зависит от настроенной области получателя:

    - Если область получателей определена лесом Active Directory, расположение по умолчанию — это контейнер пользователей в домене, к которому присоединен компьютер с Центром администрирования Exchange.

    - Если в качестве области получателей задан определенный домен, расположение по умолчанию — это контейнер пользователей в этом домене.

    - Если область получателей — это определенное подразделение, расположением по умолчанию будет это подразделение.

    Чтобы выбрать другое подразделение, нажмите кнопку **Обзор**. В открывшемся диалоговом окне **Выберите подразделение** показаны все доступные подразделения в лесу, входящие в указанную область получателей. Выберите необходимое подразделение и нажмите кнопку **ОК**.

- * **Владельцы**: по умолчанию владелец группы создает группу. Для каждой группы должен существовать по крайней мере один владелец. Владельцы групп могут следующее:

    - изменять свойства группы;

    - Изменять свойства группы.

- удалять группу;
- утверждать сообщения, отправленные группе (если включена функция модерирования).

Чтобы добавить владельцев, нажмите кнопку **+** В открывшемся диалоговом окне **Выберите владельцев** укажите одного или нескольких владельцев, а затем последовательно нажмите кнопки **Добавить** и **ОК**.

Чтобы удалить владельцев, выберите владельца в списке и нажмите кнопку **Удалить**—

- **Участники**

  Чтобы добавить участников в группу, щелкните **Добавить**+ В открывшемся диалоговом окне **Выбор членов** укажите одного или нескольких членов, а затем последовательно нажмите кнопки **Добавить** и **ОК**.

  Чтобы удалить участников, выберите участника в списке и нажмите кнопку **Удалить**—.

- **Добавление владельцев групп в качестве участников**. Если установлен этот флажок, вам не нужно вручную включать владельцев групп в список участников. Если вы не хотите, чтобы владельцы группы были ее членами, снимите этот флажок.

- **Требуется утверждение владельца**. Для групп безопасности с поддержкой почты запросы пользователей на присоединение к группе не отправляются владельцам групп, независимо от состояния этого флажка (установлен или не установлен). Владельцу группы необходимо вручную добавлять членов в группу безопасности с поддержкой электронной почты и удалять их из нее.

После завершения нажмите кнопку **Сохранить**.

Создание группы безопасности с поддержкой электронной почты при помощи командной консоли Exchange

Для создания группы безопасности с поддержкой электронной почты используйте указанный ниже синтаксис.

PowerShell

```
New-DistributionGroup -Type Security -Name <UniqueName> [-
IgnoreNamingPolicy] [-Alias <Alias>] [-DisplayName "<DisplayName>"] [-Notes
"<Description>"] [-OrganizationalUnit <OU>] [-ManagedBy "<owner1>","
<owner2>"...] [-Members "<member1>","<member2>"...] [-CopyOwnerToMember] [-
MemberJoinRestriction <Closed | ApprovalRequired>] [-
RequireSenderAuthenticationEnabled <$true | $false>]
```

В этом примере создается группа безопасности с указанными ниже параметрами.

- **Имя**: Диспетчеры файлового сервера. Это значение также используется для отображаемого имени, так как мы не используем параметр *DisplayName* . Если применяется политика именования групп, вы можете использовать параметр *IgnoreNamingPolicy* для ее переопределения.
- **Псевдоним**: fsadmin. Если бы мы не использовали параметр *Alias* , использовалось бы значение параметра *Name* с удаленными пробелами (FileServerManagers в этом примере).
- **Описание**: нет, так как мы не используем параметр *Notes* .
- **Подразделение**. Расположение по умолчанию, указанное в области получателя, так как мы не используем параметр *OrganizationalUnit* .
- **Владельцы**. Учетная запись пользователя, создающая группу, является единственным владельцем, так как мы не используем параметр *ManagedBy* .
- **Участники**: Бишамон Тамура и Валерия Барриос. Так как мы используем параметр *CopyOwnerToMember*, владелец группы является также ее членом.
- **Запросы пользователей на присоединение к группе**. Для групп безопасности с поддержкой почты запросы пользователей на присоединение к группе не отправляются владельцам групп, независимо от значения параметра *MemberJoinRestriction* (`ApprovalRequired` или `Closed`). Владельцу группы необходимо вручную добавлять членов в группу безопасности с поддержкой электронной почты и удалять их из нее.
- **Принимать сообщения от внешних отправителей**. Нет, так как мы не используем параметр *RequireSenderAuthenticationEnabled* , а значение по умолчанию — `$true`.

PowerShell

```
New-DistributionGroup -Type Security -Name "File Server Managers" -Alias
fsadmin -Members "Bishamon Tamura","Valeria Barrios" -CopyOwnerToMember
```

Подробные сведения о синтаксисе и параметрах см. в статье New-DistributionGroup.

Как проверить, все ли получилось?

Чтобы убедиться в успешном создании группы безопасности с поддержкой электронной почты, выполните одно из указанных ниже действий.

- В EAC перейдите в раздел **Группы получателей**>. Убедитесь, что группа присутствует в списке, а в качестве значения **Тип группы** указан вариант **Группа безопасности**.
- В командной консоли Exchange запустите указанную ниже команду и убедитесь, что группа присутствует в списке.

```
PowerShell

Get-DistributionGroup -Filter "RecipientType -eq
'MailUniversalSecurityGroup'"
```

- В командной консоли Exchange замените <*GroupIdentity*> идентификатором группы (например, именем, псевдонимом или адресом электронной почты) и выполните следующую команду, чтобы проверить значения свойств:

```
PowerShell

Get-DistributionGroup -Identity <GroupIdentity> | Format-List
```

Просмотр групп безопасности с поддержкой электронной почты и их изменение

- Когда вы изменяете группы в Центре администрирования Exchange, можете указать значение свойства **Отображаемое имя**, содержащее до 256 символов, которое не уникально. Это значение больше не влияет на значение невидимого свойства **Name** (уникального идентификатора для объекта группы в лесу). Невозможно изменить значение **Name** существующей группы в Центре администрирования Exchange.
- При изменении групп в командной консоли Exchange максимальная длина значения параметра *Name* по-прежнему составляет 64 символа, а значение должно быть уникальным. Максимальная длина значения параметра

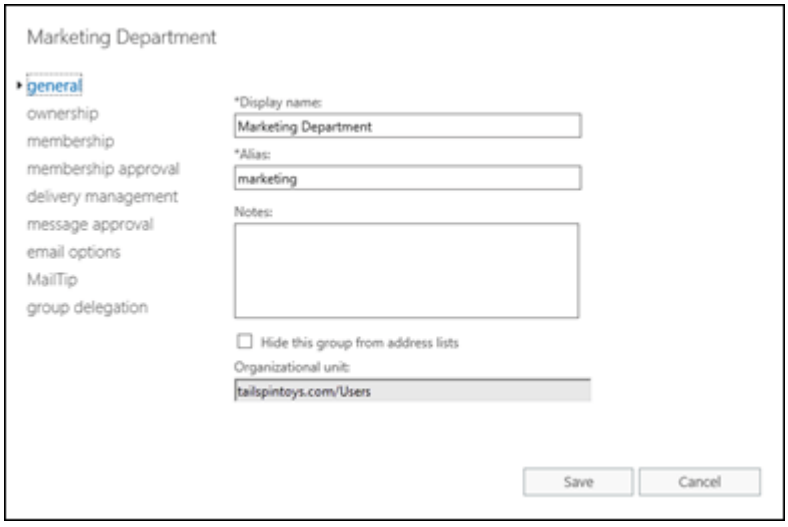
DisplayName по-прежнему составляет 256 символов, и значение не обязательно должно быть уникальным.

Просмотр или изменение группы безопасности с поддержкой электронной почты при помощи Центра администрирования Exchange

1. В EAC перейдите в раздел **Группы получателей**>.
2. В списке групп найдите группу безопасности с поддержкой электронной почты, которую требуется просмотреть или изменить. Варианты действий:
   - Прокрутите список групп.
   - Щелкните 🔎 введите часть имени, адреса электронной почты или псевдонима группы.
   - Щелкните **Значок Дополнительные параметры•••**>**Расширенный поиск** для поиска группы.
   - Щелкните заголовок столбца **Тип группы**, чтобы отсортировать группы по значению **Группа безопасности**.

     Когда вы найдете группу безопасности с поддержкой почты, которую вы хотите изменить, выберите ее и нажмите кнопку **Изменить**.✎
3. На открывшейся странице **Изменить группу безопасности** щелкните одну из указанных ниже вкладок, чтобы просмотреть или изменить параметры группы.
   - Общие.
   - Владение.
   - Членство.
   - Утверждение членства.
   - Управление доставкой.
   - Утверждение сообщений.
   - Параметры электронной почты.
   - Подсказка

- Делегирование группы.



По завершении нажмите кнопку **Сохранить** или **Отменить**.

Общие

Эта вкладка позволяет просмотреть или изменить основные сведения о группе.

- **Отображаемое имя**. Это значение должно помочь пользователям сразу распознать, для чего используется группа. Это имя отображается в глобальном списке адресов, в строке "Кому" отправляемого группе сообщения, а также в списке **Группы** Центра администрирования Exchange. Значение может содержать до 256 символов и не быть уникальным.

- **Псевдоним**. Это значение используется для создания основного адреса электронной *почты (<домена псевдонима>*@ <).> Это значение может содержать буквы, цифры и символы !, #, $, %, &, ', *, +, -, /, =, ?, ^, _, ', {, |, } и ~. Точки (.) можно использовать, но каждая точка должна быть окружена другими допустимыми символами (например, help.desk). Символы Юникода от U+00A1 до U+00FF также разрешены, но сопоставляются с текстовыми символами US-ASCII на основном адресе электронной почты (например, U+00F6 (ö) изменен на oe). Псевдоним не может превышать 64 символов и должен быть уникальным в лесу. Когда пользователь вводит псевдоним в строке Кому: сообщения электронной почты, он разрешается в отображаемое имя группы.

  Когда вы изменяете значение псевдонима, предыдущий основной адрес электронной почты хранится в качестве прокси-адреса для этой группы.

- **Примечания**. Используйте это поле для описания назначения группы. Такое описание отображается в глобальном списке адресов и области сведений в

Центре администрирования Exchange.

- **Скрыть эту группу из списков адресов**. Установите этот флажок, если вы не хотите, чтобы пользователи видели группу в глобальном списке адресов. Если этот флажок установлен, отправителю необходимо знать и ввести псевдоним или электронный адрес группы для отправки сообщений группе.

- **Подразделение**. В этом поле только для чтения отображается расположение объекта группы в Active Directory. Чтобы переместить группу в другое подразделение, необходимо использовать оснастку "Пользователи и компьютеры Active Directory".

Собственность

Этот раздел используется для назначения владельцев группы. Для каждой группы должен существовать по крайней мере один владелец. Владельцы групп могут следующее:

- изменять свойства группы;

- Изменять свойства группы.

- Добавлять и удалять участников группы.

- утверждать запросы на выход из группы и присоединение к ней (если таковые имеются);

- утверждать сообщения, отправленные группе (если включена функция модерирования).

Чтобы добавить владельцев, нажмите кнопку ✚ В открывшемся диалоговом окне **Выберите владельцев** укажите одного или нескольких владельцев, а затем последовательно нажмите кнопки **Добавить** и **ОК**.

Чтобы удалить владельцев, выберите владельца в списке и нажмите кнопку **Удалить**━

Участие

Эта вкладка используется для добавления или удаления членов группы. Владельцам группы не обязательно быть ее участниками.

Чтобы добавить участников в группу, щелкните **Добавить**✚ В открывшемся диалоговом окне **Выбор членов** укажите одного или нескольких членов, а затем

последовательно нажмите кнопки **Добавить** и **ОК**.

Чтобы удалить участников, выберите участника в списке и нажмите кнопку **Удалить** ➖.

Утверждение членства

Независимо от того, установлен флажок **Требуется утверждение владельца** или нет, запросы пользователей на вступление в группу безопасности с поддержкой электронной почты не отправляются владельцам группы. Владельцу группы необходимо вручную добавлять членов в группу безопасности с поддержкой электронной почты и удалять их из нее.

Управление доставкой

Эта вкладка позволяет предоставлять разрешения на отправку сообщений группе.

- **Только отправители внутри моей организации**. Группа принимает только сообщения от аутентифицированных (внутренних) отправителей. Это параметр по умолчанию.
- **Отправители внутри и за пределами моей организации**. Группа принимает сообщения от аутентифицированных и не прошедших проверку подлинности (внутренних и внешних) отправителей.
- Ограничьте внутренних отправителей, которые могут отправлять сообщения в группу, нажав ➕ В открывшемся диалоговом окне **Выбор разрешенных отправителей** укажите одного или нескольких отправителей, а затем последовательно нажмите кнопки **Добавить** и **ОК**. Только выбранные пользователи смогут отправлять сообщения этой группе.

  Чтобы удалить внутренних отправителей, которым разрешено отправлять сообщения в группу, выберите отправителя в списке и нажмите кнопку **Удалить**➖

> ⓘ **Важно!**
>
> Почтовые контакты всегда считаются отправителями, не прошедшими проверку подлинности (внешними пользователями). Если выбрать параметр **Отправители только в этой организации** и добавить почтовый контакт в список утвержденных внутренних отправителей, сообщения, отправляемые группе этим почтовым контактом, будут отклонены.

Утверждение сообщений

Эта вкладка используется для настройки параметров модерирования сообщений, отправляемых группе.

- **Сообщения, отправленные в эту группу, должны быть утверждены модератором**. Этот флажок не установлен по умолчанию. Если установить этот флажок, отправляемые группе сообщения должны быть утверждены определенным модератором, прежде чем они будут доставлены членам группы. При выборе этого параметра можно настроить дополнительные параметры, описанные ниже.

  - **Модераторы групп**. Для групп безопасности с поддержкой почты владельцы групп не используются автоматически в качестве модераторов. Если включена функция модерирования, здесь необходимо указать хотя бы одного модератора.

    Чтобы добавить модераторов, щелкните **Добавить**➕. В появившемся диалоговом окне **Выбрать модераторов группы** укажите одного или нескольких модераторов (среди них может быть любой из владельцев группы), а затем последовательно нажмите кнопки **Добавить** и **ОК**.

    Чтобы удалить модераторов, выберите модератора в списке и нажмите кнопку **Удалить**➖

  - **Отправители, которым не требуется утверждение сообщений**. Чтобы настроить отправителей, которые могут обходить модерацию для группы (отправлять сообщения непосредственно участникам группы), нажмите кнопку **Добавить**➕ В открывшемся диалоговом окне **Выбрать отправителей** укажите одного или нескольких отправителей, а затем последовательно нажмите кнопки **Добавить** и **ОК**.

    Чтобы удалить отправителей, выберите отправителя в списке и нажмите кнопку **Удалить**➖

    Вам не нужно вносить модераторов в список отправителей, способных обходить модерирование. На сообщения, которые отправляет группе модератор, не распространяется модерирование.

  - **Выбор уведомлений об модерации**. Этот параметр настраивает способ уведомления отправителей сообщений, когда их сообщения не утверждены модератором:

- **Уведомлять всех отправителей о том, что их сообщения не утверждены**. Аутентифицированные и не прошедшие проверку подлинности (внутренние и внешние) отправителя получают уведомление, когда их сообщения не утверждены модератором группы. Это значение используется по умолчанию.

- **Уведомлять отправителей в вашей организации о том, что их сообщения не утверждены**. Уведомляются только аутентифицированные (внутренние) отправители, если их сообщения не утверждены модератором группы.

- **Не уведомляйте никого о том, что сообщение не утверждено**: отправителям не сообщаются, когда их сообщения не утверждены модератором группы.

Параметры электронной почты

Эта вкладка позволяет просмотреть или изменить электронные адреса, настроенные для этой группы.

- **Email адрес**. По умолчанию этот параметр используется для добавления дополнительных адресов электронной почты для группы (также известных как прокси-адреса).

  По умолчанию основной электронный адрес, или обратный адрес, настраивается с помощью политики электронных адресов, применяемой к группе. Дополнительные сведения о политиках адресов электронной почты см. в разделе политики адресов Email в Exchange Server. Основной электронный адрес, отображенный здесь, выделен жирным шрифтом, а значение **SMTP** в столбце **Тип** указано прописными буквами.

  Чтобы вручную указать основной электронный адрес группы, необходимо снять флажок **Автоматически обновлять адреса электронной почты на основе политики адресов электронной почты, применимой к этому получателю**. Обратите внимание на то, что снятие этого флажка предотвращает автоматические обновления электронных адресов группы с помощью политик электронных адресов.

  - Чтобы добавить новый адрес электронной почты для группы, щелкните **Добавить**➕ In the **New email address** page that opens, select one of these options:

  - **Email тип адреса**: выберите **SMTP**. В **поле адрес Email** введите адрес электронной почты (например, helpdesk@contoso.com). В качестве домена

должен использоваться обслуживаемый домен, настроенный для организации. Дополнительные сведения см. в разделе Обслуживаемые домены в Exchange Server.

- Если на предыдущей странице не был снят флажок **Автоматически обновлять адреса электронной почты на основе политики адресов электронной почты, применимой к этому получателю**, электронный адрес будет добавлен в группу в качестве прокси-адреса (на этой странице отсутствует флажок **Назначить адресом для ответа**).

- Если на предыдущей странице был снят флажок **Автоматически обновлять адреса электронной почты на основе политики адресов электронной почты, применимой к этому получателю**, можно выбрать вариант **Назначить адресом для ответа**. Этот параметр используется, чтобы добавить новый электронный адрес в качестве основного, а предыдущий оставить в качестве прокси-адреса. Если не установить флажок **Назначить адресом для ответа**, электронный адрес будет добавлен в качестве прокси-адреса, и это не повлияет на основной электронный адрес.

- **Email тип адреса**. Выберите **Ввести пользовательский тип адреса**. Введите пользовательский тип электронного адреса (например, X400). В поле **Адрес электронной почты** введите пользовательский электронный адрес.

Примечание. За исключением адресов X.400, Exchange не проверяет пользовательские адреса электронной почты на правильность форматирования. Необходимо убедиться, что пользовательский адрес электронной почты соответствует требованиям к формату для этого типа адреса.

После этого нажмите кнопку **ОК**.

- Чтобы изменить существующий адрес электронной почты для группы, выберите его в списке и нажмите кнопку **Изменить**. Обратите внимание на то, что изменить можно только электронный адрес, но не его тип.

- Чтобы удалить существующий адрес электронной почты из группы, выберите его в списке и нажмите кнопку **Удалить**. Обратите внимание на то, что основной электронный адрес удалить невозможно.

Подсказка

Эта вкладка позволяет добавить настраиваемую подсказку для группы. Прежде чем пользователи отправят сообщение группе, они получают подсказки, оповещающие

о потенциальных проблемах. Дополнительные сведения см. в статье Configure Custom MailTips for Recipients.

> ⓘ **Примечание**
>
> Подсказки могут содержать HTML-теги, но сценарии не допускаются. Длина пользовательской подсказки не должна превышать 175 отображаемых символов. HTML-теги при этом не учитываются.

Делегирование группы

Эта вкладка позволяет назначать разрешения в отношении группы тому или иному пользователю (*делегату*).

- **Отправить как**. Указанные пользователи могут отправлять сообщения, которые, как представляется, отправляются группой. Фактический отправитель при этом не отображается, а ответы доставляются группе.
- **Отправить от имени**. Указанные пользователи могут отправлять сообщения от имени группы. Хотя сообщения, отправляемые от имени группы, четко показывают отправителя в строке От (<*Отправитель*> от имени <*группы*>), ответы на эти сообщения доставляются группе, а не отправителю.

Чтобы добавить делегатов, щелкните **добавить** ✚ для соответствующего разрешения. В появившемся диалоговом окне выберите одного или нескольких делегатов, а затем последовательно нажмите кнопки **Добавить** и **ОК**.

Когда вы назначите одно из этих разрешений, делегат сможет выбрать группу, чтобы указать ее в поле **От** в Outlook или Outlook в Интернете (ранее Outlook Web App).

Чтобы удалить делегатов, выберите делегата в соответствующем списке и нажмите кнопку **Удалить** ━

Изменение группы безопасности с поддержкой электронной почты при помощи командной консоли Exchange

Командлет **Set-DistributionGroup** используется для изменения групп безопасности с поддержкой почты. Ниже приведены некоторые интересные параметры, которые

можно настроить с помощью командлета **Set-DistributionGroup** , который недоступен в EAC или командлете **New-DistributionGroup** :

- Настройте значения для свойств **CustomAttribute1** – **CustomAttribute15** (параметры *CustomAttribute1* – *CustomAttribute15*).
- Настройка подсказок на разных языках (параметр *MailTipTranslations*).
- Настройте максимальный размер сообщения, которое можно отправить или отправить из группы (параметры *MaxReceiveSize* и *MaxSendSize*).
- Вместо указания внутренних получателей , *которым* разрешено отправлять сообщения в группу, можно указать внутренних получателей, которым *запрещено* отправлять сообщения в группу (параметр *RejectMessagesFromSendersOrMembers*).

Подробные сведения о синтаксисе и параметрах см. в статье Set-DistributionGroup.

В этом примере показано, как настроить значение DoNotMigrate для свойства **CustomAttribute5** группы Experimental Project (Экспериментальный проект).

PowerShell

```
Set-DistributionGroup -Identity "Experimental Project" -CustomAttribute5
DoNotMigrate
```

В этом примере добавляется перевод на испанский язык для существующей подсказки на английском языке: "Пожалуйста, разрешите 4 рабочих дня для ответа на сообщения, отправленные этой группе", настроенной в группе events@contoso.comбезопасности с поддержкой почты .

PowerShell

```
Set-DistributionGroup -Identity events@contoso.com -MailTipTranslations
@{Add="ES:Espere 4 días hábiles para responder a los mensajes enviados a
este grupo."}
```

Как проверить, все ли получилось?

Чтобы проверить, получилось ли изменить группу безопасности с поддержкой электронной почты, выполните одно из указанных ниже действий.

- В Центре администрирования Майкрософт перейдите в раздел**Группы**> получателей, выберите группу безопасности с поддержкой **почты**> (значение

Тип группы — **Группа безопасности**), > щелкните ✎ проверьте значения свойств.

- В командной консоли Exchange замените <*GroupIdentity*> идентификатором группы (например, именем, псевдонимом или адресом электронной почты) и выполните следующую команду, чтобы проверить значения свойств:

```
PowerShell

Get-DistributionGroup -Identity <GroupIdentity> | Format-List
```

Просмотр групп безопасности с поддержкой электронной почты при помощи командной консоли Exchange

Командлет **Get-DistributionGroup** позволяет просматривать группы безопасности с поддержкой электронной почты.

Этот пример кода возвращает сводный список всех групп безопасности в организации.

```
PowerShell

Get-DistributionGroup -ResultSize unlimited -Filter "RecipientTypeDetails -
eq 'MailUniversalSecurityGroup'"
```

Этот пример кода возвращает подробные сведения о группе безопасности с поддержкой электронной почты, именуемой Help Desk (Служба технической поддержки).

```
PowerShell

Get-DistributionGroup -Identity "Help Desk" | Format-List
```

Подробные сведения о синтаксисе и параметрах см. в статье Get-DistributionGroup.

Удаление групп безопасности с поддержкой электронной почты

Удаление группы безопасности с поддержкой электронной почты при помощи Центра администрирования Exchange

1. В EAC перейдите в раздел **Группы получателей**>.
2. В списке групп найдите группу безопасности, которую требуется удалить. Варианты поиска:
   - Прокрутите список групп.
   - Щелкните введите часть имени, адреса электронной почты или псевдонима группы.
   - Щелкните **Значок Дополнительные параметры** > **Расширенный поиск** для поиска группы.
   - Щелкните заголовок столбца **Тип группы**, чтобы отсортировать группы по значению **Группа безопасности**.

   После того как вы найдете группу безопасности, которую нужно удалить, выберите ее, щелкните **значок Удалить** а затем нажмите кнопку **Да** в появившемся предупреждающем сообщении.

Удаление группы безопасности с поддержкой электронной почты при помощи командной консоли Exchange

Для удаления группы безопасности с поддержкой электронной почты используйте указанный ниже синтаксис.

PowerShell

```
Remove-DistributionGroup -Identity <GroupIdentity>
```

Этот пример кода удаляет группу безопасности с поддержкой электронной почты, для которой задан псевдоним со значением contractors.

PowerShell

```
Remove-DistributionGroup -Identity contractors
```

Как проверить, все ли получилось?

Чтобы убедиться в успешном удалении группы безопасности с поддержкой электронной почты, выполните одно из указанных ниже действий.

- В EAC перейдите в раздел **Группы получателей**> и убедитесь, что группа отсутствует в списке. Обратите внимание, что может потребоваться нажать
- В командной консоли Exchange запустите указанную ниже команду и убедитесь, что группа не указана в списке.

  PowerShell

  ```
  Get-DistributionGroup -Filter "RecipientType -eq
  'MailUniversalSecurityGroup'"
  ```

- В командной консоли Exchange замените <*GroupIdentity*> удостоверением группы (например, именем, псевдонимом или адресом электронной почты) и выполните следующую команду, чтобы убедиться, что группа не возвращена:

  PowerShell

  ```
  Get-DistributionGroup -Identity <GroupIdentity> | Format-List
  ```

- В командной консоли Exchange запустите указанную ниже команду и убедитесь, что группа присутствует в списке.

  PowerShell

  ```
  Get-Group -Filter "RecipientTypeDetails -eq 'UniversalSecurityGroup'"
  ```

Включение или выключение поддержки электронной почты для существующих групп безопасности

Включить или отключить поддержку электронной почты для существующих групп безопасности (в том числе универсальных) невозможно в Центре администрирования Exchange. Можно использовать только командную консоль Exchange.

Включение поддержки электронной почты для существующей группы безопасности с помощью командной консоли Exchange

Чтобы включить поддержку электронной почты для существующей универсальной группы безопасности, используйте указанный ниже синтаксис.

PowerShell

```
Enable-DistributionGroup -Identity <GroupIdentity> [-Alias <Alias>] [-
DisplayName <DisplayName>] [-PrimarySMTPAddress <EmailAddress>]
```

Этот пример кода включает поддержку электронной почты для существующей универсальной группы безопасности Help Desk (Служба технической поддержки). При этом используются указанные ниже параметры.

- **Псевдоним**: hdesk. Если бы мы не использовали параметр *Alias* , то было бы использовано значение параметра *Name* с удаленными пробелами (HelpDesk в этом примере).
- **Отображаемое имя**. Так как мы не используем параметр *DisplayName* , для отображаемого имени используется существующее значение свойства **Name** группы.
- **Основной адрес электронной почты**. Так как мы используем параметр *Alias*, основным адресом электронной почты группы является *<домен псевдонима>@ <, где домен указывается политикой адресов электронной почты, применяемой к группе.>>>* < Если задано значение для параметра *PrimarySMTPAddress* , свойству **EmailAddressPolicyEnabled будет присвоено** значение `$false`, что означает, что адреса электронной почты группы не обновляются автоматически политиками адресов электронной почты.

PowerShell

```
Enable-DistributionGroup -Identity "Help Desk" -Alias hdesk
```

После включения электронной почты группа безопасности будет отображаться для всех остальных командлетов ***-DistributionGroup** .

Подробные сведения о синтаксисе и параметрах см. в статье Enable-DistributionGroup.

Как проверить, все ли получилось?

Чтобы проверить, получилось ли включить поддержку электронной почты для существующей группы безопасности, выполните одно из указанных ниже действий.

- В EAC перейдите в раздел **Группы получателей**>. Убедитесь, что группа присутствует в списке, а в качестве значения **Тип группы** указан вариант **Группа безопасности**. Обратите внимание, что может потребоваться нажать 🔄 если EAC уже открыт.

- В командной консоли Exchange запустите указанную ниже команду и убедитесь, что группа присутствует в списке.

  PowerShell

  ```
  Get-DistributionGroup -Filter "RecipientType -eq
  'MailUniversalSecurityGroup'"
  ```

- В командной консоли Exchange замените <*GroupIdentity*> идентификатором группы (например, именем, псевдонимом или адресом электронной почты) и выполните следующую команду, чтобы проверить значения свойств:

  PowerShell

  ```
  Get-DistributionGroup -Identity <GroupIdentity> | Format-List
  ```

Отключение поддержки электронной почты для существующей группы безопасности при помощи командной консоли Exchange

Чтобы отключить поддержку электронной почты для существующей универсальной группы безопасности, используйте указанный ниже синтаксис.

PowerShell

```
Disable-DistributionGroup -Identity <GroupIdentity> [-IgnoreDefaultScope]
```

Этот пример кода отключает поддержку электронной почты для группы безопасности, именуемой Human Resources (Управление персоналом).

PowerShell

```
Disable-DistributionGroup -Identity "Human Resources"
```

Примечания.

- Если группа рассылки не отображается из-за ограниченной области получателей, необходимо использовать параметр *IgnoreDefaultScope* , чтобы просмотреть все группы в лесу Active Directory. При использовании этого параметра необходимо определить группу по ее различающемуся имени. Например, `"CN=<Group Name>,CN=North America,CN=Users,DC=contoso,DC=com"`.

- После отключения группы безопасности по почте группа будет невидимой для всех командлетов ***-DistributionGroup** , кроме **Enable-DistributionGroup**.

Подробные сведения о синтаксисе и параметрах см. в статье Disable-DistributionGroup.

Как проверить, все ли получилось?

Чтобы проверить, получилось ли отключить поддержку электронной почты для существующей универсальной группы безопасности, выполните одно из указанных ниже действий.

- В EAC перейдите в раздел **Группы получателей**> и убедитесь, что группа отсутствует в списке. Обратите внимание, что может потребоваться нажать 🔄 если EAC уже открыт.

- В командной консоли Exchange запустите указанную ниже команду и убедитесь, что группа не указана в списке.

```
PowerShell

Get-DistributionGroup -Filter "RecipientType -eq
'MailUniversalSecurityGroup'"
```

- В командной консоли Exchange замените <*GroupIdentity*> именем группы и выполните следующую команду, чтобы убедиться, что группа не возвращена:

```
PowerShell

Get-DistributionGroup -Identity <GroupIdentity> | Format-List
```

- В командной консоли Exchange запустите указанную ниже команду и убедитесь, что группа присутствует в списке.

```
PowerShell
```

```
Get-Group -Filter "RecipientTypeDetails -eq 'UniversalSecurityGroup'"
```

Управление динамическими группами рассылки

Статья • 04.04.2023

Динамические группы рассылки — это объекты групп Active Directory с включенной поддержкой почты, которые создаются для упрощения массовой отправки сообщений электронной почты и другой информации в пределах организации Exchange.

В отличие от обычных групп рассылки, которые содержат определенный набор членов, список членов для динамических групп рассылки рассчитывается при каждой отправке сообщения в группу в соответствии с определяемыми пользователем фильтрами и условиями. Если электронное сообщение отправляется динамической группе рассылки, оно доставляется всем получателям, соответствующим заданным для группы критериям, в организации.

> ⓘ **Важно!**
>
> В динамическую группу рассылки включается любой получатель из Active Directory, имеющий атрибуты, соответствующие применяемому фильтру. Если после изменения свойств получателя они начинают отвечать критериям фильтра, такой получатель может случайно стать членом группы и начать получать сообщения, отправляемые группе рассылки. Строгая и последовательная процедура подготовки учетной записи позволяет снизить вероятность возникновения такой ситуации.

Что нужно знать перед началом работы?

- Осталось времени до завершения: от 2 до 5 минут.
- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Динамические группы рассылки" в разделе Разрешения получателей .

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Создание динамической группы рассылки

Использование EAC для создания динамической группы рассылки

1. В EAC перейдите в раздел**Группы**>**получателей**>**Новая**>**динамическая группа рассылки**.

2. На странице **новой динамической группы рассылки** заполните следующие поля:

   - * **Отображаемое имя**: используйте это поле для ввода отображаемого имени. Это имя отображается в общей адресной книге в строке "Кому" при отправке в эту группу электронного сообщения и в списке "Группы" в центре администрирования Exchange. Отображаемое имя обязательно и должно быть понятным, чтобы пользователи могли понять его назначение. Это имя также должно быть уникальным в лесу.

     > **Примечание**
     >
     > Политика именования групп не применяется к динамической группе рассылки.

   - * **Псевдоним**. Используйте это поле, чтобы ввести имя псевдонима для группы. Длина псевдонима не должна превышать 64 знака, и он должен быть уникальным в данном лесу. Когда пользователь вводит псевдоним в строку "Кому" электронного сообщения, он сопоставляется с кратким именем группы.

   - **Описание**. Используйте это поле, чтобы описать группу, чтобы пользователи знали, каково назначение группы. Это описание

отображается в общей адресной книге.

- **Подразделение**. Вы можете выбрать подразделение, отличное от стандартного (который является областью получателя). Если область получателей установлена на уровне леса, будет установлено значение по умолчанию для контейнера "Пользователи" домена Active Directory, в котором находится компьютер с запущенным центром администрирования Exchange. Если область получателей настроена на определенный домен, то контейнер пользователей в этом домене выбирается по умолчанию. Если в качестве области получателей задано определенное подразделение организации, то оно выбирается по умолчанию.

  Нажмите кнопку **Обзор**, чтобы выбрать другое подразделение. В этом диалоговом окне отображаются все подразделения в лесу, которые находятся внутри определенной области. Выберите нужное подразделение и нажмите кнопку **OK**.

- **Владелец**. Владелец динамической группы рассылки является необязательным. В число владельцев можно добавлять других пользователей, нажав **Обзор** и выбрав пользователей из списка.

3. Раздел **Участники** используется для указания типов получателей группы и задания правил, которые будут определять членство. Выберите одно из приведенных ниже значений.

   - **Все типы получателей**. Выберите этот параметр, чтобы отправлять сообщения, соответствующие условиям, определенным для этой группы, всем типам получателей.

   - **Только следующие типы получателей**: Сообщения, которые соответствуют критериям, определенным для этой группы, будут отправляться одному или нескольким из следующих типов получателей:

   - **Пользователи с почтовыми ящиками Exchange**. Установите этот флажок, если вы хотите включить пользователей с почтовыми ящиками Exchange. К пользователям с почтовыми ящиками Exchange относятся пользователи, имеющие учетную запись домена пользователя и почтовый ящик в организации Exchange.

   - **Пользователи с внешними адресами электронной почты**. Установите этот флажок, если вы хотите включить пользователей с внешними адресами электронной почты. Пользователи с внешними учетными

записями электронной почты имеют учетные записи домена Active Directory, но используют учетные записи электронной почты, которые являются внешними для организации. Это позволяет включать их в глобальный список адресов (GAL) и добавлять в списки рассылки.

- **Почтовые ящики ресурсов**. Установите этот флажок, если вы хотите включить почтовые ящики ресурсов Exchange. Почтовые ящики ресурсов позволяют администрировать ресурсы компании, например, конференц-зал или транспортное средство компании, через почтовый ящик.

- **Контакты с внешними адресами электронной почты**. Установите этот флажок, если вы хотите включить контакты с внешними адресами электронной почты. Контакты с внешними адресами электронной почты не имеют учетных записей домена Active Directory, но используют внешние адреса электронной почты, доступные в глобальном списке адресов.

- **Группы с поддержкой почты**. Установите этот флажок, если вы хотите включить группы безопасности или группы рассылки, для которых включена почта. Группы с включенной поддержкой почты подобны группам рассылки. Сообщения электронной почты, отправленные на учетную запись группы с включенной поддержкой почты, будут доставлены нескольким получателям.

4. Щелкните **Добавить правило**, чтобы определить условия членства в этой группе.

5. Выберите один из следующих атрибутов получателя из раскрывающегося списка и введите соответствующее значение. Если значение для выбранного атрибута соответствует заданному значению, получатель получает сообщение, отправленное в эту группу.

Атрибут	**Отправить сообщение получателю, если...**
Контейнер получателей	Объект получателя находится в указанном домене или подразделении.
Область, край;	Указанное значение соответствует свойству области или краю получателя.
Company	Указанное значение соответствует свойству организации получателя.

Атрибут	Отправить сообщение получателю, если...
Department	Указанное значение соответствует свойству отдела получателя.
Пользовательский атрибут N (где N — это число от 1 до 15)	Указанное значение соответствует свойству CustomAttributeN получателя.

> ⓘ **Важно!**
>
> Значения, вводимые для выбранного атрибута, должны точно совпадать со значениями, отображаемыми в свойствах получателя. Например, если вы введете **Вашингтон** для **штата или провинции**, но значение свойства получателя — **WA**, условие не будет выполнено. Кроме того, в указанных текстовых значениях регистр не учитывается. Например, если указать **Contoso** для атрибута **Организация**, сообщения будут отправлены получателю и в том случае, если задано значение **contoso**.

6. В окне **Укажите слова или фразы** введите значение в текстовом поле. Нажмите кнопку **Добавить**, а затем — кнопку **OK**.

7. Чтобы добавить правило для определения условий членства, щелкните **Добавить правило** под предыдущим правилом.

> ⓘ **Важно!**
>
> Если добавлено несколько правил, определяющих членство, получатель должны соответствовать условиям каждого правила для получения сообщений, отправляемых группе. Другими словами, правила связаны логическим оператором **И**.

8. Закончив, щелкните **Сохранить** для создания динамической группы рассылки.

> ⓘ **Примечание**
>
> Если вы хотите указать правила для атрибутов, отличных от доступных в EAC, необходимо использовать командную консоль Exchange для создания динамической группы рассылки. Помните, что параметрами фильтра и условий для динамических групп рассылки с настраиваемыми фильтрами получателей можно управлять только с помощью командной консоли Exchange. Пример создания динамической группы рассылки с

пользовательским запросом см. в следующем разделе об использовании командной консоли Exchange для создания динамической группы рассылки.

Создание динамической группы рассылки с помощью командной консоли Exchange

> ⓘ **Примечание**
>
> Если в командлетах не указано подразделение, они применяются к локальному подразделению (подразделению, в котором создается динамическая группа рассылки). С помощью командлета `New-DynamicDistributionGroup` `RecipientContainer` используйте параметр , чтобы указать подразделение.

В этом примере создается динамическая группа рассылки "Mailbox Users DDG", в которую входят только пользователи почтовых ящиков.

PowerShell

```
New-DynamicDistributionGroup -IncludedRecipients MailboxUsers -Name "Mailbox Users DDG" -RecipientContainer Users
```

В этом примере создается динамическая группа рассылки с настраиваемым фильтром получателей. Динамическая группа рассылки включает в себя всех пользователей почтовых ящиков на сервере Server1:

PowerShell

```
New-DynamicDistributionGroup -Name "Mailbox Users on Server1" -
RecipientContainer Users -RecipientFilter "(RecipientTypeDetails -eq
'UserMailbox') -and (ServerName -eq 'Server1')"
```

В этом примере создается динамическая группа рассылки с настраиваемым фильтром получателей. Динамическая группа рассылки включает в себя всех пользователей почтовых ящиков, которые имеют значение"FullTimeEmployee"в свойстве **CustomAttribute10**.

PowerShell

```
New-DynamicDistributionGroup -Name "Full Time Employees" -RecipientFilter "
(RecipientTypeDetails -eq 'UserMailbox') -and (CustomAttribute10 -eq
'FullTimeEmployee')"
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе New-DynamicDistributionGroup.

Как проверить, все ли получилось?

Чтобы убедиться в успешном создании динамической группы рассылки, выполните одно из следующих действий:

- В Центре администрирования Exchange (EAC) выберите **Получатели**>**Группы**. В списке групп отображается новая динамическая группа рассылки. В разделе **Тип группы** указано **Динамическая группа рассылки**.
- В командной консоли Exchange выполните следующую команду, чтобы отобразить сведения о новой динамической группе рассылки.

  PowerShell

  ```
  Get-DynamicDistributionGroup | Format-List
  Name,RecipientTypeDetails,RecipientFilter,PrimarySmtpAddress
  ```

Изменение свойств динамической группы рассылки

Использование EAC для изменения свойств динамической группы рассылки

1. В Центре администрирования Exchange (EAC) выберите **Получатели**>**Группы**.
2. В списке групп щелкните динамическую группу рассылки, которую нужно просмотреть или изменить, а затем щелкните **Изменить**.
3. На странице свойств группы щелкните один из следующих разделов, чтобы просмотреть или изменить свойства.
   - General
   - Владение.

- Членство
- Управление доставкой
- Утверждение сообщений.
- Параметры электронной почты.
- Подсказка
- Делегирование группы

Общие

Этот раздел используется для просмотра или изменения базовых сведений о группе.

- * **Отображаемое имя**: это имя отображается в адресной книге, в строке Кому: при отправке сообщения электронной почты в эту группу, а также в списке Группы. Отображаемое имя обязательно и должно быть понятным, чтобы пользователи могли понять его назначение. Кроме того, оно должно быть уникальным в пределах домена.
- * **Псевдоним**: это часть адреса электронной почты, которая отображается слева от символа (@). Если изменить псевдоним, основной адрес SMTP группы также изменится и будет содержать новый псевдоним. Кроме того, адрес электронной почты с предыдущим псевдонимом сохранится в качестве прокси-адреса группы.
- **Описание**. Используйте это поле, чтобы описать группу, чтобы пользователи знали, каково назначение группы. Это описание отображается в адресной книге на панели подробностей в центре администрирования Exchange.
- **Скрыть эту группу из списков адресов**. Установите этот флажок, если вы не хотите, чтобы пользователи видели эту группу в адресной книге. Чтобы отправить электронное сообщение этой группе, отправитель должен ввести псевдоним группы или адрес электронной почты в строки "Кому" или "Копия" .
- **Подразделение**. В этом поле только для чтения отображается подразделение, содержащее динамическую группу рассылки. Необходимо использовать оснастку "Пользователи и компьютеры Active Directory", чтобы переместить группу в другое подразделение.

Собственность

Этот раздел используется для назначения владельцев группы. Динамическая группа рассылки может иметь только одного владельца. Владелец группы отображается на вкладке **Управляется** объекта в разделе "Active Directory — пользователи и компьютеры".

В число владельцев можно добавлять других пользователей, нажав **Обзор** и выбрав пользователей из списка. Чтобы удалить владельца, нажмите кнопку **Очистить** (**X**) и нажмите кнопку **Сохранить**.

Участие

Используйте этот раздел, чтобы изменить условия, определяющие состав группы. Можно удалить или изменить существующие правила членства и добавить новые правила. Процедуры, в которые показано, как это сделать, см. в статье Создание динамической группы рассылки с помощью EAC в процедурах настройки членства при использовании EAC для создания новой динамической группы рассылки.

Управление доставкой

В этом разделе можно определить, кто может отправлять почту в эту группу.

- **Только отправители внутри моей организации**. Выберите этот параметр, чтобы разрешить только отправителям в вашей организации отправлять сообщения в группу. Это означает, что если кто-то снаружи организации отправляет сообщение электронной почты в эту группу рассылки, оно отклоняется. Это параметр по умолчанию.

- **Отправители внутри и за пределами моей организации**. Выберите этот параметр, чтобы разрешить всем пользователям отправлять сообщения в группу.

  Можно дополнительно ограничить круг пользователей, имеющих право отправлять сообщения в эту группу, указав только определенных отправителей. Щелкните **Добавить**➕ а затем выберите одного или нескольких получателей. Если в этот список будут добавлены отправители, они станут единственными пользователями, которые будут иметь право на отправку сообщений в эту группу. Сообщения электронной почты, отправленные кем-либо, не содержащимся в этом списке, будут отклоняться.

  Чтобы удалить пользователя или группу из списка, выберите их в списке и нажмите кнопку **Удалить**➖

> ⓘ **Важно!**
>
> Если настроить эту группу так, чтобы разрешить отправлять сообщения в эту группу только для отправителей внутри организации, письмо, отправленное от почтового контакта, будет отклонено, даже если он добавлен в этот список.

Утверждение сообщений

В этом разделе можно установить параметры изменения группы. Модераторы утверждают или отклоняют отправленные в группу сообщения перед их доставкой членам группы.

- **Сообщения, отправленные в эту группу, должны быть утверждены модератором**. Этот флажок не установлен по умолчанию. Если установить этот флажок, входящие сообщения перед доставкой будут проверяться модераторами группы. Модераторы группы могут утвердить или отклонить входящее сообщение.

- **Модераторы групп**. Чтобы добавить модераторов групп, нажмите кнопку **Добавить**➕ Чтобы удалить модератора, выберите его и нажмите кнопку **Удалить**➖ Если вы выбрали "Сообщения, отправленные в эту группу, должны быть утверждены модератором" и не выбираете модератора, сообщения в группу отправляются владельцам групп для утверждения.

- **Отправители, которым не требуется утверждение сообщений**. Чтобы добавить людей или группы, которые могут обойти модерацию для этой группы, щелкните **Добавить**➕ Чтобы удалить пользователя или группу, выберите элемент и нажмите кнопку **Удалить**➖.

- **Выбор уведомлений о модерации**. Используйте этот раздел, чтобы задать способ уведомления пользователей об утверждении сообщений.

    - **Уведомление всех отправителей о том, что их сообщения не утверждены**. Это параметр по умолчанию. Все отправители, которые находятся внутри и вне организации, будут уведомляться в том случае, если их сообщения не были утверждены.

    - **Уведомлять отправителей в организации только в том случае, если их сообщения не утверждены**. При выборе этого параметра только пользователи или группы в вашей организации получают уведомления, когда сообщение, отправленное ими группе, не утверждено модератором.

- **Не уведомляйте никого о том, что сообщение не утверждено**. При выборе этого параметра уведомления не отправляются отправителям сообщений, сообщения которых не утверждены модераторами групп.

Параметры электронной почты

Этот раздел используется для просмотра и изменения адресов электронной почты, связанных с группой. Он включает основные адреса SMTP группы и любые связанные прокси-адреса. Основной адрес SMTP (также известный как *адрес ответа*) отображается жирным шрифтом в списке адресов и прописными буквами **SMTP** в столбце **Тип**.

- **Добавить: щелкните**➕ чтобы добавить новый адрес электронной почты для этого почтового ящика. Выберите один из следующих типов адресов:
  - **SMTP**. Это тип адреса по умолчанию. Нажмите эту кнопку, а затем введите новый адрес SMTP в поле ***Адрес электронной почты**.

    > ⓘ **Примечание**
    >
    > Чтобы новый адрес был основным адресом SMTP группы, установите флажок в поле **Сделать этот адрес адресом ответа**.

  - **Пользовательский тип адреса**. Нажмите эту кнопку и введите один из поддерживаемых типов адресов электронной почты, **отличных от** SMTP, в поле *Email адрес.

    > ⓘ **Примечание**
    >
    > Настраиваемый адрес. Чтобы добавить настраиваемый адрес (например, факс или X.400), нажмите эту кнопку и используйте соответствующее диалоговое окно.

- **Изменить**. Чтобы изменить адрес электронной почты, связанный с группой, выберите его в списке и нажмите кнопку **Изменить**.✏️

  > ⓘ **Примечание**
  >
  > Чтобы сделать существующий адрес основным адресом SMTP группы, установите флажок в поле **Сделать этот адрес адресом ответа**.

- **Удалить**. Чтобы удалить адрес электронной почты, связанный с группой, выберите его из списка и нажмите кнопку **Удалить**➖.

- **Автоматически обновлять адреса электронной почты на основе политики адресов электронной почты, которая применяется к этому получателю**. Установите этот флажок, чтобы адреса электронной почты получателей автоматически обновлялись на основе изменений политики адресов электронной почты организации. По умолчанию этот флажок установлен.

Подсказка

Используйте этот раздел для добавления подсказок, предупреждающих пользователей о возможных проблемах перед отправкой сообщения определенной группе. Подсказка — это текст, который отображается на панели информации при добавлении этой группы в строки "Кому", "Копия" и "СК" нового сообщения электронной почты. Например, можно добавить подсказку для больших аудиторий, чтобы предупредить возможных отправителей о том, что сообщение отправится большому числу получателей.

> ⓘ **Примечание**
>
> Подсказки могут содержать HTML-теги, но сценарии не допускаются. Длина пользовательской подсказки не должна превышать 175 отображаемых символов. HTML-теги при этом не учитываются.

Делегирование группы

Этот раздел используется для назначения разрешений пользователю (известному как *представитель*), чтобы разрешить ему отправлять сообщения в качестве группы или от ее имени. Можно назначать следующие разрешения:

- **Отправить как**. Это разрешение позволяет делегату отправлять сообщения в качестве группы. После того, как разрешение будет назначено, представитель сможет добавить группу в строку **От**, чтобы указать, что сообщение было отправлено группой.

- **Отправить от имени:** это разрешение также позволяет делегату отправлять сообщения от имени группы. После назначения этого разрешения делегат может добавить группу в строку **От**. Это сообщение отобразится как отправленное группой, и в нем будет сообщаться, что оно было отправлено представителем от имени группы.

Для назначения разрешений представителям нажмите кнопку **Добавить** под соответствующим разрешением, чтобы открыть страницу **Выбрать получателя**, в которой отображается список всех получателей в организации Exchange, которым можно назначить разрешение. Выберите нужных получателей, добавьте их в список и нажмите кнопку **ОК**. Чтобы найти конкретного получателя, введите его имя в поле поиска и нажмите **Поиск**.

Изменение свойств динамической группы рассылки с помощью командной консоли Exchange

Используйте командлеты **Get-DynamicDistributionGroup** и **Set-DynamicDistributionGroup** для просмотра и изменения свойств динамических групп рассылки. Преимущества использования командной консоли Exchange — это возможность изменять свойства, недоступные в EAC, и изменять свойства для нескольких групп. Сведения о том, какие параметры соответствуют свойствам группы рассылки, см. в следующих разделах:

- Получить DynamicDistributionGroup
- Настроить DynamicDistributionGroup

Ниже приведены некоторые примеры использования командной консоли Exchange для изменения свойств динамической группы рассылки.

В этом примере изменяются следующие параметры для всех динамических групп рассылки в организации:

- Скрыть все динамические группы рассылки из адресной книги
- Задать максимальный размер сообщений, отправляемых в группу, как 5 МБ
- Включить модерацию
- Назначить администратора модератором группы

PowerShell

```
Get-DynamicDistributionGroup -ResultSize unlimited | Set-
DynamicDistributionGroup -HiddenFromAddressListsEnabled $true -
MaxReceiveSize 5MB -ModerationEnabled $true -ModeratedBy administrator
```

В этом примере в группу Все сотрудники добавляется SMTP-адрес Seattle.Employees@contoso.comпрокси-сервера.

PowerShell

```
Set-DynamicDistributionGroup -Identity "All Employees" -EmailAddresses
SMTP:All.Employees@contoso.com, smtp:Seattle.Employees@contoso.com
```

Как проверить, все ли получилось?

Чтобы убедиться в том, что свойства динамической группы рассылки успешно изменены, выполните следующие действия:

- В EAC выберите группу и нажмите кнопку **Изменить** чтобы просмотреть измененное свойство или функцию. В зависимости от свойства, которое было изменено, оно может отображаться в панели подробностей выбранной группы.

- В командной консоли Exchange используйте командлет **Get-DynamicDistributionGroup** для проверки изменений. Одним из преимуществ использования командной консоли Exchange является возможность просмотра нескольких свойств для нескольких групп. В первом примере следует выполнить следующую команду, чтобы проверить новые значения.

  PowerShell

  ```
  Get-DynamicDistributionGroup -ResultSize unlimited | Format-List
  Name,HiddenFromAddressListsEnabled,MaxReceiveSize,ModerationEnabled,Mod
  eratedBy
  ```

  Чтобы увидеть указанный выше пример, в котором изменяются пределы сообщения, выполните эту команду.

  PowerShell

  ```
  Get-Mailbox -OrganizationalUnit "Marketing" | Format-List
  Name,IssueWarningQuota,ProhibitSendQuota,ProhibitSendReceiveQuota,UseDa
  tabaseQuotaDefaults
  ```

Просмотр членов динамической группы рассылки

Статья • 04.04.2023

Динамические группы рассылки — это группы рассылки, членство в которых основано на заданных фильтрах получателей, а не на определенном списке получателей. Дополнительные сведения см. в разделе Управление динамическими группами рассылки.

С помощью Центра администрирования Exchange (EAC) невозможно просматривать сведения об участниках динамической группы рассылки. Можно использовать только командную консоль Exchange.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 2 минуты.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Динамические группы рассылки" в разделе Разрешения получателей .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форум по **адресу Exchange Server** .

Просмотр членов динамической группы рассылки с помощью командной консоли Exchange

Чтобы просмотреть члены динамической группы рассылки, используйте следующий синтаксис:

```
PowerShell
```

```
$<VariableName> = Get-DynamicDistributionGroup -Identity
<DynamicDistributionGroupIdentity>

Get-Recipient -RecipientPreviewFilter ($<VariableName>.RecipientFilter) [-
OrganizationalUnit ($<VariableName>.RecipientContainer)]
```

- `<DynamicDistributionGroupIdentity>` — это имя, псевдоним или адрес электронной почты динамической группы рассылки.
- Параметр *OrganizationalUnit* является обязательным, только если вы использовали параметр *RecipientContainer* в фильтре динамической группы рассылки для указания подразделения или контейнера, отличающегося от того, где находится объект динамической группы рассылки (обычно это контейнер Users). Включить параметр *OrganizationalUnit* можно, даже если он не требуется.

В этом примере возвращается список членов динамической группы рассылки Full Time Employees. Первая команда сохраняет объект динамической группы распространения в переменной `$FTE`. Во второй команде используется командлет **Get-Recipient** для отображения списка получателей, соответствующих критериям, определенным для динамической группы рассылки.

PowerShell

```
$FTE = Get-DynamicDistributionGroup -Identity "Full Time Employees"

Get-Recipient -RecipientPreviewFilter ($FTE.RecipientFilter)
```

В этом примере возвращаются члены динамической группы рассылки с именем Project X, которая существует в контейнере Users, но использует подразделение ContosoProjects в фильтре для группы.

PowerShell

```
$ProjectX = Get-DynamicDistributionGroup -Identity "Project X"

Get-Recipient -RecipientPreviewFilter ($ProjectX.RecipientFilter) -
OrganizationalUnit ($ProjectX.RecipientContainer)
```

Дополнительные сведения о синтаксисе и параметрах см. в разделах Get-DynamicDistributionGroup и Get-Recipient.

Управление почтовыми контактами

Статья • 04.04.2023

Почтовые контакты — это, по сути, контакты для пользователей за пределами Exchange или организации. Дополнительные сведения о почтовых контактах см. в статье Получатели.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 2 минуты.
- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения подготовки получателей" раздела Разрешения получателей .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Создание почтового контакта

Создание почтового контакта с помощью Центра администрирования Exchange

1. В EAC перейдите к **разделу Получатели**>**Контакты**.
2. Щелкните **Значок "Создать**+>**Почтовый контакт**.
3. На странице **Создание почтового контакта** заполните следующие поля.
    - **Имя**. Используйте это поле, чтобы ввести имя контакта.

- **Инициалы**. Используйте это поле, чтобы ввести инициалы контакта.
- **Фамилия**: используйте это поле, чтобы ввести фамилию контакта.
- * **Отображаемое имя**: используйте это поле, чтобы ввести отображаемое имя контакта. Это имя указывается в списке контактов Центра администрирования Exchange и адресной книге вашей организации. По умолчанию в это поле добавляются имена, введенные в полях **Имя**, **Инициалы** и **Фамилия**. Если эти поля не используются, все равно необходимо ввести имя в это поле, поскольку оно является обязательным для заполнения. Длина имени не может превышать 64 символов.
- * **Имя**: используйте это поле, чтобы ввести имя контакта. Это имя, которое указано в службе каталогов. Как и отображаемое имя, по умолчанию это поле заполняется значениями, введенными в полях **Имя**, **Инициалы** и **Фамилия**. Если эти поля не используются, все равно необходимо ввести имя в это поле, поскольку оно является обязательным для заполнения. Длина имени не может превышать 64 символов.
- * **Псевдоним**: используйте это поле, чтобы ввести псевдоним (64 символа или меньше) для контакта. Это поле является обязательным.
- * **Внешний адрес электронной почты**. Используйте это поле для ввода внешней учетной записи электронной почты контакта. Это поле является обязательным. Сообщения электронной почты, отправляемые данному контакту, пересылаются на этот адрес электронной почты.
- **Подразделение**. Вы можете выбрать подразделение, отличное от используемого по умолчанию, которое является областью получателя. Если область получателей установлена на уровне леса, то значение по умолчанию настроено в контейнере пользователей в домене, содержащем компьютер под управлением Центра администрирования Exchange. Если область получателей настроена на определенный домен, то контейнер пользователей в этом домене выбирается по умолчанию. Если в качестве области получателей задано определенное подразделение организации, то оно выбирается по умолчанию.

  Нажмите кнопку **Обзор**, чтобы выбрать другое подразделение. В этом диалоговом окне отображаются все подразделения в лесу, которые находятся внутри определенной области. Выберите нужное подразделение и нажмите кнопку **ОК**.

4. После завершения нажмите кнопку **Сохранить**.

Создание почтового контакта с помощью командной консоли Exchange

В этом примере показано, как создать почтовый контакт "Debra Garcia" в Exchange Server 2016.

```
PowerShell

New-MailContact -Name "Debra Garcia" -ExternalEmailAddress
dgarcia@tailspintoys.com -OrganizationalUnit Users
```

В этом примере включается поддержка почты для существующего контакта "Karen Toh" в Exchange Server 2016.

```
PowerShell

Enable-MailContact -Identity "Karen Toh" -ExternalEmailAddress
ktoh@tailspintoys.com
```

Как проверить, все ли получилось?

Чтобы проверить, успешно ли создан почтовый контакт, выполните одно из следующих действий.

- В EAC перейдите к **разделу Получатели**>**Контакты**. Новый почтовый контакт будет отображаться в списке контактов. Под **тип контакта**, тип является **почтового контакта**.
- Для отображения информации о новом почтовом контакте выполните указанную ниже команду в командной консоли Exchange.

  ```
  PowerShell

  Get-MailContact <Name> | Format-List
  Name,RecipientTypeDetails,ExternalEmailAddress
  ```

Изменение свойств почтового контакта

Использование Центра администрирования Exchange для настройки свойств контакта

1. В EAC перейдите к **разделу Получатели**>**Контакты**.
2. В списке почтовых контактов и почтовых пользователей щелкните почтовый контакт, для которого нужно изменить свойства, а затем нажмите кнопку **Изменить**.✎
3. На странице свойств контакта щелкните один из следующих разделов, чтобы просмотреть или изменить свойства.
   - Общие
   - Контактные данные
   - Организация
   - Параметры Email
   - Подсказка

Общие сведения

Чтобы просмотреть или изменить основные сведения о почтовом контакте, используйте раздел **Общие**.

- **Имя**, **Отчество**, **Фамилия**
- * **Имя**: это имя, указанное в Active Directory. Если вы решите изменить это имя, помните, что оно не может превышать 64 символа.
- * **Отображаемое имя**: это имя отображается в адресной книге вашей организации, в строках "По" и "От" в сообщении электронной почты, а также в списке Почтовый ящик. Это имя не может содержать пробелы до или после отображаемого имени.
- * **Псевдоним**: это псевдоним почтового контакта. При изменении этого параметра он должен быть уникальным в организации и содержать не более 64 знаков.
- * **Внешний адрес электронной почты**. Это основной SMTP-адрес почтового контакта и его внешняя учетная запись электронной почты. Сообщения электронной почты, отправляемые данному контакту, пересылаются на этот адрес электронной почты.

- Щелкните **Дополнительно** для отображения подразделения, содержащего учетную запись почтового контакта. Чтобы переместить контакт в другое подразделение, используйте оснастку "Active Directory — пользователи и компьютеры".

Контактные данные

Используйте раздел **Контактная информация** для просмотра или изменения контактной информации получателя, например номера телефона и адреса. Эти данные отображаются в адресной книге.

Организация

В разделе **Организация** можно указать подробные сведения о роли контакта в организации. Эти данные отображаются в адресной книге. Кроме того, можно создать виртуальную организационную диаграмму, доступную из клиентов электронной почты, таких как Outlook.

- **Заголовок**: используйте это поле для просмотра или изменения заголовка контакта.

- **Отдел**. Используйте это поле для просмотра или изменения отдела, в котором работает контакт. Это свойство можно использовать, чтобы создавать условия получателей для динамических групп рассылки или списков адресов.

- **Компания**. Используйте это поле, чтобы просмотреть или изменить компанию, в которой работает контакт. Также можно использовать его для создания условий получателя в динамической группе рассылки.

- **Диспетчер**. Чтобы добавить руководителя, нажмите кнопку **Обзор**. В окне **Выбор руководителя** выберите соответствующего человека и нажмите кнопку **ОК**.

- **Прямые отчеты**. Изменить это поле нельзя. *Подчиненный* — это получатель, подотчетный определенному руководителю. Если для получателя указан руководитель, то он будет выводиться в качестве непосредственного подчиненного в сведениях о почтовом ящике руководителя. Например, Григорий руководит Мартой и Никитой, для которых созданы почтовые контакты, поэтому Григорий будет указан в поле **Руководитель** в свойствах организации для Марты и Никиты, а Марта и Никита будут отображаться в поле **Подчиненные** в свойствах ящика Григория.

Параметры электронной почты

Используйте раздел **Параметры электронной почты** для добавления или удаления прокси-адресов для почтового контакта или изменения существующих прокси-адресов. Основной SMTP-адрес электронной почты контакта также отображается в этом разделе, но вы не можете изменить его. Чтобы изменить его, нужно изменить внешний адрес электронной почты контакта в разделе **Общие**.

Подсказка

Используйте раздел **Подсказка** для добавления подсказок, предупреждающих пользователей о возможных проблемах при отправке сообщения этому получателю. Подсказка — это текст, который отображается на панели информации при добавлении этого получателя в поля "Кому", "Копия" и "Скрытая копия" нового сообщения электронной почты.

> ⓘ **Примечание**
>
> Подсказки могут содержать HTML-теги, но сценарии не допускаются. Длина пользовательской подсказки не должна превышать 175 отображаемых символов. HTML-теги при этом не учитываются.

Использование командной консоли Exchange для настройки свойств контакта

Свойства почтового контакта хранятся в Exchange и в Active Directory. В общем случае следует использовать командлеты **Get-Contact** и **Set-Contact** для просмотра и изменения свойств организации и контактов. Для просмотра и изменения свойств, связанных с электронной почтой, таких как адреса электронной почты, подсказки, настраиваемые атрибуты, а также указания того, скрыт ли контакт в списках адресов, используйте командлеты **Get-MailContact** и **Set-MailContact**.

Дополнительные сведения приведены в следующих разделах:

- Get-Contact
- Set-Contact
- Get-MailContact
- Set-MailContact

Ниже приведено несколько примеров использования командной консоли Exchange для изменения свойств почтового контакта.

В этом примере показано, как настроить должность, отдел, организацию и руководителя для почтового контакта Kai Axford.

PowerShell

```
Set-Contact "Kai Axford" -Title Consultant -Department "Public Relations" -
Company Fabrikam -Manager "Karen Toh"
```

В этом примере задается свойство CustomAttribute1, равное PartTime, для всех почтовых контактов, а сами контакты скрываются в адресной книге организации.

PowerShell

```
Get-MailContact | Set-MailContact -CustomAttribute1 PartTime -
HiddenFromAddressListsEnabled $true
```

В этом примере устанавливается значение свойства CustomAttribute15, равное TemporaryEmployee, для всех почтовых контактах в отдел по связям с общественностью (Public Relations).

PowerShell

```
Get-Contact -Filter "Department -eq 'Public Relations'" | Set-MailContact -
CustomAttribute15 TemporaryEmployee
```

Как проверить, все ли получилось?

Чтобы убедиться, что свойства почтового контакта успешно изменены, выполните следующие действия.

- В EAC выберите почтового контакта и нажмите кнопку **Изменить**✎ чтобы просмотреть измененное свойство.
- В командной консоли Exchange используйте командлеты **Get-Contact** и **Get-MailContact**, чтобы проверить изменения. Одно из преимуществ использования командной консоли Exchange состоит в том, что можно просматривать несколько свойств для нескольких почтовых контактов. В примере выше, где все почтовые контакты получили свойство CustomAttribute1, равное PartTime, и были скрыты из адресной книги, выполните команду ниже, чтобы проверить изменения.

PowerShell

```
Get-MailContact | Format-List
Name,CustomAttribute1,HiddenFromAddressListsEnabled
```

В приведенном выше примере, где для всех почтовых контактов в отделе "Связи с общественностью" было установлено свойство CustomAttribute15, выполните следующую команду, чтобы проверить изменения.

PowerShell

```
Get-Contact -Filter "Department -eq 'Public Relations'" | Get-
MailContact | Format-List Name,CustomAttribute15
```

Массовое изменение почтовых контактов

Чтобы изменить выбранные свойства для нескольких почтовых контактов, можно использовать Центр администрирования Exchange. Если вы выберете несколько почтовых контактов в списке в EAC, свойства, для которых возможно массовое изменение, отображаются в области сведений. При изменении одного из свойств это изменение применяется ко всем выбранным получателям.

При массовом изменении почтовых контактов для изменения доступны следующие области свойств:

- **Контактные сведения**: В этом поле можно изменить общие свойства, такие как название улицы, почтовый индекс и название города.
- **Организация**. Измените общие свойства, такие как название отдела, название компании и руководителя, которому сообщают выбранные почтовые контакты или почтовые пользователи.

Массовое изменение почтовых контактов с помощью Центра администрирования Exchange

1. В EAC перейдите к **разделу Получатели**>**Контакты**.
2. В списке контактов выберите несколько почтовых контактов. Нельзя выполнять массовое редактирование группы из почтовых контактов и почтовых пользователей.

> **Совет**

Вы можете выбрать несколько смежных почтовых контактов, удерживая нажатой клавишу SHIFT, щелкнув первый почтовый контакт, а затем щелкнув последний почтовый контакт, который вы хотите изменить. Вы также можете выбрать несколько почтовых контактов, удерживая нажатой клавишу CTRL и щелкнув каждый из них, который нужно изменить.

3. В области сведений в разделе **Групповое изменение** выберите **Обновить** для **Контактные сведения** или **Организация**.

4. Внесите необходимые изменения на странице свойств, а затем сохраните изменения.

Как проверить, все ли получилось?

Чтобы убедиться в том, что массовое изменение почтовых контактов прошло успешно, выполните одно из следующих действий:

- В EAC выберите каждый из почтовых контактов, которые вы массово редактировали, и нажмите кнопку **Изменить**✎ чтобы просмотреть измененные свойства.

- В командной консоли Exchange используйте командлет **Get-Contact** для проверки изменений. Например, вы использовали массовое изменение в EAC для изменения руководителя и офиса всех почтовых контактов из компании-поставщика A. Datum Corporation. Чтобы проверить эти изменения, можно выполнить следующую команду в командной консоли Exchange.

```
PowerShell

Get-Contact -ResultSize unlimited -Filter "Company -eq 'Adatum'" |
Format-List Name,Office,Manager
```

Управление почтовыми пользователями

Статья • 04.04.2023

Пользователи почты сходны с почтовыми контактами. Оба имеют внешние адреса электронной почты и содержат сведения о людях за пределами организации Exchange, которые могут отображаться в общей адресной книге и других списках адресов. Однако, в отличие от почтового контакта, почтовый пользователь имеет учетные данные для входа в вашу организацию Exchange и может получить доступ к ресурсам. Подробнее см. в разделе Recipients.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 2 минуты.
- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения подготовки получателей" раздела Разрешения получателей .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Создание пользователя почты

Использование Центра администрирования Exchange (EAC) для создания пользователя почты

1. В EAC перейдите в раздел **Получатели**>**Контакты**>**Новый**>**пользователь почты**.

2. На странице **Новый почтовый пользователь** в поле *** Псевдоним** введите псевдоним пользователя почты. Псевдоним не может превышать 64 символов и должен быть уникальным в лесу. Оно является обязательным.

3. Чтобы указать тип адреса электронной почты для пользователя почты, выполните одно из следующих действий.

    - Чтобы указать адрес SMTP электронной почты для внешнего адреса электронной почты пользователя почты, щелкните **SMTP**.

    > ⓘ **Примечание**
    >
    > Exchange проверяет правильность формата адресов SMTP. Если запись не соответствует формату SMTP, на экран будет выведено сообщение об ошибке после нажатия кнопки **Сохранить**, чтобы создать пользователя почты.

    - Чтобы указать настраиваемый тип адреса, щелкните переключатель и введите тип настраиваемого адреса. Например, можно указать адрес X.500, GroupWise или Lotus Notes.

4. В поле *** Внешний адрес электронной почты** введите внешний адрес электронной почты пользователя почты. Сообщения электронной почты, отправляемые данному почтовому пользователю, переадресуются на этот адрес электронной почты. Оно является обязательным.

5. Выберите один из приведенных ниже вариантов.

    - **Существующий пользователь**: выберите, чтобы включить отправку почты существующему пользователю.

      Нажмите кнопку **Обзор**, чтобы открыть диалоговое окно **Выбор пользователя — весь лес**. В данном диалоговом окне отображается список учетных записей пользователей в данной организации, для которых не включена поддержка почты или у которых нет почтовых ящиков. Выберите учетную запись пользователя, для которой необходимо включить поддержку почты, а затем нажмите кнопку **OK**. При выборе этого параметра не требуется указывать данные учетной записи пользователя, потому что они уже присутствуют в службе Active Directory.

- **Новый пользователь**. Выберите, чтобы создать учетную запись пользователя в Active Directory и включить почту пользователя. В случае выбора этой опции необходимо указать необходимые данные учетной записи пользователя.

6. Если вы выбрали **Новый пользователь** на шаге 5, заполните следующие сведения на странице **Новый почтовый пользователь** . В противном случае перейдите к шагу 7.

    - **Имя**. Введите имя пользователя почты.
    - **Инициалы**. Введите инициалы почтового пользователя.
    - **Фамилия**: введите фамилию пользователя почты.
    - * **Отображаемое имя**: используйте это поле, чтобы ввести отображаемое имя пользователя. Это имя указывается в списке контактов Центра администрирования Exchange и адресной книге вашей организации. По умолчанию в это поле добавляются имена, введенные в полях **Имя**, **Инициалы** и **Фамилия**. Если эти поля не используются, все равно необходимо ввести имя в это поле, поскольку оно является обязательным для заполнения. Длина имени не может превышать 64 символов.
    - * **Имя**: используйте это поле, чтобы ввести имя пользователя почты. Это имя, которое указано в службе каталогов. В это поле также добавляются имена, введенные в поля **Имя**, **Отчество** и **Фамилия**. Если вы не использовали эти поля, все равно необходимо ввести имя, так как это обязательно. Кроме того, длина имени не может превышать 64 символа.
    - **Подразделение**. Вы можете выбрать подразделение, отличное от стандартного (который является областью получателя). Если область получателей установлена на уровне леса, то значение по умолчанию настроено в контейнере пользователей в домене, содержащем компьютер под управлением Центра администрирования Exchange. Если область получателей настроена на определенный домен, то контейнер пользователей в этом домене выбирается по умолчанию. Если в качестве области получателей задано определенное подразделение организации, то оно выбирается по умолчанию.

      Нажмите кнопку **Обзор**, чтобы выбрать другое подразделение. В этом диалоговом окне отображаются все подразделения в лесу, которые

находятся внутри определенной области. Выберите нужное подразделение и нажмите кнопку **OK**.

- * **Имя входа пользователя**. Введите имя, которое почтовый пользователь будет использовать для входа в домен. Имя входа пользователя состоит из имени пользователя в левой части символа (@) и суффикса в правой части. Обычно в качестве суффикса выступает имя домена, в котором размещается учетная запись пользователя.

- * **Новый пароль**. Введите пароль, который пользователь почты должен использовать для входа в домен. Убедитесь, что введенный пароль соответствует требованиям к длине, сложности и журналу паролей, предъявляемым для домена, в котором создается учетная запись пользователя.

- * **Подтверждение пароля**. Используйте это поле для подтверждения пароля, введенного в поле **Пароль** .

- **Требовать изменение пароля при следующем входе**. Установите этот флажок, если вы хотите, чтобы почтовые пользователи сбрасывали пароль при первом входе в домен.

  Если этот флажок установлен, при первом входе нового пользователя почты будет отображено диалоговое окно, в котором необходимо изменить пароль. Пользователь почты не сможет выполнять никакие задачи, пока пароль не будет успешно изменен.

7. Когда вы закончили, нажмите кнопку **Сохранить**, чтобы создать пользователя почты.

Создание почтового пользователя с помощью командной консоли Exchange

В этом примере создается учетная запись пользователя с поддержкой почты для Jeffrey Zeng в Exchange Server 2016 г. со следующими сведениями:

- Имя и отображаемое имя — Григорий Иванов.
- Псевдоним — gregoryiv.
- Внешний адрес электронной почты — jzeng@tailspintoys.com.
- Имя — Григорий, фамилия — Иванов.

- Имя входа — jeffreyz@contoso.com.
- Пароль — Pa$$word1.
- Пользователь почты будет создан в подразделении по умолчанию. Чтобы указать другое подразделение, можно использовать параметр *OrganizationalUnit* .

PowerShell

```
New-MailUser -Name "Jeffrey Zeng" -Alias jeffreyz -ExternalEmailAddress
jzeng@tailspintoys.com -FirstName Jeffrey -LastName Zeng -UserPrincipalName
jeffreyz@contoso.com -Password (ConvertTo-SecureString -String 'Pa$$word1' -
AsPlainText -Force)
```

Подробные сведения о синтаксисе и параметрах см. в разделе New-MailUser.

Как проверить, все ли получилось?

Чтобы убедиться, что пользователь почты создан успешно, выполните одно из следующих действий.

- В EAC перейдите к **разделу Получатели**>**Контакты**. Новый пользователь почты отображается в списке контактов. В разделе **Тип контакта** указан тип **Пользователь почты**.
- В командной консоли Exchange выполните следующую команду, чтобы отобразить сведения о новом почтовом пользователе.

  PowerShell

  ```
  Get-MailUser <Name> | Format-List
  Name,RecipientTypeDetails,ExternalEmailAddress
  ```

Изменение свойств пользователя почты

После создания почтового пользователя можно внести изменения и задать дополнительные свойства с помощью EAC или командной консоли Exchange.

Также можно одновременно менять свойства нескольких почтовых ящиков пользователей. Дополнительные сведения см . в статье Использование EAC для массового редактирования пользователей почты.

Время выполнения этой задачи зависит от количества свойств, которые нужно просмотреть или изменить.

Использование Центра администрирования Exchange для настройки свойств почтового ящика пользователя

1. В EAC перейдите к **разделу Получатели**>**Контакты**.
2. В списке контактов выберите пользователя почты, для которого нужно изменить свойства, а затем нажмите кнопку **Изменить**.✎
3. На странице свойств пользователя почты щелкните один из следующих разделов, чтобы просмотреть или изменить свойства.
    - Общие
    - Контактные данные
    - Организация
    - Адреса электронной почты
    - Параметры потока почты
    - Участник
    - Подсказка

Общие сведения

В разделе **Общие** можно просматривать или изменять основные сведения о пользователе почты.

- **Имя**, **Отчество**, **Фамилия**
- * **Имя**: это имя, указанное в Active Directory. Если вы решите изменить это имя, помните, что оно не может превышать 64 символа.
- * **Отображаемое имя**: это имя отображается в адресной книге вашей организации, в строках "До" и "От": в сообщении электронной почты, а также в списке контактов в EAC. Это имя не может содержать пробелы до или после отображаемого имени.
- * **Имя входа пользователя**. Это имя, которое пользователь использует для входа в домен.

- **Скрыть из списков адресов**. Установите этот флажок, чтобы запретить отображение почтового пользователя в адресной книге и других списках адресов, определенных в вашей организации Exchange. После установки этого флажка пользователи все еще могут отправлять сообщения этому получателю на его адрес электронной почты.

- **Требовать смену пароля при следующем входе**. Установите этот флажок, если вы хотите, чтобы пользователь сбросил пароль при следующем входе в домен.

Щелкните **Дополнительные параметры**, чтобы просмотреть или изменить дополнительные свойства:

- **Подразделение**. В этом поле только для чтения отображается подразделение, содержащее учетную запись почтового пользователя. Чтобы переместить учетную запись в другое подразделение, используйте оснастку "Active Directory — пользователи и компьютеры".

- **Настраиваемые атрибуты**. В этом разделе отображаются настраиваемые атрибуты, определенные для пользователя почты. Чтобы указать значения настраиваемых атрибутов, нажмите кнопку **Изменить**. Для получателя можно указать до 15 настраиваемых атрибутов.

Контактные данные

В разделе **Сведения о контактах** можно просмотреть или изменить контактные данные пользователя. Информация на этой странице отображается в адресной книге. Нажмите кнопку **Дополнительные сведения** для отображения дополнительных полей.

> **Совет**
>
> Поле **Область/Край** можно использовать, чтобы создать условия получателей для образования динамической группы рассылки, политики адресов электронной почты или списка адресов.

Организация

В разделе **Организация** можно указать подробные сведения о роли пользователя в организации. Эти данные отображаются в адресной книге. Кроме того, можно

создать виртуальную организационную диаграмму, доступную из клиентов электронной почты, таких как Outlook.

- Вкладка **Организация** используется для просмотра и изменения сведений о роли получателя в организации.
- **Отдел**. Используйте это поле для просмотра или изменения отдела, в котором работает пользователь. Это поле можно использовать, чтобы создавать условия получателей для динамических групп рассылки, политик адресов электронной почты или списков адресов.
- **Компания**. Используйте это поле для просмотра или изменения компании, в которой работает пользователь. Это поле можно использовать, чтобы создавать условия получателей для динамических групп рассылки, политик адресов электронной почты или списков адресов.
- **Диспетчер**. Чтобы добавить руководителя, нажмите кнопку **Обзор**. В окне **Выбор руководителя** выберите соответствующего человека и нажмите кнопку **OK**.
- **Прямые отчеты**. Изменить это поле нельзя. *Подчиненный* — это пользователь, подотчетный определенному руководителю. Если вы указали руководителя для пользователя, он отображается как прямой отчет в сведениях о почтовом ящике руководителя. Например, Кари управляет Крисом и Кейт, поэтому Кари указывается в поле **Менеджер** для Криса и Кейт, а Крис и Кейт отображаются в поле **Прямые отчеты** в свойствах учетной записи Кари.

Адреса электронной почты

В разделе **Адреса электронной почты** можно просмотреть или изменить адреса электронной почты, связанные с пользователем почты. Это включает основной адрес SMTP пользователя почты, внешний адрес электронной почты пользователя и все связанные прокси-адреса. Основной адрес SMTP (также называется *адрес ответа по умолчанию*) отображается жирным шрифтом в списке адресов со значением **SMTP** (прописными буквами) в столбце **Тип**. По умолчанию после создания пользователя почты основной адрес SMTP и внешний адрес электронной почты совпадают.

- **Добавить: щелкните**➕ чтобы добавить новый адрес электронной почты для этого почтового ящика. Выберите один из следующих типов адресов:
  - **SMTP**. Это тип адреса по умолчанию. Нажмите эту кнопку, а затем введите новый адрес SMTP в поле ***Адрес электронной почты**.

- **Пользовательский тип адреса**. Нажмите эту кнопку и введите один из поддерживаемых типов адресов электронной почты, **отличных от** SMTP, в поле *Email адрес.

  Примечание. За исключением адресов X.400, Exchange не проверяет пользовательские адреса на правильность форматирования. Чтобы добавить настраиваемый адрес (например, факс или X.400), нажмите эту кнопку и используйте соответствующее диалоговое окно.

- **Задайте внешний адрес электронной почты**. Используйте это поле, чтобы изменить внешний адрес почтового пользователя. Сообщения электронной почты, отправляемые данному почтовому пользователю, переадресуются на этот адрес электронной почты.

- **Автоматически обновлять адреса электронной почты на основе политики адресов электронной почты, которая применяется к этому получателю**. Установите этот флажок, чтобы адреса электронной почты получателей автоматически обновлялись на основе изменений политики адресов электронной почты организации. По умолчанию этот флажок установлен.

Параметры потока почты

В разделе **Параметры потока почты** можно просмотреть или изменить такие параметры:

- **Ограничения размера сообщений**. Эти параметры определяют размер сообщений, которые пользователь может отправлять и получать. Щелкните **Подробнее**, чтобы просмотреть и изменить максимальный размер отправленных и полученных сообщений.

  - **Отправленные сообщения**. Чтобы указать максимальный размер сообщений, отправленных этим пользователем, установите флажок **Максимальный размер сообщения (КБ)** и введите в поле значение. Размер сообщений должен находиться в диапазоне от 0 до 2 097 151 КБ. Если размер отправляемого пользователем сообщения превышает указанный размер, оно будет возвращено отправителю с соответствующим сообщением об ошибке.

  - **Полученные сообщения**. Чтобы указать максимальный размер сообщений, полученных этим пользователем, установите флажок **Максимальный размер сообщения (КБ)** и введите значение в поле . Размер сообщений должен находиться в диапазоне от 0 до 2 097 151 КБ. Если пользователь получает сообщение, размер которого превышает установленное

значение, это сообщение будет возвращено отправителю с описательным сообщением об ошибке.

- **Ограничения доставки сообщений**. Эти параметры определяют, кто может отправлять сообщения электронной почты этому пользователю почты. Щелкните **Подробнее**, чтобы просмотреть и изменить эти ограничения.

  - **Принять сообщения из**: используйте этот раздел, чтобы указать, кто может отправлять сообщения этому пользователю.

  - **Все отправители**. Выберите этот параметр, чтобы указать, что пользователь может принимать сообщения от всех отправителей. Сюда относятся отправители из вашей организации Exchange и внешние отправители. Этот вариант выбран по умолчанию. Этот параметр включает внешних пользователей, только если снят флажок **Требовать проверку подлинности всех отправителей**. Если этот флажок установлен, сообщения от внешних пользователей будут отклоняться.

  - **Только отправители в следующем списке**. Выберите этот параметр, чтобы указать, что пользователь может принимать сообщения только от указанного набора отправителей в организации Exchange. **Щелкните**➕ Чтобы открыть страницу **Выбор получателей**, на которой отображается список всех получателей в организации Exchange. Выберите нужных получателей, добавьте их в список и нажмите **OK**. Вы также можете выполнить поиск определенного получателя, введя имя получателя в поле поиска и щелкнув 🔎.

  - **Требовать проверку подлинности всех отправителей**. Выберите этот параметр, чтобы запретить анонимным пользователям отправлять сообщения пользователю.

  - **Отклонить сообщения из**: используйте этот раздел, чтобы запретить пользователям отправлять сообщения этому пользователю.

  - **Нет отправителей**. Выберите этот параметр, чтобы указать, что почтовый ящик не будет отклонять сообщения от отправителей в организации Exchange. Этот вариант выбран по умолчанию.

  - **Отправители в следующем списке**. Выберите этот параметр, чтобы указать, что почтовый ящик будет отклонять сообщения от указанного набора отправителей в организации Exchange. **Щелкните**➕ Чтобы открыть страницу **Выбор получателей**, на которой отображается список всех получателей в организации Exchange. Выберите нужных получателей,

добавьте их в список и нажмите **OK**. Вы также можете выполнить поиск определенного получателя, введя имя получателя в поле поиска и щелкнув 🔎.

Участник

Используйте раздел **Member Of** для просмотра списка групп рассылки или групп безопасности, к которым принадлежит этот пользователь. На этой странице нельзя изменять сведения о членстве. Обратите внимание, что пользователь может соответствовать критериям для одной или нескольких динамических групп рассылки в вашей организации. Однако динамические группы рассылки не отображаются на этой странице, так как их членство вычисляется при каждом использовании.

Подсказка

Используйте раздел **Подсказка** для добавления подсказок, предупреждающих пользователей о возможных проблемах при отправке сообщения этому получателю. Подсказка — это текст, который отображается на панели информации при добавлении этого получателя в поля "Кому", "Копия" и "Скрытая копия" нового сообщения электронной почты.

> ⓘ **Примечание**
>
> Подсказки могут содержать HTML-теги, но сценарии не допускаются. Длина пользовательской подсказки не должна превышать 175 отображаемых символов. HTML-теги при этом не учитываются.

Изменение свойств пользователя почты с помощью командной консоли Exchange

Свойства пользователя почты хранятся в службах Active Directory и Exchange. Как правило используйте командлеты **Get-User** и **Set-User**, чтобы просматривать и изменять свойства организации и контактных данных. Используйте командлеты **Get-MailUser** и **Set-MailUser**, чтобы просматривать или изменять свойства, связанные с почтой, например адреса электронной почты, подсказки, настраиваемые атрибуты, и указать, скрывать ли пользователя почты из списков адресов.

Используйте командлеты **Get-MailUser** и **Set-MailUser**, чтобы просмотреть и изменить свойства для пользователей почты. Дополнительные сведения см. в следующих разделах:

- Get-User
- Set-User
- Get-MailUser
- Set-MailUser

Ниже приведены некоторые примеры использования командной консоли Exchange для изменения свойств пользователя почты.

В этом примере настраивается внешний адрес электронной почты для пользователя Марты Артемьевой.

PowerShell

```
Set-MailUser "Pilar Pinilla" -ExternalEmailAddress pilarp@tailspintoys.com
```

В этом примере из адресной книги организации скрываются все пользователи почты.

PowerShell

```
Get-MailUser | Set-MailUser -HiddenFromAddressListsEnabled $true
```

В этом примере значение "Компания" задано как Contoso для всех почтовых пользователей.

PowerShell

```
Get-User -ResultSize unlimited -Filter "RecipientTypeDetails -eq 'mailuser'"
| Set-User -Company Contoso
```

В этом примере значение ContosoEmployee настраивается для свойства CustomAttribute1 для всех пользователей почты, для которых в свойстве компании указано значение Contoso.

PowerShell

```
Get-User -ResultSize unlimited -Filter "(RecipientTypeDetails -eq
'mailuser') -and (Company -eq 'Contoso')" | Set-MailUser -CustomAttribute1
```

```
ContosoEmployee
```

Подробные сведения о синтаксисе и параметрах см. в разделе Set-MailUser.

Как проверить, все ли получилось?

Чтобы убедиться, что свойства для пользователей почты изменены успешно, выполните следующие действия.

- В EAC выберите почтового пользователя и нажмите ✎ чтобы просмотреть измененное свойство.
- В командной консоли Exchange используйте командлеты **Get-User** и **Get-MailUser** , чтобы проверить изменения. Одно из преимуществ использования командной консоли Exchange состоит в том, что можно просматривать несколько свойств для нескольких почтовых контактов.

  PowerShell

  ```
  Get-MailUser | Format-List Name,CustomAttribute1
  ```

  В примере ранее, в котором значение Contoso было настроено для свойства компании для всех контактов почты, выполните следующую команду, чтобы проверить изменения:

  PowerShell

  ```
  Get-User -ResultSize unlimited -Filter "RecipientTypeDetails -eq
  'mailuser'" | Format-List Name,Company
  ```

  В примере ранее, в котором значение ContosoEmployee было настроено для свойства CustomAttribute1 для всех пользователей почты, выполните следующую команду, чтобы проверить изменения.

  PowerShell

  ```
  Get-MailUser | Format-List Name,CustomAttribute1
  ```

Массовое изменение пользователей почты

С помощью Центра администрирования Exchange (EAC) можно также изменять выбранные свойства для нескольких пользователей почты. При выборе двух и

более пользователей почты в списке контактов в Центре администрирования Exchange (EAC) свойства, которые можно изменить массово, отображены в области сведений. При изменении одного из свойств это изменение применяется ко всем выбранным получателям.

При массовом изменении пользователей почты можно изменить следующие области свойств:

- **Контактные сведения**: В этом поле можно изменить общие свойства, такие как название улицы, почтовый индекс и название города.
- **Организация**. Измените общие свойства, такие как название отдела, название компании и руководителя, которому сообщают выбранные почтовые контакты или почтовые пользователи.

Использование Центра администрирования Exchange (EAC) для массового изменения пользователей почты

1. В EAC перейдите к **разделу Получатели**>**Контакты**.
2. В списке контактов выберите два или более пользователя почты. Нельзя выполнять массовое редактирование группы из почтовых контактов и почтовых пользователей.

   Примечание. Вы можете выбрать нескольких смежных пользователей почты, удерживая нажатой клавишу SHIFT и щелкнув первого пользователя почты, а затем щелкнув последнего пользователя почты, которого вы хотите изменить. Вы также можете выбрать несколько пользователей почты, удерживая нажатой клавишу CTRL и щелкнув каждого пользователя, который нужно изменить.
3. В области сведений в разделе **Групповое изменение** выберите **Обновить** для **Контактные сведения** или **Организация**.
4. Внесите необходимые изменения на странице свойств, а затем сохраните изменения.

Как проверить, все ли получилось?

Чтобы убедиться, что массовое изменение пользователей почты проведено успешно, выполните одно из следующих действий.

- В EAC выберите каждого из пользователей почты, которых вы массово редактировали, и нажмите кнопку **Изменить** чтобы просмотреть измененные свойства.

- В командной консоли Exchange используйте командлет **Get-User** для проверки изменений. Например, выполнено следующее массовое изменение компонента: для всех пользователей почты из компании-поставщика A. Datum Corporation с помощью Центра администрирования Exchange (EAC) был изменен руководитель и офис. Чтобы проверить эти изменения, можно выполнить следующую команду в командной консоли Exchange:

  PowerShell

  ```
  Get-User -ResultSize unlimited -Filter "(RecipientTypeDetails -eq
  'mailuser') -and (Company -eq 'Adatum')" | Format-List
  Name,Office,Manager
  ```

Создание почтовых ящиков помещений и управление ими

Статья • 18.10.2023

Почтовый ящик помещения — это почтовый ящик ресурса, назначенный физическому местоположению, например конференц-залу, аудитории или учебному классу. Пользователи могут резервировать эти помещения, добавляя почтовые ящики помещений в приглашения на собрания. При этом почтовый ящик помещения использует настраиваемые параметры, с помощью которых вы можете принять или отклонить приглашение.

Чтобы создать почтовый ящик помещения, вы должны быть администратором и состоять в группе ролей Organization Management или Recipient Management.

Если вы хотите, чтобы пользователь мог напрямую управлять календарем помещения, предоставьте ему доступ к почтовому ящику помещения, воспользовавшись инструкциями в статье Управление разрешениями для получателей. После этого пользователь сможет открыть почтовый ящик, воспользовавшись инструкциями в статье Открытие и использование общего почтового ящика в Outlook для Windows .

ВАЖНО Почтовые ящики комнат никогда не должны быть заданы в качестве организатора собрания. Комнаты следует добавлять в собрания, только включив их в поля "Участник" или "Расположение".

Также не рекомендуется использовать разрешения полного доступа для непосредственного управления ответом календарей ресурсов на приглашение на собрание. В случаях, когда пользователю необходимо управлять календарем ресурсов, он должен быть предоставлен пользователю напрямую как общий календарь. Пользователь может принять приглашение общего доступа, чтобы добавить календарь, чтобы начать управление собраниями комнаты. Если к календарю комнаты предоставлен общий доступ с разрешениями делегата, пользователь также будет получать копии всех приглашений на собрание, отправленных в комнату в своем собственном почтовом ящике.

Предоставление пользователю общего доступа к календарю комнаты не препятствует включению параметра *Автопринятие* в комнате. Если календарь комнаты является общим и включен *автоматический прием* , запросы будут приниматься по умолчанию, но ответ всегда может быть изменен любым пользователем с разрешениями редактора или делегирования для календаря комнаты. Если ваша организация хочет использовать почтовый ящик помещения в

качестве календаря, рассмотрите возможность использования функций общего календаря Exchange.

Сведения о типах получателей, доступных в Exchange Server, см. в статье Получатели. Сведения о других типах почтовых ящиков ресурсов см. в статье Управление почтовыми ящиками оборудования.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Чтобы открыть Центр администрирования Exchange, см. статью Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения подготовки получателей" раздела Разрешения получателей .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.
- Если вы используете почтовые ящики комнат или оборудования в Microsoft 365 или Office 365, дополнительные сведения см. в разделе Почтовые ящики комнат и оборудования.

> ⓘ **Важно!**
>
> Если вы используете Exchange 2013 в гибридном сценарии, убедитесь, что вы создали почтовые ящики помещений в соответствующем месте. Создайте почтовые ящики комнат для локальной организации, а почтовые ящики комнат для Exchange Online должны создаваться в облаке. Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Создание почтового ящика помещения

1. В Центре администрирования Exchange перейдите в раздел **Ресурсы получателей**>.

2. Чтобы создать почтовый ящик комнаты, нажмите ➕>**Почтовый ящик комнаты**.

3. С помощью указанных на странице опций задайте параметры для нового почтового ящика ресурса.

    - **Название помещения**. Поле для ввода названия почтового ящика помещения. Это название, указываемое в списке почтовых ящиков ресурсов в Центре администрирования Exchange и адресной книге организации. Это название является обязательным и не может превышать в длину 64 символов.

    > **Совет**
    >
    > Хотя сведения о помещении включают и другие поля, например "Местоположение" и "Вместительность", стоит указывать самые важные сведения о помещении в имени, используя согласованную схему именования. Почему? При этом пользователи смогут видеть сведения при выборе помещения в адресной книге в приглашении на собрание.

    - **Псевдоним**. У почтового ящика помещения есть адрес электронной почты, на который отправляются запросы на резервирование. Он состоит из псевдонима слева от символа @ (псевдоним должен быть уникален в пределах леса) и доменного имени справа от этого символа. Указывать псевдоним обязательно.

    - **Местоположение**, **Телефон**, **Вместительность**. В этих полях задаются сведения о помещении. Тем не менее, как объяснялось ранее, все или некоторые из этих сведений можно включить в имя помещения, чтобы пользователи могли их видеть.

4. По завершении нажмите кнопку **Сохранить**, чтобы создать почтовый ящик помещения.

После этого вы можете Настройка обработки приглашений на собрания почтовым ящиком помещения (в том числе выбрать автоматическую обработку или назначить ответственного за это). По умолчанию приглашения принимаются или отклоняются автоматически в зависимости от того, конфликтуют ли они с уже запланированными собраниями в календаре. В частности, принимаются приглашения на повторяющиеся собрания и собрания продолжительностью не более 24 часов, до которых остается не более 180 дней (приглашения на более

поздние собрания отклоняются). Чтобы изменить другие параметры, перейдите к разделу Изменение других свойств почтового ящика помещения.

Сведения о том, как создать почтовый ящик помещения с помощью командной консоли Exchange, см. в примерах 2 и 3 из статьи New-Mailbox.

Настройка обработки приглашений на собрания почтовым ящиком помещения

1. В Центре администрирования Exchange перейдите в раздел **Ресурсы получателей**>.

2. В списке почтовых ящиков ресурсов щелкните почтовый ящик комнаты, для которого требуется изменить свойства, а затем щелкните **Изменить**.✎

3. На странице свойств почтового ящика комнаты выберите **Пункты резервирования делегатов** (разрешить автоматические ответы или нет) или **Параметры резервирования** (разрешить повторяющиеся собрания, отклонить собрания, запланированные слишком далеко, и т. д.).

В разделе **Резервирование представителей** вы можете просмотреть и изменить реакцию почтового ящика размещения на запросы резервирования и указать, кто сможет принимать или отклонять запросы на резервирование, если это не происходит автоматически.

- Выберите один из приведенных ниже вариантов обработки приглашений на собрания.

    - **Запросы на резервирование принимаются или отклоняются автоматически**. Если выбран этот вариант, приглашения на собрания автоматически отклоняются при возникновении конфликтов в расписании или нарушении ограничений, установленных для ресурса (например, превышении допустимой продолжительности).

    - **Выбрать делегатов, которые могут принимать и отклонять запросы на резервирование**. Если выбран этот вариант, один из пользователей, добавленных в расположенный ниже список **Делегаты**, будет отвечать за принятие и отклонение приглашений на собрания, отправляемых в почтовый ящик помещения. Если назначено несколько делегатов ресурса, только один из них должен будет отреагировать на то или иное приглашение.

Используйте раздел **Параметры резервирования** для просмотра или изменения параметров политики резервирования, которая определяет, когда можно запланировать помещение, как надолго его можно зарезервировать и насколько рано это можно сделать.

- **Разрешить повторяющиеся собрания**. Этот параметр разрешает или запрещает повторяющиеся собрания для помещения.

- **Разрешить планирование только в рабочее время**. Этот параметр принимает или отклоняет приглашения на собрания, которые не выполняются в рабочее время, определенное для комнаты. По умолчанию с 8:00 до 17:00 с понедельника по пятницу. Вы можете настроить рабочее время почтового ящика помещения, войдя в почтовый ящик с помощью Outlook в Интернете и перейдя на страницу**внешнего вида календаряПараметры**>**календаря**> или с помощью Set-MailboxCalendarConfiguration.

- **Всегда отклонять, если конечная дата выходит за рамки этого ограничения**. Этот параметр управляет поведением повторяющихся собраний, выходящих за дату, указанную как максимальное время упреждения при резервировании.

  - Если включить этот параметр, запрос на повторяющееся бронирование автоматически отклоняется, если бронирование начинается не позже даты, указанной в поле **Максимальное время начала бронирования**, и выходит за указанную дату. Это устанавливается по умолчанию.

  - Если отключить этот параметр, запрос на повторяющееся бронирование автоматически принимается, если эти запросы начинаются не позже даты, указанной в поле **Максимальное время начала бронирования**, и выходят за указанную дату. Однако при этом количество бронирований сокращается, поэтому они не состоятся после указанной даты.

- **Максимальное время упреждения при резервировании (в днях)**. Этот параметр задает максимальное количество дней, за которое можно зарезервировать помещение. Допустимый диапазон — целое число от 0 до 1080. Значение по умолчанию составляет 180 дней.

- **Максимальная продолжительность (в часах)**. Этот параметр задает максимальную продолжительность, на которую можно зарезервировать помещение в запросе на резервирование. Допустимое значение ——— целое число от 0 до 35791394. Значение по умолчанию составляет 24 часа. Если установлено значение 0, продолжительность собрания не ограничивается.

Для повторяющихся запросов максимальная продолжительность относится к продолжительности каждого повторения бронирования.

На этой станице также есть поле для ввода сообщения, которое будет отправляться пользователям, посылающим запросы на бронирование помещения.

Изменение параметров планирования ресурса

Администратор или пользователь с полным доступом к почтовому ящику ресурса может вносить изменения в параметры планирования ресурса.

1. Войдите в Outlook Web App и щелкните **Ваше имя** в правом верхнем углу.
2. Щелкните **Открыть другой почтовый ящик**. Найдите нужный ресурс помещения для собрания и нажмите **Открыть**.
3. Перейдите в **Параметры** и щелкните **Календарь**.
4. Перейдите в раздел **Планирование ресурсов**.
5. Настройте параметры планирования и разрешения планирования нужным образом. (Подробные описания всех параметров см. в следующих двух разделах.)
6. Нажмите **Сохранить** после внесения изменений.

Параметры резервирования

- **Автоматически обрабатывать приглашения на собрания и отказы**

Включает или отключает все параметры ниже, а также параметры в разделе разрешений планирования. Если этот флажок не установлен, владелец должен управлять каждым запросом вручную. По умолчанию этот флажок не установлен.

- **Отключить оповещения**

Включает или отключает напоминания о событиях в этом календаре. Этот параметр применяется только к ресурсу. Организатор и участники по-прежнему будут получать напоминания, если они согласились с ними.

- **Максимальный срок предварительного резервирования ресурсов (дн.)**

Ограничивает максимальный срок предварительного планирования события. Значение по умолчанию составляет 180 дней.

- **Всегда отклонять, если конечная дата выходит за рамки этого ограничения**

Запросы, превышающие указанное максимальное количество дней, будут автоматически отклоняться. Допустимые значения: от 0 (сегодня) до 1080 (около трех лет в будущем).

- **"Ограничивает продолжительность собрания" и "Максимальное разрешенное количество минут"**

Ограничивает количество времени, на которое можно зарезервировать помещение в течение одного дня. Если этот флажок не установлен, для помещения отсутствует ограничение. Установив этот флажок, можно выбрать ограничение от 0 до 1440 минут.

- **Разрешить планирование только в рабочее время**

Если этот флажок установлен, событие можно запланировать только в течение часов, указанных в календаре рабочей недели на вкладке "Календарь". События за пределами рабочего времени будут автоматически отклоняться.

- **Разрешить повторяющиеся собрания**

Разрешает резервирование помещения с регулярным интервалом. Событие можно настроить на повторение через указанный промежуток времени (часто называется повторяющимся).

- **Разрешить конфликты**

Разрешение или запрет конфликтующих приглашений на собрания (двойное резервирование). Если повторяющиеся собрания также разрешены, этот параметр будет применяться только к повторяющимся собраниям. Если приглашается ресурс, его требуется ввести в поле "Участники" вместо выбора с помощью кнопки "Добавить помещения".

- **Разрешить не более следующего количества индивидуальных конфликтов**

Этот параметр указывает максимальное количество конфликтов, допустимых для новых приглашений на повторяющиеся собрания. Когда присвоено значение "0", повторяющееся событие не удастся запланировать, если уже существует одна или несколько конфликтующих встреч. Если указано число больше 0, для повторяющегося события разрешается указанное количество конфликтов до отклонения.

- **Разрешить такой процент индивидуальных конфликтов**

Этот параметр указывает максимальный процент конфликтов собраний, допустимых для новых приглашений на повторяющиеся собрания. Это аналогично указанию количества индивидуальных конфликтов (описано выше), но в этом случае для повторяющегося события разрешается указанный процент конфликтов до отклонения.

Разрешения резервирования

- **Эти пользователи могут выполнять автоматическое планирование, если ресурс доступен**

По умолчанию все могут планировать этот ресурс без утверждения вручную владельцем ресурса. Если выбран параметр **Выбрать пользователей и группы**, только указанные пользователи и группы смогут осуществлять автоматическое планирование. Все остальные пользователи и группы получать сообщение об отклонении. Если выбран параметр **Выбрать пользователей и группы**, но не указаны пользователи и группы, этот параметр игнорируется.

- **Эти пользователи могут отправить запрос на утверждение владельца, если ресурс доступен**

Если выбраны все пользователи, любые запросы должны утверждаться вручную владельцем ресурса. Если выбран параметр **Выбрать пользователей и группы**, только для указанных пользователей и групп потребуется ручное утверждение владельцем ресурса. Параметр **Выбрать пользователей и группы** выбран и оставлен пустым по умолчанию, чтобы все запросы утверждались автоматически.

- **Эти пользователи могут выполнять автоматическое планирование, если ресурс доступен, и отправлять запрос на утверждение владельца, если ресурс недоступен**

Если выбраны все пользователи (параметр по умолчанию), любой запрос в рабочее время будет утверждаться автоматически. Если помещение зарезервировано на запрошенное время, владельцу ресурса отправляется форма на утверждение вручную. Если выбран параметр **Выбрать пользователей и группы**, только указанные в списке получат возможность на утверждение запроса вручную. Для всех остальных конфликтующие запросы будут отклонены без возможности утверждения вручную владельцем ресурса.

Изменение других свойств почтового ящика помещения

После создания почтового ящика помещения вы можете изменять и добавлять свойства с помощью Центра администрирования Exchange или командной консоли Exchange.

Использование Центра администрирования Exchange для изменения свойств почтового ящика помещения

1. В Центре администрирования Exchange перейдите в раздел **Ресурсы получателей**>.
2. В списке почтовых ящиков ресурсов щелкните почтовый ящик комнаты, для которого требуется изменить свойства, а затем щелкните **Изменить**.✎
3. На странице свойств почтового ящика помещения выберите один из перечисленных ниже разделов, чтобы просмотреть или изменить свойства (параметры резервирования описываются в разделе Настройка обработки приглашений на собрания почтовым ящиком помещения).
    - Общие
    - Контактные данные
    - Адрес электронной почты
    - Подсказка

Общие сведения

Используйте раздел **Общие**, чтобы просмотреть или изменить общие сведения о ресурсе.

- **Название помещения**. Это название отображается в списке почтовых ящиков ресурсов в Центре администрирования Exchange и адресной книге вашей организации. Его длина в случае изменения не может превышать 64 символов.
- **Электронный адрес**. В этом поле, доступном только для чтения, отображается адрес электронной почты почтового ящика помещения. Вы можете изменить его в разделе Адрес электронной почты.

- **Вместительность**. Поле для ввода максимального количества людей для безопасного размещения в помещении.

Щелкните **Дополнительные параметры**, чтобы просмотреть или изменить дополнительные свойства:

- **Подразделение**. Это поле, доступное только для чтения, содержит подразделение, в которое входит учетная запись почтового ящика помещения. Чтобы переместить учетную запись в другое подразделение, используйте оснастку "Active Directory — пользователи и компьютеры".

- **База данных почтовых ящиков**. В этом поле, доступном только для чтения, отображается имя базы данных почтовых ящиков, в которой размещен почтовый ящик помещения. Используйте страницу **Миграция** в Центре администрирования Exchange, чтобы переместить почтовый ящик в другую базу данных.

- **Псевдоним**. Это поле используется для изменения псевдонима почтового ящика помещения.

- **Не отображать в списках адресов**. Установите этот флажок, чтобы почтовый ящик помещения не отображался в адресной книге и других списках адресов, определенных в организации Exchange. После установки этого флажка пользователи все еще могут отправлять сообщения о резервировании на почтовый ящик помещения, используя адрес электронной почты.

- **Отдел**. В этом поле можно указать название отдела, с которым связано помещение. Это свойство можно использовать, чтобы создавать условия получателей для динамических групп рассылки или списков адресов.

- **Компания**. В этом поле можно указать название компании, с которой связано помещение, если это возможно. Как и свойство "Отдел", это свойство можно использовать, чтобы создавать условия получателей для динамических групп рассылки или списков адресов.

- **Политика адресных книг**. Используйте этот параметр, чтобы указать политику адресных книг для почтового ящика помещения. Политики адресных книг содержат глобальный список адресов, автономную адресную книгу, список помещений и набор списков адресов. Дополнительные сведения см. в разделе Политики адресных книг в Exchange Server.

  Из раскрывающегося списка выберите политику, которую нужно сопоставить с этим почтовым ящиком.

- **Настраиваемые атрибуты**. В этом разделе отображаются настраиваемые атрибуты, определенные для почтового ящика помещения. Чтобы указать значения настраиваемых атрибутов, нажмите кнопку **Изменить**✎ Для получателя можно указать до 15 настраиваемых атрибутов.

Контактные данные

В разделе **Контактные данные** можно просмотреть или изменить контактные данные помещения. Информация на этой странице отображается в адресной книге.

> **Совет**
>
> Поле **Область/Край** можно использовать, чтобы создать условия получателей для образования динамической группы рассылки, политики адресов электронной почты или списка адресов.

Адрес электронной почты

В разделе **Адрес электронной почты** можно просмотреть или изменить адреса электронной почты, связанные с почтовым ящиком помещения. Это включает SMTP-адрес основного почтового ящика и все связанные прокси-адреса. Основной адрес SMTP (также известный как *адрес ответа*) отображается жирным шрифтом в списке адресов и прописными буквами **SMTP** в столбце **Тип**.

- **Добавить: щелкните**+ чтобы добавить новый адрес электронной почты для этого почтового ящика. Выберите один из следующих типов адресов:
  - **SMTP**. Это тип адреса по умолчанию. Нажмите эту кнопку и введите новый SMTP-адрес в поле **Электронный адрес**.
  - **EUM**. Адрес EUM (единой системы обмена сообщениями Exchange) используется службой единой системы обмена сообщениями Microsoft Exchange в Exchange 2016 для поиска получателей с включенной поддержкой единой системы обмена сообщениями в организации Exchange. Адреса единой системы обмена сообщениями Exchange содержат добавочный номер и абонентскую группу единой системы обмена сообщениями для пользователя с включенной поддержкой единой системы обмена сообщениями. Нажмите эту кнопки и введите добавочный номер в поле **Адрес/добавочный номер**. Затем нажмите кнопку **Обзор** и

выберите абонентскую группу для почтового ящика. (**Примечание**. Единая система обмена сообщениями недоступна в Exchange 2019.)

- **Пользовательский тип адреса**. Нажмите эту кнопку и введите один из поддерживаемых типов адресов электронной почты (не SMTP) в поле **Электронный адрес**.

  Примечания.

  - В Exchange не выполняется проверка правильности формата настраиваемых адресов (за исключением адресов X.400). Убедитесь, что указанный настраиваемый адрес соответствует требованиям формата для этого типа адреса.

  - При добавлении нового адреса электронной почты вы можете сделать его основным SMTP-адресом.

- **Автоматически обновлять адреса электронной почты на основе политики адресов электронной почты, которая применяется к этому получателю**. Установите этот флажок, чтобы адреса электронной почты получателей автоматически обновлялись на основе изменений политики адресов электронной почты организации.

Подсказка

В разделе **Подсказка** можно добавлять подсказки, чтобы предупредить пользователей о возможных проблемах при отправке запросов бронирования на почтовый ящик помещения. Подсказка — это текст, который отображается на панели информации при добавлении этого получателя в поля "Кому", "Копия" и "Скрытая копия" нового сообщения электронной почты.

> ⓘ **Примечание**
>
> Подсказки могут содержать HTML-теги, но сценарии не допускаются. Длина пользовательской подсказки не должна превышать 175 отображаемых символов. HTML-теги при этом не учитываются.

Изменение свойств почтовых ящиков помещений с помощью командной консоли Exchange

Используйте следующий набор командлетов для просмотра и изменения свойств почтового ящика помещения: командлеты **Get-Mailbox** и **Set-Mailbox** для просмотра и изменения общих свойств и адресов электронной почты почтовых ящиков помещения. Используйте командлеты **Get-CalendarProcessing** и **Set-CalendarProcessing** для просмотра и изменения делегатов и параметров бронирования.

- **Get-User** и **Set-User**. Используйте эти командлеты для просмотра и задания общих свойств, например местоположения, отдела и названия компании.
- **Get-Mailbox** и **Set-Mailbox**. Используйте эти командлеты для просмотра и задания свойств почтовых ящиков, например адресов электронной почты или базы данных почтовых ящиков.
- **Get-CalendarProcessing** и **Set-CalendarProcessing**. Используйте эти командлеты для просмотра и изменения делегатов и параметров резервирования.

Дополнительные сведения об этих командлетах см. в следующих разделах:

- Get-User
- Set-User
- Get-Mailbox
- Set-Mailbox
- Get-CalendarProcessing
- Set-CalendarProcessing

Ниже приведены примеры изменения свойств почтового ящика помещения с помощью командной консоли Exchange.

В этом примере изменяется отображаемое имя, основной SMTP-адрес (называемый обратным адресом по умолчанию) и вместительность помещения. Также предыдущий обратный адрес хранится как адрес прокси-сервера.

PowerShell

```
Set-Mailbox "Conf Room 123" -DisplayName "Conf Room 31/123 (12)" -
EmailAddresses SMTP:Rm33.123@contoso.com,smtp:rm123@contoso.com -
ResourceCapacity 12
```

В этом примере настраиваются почтовые ящики помещения, чтобы можно было планировать запросы на бронирование только в рабочее время, и задается

максимальная продолжительность в 9 часов.

PowerShell

```
Get-Mailbox -ResultSize unlimited -Filter "RecipientTypeDetails -eq
'RoomMailbox'" | Set-CalendarProcessing -ScheduleOnlyDuringWorkHours $true -
MaximumDurationInMinutes 540
```

В этом примере используется командлет **Get-User** для поиска всех почтовых ящиков помещения, которые отвечают частным конференц-залам, а затем — командлет **Set-CalendarProcessing** для отправки запросов на бронирование делегату Робину Вуду, которых их примет или отклонит.

PowerShell

```
Get-User -ResultSize unlimited -Filter "(RecipientTypeDetails -eq
'RoomMailbox') -and (DisplayName -like 'Private*')" | Set-CalendarProcessing
-AllBookInPolicy $false -AllRequestInPolicy $true -ResourceDelegates "Robin
Wood"
```

Создание почтового ящика помещения

Если вы планируете иметь сотни комнат, используйте несколько списков комнат, чтобы упорядочить свои комнаты. Если компания использует несколько зданий с помещениями, которые можно резервировать для собраний, может быть полезно создать список помещений каждого здания. Списки помещений — это специально помеченные группы рассылки, которые можно использовать соответствующим образом. Однако списки помещений можно создавать только в командной консоли Exchange.

> ⓘ **Примечание**
>
> Хотя количество комнат в списке комнат не ограничено, максимальное количество комнат, которое может быть возвращено в запросе на получение списка помещений, составляет 100 (в том числе при создании приглашения на собрание с помощью Microsoft Teams). Возможным решением может быть дополнительное разделение помещений на списки меньшего размера.

> ⓘ **Примечание**

При использовании Microsoft Teams список комнат отображается в случайном порядке. Внутренний процесс получения списка не сортирует выходные данные, поэтому список может быть не в алфавитном порядке.

Использование командной консоли Exchange для создания списка помещений

В этом примере создается список помещений здания 32.

PowerShell

```
New-DistributionGroup -Name "Building 32 Conference Rooms" -
OrganizationalUnit "contoso.com/rooms" -RoomList
```

Использование командной консоли Exchange для добавления помещения в список помещений

В этом примере добавляется помещение confroom3223 к списку помещений здания 32.

PowerShell

```
Add-DistributionGroupMember -Identity "Building 32 Conference Rooms" -Member
confroom3223@contoso.com
```

Использование командной консоли Exchange для преобразования группы рассылки в список помещений

Возможно, группы рассылки, содержащие переговорные, уже созданы. Нет необходимости создавать их заново — их можно быстро превратить в список помещений.

В этом примере выполняется преобразование группы рассылки переговорных комнат здания 34 в список помещений.

PowerShell

```
Set-DistributionGroup -Identity "Building 34 Conference Rooms" -RoomList
```

Как проверить, что все получилось?

Чтобы проверить, успешно ли изменены свойства почтового ящика помещения, выполните следующие действия.

- В Центре администрирования Exchange выберите почтовый ящик и нажмите кнопку **Изменить** ✎ чтобы просмотреть измененное свойство или функцию. В зависимости от измененного свойства оно может отображаться в области "Сведения" выбранного почтового ящика.

- В командной консоли Exchange для проверки изменений используется командлет **Get-Mailbox**. С помощью командной консоли Exchange можно просмотреть несколько свойств нескольких почтовых ящиков. В примере выше, где запросы на бронирование можно спланировать только в рабочее время, а их максимальная продолжительность составляет 9 часов, выполните следующую команду для проверки новых значений.

  PowerShell

  ```
  Get-Mailbox -ResultSize unlimited -Filter "RecipientTypeDetails -eq 'RoomMailbox'" | Get-CalendarProcessing | Format-List Identity,ScheduleOnlyDuringWorkHours,MaximumDurationInMinutes
  ```

Управление почтовыми ящиками оборудования

Статья • 04.04.2023

В Exchange Server *почтовый ящик оборудования — это почтовый* ящик ресурса, назначенный ресурсу, который не является конкретным расположением, например портативным компьютером, проектором, микрофоном или корпоративным автомобилем. После того, как администратор создаст почтовый ящик оборудования, пользователи смогут с легкостью зарезервировать часть оборудования путем включения соответствующего почтового ящика оборудования в приглашение на собрание. Вы можете использовать Центр администрирования Exchange (EAC) и командную консоль Exchange для создания почтового ящика оборудования или изменения свойств почтового ящика оборудования. Дополнительные сведения см. в статье Recipients.

Сведения о другом типе почтового ящика ресурсов, почтовом ящике комнаты, см. в статье Создание почтовых ящиков комнат и управление ими.

Что нужно знать перед началом работы

- Осталось времени до завершения: от 2 до 5 минут.
- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения подготовки получателей" раздела Разрешения получателей .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Создайте почтовый ящик оборудования

Используйте Центр администрирования Exchange (EAC) для создания почтового ящика оборудования

1. В EAC перейдите к **разделу Ресурсы получателей**>.
2. Чтобы создать почтовый ящик оборудования, щелкните **Создать**>**почтовый ящик оборудования**. Чтобы создать почтовый ящик комнаты, щелкните **Создать**>**почтовый ящик комнаты**.
3. С помощью указанных на странице опций задайте параметры для нового почтового ящика ресурса.

    - * **Имя оборудования**: используйте это поле, чтобы ввести имя почтового ящика оборудования. Это имя, указываемое в списке почтовых ящиков ресурсов в центре администрирования Exchange и адресной книге организации. Это название является обязательным и не может превышать в длину 64 символов.

    > **Совет**
    >
    > Хотя сведения о помещении включают и другие поля, например «Вместительность», стоит указывать самые важные сведения в имени оборудования, используя согласованную схему именования. Почему? При этом пользователи смогут видеть сведения при выборе оборудования в адресной книге в приглашении на собрание.

    - * **Email адрес**: почтовый ящик оборудования имеет адрес электронной почты для получения запросов на резервирование. Он состоит из псевдонима слева от символа @ (псевдоним должен быть уникален в пределах леса) и доменного имени справа от этого символа. Адрес электронной почты является обязательным.
4. По завершении нажмите кнопку **«Сохранить»**, чтобы создать почтовый ящик оборудования.

После создания почтового ящика оборудования вы можете изменить почтовый ящик оборудования, чтобы обновить сведения о вариантах бронирования, подсказках и делегатах. Чтобы изменить свойства почтового ящика комнаты,

ознакомьтесь с разделом Изменение свойств почтового ящика оборудования ниже.

Создание почтового ящика оборудования с помощью командной консоли Exchange

В этом примере создается почтовый ящик оборудования со следующими параметрами:

- Почтовый ящик оборудования находится в базе данных почтовых ящиков Mailbox Database 1.
- Именем оборудования является MotorVehicle2, и имя будет отображаться в глобальном списке адресов как Motor Vehicle 2.
- Адрес электронной почты — MotorVehicle2@contoso.com.
- Почтовый ящик относится к подразделению «Оборудование».
- Параметр *Equipment* указывает, что этот почтовый ящик будет создан как почтовый ящик оборудования.

PowerShell

```
New-Mailbox -Database "Mailbox Database 1" -Name MotorVehicle2 -
OrganizationalUnit Equipment -DisplayName "Motor Vehicle 2" -Equipment
```

Дополнительные сведения о синтаксисе и параметрах см. в статье New-Mailbox.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли создан почтовый ящик пользователя, выполните одно из следующих действий.

- В EAC перейдите к **разделу Ресурсы получателей**>. Новый почтовый ящик пользователя отображается в списке почтовых ящиков. В разделе **Тип почтового ящика** указан тип **Оборудование**.
- В командной консоли Exchange выполните следующую команду, чтобы отобразить сведения о новом почтовом ящике оборудования.

  PowerShell

```
Get-Mailbox <Name> | Format-List
Name,RecipientTypeDetails,PrimarySmtpAddress
```

Изменение свойств почтового ящика оборудования

После создания почтового ящика оборудования можно внести изменения и задать дополнительные свойства с помощью EAC или командной консоли Exchange.

Используйте центр администрирования Exchange для настройки свойств почтового ящика оборудования

1. В EAC перейдите к **разделу Ресурсы получателей**>.
2. В списке почтовых ящиков ресурсов щелкните почтовый ящик оборудования, для которого требуется изменить свойства, а затем щелкните **Изменить**.✎
3. На странице свойств почтового ящика оборудования щелкните один из следующих разделов, чтобы просмотреть или изменить свойства.
   - Общие
   - Представители
   - Варианты бронирования
   - Контактные данные
   - Адрес электронной почты
   - Подсказка

Общие сведения

Используйте раздел **Общие**, чтобы просмотреть или изменить общие сведения о ресурсе.

- * **Имя оборудования**. Это имя отображается в списке почтовых ящиков ресурсов в EAC и в адресной книге вашей организации. Его длина в случае изменения не может превышать 64 символов.

- * **Email адрес**. В этом поле только для чтения отображается адрес электронной почты для почтового ящика оборудования. Вы можете изменить его в разделе Адрес электронной почты.

- **Емкость**. Используйте это поле, чтобы ввести максимальное число пользователей, которые могут использовать этот ресурс. Если применимо, например, если почтовый ящик оборудования соответствует компактному автомобилю, можно ввести **4**.

Щелкните **Дополнительные параметры**, чтобы просмотреть или изменить дополнительные свойства:

- **Подразделение**. В этом поле только для чтения отображается подразделение, содержащее учетную запись почтового ящика оборудования. Чтобы переместить учетную запись в другое подразделение, используйте оснастку "Active Directory — пользователи и компьютеры".

- **База данных почтовых ящиков**. В этом поле только для чтения отображается имя базы данных почтовых ящиков, в котором размещается почтовый ящик оборудования. Используйте страницу **Миграция** в центре администрирования Exchange, чтобы переместить почтовый ящик в другую базу данных.

- * **Псевдоним**. Данное поле используется для изменения псевдонима почтового ящика оборудования.

- **Скрыть из списков адресов**. Установите этот флажок, чтобы предотвратить появление почтового ящика оборудования в адресной книге и других списках адресов, определенных в организации Exchange. После установки этого флажка пользователи все еще могут отправлять сообщения о резервировании на почтовый ящик оборудования используя адрес электронной почты.

- **Отдел**. Используйте это поле, чтобы указать имя отдела, с которым связан ресурс. Это свойство можно использовать, чтобы создавать условия получателей для динамических групп рассылки или списков адресов.

- **Компания**. Используйте это поле, чтобы указать компанию, с которым связан ресурс. Как и свойство "Отдел", это свойство можно использовать, чтобы создавать условия получателей для динамических групп рассылки или списков адресов.

- **Политика адресной книги**. Используйте этот параметр, чтобы указать политику адресной книги (АВР) для ресурса. Политики адресных книг содержат глобальный список адресов, автономную адресную книгу, список

помещений и набор списков адресов. Дополнительные сведения см. в разделе Политики адресных книг в Exchange Server.

Из раскрывающегося списка выберите политику, которую нужно сопоставить с этим почтовым ящиком.

- **Настраиваемые атрибуты**. В этом разделе отображаются настраиваемые атрибуты, определенные для почтового ящика оборудования. Чтобы указать значения настраиваемых атрибутов, нажмите кнопку **Изменить**✎. Для получателя можно указать до 15 настраиваемых атрибутов.

Делегаты

В этом разделе можно просмотреть или изменить то, как почтовый ящик оборудования обрабатывает запросы на резервирование и определить, кто может принять или отклонить запросы, если это не будет сделано автоматически.

- **Запросы на резервирование**. Выберите один из следующих вариантов для обработки запросов на резервирование.
  - **Автоматическое принятие или отклонение запросов на резервирование**. Допустимый запрос на собрание автоматически резервирует ресурс. При наличии конфликта с существующим резервированием или в случае, если запрос нарушает условия резервирования ресурса (например, собрание продлится слишком долго), приглашение на собрание автоматически отклоняется.
  - **Выберите делегатов, которые могут принимать или отклонять запросы на резервирование**. Делегаты ресурсов отвечают за принятие или отклонение запросов на собрания, отправляемых в почтовый ящик оборудования. Если назначено несколько делегатов ресурса, только один из них должен будет отреагировать на то или иное приглашение.
- **Делегаты**. Если выбран параметр, требующий отправки запросов на резервирование делегатам, будут перечислены указанные делегаты. Нажмите ➕ или **удалить**➖, чтобы добавить или удалить делегатов из этого списка.

Варианты бронирования

Используйте раздел **Параметры резервирования** для просмотра или изменения параметров политики резервирования, которая определяет запланированное время, возможность и длительность резервирования.

- **Разрешить повторяющиеся собрания**. Этот параметр разрешает или запрещает повторяющиеся собрания для ресурса. По умолчанию этот параметр включен, поэтому повторяющиеся собрания разрешены.

- **Разрешить планирование только в рабочее время**. Этот параметр принимает или отклоняет приглашения на собрания, которые не выполняются в рабочее время, определенное для ресурса. По умолчанию этот параметр отключен, поэтому приглашения на собрания разрешены в нерабочее время. По умолчанию рабочие часы : с 8:00 до 17:00 с понедельника по пятницу. Рабочее время почтового ящика оборудования можно настроить в разделе Внешний вид на странице Календарь.

- **Всегда отклонять, если конечная дата выходит за рамки этого ограничения**. Этот параметр управляет поведением повторяющихся собраний, выходящих за дату, указанную как максимальное время упреждения при резервировании.

    - Если включить этот параметр, запрос на повторяющееся бронирование автоматически отклоняется, если бронирование начинается не позже даты, указанной в поле **Максимальное время начала бронирования**, и выходит за указанную дату. Это устанавливается по умолчанию.

    - Если отключить этот параметр, повторяющийся запрос на бронирование автоматически принимается, если бронирование начинается не позже даты, указанной в поле **Максимальное время начала бронирования**, и выходит за указанную дату. Однако при этом количество бронирований сокращается, поэтому они не состоятся после указанной даты.

- **Максимальное время резервирования (в днях)**: этот параметр указывает максимальное количество дней до того, как можно забронировать ресурс. Допустимый диапазон — целое число от 0 до 1080. Значение по умолчанию составляет 180 дней.

- **Максимальная продолжительность (часы)**: этот параметр указывает максимальную длительность резервирования ресурса в запросе на резервирование. Значение по умолчанию составляет 24 часа.

  Для повторяющихся запросов максимальная продолжительность относится к продолжительности каждого повторения бронирования.

На этой странице также есть окно, в котором можно создать сообщение для отправки пользователям, которые посылают приглашения на собрания для резервирования ресурса.

Контактные данные

В разделе **Сведения о контактах** можно просмотреть или изменить контактные данные ресурса. Информация на этой странице отображается в адресной книге.

> **Совет**
>
> Поле **Область/Край** можно использовать, чтобы создать условия получателей для образования динамической группы рассылки, политики адресов электронной почты или списка адресов.

Адрес электронной почты

В разделе **Адрес электронной почты** можно просмотреть или изменить адреса электронной почты, связанные с почтовым ящиком оборудования. Это включает SMTP-адрес основного почтового ящика и все связанные прокси-адреса. Основной адрес SMTP (также известный как *адрес ответа*) отображается жирным шрифтом в списке адресов и прописными буквами **SMTP** в столбце **Тип**.

- **Добавить: щелкните**+ чтобы добавить новый адрес электронной почты для этого почтового ящика. Выберите один из следующих типов адресов:
  - **SMTP**. Это тип адреса по умолчанию. Нажмите эту кнопку, а затем введите новый адрес SMTP в поле ***Адрес электронной почты**.
  - **EUM**. Адрес единой системы обмена сообщениями Exchange используется службой единой системы обмена сообщениями Exchange в Exchange 2016 для поиска получателей с поддержкой единой системы обмена сообщениями в организации Exchange. Адреса единой системы обмена сообщениями Exchange содержат добавочный номер и абонентскую группу единой системы обмена сообщениями для пользователя с включенной поддержкой единой системы обмена сообщениями. Нажмите эту кнопки и введите добавочный номер в поле **Адрес/добавочный номер**. Затем нажмите кнопку **Обзор** и выберите абонентскую группу для почтового ящика. (**Примечание**. Единая система обмена сообщениями недоступна в Exchange 2019.)
  - **Пользовательский тип адреса**. Нажмите эту кнопку и введите один из поддерживаемых типов адресов электронной почты, **отличных от** SMTP, в поле *Email адрес.

    Примечания.

    - В Exchange не выполняется проверка правильности формата настраиваемых адресов (за исключением адресов X.400). Убедитесь, что указанный настраиваемый адрес соответствует требованиям формата для этого типа адреса.
    - При добавлении нового адреса электронной почты вы можете сделать его основным SMTP-адресом.

- **Автоматически обновлять адреса электронной почты на основе политики адресов электронной почты, которая применяется к этому получателю**. Установите этот флажок, чтобы адреса электронной почты получателей автоматически обновлялись на основе изменений политики адресов электронной почты организации.

Подсказка

Используйте раздел **Подсказка** для добавления подсказок, предупреждающих пользователей о возможных проблемах при отправке запроса на бронирование на почтовый ящик оборудования. Подсказка — это текст, который отображается на панели информации при добавлении этого получателя в поля "Кому", "Копия" и "Скрытая копия" нового сообщения электронной почты.

> ⓘ **Примечание**
>
> Подсказки могут содержать HTML-теги, но сценарии не допускаются. Длина пользовательской подсказки не должна превышать 175 отображаемых символов. HTML-теги при этом не учитываются.

Изменение свойств почтового ящика оборудования с помощью командной консоли Exchange

Используйте следующий набор командлетов для просмотра и изменения свойств почтового ящика оборудования: командлеты **Get-Mailbox** и **Set-Mailbox** для просмотра и изменения общих свойств и адресов электронной почты для почтовых ящиков оборудования. Используйте командлеты **Get-CalendarProcessing** и **Set-CalendarProcessing** для просмотра и изменения делегатов и параметров бронирования.

- **Get-User** и **Set-User**. Используйте эти командлеты для просмотра и задания общих свойств, таких как названия отделов и компаний.

- **Get-Mailbox** и **Set-Mailbox**. Используйте эти командлеты для просмотра и задания свойств почтовых ящиков, например адресов электронной почты или базы данных почтовых ящиков.
- **Get-CalendarProcessing** и **Set-CalendarProcessing**. Используйте эти командлеты для просмотра и изменения делегатов и параметров резервирования.

Дополнительные сведения об этих командлетах см. в следующих разделах:

- Get-User
- Set-User
- Get-Mailbox
- Set-Mailbox
- Get-CalendarProcessing
- Set-CalendarProcessing

Ниже приведены некоторые примеры использования командной консоли Exchange для изменения свойств почтового ящика оборудования.

В этом примере изменяется отображаемое имя и основной адрес SMTP (так называемый адрес ответа по умолчанию) для почтового ящика оборудования MotorPool 1. Предыдущий адрес ответа хранится в виде адреса прокси-сервера.

PowerShell

```
Set-Mailbox "MotorPool 1" -DisplayName "Motor Pool 1 - Compact" -
EmailAddresses SMTP:MP1.compact@contoso.com,smtp:MP.1@contoso.com
```

В этом примере почтовые ящики оборудования настраиваются таким образом, чтобы запросы на бронирование планировались только в рабочее время.

PowerShell

```
Get-Mailbox -ResultSize unlimited -Filter "RecipientTypeDetails -eq
'EquipmentMailbox'" | Set-CalendarProcessing -ScheduleOnlyDuringWorkHours
$true
```

В этом примере командлет **Get-User** используется для поиска всех почтовых ящиков оборудования в отделе Audio Visual, а затем при помощи командлета **Set-CalendarProcessing** отправляется запрос на бронирование для принятия или отклонения делегату с именем Анна Белова.

PowerShell

```
Get-User -ResultSize unlimited -Filter "(RecipientTypeDetails -eq
'EquipmentMailbox') -and (Department -eq 'Audio Visual')" | Set-
CalendarProcessing -AllBookInPolicy $false -AllRequestInPolicy $true -
ResourceDelegates "Ann Beebe"
```

Как проверить, все ли получилось?

Чтобы подтвердить, что вы успешно изменили свойства почтового ящика оборудования, выполните следующее:

- В EAC выберите почтовый ящик и щелкните ✎ чтобы просмотреть измененное свойство или функцию. В зависимости от измененного свойства оно может отображаться в области "Сведения" выбранного почтового ящика.

- В командной консоли Exchange для проверки изменений используется командлет **Get-Mailbox**. С помощью командной консоли Exchange можно просмотреть несколько свойств нескольких почтовых ящиков. В приведенном выше примере, где запросы на бронирование могут быть запланированы только в рабочее время, выполните следующую команду, чтобы проверить новое значение.

  PowerShell

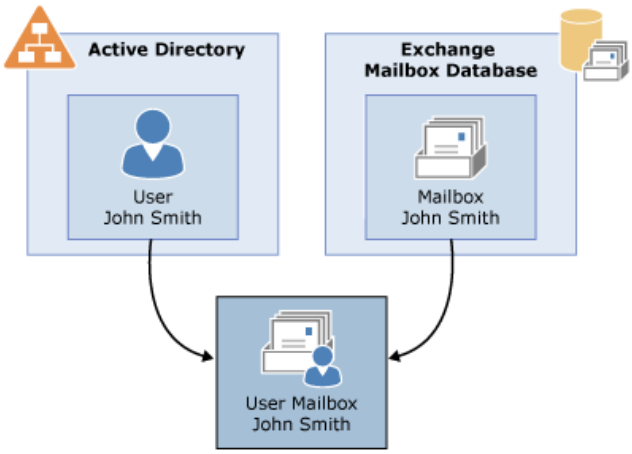
  ```
  Get-Mailbox -ResultSize unlimited -Filter "RecipientTypeDetails -eq
  'EquipmentMailbox'" | Get-CalendarProcessing | Format-List
  Identity,ScheduleOnlyDuringWorkHours
  ```

Отключенные почтовые ящики в Exchange Server

Статья • 04.04.2023

Каждый почтовый ящик Microsoft Exchange состоит из данных учетной записи пользователя Active Directory и почтового ящика, которые хранятся в базе данных почтовых ящиков Exchange. Все данные конфигурации для почтового ящика хранятся в атрибутах Exchange объекта-пользователя Active Directory. В базе данных почтовых ящиков хранятся почтовые данные, находящиеся в почтовом ящике, сопоставленном с учетной записью пользователя. На следующем рисунке показаны компоненты почтового ящика.

Компоненты почтового ящика



Отключенный почтовый ящик — это объект почтового ящика в базе данных почтовых ящиков, не связанный с учетной записью пользователя Active Directory. Существует два типа отключенных почтовых ящиков:

- **Отключенные почтовые ящики**. Если почтовый ящик отключен или удален в Центре администрирования Exchange или с помощью командлета **Disable-Mailbox** или **Remove-Mailbox** в командной консоли Exchange, Exchange сохраняет удаленный почтовый ящик в базе данных почтовых ящиков и переключает его в отключенное состояние. Поэтому отключенные или удаленные почтовые ящики называются *отключенными*. Отличие состоит в том, что при отключении почтового ящика атрибуты Exchange удаляются из соответствующей учетной записи пользователя Active Directory, но сама учетная запись пользователя сохраняется. При удалении почтового ящика удаляются атрибуты Exchange и учетная запись пользователя Active Directory.

  Отключенные и удаленные почтовые ящики хранятся в базе данных почтовых ящиков до тех пор, пока не истечет срок хранения удаленных почтовых ящиков, который по умолчанию составляет 30 дней. По истечении срока хранения почтовый ящик окончательно удаляется (или *очищается*). Если почтовый ящик удаляется с помощью командлета **Remove-Mailbox**, он также сохраняется в течение срока хранения.

  > **ⓘ Важно!**
  >
  > Если почтовый ящик удаляется с помощью командлета **Remove-Mailbox** и параметра *Permanent* или *StoreMailboxIdentity*, он будет немедленно удален из базы данных почтовых ящиков.

  Чтобы определить отключенные почтовые ящики в организации, выполните следующие команды в командной консоли Exchange:

  ```
  PowerShell
  ```

```
$dbs = Get-MailboxDatabase
$dbs | foreach {Get-MailboxStatistics -Database $_.DistinguishedName} | where
{$_.DisconnectReason -eq "Disabled"} | Format-Table DisplayName,Database,DisconnectDate
```

- **Обратимо удаленные почтовые ящики**. Когда почтовый ящик перемещается в другую базу данных почтовых ящиков, Exchange не полностью удаляет почтовый ящик из базы данных исходного почтового ящика по завершении перемещения. Вместо этого почтовый ящик в исходной базе данных почтовых ящиков переходит в состояние *soft-deleted*. Как и отключенные почтовые ящики, обратимо удаленные почтовые ящики сохраняются в исходной базе данных до тех пор, пока не истечет срок хранения удаленных почтовых ящиков или не будет использован командлет **Remove-StoreMailbox**, очищающий почтовый ящик.

  Выполните следующие команды, чтобы определить обратимо удаленные почтовые ящики в организации.

  PowerShell

  ```
  $dbs = Get-MailboxDatabase
  $dbs | foreach {Get-MailboxStatistics -Database $_.DistinguishedName} | where
  {$_.DisconnectReason -eq "SoftDeleted"} | Format-Table DisplayName,Database,DisconnectDate
  ```

Работа с отключенными почтовыми ящиками

В отключенном почтовом ящике можно выполнить несколько приведенных ниже операций, прежде чем он будет очищен из базы данных почтовых ящиков.

- Повторное подключение к той же учетной записи пользователя.
- Подключение к другой учетной записи пользователя без поддержки почты (то есть без почтового ящика).
- Восстановление в учетной записи пользователя с существующим почтовым ящиком. Например, если у пользователя, чей почтовый ящик был удален, есть новый почтовый ящик, в последнем можно восстановить отключенный почтовый ящик пользователя.
- Окончательное удаление из базы данных почтовых ящиков Exchange.

Подключение или восстановление отключенного почтового ящика

Ниже приведены сценарии, при которых может понадобиться подключить или восстановить отключенный почтовый ящик до истечения срока его хранения или окончательного удаления.

- Почтовый ящик отключен, и его необходимо повторно подключить к той же учетной записи пользователя Active Directory.

- Почтовый ящик удален с помощью центра администрирования Exchange или командлета Remove-Mailbox, и его необходимо повторно подключить к другой учетной записи пользователя Active Directory.

- Почтовый ящик удален, и его необходимо восстановить в существующем почтовом ящике. Например, если у пользователя, чей почтовый ящик был удален, есть новый почтовый ящик, в последнем можно восстановить отключенный почтовый ящик пользователя.

- Необходимо преобразовать почтовый ящик пользователя в связанный почтовый ящик, сопоставленный с учетной записью пользователя, внешней по отношению к лесу, в котором находится организация Exchange. Например, сопоставление почтового ящика с внешней учетной записью может

быть полезно при использовании леса ресурсов. В этом сценарии объекты-пользователи в лесу Exchange имеют почтовые ящики, однако для этих объектов-пользователей отключен вход в систему. Необходимо сопоставить почтовый ящик в лесу Exchange с учетной записью пользователя в лесу внешней учетной записи.

Существует два способа повторного подключения или восстановления отключенного почтового ящика. Первый способ — использовать центр администрирования Exchange или командлет **Connect-Mailbox** для подключения отключенного почтового ящика к учетной записи пользователя. Процедуры повторного подключения отключенных почтовых ящиков см. в разделе Подключение отключенного почтового ящика.

Второй способ — использовать командлет **New-MailboxRestoreRequest** для слияния содержимого отключенного и существующего почтовых ящиков. Данный командлет использует службу репликации почтовых ящиков (MRS) для восстановления почтового ящика. Процедуры восстановления отключенных почтовых ящиков см. в статье Подключение или восстановление удаленного почтового ящика.

Окончательное удаление отключенного почтового ящика

Как говорилось ранее, в приложении Exchange отключенные почтовые ящики сохраняются в базе данных почтовых ящиков в соответствии с параметрами хранения удаленных почтовых ящиков этой базы данных. По истечении указанного срока хранения отключенный почтовый ящик очищается из базы данных почтовых ящиков Exchange. Окончательно удалить отключенный почтовый ящик и содержимое всех его сообщений из базы данных почтовых ящиков также можно с помощью командлета **Remove-StoreMailbox**. После автоматического очищения отключенного почтового ящика или его окончательного удаления администратором данные будут окончательно потеряны, а почтовый ящик нельзя будет восстановить.

Дополнительные сведения см. в разделе Окончательное удаление почтового ящика.

Работа с отключенными архивными почтовыми ящиками

Архивные почтовые ящики становятся отсоединенными после их отключения. Как и отключенный основной почтовый ящик, отключенный архивный почтовый ящик можно подключить с помощью командлета **Connect-Mailbox** с параметром *Archive* .

Основной и архивный почтовые ящики имеют одно устаревшее различающееся имя, поэтому необходимо подключить архивный почтовый ящик к тому же пользовательскому почтовому ящику, к которому он был ранее подключен. Архивный почтовый ящик нельзя подключить к почтовому ящику другого пользователя.

С отключенным архивным почтовым ящиком можно выполнить две следующие операции.

- **Подключение к существующему основному почтовому ящику**. Как и отключенный основной почтовый ящик, отключенный архивный почтовый ящик хранится в базе данных почтовых ящиков до истечения срока хранения удаленного почтового ящика, который по умолчанию составляет 30 дней. В течение этого времени архивный почтовый ящик можно восстановить, повторно подключив его к учетной записи пользователя, к которой он был подключен до отключения.

  > ⓘ **Примечание**
  >
  > Если отключить архивный почтовый ящик для почтового ящика пользователя, а потом включить его для этого же пользователя, данный почтовый ящик пользователя получит новый архивный почтовый ящик. С помощью командлета **Connect-Mailbox** вы можете подключить основной почтовый ящик для пользователя, а для подсоединения отключенного архивного почтового ящика к существующему почтовому ящику необходимо использовать командлет **Enable-Mailbox**.

Дополнительные сведения см. в статье Управление архивами In-Place в Exchange Server.

- **Окончательное удаление из базы данных почтовых ящиков Exchange**. Exchange сохраняет отключенные архивные почтовые ящики на основе параметров хранения удаленных почтовых ящиков, настроенных для базы данных почтовых ящиков. По умолчанию период хранения равен 30 дням. По истечении указанного срока хранения отключенный архивный почтовый ящик окончательно очищается из базы данных почтовых ящиков Exchange.

  Подобно отключенному основному почтовому ящику, отключенный архивный почтовый ящик можно окончательно удалить в любое время с помощью командлета **Remove-StoreMailbox**. Дополнительные сведения см. в разделе Окончательное удаление почтового ящика.

Работа с обратимо удаленными почтовыми ящиками

Обратимо удаленный почтовый ящик создается при перемещении почтового ящика из одной базы почтовых ящиков Exchange в любую другую базу данных почтовых ящиков. При возникновении сбоя в процессе перемещения почтового ящика в базу данных назначения сервер Exchange не удаляет его окончательно из исходной базы данных. Исходный почтовый ящик можно в любое время восстановить и переместить повторно. Обратимо удаленные почтовые ящики хранятся в Exchange в течение срока хранения почтовых ящиков.

С обратимо удаленным почтовым ящиком можно выполнить две следующие операции.

- Восстановление в существующем почтовом ящике.
- Окончательное удаление из базы данных почтовых ящиков Exchange.

Процедуры по восстановлению и окончательному удалению обратимо удаленного почтового ящика похожи на соответствующие процедуры для отключенного почтового ящика. Дополнительную информацию см. в следующих статьях:

- Подключение или восстановление удаленного почтового ящика
- Окончательное удаление почтового ящика

Краткое изложение сведений о работе с отключенными почтовыми ящиками

В следующей таблице резюмированы сведения об отключенных почтовых ящиках, включая способ отключения почтового ящика, действия с соответствующей учетной записью пользователя Active Directory при отключении почтового ящика, а также имеющиеся варианты и средства подключения или восстановления отключенных почтовых ящиков.

Способ отключения почтового ящика	**Значение свойства *DisconnectReason***	**Сохранена ли учетная запись Active Directory?**	**Варианты подключения или восстановления**	**Инструменты**

Способ отключения почтового ящика	Значение свойства *DisconnectReason*	Сохранена ли учетная запись Active Directory?	Варианты подключения или восстановления	Инструменты
EAC:"**Отключитьпочтовые ящики получателей**>"> Командлет Disable-Mailbox командной консоли Exchange: **Disable-Mailbox**	Отключено	Да	Подключение к той же учетной записи пользователя	EAC: почтовые**ящики**>**получателей**>**Подключение почтового ящика** Командлет **Connect-Mailbox** для командной консоли Exchange
EAC:**Удалениепочтовых**> ящиков **получателей**> Командлет **Remove-Mailbox** для командной консоли Exchange	Отключено	Нет	Подключение к учетной записи другого пользователя Восстановление в другой почтовый ящик	EAC: почтовые**ящики**>**получателей**>**Подключение почтового ящика** Командная консоль Exchange: • Командлет **Connect-Mailbox** • **Командлет Enable-Mailbox** • Командлет **New-MailboxRestore**
Перемещение в другую базу данных почтовых ящиков	SoftDeleted	Да	Подключение к учетной записи другого пользователя Восстановление в другой почтовый ящик	EAC: почтовые**ящики**>**получателей**>**Подключение почтового ящика** Командная консоль Exchange: • Командлет **Connect-Mailbox** • **Командлет Enable-Mailbox** • Командлет **New-MailboxRestore**

Документация по отключенным почтовым ящикам

В следующей таблице приведены ссылки на разделы по управлению отключенными почтовыми ящиками. Они включают сведения по управлению отключенными почтовыми ящиками пользователя, связанными почтовыми ящиками, почтовыми ящиками ресурсов и общими почтовыми ящиками.

Статья	Описание
Отключение или удаление почтового ящика в Exchange Server	Узнайте, как отключать или удалять почтовые ящики.
Подключение отключенного почтового ящика	Узнайте, как подключить отключенный почтовый ящик к существующей учетной записи пользователя.
Подключение или восстановление удаленного почтового ящика	Узнайте, как подключить удаленный почтовый ящик к учетной записи пользователя или восстановить его содержимое в существующей почтовой папке.
Manage Mailbox Restore Requests	Узнайте, как управлять запросами на восстановление почтовых ящиков с помощью командной консоли Exchange.
Окончательное удаление почтового ящика	Узнайте, как окончательно удалить почтовый ящик.

Отключение или удаление почтового ящика в Exchange Server

Статья • 04.04.2023

В Exchange Server для отключения или удаления почтовых ящиков можно использовать Центр администрирования Exchange (EAC) или командную консоль Exchange. Отключенные или удаленные почтовые ящики также *называются отключенными почтовыми ящиками*. Дополнительные сведения об отключенных почтовых ящиках см. в разделе Отключенные почтовые ящики.

Примечание. Если вам нужно удалить почтовый ящик в Microsoft 365 или Office 365, см. статью Удаление или восстановление почтовых ящиков пользователей в Exchange Online.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 2 минут.
- Дополнительные сведения о доступе и использовании Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения подготовки получателей" раздела Разрешения получателей .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Отключение почтовых ящиков

При отключении почтового ящика все атрибуты Exchange удаляются из связанной учетной записи пользователя в Active Directory. Отключенный почтовый ящик скрывается и помечается для удаления. Дата окончательного удаления отключенного почтового ящика зависит от значения свойства **MailboxRetention** для базы данных почтовых ящиков (значение по умолчанию — 30 дней). До этого времени его можно подключить к новой или существующей учетной записи пользователя без связанного почтового ящика. Дополнительные сведения см. в разделе Подключение отключенного почтового ящика.

Примечание. Отключение почтового ящика со связанным архивом помечает основной и архивный почтовые ящики для удаления. Сведения о том, как пометить архивный почтовый ящик только для удаления, не затрагивая основной почтовый ящик, см. в статье Отключение архивного почтового ящика.

Отключение почтового ящика в Центре администрирования Exchange

1. В Центре администрирования Exchange выберите **Получатели** и перейдите на вкладку нужного типа почтового ящика:

    - **Почтовые ящики** — почтовые ящики пользователей и связанные почтовые ящики.
    - **Общие** — общие почтовые ящики.

2. Найдите и выберите нужный почтовый ящик. Пример:

    - Прокрутите список. Чтобы отсортировать почтовые ящики, щелкните заголовок столбца.
    - Нажмите **Поиск** и введите текст для фильтрации списка почтовых ящиков.
    - Чтобы выбрать несколько почтовых ящиков, выберите один из них и, удерживая клавишу SHIFT, щелкните другой ниже в списке или удерживайте при выборе клавишу CTRL.

3. Выбрав почтовый ящик или почтовые ящики, которые нужно отключить, щелкните значок **Дополнительные** ••• выберите **Отключить**, а затем нажмите кнопку **Да** в появившемся предупреждающем сообщении.

Отключения почтового ящика с помощью командной консоли Exchange

Чтобы отключить почтовый ящик, используйте следующий синтаксис:

PowerShell

```
Disable-Mailbox <MailboxIdentity> [-Arbitration] [-Archive] [-PublicFolder]
[-RemoteArchive]
```

В этом примере отключается почтовый ящик пользователя с псевдонимом danj.

PowerShell

```
Disable-Mailbox danj
```

В этом примере отключается почтовый ящик помещения Conf Room 31/1234 (12).

PowerShell

```
Disable-Mailbox "Conf Room 31/1234 (12)"
```

В этом примере отключается общий почтовый ящик с адресом sharedmbx@contoso.comэлектронной почты .

PowerShell

```
Disable-Mailbox sharedmbx@contoso.com
```

Подробные сведения о синтаксисе и параметрах см. в статье Disable-Mailbox.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно отключили почтовый ящик, выполните одно из следующих действий:

- В Центре администрирования Exchange нажмите **Получатели**, перейдите на соответствующую вкладку и убедитесь, что почтового ящика нет в списке. Обратите внимание, что может потребоваться нажать 🔄
- В средстве "Пользователи и компьютеры Active Directory" щелкните правой кнопкой мыши учетную запись пользователя, почтовый ящик которого вы отключили, и выберите **Свойства**. На вкладке **Общие** убедитесь, что поле **Адрес электронной почты** пустое.

- В командной консоли Exchange замените *<DisplayName>* отображаемым именем пользователя и выполните следующие команды, чтобы проверить значение `Disabled` свойства **DisconnectReason** (указывает, что почтовый ящик помечен для удаления):

  PowerShell

  ```
  $dbs = Get-MailboxDatabase
  $dbs | foreach {Get-MailboxStatistics -Database $_.DistinguishedName} |
  where {$_.DisplayName -eq "<DisplayName>"} | Format-List
  DisconnectReason,DisconnectDate
  ```

  Примечания.

  - Свойство **DisconnectReason** не различает отключенные и удаленные почтовые ящики (значение для обоих — `Disabled`). Наличие связанной учетной записи пользователя указывает на то, что почтовый ящик отключен.

    При удалении почтового **ящика значение свойства DisconnectReason** также `Disabled`равно , но соответствующая учетная запись пользователя Active Directory также удаляется.

  - Если команда не возвращает результатов, замените *<DatabaseName>* именем базы данных почтовых ящиков, в которой находится отключенный почтовый ящик, и выполните следующую команду, чтобы синхронизировать состояние почтового ящика для всех отключенных почтовых ящиков в базе данных:

    PowerShell

    ```
    Get-MailboxStatistics -Database "<DatabaseName>" | foreach {Update-
    StoreMailboxState -Database $_.Database -Identity $_.MailboxGuid -
    Confirm:$false}
    ```

  После этого выполните предыдущую команду, которая теперь должна дать результаты.

- В командной консоли Exchange замените *<UserIdentity>* именем или именем участника-пользователя (например,), и выполните эту команду, user@contoso.comчтобы убедиться, что значение свойства **RecipientType** равно `User`, а не `UserMailbox`.

  PowerShell

```
Get-User -Identity <UserIdentity>
```

Удаление почтовых ящиков

При удалении почтового ящика почтовый ящик отключается от связанной учетной записи пользователя, а учетная запись удаляется из Active Directory. Отключенный почтовый ящик скрывается и помечается для удаления. Дата окончательного удаления отключенного почтового ящика зависит от значения свойства **MailboxRetention** для базы данных почтовых ящиков (значение по умолчанию — 30 дней). До этого времени его можно подключить к новой или существующей учетной записи пользователя без связанного почтового ящика. Дополнительные сведения см. в статье Подключение или восстановление удаленного почтового ящика.

Примечание. Удаление почтового ящика со связанным архивом помечает основной и архивный почтовые ящики для удаления. Сведения о том, как пометить архивный почтовый ящик только для удаления, не затрагивая основной почтовый ящик, см. в статье Отключение архивного почтового ящика.

Удаление почтового ящика в Центре администрирования Exchange

1. В Центре администрирования Exchange и перейдите на вкладку нужного типа почтового ящика:

    - **Получателей**>**Почтовые ящики** для почтовых ящиков пользователей и связанных почтовых ящиков.
    - **Получателей**>**Ресурсы** для почтовых ящиков помещений и оборудования.
    - **Получателей**>**Общий доступ** для общих почтовых ящиков.
    - **Общедоступные папки**>**Почтовые ящики общедоступных папок для почтовых** ящиков общедоступных папок.

2. Найдите и выберите нужный почтовый ящик. Пример:

    - Прокрутите список. Чтобы отсортировать почтовые ящики, щелкните заголовок столбца.

- Нажмите **Поиск** и введите текст для фильтрации списка почтовых ящиков.
- Чтобы выбрать несколько почтовых ящиков, выберите один из них и, удерживая клавишу SHIFT, щелкните другой ниже в списке или удерживайте при выборе клавишу CTRL.

3. Выбрав почтовый ящик или почтовые ящики, которые нужно удалить, щелкните 🗑, а затем нажмите кнопку **Да** в появившемся предупреждающем сообщении.

Удаление почтового ящика с помощью командной консоли Exchange

Чтобы удалить почтовый ящик, используйте следующий синтаксис:

PowerShell

```
Remove-Mailbox <MailboxIdentity> [-Arbitration] [-PublicFolder]
```

В этом примере удаляется почтовый ящик с адресом pilarp@contoso.comэлектронной почты .

PowerShell

```
Remove-Mailbox pilarp@contoso.com
```

В этом примере удаляется почтовый ящик оборудования Fleet Van (16).

PowerShell

```
Remove-Mailbox "Fleet Van (16)"
```

В этом примере удаляется почтовый ящик с псевдонимом corpprint.

PowerShell

```
Remove-Mailbox corpprint
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе Remove-Mailbox.

Примечание. Если вы используете командлет **Remove-Mailbox** с параметром *Purge* , почтовый ящик немедленно очищается и не может быть восстановлен. Дополнительные сведения см. в разделе Окончательное удаление почтового ящика.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно удалили почтовый ящик, выполните одно из следующих действий:

- В Центре администрирования Exchange нажмите **Получатели**, перейдите на соответствующую вкладку и убедитесь, что почтового ящика нет в списке. Обратите внимание, что может потребоваться нажать 🔄
- Убедитесь, что связанная учетная запись больше не отображается в средстве "Пользователи и компьютеры Active Directory". Обратите внимание, что у почтовых ящиков помещений, оборудования, разрешения конфликтов, общедоступных папок и общих почтовых ящиков также есть связанные учетные записи пользователей, которые отключены.
- В командной консоли Exchange замените <*DisplayName*> отображаемым именем пользователя и выполните следующие команды, чтобы проверить значение `Disabled` свойства **DisconnectReason** (указывает, что почтовый ящик помечен для удаления):

  PowerShell

  ```
  $dbs = Get-MailboxDatabase
  $dbs | foreach {Get-MailboxStatistics -Database $_.DistinguishedName} |
  where {$_.DisplayName -eq "<DisplayName>"} | Format-List
  DisconnectReason,DisconnectDate
  ```

  Примечания.

  - Свойство **DisconnectReason** не различает отключенные и удаленные почтовые ящики (значение для обоих — `Disabled`). Отсутствие связанной учетной записи пользователя указывает на то, что почтовый ящик удален.
  - Если команда не возвращает результатов, замените <*DatabaseName*> именем базы данных почтовых ящиков, в которой находится отключенный почтовый ящик, и выполните следующую команду, чтобы синхронизировать состояние почтового ящика для всех отключенных почтовых ящиков в базе данных:

PowerShell

```
Get-MailboxStatistics -Database "<DatabaseName>" | foreach {Update-StoreMailboxState -Database $_.Database -Identity $_.MailboxGuid -Confirm:$false}
```

После этого выполните предыдущую команду, которая теперь должна дать результаты.

- В командной консоли Exchange замените *<UserIdentity>* именем или именем участника-пользователя (например,), и выполните эту команду, user@contoso.comчтобы убедиться, что пользователь не найден.

PowerShell

```
Get-User <UserIdentity>
```

Дополнительные сведения

Если вы удалите учетную запись пользователя Active Directory, связанную с почтовым ящиком, Exchange определит, что почтовый ящик больше не подключен к учетной записи пользователя и пометит его для удаления, даже если он помещен на хранение для судебного разбирательства или хранение на месте. Чтобы сохранить почтовый ящик, сделайте следующее:

- Не удаляйте учетную запись пользователя, а отключите ее.
- Измените свойства почтового ящика, чтобы ограничить его использование и доступ к нему. Например, задайте 1 в качестве квот на отправку и получение, заблокируйте потенциальных отправителей сообщений на этот почтовый ящик и ограничьте доступ к нему.
- Храните почтовый ящик, пока не будут удалены все данные или не исчезнет потребность в их хранении.

Дополнительные сведения см. в разделе Удержание на месте и удержание для судебного разбирательства в Exchange Server.

Подключение отключенного почтового ящика в Exchange Server

Статья • 04.04.2023

При отключении почтового ящика Exchange сохраняет его в базе данных почтовых ящиков и переводит его в отключенное состояние. Атрибуты Exchange также удаляются из соответствующей учетной записи пользователя Active Directory, но учетная запись остается. Почтовый ящик сохраняется до истечения срока хранения удаленного почтового ящика,который по умолчанию составляет 30 дней, прежде чем он будет окончательно удален (или *очищен*) из базы данных почтовых ящиков.

Пока отключенный почтовый ящик не будет окончательно удален из базы данных почтовых ящиков Exchange, вы можете заново подключить его к учетной записи пользователя Active Directory с помощью Центра администрирования Exchange или командной консоли Exchange.

Дополнительные сведения об отключенных почтовых ящиках и других задачах управления приведены в следующих разделах:

- Отключенные почтовые ящики
- Отключение или удаление почтового ящика в Exchange Server
- Подключение или восстановление удаленного почтового ящика
- Окончательное удаление почтового ящика

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 2 минуты.
- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Выполните командлет **Get-User** в командной консоли Exchange, чтобы убедиться, что учетная запись пользователя Active Directory, к которой требуется подключить отключенный почтовый ящик, существует и что она еще не связана с другим почтовым ящиком. Чтобы подключить отключенный почтовый ящик к учетной записи пользователя, учетная запись должна

существовать, а значение свойства *RecipientType* должно иметь `User` значение , указывающее, что учетная запись еще не включена.

Эти сведения также можно проверить в Пользователи и компьютеры Active Directory.

- Замените <*DisplayName*> отображаемым именем почтового ящика и выполните следующие команды в командной консоли Exchange, чтобы убедиться, что отключенный почтовый ящик, который требуется подключить к учетной записи пользователя, существует и не является обратимо удаленным почтовым ящиком.

  PowerShell

  ```
  $dbs = Get-MailboxDatabase
  $dbs | foreach {Get-MailboxStatistics -Database $_.DistinguishedName} |
  where {$_.DisplayName -eq "<DisplayName>"} | Format-List
  DisplayName,Database,DisconnectReason
  ```

  Чтобы иметь возможность подключить отключенный почтовый ящик, почтовый ящик должен существовать в базе данных почтовых ящиков, а значение свойства *DisconnectReason* должно иметь значение `Disabled`. Если почтовый ящик был удален из базы данных, команда не даст никаких результатов.

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения подготовки получателей" раздела Разрешения получателей .

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование EAC для подключения отключенного почтового ящика

Следующая процедура показывает, как подключить отключенный почтовый ящик пользователя. Можно также заново подключить отключенные связанные почтовые ящики и отключенные общие почтовые ящики к соответствующей учетной записи пользователя.

1. В Центре администрирования Exchange (EAC) выберите **Получатели**>**Почтовые ящики**.
2. Щелкните ••• выберите **Подключить почтовый ящик**.

   Появится список отключенных почтовых ящиков на сервере Exchange Server в вашей организации Exchange.

   > ⓘ **Примечание**
   >
   > Это список отключенных почтовых ящиков содержит выключенные почтовые ящики, удаленные почтовые ящики (в том числе с возможностью восстановления).

3. Щелкните выключенный почтовый ящик, который необходимо повторно подключить, а затем щелкните **Подключить**.
4. Нажмите кнопку **Да** в окне предупреждения, запрашивающего подтверждение подключения ящика.

   Exchange подключит отключенный почтовый ящик к соответствующей учетной записи пользователя.

Подключение отключенного почтового ящика или личного архива с помощью командной консоли Exchange

Используйте командлет **Connect-Mailbox** в командной консоли Exchange, чтобы подключить отключенный почтовый ящик к учетной записи пользователя. Необходимо указать тип подключаемого почтового ящика. В следующих примерах показан синтаксис повторного подключения почтовых ящиков пользователей, связанных, общих и архивных почтовых ящиков.

В этом примере подключается почтовый ящик пользователя. Параметр *Identity* указывает отключенный почтовый ящик в базе данных Exchange. Параметр *User*

указывает учетную запись пользователя Active Directory для повторного подключения почтового ящика.

PowerShell

```
Connect-Mailbox -Identity "Jeffrey Zeng" -Database MBXDB01 -User "Jeffrey Zeng"
```

В этом примере подключается связанный почтовый ящик. Параметр *Identity* указывает отключенный почтовый ящик в базе данных Exchange. Параметр *LinkedMasterAccount* указывает учетную запись пользователя Active Directory в лесу учетных записей, к которому требуется повторно подключить почтовый ящик. Параметр *Alias* указывает псевдоним, который является частью адреса электронной почты в левой части символа (@) для повторно подключенного почтового ящика.

PowerShell

```
Connect-Mailbox -Identity "Kai Axford" -Database MBXDB02 -
LinkedDomainController FabrikamDC01 -LinkedMasterAccount
kai.axford@fabrikam.com -Alias kaia
```

В данном примере подключается общий почтовый ящик.

PowerShell

```
Connect-Mailbox -Identity "Corporate Shared Mailbox" -Database "Mailbox Database 03" -User "Corporate Shared Mailbox" -Alias corpshared -Shared
```

> ⓘ **Примечание**
>
> Если параметр Alias не включен при *выполнении* командлета **Connect-Mailbox** , значение, указанное в параметре *User* или *LinkedMasterAccount* , будет использоваться для создания псевдонима адреса электронной почты для повторно подключенного почтового ящика.

В этом примере личный архив подключается к основному почтовому ящику с помощью GUID почтового ящика, хранящегося в базе данных почтовых ящиков DB01.

PowerShell

```
Enable-Mailbox -Identity "Megan Bown" -ArchiveGUID "95352f8b-e5aa-496f-ac7f-ce93357d7b0c" -ArchiveDatabase "DB01" -Archive
```

Если имя личного архива неизвестно, его можно просмотреть в командной консоли Exchange, выполнив следующую команду. В этом примере возвращаются все личные архивные почтовые ящики в базе данных почтовых ящиков DB01.

PowerShell

```
Get-MailboxDatabase "DB01" | Get-MailboxStatistics | Where
{($_.DisconnectDate -ne $null) -and ($_.IsArchiveMailbox -eq $true)} |
Format-Table DisplayName,MailboxGuid -AutoSize
```

Примечание

Личный архивный почтовый ящик можно подключить к любому основному почтовому ящику, даже если он не является почтовым ящиком исходного владельца. Используйте параметр *AllowLegacyDNMismatch* , чтобы разрешить подключение архивного почтового ящика к другому основному почтовому ящику.

Дополнительные сведения о синтаксисе и параметрах см. в разделе Connect-Mailbox.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно подключили отключенный почтовый ящик к учетной записи пользователя, выполните одно из следующих действий:

- В EAC щелкните **Получатели**, перейдите на соответствующую страницу с типом почтового ящика, который вы повторно подключили, щелкните и убедитесь, что почтовый ящик указан в списке.
- В оснастке "Пользователи и компьютеры Active Directory" щелкните правой кнопкой мыши учетную запись пользователя, чей почтовый ящик вы отключили, а затем выберите пункт **Свойства**. Обратите внимание, что в поле **Адрес электронной почты** на вкладке **Общие** указан электронный адрес подключенного почтового ящика.
- В командной консолиExchange замените <Identity> именем учетной записи пользователя и выполните следующую команду:

  PowerShell

  ```
  Get-User "<Identity>"
  ```

Значение **UserMailbox** для свойства *RecipientType* указывает, что учетная запись пользователя и почтовый ящик подключены. Для проверки того, что почтовый ящик существует, можно запустить командлет **Get-Mailbox**.

Подключение или восстановление удаленного почтового ящика в Exchange Server

Статья • 04.04.2023

При удалении почтового ящика Exchange сохраняет ящик в базе данных почтовых ящиков и переводит его в отключенное состояние. Удаляется также связанная с ним учетная запись пользователя Active Directory. Почтовый ящик сохраняется до истечения срока хранения удаленного почтового ящика, который по умолчанию составляет 30 дней, а затем окончательно удаляется (или *очищается*) из базы данных почтовых ящиков.

Пока удаленный почтовый ящик не будет окончательно удален из базы данных почтовых ящиков Exchange, его можно подключить к учетной записи пользователя в Active Directory, используя Центр администрирования Exchange или командную консоль Exchange. Вы также можете восстановить содержимое удаленного почтового ящика в существующем почтовом ящике, используя командную консоль Exchange.

Дополнительные сведения об отключенных почтовых ящиках и других задачах управления приведены в следующих разделах:

- Отключенные почтовые ящики
- Отключение или удаление почтового ящика в Exchange Server
- Подключение отключенного почтового ящика
- Окончательное удаление почтового ящика

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 2 минуты.
- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Создайте новую учетную запись пользователя в Active Directory для подключения удаленного почтового ящика. Или выполните командлет **Get-User** в командной консоли Exchange, чтобы убедиться, что учетная запись

пользователя в Active Directory, к которой вы хотите подключить удаленный почтовый ящик, существует и не связана с другим почтовым ящиком. Чтобы подключить удаленный почтовый ящик к учетной записи пользователя, учетная запись должна существовать, а значение свойства *RecipientType* должно иметь `User`значение , указывающее, что учетная запись еще не включена.

В локальных организациях Exchange также можно проверить эти сведения с помощью оснастки "Пользователи и компьютеры Active Directory".

> **ⓘ Важно!**
>
> При подключении удаленных связанных почтовых ящиков, почтовых ящиков ресурсов или общих почтовых ящиков учетная запись пользователя Active Directory, к которой подключается почтовый ящик, должна быть отключена.

- Чтобы убедиться, что удаленный почтовый ящик, к которому вы хотите подключить учетную запись пользователя, существует в базе данных почтовых ящиков и не является обратимо удаленным почтовым ящиком, выполните следующую команду:

  PowerShell

  ```
  Get-MailboxDatabase | foreach {Get-MailboxStatistics -Database $_.name} | where {$_.DisplayName -eq "<display name>"} | Format-List DisplayName,Database,DisconnectReason
  ```

  Удаленный почтовый ящик должен существовать в базе данных почтовых ящиков, а значение свойства *DisconnectReason* должно иметь значение `Disabled`. Если почтовый ящик был удален из базы данных, команда не даст никаких результатов.

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения подготовки получателей" раздела Разрешения получателей .

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

- Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server, Exchange Online или Exchange Online Protection.

Подключить удаленный почтовый ящик

При подключении удаленного почтового ящика вы связываете его с учетной записью пользователя, которая не включена. Это означает, что у него нет существующего почтового ящика. Для подключения удаленного почтового ящика к учетной записи пользователя, имеющего почтовый ящик, следует восстановить удаленный почтовый ящик. Дополнительные сведения см. в подразделе Restore a deleted mailbox далее в этом разделе.

Использовать Центр администрирования Exchange для подключения удаленного почтового ящика

В приведенной ниже процедуре описано, как подключить удаленный почтовый ящик к учетной записи пользователя. Эту процедуру также можно использовать для подключения связанных почтовых ящиков, почтовых ящиков ресурсов и общих почтовых ящиков, которые были удалены из учетной записи пользователя.

1. В EAC перейдите в раздел **Почтовые ящики получателей**>.
2. Щелкните ••• выберите **Подключить почтовый ящик**.

   Появится список отключенных почтовых ящиков на сервере Exchange Server в вашей организации Exchange.

   > ⓘ **Примечание**
   >
   > Это список отключенных почтовых ящиков содержит выключенные почтовые ящики, удаленные почтовые ящики (в том числе с возможностью восстановления).

3. Щелкните удаленный почтовый ящик, который требуется подключить, а затем щелкните **Подключить**.
4. Нажмите кнопку **Да** в окне предупреждения, запрашивающего подтверждение подключения ящика.

   Отображается список учетных записей пользователей, для которых не включена поддержка почты.

5. Щелкните пользователя, для которого требуется подключить ящик, а затем щелкните **OK**.

Exchange подключит удаленный почтовый ящик к выбранной учетной записи пользователя.

Подключение удаленного почтового ящика в командной консоли Exchange

Используйте командлет **Connect-Mailbox** в командной консоли Exchange, чтобы подключить удаленный почтовый ящик к не поддерживающей почту учетной записи пользователя. Необходимо указать тип подключаемого почтового ящика. Ниже показан синтаксис для подключения почтовых ящиков пользователей, помещений и оборудования, а также связанных и общих почтовых ящиков. Во всех примерах необязательный параметр *Alias* используется для указания псевдонима электронной почты, который является частью адреса электронной почты в левой части символа (@). Если параметр *Alias* не включен, значение, указанное в параметре *User* или *LinkedMasterAccount* , используется для создания псевдонима для адреса электронной почты для повторно подключенного почтового ящика.

> ⓘ **Примечание**
>
> Как отмечалось ранее, при подключении связанного почтового ящика, почтового ящика ресурса или общего почтового ящика учетная запись пользователя Active Directory, с которой связывается почтовый ящик, должна быть отключена.

В этом примере удаленный почтовый ящик пользователя подключается к учетной записи пользователя, не поддерживающей почту. Параметр *Identity* указывает отображаемое имя удаленного почтового ящика, сохраненного в базе данных почтовых ящиков с именем MBXDB01. Параметр *User* указывает учетную запись пользователя Active Directory для подключения почтового ящика.

PowerShell

```
Connect-Mailbox -Identity "Paul Cannon" -Database MBXDB01 -User "Robin Wood"
-Alias robinw
```

> ⓘ **Примечание**
>
> Вы также можете использовать значения свойств или `MailboxGuid` для `LegacyDN` идентификации удаленного почтового ящика.

В этом примере подключается связанный почтовый ящик. Параметр *Identity* указывает удаленный почтовый ящик в базе данных почтовых ящиков с именем MBXDB02. Параметр *LinkedMasterAccount* указывает учетную запись пользователя Active Directory в лесу учетных записей, к которому требуется подключить почтовый ящик. Параметр *LinkedDomainController* указывает контроллер домена в лесу учетных записей.

PowerShell

```
Connect-Mailbox -Identity "Temp User" -Database MBXDB02 -
LinkedDomainController FabrikamDC01 -LinkedMasterAccount
danpark@fabrikam.com -Alias dpark
```

В данном примере подключается почтовый ящик помещения.

PowerShell

```
Connect-Mailbox -Identity "rm2121" -Database "MBXResourceDB" -User
"Conference Room 2121" -Alias ConfRm2121 -Room
```

В данном примере подключается почтовый ящик оборудования.

PowerShell

```
Connect-Mailbox -Identity "MotorPool01" -Database "MBXResourceDB" -User
"Van01 (12 passengers)" -Alias van01 -Equipment
```

В данном примере подключается общий почтовый ящик.

PowerShell

```
Connect-Mailbox -Identity "Printer Support" -Database MBXDB01 -User "Corp
Printer Support" -Alias corpprint -Shared
```

> ⓘ **Примечание**
>
> Вы также можете использовать `LegacyDN` значения или `MailboxGuid` для идентификации удаленного почтового ящика.

Дополнительные сведения о синтаксисе и параметрах см. в разделе Connect-Mailbox.

Как проверить, все ли получилось?

Чтобы убедиться, что удаленный почтовый ящик успешно подключен к учетной записи пользователя, выполните одно из следующих действий.

- В EAC щелкните **Получатели**, перейдите на соответствующую страницу с типом подключенного почтового ящика, щелкните 🔄 и убедитесь, что почтовый ящик указан в списке.
- В оснастке "Active Directory — пользователи и компьютеры" щелкните правой кнопкой мыши учетную запись пользователя, чей почтовый ящик был подключен, и выберите **Свойства**. На вкладке **Общие** обратите внимание, что в поле **Адрес электронной почты** указан адрес подключенного почтового ящика.
- В командной консоли Exchange выполните приведенную ниже команду.

  PowerShell

  ```
  Get-User <identity>
  ```

  Значение **UserMailbox** для свойства *RecipientType* указывает, что учетная запись пользователя и почтовый ящик подключены. Для проверки того, что почтовый ящик подключен, можно запустить командлет **Get-Mailbox <identity>**.

Восстановление удаленного почтового ящика

Чтобы восстановить удаленный почтовый ящик в существующем почтовом ящике, используйте командлет **New-MailboxRestoreRequest** в командной консоли Exchange. При восстановлении удаленного почтового ящика его содержимое копируется в существующий почтовый ящик, который называется *целевым почтовым ящиком*. После восстановления удаленного почтового ящика он хранится в базе данных почтовых ящиков до окончательного удаления администратором или очистки после истечения периода хранения удаленных почтовых ящиков.

Восстановленный почтовый ящик удаляется спустя 30 дней. Чтобы удалить его раньше, используйте командлета **Remove-StoreMailbox**.

> ⓘ **Примечание**
>
> Для восстановления удаленного почтового ящика нельзя использовать Центр администрирования Exchange.

Восстановление удаленного почтового ящика в командной консоли Exchange

Для создания запроса на восстановление почтового ящика нужно использовать отображаемое имя, различающееся имя прежней версии (DN) или идентификатор GUID из удаленного почтового ящика. Используйте командлет **Get-MailboxStatistics** , чтобы отобразить значения `DisplayName` свойств , `MailboxGuid` и `LegacyDN` для удаленного почтового ящика, который требуется восстановить. Например, выполните следующие команды, чтобы вернуть эти сведения для всех отключенных и удаленных почтовых ящиков в вашей организации.

PowerShell

```
$dbs = Get-MailboxDatabase
$dbs | foreach {Get-MailboxStatistics -Database $_.DistinguishedName} |
where {$_.DisconnectReason -eq "Disabled"} | Format-Table
DisplayName,MailboxGuid,Database,DisconnectDate
```

В этом примере удаленный почтовый ящик, который определяется параметром *SourceStoreMailbox* и находится в базе данных почтовых ящиков MBXDB01, восстанавливается в целевой почтовый ящик Debra Garcia. Используется параметр *AllowLegacyDNMismatch* , чтобы исходный почтовый ящик можно было восстановить в другой почтовый ящик, который не имеет прежнее значение DN.

PowerShell

```
New-MailboxRestoreRequest -SourceStoreMailbox e4890ee7-79a2-4f94-9569-
91e61eac372b -SourceDatabase MBXDB01 -TargetMailbox "Debra Garcia" -
AllowLegacyDNMismatch
```

В этом примере выполняется восстановление удаленного архивного почтового ящика Pilar Pinilla в текущем архивном почтовом ящике. Параметр *AllowLegacyDNMismatch* не является обязательным, так как основной почтовый ящик и соответствующий архивный почтовый ящик имеют одно и то же устаревшее DN.

PowerShell

```
New-MailboxRestoreRequest -SourceStoreMailbox "Personal Archive - Pilar Pinilla" -SourceDatabase "MDB01" -TargetMailbox pilarp@contoso.com -TargetIsArchive
```

Подробные сведения о синтаксисе и параметрах см. в разделе New-MailboxRestoreRequest.

Как проверить, все ли получилось?

Чтобы убедиться, что удаленный почтовый ящик успешно восстановлен в целевом почтовом ящике, выполните командлет **Get-MailboxRestoreRequest**, чтобы вывести сведения о запросе на восстановление. Если запрос на восстановление был успешно создан, свойство *Status* будет иметь значение `Queued`, `InProgress`или `Completed`. После завершения запроса на восстановление содержимое удаленного почтового ящика будет присутствовать в целевом почтовом ящике.

Дополнительные сведения см. в следующих разделах:

- Manage Mailbox Restore Requests
- Get-MailboxRestoreRequest
- Get-MailboxRestoreRequestStatistics

Окончательное удаление почтового ящика в Exchange Server

Статья • 04.04.2023

При окончательном удалении активных и отключенных почтовых ящиков все их содержимое навсегда удаляется из базы данных почтовых ящиков Exchange. При окончательном удалении активного почтового ящика связанная с ним учетная запись пользователя в Active Directory также удаляется.

Альтернативой окончательному удалению почтового ящика является его отключение. После отключения почтового ящика Exchange по умолчанию хранит данные в базе данных почтовых ящиков в течение 30 дней. Это дает вам возможность снова подключить или восстановить почтовый ящик до его удаления из базы данных.

Дополнительные сведения об отключенных почтовых ящиках и других задачах управления в Exchange см. в следующих разделах:

- Отключенные почтовые ящики
- Отключение или удаление почтового ящика в Exchange Server
- Подключение отключенного почтового ящика
- Подключение или восстановление удаленного почтового ящика

> ⓘ **Примечание**
>
> Для окончательного удаления активного или отключенного почтового ящика нельзя использовать Центр администрирования Exchange.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 2 минуты.
- Для процедур, описанных в этом разделе, требуется командная консоль Exchange. Дополнительные сведения см. в разделе Открытие командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе

"Разрешения подготовки получателей" раздела Разрешения получателей .

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Окончательное удаление активного почтового ящика в командной консоли Exchange

Если не включить параметр *Permanent* при удалении почтового ящика, удаленный почтовый ящик будет храниться в базе данных почтовых ящиков в течение 30 дней (по умолчанию) до окончательного удаления.

Выполните следующую команду, чтобы окончательно удалить активный почтовый ящик и связанную с ним учетную запись пользователя Active Directory:

PowerShell

```
Remove-Mailbox -Identity <Identity> -Permanent $true
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе Remove-Mailbox.

Как проверить, все ли получилось?

Чтобы убедиться в том, что активный почтовый ящик удален, выполните следующие действия:

1. Убедитесь, что почтовый ящик больше не указан в Центре администрирования Exchange (EAC).
2. Убедитесь, что связанная учетная запись пользователя больше не отображается в средстве "Пользователи и компьютеры Active Directory".

3. Замените *<DisplayName>* отображаемым именем почтового ящика и выполните следующие команды в командной консоли Exchange, чтобы убедиться, что почтовый ящик успешно очищен из базы данных почтовых ящиков Exchange:

   PowerShell

   ```
   $dbs = Get-MailboxDatabase
   $dbs | foreach {Get-MailboxStatistics -Database $_.DistinguishedName} |
   where {$_.DisplayName -eq "<DisplayName>"}
   ```

   Если почтовый ящик успешно очищен, команда не даст никаких результатов. Если почтовый ящик не был очищен, команда вернет сведения о почтовом ящике.

Использование командной консоли Exchange для поиска типа отключенного почтового ящика

Отключенный почтовый ящик можно отключить или удалить обратимо. Чтобы окончательно удалить отключенный почтовый ящик, необходимо указать правильный тип. В противном случае команда завершится ошибкой.

Замените *<DisplayName>* отображаемым именем почтового ящика и выполните следующую команду, чтобы определить, отключен или обратимо удален отключенный почтовый ящик:

PowerShell

```
$dbs = Get-MailboxDatabase
$dbs | foreach {Get-MailboxStatistics -Database $_.DistinguishedName} |
where {$_.DisplayName -eq "<DisplayName>"} | Format-List
DisplayName,MailboxGuid,Database,DisconnectReason
```

Значение свойства *DisconnectReason* будет иметь значение `Disabled` или `SoftDeleted`.

Чтобы отобразить тип для всех отключенных почтовых ящиков в организации, можно выполнить следующие команды:

PowerShell

```
$dbs = Get-MailboxDatabase
$dbs | foreach {Get-MailboxStatistics -Database $_.DistinguishedName} |
where {$_.DisconnectReason -ne $null} | Format-List
DisplayName,MailboxGuid,Database,DisconnectReason
```

Окончательное удаление отключенного почтового ящика в командной консоли Exchange

> ⊗ **Внимание!**
>
> При использовании командлета **Remove-StoreMailbox** для очистки отключенного почтового ящика и всего его содержимого из базы данных почтовых ящиков происходит окончательная потеря данных.

В этом примере окончательно удаляется отключенный почтовый ящик с идентификатором GUID 2ab32ce3-fae1-4402-9489-c67e3ae173d3 из базы данных почтовых ящиков с именем MBD01.

PowerShell

```
Remove-StoreMailbox -Database MBD01 -Identity "2ab32ce3-fae1-4402-9489-
c67e3ae173d3" -MailboxState Disabled
```

В этом примере безвозвратно удаляется обратимо удаленный почтовый ящик для Dan Jump из базы данных почтовых ящиков с именем MBD01.

PowerShell

```
Remove-StoreMailbox -Database MBD01 -Identity "Dan Jump" -MailboxState
SoftDeleted
```

В этом примере окончательно удаляются все обратимо удаленные почтовые ящики из базы данных почтовых ящиков с именем MBD01.

PowerShell

```
Get-MailboxStatistics -Database MBD01 | where {$_.DisconnectReason -eq
"SoftDeleted"} | ForEach {Remove-StoreMailbox -Database $_.Database -
Identity $_.MailboxGuid -MailboxState SoftDeleted}
```

Дополнительные сведения о синтаксисе и параметрах см. в разделах Remove-StoreMailbox и Get-MailboxStatistics.

Как проверить, все ли получилось?

Чтобы убедиться, что вы окончательно удалили отключенный почтовый ящик и что он был успешно очищен из базы данных почтовых ящиков, замените *<DisplayName>* отображаемым именем почтового ящика и выполните следующую команду:

PowerShell

```
$dbs = Get-MailboxDatabase
$dbs | foreach {Get-MailboxStatistics -Database $_.DistinguishedName} |
where {$_.DisplayName -eq "<DisplayName>"}
```

Если почтовый ящик успешно очищен, команда не даст никаких результатов. Если почтовый ящик не был очищен, команда вернет сведения о почтовом ящике.

Пользовательские атрибуты в Exchange Server

Статья • 04.04.2023

Exchange Server включает 15 атрибутов расширения, которые можно использовать для добавления сведений о получателе, таких как идентификатор сотрудника, подразделение или другое пользовательское значение, для которого нет существующего атрибута.

В более ранних версиях Exchange, чтобы сохранить такие сведения в Active Directory, необходимо было создать атрибут и расширить схему Active Directory. Для расширения схемы требовались планирование, получение идентификаторов объектов для новых атрибутов и проверка процесса расширения в тестовой среде перед его реализацией в производственной среде. Exchange Server не позволяет использовать расширения схемы в фильтрах получателей, которые используются списками адресов, политиками адресов электронной почты и динамическими группами рассылки.

Настраиваемые атрибуты, доступные Exchange Server, помечены в Active Directory как **ms-Exch-Extension-Attribute1** по **ms-Exch-Extension-Attribute15**. В командной консоли Exchange соответствующие параметры: *CustomAttribute1* – *CustomAttribute15*. Эти атрибуты не используются никакими компонентами Exchange. С их помощью можно хранить данные Active Directory, не расширяя схему Active Directory.

> ⓘ **Примечание**
>
> **Ms-Exch-Extension-Attribute-16** to **ms-Exch-Extension-Attribute-45** присутствуют в Active Directory, но недоступны в Центре администрирования Exchange (EAC) или командной консоли Exchange. Не используйте средства, отличные от Exchange, для изменения этих атрибутов, так как они могут использоваться для будущих функций Exchange.

Преимущества настраиваемых атрибутов

У настраиваемых атрибутов есть ряд преимуществ:

- Не требуется расширять схему Active Directory.

- Вам не нужно ничего делать, так как атрибуты создаются при установке Exchange.
- Для управления атрибутами можно использовать EAC или командную консоль Exchange. Не нужно создавать пользовательские элементы управления и писать скрипты для заполнения и отображения этих атрибутов.
- Атрибуты можно фильтровать и повторно использовать, так как атрибуты являются фильтруемыми свойствами, которые можно использовать в *параметре Filter* с помощью командлетов получателей, таких как **Get-Mailbox**. Их также можно использовать в Центре администрирования Exchange и командной консоли Exchange, чтобы создавать фильтры для политик адресов электронной почты, списков адресов и динамических групп рассылки.

Многозначные настраиваемые атрибуты

Начиная с Exchange 2010 с пакетом обновления 2 (SP2) в Exchange были добавлены пять многозначных настраиваемых атрибутов, которые позволяют хранить дополнительные сведения для получателей почты, если традиционные настраиваемые атрибуты не соответствуют вашим потребностям. Параметры *ExtensionCustomAttribute1* to *ExtensionCustomAttribute5* могут содержать до 1300 значений каждый. Вы можете указать несколько значений в виде списка, разделенного запятыми. Эти новые параметры поддерживаются в следующих командлетах:

- Настроить DistributionGroup
- Настроить DynamicDistributionGroup
- Set-Mailbox
- Set-MailContact
- Set-MailPublicFolder
- Set-RemoteMailbox

Дополнительные сведения о многозначных свойствах см. в разделе Modifying multivalued properties.

Примеры настраиваемых атрибутов

Распространенный сценарий во многих развертываниях Exchange — создание политики адресов электронной почты для всех получателей в подразделении. Подразделение не является фильтруемым свойством, которое можно использовать в *параметре RecipientFilter* политики адресов электронной почты или списка адресов.

> ⓘ **Примечание**
>
> У динамических групп рассылки есть дополнительный параметр, с помощью которого можно ограничивать их до получателей в определенном подразделении или контейнере.

Если получатели в этом подразделении не используют совместно какие-либо общие свойства, по которым можно выполнить фильтрацию, например отдел или местоположение, то один из настраиваемых атрибутов можно заполнить общим значением, как показано в приведенном ниже примере.

PowerShell

```
Get-Mailbox -OrganizationalUnit Sales | Set-Mailbox -CustomAttribute1
"SalesOU"
```

Теперь можно создать политику адресов электронной почты для всех получателей, у которых для свойства *CustomAttribute1* задано значение SalesOU, как показано в приведенном ниже примере.

PowerShell

```
New-EmailAddressPolicy -Name "Sales" -RecipientFilter "CustomAttribute1 -eq
'SalesOU'" -EnabledEmailAddressTemplates "SMTP:%s%2g@sales.contoso.com"
```

Пример настраиваемого атрибута с параметром ConditionalCustomAttributes

При создании динамических групп рассылки, политик адресов электронной почты или списков адресов не требуется использовать параметр *RecipeintFilter* для указания настраиваемых атрибутов. Вместо этого можно использовать параметры *ConditionalCustomAttribute1* to *ConditionalCustomAttribute15* .

В этом примере создается динамическая группа рассылки на основе получателей, для которых *customAttribute1* имеет значение SalesOU.

PowerShell

```
New-DynamicDistributionGroup -Name "Sales Users and Contacts" -
IncludedRecipients "MailboxUsers,MailContacts" -ConditionalCustomAttribute1
"SalesOU"
```

ⓘ Примечание

Если используется параметр *Conditional*, необходимо использовать параметр *IncludedRecipients*. Кроме того, нельзя использовать *условные* параметры, если используется параметр *RecipientFilter* . Чтобы включить дополнительные фильтры для создания динамической группы рассылки, политик адресов электронной почты или списков адресов, следует использовать параметр *RecipientFilter*.

Пример настраиваемых атрибутов с использованием параметра ExtensionCustomAttributes

В этом примере почтовый ящик для Kweku будет иметь *ExtensionCustomAttribute1* , чтобы отразить, что он зарегистрирован в следующих учебных классах: MATH307, ECON202 и ENGL300.

PowerShell

```
Set-Mailbox -Identity Kweku -ExtensionCustomAttribute1
MATH307,ECON202,ENGL300
```

Далее создается динамическая группа рассылки для всех учащихся, зарегистрированных в MATH307, с помощью параметра *RecipientFilter, где ExtensionCustomAttribute1* равен MATH307. При использовании параметров *ExtentionCustomAttributes* вместо оператора можно использовать `-eq` оператор `-like` .

PowerShell

```
New-DynamicDistributionGroup -Name Students_MATH307 -RecipientFilter
"ExtensionCustomAttribute1 -eq 'MATH307'"
```

В этом примере значения *ExtensionCustomAttribute1* в Kweku обновляются, чтобы отразить, что он добавил класс ENGL210 и удалил класс ECON202.

PowerShell

```
Set-Mailbox -Identity Kweku -ExtensionCustomAttribute1 @{Add="ENGL210";
Remove="ECON202"}
```

Управление разрешениями для получателей

Статья • 04.04.2023

В Exchange Server можно использовать Центр администрирования Exchange (EAC) или командную консоль Exchange для назначения разрешений почтовому ящику или группе, чтобы другие пользователи могли получить доступ к почтовому ящику (разрешение полного доступа) или отправлять сообщения электронной почты, которые, как представляется, приходят из почтового ящика или группы (разрешения Отправить как или Отправить от имени). Пользователи, которым назначены эти разрешения для других почтовых ящиков или групп, называются *делегатами*.

Разрешения, которые можно назначить делегатам для почтовых ящиков и групп в Exchange Server, описаны в следующей таблице:

Примечание. Хотя вы можете использовать командную консоль Exchange для назначения некоторых или всех этих разрешений другим типам делегатов для других типов объектов-получателей, этот раздел посвящен типам объектов делегатов и получателей, которые дают полезные результаты.

Разрешение	Описание	Типы получателей в EAC	Дополнительные типы получателей в PowerShell	Типы делегатов в EAC	Дополнительные типы делегатов в PowerShell
Полный доступ	Позволяет представителю открывать почтовый ящик, а также просматривать, добавлять и удалять его содержимое. Не разрешает представителю отправлять сообщения от имени почтового ящика. Если назначить разрешение на полный доступ почтовому ящику, скрытому из списков адресов, делегат не сможет открыть почтовый ящик. По умолчанию почтовые ящики разрешения конфликтов и найденных сообщений скрыты в списке адресов. По умолчанию функция автоматического сопоставления почтовых ящиков	почтовые ящики пользователей; Связанные почтовые ящики Почтовые ящики ресурса Общие почтовые ящики	Почтовые ящики разрешения конфликтов Почтовые ящики обнаружения	Почтовые ящики с учетными записями пользователей Почтовые пользователи с учетными записями Группы безопасности, поддерживающие почту	Учетные записи пользователей, не поддерживающие почту. Универсальные, глобальные и доменные локальные группы безопасности, не поддерживающие почту.

Разрешение	Описание	Типы получателей в EAC	Дополнительные типы получателей в PowerShell	Типы делегатов в EAC	Дополнительные типы делегатов в PowerShell
	использует автообнаружения для автоматического открытия почтового ящика в профиле Outlook делегата (в дополнение к собственному почтовому ящику). Обратите внимание, что автоматическое сопоставление будет работать только для отдельных пользователей, которым предоставлены соответствующие разрешения, и не будет работать для любой группы. Если вы не хотите, чтобы почтовые ящики были автоматически сопоставлены, необходимо выполнить одно из следующих действий: • Используйте командлет **Add-MailboxPermission** в командной консоли Exchange, чтобы назначить разрешение полный доступ с параметром `-AutoMapping $false`. Дополнительные сведения см. в разделе Использование командной консоли Exchange для назначения разрешения на полный доступ для почтовых ящиков этого раздела.				

Разрешение	Описание	Типы получателей в EAC	Дополнительные типы получателей в PowerShell	Типы делегатов в EAC	Дополнительные типы делегатов в PowerShell
	• Назначьте разрешение "Полный доступ" группе безопасности, поддерживающей почту. Почтовый ящик не открывается в профиле Outlook каждого участника.				
Отправить как	Позволяет представителю отправлять сообщения так, будто они поступают непосредственно от почтового ящика или группы. Нет никаких признаков того, что сообщение было отправлено представителем. Не разрешает представителю просматривать содержимое почтового ящика. Если назначить разрешение "Отправить как" почтовому ящику, скрытому из списков адресов, делегат не сможет отправлять сообщения из почтового ящика.	почтовые ящики пользователей; Связанные почтовые ящики Почтовые ящики ресурса Общие почтовые ящики группы рассылки; динамические группы рассылки группы безопасности с включенной поддержкой почты.	н/д	Почтовые ящики с учетными записями пользователей Почтовые пользователи с учетными записями Группы безопасности, поддерживающие почту	н/д

Разрешение	Описание	Типы получателей в EAC	Дополнительные типы получателей в PowerShell	Типы делегатов в EAC	Дополнительные типы делегатов в PowerShell
Отправить от имени	Позволяет представителю отправлять сообщения от имени почтового ящика или группы. В поле От адреса этих сообщений четко показано, что сообщение было отправлено делегатом (" *<Делегат>* от имени *<MailboxOrGroup>*"). Тем не менее ответы на эти сообщения отправляются почтовому ящику или группе, а не представителю. Не разрешает представителю просматривать содержимое почтового ящика. Если назначить разрешение Отправить от имени почтовому ящику, скрытому из списков адресов, делегат не сможет отправлять сообщения из почтового ящика.	почтовые ящики пользователей; Связанные почтовые ящики Почтовые ящики ресурса группы рассылки; динамические группы рассылки группы безопасности с включенной поддержкой почты.	Общие почтовые ящики	Почтовые ящики с учетными записями пользователей Почтовые пользователи с учетными записями группы безопасности с включенной поддержкой почты. Группы рассылки	н/д

> ⓘ **Примечание**
>
> Если у пользователя есть разрешения "Отправить как" и "Отправить от имени" в почтовый ящик или группу, разрешение "Отправить как" всегда используется.| Почтовые ящики пользователей

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 2 минут.
- Вам должны быть назначены разрешения, прежде чем вы сможете выполнять процедуры, описанные в этом разделе. Сведения о необходимых разрешениях см. в записи "Разрешения подготовки получателей" в разделе Разрешения получателей .
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

- Для процедур, описанных в этом разделе, требуются определенные разрешения. Сведения о разрешениях см. в каждой процедуре.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**.

Назначение разрешений отдельным почтовым ящикам с помощью Центра администрирования Exchange

1. В Центре администрирования Exchange выберите **Получатели** в области функций. В зависимости от типа почтового ящика, которому требуется назначить разрешения, выберите одну из следующих вкладок:
   - **Почтовые ящики**: пользовательские или связанные почтовые ящики.
   - **Ресурсы**: почтовые ящики комнат или оборудования.
   - **Общий**: общие почтовые ящики.
2. В списке почтовых ящиков выберите почтовый ящик, для которого требуется назначить разрешения, и нажмите кнопку **Изменить**.
3. На открывшейся странице свойств почтового ящика нажмите **Делегирование почтового ящика** и настройте одно или несколько из следующих разрешений:
   - **Отправить как**. Сообщения, отправленные делегатом, поступают из почтового ящика.
   - **Отправить от имени**. Сообщения, отправленные делегатом, имеют значение "<*Делегат*> от имени *почтового ящика*<>" в адресе От. Обратите внимание, что это разрешение недоступно в Центре администрирования Exchange для общих почтовых ящиков.
   - **Полный доступ**. Делегат может открыть почтовый ящик и выполнять любые действия, кроме отправки сообщений.

   Чтобы назначить разрешения делегатам, щелкните **добавить** Под соответствующим разрешением. Появится диалоговое окно со списком пользователей или групп, которым может быть назначено разрешение. Выберите пользователя или группу из списка и нажмите кнопку **Добавить**. Повторите эти действия необходимое количество раз. Вы также можете искать пользователей или группы в поле поиска, введя все или часть имени, а затем щелкнув . Завершив выбор делегатов, нажмите кнопку **OK**.

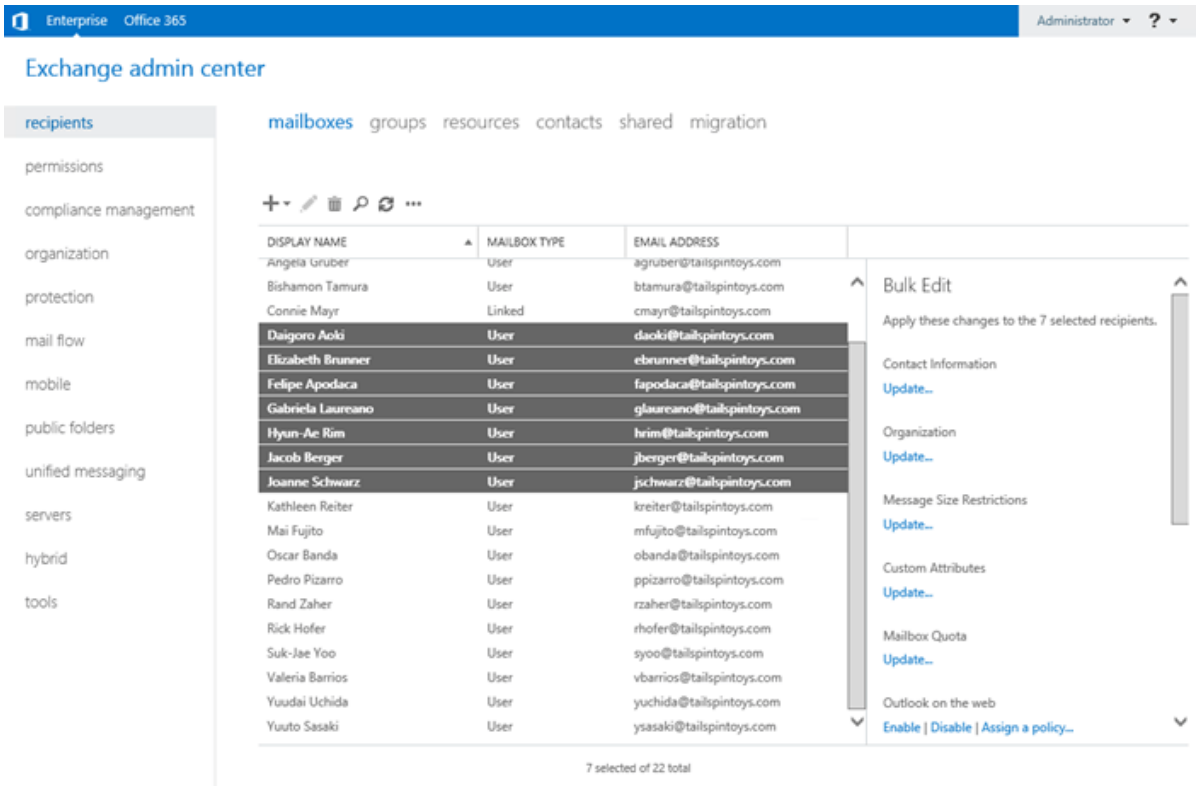
   Чтобы удалить разрешение делегата, выберите делегата в списке с соответствующим разрешением и нажмите кнопку **Удалить**

4. По завершении нажмите кнопку **Сохранить**.

Назначение разрешений нескольким почтовым ящикам одновременно с помощью Центра администрирования Exchange

1. В Центре администрирования Exchange (EAC) выберите **Получатели**>**Почтовые ящики**.

2. Выберите почтовые ящики, для которого требуется назначить разрешения. Для выбора диапазона почтовых ящиков используйте клавиши +SHIFT+щелчок, или клавиши CTRL+ щелчок, чтобы выбрать несколько отдельных почтовых ящиков. Заголовок области сведений изменится на **Массовое изменение** , как показано на следующей схеме.



Обратите внимание, что необходимо выбирать почтовые ящики одного типа. Например, если выбрать и почтовые ящики пользователей, и связанные почтовые ящики, в области сведений появится предупреждение о том, что массовое изменение невозможно.

3. В нижней части области сведений нажмите **Дополнительные параметры**. В появившемся параметре **Делегирование почтового ящика** выберите **Добавить** или **Удалить**. В зависимости от выбранной команды выполните одно из следующих действий:

   - **Добавить**. В появившемся диалоговом окне **Массовое добавление делегирования** щелкните ✚ Под соответствующим разрешением (**Отправить как**, **Отправить от имени** или **Полный доступ**). Завершив выбор пользователей или групп для добавления в качестве делегатов, нажмите кнопку **Сохранить**.

   - **Удалить**. В появившемся диалоговом окне **Массовое удаление делегирования** щелкните ✚ Под соответствующим разрешением (**Отправить как**, **Отправить от имени** или **Полный**

доступ). Завершив выбор пользователей или групп для удаления из существующих делегатов, нажмите кнопку **Сохранить**.

Назначение разрешений группам с помощью Центра администрирования Exchange

1. В Центре администрирования Exchange (EAC) выберите **Получатели**>**Группы**.
2. В списке групп выберите группу, для которой требуется назначить разрешения, и нажмите кнопку **Изменить**.
3. На открывшейся странице свойств группы нажмите **Делегирование группы** и настройте одно из следующих разрешений:
   - **Отправить как**. Сообщения, отправленные делегатом, по-видимому, поступают из группы.
   - **Отправить от имени**: сообщения, отправленные делегатом, имеют значение " <*Делегат*> от имени <*группы*>" в адресе От.
4. Чтобы назначить разрешения делегатам, щелкните **добавить** Под соответствующим разрешением. Появится диалоговое окно со списком пользователей или групп, которым может быть назначено разрешение. Выберите пользователя или группу из списка и нажмите кнопку **Добавить**. Повторите эти действия необходимое количество раз. Вы также можете искать пользователей или группы в поле поиска, введя все или часть имени, а затем щелкнув . Завершив выбор делегатов, нажмите кнопку **ОК**.

   Чтобы удалить разрешение делегата, выберите делегата в списке с соответствующим разрешением и нажмите кнопку **Удалить**
5. По завершении нажмите кнопку **Сохранить**.

Назначение разрешения на полный доступ почтовым ящикам с помощью командной консоли Exchange

Для управления разрешением "Полный доступ" для почтовых ящиков используются командлеты **Add-MailboxPermission** и **Remove-MailboxPermission**. В этих командлетах используется одинаковый базовый синтаксис.

PowerShell

```
Add-MailboxPermission -Identity <MailboxIdentity> -User <DelegateIdentity> -AccessRights
FullAccess -InheritanceType All [-AutoMapping $false]
```

Дополнительные сведения см. в статье Add-MailboxPermission.

PowerShell

```
Remove-MailboxPermission -Identity <MailboxIdentity> -User <DelegateIdentity> -AccessRights
FullAccess -InheritanceType All
```

Дополнительные сведения см. в статье Remove-MailboxPermission.

В этом примере разрешение полного доступа к почтовому ящику Терри Адамса назначается представителю Рэймонду Сэму.

PowerShell

```
Add-MailboxPermission -Identity "Terry Adams" -User raymonds -AccessRights FullAccess -
InheritanceType All
```

В этом примере Эстер Валле назначается разрешение на полный доступ для почтового ящика поиска обнаружения по умолчанию организации и предотвращается автоматическое открытие почтового ящика в Outlook Эстер Валле.

PowerShell

```
Add-MailboxPermission -Identity "DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-
7E09334BB852}" -User estherv -AccessRights FullAccess -InheritanceType All -AutoMapping
$false
```

В этом примере членам поддерживающей почту группы безопасности Helpdesk назначается разрешение на полный доступ к общему почтовому ящику под названием Helpdesk Tickets.

PowerShell

```
Add-MailboxPermission -Identity "Helpdesk Tickets" -User Helpdesk -AccessRights FullAccess -
InheritanceType All
```

В этом примере из почтового ящика пользователя Ayla Kol удаляется разрешение на полный доступ для пользователя Jim Hance.

PowerShell

```
Remove-MailboxPermission -Identity ayla -User "Jim Hance" -AccessRights FullAccess -
InheritanceType All
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно назначили или удалили разрешение на полный доступ для делегата в почтовом ящике, выполните одно из следующих действий:

- В свойствах почтового ящика в EAC убедитесь, что делегат указан или отсутствует в списке**Полный доступ кделегированию**> почтовых ящиков.
- Замените <*MailboxIdentity*> удостоверением почтового ящика и выполните следующую команду в командной консоли Exchange, чтобы убедиться, что делегат указан или отсутствует в списке.

  PowerShell

  ```
  Get-MailboxPermission <MailboxIdentity> | where {$_.AccessRights -like 'Full*'} |
  Format-Table -Auto User,Deny,IsInherited,AccessRights
  ```

Дополнительные сведения см. в статье Get-MailboxPermission.

Использование командной консоли Exchange для назначения разрешения "Отправить как" почтовым ящикам и группам

Командлеты Add-AdPermission и **Remove-AdPermission** используются для управления разрешением Отправить как для почтовых ящиков. В этих командлетах используется одинаковый базовый синтаксис.

```
PowerShell

<Add-AdPermission | Remove-AdPermission> -Identity <MailboxOrGroupNameOrDN> -User
<DelegateIdentity> [-AccessRights ExtendedRight] -ExtendedRights "Send As"
```

Дополнительные сведения см. в статьях Add-AdPermission и Remove-AdPermission.

Примечания.

- В качестве параметра *Identity* необходимо использовать значение **Name** или **DistinguishedName** (DN) почтового ящика или группы.
  - **Имя**. Это значение может быть или не совпадать с отображаемым именем. Например, `Felipe Apodaca`.
  - **Различающееся имя**. Это значение всегда содержит значение **Name** и использует синтаксис Active Directory LDAP. Например, `CN=Felipe Apodaca,CN=Users,DC=contoso,DC=com`.

  Чтобы найти эти значения для почтового ящика или группы, можно использовать командлет **Get-Recipient**, принимающий множество различных значений параметра *Identity*. Например:

  ```
  PowerShell

  Get-Recipient -Identity helpdesk@contoso.com | Format-List Name,DistinguishedName
  ```

- Команды работают с или без `-AccessRights ExtendedRight`, поэтому они отображаются как необязательные в синтаксисе.

В этом примере поддерживающей почту группе безопасности Helpdesk назначается разрешение "Отправить как" для общего почтового ящика Helpdesk Support Team.

```
PowerShell

Add-ADPermission -Identity "Helpdesk Support Team" -User Helpdesk -ExtendedRights "Send As"
```

В этом примере показывается удаление разрешения "Отправить как" для пользователя Елены Матвеевой на почтовом ящике Николая Белых.

```
PowerShell

Remove-ADPermission -Identity "James Alvord" -User pilarp -ExtendedRights "Send As"
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно назначили или удалили разрешение "Отправить как" для делегата в почтовом ящике или группе, выполните одно из следующих действий:

- В свойствах почтового ящика или группы в EAC убедитесь, что делегат указан или отсутствует в списке **Делегирование**> почтовых ящиков**Отправить как** или Отправить**какделегирование**> группы.
- Замените <*MailboxOrGroupNameOrDN*> именем или различающимися именами почтового ящика или группы и выполните следующую команду в командной консоли Exchange, чтобы убедиться, что делегат указан или отсутствует в списке.

  PowerShell

  ```
  Get-ADPermission -Identity <MailboxOrGroupNameOrDN> | where {$_.ExtendedRights -like 'Send*'} | Format-Table -Auto User,Deny,ExtendedRights
  ```

  Дополнительные сведения см. в статье Get-AdPermission.

Использование командной консоли Exchange для назначения разрешения Отправить от имени почтовым ящикам и группам

Параметр *GrantSendOnBehalfTo* используется в различных командлетах **set-** и group для управления разрешением Отправить от имени для почтовых ящиков и групп:

- **Set-Mailbox**
- **Set-DistributionGroup**: группы рассылки и группы безопасности с поддержкой почты.
- **Настроить DynamicDistributionGroup**

Базовый синтаксис этих командлетов:

PowerShell

```
<Cmdlet> -Identity <MailboxOrGroupIdentity> -GrantSendOnBehalfTo <Delegates>
```

Параметр *GrantSendOnBehalfTo* имеет следующие параметры для значений делегатов:

- **Замените существующие делегаты**: `<DelegateIdentity>` или `"<DelegateIdentity1>","<DelegateIdentity2>",...`
- **Добавление или удаление делегатов без влияния на других делегатов**: `@{Add="\<value1\>","\<value2\>"...; Remove="\<value1\>","\<value2\>"...}`
- **Удалить все делегаты**: используйте значение `$null`.

В этом примере показывается назначение разрешения "Отправить от имени" для пользователя Александры Вороновой почтовому ящику Глеба Селезнева.

PowerShell

```
Set-Mailbox -Identity seanc@contoso.com -GrantSendOnBehalfTo hollyh
```

В этом примере группа tempassistants@contoso.com добавляется в список делегатов, имеющих разрешение Отправить от имени в общий почтовый ящик Contoso Executives.

PowerShell

```
Set-Mailbox "Contoso Executives" -GrantSendOnBehalfTo @{Add="tempassistants@contoso.com"}
```

В этом примере показывается назначение разрешения "Отправить от имени" для пользователя Валентины Александровой группе рассылки поддержки принтеров.

PowerShell

```
Set-DistributionGroup -Identity printersupport@contoso.com -GrantSendOnBehalfTo sarad
```

В этом примере удаляется разрешение "Отправить от имени", назначенное администратору динамической группы рассылки All Employees.

PowerShell

```
Set-DynamicDistributionGroup "All Employees" -GrantSendOnBehalfTo @{Remove="Administrator"}
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно назначили или удалили разрешение Отправить от имени для делегата в почтовом ящике или группе, выполните одно из следующих действий:

- В свойствах почтового ящика или группы в EAC убедитесь, что делегат указан или отсутствует в списке **Делегирование**> почтовых ящиков**Отправить как** или Отправить**какделегирование**> группы.
- Замените <*MailboxIdentity*> или <*GroupIdentity*> удостоверением почтового ящика или группы и выполните одну из приведенных ниже команд в командной консоли Exchange, чтобы убедиться, что делегат указан или отсутствует в списке.
  - Почтовых ящиков:

    PowerShell

    ```
    Get-Mailbox -Identity <MailboxIdentity> | Format-List GrantSendOnBehalfTo
    ```

  - Группы:

    PowerShell

```
Get-DistributionGroup -Identity <GroupIdentity> | Format-List GrantSendOnBehalfTo
```

- Динамическая группа рассылки:

```
PowerShell

Get-DynamicDistributionGroup -Identity <GroupIdentity> | Format-List
GrantSendOnBehalfTo
```

Дальнейшие действия

Дополнительные сведения о том, как представители могут использовать назначенные им разрешения для почтовых ящиков и групп, см. в следующих статьях:

- Доступ к почтовому ящику другого пользователя
- Открытие и использование общего почтового ящика в Outlook для Windows
- Открытие и использование общего почтового ящика в Outlook в Интернете

Почтовый ящик перемещается в Exchange Server

Статья • 04.04.2023

Вы можете перемещать почтовые ящики в организацию Exchange, из нее и в ее пределах. Ниже перечислены основные типы перемещения почтовых ящиков.

- **Перемещение локальных почтовых ящиков**. Вы перемещаете почтовые ящики из одной базы данных почтовых ящиков в другую на серверах Exchange в пределах одного леса Active Directory. Инструкции см. в статье Управление перемещением локальных почтовых ящиков в Exchange Server.
- **Перемещение почтовых ящиков между лесами**. Вы перемещаете почтовые ящики на серверы Exchange в другом лесу Active Directory. Перемещение можно инициировать из леса, в который нужно переместить почтовые ящики (тип перемещения *извлечение*), или из леса, в котором в настоящий момент размещаются почтовые ящики (тип перемещения *отправка*). Дополнительные сведения см. в статье Подготовка почтовых ящиков для запросов на перемещение между лесами.
- **Удаленный почтовый ящик перемещается в гибридных развертываниях**. В гибридных развертываниях между локальной средой Exchange и Microsoft Office 365 вы можете перемещать почтовые ящики из Exchange в Microsoft 365 или Office 365 (известный как подключение *к миграции удаленного перемещения*), а также из Microsoft 365 или Office 365 в Exchange (известное как *отключение удаленной миграции перемещения*). Дополнительные сведения см. в статье Перемещение почтовых ящиков между локальными и Exchange Online организациями в гибридных развертываниях.

> ⓘ **Примечание**
>
> Дополнительные сведения о переносе локальных организаций Exchange в Microsoft 365 или Office 365 см. в статье **Способы переноса нескольких учетных записей электронной почты в Microsoft 365 или Office 365**.

Перемещение почтовых ящиков в Exchange 2016 и Exchange 2019 использует архитектуру пакетного перемещения, представленную в Exchange 2013. Архитектура пакетного перемещения позволяет перемещать почтовые ящики пакетами. Улучшенные возможности управления в архитектуре пакетного перемещения включают в себя:

- Электронное уведомление во время перемещения с созданием отчета.
- Автоматическая повторная попытка и автоматическое определение приоритетов перемещений.
- Перемещение основных и личных архивных почтовых ящиков вместе или по отдельности.
- Возможность завершения перемещения вручную, чтобы вы могли проверить перемещение до завершения.
- Периодическая добавочная синхронизация позволяет обновить изменения миграции.

Почтовые ящики можно перемещать в Центре администрирования Exchange и с помощью командлетов New-MoveRequest или New-MigrationBatch в командной консоли Exchange.

Сценарии перемещения почтовых ящиков (локального и между лесами)

Ниже приведены сценарии локального перемещения почтовых ящиков.

- **Обновление**. При обновлении с более ранней версии Exchange вы перемещаете почтовые ящики с существующих серверов Exchange на сервер почтовых ящиков Exchange.
- **Перераспределение**. Например, может потребоваться переместить почтовый ящик в базу данных с большим ограничением на размер почтового ящика.
- **Изучение проблемы**. Если вам нужно изучить проблему с почтовым ящиком, вы можете переместить этот почтовый ящик на другой сервер. Например, можно переместить на один сервер все почтовые ящики с большей активностью.
- **Поврежденные почтовые ящики**. Если вы столкнулись с поврежденными почтовыми ящиками, их можно переместить на другой сервер или базу данных. Поврежденные сообщения не перемещаются.
- **Изменения физического расположения**. Почтовые ящики можно перемещать на сервер на другом сайте Active Directory. Например, если пользователь перемещается в другое физическое местоположение, то его

почтовый ящик можно переместить на сервер, находящийся ближе к новому местоположению.

Ниже приведены сценарии перемещения почтовых ящиков между лесами.

- **Разделение административных ролей**. Может потребоваться отделить администрирование Exchange от администрирования учетных записей пользователей Active Directory. Для этого можно переместить почтовые ящики из одного леса в лес ресурсов. В этом сценарии почтовые ящики Exchange находятся в одном лесу, а связанные с ними учетные записи пользователей Active Directory — в другом лесу.

- **Администрирование электронной почты на стороне**. Возможно, вам потребуется передать на аутсорсинг администрирование электронной почты и сохранить администрирование учетных записей пользователей Active Directory. Для этого можно переместить почтовые ящики из одного леса в лес ресурсов.

- **Интеграция администрирования электронной почты и учетных записей пользователей**. Вам может потребоваться изменить модель администрирования электронной почты с разделим или аутсорсингом на модель, в которой электронной почтой и учетными записями пользователей можно управлять из одного леса. С этой целью можно переместить почтовые ящики из леса ресурсов в один лес. В этом сценарии почтовые ящики Exchange и учетные записи пользователей Active Directory находятся в одном лесу.

CSV-файлы для перемещения почтовых ящиков

Одним из основных преимуществ архитектуры пакетного перемещения является возможность указывать почтовые ящики для перемещения, используя CSV-файл. Сведения, которые необходимо указать в CSV-файле, зависят от типа перемещения. Дополнительные сведения см. в статье CSV Files for Mailbox Migration.

Конечные точки миграции для перемещения почтовых ящиков (между лесами и удаленного)

Конечные точки миграции используются для перемещения почтовых ящиков между лесами, а удаленный почтовый ящик перемещается между Exchange и Microsoft 365 или Office 365 в гибридных развертываниях. Не используйте конечные точки миграции для локального перемещения почтовых ящиков.

Конечные точки миграции указывают информацию об удаленном сервере, параметры регулирования исходной организации и необходимые учетные данные для переноса почтовых ящиков.

- Для перемещения почтовых ящиков между лесами требуется конечная точка миграции ExchangeRemoteMove.
- Для переноса почтовых ящиков в гибридных организациях (из Exchange в Microsoft 365 или Office 365) требуется конечная точка миграции ExchangeRemoteMove в качестве *источника* пакета миграции.
- Для переноса переносов почтовых ящиков в гибридных организациях (из Microsoft 365 или Office 365 в Exchange) требуется конечная точка миграции ExchangeRemoteMove в качестве *целевого объекта* пакета миграции.

Конечные точки миграции можно создавать в Центре администрирования Exchange и с помощью командлета New-MigrationEndpoint в командной консоли Exchange.

Конечные точки прокси-сервера MRS для перемещения почтовых ящиков (между лесами и удаленного)

Прокси-сервер службы репликации почтовых ящиков (MRS) облегчает перемещение почтовых ящиков между лесами и миграцию с удаленным перемещением. По умолчанию виртуальные каталоги EWS на серверах почтовых ящиков не настроены для приема входящих запросов на перемещение, поэтому необходимо включить конечную точку прокси-сервера MRS.

- При перемещении между лесами из целевого леса (перемещение по запросу) необходимо включить конечную точку прокси-сервера MRS виртуальных каталогов EWS на серверах почтовых ящиков в исходном лесу.
- При перемещении между лесами из исходного леса (push-перемещения) необходимо включить конечную точку прокси-сервера MRS виртуальных каталогов EWS на серверах почтовых ящиков в целевом лесу.

- Для подключения и отключения миграции удаленного перемещения в гибридных развертываниях необходимо включить конечную точку прокси-сервера MRS виртуальных каталогов EWS на серверах почтовых ящиков в локальной организации Exchange.

Дополнительные сведения см. в статье Включение конечной точки прокси-сервера MRS для удаленных перемещений.

Импорт и экспорт почтовых ящиков в Exchange Server

Статья • 04.04.2023

Exchange Server использует службу репликации почтовых ящиков Microsoft Exchange (MRS) для импорта PST-файлов в почтовые ящики и экспорта почтовых ящиков в PST-файлы. Ниже перечислены преимущества использования службы репликации почтовых ящиков вместо Outlook для импорта и экспорта почтовых ящиков.

- Запросы на импорт и экспорт являются асинхронными (вы можете импортировать и экспортировать несколько PST-файлов одновременно).
- Операции импорта и экспорта используют функции очередей и регулирования, имеющиеся в службе репликации почтовых ящиков.
- Вы можете импортировать PST-файл непосредственно в архивный почтовый ящик пользователя.
- Исходные или конечные PST-файлы можно хранить в любой сетевой папке, к которой есть доступ у ваших серверов Exchange.

Впервые эта функция появилась в Exchange 2010 с пакетом обновления 1 (SP1). В Exchange 2010 служба репликации почтовых ящиков работает на серверах клиентского доступа. В Exchange 2013 и более поздних версий служба репликации почтовых ящиков работает во внутренних службах на серверах почтовых ящиков (а не в службах клиентского доступа переднего плана).

> ⓘ **Примечание**
>
> Операции импорта и экспорта доступны только для роли "Импорт и экспорт почтового ящика", которая по умолчанию не назначена группе ролей. Чтобы использовать эти функции, добавьте роль "Импорт и экспорт почтового ящика" в группу ролей, в которую вы входите (например, в группу ролей "Управление организацией"). Дополнительные сведения см. в разделе **Добавление роли в группу ролей**.

Причины для импорта или экспорта почтовых ящиков

Администратору может требоваться импортировать PST-файлы в почтовые ящики или экспортировать почтовые ящики в PST-файлы. Например:

- **Требования к соответствию**. Вы можете экспортировать почтовый ящик в PST-файл для юридических целей обнаружения. По завершении экспорта вы можете импортировать PST-файл в почтовый ящик, специально используемый для целей обеспечения соответствия требованиям.

- **Создание моментального снимка почтового ящика на определенный момент времени**. Предположим, что вы храните резервную копию всей базы данных почтового ящика для нескольких почтовых ящиков. Выполняя экспорт этих почтовых ящиков в PST-файлы, вы можете отказаться от создания резервных копий базы данных почтовых ящиков.

- **Получение содержимого из PST-файлов и в почтовые ящики**. Как правило, пользователи Outlook могут сохранять сообщения электронной почты локально в PST-файлах. Вы можете импортировать PST-файлы пользователей в их основные или архивные почтовые ящики. Это простой способ передачи электронной почты с локального компьютера пользователя на сервер Exchange Server.

Рекомендации

Прежде чем импортировать PST-файлы в почтовые ящики или экспортировать почтовые ящики в PST-файлы, изучите указанные ниже проблемы.

- Необходимо использовать сетевую папку UNC (\ <*Server*>\ <*Share*>\ или \ <*LocalServerName*>\c$). Группе безопасности доверенной подсистемы Exchange необходимы разрешения на доступ к сетевой папке (разрешение на чтение для операций импорта, и разрешение на чтение и запись для операций экспорта). Если у сетевой папки нет этих разрешений, то когда вы попытаетесь импортировать или экспортировать PST-файлы, возникнет ошибка.

- Мы рекомендуем вам не пытаться импортировать или экспортировать PST-файлы размером более 50 гигабайтов (ГБ), так как 50 ГБ — это максимальный размер PST-файлов, поддерживаемый текущими версиями Outlook. Вы можете экспортировать почтовые ящики размером более 50 ГБ в PST-файлы, используя несколько запросов на экспорт, включающих или исключающих определенные папки, либо с помощью фильтра содержимого.

- На выполнение этих операций может потребоваться несколько часов в зависимости от размера PST-файлов или почтовых ящиков, доступной полосы пропускания сети и регулирования службы репликации почтовых ящиков.
- Вам не удается импортировать PST-файлы в общедоступные папки.

Импорт PST-файлов в почтовые ящики

Ниже указан ряд моментов, которые необходимо учесть при импорте PST-файлов в почтовые ящики.

- Вы можете создавать запросы на импорт новых почтовых ящиков в Центре администрирования или командной консоли Exchange. Командная консоль Exchange также необходима для просмотра, изменения, приостановки, возобновления или удаления запросов на импорт почтовых ящиков.
- Вы можете импортировать PST-файл в другой почтовый ящик. Например, можно экспортировать данные из john@contoso.com и импортировать их в legaldiscovery@contoso.com.
- Вы можете импортировать PST-файл непосредственно в личный архив пользователя, а не в его основной почтовый ящик.
- По умолчанию если в PST-файле имеются сопоставленные сообщения, то они будут импортированы. Сопоставленные сообщения — это особые сообщения, которые содержат скрытые данные о правилах, представлениях и формах. Этот параметр можно изменить в командной консоли Exchange (параметр *AssociatedMessagesCopyOption*).
- По умолчанию если в PST-файле есть папка "Элементы, подлежащие восстановлению", она будет импортирована. Этот параметр можно изменить в командной консоли Exchange (параметр *ExcludeDumpster*).
- В командную консоль Exchange можно включить или исключить определенные папки для импорта (параметры *IncludeFolders*, *ExcludeFolders* или *SourceRootFolder*).
- В командной консоли Exchange можно указать папку назначения для импортированных элементов в целевом почтовом ящике (параметр *TargetRootFolder*).
- В командной консоли Exchange можно увеличить или уменьшить значение приоритета для запросов на импорт почтовых ящиков (параметр *Priority*).

Процедуры импорта почтовых ящиков см. в разделе Процедуры импорта почтовых ящиков из PST-файлов в Exchange Server.

Экспорт почтовых ящиков в PST-файлы

Ниже указан ряд моментов, которые необходимо учесть при экспорте почтовых ящиков в PST-файлы.

- Вы можете создать запросы на экспорт новых почтовых ящиков в Центре администрирования Exchange или в Командная консоль Exchange. Чтобы просматривать, изменять, приостанавливать, возобновлять или удалять запросы на экспорт почтовых ящиков, вам потребуется использовать Командная консоль Exchange.

- Вы можете экспортировать почтовый ящик или архивный почтовый ящик пользователя в PST-файл.

- По умолчанию сопоставленные сообщения будут экспортированы из почтового ящика. Сопоставленные сообщения — это особые сообщения, которые содержат скрытые данные о правилах, представлениях и формах. Этот параметр можно изменить в командной консоли Exchange (параметр *AssociatedMessagesCopyOption*).

- По умолчанию папка "Элементы, подлежащие восстановлению" будет экспортирована из почтового ящика. Этот параметр можно изменить в командной консоли Exchange (параметр *ExcludeDumpster*).

- В командной консоли Exchange можно отфильтровать сообщения для экспорта из почтового ящика (параметр *ContentFilter*). Вы можете выполнить фильтрацию по контенту сообщений, вложениям, отправителям, получателям, категории папки "Входящие", важности, типам и размерам сообщений, времени и дате отправки, получения и истечения срока действия сообщений.

- В командную консоль Exchange можно включить или исключить определенные папки для экспорта (параметры *IncludeFolders*, *ExcludeFolders* или *SourceRootFolder*).

- В командной консоли Exchange можно указать папку назначения для экспортированных элементов в целевом PST-файле (параметр *TargetRootFolder*).

- В командной консоли Exchange можно увеличить или уменьшить значение приоритета для запросов на экспорт почтовых ящиков (параметр *Priority*).

Процедуры экспорта почтовых ящиков см. в статье Процедуры экспорта почтовых ящиков в PST-файлы в Exchange Server.

Процедуры импорта почтовых ящиков из PST-файлов в Exchange Server

Статья • 04.04.2023

Запросы на импорт почтовых ящиков используют службу репликации почтовых ящиков Microsoft Exchange (MRS) для импорта содержимого PST-файлов в почтовые ящики. Дополнительные сведения см. в статье Импорт и экспорт почтовых ящиков в Exchange Server.

В этой статье показано, как:

- создавать запросы на импорт почтовых ящиков;
- просматривать запросы на импорт почтовых ящиков;
- менять невыполненные запросы на импорт почтовых ящиков;
- приостанавливать невыполненные или неудачные запросы на импорт почтовых ящиков;
- возобновлять приостановленные или неудачные запросы на импорт почтовых ящиков;
- удалять запросы на импорт почтовых ящиков.

Что нужно знать перед началом работы

> ⓘ **Важно!**
>
> Для процедур, описанных в данной статье, требуется роль импорта и экспорта почтового ящика, которая не назначается по умолчанию группам ролей. Как назначить ее вашей группе ролей, см. в статье **Добавление роли в группу ролей**. Обратите внимание: чтобы изменения в разрешении вступили в силу, необходимо выйти из системы и войти в нее.

- Предполагаемое время для завершения каждой процедуры: 5 минут
- Необходимо импортировать PST-файлы из UNC-сетевой папки (\ <*Server*>\ <*Share*>\ или \ <*LocalServerName*>\c$). Группе безопасности доверенной

подсистемы Exchange требуется разрешение на чтение для сетевой папки. Если это разрешение для папки не задано, при импорте PST-файлов в почтовые ящики будут происходить ошибки.

- Запросы на импорт почтовых ящиков можно создавать в Центре администрирования Exchange (EAC) или в командной консоли Exchange. Все остальные процедуры можно выполнить только в командной консоли Exchange. Дополнительные сведения о доступе и использовании Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

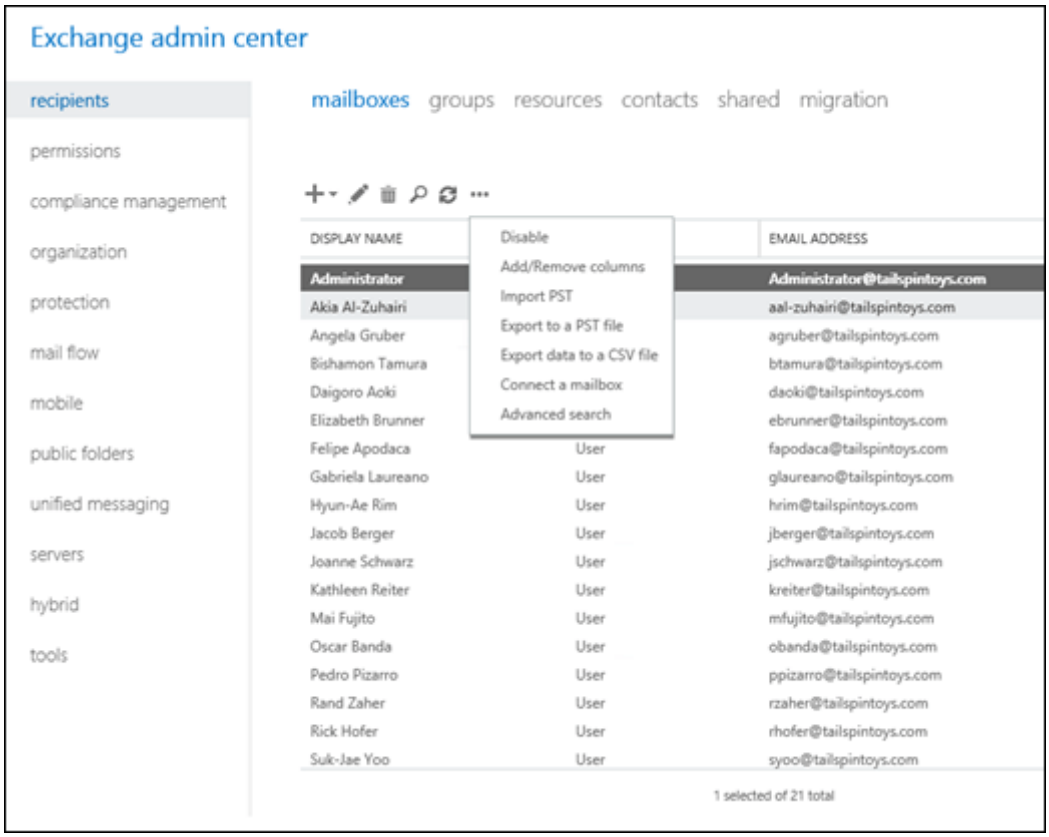
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

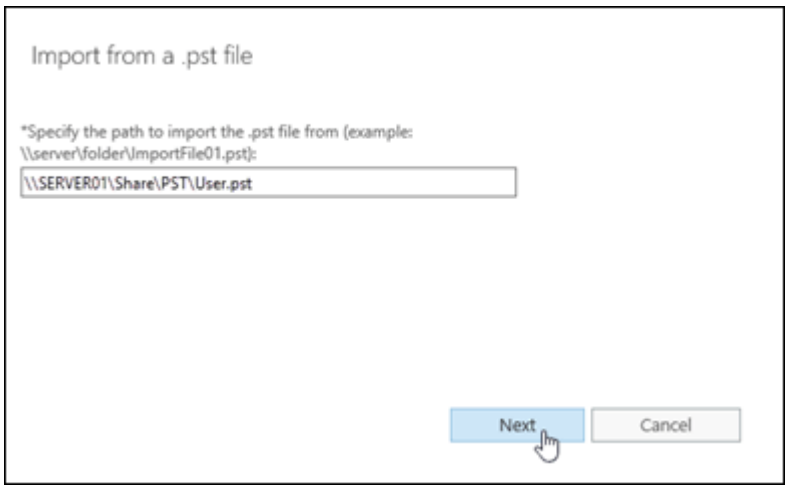
Создание запросов на импорт почтовых ящиков

Создание запроса на импорт почтового ящика с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел **Почтовые ящики**>> получателей, щелкните ••• **параметры** и выберите **Импорт PST**.



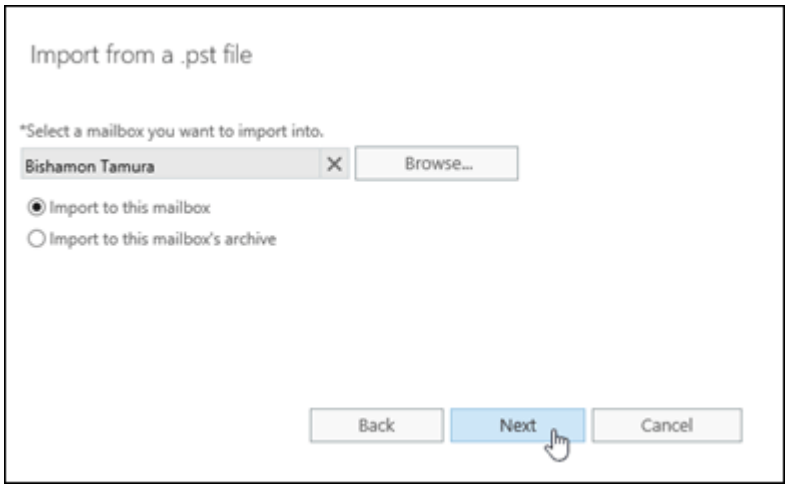
2. Откроется **мастер импорта из PST-файла**. На первой странице введите UNC-путь и имя исходного PST-файла.



   По завершении нажмите кнопку **Далее**.

3. На следующей странице выберите целевой почтовый ящик, а затем — один из следующих вариантов:

   - **Импорт в этот почтовый ящик**
   - **Импорт в архив этого почтового ящика**

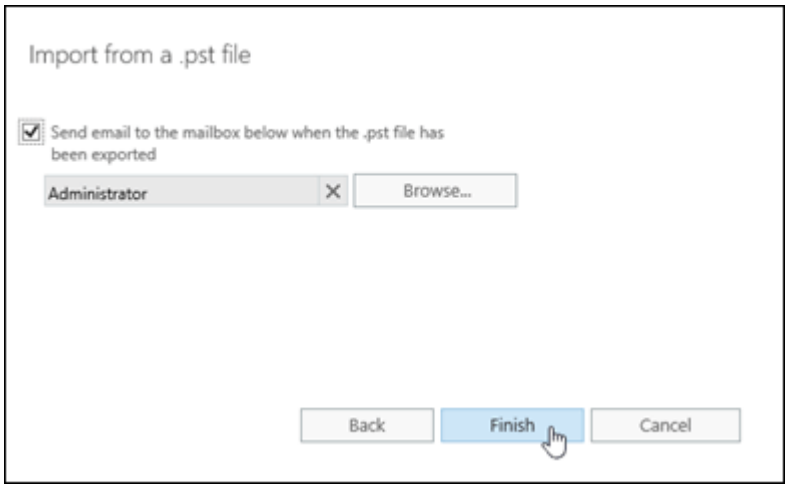


По завершении нажмите кнопку **Далее**.

4. На последней странице настройте один из этих параметров:

   - Не снимайте флажок **Отправлять сообщение на указанный ниже почтовый ящик при экспорте файла .pst**. Нажмите кнопку **Обзор**, чтобы добавить или удалить получателей уведомления.

   - Снимите флажок **Отправлять сообщение на указанный ниже почтовый ящик при экспорте файла .pst**.



Закончив, нажмите кнопку **Готово**.

Создание запроса на импорт почтового ящика с помощью командной консоли Exchange

Чтобы создать запрос на импорт почтового ящика, используйте следующий синтаксис:

```
PowerShell
```

```
New-MailboxImportRequest  [-Name <UniqueName>] -FilePath <UNCPathToPST> -
Mailbox <TargetMailboxIdentity> [-IsArchive] [-SourceRootFolder <PSTFolder>]
[-TargetRootFolder <MailboxFolder>] [-IncludeFolders <MailboxFolder1>,
<MailboxFolder2>...] [-ExcludeFolders <MailboxFolder1>,<MailboxFolder2>...]
[-Priority <PriorityValue>]
```

В этом примере создается запрос на импорт почтового ящика со следующими параметрами:

- **Имя запроса на импорт почтового ящика**. Используется значение `MailboxImport` по умолчанию, так как мы не используем параметр *Name* . Уникальное удостоверение запроса на импорт почтового ящика — `<MailboxIdentity>\MailboxImportX` (*X* отсутствует или имеет значение от 0 до 9).
- **Исходный PST-файл**: \\SERVER01\PSTFiles\Archives\Vbarrios.pst
- **Целевой почтовый ящик**: Валерия Барриос
- **Содержимое и папки**. Содержимое во всех путях к папкам в PST-файле реплицируется в целевом почтовом ящике. В противном случае создается новая папка.
- **Priority**: `Normal`, так как мы не используем параметр *Priority* .

PowerShell

```
New-MailboxImportRequest -FilePath \\SERVER01\PSTFiles\Archives\Vbarrios.pst
-Mailbox "Valeria Barrios"
```

В этом примере создается запрос на импорт почтового ящика со следующими параметрами:

- **Имя запроса на импорт почтового ящика**. Настраиваемое имя Kathleen Reiter Import указывается параметром *Name* . При указании настраиваемого имени допускается более 10 запросов на импорт почтового ящика. Уникальное значение удостоверения запроса на импорт почтового ящика — `<MailboxIdentity>\<MailboxImportRequestName>` (например, `kreiter\Kathleen Reiter Import`).
- **Исходный PST-файл**: \\SERVER01\PSTFiles\Archives\Recovered.pst
- **Целевой почтовый ящик**: архивный почтовый ящик для Кэтлин Рейтер (основной псевдоним почтового ящика Kathleen — kreiter).

- **Содержимое и папки**. Импортируется только содержимое из папки "Входящие" PST-файла (независимо от локализованного имени папки) и импортируется в папку "Восстановленные файлы" в целевом почтовом ящике.
- **Приоритет**: `High`

PowerShell

```
New-MailboxImportRequest -Name "Kathleen Reiter Import" -FilePath
\\SERVER01\PSTFiles\Recovered.pst -Mailbox kreiter -IsArchive -
IncludeFolders "#Inbox#" -TargetRootFolder "Recovered Files" -Priority High
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе New-MailboxImportRequest.

Как проверить, все ли получилось?

Чтобы убедиться, что запрос на импорт почтового ящика успешно создан, выполните одно из указанных ниже действий.

- В Центре администрирования Майкрософт щелкните 🔔 средства просмотра уведомлений. Чтобы просмотреть состояние запроса.
- Если вы создали запрос на импорт почтового ящика в Центре администрирования Exchange и установили флажок для отправки уведомлений по электронной почте, проверьте, пришли ли сообщения. Отправитель — Microsoft Exchange. Первое сообщение содержит тему `Your Import PST request has been received`. Если запрос на импорт успешно выполнен, вы получите другое сообщение с темой `Import PST has finished`.
- Замените <*MailboxIdentity*> именем, адресом электронной почты или псевдонимом целевого почтового ящика и выполните следующую команду в командной консоли Exchange, чтобы проверить основные значения свойств:

  PowerShell

  ```
  Get-MailboxImportRequest -Mailbox "<MailboxIdentity>" | Format-List
  Name,FilePath,Mailbox,Status
  ```

- Замените <*MailboxIdentity*> и <*MailboxImportRequestName*> соответствующими значениями и выполните следующую команду в командной консоли Exchange, чтобы проверить сведения:

PowerShell

```
Get-MailboxImportRequestStatistics -Identity "<MailboxIdentity>\
<MailboxImportRequestName>"
```

Просмотр запросов на импорт почтовых ящиков с помощью командной консоли Exchange

По умолчанию командлет **Get-MailboxImportRequest** возвращает имя, целевой почтовый ящик и состояние запроса на импорт почтового ящика. Если передать команду конвейерным образом в командлет **Format-List**, вы получите только ограниченное число дополнительных полезных сведений:

- **FilePath**: исходный PST-файл.
- **RequestGUID**: уникальное значение GUID запроса на импорт почтового ящика.
- **RequestQueue**: база данных почтовых ящиков, в которой выполняется запрос на импорт.
- **BatchName**: необязательное имя пакета для запроса на импорт почтового ящика.
- **Identity**: уникальное значение удостоверения запроса на импорт почтового ящика (<*MailboxIdentity*>\ <*MailboxImportRequestName*>).

По умолчанию командлет **Get-MailboxImportRequestStatistics** возвращает имя, состояние и псевдоним целевого почтового ящика, а также процент выполнения запроса на импорт почтового ящика. Отправив команду конвейерным образом в командлет **Format-List**, вы увидите подробные сведения о запросе на импорт почтового ящика.

В этом примере возвращается сводный список всех запросов на импорт почтовых ящиков.

PowerShell

```
Get-MailboxImportRequest
```

В этом примере возвращаются дополнительные сведения о запросах на импорт в почтовый ящик Akia Al-Zuhairi.

PowerShell

```
Get-MailboxImportRequest -Mailbox "Akia Al-Zuhairi" | Format-List
```

В этом примере возвращается сводный список выполняющихся запросов на импорт для почтовых ящиков, которые хранятся в базе данных почтовых ящиков с именем DB01.

PowerShell

```
Get-MailboxImportRequest -Status InProgress -Database DB01
```

В этом примере возвращается сводный список выполненных запросов на импорт почтовых ящиков в пакете с именем Import DB01 PSTs.

PowerShell

```
Get-MailboxImportRequest -Status Completed -BatchName "Import DB01 PSTs"
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Get-MailboxImportRequest.

Чтобы просмотреть подробные сведения о запросе на импорт почтового ящика, используйте следующий синтаксис:

PowerShell

```
Get-MailboxImportRequestStatistics -Identity <MailboxImportRequestIdentity>
[-IncludeReport] | Format-List
```

Где <*MailboxImportRequestIdentity*> — это значение удостоверения запроса на импорт почтового ящика (<*MailboxIdentity*>\ <*MailboxImportRequestName*> или <*RequestGUID*>).

В этом примере возвращаются подробные сведения о запросе MailboxExport на импорт в почтовый ящик пользователя Akia Al-Zuhairi, включая журнал действий в свойстве **Report**.

PowerShell

```
Get-MailboxImportRequestStatistics -Identity "aal-zuhairi\MailboxImport" -
IncludeReport | Format-List
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Get-MailboxImportRequestStatistics.

Изменение запросов на импорт почтовых ящиков с помощью командной консоли Exchange

Вы можете менять невыполненные запросы на импорт почтовых ящиков. Невозможно изменить базовые параметры существующего запроса (например, исходный PST-файл, целевой почтовый ящик, исходное содержимое в PST-файле или назначение в конечном почтовом ящике).

Чтобы изменить запрос на импорт почтового ящика, используйте следующий синтаксис:

PowerShell

```
Set-MailboxImportRequest -Identity <MailboxIdentity>\
<MailboxImportRequestName> [-BadItemLimit <value>] [-LargeItemLimit <value>]
[-AcceptLargeDataLoss]
```

В этом примере показано, как изменить неудачный запрос на импорт в почтовый ящик пользователя Valeria Barrios, чтобы принималось не более пяти поврежденных элементов почтового ящика.

PowerShell

```
Set-MailboxImportRequest -Identity "Valeria Barrios\MailboxImport" -
BadItemLimit 5
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Set-MailboxImportRequest.

Примечание. После изменения приостановленного или неудачного запроса на импорт почтового ящика необходимо возобновить его с помощью командлета **Resume-MailboxImportRequest**.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно изменили запрос на импорт почтового ящика, замените *<MailboxIdentity>* и *<MailboxImportRequestName>* соответствующими

значениями и выполните следующую команду в командной консоли Exchange, чтобы проверить сведения:

```
PowerShell

Get-MailboxImportRequestStatistics -Identity "<MailboxIdentity>\
<MailboxImportRequestName>" | Format-List
```

Приостановка запросов на импорт почтовых ящиков с помощью командной консоли Exchange

Вы можете приостанавливать выполняющиеся запросы на импорт почтовых ящиков. Невозможно приостанавливать выполненные или неудачные запросы на импорт почтовых ящиков.

Чтобы приостановить запрос на импорт почтового ящика, используйте следующий синтаксис:

```
PowerShell

Suspend-MailboxImportRequest -Identity <MailboxIdentity>\
<MailboxImportRequestName> [-SuspendComment "<Descriptive Comment>"]
```

В этом примере приостанавливается запрос Kathleen Reiter Export на импорт в почтовый ящик пользователя Kathleen Reiter.

```
PowerShell

Suspend-MailboxImportRequest -Identity "kreiter@contoso.com\Kathleen Reiter
Import"
```

В этом примере приостанавливаются все выполняющиеся запросы на импорт почтовых ящиков с примечанием "OK to resume after 10 P.M. on Monday 6/19" (Возобновить после 22:00 в понедельник 19.06)

```
PowerShell

Get-MailboxImportRequest -Status InProgress | Suspend-MailboxImportRequest -
SuspendComment "OK to resume after 10 P.M. on Monday 6/19"
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Suspend-MailboxImportRequest.

Примечания.

- Вы также можете использовать командлет **New-MailboxImportRequest** с параметром *Suspend*, чтобы создать приостановленный запрос на импорт почтового ящика.
- Параметр **Resume-MailboxImportRequest** используется для возобновления приостановленных запросов на импорт почтовых ящиков.

Как проверить, все ли получилось?

Чтобы убедиться, что запрос на импорт почтового ящика успешно приостановлен, выполните одно из следующих действий:

- Замените <*MailboxIdentity*> именем, адресом электронной почты или псевдонимом целевого почтового ящика, выполните эту команду в командной консоли Exchange и убедитесь, что свойство **Status** имеет значение `Suspended`:

  PowerShell

  ```
  Get-MailboxImportRequest -Mailbox "<MailboxIdentity>" | Format-List Name,FilePath,Mailbox,Status
  ```

- Выполните следующую команду в командной консоли Exchange и убедитесь, что запрос на импорт приостановленного почтового ящика указан:

  PowerShell

  ```
  Get-MailboxImportRequest -Status Suspended
  ```

Возобновление запросов на импорт почтовых ящиков с помощью командной консоли Exchange

Вы можете возобновлять приостановленные или неудачные запросы на импорт почтовых ящиков.

Чтобы возобновить запрос на импорт почтового ящика, используйте следующий синтаксис:

```
PowerShell

Resume-MailboxImportRequest -Identity <MailboxIdentity>\
<MailboxImportRequestName>
```

В этом примере возобновляется неудачный запрос на импорт почтового ящика пользователя Valeria Barrios.

```
PowerShell

Resume-MailboxImportRequest -Identity vbarrios\MailboxImport
```

В этом примере возобновляются все приостановленные запросы на импорт почтовых ящиков.

```
PowerShell

Get-MailboxImportRequest -Status Suspended | Resume-MailboxImportRequest
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Resume-MailboxImportRequest.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно возобновили запрос на импорт почтового ящика, замените *<MailboxIdentity>* именем, адресом электронной почты или псевдонимом целевого почтового ящика, выполните следующую команду в командной консоли Exchange и убедитесь, что свойство **Status** не имеет значения `Suspended`:

```
PowerShell

Get-MailboxImportRequest -Mailbox <MailboxIdentity> | Format-List
Name,FilePath,Mailbox,Status
```

Удаление запросов на импорт с помощью командной консоли Exchange

Вы можете удалить полностью или частично выполненные запросы на импорт почтовых ящиков.

- При удалении частично выполненного запроса на импорт почтового ящика этот запрос удаляется из очереди заданий в службе репликации почтовых ящиков (MRS). Содержимое, уже импортированное из PST-файла, не удаляется из целевого почтового ящика.

- По умолчанию завершенный запрос на импорт почтового ящика удаляется через 30 дней (это значение можно переопределить с помощью параметра *CompletedRequestAgeLimit*), а неудачные запросы не удаляются автоматически. Но если при создании или изменении запроса на импорт почтового ящика используется параметр *RequestExpiryInterval*, доступны следующие результаты:

  - **RequestExpiryInterval со значением интервала времени**. Завершенные и неудачные запросы автоматически удаляются после указанного интервала времени.

  - **RequestExpiryInterval со значением unlimited**: завершенные и неудачные запросы не удаляются автоматически.

В этом примере удаляется запрос с именем MailboxImport на импорт в почтовый ящик пользователя Akia Al-Zuhairi.

PowerShell

```
Remove-MailboxImportRequest -Identity "aal-zuhairi\MailboxImport"
```

В этом примере удаляются все выполненные запросы на импорт почтовых ящиков.

PowerShell

```
Get-MailboxImportRequest -Status Completed | Remove-MailboxImportRequest
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Remove-MailboxImportRequest.

Как проверить, все ли получилось?

Чтобы убедиться, что запрос на импорт почтового ящика успешно удален, замените *<MailboxIdentity>* именем, адресом электронной почты или псевдонимом целевого почтового ящика, выполните следующую команду в командной консоли Exchange и убедитесь, что запрос на импорт почтового ящика отсутствует в списке:

PowerShell

```
Get-MailboxImportRequest -Mailbox <MailboxIdentity> | Format-List
Name,FilePath,Mailbox,Status
```

Процедуры экспорта почтовых ящиков в PST-файлы в Exchange Server

Статья • 04.04.2023

Запросы на экспорт почтовых ящиков используют службу репликации почтовых ящиков Microsoft Exchange (MRS) для экспорта содержимого почтовых ящиков в PST-файлы. Дополнительные сведения см. в статье Импорт и экспорт почтовых ящиков в Exchange Server.

В этой статье рассказывается, как:

- создавать запросы на экспорт почтовых ящиков;
- просматривать запросы на экспорт почтовых ящиков;
- изменять невыполненные запросы на экспорт почтовых ящиков;
- приостанавливать невыполненные или неудачные запросы на экспорт почтовых ящиков;
- возобновлять приостановленные или неудачные запросы на экспорт почтовых ящиков;
- удалять запросы на экспорт почтовых ящиков.

Что нужно знать перед началом работы

> ⓘ **Важно!**
>
> Для процедур, описанных в данной статье, требуется роль импорта и экспорта почтового ящика, которая не назначается по умолчанию группам ролей. Как назначить ее вашей группе ролей, см. в статье **Добавление роли в группу ролей**. Обратите внимание: чтобы изменения в разрешении вступили в силу, необходимо выйти из системы и войти в нее.

- Предполагаемое время для завершения каждой процедуры: 5 минут
- Необходимо экспортировать почтовые ящики в PST-файлы в сетевой папке UNC (\ <*Server*>\ <*Share*>\ или \ <*LocalServerName*>\c$). Группе безопасности

доверенных подсистем Exchange необходимо разрешение на чтение и запись для сетевой папки. Если данное разрешение для папки не установлено, при экспорте почтовых ящиков в PST-файлы будут происходить ошибки.

- Запросы на экспорт почтовых ящиков можно создавать в Центре администрирования Exchange (EAC) или в командной консоли Exchange. Все остальные процедуры можно выполнить только в командной консоли Exchange. Дополнительные сведения о доступе и использовании Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

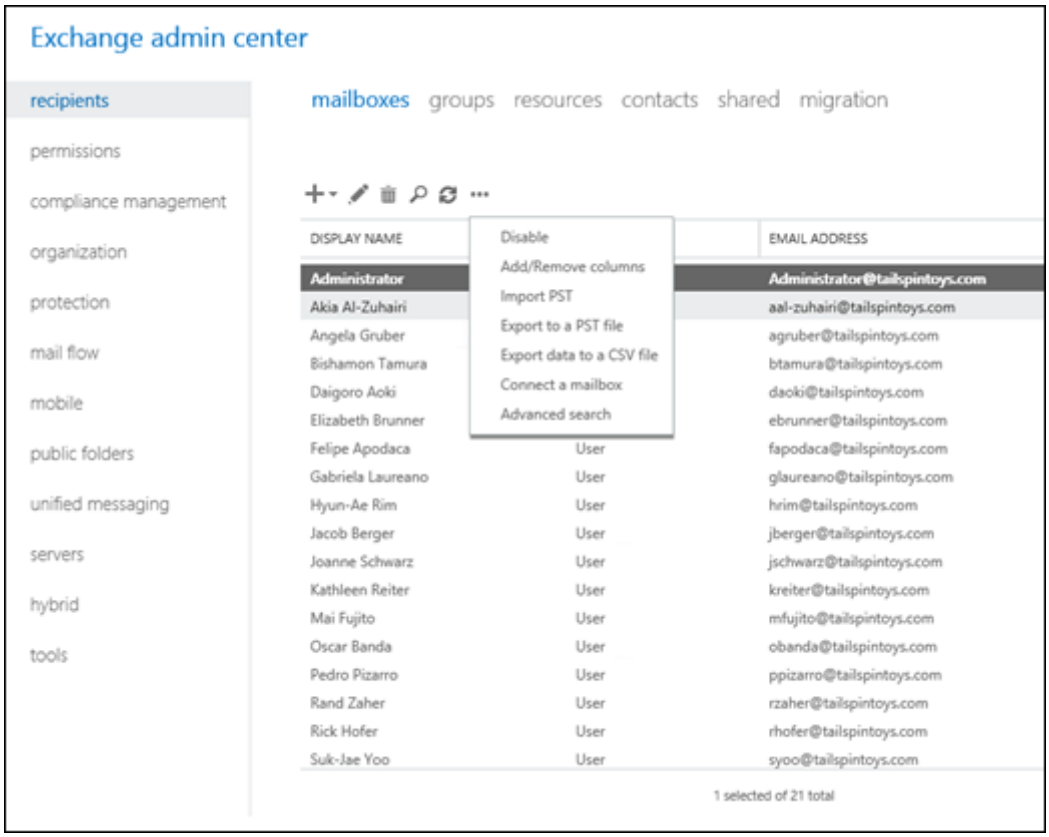
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Создание запросов на экспорт почтовых ящиков

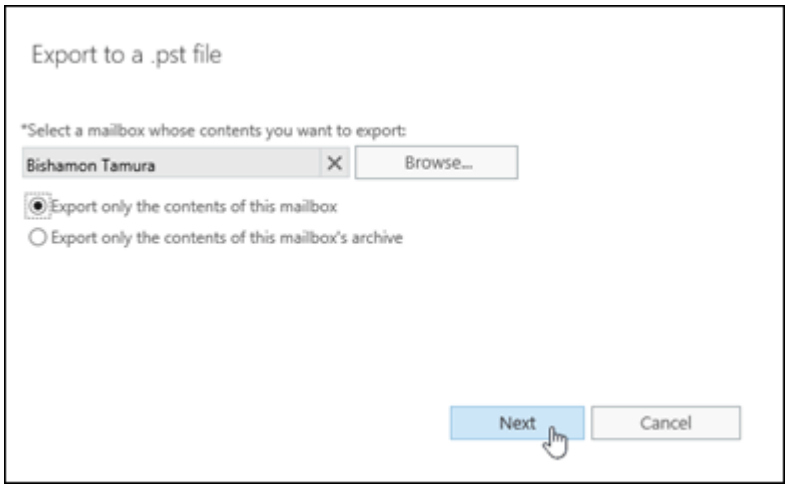
Использование Центра администрирования Exchange для создания запроса на экспорт почтового ящика

1. В EAC перейдите в раздел **Почтовые ящики**>> получателей, щелкните ••• **Дополнительные параметры** и выберите **Экспорт в PST-файл**.



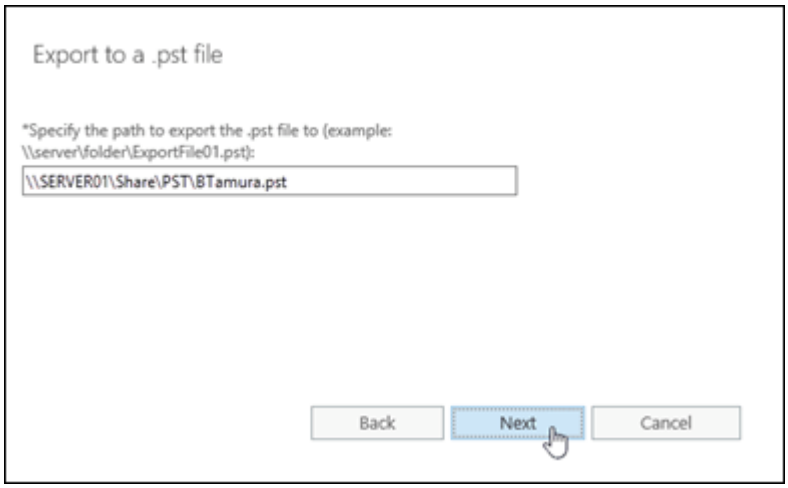
2. Откроется мастер **Экспорт в PST-файл**. На первой странице выберите исходный почтовый ящик, а затем — один из следующих вариантов:

   - **Экспортировать только содержимое данного почтового ящика**.
   - **Экспортировать только содержимое архива данного почтового ящика**.



   По завершении нажмите кнопку **Далее**.

3. На следующей странице введите UNC-путь и имя конечного PST-файла.

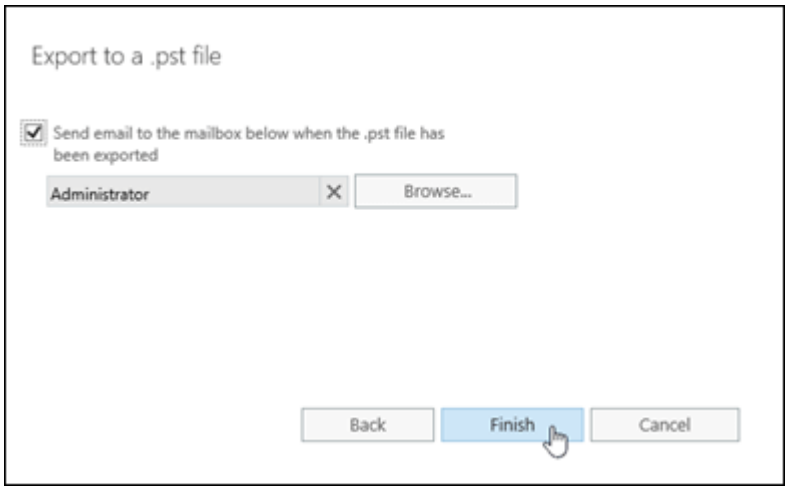


По завершении нажмите кнопку **Далее**.

4. На последней странице настройте один из этих параметров:

   - Не снимайте флажок **Отправлять сообщение на указанный ниже почтовый ящик при экспорте файла .pst**. Нажмите кнопку **Обзор**, чтобы добавить или удалить получателей уведомления.

   - Снимите флажок **Отправлять сообщение на указанный ниже почтовый ящик при экспорте файла .pst**.



Закончив, нажмите кнопку **Готово**.

Создание запроса на экспорт почтового ящика с помощью командной консоли Exchange.

Чтобы создать запрос на экспорт почтового ящика, используйте данный синтаксис:

PowerShell

```
New-MailboxExportRequest  [-Name <UniqueName>] -Mailbox
<TargetMailboxIdentity> -FilePath <UNCPathToPST> [-IsArchive] [-
```

```
SourceRootFolder <MailboxFolder>] [-TargetRootFolder <PSTFolder>] [-
IncludeFolders <MailboxFolder1>,<MailboxFolder2>...] [-ExcludeFolders
<MailboxFolder1>,<MailboxFolder2>...] [-ContentFilter <Filter>] [-Priority
<PriorityValue>]
```

В этом примере создается запрос на экспорт почтового ящика со следующими параметрами:

- **Имя запроса на экспорт почтового ящика**. Используется значение `MailboxExport` по умолчанию, так как мы не используем параметр *Name* . Уникальное удостоверение запроса на экспорт почтового ящика — `<MailboxIdentity>\MailboxExportX` (*X* отсутствует или имеет значение от 0 до 9).
- **Исходный почтовый ящик**: Валерия Барриос
- **Целевой PST-файл**: \SERVER01\PSTFiles\Vbarrios.pst
- **Содержимое и папки**. Содержимое во всех путях к папкам в исходном почтовом ящике реплицируется в целевой PST-файл.
- **Priority**: `Normal`, так как мы не используем параметр *Priority* .

PowerShell

```
New-MailboxExportRequest -Mailbox "Valeria Barrios" -FilePath
\\SERVER01\PSTFiles\Vbarrios.pst
```

В этом примере создается запрос на экспорт почтового ящика со следующими параметрами:

- **Имя запроса на экспорт почтового ящика**. Настраиваемое имя Kathleen Reiter Export указывается с помощью параметра *Name* . Указание настраиваемого имени дает возможность создавать более 10 запросов на экспорт для почтового ящика. Уникальное значение удостоверения запроса на экспорт почтового ящика — `<MailboxIdentity>\<MailboxExportRequestName>` (например, `kreiter\Kathleen Reiter Export`).
- **Исходный почтовый ящик**: архивный почтовый ящик для Кэтлин Рейтер (основной псевдоним почтового ящика Кэтлин — kreiter).
- **Целевой PST-файл**: \SERVER01\PSTFiles\Archives\Kathleen Reiter.pst
- **Содержимое и папки**. Экспортируется только содержимое папки "Входящие" почтового ящика (независимо от локализованного имени папки).

- **Приоритет**: `High`

```
PowerShell

New-MailboxExportRequest -Name "Kathleen Reiter Export" -Mailbox kreiter -
FilePath "\\SERVER01\PSTFiles\Kathleen Reiter.pst" -IsArchive -
IncludeFolders "#Inbox#" -Priority High
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе New-MailboxExportRequest.

Как проверить, все ли получилось?

Чтобы убедиться в успешном создании запроса на экспорт почтового ящика, выполните одно из следующих действий:

- В Центре администрирования Майкрософт щелкните 🔔 средства просмотра уведомлений. Чтобы просмотреть состояние запроса.
- Если вы создали запрос на экспорт почтового ящика в Центре администрирования Exchange и установили флажок для отправки уведомлений по электронной почте, проверьте, пришли ли сообщения. Отправитель — Microsoft Exchange. Первое сообщение содержит тему `Your Export PST request has been received`. Если запрос на экспорт успешно выполнен, вы получите другое сообщение с темой `Export PST has finished`.
- Замените <*MailboxIdentity*> именем, адресом электронной почты или псевдонимом исходного почтового ящика и выполните следующую команду в командной консоли Exchange, чтобы проверить основные значения свойств:

  ```
  PowerShell

  Get-MailboxExportRequest -Mailbox "<MailboxIdentity>" | Format-List
  Name,FilePath,Mailbox,Status
  ```

- Замените <*MailboxIdentity*> и <*MailboxExportRequestName*> соответствующими значениями и выполните следующую команду в командной консоли Exchange, чтобы проверить сведения:

  ```
  PowerShell

  Get-MailboxExportRequestStatistics -Identity "<MailboxIdentity>\
  <MailboxExportRequestName>"
  ```

Просмотр запросов на экспорт почтовых ящиков с помощью командной консоли Exchange

По умолчанию командлет **Get-MailboxExportRequest** возвращает имя, исходный почтовый ящик и состояние запросов на экспорт почтового ящика. Если передать команду конвейерным образом в командлет **Format-List**, вы получите только ограниченное число дополнительных полезных сведений:

- **FilePath**: целевой PST-файл.
- **RequestGUID**— уникальное значение GUID запроса на экспорт почтового ящика.
- **RequestQueue**: база данных почтовых ящиков, в которой выполняется запрос на экспорт.
- **BatchName**: необязательное имя пакета для запроса на экспорт почтового ящика.
- **Identity**: уникальное значение удостоверения запроса на экспорт почтового ящика (*<MailboxIdentity>*\ *<MailboxExportRequestName>*).

По умолчанию командлет **Get-MailboxExportRequestStatistics** возвращает имя, состояние, псевдоним исходного почтового ящика и выполнение запросов на экспорт почтового ящика в процентах. Если отправить команду конвейерным образом в командлет **Format-List**, отобразятся подробные сведения о запросе на экспорт почтового ящика.

Этот пример возвращает сводный список всех запросов на экспорт почтового ящика.

PowerShell

```
Get-MailboxExportRequest
```

Этот пример возвращает дополнительные сведения о запросах на экспорт из почтового ящика Akia Al-Zuhairi.

PowerShell

```
Get-MailboxExportRequest -Mailbox "Akia Al-Zuhairi" | Format-List
```

Этот пример возвращает сводный список выполняющихся запросов на экспорт для почтовых ящиков, которые хранятся в базе данных почтовых ящиков с именем DB01.

```
PowerShell

Get-MailboxExportRequest -Status InProgress -Database DB01
```

Этот пример возвращает сводный список выполненных запросов на экспорт почтовых ящиков в пакете с именем Export DB01 PSTs.

```
PowerShell

Get-MailboxExportRequest -Status Completed -BatchName "Export DB01 PSTs"
```

Подробные сведения о синтаксисе и параметрах см. в статье Get-MailboxExportRequest.

Чтобы просмотреть подробные сведения о запросе на экспорт почтового ящика, используйте этот синтаксис:

```
PowerShell

Get-MailboxExportRequestStatistics -Identity <MailboxExportRequestIdentity>
[-IncludeReport] | Format-List
```

Где <*MailboxExportRequestIdentity*> — это значение удостоверения запроса на экспорт почтового ящика (<*MailboxIdentity*>\ <*MailboxExportRequestName*> или <*RequestGUID*>).

Этот пример возвращает подробные сведения для запроса на экспорт почтового ящика с именем MailboxExport пользователя Akia Al-Zuhairi, включая журнал действий в свойстве **Report**.

```
PowerShell

Get-MailboxExportRequestStatistics -Identity "aal-zuhairi\MailboxExport" -
IncludeReport | Format-List
```

Подробные сведения о синтаксисе и параметрах см. в статье Get-MailboxExportRequestStatistics.

Изменение запросов на экспорт почтовых ящиков с помощью командной консоли Exchange

Вы можете изменять невыполненные запросы на экспорт почтовых ящиков. Невозможно изменить базовые параметры существующего запроса (например, исходный почтовый ящик, конечный PST-файл, исходное содержимое в почтовом ящике или назначение в конечном PST-файле).

Чтобы изменить запрос на экспорт почтового ящика, используйте данный синтаксис:

PowerShell

```
Set-MailboxExportRequest -Identity <MailboxIdentity>\
<MailboxExportRequestName> [-BadItemLimit <value>] [-LargeItemLimit <value>]
[-AcceptLargeDataLoss]
```

В этом примере изменяется неудачный запрос на экспорт почтового ящика пользователя Valeria Barrios для приема не более пяти поврежденных элементов почтового ящика.

PowerShell

```
Set-MailboxExportRequest -Identity "Valeria Barrios\MailboxExport" -
BadItemLimit 5
```

Подробные сведения о синтаксисе и параметрах см. в статье Set-MailboxExportRequest.

Примечание. После изменения приостановленного или неудачного запроса на экспорт почтового ящика необходимо возобновить его с помощью командлета **Resume-MailboxExportRequest**.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно изменили запрос на экспорт почтового ящика, замените *<MailboxIdentity>* и *<MailboxExportRequestName>* соответствующими значениями и выполните следующую команду в командной консоли Exchange, чтобы проверить сведения:

PowerShell

```
Get-MailboxExportRequestStatistics -Identity "<MailboxIdentity>\
<MailboxExportRequestName>" | Format-List
```

Приостановка запросов на экспорт почтовых ящиков с помощью командной консоли Exchange

Вы можете приостановить выполняющиеся запросы на экспорт почтовых ящиков. Невозможно приостановить выполненные или неудачные запросы на экспорт почтовых ящиков.

Чтобы приостановить запрос на экспорт почтового ящика, используйте данный синтаксис:

PowerShell

```
Suspend-MailboxExportRequest -Identity <MailboxIdentity>\
<MailboxExportRequestName> [-SuspendComment "<Descriptive Comment>"]
```

В этом примере приостанавливается запрос с именем Kathleen Reiter Export на экспорт почтового ящика пользователя Kathleen Reiter.

PowerShell

```
Suspend-MailboxExportRequest -Identity "kreiter@contoso.com\Kathleen Reiter
Export"
```

В этом примере приостанавливаются все выполняющиеся запросы на экспорт почтовых ящиков с примечанием "OK to resume after 10 P.M. on Monday 6/19" (Возобновить после 22:00 в понедельник 19.06)

PowerShell

```
Get-MailboxExportRequest -Status InProgress | Suspend-MailboxExportRequest -
SuspendComment "OK to resume after 10 P.M. on Monday 6/19"
```

Подробные сведения о синтаксисе и параметрах см. в статье Suspend-MailboxExportRequest.

Примечания.

- Вы также можете использовать командлет **New-MailboxExportRequest** с параметром *Suspend* , чтобы создать приостановленный запрос на экспорт почтового ящика.
- Параметр **Resume-MailboxExportRequest** используется для возобновления приостановленных запросов на экспорт почтовых ящиков.

Как проверить, все ли получилось?

Чтобы убедиться в успешной приостановке запроса на экспорт почтового ящика, выполните одно из следующих действий:

- Замените <*MailboxIdentity*> именем, адресом электронной почты или псевдонимом исходного почтового ящика, выполните эту команду в командной консоли Exchange и убедитесь, что свойство **Status** имеет значение `Suspended`:

  PowerShell

  ```
  Get-MailboxExportRequest -Mailbox "<MailboxIdentity>" | Format-List Name,FilePath,Mailbox,Status
  ```

- Выполните указанную ниже команду в командной консоли Exchange и убедитесь, что отображается приостановленный запрос на экспорт почтового ящика.

  PowerShell

  ```
  Get-MailboxExportRequest -Status Suspended
  ```

Возобновление запросов на экспорт почтовых ящиков с помощью командной консоли Exchange

Вы можете возобновлять приостановленные или неудачные запросы на экспорт почтовых ящиков.

Чтобы возобновить запрос на экспорт почтового ящика, используйте данный синтаксис:

PowerShell

```
Resume-MailboxExportRequest -Identity <MailboxIdentity>\
<MailboxExportRequestName>
```

В этом примере возобновляется неудачный запрос на экспорт почтового ящика пользователя Valeria Barrios.

PowerShell

```
Resume-MailboxExportRequest -Identity vbarrios\MailboxExport
```

В этом примере возобновляются все приостановленные запросы на экспорт почтовых ящиков.

PowerShell

```
Get-MailboxExportRequest -Status Suspended | Resume-MailboxExportRequest
```

Подробные сведения о синтаксисе и параметрах см. в статье Resume-MailboxExportRequest.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно возобновили запрос на экспорт почтового ящика, замените *<MailboxIdentity>* именем, адресом электронной почты или псевдонимом исходного почтового ящика, выполните следующую команду в командной консоли Exchange и убедитесь, что свойство **Status** не имеет значения `Suspended`:

PowerShell

```
Get-MailboxExportRequest -Mailbox <MailboxIdentity> | Format-List
Name,FilePath,Mailbox,Status
```

Удаление запросов на экспорт почтовых ящиков в командной консоли Exchange

Вы можете удалить полностью или частично выполненные запросы на экспорт почтовых ящиков.

- При удалении частично выполненного запроса на экспорт почтового ящика этот запрос удаляется из очереди заданий службы репликации почтовых

ящиков (MRS). Экспортированное из исходного почтового ящика содержимое не удаляется из конечного PST-файла.

- По умолчанию завершенный запрос на экспорт почтового ящика удаляется через 30 дней (это значение можно переопределить с помощью параметра *CompletedRequestAgeLimit*), а неудачные запросы не удаляются автоматически. Если вы используете параметр *RequestExpiryInterval* при создании или изменении запроса на экспорт почтового ящика, доступны следующие результаты:

  - **RequestExpiryInterval со значением интервала времени**. Завершенные и неудачные запросы автоматически удаляются после указанного интервала времени.

  - **RequestExpiryInterval со значением unlimited**: завершенные и неудачные запросы не удаляются автоматически.

В этом примере удаляется запрос с именем MailboxExport на экспорт почтового ящика пользователя Akia Al-Zuhairi.

PowerShell

```
Remove-MailboxExportRequest -Identity "aal-zuhairi\MailboxExport"
```

В этом примере удаляются все выполненные запросы на экспорт почтовых ящиков.

PowerShell

```
Get-MailboxExportRequest -Status Completed | Remove-MailboxExportRequest
```

Подробные сведения о синтаксисе и параметрах см. в статье Remove-MailboxExportRequest.

Как проверить, все ли получилось?

Чтобы убедиться, что запрос на экспорт почтового ящика успешно удален, *замените< MailboxIdentity>* именем, адресом электронной почты или псевдонимом исходного почтового ящика, выполните следующую команду в командной консоли Exchange и убедитесь, что запрос на экспорт почтового ящика отсутствует в списке:

PowerShell

```
Get-MailboxExportRequest -Mailbox <MailboxIdentity> | Format-List
Name,FilePath,Mailbox,Status
```

Клиенты и мобильные устройства в Exchange Server

Статья • 04.04.2023

Существует множество различных клиентов, которые можно использовать для доступа к информации в почтовом ящике Exchange. К этим клиентам относятся классические программы, такие как Outlook, Outlook в Интернете (ранее известный как Outlook Web App), а также мобильные клиенты, такие как мобильные телефоны, планшеты и другие мобильные устройства. Каждый из этих клиентов предлагает разнообразные возможности.

В следующей таблице содержатся ссылки на разделы, которые помогут вам узнать о некоторых клиентах и методах доступа клиентов, которые можно использовать для доступа к почтовому ящику Exchange, и управлять ими.

Статья	Описание
MAPI через HTTP в Exchange Server	Узнайте о последнем методе клиентского доступа, который обеспечивает подключение к Outlook.
Outlook Anywhere	Узнайте о более раннем методе клиентского доступа, который обеспечивает подключение к Outlook. (Предыдущее название этой функции — RPC/HTTP.)
Exchange ActiveSync	Узнайте о протоколе, который обеспечивает подключение к широкому спектру мобильных телефонов и планшетов. С помощью Exchange ActiveSync пользователи могут получить доступ к электронной почте, календарю, контактам и сведениям о задачах.
POP3 и IMAP4 в Exchange Server	Узнайте, как пользователи могут получить доступ к своим почтовым ящикам Exchange с помощью почтовых программ, использующих POP3 или IMAP4.
Outlook для iOS и Android	Узнайте о приложении Outlook для iOS и Android и удаленном безопасном доступе к данным почтового ящика с устройств iOS и Android.
Установка Office Online Server в организации Exchange	Узнайте, как интеграция Office Online Server помогает обеспечить расширенные возможности предварительного просмотра вложений в Outlook в Интернете.

Статья	Описание
Outlook в Интернете в Exchange Server	Узнайте о Outlook в Интернете, которая предоставляет пользователям доступ к почтовому ящику Exchange через веб-браузер.
Подсказки в Exchange	Подробнее о подсказках — информационных сообщениях, которые пользователи видят при составлении сообщения.

MAPI через HTTP в Exchange Server

Статья • 04.04.2023

MAPI over HTTP — транспортный протокол, который повышает надежность и стабильность подключений Outlook и Exchange посредством перемещения транспортного уровня в стандартную модель HTTP. Это обеспечивает большую видимость ошибок транспорта и улучшенный способ восстановления. Дополнительные возможности включают поддержку явной функции приостановки и возобновления. Благодаря этому поддерживаемые клиенты могут менять сети или выходить из режима гибернации, сохраняя тот же контекст сервера.

При внедрении протокола MAPI через HTTP Outlook сможет использовать и другие протоколы для доступа к Exchange. Клиенты Outlook, не поддерживающие протокол MAPI через HTTP, все равно могут использовать мобильный Outlook (протокол RPC через HTTP) для доступа к Exchange через сервер клиентского доступа с включенной поддержкой интерфейса MAPI.

В Exchange 2016 и Exchange 2019 MAPI по протоколу HTTP можно применять во всей организации или на уровне отдельного почтового ящика.

Преимущества протокола MAPI через HTTP

MAPI по протоколу HTTP предоставляет клиентам, поддерживающим его, следующие преимущества:

- Обеспечение дальнейших нововведений в проверку подлинности благодаря использованию протокола на основе HTTP.
- Обеспечивает более быстрое повторное подключение после прерывания связи, так как необходимо перестроить только TCP-подключения (а не подключения RPC). Примеры разрывов связи приведены ниже.
    - Гибернация устройства
    - Замена проводной сети на беспроводную или сеть мобильной связи
- Предоставление контекста сеанса, не зависящего от подключения. Сервер поддерживает контекст сеанса в течение настраиваемого периода времени, даже если пользователь изменяет сети.

MAPI через HTTP при обновлении Exchange

В Exchange 2016 или более поздней версии MAPI по ПРОТОКОЛу HTTP включен по умолчанию на уровне организации, хотя вам по-прежнему необходимо настроить виртуальные каталоги, как описано в разделе Настройка MAPI через HTTP , чтобы пользователи пользовались преимуществами.

Сценарии, в которых mapI через HTTP включен или отключен по умолчанию на уровне организации, описаны в следующей таблице:

Сценарий	Exchange 2019	Exchange 2016
Обновление среды Exchange 2016	MAPI по протоколу HTTP включен по умолчанию	н/д
Обновление из среды, содержащей все серверы Exchange 2013	MAPI через HTTP отключен по умолчанию	MAPI через HTTP отключен по умолчанию
Обновление среды Exchange 2010	н/д	MAPI по протоколу HTTP включен по умолчанию

Во время обновления организации, содержащей серверы Exchange 2013, администраторы получат предупреждение о проверке готовности MAPI по протоколу HTTP не включено [WarnMapiHttpNotEnabled] , и рекомендуется включить MAPI через HTTP после установки. В любой организации, содержащей серверы Exchange 2013, mapi через HTTP не будет включена по умолчанию, и администраторам потребуется выполнить действия, описанные в разделе Настройка MAPI через HTTP , чтобы включить его.

Возможности поддержки и необходимые компоненты

Соблюдайте приведенные ниже требования при включении протокола MAPI over HTTP.

Поддержка

Убедитесь, что ваши клиенты и серверы поддерживают протокол MAPI over HTTP, воспользовавшись приведенной ниже матрицей.

Продукт	Exchange 2019	Exchange 2016	Exchange 2013 SP1	Exchange 2013 RTM	Exchange 2010 SP3

Продукт	Exchange 2019	Exchange 2016	Exchange 2013 SP1	Exchange 2013 RTM	Exchange 2010 SP3
Outlook 2013 с пакетом обновления 1 (SP1) и все более поздние версии Outlook	MAPI/HTTP Мобильный Outlook	Протокол MAPI over HTTP Мобильный Outlook	Протокол MAPI over HTTP Мобильный Outlook	Мобильный Outlook	RPC Мобильный Outlook
Outlook 2010 с пакетом обновления 2 (SP2) с обновлениями KB2956191 и KB2965295 (14 апреля 2015 г.)	MAPI/HTTP Мобильный Outlook	Протокол MAPI over HTTP Мобильный Outlook	Протокол MAPI over HTTP Мобильный Outlook	Мобильный Outlook	RPC Мобильный Outlook
Outlook 2013 RTM	Мобильный Outlook	Мобильный Outlook	Мобильный Outlook	Мобильный Outlook	RPC Мобильный Outlook
Все более ранние версии Outlook	Мобильный Outlook	Мобильный Outlook	Мобильный Outlook	Мобильный Outlook	RPC Мобильный Outlook

Предварительные требования

Для поддержки MAPI через HTTP с Exchange Server клиентами и серверами требуются следующие условия. Когда вы их установите, следуйте инструкциям из статьи Configure MAPI over HTTP, чтобы включить этот протокол в организации.

- Поддерживаемые клиенты Outlook (см. таблицу в предыдущем разделе).
- платформа .NET Framework 4.5.2 или более поздней версии. Обратите внимание, что это больше не является проблемой для Exchange 2016 с накопительным пакетом обновления 5 (CU5) или более поздней версии. Дополнительные сведения о требованиях к платформа .NET Framework для Exchange 2016 см. в статье Поддерживаемые версии платформа .NET Framework для Exchange 2016.

Настройка MAPI через HTTP в Exchange Server

Статья • 04.04.2023

В Exchange 2016 и Exchange 2019 можно настроить MAPI через HTTP на уровне организации или на уровне отдельного почтового ящика. Параметры на уровне почтовых ящиков всегда имеют приоритет над параметрами для организации.

Сценарии, в которых mapI через HTTP включен или отключен по умолчанию на уровне организации, описаны в следующей таблице:

Сценарий	Exchange 2019	Exchange 2016
Обновление среды Exchange 2016	MAPI по протоколу HTTP включен по умолчанию	н/д
Обновление из среды, содержащей все серверы Exchange 2013	MAPI через HTTP отключен по умолчанию	MAPI через HTTP отключен по умолчанию
Обновление среды Exchange 2010	н/д	MAPI по протоколу HTTP включен по умолчанию

> ⓘ **Примечание**
>
> Если MAPI по ПРОТОКОЛУ HTTP включен на уровне организации, значение свойства *MapiHttpEnabled* , возвращаемое командлетом **Get-OrganizationConfig** , имеет значение `True`.

В этом разделе описывается, как настроить и затем включить MAPI через HTTP для организаций Exchange, содержащих серверы Exchange 2013, или для любой топологии, в которой ранее была отключена функция MAPI через HTTP. Вы также можете использовать представленные в этой статье процедуры, чтобы отключить протокол MAPI/HTTP на уровне организации.

В этом разделе также описывается включение или отключение MAPI через HTTP для отдельного почтового ящика. На уровне почтовых ящиков вы можете разрешить или заблокировать внутренние или внешние подключения по протоколу MAPI/HTTP либо подключения обоих типов. Во всех случаях, когда протокол MAPI/HTTP отключен, подключение выполняется из мобильного Outlook.

Настройка протокола MAPI/HTTP

Выполните приведенные ниже действия, чтобы настроить протокол MAPI/HTTP для своей организации. В этих шагах предполагается, что вы уже настроили предварительные требования, описанные в разделе MAPI через HTTP в Exchange Server. После настройки (этапы 1-3) переходите к этапу 4, чтобы включить или отключить определенные сценарии разрешений на уровне организации, на уровне почтовых ящиков или на обоих уровнях.

1. **Конфигурация виртуального каталога**. По умолчанию Exchange создает виртуальный каталог для MAPI по протоколу HTTP. Командлет **Set-MapiVirtualDirectory** используется для настройки виртуального каталога. Необходимо настроить внутренний URL-адрес, внешний URL-адрес или и то, и другое. Дополнительные сведения см. в статье Set-MapiVirtualDirectory.

   Например, чтобы настроить виртуальный каталог MAPI по умолчанию на локальном сервере Exchange Server, задав для внутреннего URL-адреса значение https://contoso.com/mapi, а для метода проверки подлинности — `Negotiate`, выполните следующую команду:

   PowerShell

   ```
   Set-MapiVirtualDirectory -Identity "Contoso\mapi (Default Web Site)" -
   InternalUrl https://Contoso.com/mapi -IISAuthenticationMethods Negotiate
   ```

2. **Конфигурация сертификата**. Цифровой сертификат, используемый средой Exchange, должен содержать те же значения *InternalURL* и *ExternalURL* , которые определены в виртуальном каталоге MAPI. Дополнительные сведения об управлении сертификатами Exchange см. в разделе Цифровые сертификаты и шифрование в Exchange Server. Убедитесь, что сертификат Exchange является доверенным на клиентской рабочей станции Outlook и что ошибки сертификата отсутствуют, особенно при доступе к URL-адресам, настроенным в виртуальном каталоге MAPI.

3. **Правила сервера обновления**. Убедитесь, что подсистемы балансировки нагрузки, обратные прокси-серверы и брандмауэры настроены так, чтобы разрешить доступ к виртуальному каталогу MAPI через HTTP.

4. Выполните указанные ниже действия, чтобы включить протокол MAPI/HTTP во всей организации Exchange либо для одного или нескольких отдельных почтовых ящиков.

   > **Примечание**
   >
   > После выполнения приведенных ниже команд клиенты Outlook с включенным протоколом MAPI по HTTP увидят сообщение о перезапуске

Outlook для использования MAPI по протоколу HTTP.

Включите MAPI через HTTP в организации Exchange:

Чтобы включить или отключить MAPI через HTTP на уровне организации, используйте командлет **Set-OrganizationConfig** с *параметром MapiHttpEnabled* . Допустимые значения:

- **$true**: подключения MAPI по протоколу HTTP разрешены для всех почтовых ящиков в организации (если для определенного почтового ящика не отключен параметр MAPI по протоколу HTTP).
- **$false**: подключения MAPI по ПРОТОКОЛу HTTP разрешены не для всех почтовых ящиков в организации (если только mapI через HTTP не включен в определенном почтовом ящике).

В приведенном ниже примере показано, как разрешить подключения по протоколу MAPI/HTTP для всей организации.

PowerShell

```
Set-OrganizationConfig -MapiHttpEnabled $true
```

Включите MAPI через HTTP для отдельного почтового ящика:

Чтобы включить или отключить MAPI через HTTP на уровне почтового ящика, используйте командлет **Set-CasMailbox** с *параметром MapiHttpEnabled* . Допустимые значения:

- **$null**. Почтовый ящик соответствует параметрам на уровне организации. Это значение используется по умолчанию.
- **$true**: включите MAPI через HTTP для почтового ящика. Если MAPI через HTTP отключена на уровне организации, она включена для почтового ящика.
- **$false**: отключите MAPI через HTTP для почтового ящика. Если на уровне организации включен параметр MAPI по протоколу HTTP, он отключен для почтового ящика, поэтому почтовый ящик будет использовать подключения Outlook Anywhere.

В приведенном ниже примере разрешаются подключения по протоколу MAPI/HTTP для одного почтового ящика.

PowerShell

```
Set-CasMailbox <user or mailbox ID> -MapiHttpEnabled $true
```

Проверка подключений MAPI через HTTP

Сквозное подключение MAPI через HTTP можно проверить с помощью командлета **Test-OutlookConnectivity**. Чтобы использовать командлет **Test-OutlookConnectivity**, необходимо запустить службу диспетчера работоспособности Microsoft Exchange (MSExchangeHM).

В примере ниже проверяется подключение MAPI через HTTP от сервера Exchange с именем ContosoMail.

PowerShell

```
Test-OutlookConnectivity -RunFromServerId ContosoMail -ProbeIdentity
OutlookMapiHttpSelfTestProbe
```

При успешной проверке возвращаются результаты, похожие на приведенный ниже пример.

PowerShell

```
MonitorIdentity                                          StartTime
EndTime                 Result      Error     Exception
---------------                                          ---------
-------                 ------      -----     ---------
OutlookMapiHttp.Protocol\OutlookMapiHttpSelfTestProbe    2/14/2018 7:15:00 AM
2/14/2018 7:15:10 AM    Succeeded
```

Дополнительные сведения см. в разделе Test-OutlookConnectivity.

Журналы действий MAPI через HTTP находятся в указанных ниже папках.

- %ExchangeInstallPath%Logging\MAPI Address Book Service\
- %ExchangeInstallPath%Logging\MAPI Client Access\
- %ExchangeInstallPath%Logging\HttpProxy\Mapi\

Совмещение конфигураций протокола MAPI/HTTP и внешних или внутренних подключений

Помимо параметров организации и почтовых ящиков, описанных ранее в этом разделе, можно использовать параметр *MapiBlockOutlookExternalConnectivity* в **командлете Set-CasMailbox** , чтобы разрешить или запретить внешние подключения Outlook Anywhere или MAPI через HTTP к определенному почтовому ящику. Допустимые значения:

- **True**: к почтовому ящику разрешены только внутренние подключения.
- **False**: к почтовому ящику разрешены внутренние и внешние подключения. Это значение используется по умолчанию.

В следующей таблице приведены результаты различных сочетаний параметров на уровне организации и в отдельных почтовых ящиках.

Значение MapiHttpEnabled в Set-OrganizationConfig	**Значение MapiHttpEnabled в Set-CasMailbox**	**Значение MapiBlockOutlookExternalConnectivity в Set-CasMailbox**	**Результат автообнаружения**
$true	$null	$false	MAPI/HTTP, внутренние и внешние
$true	$null	$true	MAPI/HTTP, только внутренние
$true	$true	$false	MAPI/HTTP, внутренние и внешние
$true	$true	$true	MAPI/HTTP, только внутренние
$true	$false	$false	Мобильный Outlook, внутренние и внешние
$true	$false	$true	Мобильный Outlook, только внутренние
$false	$null	$false	Мобильный Outlook, внутренние и внешние
$false	$null	$true	Мобильный Outlook, только внутренние

Значение MapiHttpEnabled в Set-OrganizationConfig	Значение MapiHttpEnabled в Set-CasMailbox	Значение MapiBlockOutlookExternalConnectivity в Set-CasMailbox	Результат автообнаружения
$false	$true	$false	MAPI/HTTP, внутренние и внешние
$false	$true	$true	MAPI/HTTP, только внутренние
$false	$false	$false	Мобильный Outlook, внутренние и внешние
$false	$false	$true	Мобильный Outlook, только внутренние

Управление протоколом MAPI через HTTP

Для управления конфигурацией протокола MAPI через HTTP используются приведенные ниже командлеты.

- Set-MapiVirtualDirectory
- Get-MapiVirtualDirectory
- New-MapiVirtualDirectory
- Remove-MapiVirtualDirectory

Включение или отключение доступа MAPI к почтовым ящикам в Exchange Server

Статья • 04.04.2023

MAPI — это клиентский протокол, который позволяет пользователям получать доступ к своим почтовым ящикам через Outlook и другие почтовые клиенты MAPI. По умолчанию доступ к почтовому ящику пользователя по протоколу MAPI включен. Если вы отключите его, он не сможет использовать Outlook для доступа к своему почтовому ящику в режиме Exchange. Но он по-прежнему сможет получить к нему доступ через Outlook в Интернете и Outlook с использованием других протоколов (например, POP3, IMAP4 или Exchange ActiveSync).

Администраторы могут включить или отключить доступ к почтовому ящику пользователя по протоколу MAPI, используя Центр администрирования Exchange или командную консоль Exchange.

Дополнительные сведения об управлении доступом пользователей к почтовым ящикам см. в следующих статьях:

- Включение или отключение Outlook в Интернете доступа к почтовым ящикам в Exchange Server
- Включение или отключение Exchange ActiveSync доступа к почтовым ящикам в Exchange Server
- Включение или отключение доступа по протоколу POP3 или IMAP4 к почтовым ящикам в Exchange Server

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Дополнительные сведения о доступе и использовании Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server.
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Параметры пользователя клиентского доступа" в разделе Разрешения клиентов и мобильных устройств .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

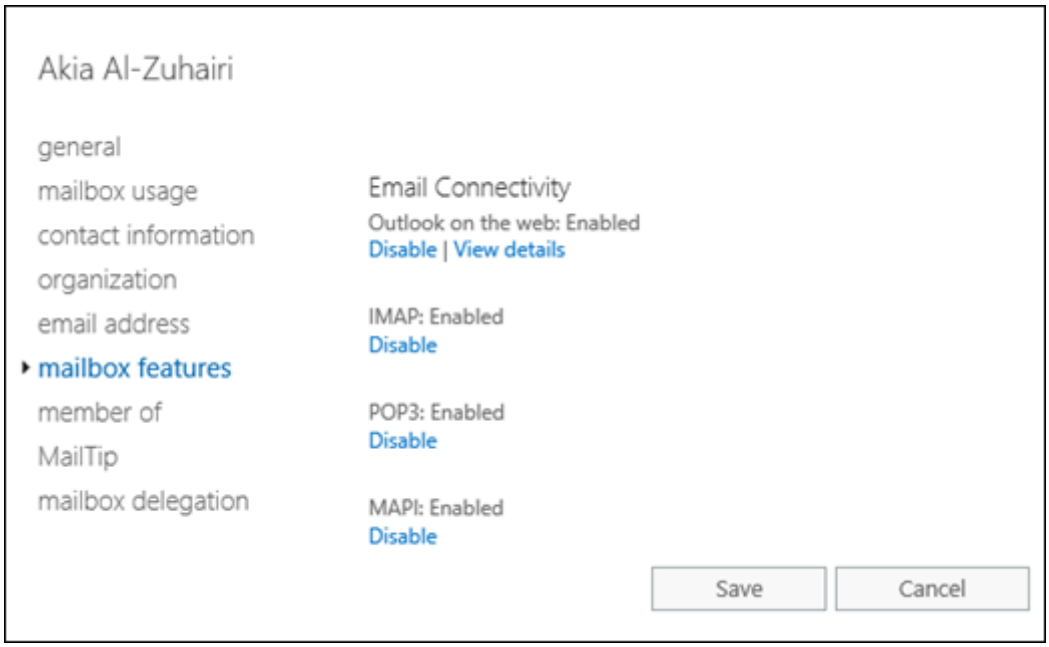
Включение и отключение доступа по протоколу MAPI к одному почтовому ящику

Включение и отключение доступа по протоколу MAPI к одному почтовому ящику в Центре администрирования Exchange

1. В EAC перейдите в раздел **Почтовые ящики получателей**>.
2. В списке почтовых ящиков найдите нужный почтовый ящик. Для этого выполните одно из следующих действий:
   - Прокрутите список почтовых ящиков.
   - Щелкните 🔎 введите часть имени пользователя, адреса электронной почты или псевдонима.
   - Щелкните **Значок Дополнительные параметры**••• > **Расширенный поиск** для поиска почтового ящика.

     Найдя почтовый ящик, который требуется изменить, выберите его и нажмите кнопку **Изменить**.
3. На открывшейся странице свойств выберите **Функции почтового ящика**.
4. В разделе **Возможность подключения электронной почты** настройте один из таких параметров:

- Если вы видите **MAPI: включено**, щелкните **Отключить**, а затем нажмите кнопку **Да** в появившемся предупреждении.
- Если вы видите **MAPI: отключено**, щелкните **Включить**.



По завершении нажмите кнопку **Сохранить**.

Включение и отключение доступа к почтовому ящику по протоколу MAPI с помощью командной консоли Exchange

Чтобы включить или отключить доступ по протоколу MAPI к одному почтовому ящику, используйте такой синтаксис:

PowerShell

```
Set-CasMailbox -Identity <MailboxIdentity> -MAPIEnabled <$true | $false>
```

В этом примере отключается доступ по протоколу MAPI к почтовому ящику Ken Sanchez.

PowerShell

```
Set-CasMailbox -Identity "Ken Sanchez" -MAPIEnabled $false
```

В этом примере включается доступ по протоколу MAPI к почтовому ящику Esther Valle.

```
```

PowerShell

```
Set-CasMailbox -Identity "Esther Valle" -MAPIEnabled $true
```

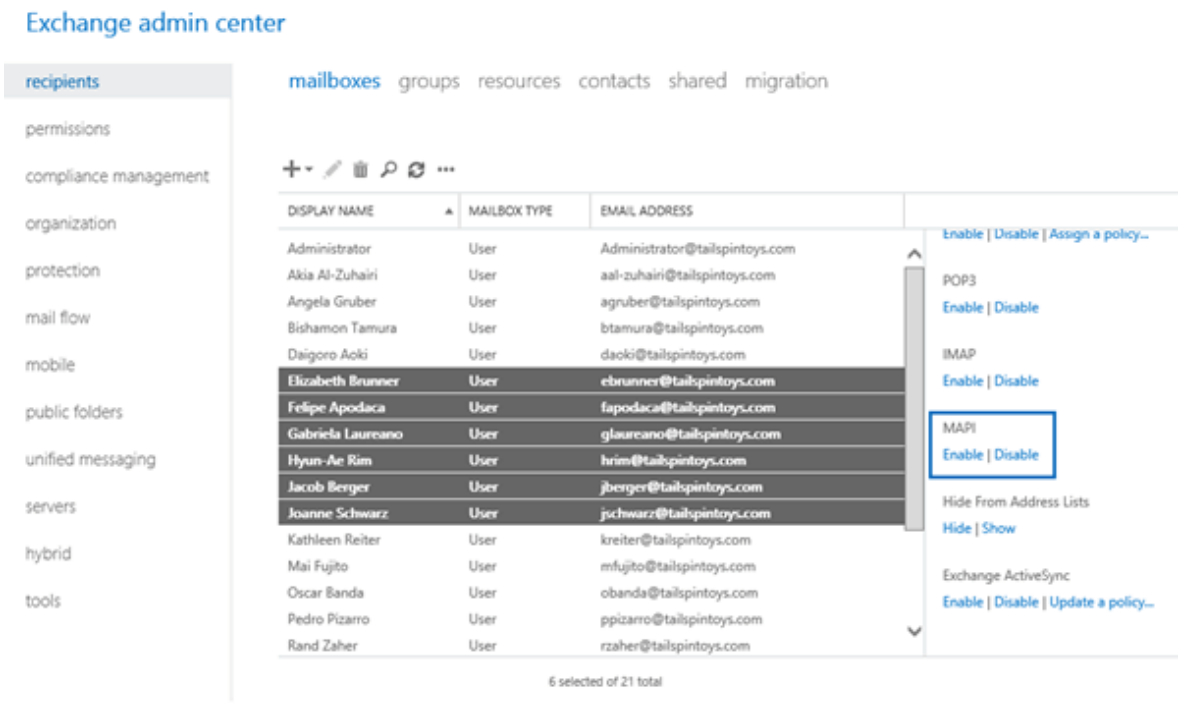
Дополнительные сведения о синтаксисе и параметрах см. в статье Set-CASMailbox.

Включение и отключение доступа по протоколу MAPI к нескольким почтовым ящикам

Включение и отключение доступа по протоколу MAPI к нескольким почтовым ящикам в Центре администрирования Exchange

1. В EAC перейдите в раздел **Почтовые ящики получателей**>.
2. В списке почтовых ящиков найдите нужные почтовые ящики. Для этого выполните одно из следующих действий:
   - Прокрутите список почтовых ящиков.
   - Щелкните 🔎 введите часть имени пользователя, адреса электронной почты или псевдонима.
   - Щелкните **Значок Дополнительные параметры**••• > **Расширенный поиск** для поиска почтового ящика.
3. В списке почтовых ящиков выберите несколько почтовых ящиков одного типа (например, **Пользователь**). Например:
   - Выберите почтовый ящик. Удерживая клавишу SHIFT, выберите другой ящик, расположенный ниже в списке.
   - Выберите нужные почтовые ящики, удерживая клавишу CTRL.

   После выбора нескольких почтовых ящиков одного типа заголовок области сведений изменится на **Массовое изменение**.
4. В области сведений найдите **MAPI**, щелкните **Включить** или **Отключить**, а затем нажмите **OK** в появившемся предупреждении.



Включение и отключение доступа по протоколу MAPI к нескольким почтовым ящикам с помощью командной консоли Exchange

Чтобы указать нужные почтовые ящики, можно использовать командлеты **Get-Mailbox**, **Get-User** или **Get-Content**. Например:

- Используйте параметр *OrganizationalUnit* для фильтрации почтовых ящиков по подразделениям.
- Используйте параметр *Filter* для создания фильтров OPATH, определяющих почтовые ящики. Дополнительные сведения см. в статье Filterable Properties for the -Filter Parameter.
- Используйте текстовый файл для указания почтовых ящиков. В каждой строке текстового файла указан один почтовый ящик (адрес электронной почты, имя или другой уникальный идентификатор), например:

  > ebrunner@tailspintoys.com
  > fapodaca@tailspintoys.com
  > glaureano@tailspintoys.com
  > hrim@tailspintoys.com

В этом примере отключается доступ по протоколу MAPI ко всем почтовым ящикам пользователей в североамериканском финансовом подразделении.

PowerShell

```
$NAFinance = Get-Mailbox -OrganizationalUnit "OU=Marketing,OU=North America,DC=contoso,DC=com" -Filter "RecipientTypeDetails -eq 'UserMailbox'" -ResultSize Unlimited; $NAFinance | foreach {Set-CasMailbox $_.Identity -MAPIEnabled $false}
```

В этом примере отключается доступ по протоколу MAPI ко всем почтовым ящикам пользователей в проектном отделе штата Вашингтон.

PowerShell

```
Get-User -Filter "RecipientType -eq 'UserMailbox' -and Department -like 'Engineering*' -and StateOrProvince -eq 'WA'" | Set-CasMailbox -MAPIEnabled $false
```

В этом примере для отключения доступа по протоколу MAPI к указанным почтовым ящикам используется текстовый файл C:\My Documents\Accounts.txt.

PowerShell

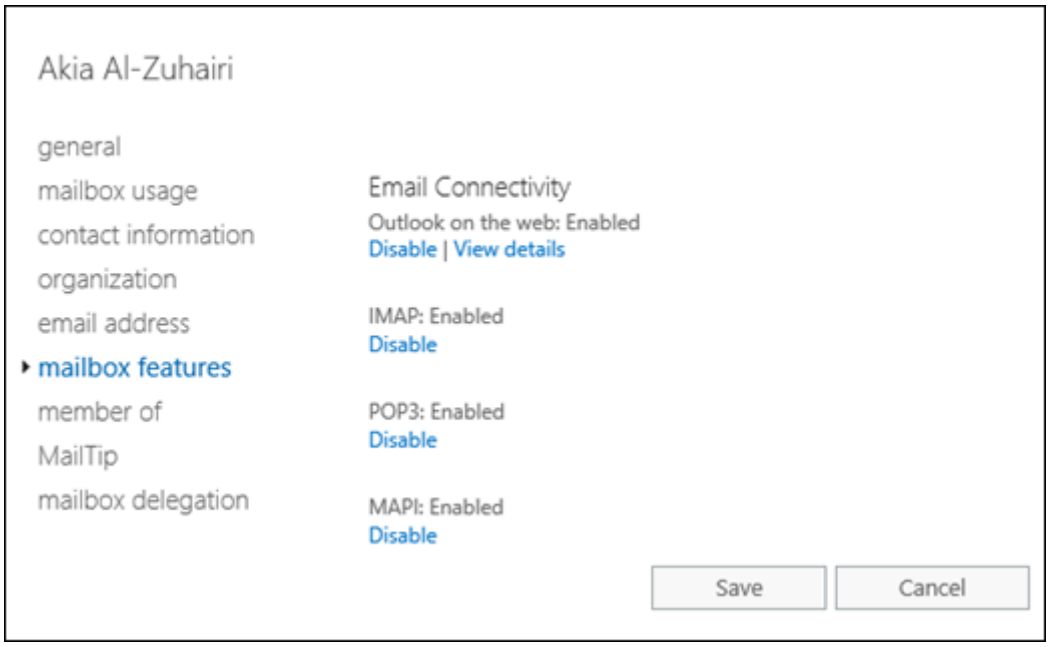
```
Get-Content "C:\My Documents\Accounts.txt" | foreach {Set-CasMailbox $_ -MAPIEnabled $false}
```

Дополнительные сведения о синтаксисе и параметрах см. в статьях Get-Mailbox и Get-User.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно включили или отключили доступ к почтовому ящику по протоколу MAPI, выполните одно из следующих действий:

- В EAC перейдите в раздел Почтовые**ящики**>**получателей**>, выберите почтовый ящик > щелкните ✎>**Функции почтового ящика** и проверьте значение **MAPI** в разделе **Email подключение**.



- В командной консоли Exchange *замените*< *MailboxIdentity*> удостоверением почтового ящика (например, именем, псевдонимом или адресом электронной почты) и выполните следующую команду:

```
PowerShell

Get-CasMailbox -Identity "<MailboxIdentity>"
```

- Используйте тот же фильтр, что и для определения почтовых ящиков, но вместо командлета **Get-CasMailbox** используйте **Set-CasMailbox**. Например:

```
PowerShell

Get-User -Filter "RecipientType -eq 'UserMailbox' -and Department -like
'Engineering*' -and StateOrProvince -eq 'WA'" | Get-CasMailbox
```

- Чтобы увидеть все почтовые ящики, для которых отключен доступ по протоколу Outlook в Интернете, выполните следующую команду в командной консоли Exchange:

```
PowerShell

Get-CasMailbox -ResultSize unlimited -Filter "MAPIEnabled -eq `$false"
```

Exchange ActiveSync в Exchange Server

Статья • 04.04.2023

Exchange ActiveSync — это протокол синхронизации Exchange, оптимизированный для работы с сетями с высокой задержкой и низкой пропускной способностью. Протокол, основанный на HTTP и XML, позволяет мобильным телефонам получать доступ к информации организации на сервере под управлением Microsoft Exchange.

Обзор Exchange ActiveSync

Exchange ActiveSync позволяет пользователям мобильных телефонов получать доступ к электронной почте, календарю, контактам и задачам и работать с этой информацией без подключения к Интернету.

Стандартные службы шифрования повышают безопасность обмена данными между мобильным устройством и сервером. Вы можете настроить Exchange ActiveSync так, чтобы при передаче данных между сервером Exchange и клиентским мобильным устройством использовалось SSL-шифрование.

> ⓘ **Примечание**
>
> Exchange ActiveSync не поддерживает общие почтовые ящики или делегированный доступ.

Функции Exchange ActiveSync

Exchange ActiveSync имеет следующие функции:

- поддержка HTML-сообщений;
- поддержка отметок к исполнению;
- Группировка сообщений электронной почты по беседам
- возможность синхронизировать или не синхронизировать всю беседу;
- синхронизация SMS с почтовым ящиком пользователя Exchange;
- поддержка просмотра состояния ответа на сообщения;

- поддержка быстрого извлечения сообщений;
- сведения об участниках собрания;
- Улучшенный поиск в Exchange
- сброс ПИН;
- усовершенствованная защита устройств с использованием политик паролей;
- автообнаружение для обслуживания через беспроводную сеть;
- Поддержка установки автоответов на случай отсутствия пользователя на месте, отпуска или командировки
- Поддержка синхронизации задач
- Direct Push.
- поддержка сведений о доступности для контактов;

Управление протоколом Exchange ActiveSync

По умолчанию протокол Exchange ActiveSync включен. Все пользователи, имеющие почтовый ящик Exchange, могут синхронизировать свое мобильное устройство с сервером Microsoft Exchange.

Можно выполнять следующие задачи Exchange ActiveSync:

- включение и отключение Exchange ActiveSync для пользователей;
- задание политик, например минимальной длины пароля, блокировки устройств и максимального числа попыток ввода неправильного пароля;
- запуск удаленной очистки для очистки всех данных с потерянного или украденного мобильного телефона;
- Запуск различных отчетов для просмотра или экспорта в разных форматах
- Контроль того, какие типы мобильных устройств могут синхронизироваться с организацией, через правила доступа устройств

Управление доступом мобильных устройств в Exchange ActiveSync

Вы можете контролировать, какие мобильные устройства могут синхронизироваться с Exchange Server. Для этого отслеживаются новые мобильные устройства, которые подключаются к организации, или настраиваются правила, которые определяют разрешенные типы мобильных устройств. Независимо от выбранного вами способа можно в любое время разрешить или запретить доступ для всех указанных мобильных устройств конкретного пользователя.

Функции обеспечения безопасности устройств в Exchange ActiveSync

В дополнение к возможности настройки параметров безопасности связи между сервером Exchange и мобильными устройствами в Exchange ActiveSync предоставляются следующие функции, предназначенные для повышения безопасности мобильных устройств:

- **Удаленная очистка**. Если мобильное устройство потеряно, украдено или скомпрометировано иным образом, вы можете выполнить команду удаленной очистки с компьютера Exchange Server или любого веб-браузера с помощью Outlook Web App. Эта команда стирает все данные с мобильного устройства.

- **Политики паролей устройств**: Exchange ActiveSync позволяет настроить несколько параметров паролей устройств. Предусмотрены следующие параметры паролей устройств:

    - **Минимальная длина пароля (символы).** Этот параметр указывает длину пароля для мобильного устройства. Длина пароля по умолчанию — 4 символа, максимальное число символов в пароле — 18.

    - **Минимальное количество наборов символов**. Используйте это текстовое поле, чтобы указать сложность буквенно-цифрового пароля и заставить пользователей использовать несколько различных наборов символов: строчные буквы, прописные буквы, символы и цифры.

    - **Требовать буквенно-цифровой пароль**. Этот параметр определяет надежность пароля. Можно потребовать использования в пароле знака или символа в дополнение к цифрам.

    - **Время бездействия (в секундах).** Этот параметр определяет, как долго мобильное устройство должно быть неактивным, прежде чем пользователю будет предложено ввести пароль для разблокировки мобильного устройства.

- **Применить журнал паролей**. Установите этот флажок, чтобы запретить пользователю повторно использовать предыдущие пароли на мобильном телефоне. Установленное число определяет количество предыдущих паролей, которое запрещается повторно использовать в мобильном телефоне.

- **Включить восстановление паролей**. Установите этот флажок, чтобы включить восстановление паролей для мобильного устройства. Администраторы могут использовать командлет **Get-ActiveSyncDeviceStatistics**, чтобы узнать пароль восстановления пользователя.

- **Очистка устройства после неудачных попыток.** Этот параметр позволяет указать, нужно ли очищать память телефона после нескольких неудачных попыток ввода пароля.

- **Политики шифрования устройств**. Существует ряд политик шифрования мобильных устройств, которые можно применить для группы пользователей. Эти политики включают в себя следующие параметры.

  - **Требовать шифрование на устройстве**. Установите этот флажок, чтобы требовать шифрование на мобильном устройстве. Это позволит повысить безопасность благодаря шифрованию всех данных для устройства.

  - **Требовать шифрование на картах памяти**. Установите этот флажок, чтобы требовать шифрование на съемной карточке мобильного устройства. Это позволит повысить безопасность благодаря шифрованию всех данных на картах памяти для устройства.

Включение или отключение Exchange ActiveSync доступа к почтовым ящикам в Exchange Server

Статья • 04.04.2023

ActiveSync — это клиентский протокол, который позволяет пользователям синхронизировать свои почтовые ящики Exchange с мобильными устройствами. По умолчанию ActiveSync включен для новых почтовых ящиков пользователей. Если вы отключите ActiveSync для почтового ящика, пользователь не сможет синхронизировать свой почтовый ящик с мобильным устройством (с помощью ActiveSync).

Администраторы могут включить или отключить доступ к почтовому ящику по протоколу Exchange ActiveSync, используя Центр администрирования Exchange или командную консоль Exchange.

Дополнительные сведения об ActiveSync см. в статье Служба Exchange ActiveSync.

Сведения о настройке электронной почты на мобильном устройстве см. в следующих статьях:

- Настройка приложений Office и электронной почты на устройствах с iOS
- Настройка приложений Office и электронной почты на Android

Дополнительные сведения об управлении доступом пользователей к почтовым ящикам см. в следующих статьях:

- Включение или отключение Outlook в Интернете доступа к почтовым ящикам в Exchange Server
- Включение или отключение доступа по протоколу POP3 или IMAP4 к почтовым ящикам в Exchange Server
- Включение или отключение доступа MAPI к почтовым ящикам в Exchange Server

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.

- Дополнительные сведения о доступе и использовании Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server.
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "параметры Exchange ActiveSync" в разделе Разрешения клиентов и мобильных устройств.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Включение и отключение доступа по протоколу Exchange ActiveSync к одному почтовому ящику

Включение и отключение доступа к почтовому ящику по протоколу Exchange ActiveSync в Центре администрирования Exchange

1. В EAC перейдите в раздел **Почтовые ящики получателей**>.
2. В списке почтовых ящиков найдите нужный почтовый ящик. Для этого выполните одно из следующих действий:
   - Прокрутите список почтовых ящиков.
   - Щелкните 🔎 введите часть имени пользователя, адреса электронной почты или псевдонима.
   - Щелкните **Значок Дополнительные параметры**•••>**Расширенный поиск** для поиска почтового ящика.

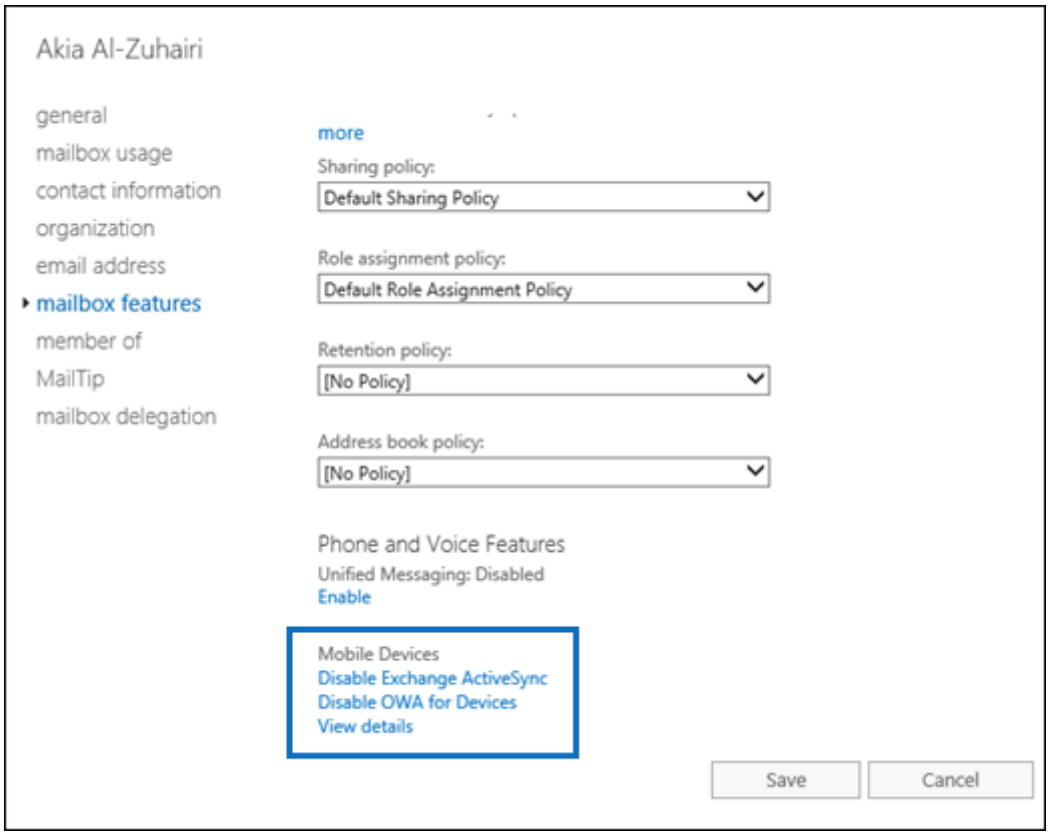
Найдя почтовый ящик, который требуется изменить, выберите его и нажмите кнопку **Изменить**.

3. На открывшейся странице свойств выберите **Функции почтового ящика**.

4. В разделе **Мобильные устройства** настройте один из таких параметров:

   - Если ActiveSync включен для почтового ящика, вы увидите ссылку **ОтключитьExchange ActiveSync**. Щелкните ссылку, чтобы отключить ActiveSync, а затем нажмите **Да** в появившемся предупреждении.

   - Если ActiveSync отключен для почтового ящика, вы увидите ссылку **Включить Exchange ActiveSync**. Щелкните ссылку, чтобы включить ActiveSync.



   По завершении нажмите кнопку **Сохранить**.

Включение и отключение доступа к почтовому ящику по протоколу Exchange ActiveSync с помощью командной консоли Exchange

Чтобы включить или отключить доступ по протоколу ActiveSync к одному почтовому ящику, используйте такой синтаксис:

```
PowerShell
```

```
Set-CasMailbox -Identity <MailboxIdentity> -ActiveSyncEnabled <$true |
$false>
```

В этом примере отключается доступ по протоколу ActiveSync к почтовому ящику Yan Li.

PowerShell

```
Set-CasMailbox -Identity "Yan Li" -ActiveSyncEnabled $false
```

В этом примере включается доступ по протоколу ActiveSync к почтовому ящику Elly Nkya.

PowerShell

```
Set-CasMailbox -Identity "Elly Nkya" -ActiveSyncEnabled $true
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Set-CASMailbox.

Включение и отключение доступа по протоколу Exchange ActiveSync к нескольким почтовым ящикам

Включение и отключение доступа по протоколу Exchange ActiveSync к нескольким почтовым ящикам в Центре администрирования Exchange

1. В EAC перейдите в раздел **Почтовые ящики получателей**>.
2. В списке почтовых ящиков найдите нужные почтовые ящики. Для этого выполните одно из следующих действий:
   - Прокрутите список почтовых ящиков.
   - Щелкните 🔎 введите часть имени пользователя, адреса электронной почты или псевдонима.
   - Щелкните **Значок Дополнительные параметры•••**>**Расширенный поиск** для поиска почтового ящика.

3. В списке почтовых ящиков выберите несколько почтовых ящиков одного типа (например, **Пользователь**). Например:

   - Выберите почтовый ящик. Удерживая клавишу SHIFT, выберите другой ящик, расположенный ниже в списке.
   - Выберите нужные почтовые ящики, удерживая клавишу CTRL.

   После выбора нескольких почтовых ящиков одного типа заголовок области сведений изменится на **Массовое изменение**.

4. В области сведений найдите **Exchange ActiveSync**, щелкните **Включить** или **Отключить**, а затем нажмите **ОК** в появившемся предупреждении.

   Выбор сразу нескольких почтовых ящиков в Центре администрирования Exchange для включения или отключения Exchange ActiveSync

Включение и отключение доступа по протоколу Exchange ActiveSync к нескольким почтовым ящикам с помощью командной консоли Exchange

Чтобы указать нужные почтовые ящики, можно использовать командлеты **Get-Mailbox**, **Get-User** или **Get-Content**. Например:

- Используйте параметр *OrganizationalUnit* для фильтрации почтовых ящиков по подразделениям.
- Используйте параметр *Filter* для создания фильтров OPATH, определяющих почтовые ящики. Дополнительные сведения см. в статье Filterable Properties for the -Filter Parameter.
- Используйте текстовый файл для указания почтовых ящиков. В каждой строке текстового файла указан один почтовый ящик (адрес электронной почты, имя или другой уникальный идентификатор), например:

  > ebrunner@tailspintoys.com
  > fapodaca@tailspintoys.com
  > glaureano@tailspintoys.com
  > hrim@tailspintoys.com

В этом примере отключается доступ по протоколу ActiveSync ко всем почтовым ящикам пользователей в североамериканском финансовом подразделении.

PowerShell

```
$NAFinance = Get-Mailbox -OrganizationalUnit "OU=Marketing,OU=North America,DC=contoso,DC=com" -Filter "RecipientTypeDetails -eq 'UserMailbox'" -ResultSize Unlimited; $NAFinance | foreach {Set-CasMailbox $_.Identity -ActiveSyncEnabled $false}
```

В этом примере отключается доступ по протоколу ActiveSync ко всем почтовым ящикам пользователей в проектном отделе штата Вашингтон.

PowerShell

```
Get-User -Filter "RecipientType -eq 'UserMailbox' -and Department -like 'Engineering*' -and StateOrProvince -eq 'WA'" | Set-CasMailbox -ActiveSyncEnabled $false
```

В этом примере для отключения доступа по протоколу ActiveSync к указанным почтовым ящикам используется текстовый файл C:\My Documents\Accounts.txt.

PowerShell

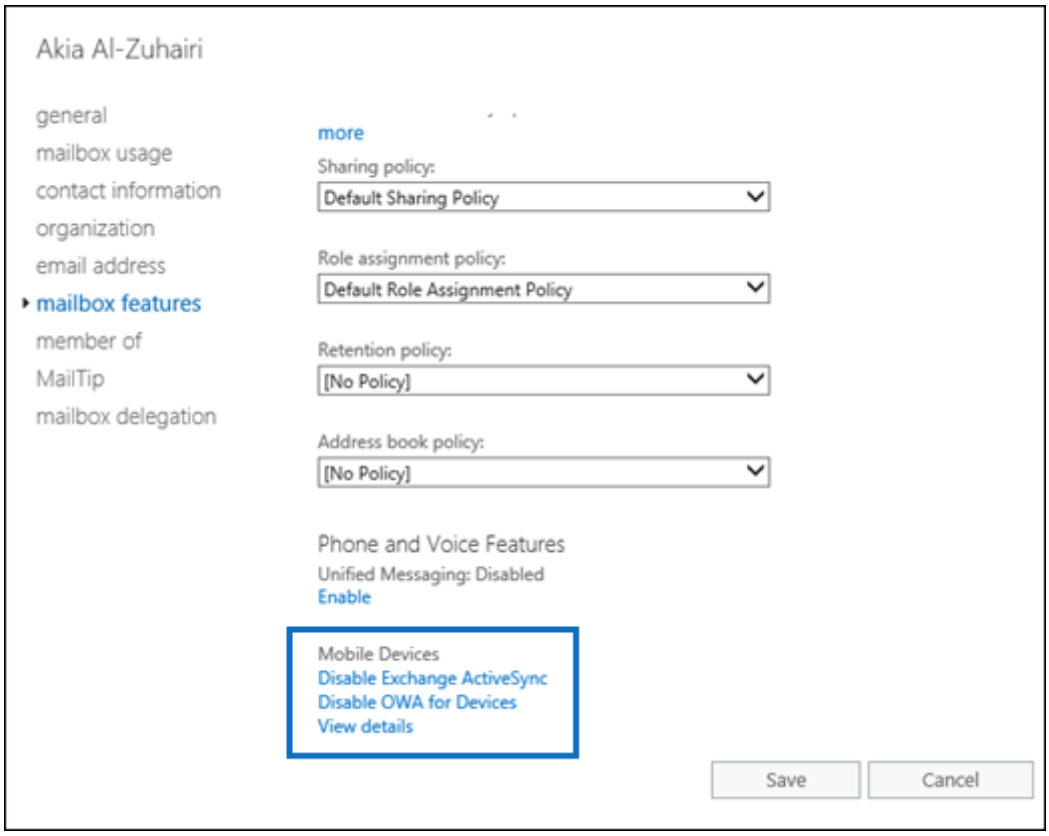
```
Get-Content "C:\My Documents\Accounts.txt" | foreach {Set-CasMailbox $_ -ActiveSyncEnabled $false}
```

Дополнительные сведения о синтаксисе и параметрах см. в статьях Get-Mailbox и Get-User.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно включили или отключили доступ к почтовому ящику по протоколу Exchange ActiveSync, выполните одно из следующих действий:

- В EAC перейдите в раздел Почтовые**ящики**>**получателей**>, выберите почтовый ящик > щелкните ✎ > Функции >**почтового ящика** и проверьте значение Exchange ActiveSync в разделе **Мобильные устройства**.
    - Если для почтового ящика включен доступ по протоколу ActiveSync, вы увидите ссылку **Отключить Exchange ActiveSync**.
    - Если для почтового ящика отключен доступ по протоколу ActiveSync, вы увидите ссылку **Включить Exchange ActiveSync**.



- В командной консоли Exchange *замените*< *MailboxIdentity*> удостоверением почтового ящика (например, именем, псевдонимом или адресом электронной почты) и выполните следующую команду:

```
PowerShell

Get-CasMailbox -Identity "<MailboxIdentity>"
```

- Используйте тот же фильтр, что и для определения почтовых ящиков, но вместо командлета **Get-CasMailbox** используйте **Set-CasMailbox**. Например:

```
PowerShell

Get-User -Filter "RecipientType -eq 'UserMailbox' -and Department -like
'Engineering*' -and StateOrProvince -eq 'WA'" | Get-CasMailbox
```

- Чтобы увидеть все почтовые ящики, для которых отключен доступ по протоколу ActiveSync, выполните следующую команду в командной консоли Exchange:

```
PowerShell

Get-CasMailbox -ResultSize unlimited -Filter "ActiveSyncEnabled -eq
`$false"
```

Политики почтовых ящиков мобильных устройств в Exchange Server

Статья • 04.04.2023

В Exchange Server можно создать политики почтовых ящиков мобильных устройств, чтобы применить общий набор политик или параметров безопасности к коллекции пользователей. После развертывания Exchange ActiveSync в организации Exchange Server можно создать новые политики почтовых ящиков мобильных устройств или изменить существующие политики. При установке Exchange Server создается политика почтовых ящиков мобильных устройств по умолчанию. Эта политика назначается всем пользователям автоматически.

Обзор политик почтовых ящиков мобильных устройств

Политики почтовых ящиков мобильных устройств можно использовать для управления множеством различных параметров. например:

- Требование ввести пароль
- Минимальная длина пароля
- Требование наличия в пароле числа или специального символа
- Период бездействия устройства перед требованием повторного ввода пароля
- Очистка устройства после указанного количества неудачных попыток ввести пароль

Дополнительные сведения о всех настраиваемых параметрах см. в разделе "Параметры политик мобильных устройств".

Политики почтовых ящиков мобильных устройств Exchange

Exchange ActiveSync — клиентский протокол, который позволяет синхронизировать мобильное устройство с почтовым ящиком Exchange. Exchange ActiveSync включен по умолчанию при установке Exchange Server.

Политики почтовых ящиков для мобильных устройств можно создавать в Центре администрирования Exchange и в командной консоли Exchange. В Центре

администрирования Exchange можно настроить только часть доступных параметров. Остальные параметры можно настроить с помощью командной консоли Exchange.

Параметры пароля мобильного устройства и биометрические данные

Многие мобильные устройства поддерживают биометрические данные, такие как Apple Touch ID или Face ID. Политики почтовых ящиков мобильных устройств Exchange не определяют, можно ли использовать биометрические данные вместо ввода ПИН-кода устройства. Политики почтовых ящиков мобильных устройств можно настроить так, чтобы требовать ПИН-код устройства, но затем пользователи определяют, используют ли они биометрические данные после выполнения требования к ПИН-коду устройства.

Параметры пароля мобильного устройства и Android

Android 9.0 и более ранних версий используют функции администрирования устройств Android для управления параметрами паролей устройств, определенными в политике почтовых ящиков мобильных устройств.

В Android 10.0 и более поздних версиях Android удалила функции администрирования устройств. Вместо этого приложения, которым требуется блокировка экрана, запрашивают сложность блокировки экрана устройства (или рабочего профиля). Приложения, которым требуется более надежная блокировка экрана, направляют пользователя к системным параметрам блокировки экрана, позволяя пользователю обновить параметры безопасности, чтобы они соответствовали требованиям. Приложение не знает пароль пользователя; приложению известно только уровень сложности пароля. Android поддерживает следующие четыре уровня сложности пароля:

Уровень сложности пароля	**Требования к паролям**
Нет	Требования к паролю не настроены
Низкая	Пароль может быть шаблоном или ПИН-кодом с повторяющимися последовательности (4444) или упорядоченными (1234, 4321, 2468)

Уровень сложности пароля	Требования к паролям
Средняя	Пароли, соответствующие одному из следующих критериев: • ПИН-код без повторяющихся последовательностей (4444) или упорядоченных (1234, 4321, 2468) с минимальной длиной в 4 символа • Алфавитные пароли длиной не менее 4 символов • Буквенно-цифровые пароли длиной не менее 4 символов
Высокая	Пароли, соответствующие одному из следующих критериев: • ПИН-код без повторяющихся последовательностей (4444) или упорядоченных (1234, 4321, 2468) с минимальной длиной 8 символов • Алфавитные пароли длиной не менее 6 символов • Буквенно-цифровые пароли длиной не менее 6 символов

С точки зрения политики почтовых ящиков мобильных устройств Exchange уровни сложности паролей Android сопоставляются со следующими параметрами политики:

Параметр политики почтового ящика мобильных устройств	Уровень сложности пароля Android
Пароль включен = false	Нет
Разрешить простой пароль = true Минимальная длина < пароля 4	Низкая
Разрешить простой пароль = true Минимальная длина < пароля 6	Средняя
Разрешить простой пароль = false Требуется буквенно-цифровой пароль = true Минимальная длина < пароля 6	Средняя
Разрешить простой пароль = true Минимальная длина > пароля 6	Высокая
Разрешить простой пароль = false Требуется буквенно-цифровой пароль = true Минимальная длина >пароля = 6	Высокая

Параметры политики почтовых ящиков мобильного устройства

В следующей таблице перечислены параметры, которые можно задать с помощью политик почтовых ящиков мобильных устройств.

Setting	**Описание**
Разрешить Bluetooth	Данный параметр определяет, будет ли мобильное устройство принимать подключения Bluetooth. Доступны следующие значения: "Отключить", "Только для громкой связи" и "Разрешить". Значение этого параметра по умолчанию — "Разрешить".
Разрешить браузер	Этот параметр определяет, разрешен ли на мобильном устройстве браузер Pocket Internet Explorer. Этот параметр не влияет на браузеры сторонних производителей, установленные на мобильном устройстве. Значение по умолчанию — `$true`.
Разрешить камеру	Этот параметр определяет, можно ли использовать камеру мобильного устройства. Значение по умолчанию — `$true`.
Разрешить пользовательскую электронную почту	Этот параметр определяет, может ли пользователь настраивать личную учетную запись электронной почты (POP3 или IMAP4) на мобильном устройстве. Значение по умолчанию — `$true`. Этот параметр не контролирует доступ посторонних почтовых программ для мобильных устройств к электронной почте.
Разрешить синхронизацию с настольным ПК	Этот параметр определяет, может ли мобильное устройство синхронизироваться с настольным компьютером через кабель, порт IrDA или Bluetooth. Значение по умолчанию — `$true`.
Разрешить управление внешним устройством	Этот параметр определяет, разрешено ли внешней программе управления устройствами управлять мобильным устройством.
Разрешить сообщения электронной почты в формате HTML	Этот параметр определяет, может ли электронная почта при синхронизации с мобильным устройством сохранять формат HTML. Если для этого параметра задано значение `$false`, все сообщения электронной почты преобразуются в обычный текст.
Разрешить общий доступ к Интернету	Этот параметр определяет, можно ли использовать мобильное устройство в качестве модема для настольного или портативного компьютера. Значение по умолчанию — `$true`.
AllowIrDA	Этот параметр определяет, разрешены ли на мобильном устройстве инфракрасные соединения.
Разрешить обновление Mobile OTA	Этот параметр определяет, можно ли отправлять параметры политики почтового ящика мобильного устройства на мобильное устройство через мобильное подключение. Значение по умолчанию — `$true`.

Setting	Описание
Разрешить неинициализируемые устройства	Этот параметр указывает, разрешено ли мобильным устройствам, поддерживающим применение всех параметров политики, подключаться к Exchange Server с помощью Exchange ActiveSync. Использование неинициализируемых мобильных устройств представляет угрозы для безопасности. Например, некоторые неинициализируемые устройства могут не применять требования организации к паролям.
Разрешить POPIMAPEmail	Этот параметр определяет, может ли пользователь настроить на мобильном устройстве учетную запись электронной почты POP3 или IMAP4. Значение по умолчанию — `$true`. Этот параметр не управляет доступом посторонних почтовых программ.
Разрешить подключение к удаленному рабочему столу	Этот параметр определяет, может ли мобильное устройство инициировать подключение к удаленному рабочему столу. Значение по умолчанию — `true`.
Разрешить использовать простой пароль	Этот параметр включает или отключает функцию использования простого пароля, например "1111" или "1234". Значение по умолчанию — `$true`.
Разрешить согласование алгоритма шифрования S/MIME	Этот параметр указывает, может ли приложение для обмена сообщениями на мобильном устройстве согласовывать алгоритм шифрования, если сертификат получателя не поддерживает указанный алгоритм шифрования.
Разрешить сертификаты программного обеспечения S/MIME	Этот параметр определяет, разрешены ли на мобильном устройстве сертификаты программного обеспечения S/MIME.
Разрешить карты памяти	Этот параметр определяет, позволяет ли мобильное устройство получать доступ к сведениям, которые хранятся на карте памяти.
Разрешить обмен текстовыми сообщениями	Этот параметр указывает, разрешен ли для мобильного устройства обмен текстовыми сообщениями. Значение по умолчанию — `$true`.
Разрешить неподписанные приложения	Этот параметр указывает, можно ли устанавливать на мобильное устройство неподписанные приложения. Значение по умолчанию — `$true`.
Разрешить неподписанные установочные пакеты	Этот параметр указывает, можно ли запускать на мобильном устройстве неподписанные установочные пакеты. Значение по умолчанию — `$true`.

Setting	Описание
Разрешить Wi-Fi	Этот параметр указывает, разрешен ли для мобильного устройства беспроводной доступ к Интернету. Значение по умолчанию — `$true`.
Требовать ввода буквенно-цифрового пароля	Этот параметр требует, чтобы пароль содержал не только цифры, но и другие символы. Значение по умолчанию — `$true`.
Список одобренных приложений	Этот параметр содержит список одобренных приложений, которые можно запускать на мобильном устройстве.
Вложения разрешены	Этот параметр разрешает загрузку вложений на мобильное устройство. Значение по умолчанию — `$true`.
Шифрование устройства включено	Этот параметр включает шифрование на мобильном устройстве. Не все мобильные устройства могут поддерживать шифрование. Дополнительные сведения см. в документации на устройство и операционную систему.
Интервал обновления политики устройства	Этот параметр указывает частоту, с которой политики почтового ящика мобильного устройства отправляется с сервера на мобильное устройство.
Служба IRM включена	Этот параметр указывает, включена ли служба управления правами доступа к данным (IRM) на мобильном устройстве.
Максимальный размер вложения	Этот параметр контролирует максимальный размер вложений, которые могут быть загружены на мобильное устройство. Значение по умолчанию — "Unlimited".
Фильтр максимального времени хранения календаря	Этот параметр задает максимальный диапазон дней календаря, который можно синхронизировать с мобильным устройством. Допустимы следующие значения: 1: Все 2: OneDay 3: Три дня 4: OneWeek 5: Две недели 6: OneMonth

Setting	Описание
Фильтр максимального времени хранения электронной почты	Этот параметр задает максимальное количество дней для сообщений электронной почты, для которых выполняется синхронизация с мобильным устройством. Допустимы следующие значения: 1: Все 2: OneDay 3: Три дня 4: OneWeek 5: Две недели 6: OneMonth
Максимальный размер усечения текста сообщений электронной почты	Этот параметр задает максимальный размер сообщений электронной почты, при котором они усекаются во время синхронизации с мобильным устройством. Значение задается в килобайтах (КБ).
Максимальный размер текста сообщений электронной почты в формате HTML	Этот параметр задает максимальный размер сообщений электронной почты в формате HTML, при котором они усекаются во время синхронизации с мобильным устройством. Значение задается в килобайтах (КБ).
Максимальное время простоя до блокировки	Этот параметр указывает период бездействия мобильного устройства, в течение которого для возобновления работы устройства не требуется вводить пароль. Можно задать интервал от 30 секунд до 1 часа. Значение по умолчанию равно 15 минутам.
Максимальное количество неудачных попыток ввода пароля	Этот параметр указывает число попыток ввода правильного пароля для мобильного устройства. Можно ввести число от 4 до 16. Значение по умолчанию — 8.
Минимальное количество сложных символов в пароле	Этот параметр задает необходимое количество наборов символов в пароле мобильного устройства. К наборам символов относятся: • Параметр MinPasswordComplexCharacters задает кодировку для пароля на мобильном устройстве. Кодировка предусматривает использование таких символов: • буквы нижнего регистра; • буквы верхнего регистра; • специальные символы (например, восклицательные знаки). Можно ввести любое число от 1 до 4. Значение по умолчанию равно 1.

Setting	Описание
Минимальная длина пароля	Этот параметр указывает минимальное число знаков в пароле мобильного устройства. Можно ввести число от 1 до 16. Значение по умолчанию — 4.
Пароль включен	Этот параметр включает пароль мобильного устройства.
Срок действия пароля	Этот параметр позволяет администратору настроить временной интервал, по истечении которого необходимо изменить пароль мобильного устройства.
Журнал пароля	Этот параметр определяет число использовавшихся паролей, хранящихся в почтовом ящике пользователя. Пользователь не может использовать сохраненный пароль повторно.
Восстановление пароля включено	При включении этого параметра на мобильном устройстве создается пароль для восстановления, который отправляется на сервер. Если пользователь забыл пароль мобильного устройства, чтобы разблокировать мобильное устройство и разрешить пользователю создать новый пароль, можно использовать пароль для восстановления.
Требовать шифрование устройства	Этот параметр определяет, необходимо ли шифрование для устройства. Если задано значение `$true`, мобильное устройство должно поддерживать и реализовывать шифрование для синхронизации с сервером.
Требовать шифрование сообщений S/MIME	Этот параметр определяет, необходимо ли шифровать сообщения S/MIME. Значение по умолчанию — `$false`.
Требовать алгоритм шифрования S/MIME	Этот параметр задает алгоритм, который должен использоваться для шифрования сообщений S/MIME.
Требовать при роуминге выполнение синхронизации вручную	Этот параметр указывает, должно ли мобильное устройство синхронизироваться вручную при роуминге. Включение автоматической синхронизации при роуминге может привести к непредвиденным расходам на мобильную связь.
Требовать подписанный алгоритм S/MIME	Этот параметр задает алгоритм, который должен использоваться для подписи сообщения.
Требовать подписанные сообщения S/MIME	Этот параметр указывает, должно ли мобильное устройство отправлять подписанные сообщения S/MIME.

Setting	Описание
Требовать шифрование карты памяти	Этот параметр определяет, необходимо ли шифровать карту памяти. Не все операционные системы для мобильных устройств поддерживают шифрование карт памяти. Дополнительные сведения см. в документации к мобильному устройству и операционной системе.
Список недопустимых приложений в ПЗУ	Этот параметр содержит список приложений, которые невозможно запускать в ПЗУ.

Мобильные устройства в Exchange Server

Статья • 04.04.2023

Для Exchange ActiveSync поддерживается множество различных мобильных телефонов и устройств. К ним относятся телефоны и планшеты с Android, а также apple iPhone, iPod и iPad.

Как телефонные, так и нефоновые мобильные устройства поддерживают Exchange ActiveSync, и в большинстве Exchange ActiveSync документации мы используем термин "*мобильное устройство*". Если описываемые компоненты нуждаются в использовании сотовой сети, например для SMS-уведомлений, этот термин относится к мобильным телефонам и другим мобильным устройствам, таким как планшеты.

Для чего используется Exchange ActiveSync?

Exchange ActiveSync — это протокол связи, который предоставляет возможность мобильного доступа по радиоканалу к сообщениям электронной почты, данным планирования, контактам и задачам. Exchange ActiveSync доступно на сторонних телефонах, которые включены для Exchange ActiveSync.

Служба Exchange ActiveSync предлагает технологию Direct Push. Технология Direct Push использует зашифрованное HTTPS-соединение, устанавливаемое и поддерживаемое между мобильным устройством и сервером и предназначенное для передачи сообщений электронной почты и других данных Exchange на телефон.

Чтобы использовать прямую отправку с Microsoft Exchange Server 2013, у пользователей должно быть мобильное устройство, предназначенное для поддержки прямой отправки.

Функции Exchange ActiveSync

Exchange ActiveSync предоставляет доступ к множеству различных функций, которые позволяют принудительно применять политики безопасности на мобильных устройствах. С помощью Exchange 2013 можно настроить несколько политик почтовых ящиков для мобильных устройств и управлять тем, какие мобильные устройства могут синхронизироваться с вашим сервером Exchange.

Exchange ActiveSync позволяет отправить удаленному устройству команду очистки, которая уничтожит все данные на мобильном устройстве в случае, если оно будет утеряно или украдено. Пользователи также могут запустить очистку удаленного устройства из приложения Outlook Web App.

Exchange ActiveSync дает пользователям возможность создать пароль для восстановления. Пароль для восстановления сохраняется на мобильном устройстве и применяется, когда пользователь забывает пароль. Пользователь создает пароль для восстановления одновременно с созданием пароля или ПИН-кода для устройства. Этот пароль для восстановления может использоваться для разблокировки мобильных устройств. Сразу после использования этого пароля для восстановления от пользователя потребуется задать новый ПИН-код.

Ограничения POP3 и IMAP4

Если ваше мобильное устройство не поддерживает Exchange ActiveSync или вам не нужен набор функций, доступный Exchange ActiveSync, вы можете использовать ПРОТОКОЛ POP3 или IMAP4 для доступа к электронной почте на мобильном устройстве. Дополнительные сведения о доступе по протоколам POP3 и IMAP4 к почтовому ящику см. в разделе POP3 и IMAP4 в Exchange Server.

Настройка мобильных телефонов для доступа к электронным сообщениям

Статья • 04.04.2023

В этой статье описано, как предоставить пользователям в вашей организации доступ к почтовым ящикам Exchange 2016 или Exchange 2019 с мобильных устройств с помощью Exchange ActiveSync.

Предварительные требования

- Вы ознакомились с документацией изготовителя на мобильный телефон, который необходимо настроить.
- В организации включена поддержка Exchange ActiveSync.

> ⓘ **Примечание**
>
> Сведения о настройке электронной почты на основе Exchange на телефоне или планшете см. в статье **Настройка приложений Office и электронной почты на мобильном устройстве**.

Настройка мобильного телефона или устройства для использования Exchange ActiveSync

Большинство мобильных телефонов и устройств могут использовать автообнаружения в Exchange для настройки мобильного почтового клиента для использования Exchange ActiveSync. Чтобы настроить учетную запись электронной почты на большинстве мобильных устройств, вам потребуется два элемента информации.

- Адрес электронной почты пользователя.
- Пароль пользователя.

Если мобильный телефон не может автоматически связаться с сервером Exchange Server через службу автообнаружения, необходимо настроить мобильный телефон вручную. Для ручной настройки требуется адрес электронной почты и пароль, а

также имя сервера Exchange ActiveSync. В большинстве организаций имя сервера Exchange ActiveSync совпадает с именем сервера Outlook в Интернете без параметра /owa, например, mail.contoso.com.

Выполнение удаленной очистки на мобильном телефоне

Статья • 04.04.2023

Пользователи каждый день носят в своих карманах конфиденциальные корпоративные данные. Если один из них потеряет свой мобильный телефон, ваши данные могут попасть в чужие руки. Если один из пользователей потеряет свой мобильный телефон, вы можете использовать Центр администрирования Exchange (EAC) или командную консоль Exchange, чтобы очистить телефон от всех корпоративных и пользовательских данных.

> ⓘ **Примечание**
>
> В этом разделе также содержатся инструкции по использованию Outlook в Интернете для выполнения удаленной очистки телефона. Чтобы выполнить удаленную очистку, пользователь должен войти в Outlook в Интернете.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Мобильные устройства" в разделе Разрешения для клиентов и мобильных устройств .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> ⓘ **Примечание**
>
> До версии EAS версии 16.1 удаленная очистка выполняла очистку на уровне устройства, восстанавливая состояние устройства до заводских условий. В EAS версии 16.1 и более поздних версиях EAS также поддерживает удаленную очистку только для учетных записей. Чтобы это работало, клиент должен поддерживать протокол EAS версии 16.1. Если клиент не поддерживает версию 16.1, очистка завершится ошибкой и будет выдана ошибка.

> ⊗ **Внимание!**

Exchange ActiveSync версии 16.1 поддерживает два разных процесса удаленной очистки: удаленную **очистку данных** и удаленную очистку **устройства только для учетных записей**. Существуют важные различия между реакцией Outlook и тем, как собственные почтовые приложения в iOS и Android реагируют на эти различные команды очистки.

Outlook для iOS и Outlook для Android поддерживают только команду **Очистка данных** , которая очищает только данные в Outlook. Приложение Outlook сброшено, и все данные электронной почты, календаря, контактов и файлов Outlook будут удалены, но никакие другие данные не будут удалены с устройства. Поэтому команда **удаленной очистки устройства только для учетных записей** является избыточной и не поддерживается Outlook для iOS или Android.

Однако если собственное почтовое приложение iOS или Android подключено к Exchange и получает команду **очистки данных** от Exchange ActiveSync, все данные на устройстве будут очищаться, включая фотографии, личные файлы и т. д.

Если собственное почтовое приложение iOS или Android подключено к Exchange и получает команду **удаленной очистки устройства только для учетных записей** от Exchange ActiveSync, очищаются только данные Exchange ActiveSync почты, календаря и учетной записи собственного почтового приложения.

Эти команды предназначены для уничтожения данных. Соблюдайте осторожность при их использовании.

После команды администратора удаленная очистка произойдет в течение несколько секунд после подключения приложения Outlook к Exchange.

Так как для каждого пользователя Outlook для iOS и Android в Exchange отображается один идентификатор мобильного устройства, команда удаленной очистки удалит данные и отношения синхронизации со всех устройств с Outlook (iPhone, iPad, Android), связанных с этим пользователем.

При удаленной очистке профиль синхронизации удаляется, поэтому, когда пользователь добавляет свою учетную запись в Outlook для iOS и Android, создается новый идентификатор устройства, который передается локальной службе Exchange.

ⓘ Примечание

Если вы используете Intune, вы должны использовать Intune для активации удаления данных, а не Exchange. В зависимости от сценария это можно выполнить с помощью **выборочной очистки политики защиты приложений** или **команд списания или очистки регистрации устройств**.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Очистка телефона пользователя с помощью Центра администрирования Exchange

Для очистки телефона пользователя или отмены еще не завершенной очистки можно использовать Центр администрирования Exchange.

1. В Центре администрирования Exchange (EAC) выберите **Получатели**>**Почтовые ящики**.
2. Выберите пользователя, а затем в разделе **Мобильные устройства** щелкните **Просмотреть сведения**.
3. На странице **Сведения о мобильном устройстве** выберите потерянное мобильное устройство, а затем выберите **Очистить данные** (или **При необходимости удаленное удаление устройства только для учетной записи**).
4. Нажмите кнопку **Сохранить**.

Очистка телефона пользователя с помощью командной консоли Exchange

Для очистки телефона пользователя можно использовать командлет **Clear-MobileDevice** в командной консоли Exchange.

Следующая команда очищает устройство с именем WM_TonySmith и отправляет сообщение подтверждения в admin@contoso.com.

PowerShell

```
Clear-MobileDevice -Identity WM_TonySmith -NotificationEmailAddresses
"admin@contoso.com"
```

Если устройство подключается к Exchange с помощью почтового приложения, отличного от Outlook, можно использовать следующую команду, чтобы очистить Exchange ActiveSync почты, календаря и учетных записей почтового приложения и оставить все остальные данные на устройстве без изменений:

PowerShell

```
Clear-MobileDevice -AccountOnly -Identity WM_TonySmith -
NotificationEmailAddresses "admin@contoso.com"
```

Параметр **-AccountOnly** не влияет на устройства Outlook, так как удаленная очистка только для учетной записи является единственным типом очистки, поддерживаемым Outlook. Дополнительные сведения см. в разделе Clear-MobileDevice .

Использование Outlook в Интернете для очистки телефона пользователя

Пользователи могут использовать Outlook в Интернете для очистки собственных телефонов.

1. В Outlook в Интернете щелкните значок **Параметры**.
2. В разделе **Параметры приложения** выберите **Почта**.
3. В разделе **Параметры** при необходимости разверните узел **Общие** , а затем выберите **Мобильные устройства**.
4. Выберите мобильный телефон.
5. Щелкните значок **Очистка устройства** (или значок **удаленной очистки устройства только для учетной записи**).

Использование нового Outlook в Интернете для очистки телефона пользователя

1. В Outlook в Интернете щелкните значок **Параметры**.

2. Щелкните **Просмотреть все параметры Outlook**.
3. Щелкните **Общие**, а затем выберите **Мобильные устройства**.
4. Выберите мобильный телефон.
5. Щелкните значок **Очистка устройства** (или значок **удаленной очистки устройства только для учетной записи**).

Как проверить, все ли получилось?

Существует несколько способов проверить, что удаленная очистка выполнена.

- Выполните командлет **Clear-MobileDevice** с настроенным параметром - *NotificationEmailAddresses* . По выполнении удаленной очистки на указанный вами адрес электронной почты будет выслано сообщение.
- В Центре администрирования Exchange проверьте состояние мобильного устройства. Состояние должно измениться с **Ожидание очистки** на **Очистка выполнена успешно**.
- В Outlook в Интернете проверьте состояние мобильного устройства. Состояние должно измениться с **Ожидание очистки** на **Очистка выполнена успешно**.

> ⓘ **Примечание**
>
> В среде на основе Microsoft 365 или Office 365 результат удаленной очистки устройства не передается обратно в Exchange. Даже если она прошла успешно, ей будет присвоено состояние **Ожидается**.

POP3 и IMAP4 в Exchange Server

Статья • 04.04.2023

Хотя пользователи обычно получают доступ к своим почтовым ящикам Exchange с помощью Outlook (MAPI), Outlook в Интернете (ранее известного как Outlook Web App) и Exchange ActiveSync, POP3 и IMAP4 доступны в Exchange Server 2016 и Exchange Server 2019 г. Для поддержки клиентов, по-прежнему использующих эти протоколы, необходимо запустить соответствующие службы и настроить параметры протоколов POP3 и IMAP4. Дополнительные сведения см. в следующих статьях:

- Включение и настройка POP3 на сервере Exchange Server
- Включение и настройка IMAP4 на сервере Exchange Server
- Настройка параметров SMTP с проверкой подлинности для клиентов POP3 и IMAP4 в Exchange Server

После включения и настройки ПРОТОКОЛА POP3 или IMAP4 на сервере Exchange Server можно включить или отключить доступ по протоколу POP3 или IMAP4 к определенным почтовым ящикам. Дополнительные сведения см. в статье Включение или отключение доступа по протоколу POP3 или IMAP4 к почтовым ящикам в Exchange Server.

Примечание. Клиенты подключаются к службам POP3 и IMAP4 в службах клиентского доступа (внешний интерфейс) на сервере почтовых ящиков. Они никогда не подключаются напрямую к серверным службам POP3 и IMAP4. Дополнительные сведения см. в разделе Архитектура протокола клиентского доступа.

Улучшения POP3 и IMAP4 в Exchange Server

Функции POP3 и IMAP4 в Exchange 2016 и Exchange 2019 практически не изменились по сравнению с Exchange 2013. Ниже перечислены улучшения протоколов POP3 и IMAP4 по сравнению с Exchange 2010.

- По умолчанию службы клиентского доступа (внешний интерфейс) в Exchange 2016 и 2019 автоматически прокси-подключения клиентов POP3 и IMAP4 с одного сайта Active Directory на правильный сервер почтовых ящиков на другом сайте Active Directory. В предыдущих версиях Exchange требовалось

вручную настраивать дополнительные параметры, чтобы разрешить клиентам POP3 и IMAP4 подключаться к своим почтовым ящикам на разных сайтах.

- Вы не можете использовать анонимные или гостевые учетные записи для доступа к почтовому ящику Exchange 2016 или Exchange 2019 с помощью ПРОТОКОЛА POP3 или IMAP4. Доступ блокируется во избежание возникновения уязвимостей при использовании нестандартных учетных записей для доступа по протоколам POP3 и IMAP4.
- С помощью протокола POP3 или IMAP4 невозможно подключиться к почтовому ящику администратора (можно использовать Outlook или Outlook Web App). Это ограничение реализовано в Exchange 2016 для усиления защиты почтового ящика администратора.

Общие сведения о функциональных возможностях протоколов POP3 и IMAP4

Протоколы POP3 и IMAP4 имеют следующие преимущества и ограничения.

- **POP3**
  - Предназначен для обработки сообщений в автономном режиме.
  - Позволяет скачивать сообщения только из одной папки (как правило, папки "Входящие") почтового ящика в одну папку в приложении, использующем POP3, на клиентском компьютере или устройстве.
  - По умолчанию скачанные сообщения удаляются с почтового сервера и хранятся только на локальном компьютере или устройстве. Следовательно, пользователи не могут получать доступ к одним и тем же электронным сообщениям с нескольких компьютеров или устройств (несмотря на это, многие приложения POP3 можно настраивать на сохранение копий скачанных сообщений в почтовом ящике на почтовом сервере).
  - Не поддерживает расширенные функции совместной работы, например ведение календаря, контакты и задачи.
- **IMAP4**
  - Обеспечивает обработку сообщений как в автономном режиме, так и через Интернет.

- Может синхронизировать сообщения из нескольких папок почтового ящика с клиентским компьютером или устройством. Например, большинство приложений, использующих IMAP4, можно настроить на хранение копии отправленных сообщений в почтовом ящике на почтовом сервере.

- По умолчанию копии скачанных сообщений остаются на почтовом сервере. Следовательно, пользователи могут получать доступ к одним и тем же сообщениям с нескольких компьютеров.

- Поддерживает дополнительные функции. Например, вы можете скачать заголовки сообщения (отправителя и тему), а затем решить, следует ли скачивать сообщение полностью.

- Не поддерживает расширенные функции совместной работы, например ведение календаря, контакты и задачи.

Примечание. Клиенты POP3 и IMAP4 имеют ограниченный доступ к сведениям календаря Exchange. Дополнительные сведения см. в разделах Настройка параметров календаря для POP3 и Настройка параметров календаря для IMAP4.

Приложения на основе POP3 и IMAP4 и их параметры

После включения и настройки необходимых служб пользователи смогут подключаться к своим почтовым ящикам Exchange с помощью любого приложения, поддерживающего протоколы POP3 и IMAP4. Например, Outlook, Почта Windows и Mozilla Thunderbird. Поддержка функций POP3 и IMAP4 зависит от конкретного приложения, поэтому следует ознакомиться с документацией по приложению.

Убедитесь, что почтовая программа на основе POP3 или IMAP4 настроена на хранение копий всех сообщений на сервере. Это позволяет пользователям получать доступ к своим сообщениям с разных компьютеров и из разных приложений.

Еще один важный параметр — частота, с которой почтовая программа связывается с сервером для отправки и получения почты. Существует три основных варианта:

- **Отправлять и получать сообщения при запуске приложения.**

- **Отправка и получение сообщений вручную**. Сообщения отправляются и получаются только тогда, когда пользователь щелкает параметр "отправить и

получить" в приложении. Этот вариант хорошо подходит для компьютеров, которые не всегда подключены к Интернету (например, с коммутируемыми или лимитными подключениями).

- **Отправлять и получать сообщения каждые заданные минуты**. Приложение периодически подключается к серверу электронной почты, чтобы отправлять сообщения и скачивать новые сообщения. Этот вариант хорошо подходит для компьютеров, которые всегда подключены к Интернету, так как приложение поддерживает актуальное состояние сообщений в почтовом ящике.

Примечание. Если приложение и сервер поддерживают команду IMAP4 **IDLE** , пользователи могут отправлять и получать сообщения практически в реальном времени (Exchange поддерживает команду **IDLE** IMAP4). В большинстве случаев пользователям не требуется настраивать параметры приложения IMAP4 для использования этого способа подключения.

Чтобы настроить клиент POP3 или IMAP4 на подключение к почтовому ящику, пользователям необходимы конкретные сведения о параметрах POP3 или IMAP4. По умолчанию Exchange использует следующие параметры для **внутренних** подключений POP3:

- **Полное доменное имя сервера POP3**: `<ServerFQDN>`. Например, `mailbox01.contoso.com`.

- **Tcp-порт и метод шифрования**: 995 для всегда зашифрованных подключений SSL/TLS и 110 для незашифрованных подключений или для оппортунистических TLS (**STARTTLS**), которые приводят к зашифрованным соединениям после подтверждения первоначального протокола обычного текста.

Чтобы разрешить **внешним** клиентам POP3 подключаться к почтовым ящикам, необходимо настроить эти параметры для внешних подключений. Дополнительные сведения см. в статье Включение и настройка POP3 на сервере Exchange Server.

По умолчанию Exchange использует следующие параметры для **внутренних** подключений IMAP4:

- **Полное доменное имя сервера IMAP4**: `<ServerFQDN>`. Например, `mailbox01.contoso.com`.

- **Tcp-порт и метод шифрования**: 993 для всегда зашифрованных подключений SSL/TLS и 143 для незашифрованных подключений или для оппортунистических TLS (**STARTTLS**), что приводит к зашифрованным

соединениям после подтверждения первоначального протокола обычного текста.

Чтобы разрешить **внешним** клиентам IMAP4 подключаться к почтовым ящикам, необходимо настроить эти параметры для внешних подключений. Дополнительные сведения см. в статье Включение и настройка IMAP4 на сервере Exchange Server.

Включение и настройка POP3 на сервере Exchange Server

Статья • 04.04.2023

По умолчанию подключение клиентов POP3 не разрешено в Exchange. Чтобы разрешить подключение клиентов POP3, необходимо выполнить указанные ниже действия.

1. Запустите службы POP3 и настройте их автоматический запуск:

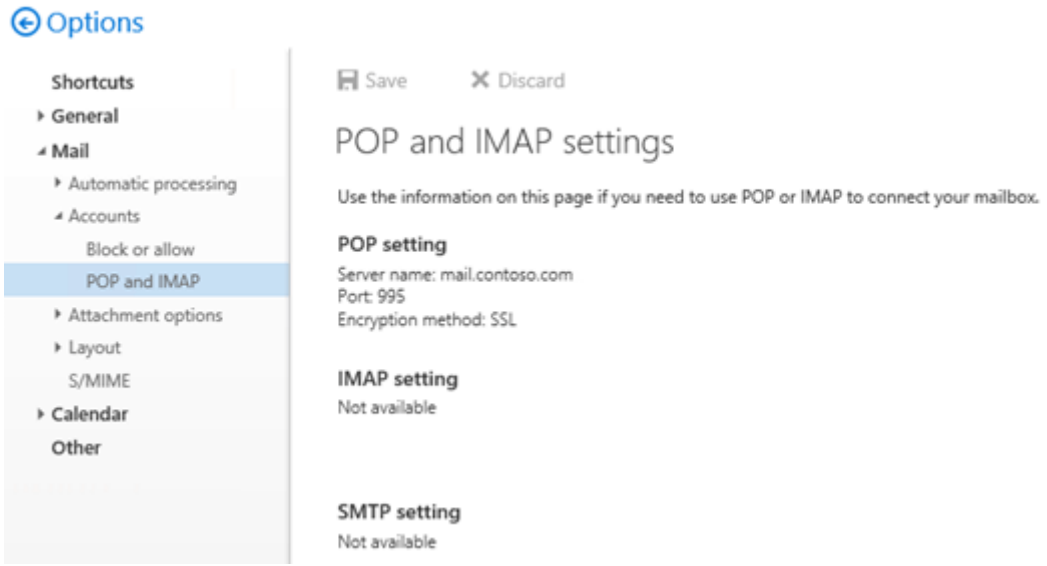
   - **Microsoft Exchange POP3**. Это служба клиентского доступа (внешний интерфейс), к которому подключаются клиенты POP3.
   - **Серверная часть POP3 Microsoft Exchange**. Клиентские подключения POP3 из службы клиентского доступа передаются через прокси-серверную службу на сервере, на который хранится активная копия почтового ящика пользователя. Дополнительные сведения см. в статье Архитектура протокола клиентского доступа.

2. Настройте параметры POP3 для внешних клиентов.

   По умолчанию Exchange использует следующие параметры для **внутренних** подключений POP3:

   - **Полное доменное имя сервера POP3**: `<ServerFQDN>`. Например, `mailbox01.contoso.com`.
   - **Tcp-порт и метод шифрования**: 995 для всегда зашифрованных подключений TLS и 110 для незашифрованных подключений или для оппортунистических TLS (**STARTTLS**), что приводит к зашифрованным соединениям после подтверждения первоначального протокола обычного текста.

   Чтобы разрешить **внешним** клиентам POP3 подключаться к почтовым ящикам, необходимо настроить полное доменное имя сервера POP3, TCP-порт и метод шифрования для внешних подключений. На этом шаге внешние параметры POP3 отображаются в Outlook в Интернете (прежнее название — Outlook Web App) в разделе **Параметры**>**Параметры**>**Учетные записи почты**>>**POP и IMAP**.



3. Перезапустите службы POP3, чтобы сохранить изменения.

4. Настройте параметры протокола SMTP с проверкой подлинности для внутренних и внешних клиентов. Дополнительные сведения см. в статье Настройка параметров SMTP с проверкой подлинности для клиентов POP3 и IMAP4 в Exchange Server.

Дополнительные сведения о POP3 см. в разделе POP3 и IMAP4 в Exchange Server.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут.

- Теперь для шифрования данных, которыми обмениваются компьютерные системы, используется протокол TLS вместо протокола SSL. Они настолько тесно связаны, что термины "SSL" и "TLS" (без версий) часто используются взаимозаменяемо. Из-за этого сходства ссылки на "SSL" в разделах Exchange, Центре администрирования Exchange и командной консоли Exchange часто используются для охвата протоколов SSL и TLS. Как правило, термин "SSL" обозначает именно протокол SSL только в тех случаях, когда указан номер версии (например, SSL 3.0). Чтобы узнать, почему следует отключить протокол SSL и переключиться на TLS, см. статью Защита от уязвимости SSL 3.0.

- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения POP3 и IMAP4" раздела Разрешения клиентов и мобильных устройств .

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Этап 1. Запуск служб POP3 и настройка их автоматического запуска

Это действие можно выполнить с помощью консоли "Службы Windows" или командной консоли Exchange.

Запуск служб POP3 и настройка их автоматического запуска с помощью консоли "Службы Windows"

1. Откройте консоль "Службы Windows" на сервере Exchange Server. Например:
   - Выполните команду `services.msc` из диалогового окна **Запуск** , окна командной строки или командной консоли Exchange.
   - Откройте диспетчер сервера и щелкните **Сервис**>**службы**.
2. В списке служб выберите **Microsoft Exchange POP3** и нажмите кнопку **Свойства действия**>.
3. Откроется окно **Свойства POP3 Microsoft Exchange**. На вкладке **Общие** настройте следующие параметры:
   - **Тип запуска**: выберите **Автоматически**.
   - **Состояние службы**: нажмите кнопку **Пуск**.

   После этого нажмите кнопку **ОК**.
4. В списке служб выберите **Серверная часть Microsoft Exchange POP3**, а затем щелкните **Свойства действия**>.
5. Откроется окно **Свойства внутреннего POP3 Microsoft Exchange**. На вкладке **Общие** настройте следующие параметры:

- **Тип запуска**: выберите **Автоматически**.
- **Состояние службы**: нажмите кнопку **Пуск**.

После этого нажмите кнопку **ОК**.

Запуск служб POP3 и настройка их автоматического запуска с помощью командной консоли Exchange

1. Выполните следующую команду, чтобы запустить службы POP3:

```
PowerShell

Start-Service MSExchangePOP3; Start-Service MSExchangePOP3BE
```

2. Выполните следующую команду, чтобы настроить автоматический запуск служб POP3:

```
PowerShell

Set-Service MSExchangePOP3 -StartupType Automatic; Set-Service
MSExchangePOP3BE -StartupType Automatic
```

Дополнительные сведения об этих командлетах см. в статьях Start-Service и Set-Service.

Как убедиться, что все получилось?

Чтобы проверить, успешно ли запущены службы POP3, выполните одно из указанных ниже действий.

- На сервере Exchange Server откройте диспетчер задач Windows. Откройте вкладку **Службы** и убедитесь, что в столбце **Состояние** для служб **MSExchangePOP3** и **MSExchangePOP3BE** указано значение **Работает**.
- В командной консоли Exchange выполните следующую команду, чтобы убедиться, что службы POP3 запущены:

```
PowerShell

Get-Service MSExchangePOP3; Get-Service MSExchangePOP3BE
```

Этап 2. Настройка параметров POP3 для внешних клиентов с помощью командной консоли Exchange

Чтобы настроить параметры POP3 для внешних клиентов, используйте следующий синтаксис:

PowerShell

```
Set-PopSettings -ExternalConnectionSettings "<FQDN1>:<TCPPort1>:<SSL | TLS | blank>", "<FQDN2>:<TCPPort2>:<SSL | TLS | blank>"...  -X509CertificateName <FQDN> [-SSLBindings "<IPv4Orv6Address1>:<TCPPort1>","<IPv4Orv6Address2>:<TCPPort2>"...] [-UnencryptedOrTLSBindings "<IPv4Orv6Address1>:<TCPPort1>","<IPv4Orv6Address2>:<TCPPort2>"...]
```

В этом примере для внешних подключений POP3 настраиваются следующие параметры:

- **Полное доменное имя сервера POP3**: mail.contoso.com
- **TCP-порт**: 995 для всегда зашифрованных подключений TLS и 110 для незашифрованных подключений или оппортунистических подключений TLS (STARTTLS).
- **Внутренний IP-адрес сервера Exchange и TCP-порт для всегда зашифрованных подключений TLS**: все доступные IPv4 и IPv6-адреса на сервере через порт 995 (параметр *SSLBindings не используется* , а значение по умолчанию — `[::]:995,0.0.0.0:995`).
- **Внутренний IP-адрес сервера Exchange и TCP-порт для незашифрованных или оппортунистических подключений TLS (STARTTLS):** все доступные адреса IPv4 и IPv6 на сервере через порт 110 (мы не используем параметр *UnencryptedOrTLSBindings* , а значение по умолчанию — `[::]:110,0.0.0.0:110`).
- **Полное доменное имя, используемое для шифрования**: mail.contoso.com. Это значение указывает сертификат, который совпадает с полным доменным именем сервера POP3 или содержит его.

PowerShell

```
Set-PopSettings -ExternalConnectionSettings "mail.contoso.com:995:SSL","mail.contoso.com:110:TLS" -X509CertificateName mail.contoso.com
```

Примечания:

- Дополнительные сведения о синтаксисе и параметрах см. в разделе Set-PopSettings.
- Полному доменному имени внешнего сервера POP3 должна соответствовать запись на общедоступном DNS-сервере, а TCP-порт (110 или 995) должен быть разрешен в брандмауэре на сервере Exchange Server.
- Сочетание методов шифрования и TCP-портов, используемых для параметра *ExternalConnectionSettings* , должны соответствовать соответствующим TCP-портам и методам шифрования, используемым для параметров *SSLBindings* или *UnencryptedOrTLSBindings* .
- Хотя для POP3 можно использовать отдельный сертификат, рекомендуется использовать тот же сертификат, что и другие службы Exchange IIS (HTTP), который, скорее всего, представляет собой сертификат с подстановочным знаком или сертификат альтернативного имени субъекта (SAN) из коммерческого центра сертификации, которому автоматически доверяют все клиенты. Дополнительные сведения см. в статье Требования к сертификатам для служб Exchange.
- Если вы используете сертификат с одним субъектом или сертификат SAN, необходимо также назначить сертификат службе Exchange POP. Вам не нужно назначать сертификат с подстановочными знаками службе POP Exchange. Дополнительные сведения см. в статье Назначение сертификатов Exchange Server службам.

Как убедиться, что все работает?

Чтобы убедиться, что вы успешно настроили параметры POP3 для внешних клиентов, выполните приведенную ниже команду в командной консоли Exchange и проверьте параметры.

PowerShell

```
Get-PopSettings | Format-List
*ConnectionSettings,*Bindings,X509CertificateName
```

Дополнительные сведения см. в статье Get-POPSettings.

Этап 3. Перезапуск служб POP3

После включения и настройки протокола POP3 необходимо перезапустить службы POP3 на сервере с помощью консоли "Службы Windows" или командной консоли Exchange.

Перезапуск служб POP3 с помощью консоли "Службы Windows"

1. Откройте консоль "Службы Windows" на сервере Exchange Server.
2. В списке служб выберите **Microsoft Exchange POP3** и нажмите кнопку**Перезапуститьдействие**>.
3. В списке служб выберите **Серверная часть Microsoft Exchange POP3** и нажмите кнопку**Перезапуститьдействие**>.

Перезапуск служб POP3 с помощью командной консоли Exchange

Чтобы перезапустить службы POP3, выполните следующую команду:

```
PowerShell

Restart-Service MSExchangePOP3; Restart-Service MSExchangePOP3BE
```

Дополнительные сведения об этом командлете см. в статье Restart-Service.

Чтобы убедиться, что службы POP3 успешно перезапущены, выполните следующую команду:

```
PowerShell

Get-Service MSExchangePOP3; Get-Service MSExchangePOP3BE
```

Этап 4. Настройка параметров протокола SMTP с проверкой подлинности для клиентов POP3

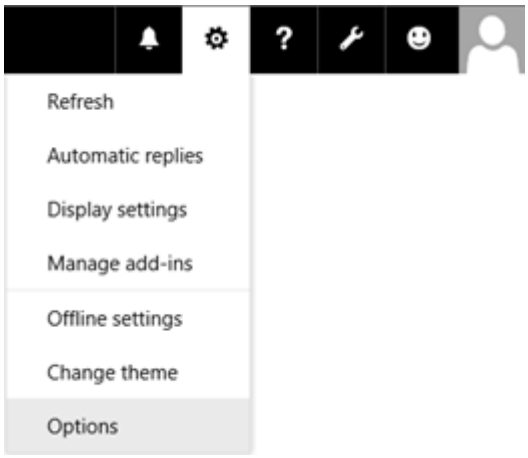
Так как протокол POP3 не используется для отправки электронных сообщений, вам необходимо настроить параметры протокола SMTP с проверкой подлинности,

которые используются внутренними и внешними клиентами POP3. Дополнительные сведения см. в разделе POP3 и IMAP4 в Exchange Server.

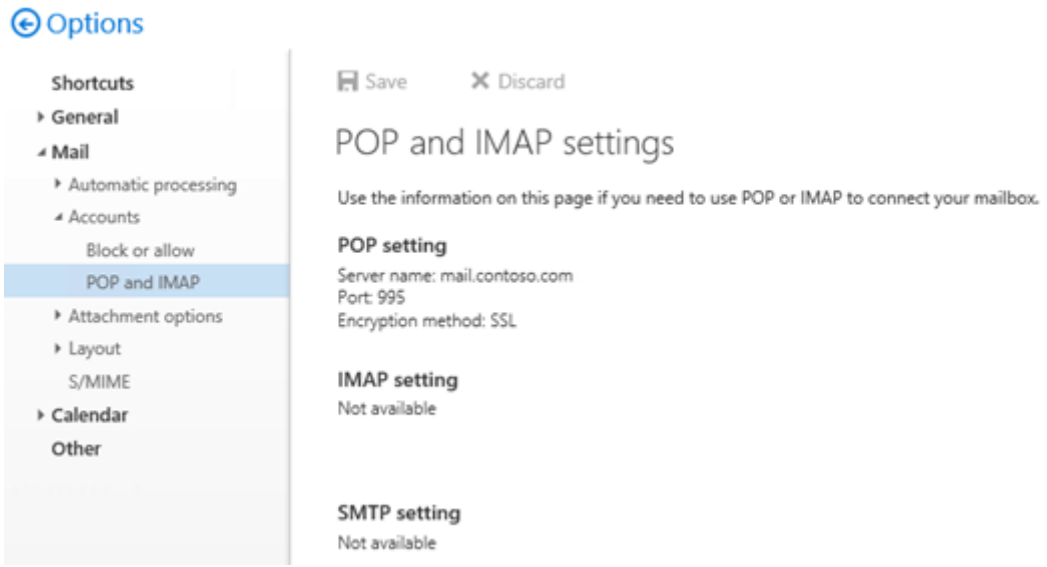
Как убедиться, что это сработало?

Чтобы убедиться, что вы включили и настроили протокол POP3 на сервере Exchange Server, выполните указанные ниже действия.

1. Откройте почтовый ящик в Outlook в Интернете и щелкните **Параметры**>.



2. Щелкните **Почтовые**>**учетные**> записи**POP и IMAP** и убедитесь, что отображаются правильные параметры POP3.



Примечание. Если вы настроили значения 995/SSL **и** 110/TLS для параметра *ExternalConnectionSettings* в **командлете Set-PopSettings**, в Outlook в Интернете отображается только значение 995/SSL. Кроме того, если настроенные внешние параметры POP3 не отображаются должным образом в Outlook в Интернете после перезапуска служб POP3 выполните команды `net stop w3svc /y` и `net start w3svc` перезапустить службы IIS.

3. Вы можете проверить подключение клиента POP3 к серверу Exchange Server следующими способами:

   - **Внутренние клиенты**. Используйте командлет **Test-PopConnectivity** . Например, `Test-PopConnectivity -ClientAccessServer <ServerName> -Lightmode -MailboxCredential (Get-Credential)`. Дополнительные сведения см. в статье Test-PopConnectivity.

     Примечание. *Переключатель Lightmode* сообщает, что команда теста POP3 войдется на сервер. Чтобы проверить отправку (SMTP) и получение (POP3) сообщения, необходимо настроить параметры SMTP, прошедшие проверку подлинности, как описано в разделах POP3 и IMAP4 в Exchange Server.

   - **Внешние клиенты**. Используйте тест **POP Email** в анализаторе удаленного подключения Майкрософт .

     Примечание. Вы не можете использовать ПРОТОКОЛ POP3 для подключения к почтовому ящику администратора. Это ограничение было намеренно включено в Exchange 2016 и Exchange 2019 для повышения безопасности почтового ящика администратора.

Дальнейшие действия

Сведения о включении или отключении доступа по протоколу POP3 к отдельным почтовым ящикам см. в статье Включение или отключение доступа по протоколу POP3 или IMAP4 к почтовым ящикам в Exchange Server.

Включение и настройка IMAP4 на сервере Exchange Server

Статья • 04.04.2023

По умолчанию подключение клиентов IMAP4 не разрешено в Exchange. Чтобы разрешить подключение клиентов IMAP4, необходимо выполнить следующие действия:

1. Запустите службы IMAP4 и настройте автоматический запуск служб:

   - **Microsoft Exchange IMAP4**. Это служба клиентского доступа (внешний интерфейс), к которому подключаются клиенты IMAP4.

   - **Серверная часть IMAP4 Microsoft Exchange**. Клиентские подключения IMAP4 из службы клиентского доступа передаются через прокси-серверную службу на сервере, на который хранится активная копия почтового ящика пользователя. Дополнительные сведения см. в статье Архитектура Exchange.

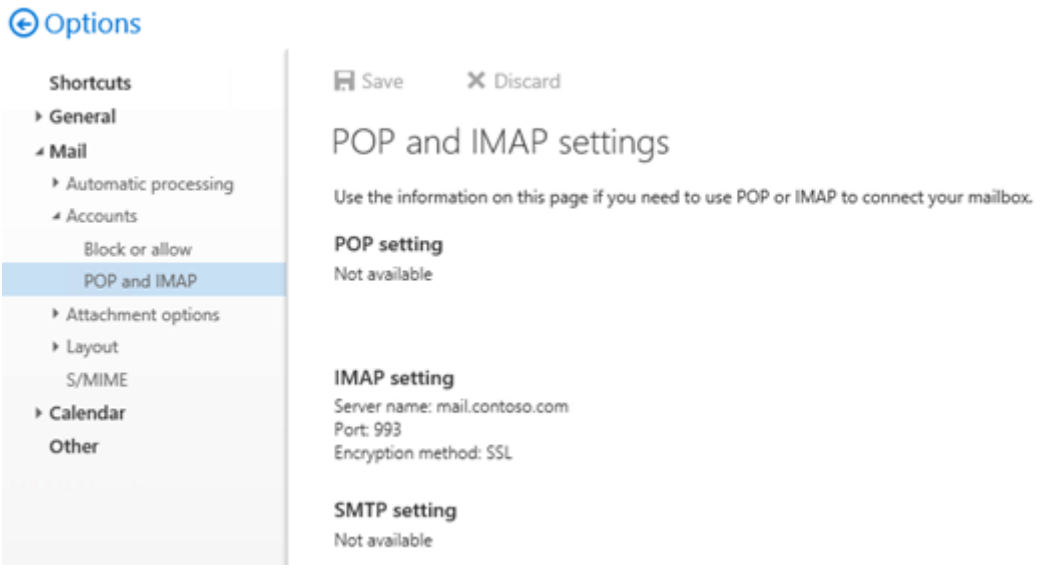
2. Настройте параметры IMAP4 для внешних клиентов.

   По умолчанию Exchange использует следующие параметры для **внутренних** подключений IMAP4:

   - **Полное доменное имя сервера IMAP4**: `<ServerFQDN>`. Например, `mailbox01.contoso.com`.

   - **Tcp-порт и метод шифрования**: 993 для всегда зашифрованных подключений TLS и 143 для незашифрованных подключений или для оппортунистических TLS (**STARTTLS**), которые приводят к зашифрованным соединениям после подтверждения первоначального подтверждения протокола обычного текста.

   Чтобы разрешить **внешним** клиентам IMAP4 подключаться к почтовым ящикам, необходимо настроить полное доменное имя сервера IMAP4, TCP-порт и метод шифрования для внешних подключений. На этом шаге внешние параметры IMAP4 отображаются в Outlook в Интернете (прежнее название — Outlook Web App) в разделе **Параметры**>**Параметры**>**Учетные записи почты**>>**POP и IMAP**.



3. Перезапустите службы IMAP4, чтобы сохранить изменения.

4. Настройте параметры протокола SMTP с проверкой подлинности для внутренних и внешних клиентов. Дополнительные сведения см . в статье Настройка параметров SMTP с проверкой подлинности для клиентов POP3 и IMAP4 в Exchange.

Дополнительные сведения об IMAP4 см. в разделе POP3 и IMAP4 в Exchange Server.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут.

- Теперь для шифрования данных, которыми обмениваются компьютерные системы, используется протокол TLS вместо протокола SSL. Они настолько тесно связаны, что термины "SSL" и "TLS" (без версий) часто используются взаимозаменяемо. Из-за этого сходства ссылки на "SSL" в разделах Exchange, Центре администрирования Exchange и командной консоли Exchange часто используются для охвата протоколов SSL и TLS. Как правило, термин "SSL" обозначает именно протокол SSL только в тех случаях, когда указан номер версии (например, SSL 3.0). Чтобы узнать, почему следует отключить протокол SSL и переключиться на TLS, см. статью Защита от уязвимости SSL 3.0 .

- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения POP3 и IMAP4" раздела Разрешения клиентов и мобильных устройств .

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Шаг 1. Запуск служб IMAP4 и настройка автоматического запуска

Это действие можно выполнить с помощью консоли "Службы Windows" или командной консоли Exchange.

Запуск служб IMAP4 и настройка автоматического запуска с помощью консоли "Службы Windows"

1. Откройте консоль "Службы Windows" на сервере Exchange Server. Например:
   - Выполните команду `services.msc` из диалогового окна **Запуск** , окна командной строки или командной консоли Exchange.
   - Откройте диспетчер сервера и щелкните **Сервис**>**службы**.
2. В списке служб выберите **Microsoft Exchange IMAP4** и нажмите кнопку **Свойства действия**>.
3. Откроется окно **Свойства IMAP4 Microsoft Exchange**. На вкладке **Общие** настройте следующие параметры:
   - **Тип запуска**: выберите **Автоматически**.
   - **Состояние службы**: нажмите кнопку **Пуск**.

   После этого нажмите кнопку **OK**.
4. В списке служб выберите **Серверная часть IMAP4 Microsoft Exchange** и нажмите кнопку **Свойства действия**>.
5. Откроется окно **Свойства внутренней службы IMAP4 Microsoft Exchange**. На вкладке **Общие** настройте следующие параметры:

- **Тип запуска**: выберите **Автоматически**.
- **Состояние службы**: нажмите кнопку **Пуск**.

После этого нажмите кнопку **ОК**.

Запуск служб IMAP4 и настройка автоматического запуска с помощью командной консоли Exchange

1. Выполните следующую команду, чтобы запустить службы IMAP4:

```
PowerShell

Start-Service MSExchangeIMAP4; Start-Service MSExchangeIMAP4BE
```

2. Выполните следующую команду, чтобы настроить автоматический запуск служб IMAP4:

```
PowerShell

Set-Service MSExchangeIMAP4 -StartupType Automatic; Set-Service
MSExchangeIMAP4BE -StartupType Automatic
```

Дополнительные сведения об этих командлетов см. в статьях Start-Service и Set-Service.

Как убедиться, что все получилось?

Чтобы проверить, успешно ли запущены службы IMAP4, выполните одно из указанных ниже действий.

- На сервере Exchange Server откройте диспетчер задач Windows. На вкладке **Службы** убедитесь, что в столбце **Состояние** для служб **MSExchangeIMAP4** и **MSExchangeIMAP4BE** указано значение **Работает**.
- В командной консоли Exchange выполните следующую команду, чтобы убедиться, что службы IMAP4 запущены:

```
PowerShell

Get-Service MSExchangeIMAP4; Get-Service MSExchangeIMAP4BE
```

Шаг 2. Настройка параметров IMAP4 для внешних клиентов с помощью командной консоли Exchange

Чтобы настроить параметры IMAP4 для внешних клиентов, используйте следующий синтаксис:

PowerShell

```
Set-ImapSettings -ExternalConnectionSettings "<FQDN1>:<TCPPort1>:<SSL | TLS | blank>", "<FQDN2>:<TCPPort2>:<SSL | TLS | blank>"...  -X509CertificateName <FQDN> [-SSLBindings "<IPv4Orv6Address1>:<TCPPort1>","<IPv4Orv6Address2>:<TCPPort2>"...] [-UnencryptedOrTLSBindings "<IPv4Orv6Address1>:<TCPPort1>","<IPv4Orv6Address2>:<TCPPort2>"...]
```

В этом примере для внешних подключений IMAP4 настраиваются следующие параметры:

- **Полное доменное имя сервера IMAP4**: mail.contoso.com
- **TCP-порт**: 993 для всегда зашифрованных подключений TLS и 143 для незашифрованных подключений или оппортунистических подключений TLS (STARTTLS).
- **Внутренний IP-адрес сервера Exchange и TCP-порт для всегда зашифрованных подключений TLS**: все доступные IPv4 и IPv6-адреса на сервере через порт 993 (параметр *SSLBindings не используется* , а значение по умолчанию — `[::]:993,0.0.0.0:993`).
- **Внутренний IP-адрес сервера Exchange и TCP-порт для незашифрованных или оппортунистических подключений TLS (STARTTLS):** все доступные адреса IPv4 и IPv6 на сервере через порт 143 (мы не используем параметр *UnencryptedOrTLSBindings* , а значение по умолчанию — `[::]:143,0.0.0.0:143`).
- **Полное доменное имя, используемое для шифрования**: mail.contoso.com. Это значение указывает сертификат, который совпадает с полным доменным именем сервера IMAP4 или содержит его.

PowerShell

```
Set-ImapSettings -ExternalConnectionSettings "mail.contoso.com:993:SSL","mail.contoso.com:143:TLS" -X509CertificateName mail.contoso.com
```

Примечания.

- Дополнительные сведения о синтаксисе и параметрах см. в разделе Set-IMAPSettings.
- Полному доменному имени внешнего сервера IMAP4 должна соответствовать запись на общедоступном DNS-сервере, а TCP-порт (143 или 993) должен быть разрешен в брандмауэре на сервере Exchange Server.
- Сочетание методов шифрования и TCP-портов, используемых для параметра *ExternalConnectionSettings* , должны соответствовать соответствующим TCP-портам и методам шифрования, используемым для параметров *SSLBindings* или *UnencryptedOrTLSBindings* .
- Хотя для IMAP4 можно использовать отдельный сертификат, рекомендуется использовать тот же сертификат, что и другие службы Exchange IIS (HTTP), который, скорее всего, является сертификатом с подстановочным знаком или сертификатом альтернативного имени субъекта (SAN) из коммерческого центра сертификации, которому автоматически доверяют все клиенты. Дополнительные сведения см. в статье Требования к сертификатам для служб Exchange.
- Если вы используете сертификат одного субъекта или сертификат SAN, необходимо также назначить сертификат службе IMAP Exchange. Вам не нужно назначать сертификат с подстановочными знаками службе IMAP Exchange. Дополнительные сведения см. в статье Назначение сертификатов Exchange Server службам.

Как убедиться, что все работает?

Чтобы убедиться, что вы успешно настроили параметры IMAP4 для внешних клиентов, выполните приведенную ниже команду в командной консоли Exchange и проверьте параметры.

PowerShell

```
Get-ImapSettings | Format-List
*ConnectionSettings,*Bindings,X509CertificateName
```

Дополнительные сведения см. в статье Get-IMAPSettings.

Шаг 3. Перезапуск служб IMAP4

После включения и настройки IMAP4 необходимо перезапустить службы IMAP4 на сервере с помощью консоли "Службы Windows" или командной консоли Exchange.

Перезапуск служб IMAP4 с помощью консоли "Службы Windows"

1. Откройте консоль "Службы Windows" на сервере Exchange Server.
2. В списке служб выберите **Microsoft Exchange IMAP4** и нажмите кнопку **Перезапуск действия**>.
3. В списке служб выберите **Серверная часть IMAP4 Microsoft Exchange** и нажмите кнопку**Перезапуститьдействие**>.

Перезапуск служб IMAP4 с помощью командной консоли Exchange

Чтобы перезапустить службы IMAP4, выполните следующую команду:

```
PowerShell

Restart-Service MSExchangeIMAP4; Restart-Service MSExchangeIMAP4BE
```

Дополнительные сведения об этом командлете см. в статье Restart-Service.

Чтобы убедиться, что службы IMAP4 успешно перезапущены, выполните следующую команду:

```
PowerShell

Get-Service MSExchangeIMAP4; Get-Service MSExchangeIMAP4BE
```

Шаг 4. Настройка параметров протокола SMTP с проверкой подлинности для клиентов IMAP4

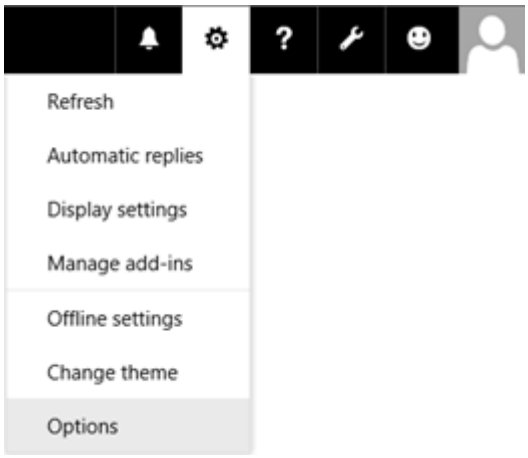
Так как IMAP4 не используется для отправки сообщений электронной почты, вам необходимо настроить параметры протокола SMTP с проверкой подлинности, которые используются внутренними и внешними клиентами IMAP4.

Дополнительные сведения см. в статье Настройка параметров SMTP с проверкой подлинности для клиентов POP3 и IMAP4 в Exchange Server.

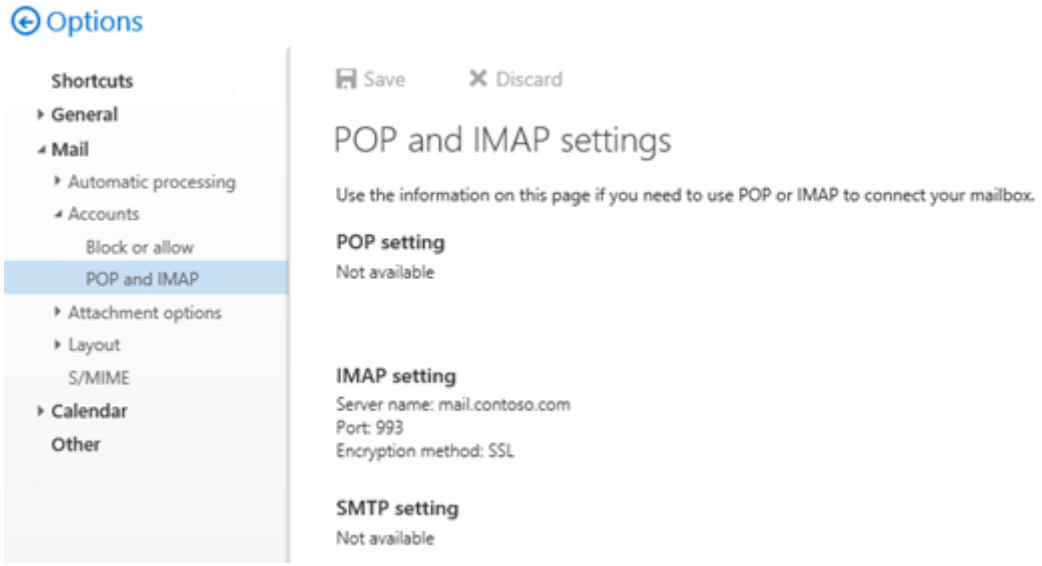
Как убедиться, что это сработало?

Чтобы убедиться, что вы включили и настроили IMAP4 на сервере Exchange Server, выполните следующие действия:

1. Откройте почтовый ящик в Outlook в Интернете и щелкните **Параметры**>.



2. > Щелкните**Почтовые учетные**> записи**POP и IMAP** и убедитесь, что отображаются правильные параметры IMAP4.



Примечание. Если вы настроили значения 993/SSL **и** 143/TLS для параметра *ExternalConnectionSettings* в **командлете Set-ImapSettings**, в Outlook в Интернете отображается только значение 993/SSL. Кроме того, если настроенные внешние параметры IMAP4 не отображаются должным образом в Outlook в Интернете после перезапуска служб IMAP4, выполните команды `net stop w3svc /y` и `net start w3svc` перезапустить службы IIS.

3. Вы можете проверить подключение клиента IMAP4 к серверу Exchange Server следующими способами:

   - **Внутренние клиенты**. Используйте командлет **Test-ImapConnectivity** . Например, `Test-ImapConnectivity -ClientAccessServer <ServerName> -Lightmode -MailboxCredential (Get-Credential)`. Дополнительные сведения см. в статье Test-ImapConnectivity.

   Примечание. *Переключатель Lightmode* сообщает, что команда тестирует вход IMAP4 на сервер. Чтобы проверить отправку (SMTP) и получение (IMAP4) сообщения, необходимо настроить параметры SMTP с проверкой подлинности, как описано в разделе Настройка параметров SMTP с проверкой подлинности для клиентов POP3 и IMAP4 в Exchange Server.

   - **Внешние клиенты**. Используйте тест **Imap Email** в анализаторе удаленного подключения Майкрософт .

   Примечание. IMAP4 нельзя использовать для подключения к почтовому ящику администратора. Это ограничение было намеренно включено в Exchange 2016 и Exchange 2019 для повышения безопасности почтового ящика администратора.

Дальнейшие действия

Сведения о включении или отключении доступа по протоколу IMAP4 к отдельным почтовым ящикам см. в статье Включение или отключение доступа по протоколу POP3 или IMAP4 к почтовым ящикам в Exchange Server.

Включение или отключение доступа по протоколу POP3 или IMAP4 к почтовым ящикам в Exchange Server

Статья • 04.04.2023

После включения и настройки POP3 или IMAP4 на сервере Exchange, как описано в разделах Включение и настройка POP3 на сервере Exchange Server и Включение и настройка IMAP4 на сервере Exchange, доступ ко всем почтовым ящикам пользователей (за исключением почтового ящика администратора) можно получить с помощью ПРОТОКОЛА POP3 или IMAP4. Вы можете использовать описанные в этой статье процедуры, чтобы отключить доступ по протоколам POP3 и IMAP4 к определенным почтовым ящикам.

Дополнительные сведения о POP3 и IMAP4 см. в разделе POP3 и IMAP4 в Exchange Server.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Чтобы открыть Центр администрирования Exchange, см. статью Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Процедуры, описанные в этой статье, не распространяются на почтовый ящик администратора, потому что к нему нельзя подключиться по протоколу POP3 или IMAP4. Это ограничение было намеренно включено в Exchange 2016 и Exchange 2019 для повышения безопасности почтового ящика администратора.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения подготовки получателей" раздела Разрешения получателей .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по **адресу Exchange Server**.

Включение или отключение доступа к одному почтовому ящику по протоколу POP3 или IMAP4

Включение или отключение доступа к почтовому ящику по протоколу POP3 или IMAP4 в Центре администрирования Exchange

1. В EAC перейдите в раздел **Почтовые ящики получателей**>.

2. В списке почтовых ящиков найдите нужный почтовый ящик. Для этого выполните одно из следующих действий:

   - Прокрутите список почтовых ящиков.

   - Щелкните **Поиск** (🔎 и введите часть имени пользователя, адреса электронной почты или псевдонима.

   - Щелкните **Дополнительные параметры** (•••) >**Расширенный поиск** для поиска почтового ящика.

   Найдя почтовый ящик, который нужно изменить, выберите его и нажмите кнопку **Изменить** (🖉

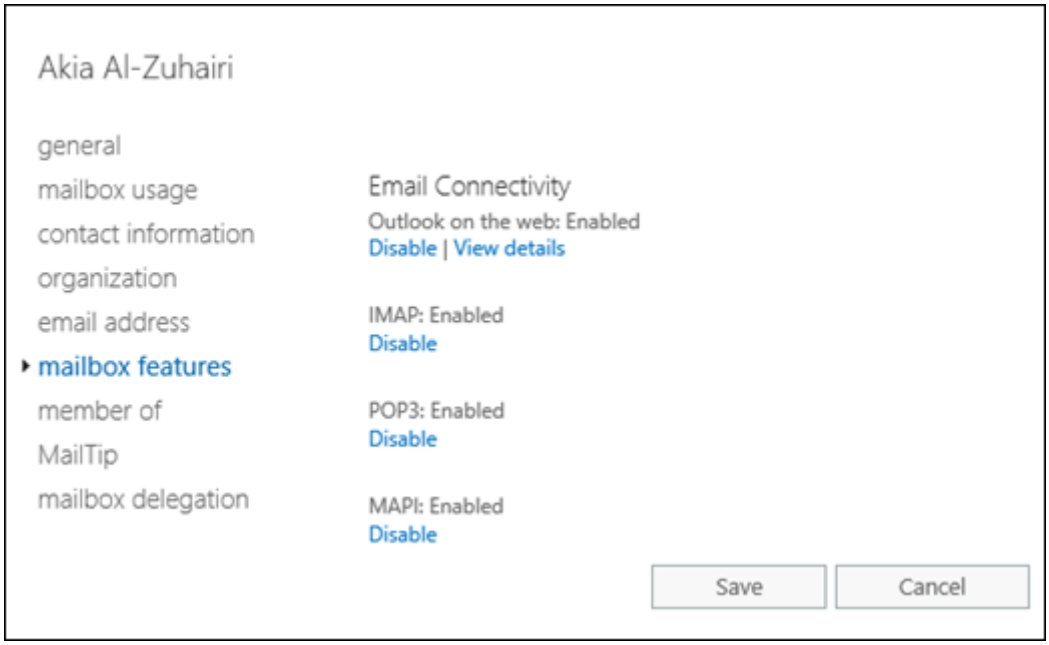
3. В открывшемся окне свойств почтового ящика выберите **Функции почтового ящика**.

   В разделе **Возможность подключения электронной почты** настройте один или несколько из этих параметров:

   - **POP3**. Чтобы отключить доступ по протоколу POP3 к почтовому ящику, нажмите кнопку **Отключить**, а затем нажмите кнопку **Да** в появившемся предупреждающем сообщении. Если протокол POP3 уже отключен, нажмите **Включить**, чтобы включить его.

   - **IMAP**. Чтобы отключить доступ по протоколу IMAP4 к почтовому ящику, нажмите кнопку **Отключить**, а затем нажмите кнопку **Да** в появившемся

предупреждающем сообщении. Если протокол IMAP4 уже отключен, нажмите **Включить**, чтобы включить его.



По завершении нажмите кнопку **Сохранить**.

Включение или отключение доступа к почтовому ящику по протоколу POP3 или IMAP4 с помощью командной консоли Exchange

Чтобы включить или отключить доступ по протоколу POP3 или IMAP4 к одному почтовому ящику, используйте следующий синтаксис:

PowerShell

```
Set-CasMailbox -Identity <MailboxIdentity> -PopEnabled <$true | $false> -
ImapEnabled <$true | $false>
```

В этом примере отключается доступ по протоколам POP3 и IMAP4 к почтовому ящику с именем Rand Zaher.

PowerShell

```
Set-CasMailbox -Identity "Rand Zaher" -PopEnabled $false -ImapEnabled $false
```

В этом примере предоставляется доступ по протоколам POP3 и IMAP4 к почтовому ящику с именем Rand Zaher.

PowerShell

```
Set-CasMailbox -Identity "Rand Zaher" -POPEnabled $true -ImapEnabled $true
```

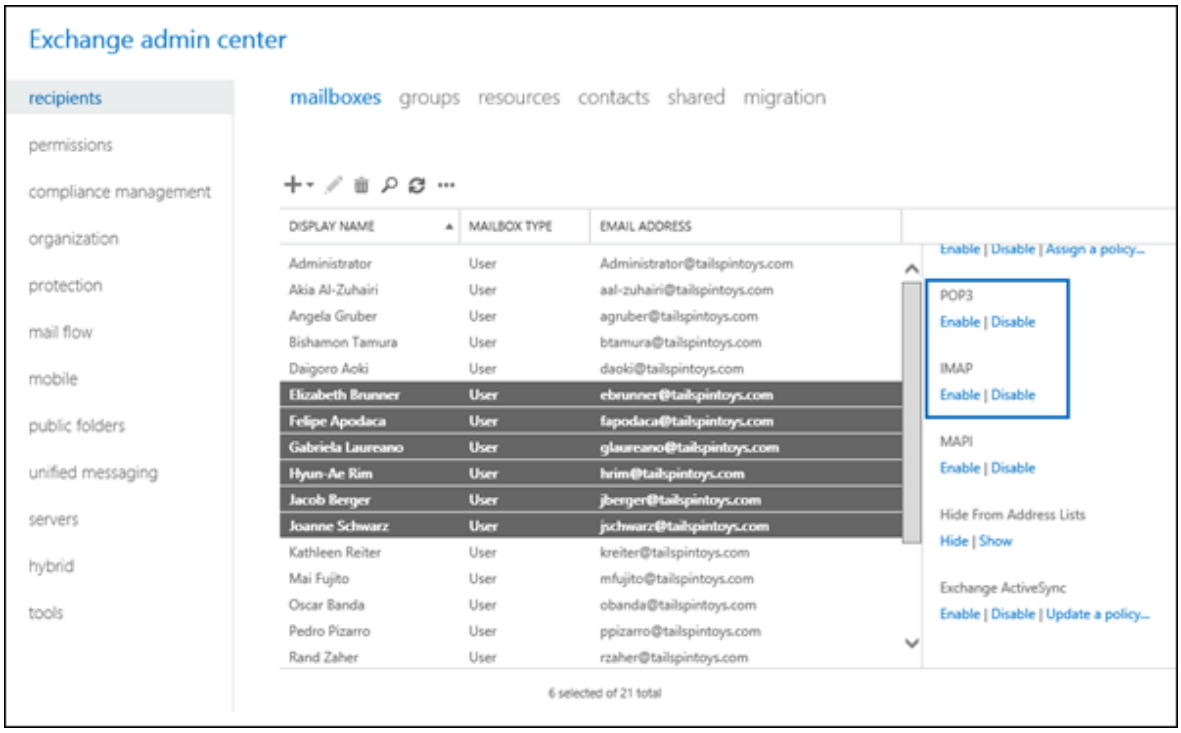
Дополнительные сведения см. в статье Set-CASMailbox.

Включение или отключение доступа к нескольким почтовым ящикам по протоколу POP3 или IMAP4

Включение или отключение доступа к нескольким почтовым ящикам по протоколу POP3 или IMAP4 в Центре администрирования Exchange

1. В EAC перейдите в раздел **Почтовые ящики получателей**>.
2. В списке почтовых ящиков найдите нужные почтовые ящики. Для этого выполните одно из следующих действий:
   - Прокрутите список почтовых ящиков.
   - Щелкните **Поиск** (🔎 и введите часть имени пользователя, адреса электронной почты или псевдонима.
   - Щелкните **Дополнительные параметры** (•••) >**Расширенный поиск** для поиска почтового ящика.
3. В списке почтовых ящиков выберите несколько почтовых ящиков одного типа (например, **Пользователь**). Например:
   - Выберите почтовый ящик. Удерживая клавишу SHIFT, выберите другой ящик, расположенный ниже в списке.
   - Выберите нужные почтовые ящики, удерживая клавишу CTRL.

   После выбора нескольких почтовых ящиков одного типа заголовок области сведений изменится на **Массовое изменение**.
4. В области сведений найдите **POP3** или **IMAP**, нажмите **Включить** или **Отключить**, а затем **OK** в появившемся предупреждении.



Включение или отключение доступа к нескольким почтовым ящикам по протоколу POP3 или IMAP4 с помощью командной консоли Exchange

Чтобы указать нужные почтовые ящики, можно использовать командлеты **Get-Mailbox**, **Get-User** и **Get-Content**. Например:

- Используйте параметр *OrganizationalUnit* для фильтрации почтовых ящиков по подразделениям.
- Используйте параметр *Filter* для создания фильтров OPATH, определяющих почтовые ящики. Дополнительные сведения см. в статье Filterable Properties for the -Filter Parameter.
- Используйте текстовый файл для указания почтовых ящиков. В каждой строке текстового файла указан один почтовый ящик (адрес электронной почты, имя или другой уникальный идентификатор), например:

> ebrunner@tailspintoys.com
> fapodaca@tailspintoys.com
> glaureano@tailspintoys.com
> hrim@tailspintoys.com

В этом примере отключается доступ по протоколам POP3 и IMAP4 для всех почтовых ящиков финансового подразделения в Северной Америке.

PowerShell

```
$NAFinance = Get-Mailbox -OrganizationalUnit "OU=Marketing,OU=North America,DC=contoso,DC=com" -Filter "RecipientTypeDetails -eq 'UserMailbox'" -ResultSize Unlimited; $NAFinance | foreach {Set-CasMailbox $_.Identity -PopEnabled $false -ImapEnabled $false}
```

В этом примере отключается доступ по протоколам POP3 и IMAP4 для всех почтовых ящиков отдела проектирования в штате Вашингтон.

PowerShell

```
Get-User -Filter "RecipientType -eq 'UserMailbox' -and Department -like 'Engineering*' -and StateOrProvince -eq 'WA'" | Set-CasMailbox -PopEnabled $false -ImapEnabled $false
```

В этом примере для отключения доступа к указанным почтовым ящикам по протоколу POP3 или IMAP4 используется текстовый файл C:\My Documents\Accounts.txt.

PowerShell

```
Get-Content "C:\My Documents\Accounts.txt" | foreach {Set-CASMailbox $_ -PopEnabled $false -ImapEnabled $false}
```

Дополнительные сведения см. в статьях Get-Mailbox и Get-User.

Повторный запуск служб POP3 и IMAP4

После изменения параметров доступа к почтовому ящику по протоколам POP3 и IMAP4 нужно перезагрузить службы POP3 и IMAP4 на сервере. Для этого можно воспользоваться консолью "Службы" Windows или командной консолью Exchange.

Перезапуск служб POP3 и IMAP4 с помощью консоли "Службы" Windows

1. Откройте консоль "Службы Windows" на сервере Exchange Server. Например:

   - Выполните команду `services.msc` из диалогового окна **Запуск** , окна командной строки или командной консоли Exchange.
   - Откройте диспетчер сервера и щелкните **Сервис**>**службы**.

2. В списке служб выполните одно или оба следующих действия:

   - **POP3**:

     a. Выберите **Microsoft Exchange POP3** и нажмите кнопку**Перезапуститьдействие**>.

     b. Выберите **Серверная часть Microsoft Exchange POP3** и нажмите кнопку**Перезапуститьдействие**>.

   - **IMAP4**:

     a. Выберите **Microsoft Exchange IMAP4** и нажмите кнопку**Перезапуститьдействие**>.

     b. Выберите **Серверная часть IMAP4 Microsoft Exchange** и нажмите кнопку**Перезапуститьдействие**>.

Перезапуск служб POP3 и IMAP4 с помощью командной консоли Exchange

Чтобы перезапустить службы POP3, выполните следующую команду:

```
PowerShell

Restart-Service MSExchangePOP3; Restart-Service MSExchangePOP3BE
```

Чтобы перезапустить службы IMAP4, выполните следующую команду:

```
PowerShell

Restart-Service MSExchangeIMAP4; Restart-Service MSExchangeIMAP4BE
```

Дополнительные сведения об этом командлете см. в статье Restart-Service.

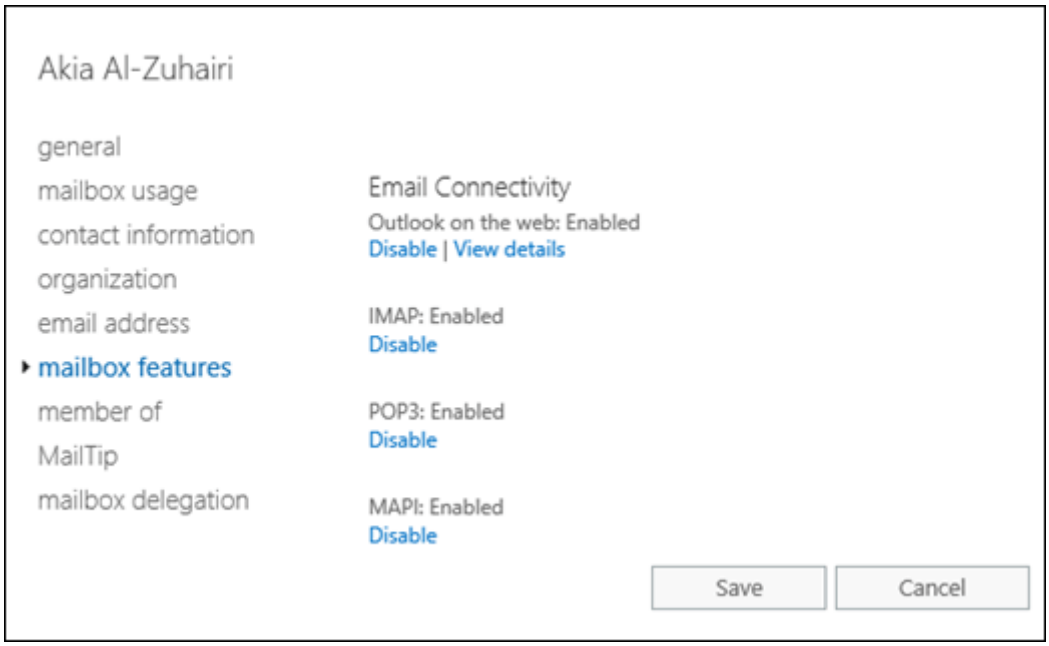
Чтобы убедиться, что службы POP3 или IMAP4 успешно перезапущены, выполните следующую команду:

```
PowerShell

Get-Service MSExchangePOP3; Get-Service MSExchangePOP3BE; Get-Service
MSExchangeIMAP4; Get-Service MSExchangeIMAP4BE
```

Как проверить, что все получилось?

Чтобы убедиться, что доступ к почтовому ящику по протоколу POP3 или IMAP4 включен или отключен, выполните одно из следующих действий:

- В EAC перейдите в раздел Почтовые**ящики**>**получателей**>, выберите почтовый ящик > щелкните > Функции >**почтового ящикаEmail подключения**.
    - Если для почтового ящика включен доступ по протоколу POP3, вы увидите сообщение **POP3: включено** и ссылку **Отключить**. Если доступ по протоколу POP3 отключен, вы увидите сообщение **POP3: отключено** и ссылку **Включить**.
    - Если для почтового ящика включен доступ по протоколу IMAP4, вы увидите сообщение **IMAP4: включено** и ссылку **Отключить**. Если доступ по протоколу IMAP4 отключен, вы увидите сообщение **IMAP4: отключено** и ссылку **Включить**.



- В командной консоли Exchange *замените*< *MailboxIdentity*> удостоверением почтового ящика (например, именем, псевдонимом или адресом электронной почты) и выполните следующую команду:

```
PowerShell

Get-CasMailbox - Identity <MailboxIdentity>
```

- Используйте тот же фильтр, что и для определения почтовых ящиков, но вместо командлета **Get-CasMailbox** используйте **Set-CasMailbox**. Например:

PowerShell

```
Get-User -Filter "RecipientType -eq 'UserMailbox' -and Department -like
'Engineering*' -and StateOrProvince -eq 'WA'" | Get-CasMailbox
```

- Чтобы увидеть все почтовые ящики, для которых отключен доступ по протоколам POP3 и IMAP4, выполните такую команду в командной консоли Exchange:

PowerShell

```
Get-CasMailbox -ResultSize unlimited -Filter "PopEnabled -eq `$false -
and ImapEnabled -eq `$false"
```

Настройка параметров SMTP с проверкой подлинности для клиентов POP3 и IMAP4 в Exchange Server

Статья • 04.04.2023

После включения и настройки POP3 или IMAP4 на сервере Exchange, как описано в разделах Включение и настройка POP3 на сервере Exchange Server и Включение и настройка IMAP4 на сервере Exchange Server, необходимо настроить параметры SMTP с проверкой подлинности для клиентов POP3 и IMAP4, чтобы они могли отправлять сообщения электронной почты.

Соединитель получения по умолчанию с именем "*Имя> интерфейсного< сервера* клиента" в службах клиентского доступа на сервере почтовых ящиков прослушивает отправку проверенных smtp-клиентов через порт 587. По умолчанию этот соединитель использует следующие параметры для **внутренних и внешних** SMTP-подключений клиентов (с проверкой подлинности):

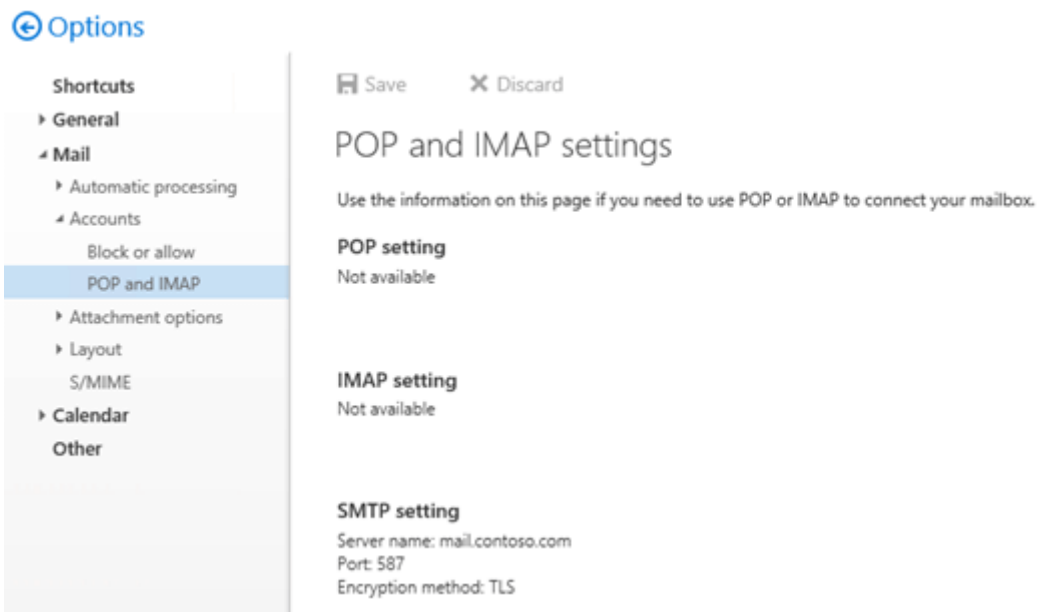
- **SMTP-сервер**: `<ServerFQDN>`. Например, `mailbox01.contoso.com`.
- **TCP-порт**: 587
- **Метод шифрования**: TLS. Обратите внимание, что это оппортунистический ПРОТОКОЛ TLS (**STARTTLS**), который приводит к зашифрованное подключение после подтверждения первоначального обычного текстового протокола.

Дополнительные сведения см. в разделах Соединители приема по умолчанию, созданные во время установки и Архитектура протокола клиентского доступа.

Чтобы настроить параметры протокола SMTP с проверкой подлинности, используемые клиентами POP3 и IMAP4, выполните указанные ниже действия.

1. Настройте полное доменное имя в соединителе получения "*Имя> внешнего< сервера* клиента".
2. Укажите сертификат, используемый для шифрования клиентских SMTP-подключений с проверкой подлинности.
3. Настройте Outlook в Интернете (прежнее название — Outlook Web App) для отображения параметров SMTP для клиентов SMTP, **прошедших проверку**

подлинности>, в разделе Параметры**Параметры**>**Учетные записи почты**>>**POP и IMAP**.



Дополнительные сведения о POP3 и IMAP4 см. в разделе POP3 и IMAP4 в Exchange Server.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Теперь для шифрования данных, которыми обмениваются компьютерные системы, используется протокол TLS вместо протокола SSL. Они настолько тесно связаны, что термины "SSL" и "TLS" (без версий) часто используются взаимозаменяемо. Из-за этого сходства ссылки на "SSL" в разделах Exchange, Центре администрирования Exchange и командной консоли Exchange часто используются для охвата протоколов SSL и TLS. Как правило, термин "SSL" обозначает именно протокол SSL только в тех случаях, когда указан номер версии (например, SSL 3.0). Чтобы узнать, почему следует отключить протокол SSL и переключиться на TLS, см. статью Защита от уязвимости SSL 3.0.
- Если у вас есть клиенты POP3 или IMAP4, которые могут отправлять почту SMTP только через порт 25, можно настроить порт 25 в соединителе получения "*Имя*> *внешнего*< *сервера* клиента", чтобы разрешить клиентам отправлять почту SMTP с проверкой подлинности. Тем не менее, так как порт 25 также настроен на соединителе "*Имя*> *внешнего*< сервера клиента" для получения электронной почты от внешних SMTP-серверов, вам потребуется изменить локальные IP-адреса, которые используются для прослушивания

порта 25 на одном или обоих соединителях. Дополнительные сведения см. в разделе Привязки локальных адресов для соединителей получения.

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Получение соединителей" в разделе Разрешения потока обработки почты .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Этап 1. Настройка полного доменного имени в соединителе получения "Клиентский интерфейсный сервер <имя сервера>".

Вы можете пропустить этот этап, если нужно оставить полное доменное имя сервера по умолчанию (например, mailbox01.contoso.com). Вы также можете указать полное доменное имя, лучше соответствующее вашему соглашению об именовании для Интернета или нужному сертификату TLS.

Если вы изменили полное доменное имя и хотите, чтобы клиенты POP3 или IMAP4 использовали этот соединитель для отправки электронной почты, то новому FQDN должна соответствовать запись на внутреннем DNS-сервере.

Независимо от полного доменного имени, если вы хотите, чтобы внешние клиенты POP3 или IMAP4 использовали этот соединитель для отправки электронной почты, то полному доменному имени должна соответствовать запись на общедоступном DNS-сервере, а TCP-порт (587) должен быть разрешен в брандмауэре на сервере Exchange Server.

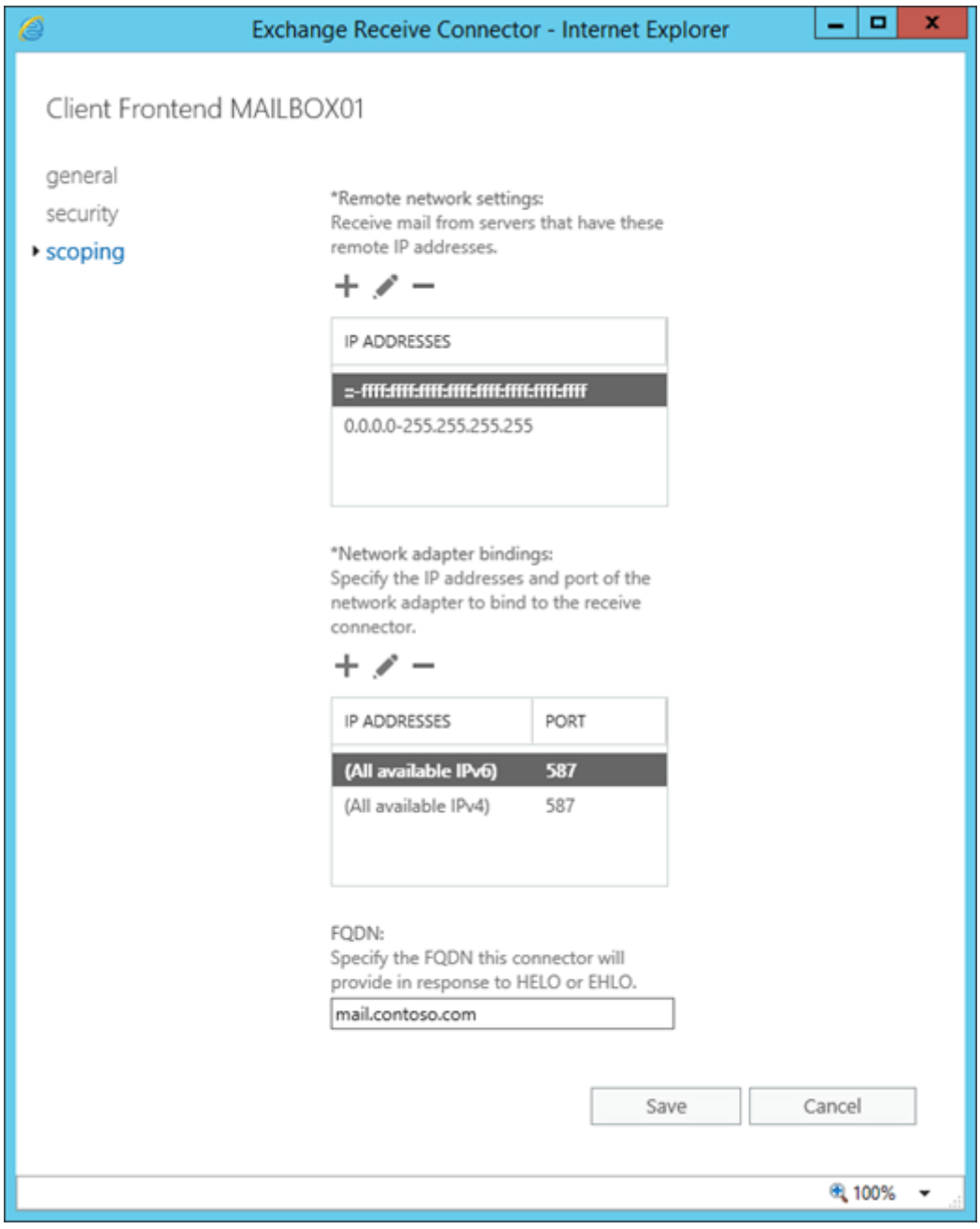
Настройка полного доменного имени для клиентов SMTP, прошедших проверку подлинности, с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел**Соединители получения** потока >**обработки почты**.

2. В списке соединителей получения выберите **Имя> клиентского интерфейсного <сервера** и нажмите кнопку **Изменить** (.

3. На открывшейся странице **Соединитель получения Exchange** нажмите **Определение области**.

4. В поле **Полное доменное имя** введите полное доменное имя SMTP-сервера, которое требуется использовать для клиентских SMTP-подключений с проверкой подлинности (например, mail.contoso.com), а затем нажмите кнопку **Сохранить**.



Настройка полного доменного имени для клиентов SMTP, прошедших проверку подлинности, с помощью командной консоли Exchange

Чтобы настроить полное доменное имя для клиентов SMTP, прошедших проверку подлинности, используйте следующий синтаксис:

```
PowerShell

Get-ReceiveConnector -Identity "Client Frontend*" | Set-ReceiveConnector -
Fqdn <FQDN>
```

В этом примере настраивается полное доменное имя mail.contoso.com.

```
PowerShell

Get-ReceiveConnector -Identity "Client Frontend*" | Set-ReceiveConnector -
Fqdn mail.contoso.com
```

Как убедиться, что все получилось?

Чтобы убедиться, что вы успешно получили полное доменное имя в соединителе "*Имя> внешнего<* сервера клиента" для получения, выполните одно из следующих действий:

- EAC, перейдите в раздел**Соединители получения** потока >**обработки почты**>, выберите **Имя> клиентского интерфейсного <сервера**, щелкните **Изменить** (>**Определение области** и проверка значения в поле **FQDN**.
- В командной консоли Exchange выполните следующую команду:

  ```
  PowerShell

  Get-ReceiveConnector -Identity "Client Frontend*" | Format-List
  Name,Fqdn
  ```

Этап 2. Указание сертификата, используемого для шифрования клиентских SMTP-подключений с проверкой подлинности, с помощью командной консоли Exchange

Сертификат должен соответствовать или содержать полное доменное имя, указанное на предыдущем шаге, а клиенты POP3 и SMTP должны доверять

сертификату, что, скорее всего, означает сертификат от коммерческого центра сертификации. Дополнительные сведения см. в статье Требования к сертификатам для служб Exchange.

Кроме того, необходимо назначить сертификат службе SMTP Exchange. Дополнительные сведения см. в статье Назначение сертификатов Exchange Server службам.

Чтобы указать сертификат, используемый для клиентских SMTP-подключений с проверкой подлинности, используйте следующий синтаксис:

PowerShell

```
$TLSCert = Get-ExchangeCertificate -Thumbprint <ThumbprintValue>
```

PowerShell

```
$TLSCertName = "<I>$($TLSCert.Issuer)<S>$($TLSCert.Subject)"
```

PowerShell

```
Get-ReceiveConnector -Identity "Client Frontend*" | Set-ReceiveConnector -
TlsCertificateName $TLSCertName
```

В этом примере используется сертификат со значением отпечатка 434AC224C8459924B26521298CE8834C514856AB.

PowerShell

```
$TLSCert = Get-ExchangeCertificate -Thumbprint
434AC224C8459924B26521298CE8834C514856AB
```

PowerShell

```
$TLSCertName = "<I>$($TLSCert.Issuer)<S>$($TLSCert.Subject)"
```

PowerShell

```
Get-ReceiveConnector -Identity "Client Frontend*" | Set-ReceiveConnector -
TlsCertificateName $TLSCertName
```

Как проверить, что шаг выполнен?

Чтобы убедиться, что вы указали сертификат, используемый для шифрования клиентских SMTP-подключений с проверкой подлинности, выполните указанные ниже действия.

1. Выполните следующую команду в Командная консоль Exchange:

```
PowerShell

Get-ReceiveConnector -Identity "Client Frontend*" | Format-List
Name,Fqdn,TlsCertificateName
```

2. Выполните следующую команду в Командная консоль Exchange:

```
PowerShell

Get-ExchangeCertificate | Format-List
Thumbprint,Issuer,Subject,CertificateDomains,Services
```

3. Убедитесь, что поле **Subject** или **CertificateDomains** сертификата, указанное в соединителе получения, содержит значение **Fqdn** соединителя получения. При этом совпадение может быть полным или частичным (с применением подстановочных знаков).

Этап 3. Настройка Outlook в Интернете на отображение параметров SMTP для клиентов SMTP, прошедших проверку подлинности, с помощью командной консоли Exchange

Чтобы настроить Outlook в Интернете на отображение параметров SMTP для клиентов SMTP, прошедших проверку подлинности, выполните следующую команду:

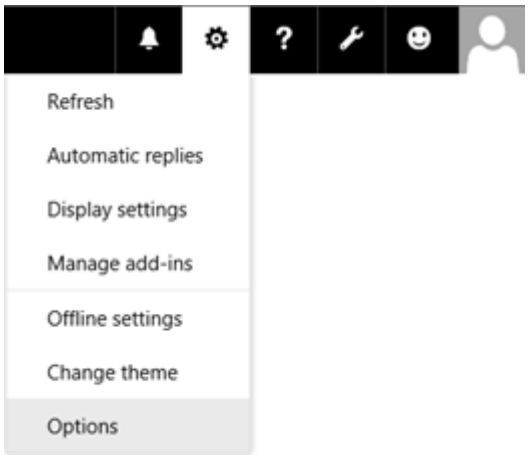
```
PowerShell

Get-ReceiveConnector -Identity "Client Frontend*" | Set-ReceiveConnector -
AdvertiseClientSettings $true
```

Примечание. Чтобы запретить отображение параметров SMTP в Outlook в Интернете, измените значение с `$true` на `$false`.

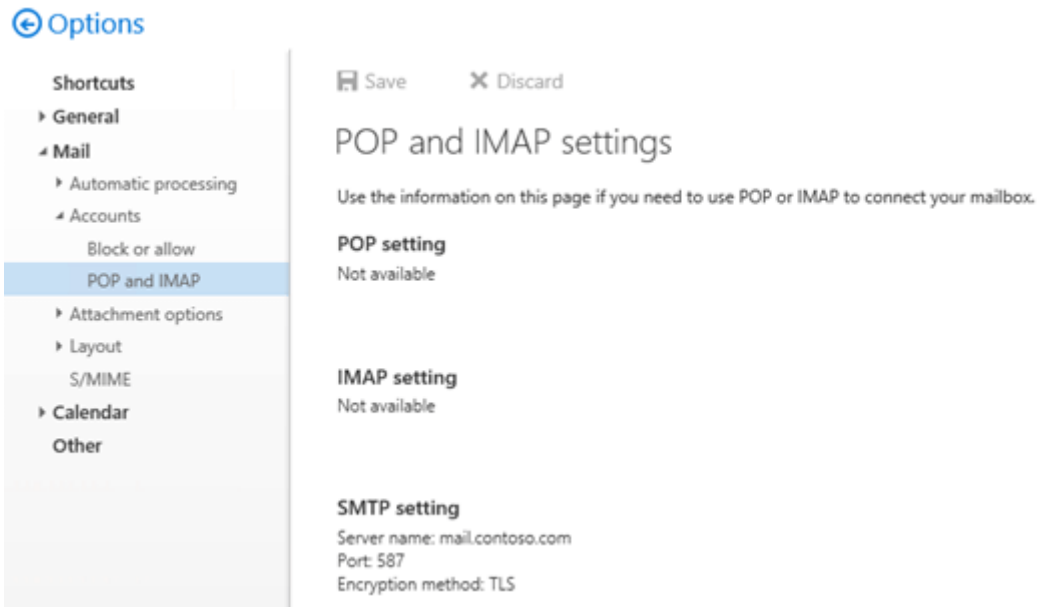
Как убедиться, что все получилось?

Чтобы убедиться, что вы настроили Outlook в Интернете на отображение параметров SMTP для клиентов SMTP, прошедших проверку подлинности, выполните следующие действия:

1. Откройте почтовый ящик в Outlook в Интернете и щелкните **Параметры**>.



2. Щелкните **Почтовые**>**учетные**> записи**POP и IMAP** и убедитесь, что отображаются правильные параметры SMTP.



Примечание. Если настроенные параметры SMTP не отображаются должным образом в Outlook в Интернете, выполните команды `net stop w3svc /y` и `net start w3svc` перезапустите службы IIS.

Как убедиться, что это сработало?

Чтобы убедиться, что вы настроили параметры протокола SMTP с проверкой подлинности на сервере Exchange Server, выполните одну или несколько из

приведенных ниже процедур.

- Используйте командлеты **Test-PopConnectivity** и **Test-ImapConnectivity**, которые отправляют тестовые сообщения по протоколу SMTP с проверкой подлинности. Дополнительные сведения см. в статьях Test-PopConnectivity и Test-ImapConnectivity.

- Включите ведение журнала протокола в соединителе получения "*Имя> внешнего<* сервера клиента", настройте клиент POP3 или IMAP4 для подключения к почтовому ящику, отправьте тестовое сообщение из внутреннего сетевого подключения и (или) внешнего подключения к Интернету и просмотрите результаты в журнале протокола. Дополнительные сведения см. в разделе Ведение журнала протокола.

  Примечание. Вы не можете использовать POP3 или IMAP4 для подключения к почтовому ящику администратора. Это ограничение было намеренно включено в Exchange 2016 и Exchange 2019 для повышения безопасности почтового ящика администратора.

Outlook для iOS и Android

Статья • 04.04.2023

Outlook для iOS и Android поддерживает два типа проверки подлинности в локальных средах Exchange: *обычную проверку подлинности* и *гибридную современную проверку подлинности*.

Outlook для iOS и Android использует обычную проверку подлинности с Exchange ActiveSync в следующих средах:

- В средах Exchange Server 2010 г.
- Если гибридная связь с Microsoft 365 или Office 365 не настроена
- Если гибридная современная проверка подлинности не включена

Дополнительные сведения см. в статье Использование обычной проверки подлинности в Outlook для iOS и Android.

Для клиентов, работающих Exchange Server 2013, Exchange Server 2016 или Exchange Server 2019 в гибридном отношении с Microsoft 365 или Office 365, Outlook для iOS и Android можно настроить на использование гибридной современной проверки подлинности. Дополнительные сведения см. в статье Использование гибридной современной проверки подлинности с Outlook для iOS и Android.

> **Примечание**
>
> Справку по использованию приложения на отдельных устройствах и информацию об устранении неполадок можно найти в Центре справки по Outlook для iOS и Android.

Различия при управлении устройствами на локальных серверах Exchange с поддержкой гибридной современной проверки подлинности (HMA)

Исторически для других реализаций EAS каждый смартфон, пытающийся подключиться к одному и тому же почтовому ящику OnPrem, подготавливается

уникальный идентификатор устройства, а abq (разрешить, блокировать, карантин) или любой MDM может управлять этими идентификаторами устройств, например для собственных приложений EAS.

Однако при подключении к локальному клиенту с поддержкой HMA с помощью Outlook Mobile существуют некоторые различия в проектировании, так как данные пользователя хранятся в центральном кэше внутри клиента Exchange Online. Чтобы понять философию проектирования и ее преимущества, см. раздел Использование гибридной современной проверки подлинности в Outlook для iOS и Android. Эта возможность также позволяет администраторам клиентов безопасно выполнять удаленную очистку данных в случаях, когда пользователь покидает компанию или скомпрометировано устройство. Ниже описаны некоторые различия.

- **Пользователи подключаются к кэшу, созданному в клиенте Exchange Online**. Когда пользователь подключается к локальному клиенту с поддержкой гибридной современной проверки подлинности с помощью приложения Outlook Mobile, во внутреннем сервере Exchange создает синхронизированный кэш пользователей с данными в течение 4 недель в защищенном пользователем почтовом ящике. Это означает, что если несколько устройств подключаются, они будут обращаться к одной конечной точке внутри Exchange. На стороне локальной среды виден уникальный идентификатор устройства. Синхронизированный кэш также называется учетной записью облачного кэша.

- **Облачный кэш может создать несколько устройств**. Локальный администратор может увидеть несколько устройств из-за начальной загрузки облачного кэша и из-за того, что срок действия устройств с истекшим сроком действия не истек. Когда Exchange впервые проверит учетную запись облачного кэша, он будет использовать универсальный идентификатор устройства. После проверки учетной записи используется новый персонализированный идентификатор устройства с именем подписка.

- **Блокировка или выдача удаленной очистки**. Если локальный администратор хочет удалить доступ к содержимому, он должен выполнить удаленную очистку в локальной среде. Облачный кэш будет выполнять удаленную очистку для всех подключенных устройств. Если локальный администратор хочет заблокировать доступ к содержимому, он должен сделать это через локальную среду. В этом случае облачный кэш не сможет синхронизировать новое содержимое. Дополнительные сведения об удаленной очистке см. в разделе Выполнение удаленной очистки на мобильном телефоне.

Рекомендации по использованию MDM

- Для управления приложением Outlook Mobile рекомендуется использовать mdm, такие как Intune, связанные с функцией условного доступа. См. раздел Управление Outlook для iOS и Android в Exchange Online

- управление Intune работает для учетных записей, подключенных с помощью гибридной современной проверки подлинности к локальным серверам. Действительно, это одно из его ценностных предложений. Все устройства, подключенные к одному облачному кэшу, имеют один и тот же идентификатор на локальном сервере, так как они используют одно и то же физическое хранилище в microsoft 365 среднего уровня. управление Intune не работает для учетных записей, подключающихся через обычную проверку подлинности к локальной среде, так как локальный администратор не имеет видимости соответствующих удостоверений Microsoft 365.

- Один локальный пользователь может иметь одно удостоверение Microsoft 365. У него может быть больше 1. Это связано с тем, что удостоверение Microsoft 365 *вычисляется* из имени входа, предоставленного пользователем клиента. Это может быть tim@contoso.com. Это может быть contoso.com/tim. Каждый из них можно использовать для управления входом на локальный сервер, но в Microsoft 365 невозможно обнаружить, что эти два разных имени представляют одного локального пользователя. Таким образом, каждый из них будет иметь разные удостоверения Microsoft 365, другой облачный кэш Microsoft 365 и предоставить другой идентификатор устройства для локального сервера EAS.

Гибридная современная проверка подлинности в случае Outlook для iOS и Android

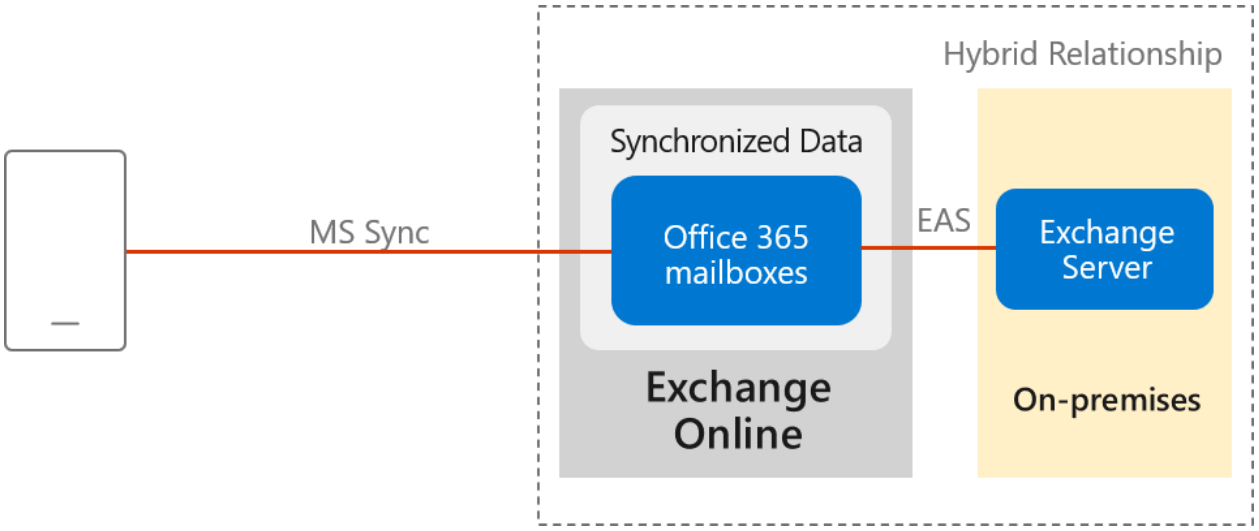
Статья • 27.10.2023

Приложение Outlook для iOS и Android разработано как лучший способ взаимодействия с Microsoft 365 или Office 365 на мобильном устройстве с помощью служб Майкрософт для поиска, планирования и определения приоритетов в повседневной жизни и работе. Outlook обеспечивает безопасность, конфиденциальность и поддержку, необходимые при защите корпоративных данных с помощью таких возможностей, как Microsoft Entra условный доступ и политики защиты приложений Intune. В следующих разделах представлен обзор гибридной архитектуры современной проверки подлинности, необходимых компонентов для ее развертывания и способов безопасного развертывания Outlook для iOS и Android для локальных почтовых ящиков Exchange.

Архитектура Microsoft Cloud для пользователей гибридной среды Exchange Server

Приложение Outlook для iOS и Android работает при поддержке облака. Эта характеристика указывает на то, что интерфейс состоит из локально установленного приложения на базе безопасной и масштабируемой службы, работающей в Microsoft Cloud.

Для почтовых ящиков Exchange Server архитектура Outlook для iOS и Android встроена непосредственно в Microsoft Cloud, предоставляя клиентам дополнительные преимущества, такие как безопасность, конфиденциальность, встроенное соответствие требованиям и прозрачные операции, которые Корпорация Майкрософт фиксирует в Центре управления безопасностью Майкрософт и Центре управления безопасностью Azure.



В архитектуре на основе Microsoft 365 или Office 365 Outlook для iOS и Android использует собственную технологию синхронизации майкрософт для синхронизации данных, которая защищена сквозным подключением, защищенным TLS, между Microsoft 365 или Office 365 и приложением.

Подключение Exchange ActiveSync (EAS) между Exchange Online и локальной средой обеспечивает синхронизацию локальных данных пользователей и включает четыре недели электронной почты, все данные календаря, все контактные данные и состояние вне офиса в клиенте Exchange Online. Эти данные автоматически удаляются из Exchange Online через 30 дней после удаления учетной записи в Microsoft Entra ID.

Синхронизация данных между локальной средой и Exchange Online происходит независимо от действий пользователя. Эта зависимость гарантирует, что мы можем быстро отправлять новые сообщения на устройства.

Обработка информации в Microsoft Cloud обеспечивает поддержку расширенных функций и возможностей, таких как категоризация электронных сообщений для сортировки почты, персонализированный интерфейс для путешествий и календаря, а также повышенную скорость поиска. Использование облака для интенсивной обработки и минимальное использование ресурсов пользовательских устройств повышают производительность и стабильность приложения. Наконец, он позволяет Outlook создавать функции, которые работают во всех учетных записях электронной почты, независимо от технологических возможностей базовых серверов (таких как различные версии Exchange Server, Microsoft 365 или Office 365).

В частности, эта новая архитектура включает следующие улучшения:

1. **поддержка Enterprise Mobility + Security**. Клиенты могут воспользоваться преимуществами Microsoft Enterprise Mobility + Security (EMS), включая

Microsoft Intune и Microsoft Entra ID P1 или P2, чтобы включить условное доступ и Intune политики защиты приложений, которые контролируют и защищают корпоративные данные обмена сообщениями на мобильном устройстве.

2. **Полностью на базе Microsoft Cloud**. Данные локального почтового ящика синхронизируются в Exchange Online, что обеспечивает преимущества безопасности, конфиденциальности, соответствия требованиям и прозрачных операций, которые корпорация Майкрософт фиксирует в Центре управления безопасностью Майкрософт.

3. **OAuth защищает пароли пользователей**. Outlook использует гибридную современную проверку подлинности (OAuth) для защиты учетных данных пользователей. Гибридная современная проверка подлинности предоставляет Outlook безопасный механизм доступа к данным Exchange, не касаясь или не сохраняя учетные данные пользователя. При входе пользователь проходит проверку подлинности непосредственно на платформе удостоверений (Microsoft Entra ID или локальном поставщике удостоверений, например ADFS) и получает маркер доступа, который предоставляет Outlook доступ к почтовому ящику или файлам пользователя. Служба не имеет доступа к паролю пользователя в любой момент времени.

4. **Уникальные идентификаторы устройств.** Каждое подключение Outlook однозначно регистрируется в Microsoft Intune, поэтому им можно управлять как уникальным подключением.

5. **Открывает новые функции в iOS и Android**. Это обновление позволяет приложению Outlook воспользоваться преимуществами собственных функций Microsoft 365 или Office 365, которые сейчас не поддерживаются в локальной среде Exchange, например использовать полный поиск Exchange Online и папку "Входящие". Эти функции доступны только при использовании Outlook для iOS и Android.

> **Примечание**
>
> Управление устройствами через локальный центр администрирования Exchange (EAC) невозможно. Для управления мобильными устройствами требуется Intune.

Средства управления безопасностью и аудитом данных, а также доступом к ним

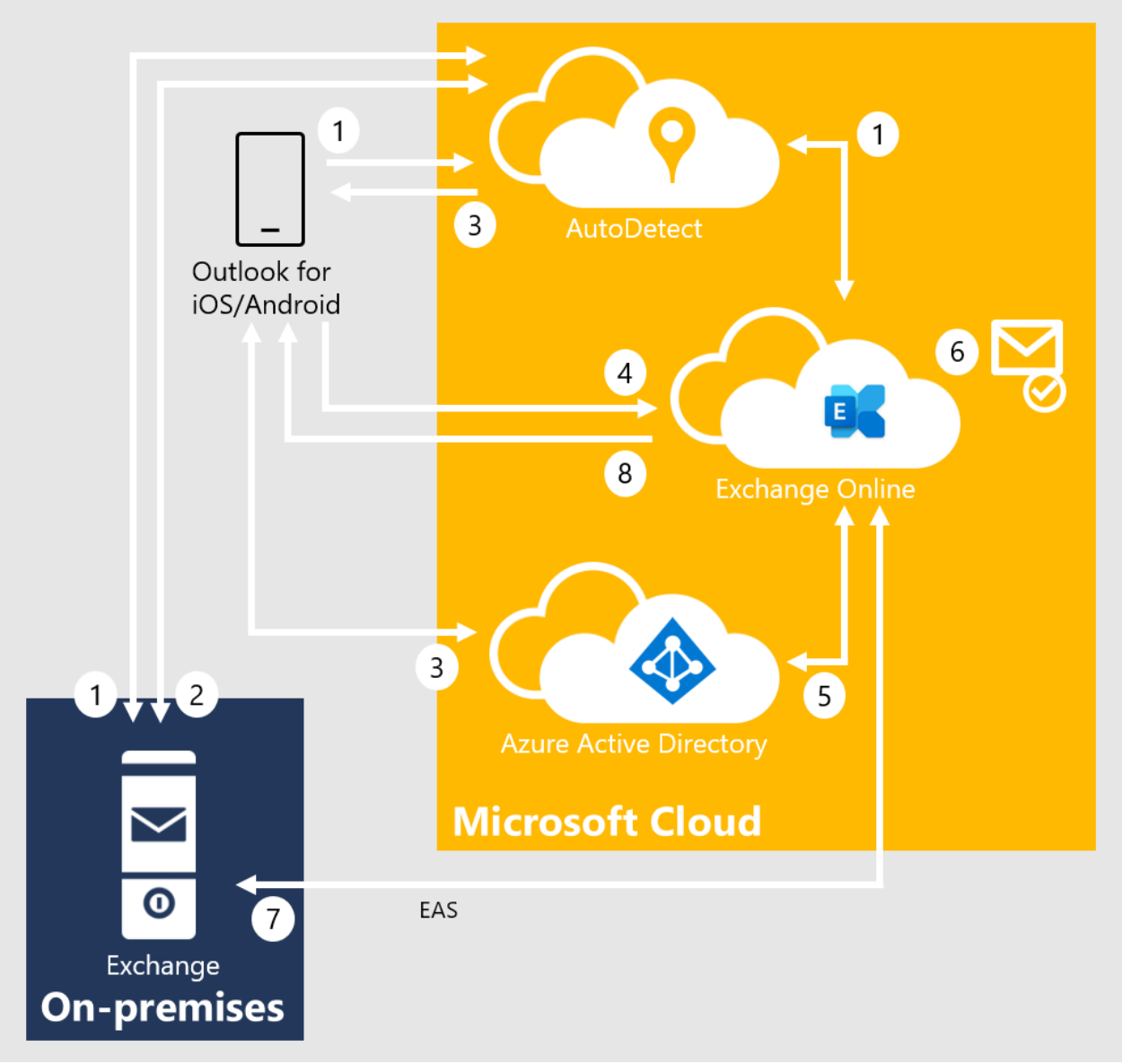
Локальные данные синхронизируются с Exchange Online, и у пользователей возникают вопросы о том, как эти данные защищаются в Exchange Online. Шифрование в Microsoft Cloud описывает использование BitLocker для шифрования на уровне тома. Шифрование службы с помощью ключа клиента Microsoft Purview поддерживается в архитектуре Outlook для iOS и Android, но обратите внимание, что пользователю должна быть лицензия Office 365 корпоративный E5 (или соответствующие версии этих планов для государственных организаций или образования), чтобы назначить политику шифрования с помощью командлета set-mailuser.

По умолчанию у инженеров Майкрософт нет постоянных административных привилегий и нулевой постоянный доступ к содержимому клиентов в Microsoft 365 или Office 365. Элементы управления административным доступом обсуждают проверку персонала, проверку фона, блокировку и блокировку клиента и многое другое.

Документация iso Audited Controls on Service Assurance содержит состояние проверенных элементов управления на основе глобальных стандартов и правил информационной безопасности, реализованных Microsoft 365 и Office 365.

Поток подключения

Когда в случае Outlook для iOS и Android используется гибридная современная проверка подлинности, применяется описанный ниже поток подключения.



1. Когда пользователь вводит свой электронный адрес, Outlook для iOS и Android подключается к службе AutoDetect. AutoDetect определяет тип почтового ящика путем запуска запроса автообнаружения для Exchange Online. Exchange Online определяет, что почтовый ящик пользователя является локальным, и возвращает отклик 302-redirect службе AutoDetect с URL-адресом локальной службы автообнаружения. AutoDetect запускает запрос к локальной службе автообнаружения, чтобы определить конечную точку ActiveSync для адреса электронной почты. URL-адрес, попробованный локально, аналогичен следующему примеру:
   `<https://autodiscover.contoso.com/autodiscover/autodiscover.json?Email=test%40contoso.com&Protocol=activesync&RedirectCount=3>`.

2. AutoDetect запускает подключение к локальному URL-адресу ActiveSync, возвращенному на шаге 1 выше, с пустым вызовом носителя. Запрос с пустым значением bearer сообщает локальной службе ActiveSync о том, что клиент поддерживает современную проверку подлинности. В ответ локальная служба ActiveSync отправляет отклик 401-challenge и включает заголовок

WWW-Authenticate: Bearer. В заголовке WWW-Authenticate: Bearer находится значение authorization_uri, определяющее конечную точку Microsoft Entra, которая должна использоваться для получения маркера OAuth.

3. AutoDetect возвращает клиенту конечную точку Microsoft Entra. Клиент начинает поток входа, и пользователю предоставляется веб-форма (или перенаправляется в приложение Microsoft Authenticator) и он может ввести учетные данные. В зависимости от конфигурации удостоверения этот процесс может включать или не включать перенаправление федеративной конечной точки к локальному поставщику удостоверений. В конечном итоге клиент получает пару маркеров (доступа и обновления) под названием AT1/RT1. Областью действия маркера доступа является клиент Outlook для iOS и Android, а аудиторией — конечная точка Exchange Online.

4. Outlook для iOS и Android устанавливает подключение к Exchange Online и выдает запрос на подготовку, включающий маркер доступа пользователя (AT1) и локальную конечную точку ActiveSync.

5. API подготовки MRS в Exchange Online использует AT1 в качестве входных данных и получает вторую пару маркеров доступа и обновления (с именем AT2/RT2) для доступа к локальному почтовому ящику через вызов on-behalf-of в Active Directory. Областью действия второго маркера доступа является клиент Exchange Online, а аудиторией — конечная точка локального пространства имен ActiveSync.

6. Если почтовый ящик не подготовлен, API подготовки создает почтовый ящик.

7. API подготовки MRS устанавливает надежное соединение с локальной конечной точкой ActiveSync и синхронизирует данные о сообщениях пользователя, используя маркер доступа AT2 в качестве механизма проверки подлинности. RT2 периодически используется для создания нового маркера AT2, чтобы данные можно было синхронизировать в фоновом режиме без участия пользователя.

8. Данные возвращаются клиенту.

Технические и лицензионные требования

Для гибридной архитектуры современной проверки подлинности действуют следующие технические требования:

> ⓘ **Примечание**

Локальные учетные записи, в которых используется гибридная современная проверка подлинности с Outlook Mobile, не поддерживаются Office 365 клиентами сообщества государственных организаций США и обороны, Office 365 клиентами из Германии и Office 365 Китае, управляемыми клиентами 21Vianet.

1. **Локальная установка Exchange.**

    - Exchange Server накопительный пакет обновления 1 (CU1) 2019 года или более поздней версии, Exchange Server накопительным пакетом обновления 8 (CU8) 2016 или более поздней версии или Exchange Server 2013 CU19 или более поздней версии на всех серверах Exchange. В гибридных развертываниях (локальное развертывание Exchange и Exchange Online) или в организациях, использующих Exchange Online Archiving (EOA) с локальным развертыванием Exchange, необходимо развернуть самый актуальный накопитель или один накопительный пакет обновления до последней версии.

    - Все серверы Exchange 2007 или Exchange 2010 должны быть удалены из среды. Эти версии Exchange не поддерживаются в основном и не работают с Outlook, управляемым Intune для iOS и Android. В этой архитектуре Outlook для iOS и Android использует OAuth в качестве механизма проверки подлинности. Одно из локальных изменений конфигурации включает конечную точку OAuth в Microsoft Cloud в качестве конечной точки авторизации по умолчанию. После внесения этого изменения клиенты могут начать переговоры об использовании OAuth. Так как это изменение охватывает всю организацию, почтовые ящики Exchange 2010 с интерфейсом Exchange 2013 или 2016 неправильно считают, что они могут выполнять OAuth (они не могут), и в конечном итоге в отключенном состоянии (Exchange 2010 не поддерживает OAuth в качестве механизма проверки подлинности).

2. **Синхронизация Active Directory.** Синхронизация Active Directory всего локального каталога получателей почты с Microsoft Entra ID через Microsoft Entra Connect. Если в конфигурации Microsoft Entra Connect включена **фильтрация приложений и атрибутов** Microsoft Entra, убедитесь, что выбраны следующие приложения:

    - Office 365 профессиональный плюс
    - Exchange Online.
    - Azure RMS
    - Intune

Если в конфигурации Microsoft Entra Connect не включена **фильтрация Microsoft Entra приложений и атрибутов**, все необходимые приложения уже выбраны по умолчанию.

> **ⓘ Важно!**
>
> Outlook для iOS и Android использует глобальный список адресов клиента Exchange Online для локальных почтовых ящиков, использующих гибридную современную проверку подлинности. Если все получатели почты не синхронизированы с Microsoft Entra ID, у пользователей возникнут проблемы с потоком обработки почты.

3. **Гибридная установка Exchange.** Требуется полностью гибридная связь между локальной средой Exchange и Exchange Online.

   - Гибридная организация Microsoft 365 или Office 365 настроена в полной гибридной конфигурации с помощью режима классической гибридной топологии Exchange и настроена, как указано в помощнике по развертыванию Exchange.

     > **ⓘ Примечание**
     >
     > Гибридная современная проверка подлинности не поддерживается **гибридным агентом**.

   - Требуется организация Microsoft 365 или Office 365 корпоративный, организация для бизнеса или образования.

   - Данные локального почтового ящика синхронизируются в том же регионе центра обработки данных, где настроена организация Microsoft 365 или Office 365, или в регион центра обработки данных, определенный в **разделе PreferredDataLocation** учетной записи. Дополнительные сведения о расположении Microsoft 365 и Office 365 данных см. в центре управления безопасностью Майкрософт. Дополнительные сведения о **PreferredDataLocation** см. в разделе Возможности с несколькими регионами.

   - Имена узлов внешних URL-адресов для Exchange ActiveSync и автообнаружения должны быть опубликованы в качестве субъектов-служб для Microsoft Entra ID с помощью мастера гибридной конфигурации.

- Пространства имен автообнаружения и Exchange ActiveSync должны быть доступны из Интернета и не могут быть открыты для решения предварительной проверки подлинности.

- Убедитесь, что разгрузка SSL или TLS не используется между подсистемой балансировки нагрузки и серверами Exchange, так как эта настройка влияет на использование маркера OAuth. Использование мостов SSL и TLS (завершение и повторное шифрование) поддерживается.

4. **настройка Intune**. Поддерживаются как Intune автономные развертывания, так и развертывания совместного управления (Базовая мобильность и безопасность для Microsoft 365 не поддерживается).

5. **Лицензирование Microsoft 365 и Office 365**:

   - Приложение Outlook для iOS и Android бесплатно предоставляется потребителям в магазинах App Store (iOS) и Google Play. Однако коммерческим пользователям требуется подписка на Microsoft 365 или Office 365, которая включает классические приложения Office: Приложения Microsoft 365 для бизнеса, Microsoft 365 бизнес стандарт Приложения Microsoft 365 для предприятий, Office 365 корпоративный E3, Office 365 корпоративный E5 или соответствующие версии этих планов для правительства или образования. Коммерческие пользователи со следующими подписками могут использовать мобильное приложение Outlook на устройствах со встроенными экранами 10,1" по диагонали или меньше: Office 365 корпоративный E1, Office 365 F1, Office 365 A1, Microsoft 365 бизнес базовый и, если вы только иметь лицензию на Exchange Online (без Office). Если у вас есть только локальная лицензия Exchange (Exchange Server), вы не имеете лицензии на использование приложения.
   - Для использования расширенных функций Exchange Online (например, шифрования служб с помощью ключа клиента или возможностей с несколькими регионами) локальному пользователю должна быть назначена соответствующая лицензия на Office 365 или подписку Microsoft 365 в центре Microsoft 365 Admin.

   Дополнительные сведения о назначении лицензии см. в статье Добавление пользователей по отдельности или массово.

6. **Лицензирование EMS.** У каждого локального пользователя должна быть одна из перечисленных ниже лицензий.

- Intune автономной Microsoft Entra ID P1 или P2 или Microsoft Entra ID P1 или P2
- "Enterprise Mobility + Security E3", "Enterprise Mobility + Security E5".

Этапы реализации

Чтобы включить в организации поддержку гибридной современной проверки подлинности, необходимо выполнить каждое из указанных ниже действий (они подробно описаны в последующих разделах).

1. создание политики условного доступа;
2. создание политики защиты приложений с использованием Intune;
3. включение гибридной современной проверки подлинности;

Создание политики условного доступа

Если в качестве почтового приложения используется только Outlook для iOS и Android, чтобы стандартизировать доступ пользователей к данным Exchange, можно настроить политику условного доступа, блокирующую другие способы доступа с мобильных устройств. Outlook для iOS и Android проходит проверку подлинности с помощью объекта удостоверения Microsoft Entra, а затем подключается к Exchange Online. Поэтому необходимо создать политики условного доступа Microsoft Entra, чтобы ограничить подключение мобильных устройств Exchange Online. Для выполнения этой задачи требуются две политики условного доступа, каждая из которых предназначена для всех потенциальных пользователей. Дополнительные сведения о создании этих политик можно найти в статье Условный доступ: требовать утвержденные клиентские приложения или политику защиты приложений.

1. Выполните действия, описанные в разделе Требовать утвержденные клиентские приложения или политику защиты приложений с мобильных устройств. Эта политика разрешает Outlook для iOS и Android, но блокирует подключение OAuth и базовой проверки подлинности Exchange ActiveSync мобильных клиентов к Exchange Online.

   > ⓘ **Примечание**
   >
   > Эта политика гарантирует, что мобильные пользователи могут получить доступ ко всем конечным точкам Office с помощью соответствующих приложений.

2. Выполните действия, описанные в разделе Блокировать Exchange ActiveSync на всех устройствах, чтобы клиенты Exchange ActiveSync, использующие обычную проверку подлинности, не подключались к Exchange Online.

   Приведенные выше политики используют элемент управления предоставлением Требовать политику защиты приложений, который гарантирует, что политика защиты приложений Intune применяется к связанной учетной записи в Outlook для iOS и Android перед предоставлением доступа. Если пользователь не назначен Intune политике защиты приложений, не лицензирован для Intune или приложение не включено в политику защиты приложений Intune, то политика запрещает пользователю получать маркер доступа и получать доступ к данным обмена сообщениями.

3. Наконец, следуйте указаниям блокировать устаревшую проверку подлинности с помощью Microsoft Entra условный доступ, чтобы заблокировать устаревшую проверку подлинности для других протоколов Exchange на устройствах iOS и Android. Эта политика должна быть ориентирована только на Microsoft 365 или Office 365 Exchange Online платформы облачных приложений и устройств iOS и Android. Такой подход гарантирует, что мобильные приложения, использующие веб-службы Exchange, протоколы IMAP4 или POP3 с обычной проверкой подлинности, не могут подключаться к Exchange Online.

> ⓘ **Важно!**
>
> Чтобы можно было применять политики условного доступа для приложений на устройствах с iOS, должно быть установлено приложение Microsoft Authenticator. Для устройств с Android требуется приложение "Корпоративный портал Intune". Дополнительные сведения см. в статье **Условный доступ на основе приложений с помощью Intune**.

Чтобы заблокировать подключение других клиентов мобильных устройств (например, собственного почтового клиента, включенного в мобильную операционную систему) к локальной среде (которая проходит проверку подлинности с помощью обычной проверки подлинности локальная служба Active Directory):

Вы можете использовать встроенные правила доступа к мобильным устройствам Exchange и заблокировать подключение всех мобильных устройств, задав следующую команду в командной консоли Exchange:

PowerShell

```
Set-ActiveSyncOrganizationSettings -DefaultAccessLevel Block
```

> ⓘ **Примечание**
>
> Команда может повлиять на пользователей, подключающихся к локальной среде Exchange с помощью мобильных устройств.

создание политики защиты приложений с использованием Intune;

После включения гибридной современной проверки подлинности все локальные мобильные пользователи могут использовать Outlook для iOS и Android с помощью архитектуры Microsoft 365 или Office 365. Следовательно, очень важно защитить корпоративные данные с помощью политики защиты приложений с использованием Intune.

Чтобы создать политики защиты приложений с использованием Intune для iOS и Android, выполните действия, описанные в статье Как создать и назначить политики защиты приложений. Как минимум, каждая политика должна соответствовать следующим условиям:

1. К ним относятся все мобильные приложения Майкрософт, такие как Word, Excel или PowerPoint, так как это включение гарантирует, что пользователи могут безопасно получать доступ к корпоративным данным и управлять ими в любом приложении Майкрософт.

2. В ней должны быть реализованы функции защиты, предоставляемые средой Exchange для мобильных устройств, в том числе:

    - запрашивание ПИН-кода для доступа (предусматривает выбор типа, длину ПИН-кода, разрешение простого ПИН-кода и разрешение отпечатков);
    - шифрование данных приложения;
    - запрет запуска управляемых приложений на взломанных и рутованных устройствах.

3. Они назначаются всем пользователям. Это широкое назначение гарантирует защиту всех пользователей независимо от того, используют ли они Outlook для iOS и Android.

Помимо указанных выше минимальных требований к политике, следует рассмотреть возможность развертывания параметров расширенной политики защиты, таких как **Ограничение вырезания, копирования и вставки с другими приложениями,** чтобы предотвратить утечку корпоративных данных. Дополнительные сведения о доступных параметрах см. в разделе Параметры политики защиты приложений Android в Microsoft Intune и параметры политики защиты приложений iOS.

> ⓘ **Важно!**
>
> Чтобы применять политики защиты приложений с использованием Intune к приложениям на устройствах с Android, не зарегистрированных в Intune, пользователь также должен установить приложение "Корпоративный портал Intune". Дополнительные сведения см. **в разделе Параметры политики защиты приложений Android в Microsoft Intune**.

включение гибридной современной проверки подлинности;

1. Если вы не включили гибридную современную проверку подлинности, ознакомьтесь с предварительными условиями, описанными в статье Общие сведения о гибридной современной проверке подлинности и предварительные требования для ее использования с локальными серверами Skype для бизнеса и Exchange Server. После выполнения предварительных требований выполните действия, описанные в статье Настройка Exchange Server локальной среды для использования гибридной современной проверки подлинности.

2. Создайте правило разрешения доступа к локальному устройству Exchange, которое позволит Exchange Online подключаться к локальной среде с помощью протокола ActiveSync:

   PowerShell

   ```
   If ((Get-ActiveSyncOrganizationSettings).DefaultAccessLevel -ne
   "Allow") {New-ActiveSyncDeviceAccessRule -Characteristic DeviceType -
   QueryString "OutlookService" -AccessLevel Allow}
   ```

   > ⓘ **Примечание**

Управление устройствами через локальный центр администрирования Exchange невозможно. Для управления мобильными устройствами требуется Intune.

3. Создайте правило доступа к локальному устройству Exchange, которое запрещает пользователям подключаться к локальной среде с помощью Outlook для iOS и Android с обычной проверкой подлинности по протоколу Exchange ActiveSync:

```
PowerShell

New-ActiveSyncDeviceAccessRule -Characteristic DeviceModel -QueryString
"Outlook for iOS and Android" -AccessLevel Block
```

> ⓘ **Примечание**
>
> После создания этого правила Outlook для iOS и Android с пользователями обычной проверки подлинности будут заблокированы.

4. Убедитесь, что локальная Exchange ActiveSync maxRequestLength настроена в соответствии с maxSendSize/MaxReceiveSize вашей конфигурации транспорта:

   - Путь: `%ExchangeInstallPath%\FrontEnd\HttpProxy\Sync\web.config`
   - Свойство: `maxRequestLength`
   - Значение: задано в кб (например, 10 МБ — 10240)

Неподдерживаемые функции клиентов

Следующие функции не поддерживаются для локальных почтовых ящиков, использующих гибридную современную проверку подлинности с Outlook для iOS и Android.

- Синхронизация папки "Черновики" и черновиков сообщений
- Просмотр электронной почты в течение более четырех недель с помощью ссылки "Загрузить дополнительные сообщения" в нижней части списка сообщений
- Общий доступ к календарю и делегирование доступа к календарю
- Общий доступ и делегирование доступа к данным почтового ящика
- Время выхода Кортаны/ Время в пути
- Многофункциональные расположения собраний
- Управление задачами с помощью Microsoft To Do

- Надстройки
- Интересные календари
- Воспроизведение моих писем
- Метки конфиденциальности
- S/MIME;
- Планирование отправки

Следующие функции поддерживаются только в том случае, если локальная инфраструктура использует Exchange Server 2016 и более поздних версий:

- Вложения календарей

Вопросы и ответы о потоке подключения

Вопрос. В моей организации есть политика безопасности, которая требует, чтобы входящие подключения к Интернету были ограничены утвержденными IP-адресами или полными доменными именами. Возможна ли такая конфигурация при использовании этой архитектуры?

О. Корпорация Майкрософт рекомендует, чтобы локальные конечные точки для протоколов автообнаружения и ActiveSync были открыты и доступны из Интернета без каких-либо ограничений. В некоторых ситуациях, которые могут оказаться невозможными. Например, если вы находитесь в период сосуществования с другим решением стороннего единого управления конечными точками (UEM), возможно, потребуется наложить ограничения на протокол ActiveSync, чтобы запретить пользователям обходить решение UEM во время миграции в Intune и Outlook для iOS и Android. Если на пограничных устройствах локального брандмауэра или шлюза необходимо установить ограничения, корпорация Майкрософт рекомендует выполнять фильтрацию на основе конечных точек полного доменного имени. Если конечные точки FQDN не могут использоваться, отфильтруйте их по IP-адресам. Убедитесь, что в список разрешенных включены следующие IP-подсети и полные доменные имена:

- Все Exchange Online полные доменные имена и диапазоны IP-подсетей, как определено в разделе Дополнительные конечные точки, не включенные в веб-службу IP-адресов и URL-адресов Microsoft 365 или Office 365.

- Полные доменные имена autoDetect и диапазоны IP-подсетей, определенные в разделе Дополнительные конечные точки, не включенные в веб-службу IP-адресов и URL-адресов Microsoft 365 или Office 365. Эти IP-подсети и полные доменные имена необходимы, так как служба автоопределяет подключения к локальной инфраструктуре.

- Все полные доменные имена приложений Outlook для iOS, Android и мобильных приложений Office, как определено в Microsoft 365 и Office 365 URL-адреса и диапазоны IP-адресов.

Вопрос. В настоящее время моя организация использует стороннее решение UEM для управления подключением к мобильному устройству. Предоставление пространства имен Exchange ActiveSync в Интернете позволяет пользователям обойти стороннее решение UEM в течение периода сосуществования. Как предотвратить эту ситуацию?

Ответ. Устранить эту проблему можно тремя способами.

1. Реализуйте правила доступа к Exchange с мобильных устройств, которые указывают, каким устройствам разрешено подключаться.
2. Некоторые сторонние решения UEM интегрируются с правилами доступа к мобильным устройствам Exchange, блокируя несанкционированный доступ, добавляя утвержденные устройства в свойство ActiveSyncAllowedDeviceIDs пользователя.
3. Реализуйте ограничения IP-адресов в пространстве имен Exchange ActiveSync.

Вопрос. Можно ли использовать Azure ExpressRoute для управления трафиком между Microsoft Cloud и локальной средой?

О. Для подключения к Microsoft Cloud требуется подключение к Интернету. Корпорация Майкрософт рекомендует предоставлять автообнаружение и Exchange ActiveSync непосредственно в Интернете. Дополнительные сведения см. в статье Принципы подключения к сети Microsoft 365 и Office 365. Однако Azure ExpressRoute поддерживается для гибридных сценариев Exchange. Дополнительные сведения см. в статье Azure ExpressRoute для Microsoft 365 и Office 365.

При использовании ExpressRoute нет пространства частных IP-адресов для подключений ExpressRoute и не может быть "частного" разрешения DNS. Любая конечная точка, которую ваша компания хочет использовать через ExpressRoute, должна разрешаться в общедоступной службе DNS. Если эта конечная точка разрешается в IP-адрес, содержащийся в объявленных префиксах, связанных с каналом ExpressRoute (при включении пиринга Майкрософт для подключения ExpressRoute компания должна настроить эти префиксы в портал Azure), исходящее подключение из Exchange Online в локальную среду направляется через канал ExpressRoute. Вашей компании необходимо убедиться, что обратный трафик, связанный с этими подключениями, проходит через канал ExpressRoute (избегая асимметричной маршрутизации).

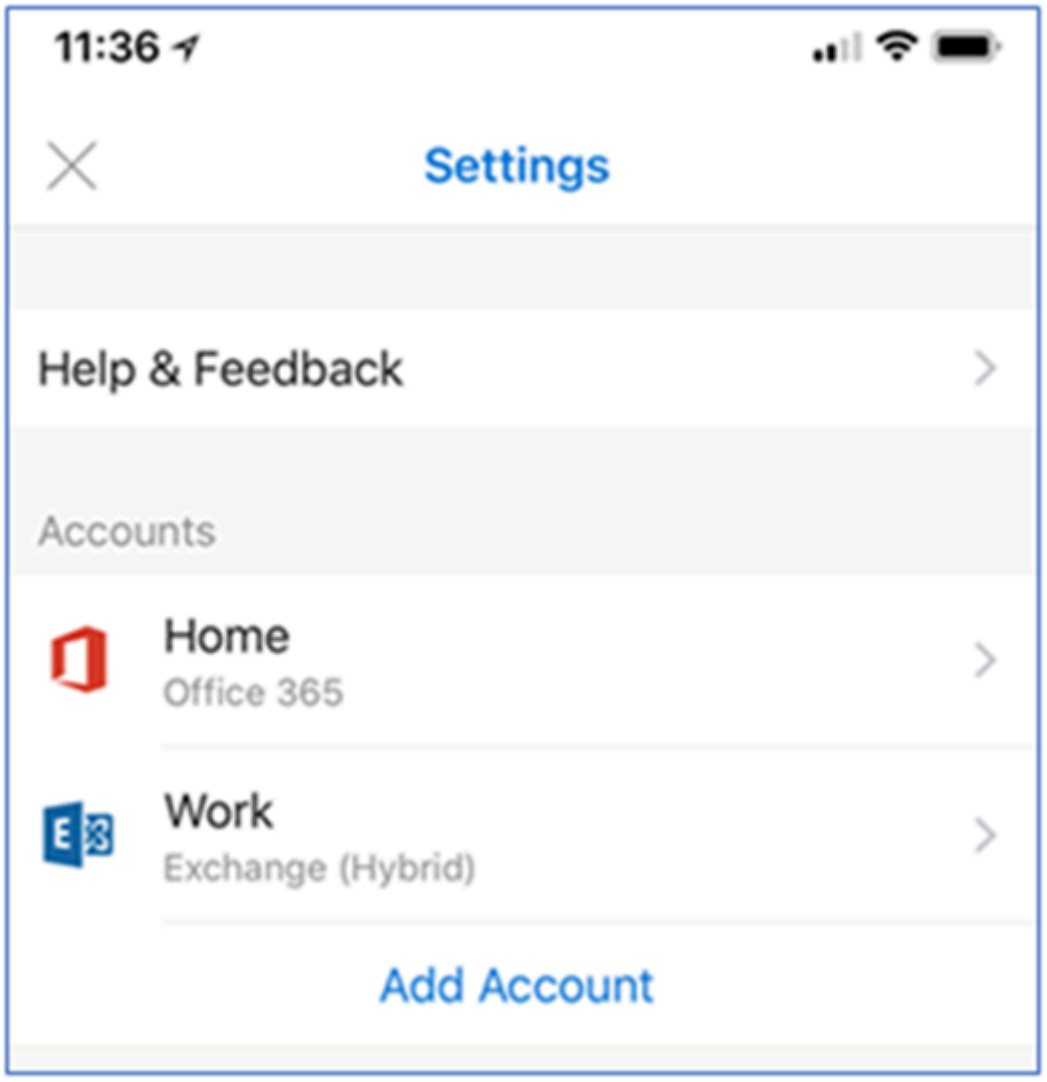
> **ⓘ Важно!**
>
> Так как Outlook для Android, iOS и Mac не поддерживает Azure ExpressRoute (а также собственные почтовые клиенты для мобильных устройств), мы не рекомендуем использовать Azure ExpressRoute, если вы планируете получить доступ к электронной почте на мобильном устройстве или устройстве Mac. Это связано с тем, что не может быть перекрытия пространства общедоступных IP-адресов, объявленного корпорации Майкрософт на канале ExpressRoute, и пространства общедоступных IP-адресов, объявленных в каналах Интернета.

Вопрос. Если данные сообщений синхронизируются с Exchange Online только за четыре недели, значит ли это, что поисковые запросы, выполняемые в Outlook для iOS и Android, не могут возвращать сведения, кроме данных, доступных на локальном устройстве?

Ответ. При выполнении поискового запроса в Outlook для iOS и Android элементы, соответствующие поисковому запросу, возвращаются, если они находятся на устройстве. Кроме того, поисковый запрос передается в локальную среду Exchange через Exchange Online. Локальная служба Exchange выполняет поисковый запрос к локальному почтовому ящику и возвращает результаты в Exchange Online, который передает результаты клиенту. Результаты локального запроса хранятся в Exchange Online в течение одного дня перед удалением.

Вопрос. Как убедиться, что учетная запись электронной почты успешно добавлена в Outlook для iOS и Android?

О. Локальные почтовые ящики, добавляемые с помощью гибридной современной проверки подлинности, помечены как **Exchange (гибридная)** в параметрах учетной записи в Outlook для iOS и Android, как показано в следующем примере:



Вопросы и ответы о проверке подлинности

Вопрос. Какие конфигурации удостоверений поддерживаются в случае гибридной современной проверки подлинности и Outlook для iOS и Android?

О. При гибридной современной проверке подлинности поддерживаются следующие конфигурации удостоверений с Microsoft Entra ID:

- Федеративное удостоверение с любым локальным поставщиком удостоверений, поддерживаемым Microsoft Entra ID
- Синхронизация хэша паролей через Microsoft Entra Connect
- Сквозная проверка подлинности через Microsoft Entra Connect

Вопрос. Какой механизм проверки подлинности используется для Outlook для iOS и Android? Хранятся ли учетные данные в Microsoft 365 или Office 365?

О. См. статью Настройка учетной записи с современной проверкой подлинности в Exchange Online.

Вопрос. Поддерживается ли единый вход в Outlook для iOS и Android, а также других мобильных приложениях Microsoft Office?

О. См. статью Настройка учетной записи с современной проверкой подлинности в Exchange Online.

Вопрос. Каков срок действия маркеров, создаваемых и используемых библиотекой проверки подлинности Active Directory (ADAL) в Outlook для iOS и Android?

О. См. статью Настройка учетной записи с современной проверкой подлинности в Exchange Online.

Вопрос. Что происходит с маркером доступа при изменении пароля пользователя?

О. См. статью Настройка учетной записи с современной проверкой подлинности в Exchange Online.

Вопрос. Может ли пользователь обойти AutoDetect, добавляя свою учетную запись в Outlook для iOS и Android?

Ответ. Да, пользователь может в любое время обойти автоопределить и вручную настроить подключение с помощью обычной проверки подлинности по протоколу Exchange ActiveSync. Чтобы пользователь не установил подключение к локальной среде с помощью механизма, который не поддерживает политики условного доступа Microsoft Entra или Intune защиты приложений, локальный администратор Exchange должен настроить правило доступа к устройству Exchange, которое блокирует подключение ActiveSync. Для выполнения этой задачи в командной консоли Exchange введите следующую команду:

PowerShell

```
New-ActiveSyncDeviceAccessRule -Characteristic DeviceModel -QueryString
"Outlook for iOS and Android" -AccessLevel Block
```

Вопрос. Что происходит, когда организация переходит от обычной проверки подлинности с помощью Outlook для iOS и Android к гибридной современной проверке подлинности?

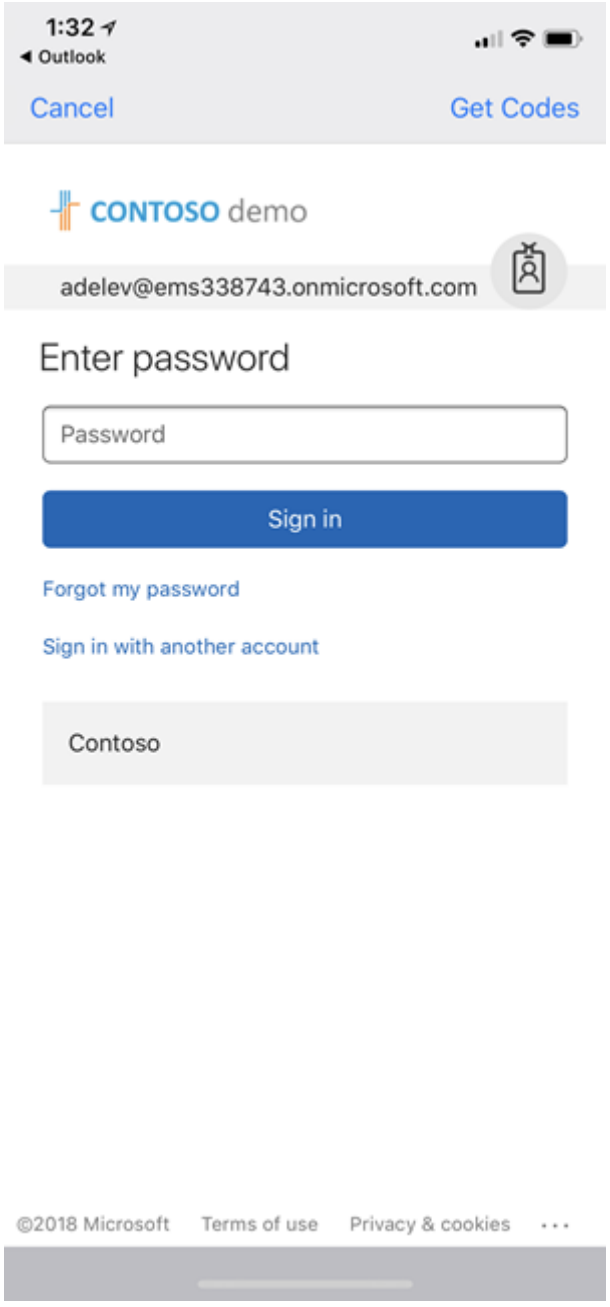
О. После того как организация включает гибридную современную проверку подлинности, выполнив описанные выше шаги по реализации, конечным пользователям необходимо удалить существующий профиль учетной записи в Outlook для iOS и Android, так как профиль использует обычную проверку подлинности. Затем пользователи могут создать новый профиль, который использует гибридную современную проверку подлинности.

Устранение неполадок

В этом разделе описываются наиболее распространенные проблемы или ошибки с локальными почтовыми ящиками, использующими гибридную современную проверку подлинности с Outlook для iOS и Android.

Автообнаружения и ActiveSync

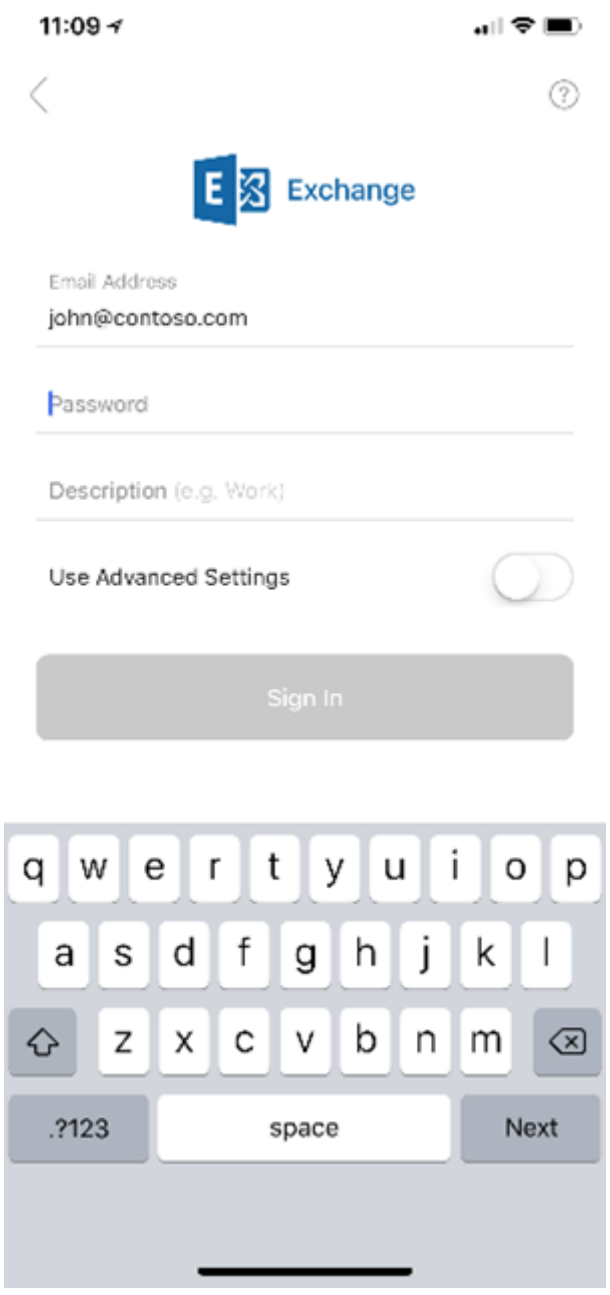
Во время создания профиля пользователю должно быть представлено диалоговое окно Современная проверка подлинности, аналогичное на следующем снимке экрана:



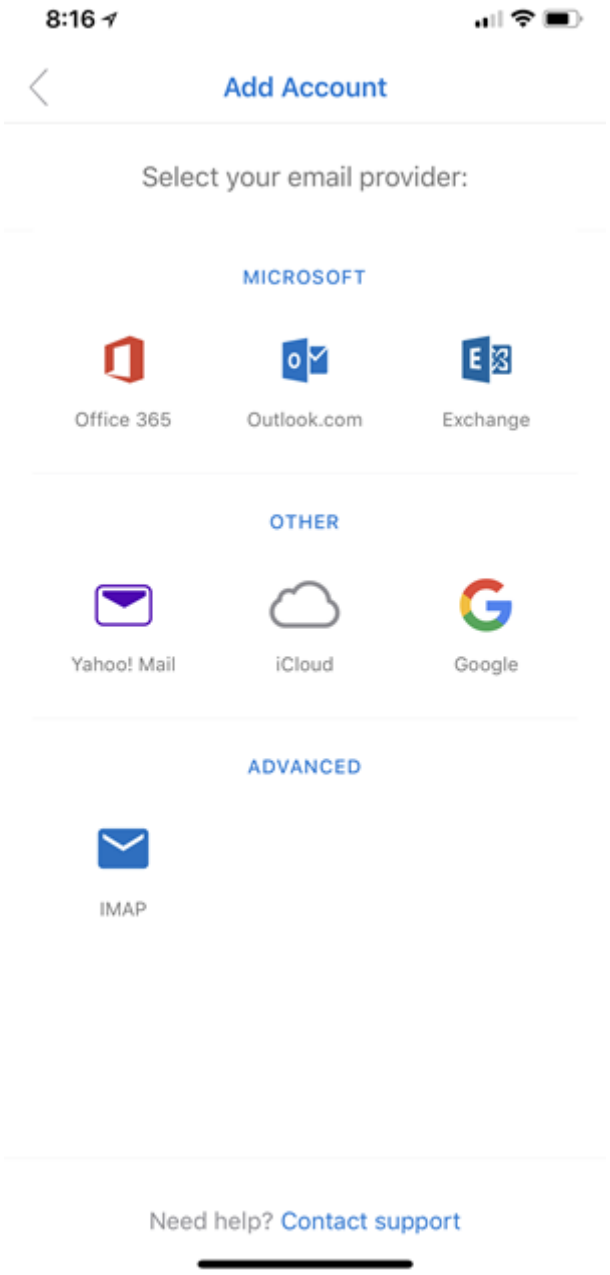
Если вместо этого пользователю предоставляется одно из следующих диалогов, возникает проблема с локальными конечными точками автообнаружения или

ActiveSync.

Ниже приведен пример того, как пользователю предоставляется устаревшая базовая проверка подлинности Exchange ActiveSync:



Ниже приведен пример того, что пользователи видят, когда автоопределить не удается обнаружить конфигурацию для локальных почтовых ящиков пользователей.



В любом сценарии убедитесь, что локальная среда настроена правильно. Для выполнения этой задачи скачайте и выполните скрипт проверки гибридной современной проверки подлинности для Outlook для iOS и Android из коллекции TechNet.

При просмотре выходных данных скрипта должны отобразиться следующие выходные данные автообнаружения:

JSON

```
{
    "Protocol": "activesync",
    "Url": "https://mail.contoso.com/Microsoft-Server-ActiveSync"
}
```

Локальная конечная точка ActiveSync должна возвращать следующий ответ, в котором заголовок WWW-Authenticate содержит authorization_uri:

Консоль

```
Content-Length →0
Date →Mon, 29 Jan 2018 19:51:46 GMT
Server →Microsoft-IIS/10.0 Microsoft-HTTPAPI/2.0
WWW-Authenticate →Bearer client_id="00000002-0000-0ff1-ce00-000000000000",
trusted_issuers="00000001-0000-0000-c000-000000000000@5de110f8-2e0f-4d45-
891d-bcf2218e253d,00000004-0000-0ff1-ce00-000000000000@contoso.com",
token_types="app_asserted_user_v1 service_asserted_app_v1",
authorization_uri="https://login.windows.net/common/oauth2/authorize"
Www-Authenticate →Basic realm="mail.contoso.com"
X-Powered-By →ASP.NET
request-id →5ca2c827-5147-474c-8457-63c4e5099c6e
```

Если ответы автообнаружения или ActiveSync не похожи на приведенные выше примеры, можно изучить следующие причины:

1. Если не удается получить доступ к конечной точке автообнаружения, скорее всего, возникла проблема с конфигурацией брандмауэра или подсистемы балансировки нагрузки (например, настроены ограничения IP-адресов и отсутствуют необходимые диапазоны IP-адресов). Кроме того, перед Exchange может находиться устройство, требующее предварительной проверки подлинности для доступа к конечной точке автообнаружения.

2. Если конечная точка автообнаружения не возвращает правильный URL-адрес, возникает проблема с конфигурацией со значением ExternalURL виртуального каталога ActiveSync.

3. Если не удается получить доступ к конечной точке ActiveSync, возникает проблема с конфигурацией брандмауэра или подсистемы балансировки нагрузки. Опять же, одним из примеров является настройка ограничений IP-адресов и отсутствуют необходимые диапазоны IP-адресов. Кроме того, перед Exchange может находиться устройство, требующее предварительной проверки подлинности для доступа к конечной точке ActiveSync.

4. Если конечная точка ActiveSync не содержит authorization_uri значение, убедитесь, что сервер проверки подлинности EvoSTS настроен в качестве конечной точки по умолчанию с помощью командной консоли Exchange:

   PowerShell

   ```
   Get-AuthServer EvoSts | Format-List IsDefaultAuthorizationEndpoint
   ```

5. Если конечная точка ActiveSync не содержит заголовок WWW-Authenticate, устройство перед Exchange может отвечать на запрос.

Проблемы с синхронизацией клиентов

Существует несколько сценариев, которые могут привести к устареть данные в Outlook для iOS и Android. Как правило, это условие данных связано с проблемой со вторым маркером доступа (маркер, используемый MRS в Exchange Online для синхронизации данных с локальной средой). Ниже приведены две наиболее распространенные причины этой проблемы.

- Разгрузка SSL/TLS в локальной среде.
- Проблемы с метаданными сертификата EvoSTS.

При разгрузке SSL/TLS маркеры выдаются для определенного URI, и это значение включает значение протокола ("https://"). Когда подсистема балансировки нагрузки разгружает ПРОТОКОЛ SSL/TLS, запрос, полученный Exchange, поступает по протоколу HTTP, что приводит к несоответствию утверждений из-за http:// значения протокола. В следующем примере показан заголовок ответа из трассировки Fiddler:

Консоль

```
Content-Length →0
Date →Mon, 29 Jan 2018 19:51:46 GMT
Server →Microsoft-IIS/10.0 Microsoft-HTTPAPI/2.0
WWW-Authenticate →Bearer client_id="00000002-0000-0ff1-ce00-000000000000",
trusted_issuers="00000001-0000-0000-c000-000000000000@00c118a9-2de9-41d3-
b39a-81648a7a5e4d",
authorization_uri="https://login.windows.net/common/oauth2/authorize",
error="invalid_token"
WWW-Authenticate →Basic realm="mail.contoso.com"
X-Powered-By →ASP.NET
request-id →2323088f-8838-4f97-a88d-559bfcf92866
x-ms-diagnostics →2000003;reason="The hostname component of the audience
claim value is invalid. Expected 'https://mail.contoso.com'. Actual
'http://mail.contoso.com'.";error_category="invalid_resource"
```

Как указано выше в разделе *Технические требования и требования к лицензированию*, разгрузка SSL/TLS не поддерживается для потоков OAuth.

Для метаданных сертификата EvoSTS метаданные сертификата, используемые EvoSTS, периодически обновляются в Microsoft 365 или Office 365. Почтовый ящик локального арбитража Exchange с возможностью организации "OrganizationCapabilityManagement" отвечает за обнаружение изменений и

обновление соответствующих метаданных в локальной среде; этот процесс выполняется каждые восемь часов.

Администраторы Exchange могут найти этот почтовый ящик, выполнив следующий командлет с помощью командной консоли Exchange:

PowerShell

```
$x=Get-mailbox -arbitration | ? {$_.PersistedCapabilities -like
"OrganizationCapabilityManagement"};Get-MailboxDatabaseCopyStatus
$x.database.name
```

На сервере, на котором размещена база данных для почтового ящика арбитража OrganizationCapabilityManagement, просмотрите журналы событий приложения на наличие событий с источником **MSExchange AuthAdmin**. События должны указать, может ли Exchange обновить метаданные. Если метаданные устарели, их можно обновить вручную с помощью следующего командлета:

PowerShell

```
Set-AuthServer EvoSts -RefreshAuthMetadata
```

Вы также можете создать запланированную задачу, которая выполняет указанную выше команду каждые 24 часа.

статистика Exchange Online

Для просмотра статистических данных для каждого синхронизированного локального почтового ящика можно использовать следующие командлеты Exchange Online.

1. Сначала получите расположение синхронизированного локального почтового ящика в клиенте, указав удостоверение локального почтового ящика (например, `jane@contoso.com`).

   PowerShell

   ```
   $m = Get-MailboxLocation <identity>
   ```

2. Чтобы просмотреть статистику, связанную с почтовыми ящиками, используйте

   PowerShell

```
Get-MailboxStatistics $m.id
```

3. Чтобы просмотреть статистику мобильных устройств (например, когда Outlook для iOS и Android в последний раз синхронизировался с Exchange Online), используйте

```
PowerShell

Get-MobileDeviceStatistics -Mailbox $m.id
```

Дополнительные сведения см. в разделах Get-MailboxStatistics и Get-MobileDeviceStatistics.

Другие проблемы

Существуют и другие проблемы, которые могут препятствовать правильной работе гибридной современной проверки подлинности. Дополнительные сведения см. в разделе об устранении неполадок в статье Объявление о гибридной современной проверке подлинности для локальной службы Exchange.

Применение обычной проверки подлинности в Outlook для iOS и Android

Статья • 04.04.2023

Приложение Outlook для iOS и Android позволяет работать с электронной почтой, календарем, контактами и другими файлами на мобильном устройстве эффективнее. В этой статье представлен обзор архитектуры и структуры хранилища приложения, чтобы администраторы Exchange могли развертывать и обслуживать Outlook для iOS и Android в своих организациях Exchange.

> **Примечание**
>
> В этой статье описывается использование приложения в среде Exchange 2010, Exchange 2013, Exchange 2016 или Exchange 2019, где **не** включена гибридная современная проверка подлинности. Дополнительные сведения об использовании гибридной современной проверки подлинности для локальных почтовых ящиков с приложением см. в статье Использование гибридной современной проверки подлинности в Outlook для iOS и Android. Сведения об использовании приложения с Exchange Online см. в статье Outlook для iOS и Android в Exchange Online.

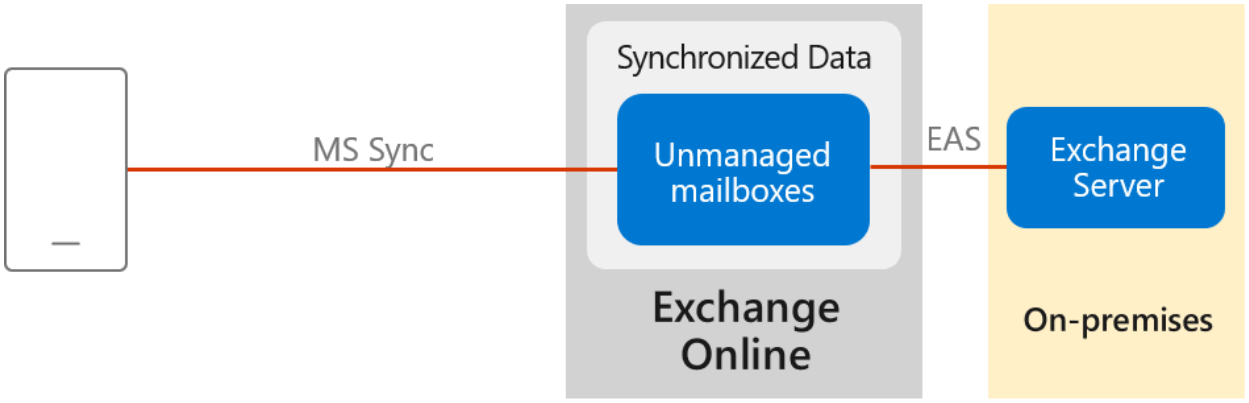
Архитектура Outlook для iOS и Android

Приложение Outlook для iOS и Android работает при поддержке облака. Эта характеристика означает, что ваш интерфейс состоит из локально установленного приложения на базе безопасной и масштабируемой службы, работающей в Microsoft Cloud.

Для почтовых ящиков Exchange Server архитектура Outlook для iOS и Android встроена непосредственно в Microsoft Cloud. Этот макет архитектуры предоставляет клиентам дополнительные преимущества безопасности, конфиденциальности, встроенного соответствия требованиям и прозрачных операций, которые Корпорация Майкрософт фиксирует в Центре управления безопасностью Майкрософт.

Следующие среды будут использовать преимущества этой архитектуры на основе Microsoft 365 или Office 365:

- В средах Exchange Server 2010
- Если гибридная связь между локальной средой Exchange 2013, 2016 или 2019 и Microsoft 365 или Office 365 не настроена
- Если гибридная современная проверка подлинности не включена между локальной средой Exchange 2013, 2016 или 2019 и Microsoft 365 или Office 365



В архитектуре Microsoft 365 или Office 365 Outlook для iOS и Android использует собственную технологию синхронизации майкрософт для синхронизации данных, которая защищена сквозными подключениями, защищенными TLS, между Microsoft 365 или Office 365 и приложением.

Подключение Exchange ActiveSync (EAS) между Exchange Online и локальной средой обеспечивает синхронизацию локальных данных пользователей и включает четыре недели электронной почты, все данные календаря, все контактные данные и состояние "нет на рабочем месте". Регион, в котором синхронизируются эти данные, зависит от IP-адреса, используемого мобильным устройством во время настройки синхронизации. Если у вас есть гибридная настройка с клиентом Exchange Online, локальные данные не синхронизируются с клиентом. Вместо этого данные синхронизируются в Outlook.com так же, как если бы у вас был Exchange Server без гибридной среды. Если вы хотите управлять локальными данными в клиенте и управлять ими, необходимо включить гибридную современную проверку подлинности с помощью Outlook для iOS и Android.

Синхронизация данных между локальной средой Exchange и Exchange Online происходит независимо от поведения пользователя. Эта характеристика обеспечивает быструю доставку новых сообщений на устройства. Дополнительные сведения о том, как модель проверки подлинности пользователя обеспечивает синхронизацию данных независимо от поведения пользователя, см. в разделе Пароли и безопасность в Outlook для iOS и Android для Exchange Server.

Обработка информации в Microsoft Cloud обеспечивает поддержку расширенных функций и возможностей, таких как категоризация электронных сообщений для

сортировки почты, персонализированный интерфейс для путешествий и календаря, а также повышенную скорость поиска. Использование облака для интенсивной обработки и минимальное использование ресурсов пользовательских устройств повышают производительность и стабильность приложения. Наконец, он позволяет Outlook создавать функции, которые работают во всех учетных записях электронной почты, независимо от технологических возможностей базовых серверов (таких как различные версии Exchange Server, Microsoft 365 или Office 365).

> **Важно!**
>
> Локальные почтовые ящики, использующие обычную проверку подлинности в Outlook для iOS и Android, не поддерживают функции Enterprise Mobility + Security, такие как условный доступ Microsoft Entra и политики защиты приложений Intune. Сведения о поддержке этих технологий см. в статье **Использование гибридной современной проверки подлинности в Outlook для iOS и Android**.

Средства управления безопасностью и аудитом данных, а также доступом к ним

Локальные данные синхронизируются с Exchange Online, и у пользователей возникают вопросы о том, как эти данные защищаются в Exchange Online. В техническом документе Шифрование в Microsoft Cloud рассматривается использование BitLocker для шифрования на уровне тома.

По умолчанию инженеры Майкрософт имеют нулевые права администратора и нулевой постоянный доступ к содержимому клиентов в Microsoft 365 и Office 365. В техническом документе Управление административным доступом в Microsoft 365 рассматриваются проверка персонала, проверка фона, блокировка и защищенное хранилище клиентов и многое другое.

В документации iso Audited Controls on Service Assurance приведены сведения о состоянии проверенных элементов управления на основе глобальных стандартов и правил информационной безопасности, реализованных Microsoft 365 и Office 365.

Требования к подключению

Корпорация Майкрософт рекомендует, чтобы локальные конечные точки для протоколов автообнаружения и ActiveSync были открыты и доступны из Интернета

без каких-либо ограничений. В некоторых ситуациях, которые могут оказаться невозможными. Если на пограничных устройствах локального брандмауэра или шлюза необходимо установить ограничения, корпорация Майкрософт рекомендует выполнять фильтрацию на основе конечных точек полного доменного имени. Если конечные точки полного доменного имени не могут использоваться, выполните фильтрацию по IP-адресам. Убедитесь, что в список разрешенных включены следующие IP-подсети и полные доменные имена:

- Все полные доменные имена Exchange Online и диапазоны IP-подсетей, определенные в URL-адресах и диапазонах IP-адресов Microsoft 365 и Office 365.
- Диапазоны полных доменных имен и IP-подсетей, определенных в разделе Дополнительные IP-адреса и URL-адреса Microsoft 365 или Office 365, не включенные в веб-службы. Эти диапазоны являются обязательными, так как служба автоопределия устанавливает подключения к локальной инфраструктуре.
- Все полные доменные имена приложений Outlook iOS, Android и мобильных приложений Office, как определено в microsoft 365 или Office 365 URL-адреса и диапазонах IP-адресов.

Неподдерживаемые функции клиентов

Следующие функции не поддерживаются для локальных почтовых ящиков, использующих обычную проверку подлинности в Outlook для iOS и Android:

- Синхронизация папки "Черновики" и черновиков сообщений
- Общий и делегированный доступ к календарям
- Общий доступ и делегирование доступа к данным почтового ящика
- Время выхода Кортаны/ Время в пути
- Многофункциональные расположения собраний
- Управление задачами с помощью Microsoft To-Do
- Избранные пользователи с уведомлениями
- Надстройки
- Интересные календари

- Поддержка аватара
- Воспроизведение моих писем
- S/MIME;
- Метки конфиденциальности
- Веб-канал обнаружения
- Параметры конфиденциальности

Следующие функции поддерживаются только в том случае, если локальная инфраструктура использует Exchange Server 2016 и более поздних версий:

- Вложения календарей

Настройка учетной записи в Outlook для iOS и Android с использованием обычной проверки подлинности

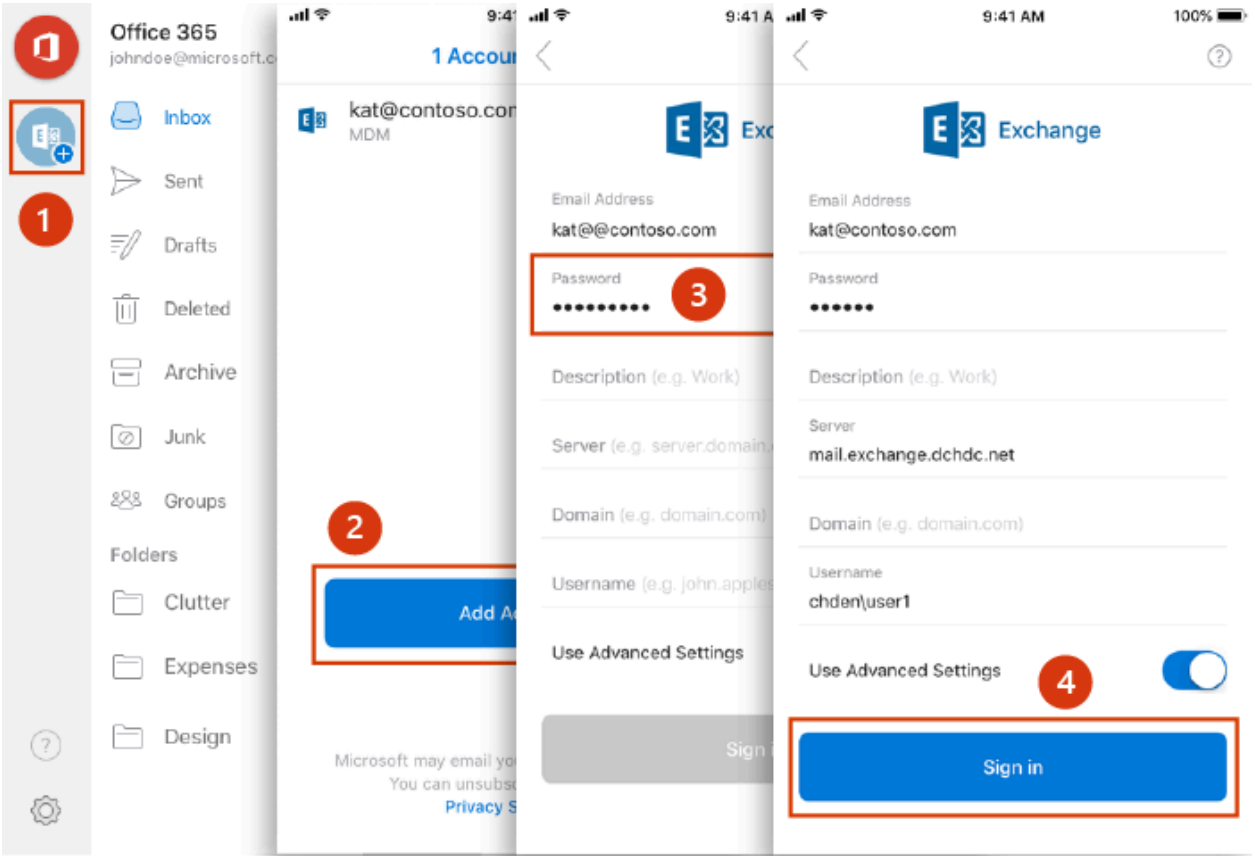
Статья • 01.11.2024

Outlook для iOS и Android предоставляет администраторам Exchange возможность "отправлять" конфигурации учетных записей локальным пользователям, которые используют обычную проверку подлинности с протоколом ActiveSync. Эта возможность работает с любым поставщиком Единого управления конечными точками (UEM), который использует управляемый канал Конфигурация приложений для iOS или Android в канале Enterprise для Android.

Для локальных пользователей, зарегистрированных в Microsoft Intune, можно развернуть параметры конфигурации учетной записи с помощью Intune в портал Azure.

После создания конфигурации учетной записи и регистрации устройства outlook для iOS и Android обнаруживает, что учетная запись найдена, и предлагает пользователю добавить учетную запись. После этого для завершения настройки пользователю нужно будет ввести лишь пароль. Затем загружается содержимое почтового ящика пользователя, и пользователь может начать использовать приложение.

На следующих изображениях показан пример процесса настройки конечным пользователем после настройки Outlook для iOS и Android в Intune.



Создание политики настройки Outlook для iOS и Android с помощью Microsoft Intune

Если вы используете Microsoft Intune в качестве поставщика управления мобильными устройствами, следующие действия позволяют развернуть параметры конфигурации учетной записи для локальных почтовых ящиков, использующих обычную проверку подлинности с протоколом ActiveSync. После создания конфигурации можно назначить параметры группам пользователей, как описано в следующем разделе Назначение параметров конфигурации.

> **Примечание**
>
> Если в вашей организации используются устройства и с iOS, и с Android for Work, вам придется создать отдельную политику настройки приложений для каждой из платформ.

1. В центре администрирования Microsoft Intune в https://intune.microsoft.com разделе**Политика приложений**> выберите >**Политики конфигурации приложений**. Или, чтобы перейти непосредственно на страницу **Политики конфигурации приложений** , используйте

https://intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/AppsMenu/~/appConfig.

2. На странице **политики Конфигурация приложений** выберите **Добавить**>**управляемые устройства**, чтобы запустить мастер политики конфигурации приложений.

3. На вкладке **Основные** сведения на открывающейся странице **Создание политики конфигурации приложения** настройте следующие параметры:

   - **Имя**. Введите уникальное описательное имя.
   - **Описание**. Введите необязательное описание параметров конфигурации приложения.
   - **Платформа**: выберите **iOS/iPadOS** или **Android Enterprise**.
   - **Целевое приложение**. Выберите **приложение**. Во всплывающем окне **Связанное приложение** выберите **Outlook**.

     > **Совет**
     >
     > Если Outlook не указан как доступное приложение, добавьте его, следуя инструкциям в **разделах Добавление приложений магазина Android в Microsoft Intune** и **Добавление приложений магазина iOS в Microsoft Intune**.

     Завершив работу во всплывающем меню **Связанное приложение** , нажмите **кнопку ОК** , чтобы вернуться на вкладку **Основные сведения** на странице **Создание политики конфигурации приложения** .

   Завершив работу на вкладке **Основные сведения** , нажмите кнопку **Далее**.

   > **Примечание**
   >
   > Если Outlook не указан как доступное приложение, его необходимо добавить, следуя инструкциям в **разделах Добавление приложений магазина Android в Microsoft Intune** и **Добавление приложений магазина iOS в Microsoft Intune**.

4. На вкладке **Параметры** настройте следующие параметры:

- **Email разделе конфигурация учетной записи**. Настройте следующие параметры:
  - Раздел **параметров конфигурации**
    - **Формат параметров конфигурации**. Выберите **Использовать конструктор конфигураций**. Этот выбор приводит к отображению многих других параметров. Пары значений ключей, используемые в этом разделе, определяются в разделе Пары значений ключей.
    - **Email разделе конфигурации учетной записи**:
      - **Настройка параметров учетной записи электронной почты**. Выберите **Да** , чтобы развернуть конфигурацию настройки учетной записи:
      - **Тип проверки подлинности**: выберите **Обычная проверка подлинности**. Это значение необходимо для локальных учетных записей, которые не используют гибридную современную проверку подлинности.
      - **Атрибут username из Microsoft Entra ID**. Выберите одно из следующих значений:
        - **"User Principal Name" (Имя участника-пользователя);**
        - **sAMAccountName**. Для этого значения требуется доменное имя NetBIOS в поле **Домен учетной записи** .
      - **атрибут Email address из Microsoft Entra ID**. Выберите **Основной SMTP-адрес**.
        - **Email сервер**. Введите доменное имя Exchange ActiveSync с внешним доступом.
        - **Email имя учетной записи**: введите описательное значение для учетной записи.
- **Раздел Общая конфигурация приложения**. Если вы хотите развернуть общие параметры конфигурации приложений, настройте нужные параметры соответствующим образом:

  - **Сортировка папки "Входящие"**: выберите одно из следующих значений:
    - **Не настроено** (по умолчанию)
    - **Включено** (приложение по умолчанию)
    - **Выкл.**

  - **Требовать биометрические данные для доступа к приложению**. Выберите одно из следующих значений:

    - **Не настроено** (по умолчанию)

    - **On**

- **Выкл** . (приложение по умолчанию)

  Значения **Вкл** . или **Выкл.** активируют параметр **Разрешить пользователю изменять параметры** :
  - Выберите **Да** (приложение по умолчанию), чтобы разрешить пользователю изменить параметр.
  - Выберите **Нет** , чтобы запретить пользователям изменять параметр. Этот параметр доступен только в Outlook для iOS.

- **Сохранить контакты**. Выберите одно из следующих значений:
  - **Не настроено** (по умолчанию)
  - **On**
  - **Выкл** . (приложение по умолчанию)

    Значения **Вкл** . или **Выкл.** , активный параметр **Разрешить пользователю изменять параметр** :
    - Выберите **Да** (приложение по умолчанию), чтобы разрешить пользователю изменить параметр.
    - Выберите **Нет** , чтобы запретить пользователям изменять параметр.

- **Сигнатура приложения по умолчанию**. Выберите одно из следующих значений:
  - **Не настроено** (по умолчанию)
  - **Включено** (приложение по умолчанию)
  - **Выкл.**

- **Блокировать внешние образы**. Выберите одно из следующих значений:
  - **Не настроено** (по умолчанию)
  - **On**
  - **Выкл** . (приложение по умолчанию)

    Значения **Вкл** . или **Выкл.** , активный параметр **Разрешить пользователю изменять параметр** :
    - Выберите **Да** (приложение по умолчанию), чтобы разрешить пользователю изменить параметр.
    - Выберите **Нет** , чтобы запретить пользователям изменять параметр.

- **Упорядочение почты по потоку**. Выберите одно из следующих значений:
  - **Не настроено** (по умолчанию)
  - **Включено** (приложение по умолчанию)
  - **Выкл.**

Завершив работу на вкладке **Параметры** , нажмите кнопку **Далее**.

5. На вкладке **Назначения** выберите, к кому применяется политика. Вы назначаете параметры группам пользователей в Microsoft Entra ID. Если у пользователя установлено приложение Microsoft Outlook, управление приложением осуществляется с помощью настроенных параметров.

   - Раздел **Включенные группы**. Выберите и настройте один из следующих параметров:
     - **Добавление групп**
     - **Добавление всех пользователей**
     - **Добавление всех устройств**

   - Раздел **Исключенные группы**. Выберите **Добавить группы**, чтобы исключить группы из политики.

     > **Совет**
     >
     > Вы не можете смешивать группы пользователей и группы устройств для включения и исключения.

   Завершив работу на вкладке **Назначения** , нажмите кнопку **Далее**.

6. На вкладке **Рецензирование и создание** просмотрите выбранные параметры.

   Выберите **Предыдущий** или используйте вкладки, чтобы вернуться и внести изменения.

   Завершив работу на вкладке **Проверка и создание** , выберите **Создать.**

На странице **Политики конфигурации приложений** отобразится только что созданная политика конфигурации.

Назначение параметров конфигурации

Вы назначаете параметры группам пользователей в Microsoft Entra ID. Если у пользователя установлено приложение Microsoft Outlook, управление

приложением осуществляется с помощью указанных параметров.

1. На странице **Политики конфигурации приложений** выберите https://intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/AppsMenu/~/appConfig политику из списка, щелкнув значение **Имя** .
2. На открывающейся странице сведений о политике выберите **Свойства** в разделе **Управление** .
3. На открывающейся странице **Свойства** выберите **Изменить** в разделе **Назначения** .
4. На вкладке **Назначения** на открывающейся странице **Изменение политики конфигурации приложения** настройте следующие параметры:

   - Раздел **Включенные группы**. Выберите и настройте один из следующих параметров:
     - **Добавление групп**
     - **Добавление всех пользователей**
     - **Добавление всех устройств**
   - Раздел **Исключенные группы**. Выберите **Добавить группы**, чтобы исключить группы из политики.

     > **Совет**
     >
     > Вы не можете смешивать группы пользователей и группы устройств для включения и исключения.

   Завершив работу на вкладке **Назначения** , выберите **Просмотр и сохранение**.

Пары "ключ-значение"

При создании политики конфигурации приложения в портал Azure или с помощью поставщика UEM вам потребуются следующие пары значений ключей:

Развернуть таблицу

Key	Значения
com.microsoft.outlook.EmailProfile.EmailAccountName	Это значение указывает учетную запись электронной почты с отображаемым именем, как оно отображается для пользователей на

Key	Значения
	их устройствах. **Тип значения**: String **Допустимые значения**: Отображаемое имя **Значение по умолчанию (если значение не указано)**: <blank> **Обязательный:** Да **Пример**: пользователь **Токен Intune***: {{username}}
com.microsoft.outlook.EmailProfile.EmailAddress	Это значение определяет электронные адреса, которые нужно использовать для отправки и получения почты. **Тип значения**: String **Допустимые значения**: Email адрес **Значение по умолчанию (если значение не указано)**: <blank> **Обязательный:** Да **Пример**: `user@contoso.com`. **Токен Intune***: {{mail}}
com.microsoft.outlook.EmailProfile.EmailUPN	Это значение указывает имя участника-пользователя или имя пользователя для профиля электронной почты, используемого для проверки подлинности учетной записи. **Тип значения**: String **Допустимые значения**: адрес имени участника-пользователя или имя пользователя **Значение по умолчанию (если значение не указано)**: <blank> **Обязательный:** Да **Пример**: `userupn@contoso.com`. **Токен Intune***: {{userprincipalname}}
com.microsoft.outlook.EmailProfile.ServerAuthentication	Это значение определяет способ проверки подлинности для пользователя. **Тип значения**: String **Допустимые значения**: "Имя пользователя и пароль" **Значение по умолчанию (если значение не указано)**: 'Username and Password'

Key	Значения
	Обязательный: Нет **Пример:** 'Username and Password'
com.microsoft.outlook.EmailProfile.ServerHostName	Это значение определяет имя узла для сервера Exchange Server. **Тип значения**: String **Допустимые значения**: Полное доменное имя ActiveSync **Значение по умолчанию (если значение не указано)**: <blank> **Обязательный:** Да **Пример**: `mail.contoso.com`.
com.microsoft.outlook.EmailProfile.AccountDomain	Это значение указывает домен учетной записи пользователя. **Тип значения**: String **Допустимые значения**: Домен **Значение по умолчанию (если значение не указано)**: <blank> **Обязательный:** Нет **Пример**: contoso
com.microsoft.outlook.EmailProfile.AccountType	Это значение указывает тип учетной записи, настраиваемой на основе модели проверки подлинности. **Тип значения**: String **Допустимые значения**: BasicAuth **Значение по умолчанию, если не указано**: BasicAuth **Обязательный:** Нет **Пример**: BasicAuth

*Microsoft Intune пользователи могут использовать маркеры, которые будут расширяться до правильного значения в соответствии с зарегистрированным пользователем. Дополнительные сведения см. в статье Добавление политик конфигурации приложений для управляемых устройств iOS .

Пароли и безопасность в Outlook для iOS и Android для Exchange Server

Статья • 04.04.2023

В этой статье описывается, как работают пароли и безопасность в Outlook для iOS и Android с Exchange Server при использовании обычной проверки подлинности с протоколом Exchange ActiveSync.

> **Важно!**
>
> Outlook для iOS и Android поддерживает гибридную современную проверку подлинности для локальных почтовых ящиков, что устраняет необходимость использования базовой проверки подлинности. Сведения, содержащиеся в этой статье, относятся только к обычной проверке подлинности. Дополнительные сведения см. в статье **Использование гибридной современной проверки подлинности с Outlook для iOS и Android**.

Создание учетной записи и защита паролей

При первом запуске в локальной среде Exchange приложение Outlook для iOS и Android создает случайный ключ AES-128. Этот ключ известен как *ключ устройства* и хранится только на устройстве пользователя.

Когда пользователь входит в Exchange с помощью обычной проверки подлинности, имя пользователя, пароль и уникальный ключ устройства AES-128 отправляются с устройства пользователя в облачную службу Outlook по протоколу TLS, где ключ устройства хранится в вычислительной памяти среды выполнения. После проверки пароля на сервере Exchange архитектура Microsoft 365 или Office 365 использует ключ устройства для шифрования пароля, а затем зашифрованный пароль сохраняется в службе. Ключ устройства, тем временем, очищается из памяти и никогда не сохраняется в архитектуре на основе Microsoft 365 или Office 365 (ключ хранится только на устройстве пользователя).

Затем, когда пользователь пытается подключиться к Exchange для получения данных почтового ящика, ключ устройства снова передается с устройства в архитектуру на основе Microsoft 365 или Office 365 через защищенное tls-подключение, где он используется для расшифровки пароля в вычислительной памяти среды выполнения. После расшифровки пароль не сохраняется в службе и не записывается на локальный диск, а ключ устройства снова удаляется из памяти.

После того как архитектура на основе Microsoft 365 или Office 365 расшифровывает пароль во время выполнения, служба может подключиться к серверу Exchange Server для синхронизации данных почты, календаря и других данных почтового ящика. Пока пользователь продолжает периодически открывать и использовать Outlook, архитектура Microsoft 365 или Office 365 будет хранить копию расшифрованного пароля пользователя в памяти, чтобы сохранить подключение к Exchange Server активным.

Рекомендации по соответствию при отправке паролей

Прежде чем включить все, что позволяет передавать пароли из локальной среды Exchange, обязательно рассмотрите возможные последствия. Например, передача паролей в архитектуру Microsoft 365 или Office 365 может привести к невозможности выполнить требования PCI-DSS или ISO/IEC 27001.

Кроме того, при подключении и синхронизации электронной почты, календарей и других данных, связанных с электронной почтой, могут возникнуть проблемы с соответствием GDPR, который ограничивает частную информацию, которую вы можете передавать без согласия владельца. Эта информация может содержаться в сообщениях электронной почты, элементах календаря и т. д.

Отсутствие активности учетной записи и удаление паролей из памяти

После трех дней бездействия архитектура Microsoft 365 или Office 365 будет удалять расшифрованный пароль из памяти. После очистки расшифрованного пароля архитектура не может получить доступ к почтовому ящику пользователя в локальной среде. Зашифрованный пароль сохраняется в архитектуре Microsoft 365 или Office 365, но расшифровать его снова невозможно без ключа устройства, доступного только с устройства пользователя.

Учетная запись пользователя может стать неактивной только в трех случаях:

- если пользователь удалит программу Outlook для iOS и Android;
- Обновление фонового приложения отключено в параметрах "Параметры", а затем принудительное закрытие применяется к Outlook.
- если устройство не подключено к Интернету и синхронизация Outlook с Exchange невозможна.

> **Примечание**
>
> Outlook не станет неактивным просто потому, что пользователь не открывает приложение в течение некоторого времени, например в выходные дни или в отпуске. Если включено обновление приложения в фоновом режиме (это настройка Outlook для iOS и Android по умолчанию), обмен push-уведомлениями и фоновая синхронизация электронной почты будут считаться активностью.

Очистка зашифрованных паролей и синхронизированных данных почтового ящика из Microsoft 365 или Office 365

Архитектура На основе Microsoft 365 или Office 365 очищает или удаляет неактивные учетные записи по еженедельной графике. После того как учетная запись пользователя станет неактивной, архитектура будет сбрасывать зашифрованный пароль и все синхронизированное содержимое почтового ящика пользователя из службы.

Сочетание защиты устройства и службы

Уникальный ключ устройства каждого пользователя никогда не хранится в архитектуре на основе Microsoft 365 или Office 365, а пароль пользователя Exchange никогда не сохраняется на устройстве. Эта архитектура означает, что злоумышленнику, чтобы получить доступ к паролю пользователя, ей потребуется как несанкционированный доступ к архитектуре Microsoft 365 или Office 365, так и физический доступ к устройству этого пользователя.

Применяя политики ПИН-кода и шифрование на устройствах в вашей организации, злоумышленнику также придется победить шифрование устройства, чтобы получить доступ к ключу устройства. Это все необходимо сделать до того, как пользователь заметит, что устройство взломано, и запросит его удаленную очистку.

Защита паролем: вопросы и ответы

Ниже приведены часто задаваемые вопросы о структуре и параметрах безопасности Outlook для iOS и Android при использовании с обычной проверкой подлинности.

Хранятся ли учетные данные пользователя в архитектуре Microsoft 365 или на основе Office 365,

если я не могу получить доступ к Exchange Server в Outlook?

Если вы заблокируете доступ Outlook для iOS и Android к вашим локальным серверам Exchange Server, начальное подключение будет отклонено Exchange. Учетные данные пользователя не будут храниться облачной службой Outlook, а учетные данные, представленные в неудачной попытке подключения, немедленно удаляются из памяти.

Как шифруются уникальный ключ устройства и пароль пользователя при передаче в архитектуру на основе Microsoft 365 или Office 365?

Весь обмен данными между приложением Outlook и архитектурой Microsoft 365 или Office 365 осуществляется через зашифрованное подключение TLS. Приложение Outlook может подключаться к архитектуре на основе Microsoft 365 или Office 365 и ничего другого.

Разделы справки удалить учетные данные пользователя и сведения о почтовом ящике из архитектуры microsoft 365 или Office 365?

Пользователь должен удалить Outlook для iOS и Android на всех устройствах. Все данные будут удалены из архитектуры Microsoft 365 или Office 365 примерно через 3–7 дней.

Приложение закрыто или удалено, но оно по-прежнему подключается к моему серверу Exchange Server. С чем это связано?

Архитектура на основе Microsoft 365 или Office 365 расшифровывает пароли пользователей в вычислительной памяти среды выполнения, а затем использует расшифрованные пароли для подключения к Exchange. Так как архитектура подключается к Exchange от имени устройства для получения и кэширования данных почтового ящика, она может продолжаться в течение короткого периода, пока служба не обнаружит, что Outlook больше не запрашивает данные.

Если пользователь удаляет приложение со своего устройства, не используя параметр **Удалить учетную запись**, архитектура Microsoft 365 или Office 365 будет

оставаться на связи с сервером Exchange Server до тех пор, пока учетная запись не станет неактивной, как описано выше в разделе "Бездействие учетной записи и сброс паролей из памяти". Чтобы остановить это действие, следуйте варианту 1 или варианту 3 из приведенных выше часто задаваемых вопросов или заблокируйте приложение, как описано в разделе Блокировка Outlook для iOS и Android.

Является ли пароль пользователя менее надежной защитой при использовании Outlook для iOS и Android, чем при использовании других клиентов Exchange ActiveSync?

Нет. Обычно клиенты EAS хранят учетные данные пользователя локально на его устройстве. Таким образом, если устройство украдено или взломано, злоумышленник может получить доступ к паролю пользователя. При разработке системы безопасности Outlook для iOS и Android злоумышленнику потребуется несанкционированный доступ к архитектуре на основе Microsoft 365 или Office 365 и физический доступ к устройству пользователя.

Что произойдет, если пользователь попытается использовать Outlook для iOS и Android после удаления данных из облачной службы Outlook?

Если учетная запись пользователя становится неактивной (например, при отключении фонового обновления приложения на устройстве или отключении устройства от Интернета в течение некоторого времени), приложение Outlook повторно подключится к архитектуре на основе Microsoft 365 или Office 365 при следующем запуске приложения, а процесс шифрования паролей и кэширования электронной почты перезапускается. Все эти процессы видны пользователю.

Можно ли предотвратить использование обычной проверки подлинности для локальных почтовых ящиков с Outlook для iOS и Android?

Да, можно развернуть гибридную современную проверку подлинности. Дополнительные сведения см. в статье Использование гибридной современной проверки подлинности с Outlook для iOS и Android.

Управление устройствами с Outlook для iOS и Android для Exchange Server

Статья • 04.04.2023

> **Важно!**
>
> Outlook для iOS и Android поддерживает гибридную современную проверку подлинности для локальных почтовых ящиков, что устраняет необходимость использования базовой проверки подлинности. Сведения, содержащиеся в этой статье, относятся только к обычной проверке подлинности. Дополнительные сведения см. в статье **Использование гибридной современной проверки подлинности с Outlook для iOS и Android**.

Корпорация Майкрософт рекомендует Exchange ActiveSync для управления мобильными устройствами, которые используются для доступа к почтовым ящикам Exchange в локальной среде. Exchange ActiveSync — это протокол синхронизации Microsoft Exchange, который предоставляет мобильным телефонам доступ к данным организации на сервере, на котором запущен Microsoft Exchange.

В этой статье рассматриваются конкретные функции и сценарии Exchange ActiveSync для мобильных устройств с Outlook для iOS и Android при проверке подлинности с помощью обычной проверки подлинности. Подробная информация о протоколе синхронизации Microsoft Exchange приведена в статье Служба Exchange ActiveSync. Кроме того, в блоге Office есть информация о принудительном применении паролей и других преимуществах использования Exchange ActiveSync с устройствами с Outlook для iOS и Android.

Политика почтовых ящиков мобильных устройств

Outlook для iOS и Android поддерживает следующие параметры политики почтовых ящиков мобильных устройств в локальной среде Exchange:

- Шифрование устройства включено
- Минимальная длина пароля (только для Android)
- Пароль включен

- Разрешить Bluetooth (используется для управления носимым приложением Outlook для Android)
    - Если allowBluetooth включен (поведение по умолчанию) или настроено для HandsfreeOnly, синхронизация носимых устройств между Outlook на устройстве Android и Outlook на носимых устройствах разрешена для рабочей или учебной учетной записи.
    - Если параметр AllowBluetooth отключен, Outlook для Android отключит синхронизацию между Outlook на устройстве Android и Outlook на носимом устройстве для указанной рабочей или учебной учетной записи (и удалит все данные, синхронизированные ранее для учетной записи). Отключение синхронизации полностью контролируется в самом Outlook; Bluetooth не отключен на устройстве или носимом устройстве, а также не затрагивается любое другое носимое приложение.

> **Примечание**
>
> Outlook для Android запустит поддержку параметра AllowBluetooth, начиная с конца августа.

Сведения о создании или изменении существующей политики почтовых ящиков мобильных устройств см. в разделе Политики почтовых ящиков мобильных устройств.

Блокировка с помощью ПИН-кода и шифрование устройства

Если политика Exchange ActiveSync организации требует использовать пароль для синхронизации электронной почты на мобильных устройствах, Outlook применит эту политику на уровне устройства. Эта функция работает по-разному на устройствах iOS и Android, так как средства, предоставляемые Apple и Google, отличаются.

На устройствах iOS Outlook проверяет, правильно ли задан секретный код или ПИН-код. Если секретный код не задан, Outlook предлагает пользователю создать его в настройках iOS. Пользователь не получит доступ к Outlook для iOS, пока не задаст секретный код.

На устройствах Android Outlook применит правила блокировки экрана. Кроме того, Google предоставляет средства, которые позволяют Outlook для Android соответствовать политикам Exchange в отношении длины и сложности пароля, а

также количества допустимых попыток разблокировки экрана до очистки телефона. Outlook для Android также будет рекомендовать включить шифрование хранилища, если оно отключено, и поможет пользователям задать необходимые настройки.

Устройства iOS и Android, которые не поддерживают эти параметры безопасности, не смогут подключиться к почтовому ящику Exchange.

Шифрование устройства

Устройства iOS поставляются со встроенным шифрованием, которое Outlook использует после включения секретного кода для шифрования всех данных, которые Outlook хранит локально на устройстве iOS. Таким образом, устройства iOS с ПИН-кодом шифруются независимо от того, требуется ли это для политики ActiveSync.

Outlook для Android поддерживает шифрование устройств с помощью политик почтовых ящиков мобильных устройств Exchange. Однако до Android 7.0 доступность и реализация этого процесса зависят от версии ОС Android и производителя устройства, что позволяет пользователю отменять во время процесса шифрования. Благодаря изменениям, введенным Google в Android 7.0, Outlook для Android теперь может применять шифрование на устройствах под управлением Android 7.0 или более поздней версии. Пользователи с устройствами под управлением этих операционных систем не смогут отменить процесс шифрования.

Даже если устройство Android незашифровано и злоумышленник владеет устройством, пока включен ПИН-код устройства, база данных Outlook остается недоступной. Это справедливо даже при включенной отладке по USB и установленном пакете SDK для Android. Если злоумышленник пытается рутировать устройство, чтобы обойти ПИН-код, чтобы получить доступ к этой информации, процесс рутинга очищает все хранилище устройства и удаляет все данные Outlook. Если устройство незашифровано и рутируется пользователем до кражи, злоумышленник может получить доступ к базе данных Outlook, включив отладку по USB на устройстве и подключив устройство к компьютеру с установленным пакетом SDK для Android.

Удаленная очистка с помощью Exchange ActiveSync

Exchange ActiveSync позволяет администраторам удаленно очищать устройства, например, если они скомпрометируются, теряются или украдены. При

использовании Outlook для iOS и Android удаленная очистка очищает только данные в самом приложении Outlook и не активирует полную очистку устройства.

Дополнительные сведения см. в статье Выполнение удаленной очистки на мобильном телефоне .

Политика доступа с устройств

Outlook для iOS и Android должен быть включен по умолчанию, но в некоторых существующих локальных средах Exchange приложение может быть заблокировано по различным причинам. Чтобы стандартизировать доступ пользователей к данным Exchange и использовать Outlook для iOS и Android в качестве единственного почтового приложения, заблокируйте другие почтовые приложения на устройствах пользователей с iOS и Android. Существует два варианта создания этих блоков в локальной среде Exchange: первый вариант блокирует все устройства и разрешает использование Только Outlook для iOS и Android; второй вариант позволяет запретить отдельным устройствам использовать собственные приложения Exchange ActiveSync.

> **Примечание**
>
> Так как идентификаторы устройств не зависят от идентификаторов *физических устройств*, они могут меняться без уведомления. Это может привести к неожиданным последствиям, например разрешенные устройства могут быть неожиданно заблокированы или помещены в карантин Exchange. Поэтому корпорация Майкрософт рекомендует администраторам устанавливать только политики доступа к мобильным устройствам, которые разрешают или блокируют устройства в зависимости от типа или модели устройства.

Способ 1. Блокировка всех почтовых приложений, кроме Outlook для iOS и Android

Вы можете определить правило блока по умолчанию, а затем настроить правило разрешения для Outlook для iOS и Android, а также для устройств Windows с помощью следующих локальных команд PowerShell Exchange. После этого все собственные приложения Exchange ActiveSync, кроме Outlook для iOS и Android, будут заблокированы.

1. Создайте правило блокировки по умолчанию:

```
PowerShell
```

```
Set-ActiveSyncOrganizationSettings -DefaultAccessLevel Block
```

2. Создайте правило, разрешающее Outlook для iOS и Android:

```
PowerShell

New-ActiveSyncDeviceAccessRule -Characteristic DeviceModel -QueryString
"Outlook for iOS and Android" -AccessLevel Allow
```

3. **Необязательно**. Создайте правила, разрешающие Exchange ActiveSync подключения к Outlook на устройствах с Windows (WindowsMail относится к почтовому приложению, включенном в Windows 10).

```
PowerShell

New-ActiveSyncDeviceAccessRule -Characteristic DeviceType -QueryString
"WindowsMail" -AccessLevel Allow
```

Способ 2. Блокировка собственных приложений Exchange ActiveSync на устройствах с Android и iOS

Кроме того, вы можете заблокировать собственные приложения Exchange ActiveSync на определенных устройствах с Android и iOS или других устройствах.

1. Убедитесь, что правила доступа к устройству Exchange ActiveSync не блокируют Outlook для iOS и Android:

```
PowerShell

Get-ActiveSyncDeviceAccessRule | where {$_.AccessLevel -eq "Block" -and
$_.QueryString -like "Outlook*"} | ft Name,AccessLevel,QueryString -
auto
```

   Если такие правила обнаружены, введите следующую команду, чтобы удалить их:

```
PowerShell

Get-ActiveSyncDeviceAccessRule | where {$_.AccessLevel -eq "Block" -and
$_.QueryString -like "Outlook*"} | Remove-ActiveSyncDeviceAccessRule
```

2. Вы можете заблокировать большинство устройств с Android и iOS с помощью следующих команд:

```
PowerShell

New-ActiveSyncDeviceAccessRule -Characteristic DeviceType -QueryString
"Android" -AccessLevel Block
New-ActiveSyncDeviceAccessRule -Characteristic DeviceType -QueryString
"iPad" -AccessLevel Block
New-ActiveSyncDeviceAccessRule -Characteristic DeviceType -QueryString
"iPhone" -AccessLevel Block
New-ActiveSyncDeviceAccessRule -Characteristic DeviceType -QueryString
"iPod" -AccessLevel Block
```

3. Не все производители устройств Android указывают "Android" как тип устройства. Изготовители могут указывать уникальное значение для каждой версии. Чтобы найти другие устройства с Android, которые подключаются к вашей среде, выполните указанную ниже команду, чтобы создать отчет обо всех устройствах, активно взаимодействующих с Exchange ActiveSync.

```
PowerShell

Get-MobileDevice | Select-Object DeviceOS,DeviceModel,DeviceType |
Export-CSV c:\temp\easdevices.csv
```

4. Создайте дополнительные правила блокировки, в зависимости от результатов, полученных на шаге 3. Например, если в вашей среде много устройств HTCOne с Android, вы можете создать правило доступа к устройству Exchange ActiveSync, чтобы пользователи могли применять только Outlook для iOS и Android на этих устройствах. В этом примере введите:

```
PowerShell

New-ActiveSyncDeviceAccessRule -Characteristic DeviceType -QueryString
"HTCOne" -AccessLevel Block
```

> 7 **Примечание**
>
> Параметр QueryString не принимает подстановочные знаки и частичные соответствия.

Дополнительные ресурсы:

- New-ActiveSyncDeviceAccessRule

- Get-MobileDevice
- Set-ActiveSyncOrganizationSettings

Блокировка Outlook для iOS и Android

В разных организациях Exchange действуют разные политики относительно безопасности и управления устройствами. Если приложение Outlook для iOS и Android не соответствует потребностям организации или не является оптимальным решением, администраторы могут заблокировать его. После этого пользователи мобильных устройств Exchange в организации смогут получать доступ к своим почтовым ящикам с помощью встроенных почтовых приложений на iOS и Android.

Командлет `New-ActiveSyncDeviceAccessRule` имеет `Characteristic` параметр, и администраторы могут использовать три `Characteristic` параметра для блокировки приложения Outlook для iOS и Android. The options are UserAgent, DeviceModel, and DeviceType. In the two blocking options described in the following sections, you will use one or more of these characteristic values to restrict the access that Outlook for iOS and Android has to the mailboxes in your organization.

Значения характеристик представлены в таблице ниже.

Развернуть таблицу

Характерные	Строка для iOS	Строка для Android
DeviceModel	Outlook для iOS и Android	Outlook для iOS и Android
DeviceType	Outlook	Outlook
UserAgent	Outlook-iOS-Android/1.0	Outlook-iOS-Android/1.0

С помощью командлета `New-ActiveSyncDeviceAccessRule` можно определить правило доступа к устройству с помощью `DeviceModel` характеристики или `DeviceType` . В обоих случаях правило блокирует доступ к почтовому ящику Exchange через приложение Outlook для iOS и Android с любого устройства на платформе iOS или Android.

Ниже приведены два примера правила доступа к устройству. В первом примере используется `DeviceModel` характеристика, во втором — `DeviceType` характеристика.

PowerShell

```
New-ActiveSyncDeviceAccessRule -Characteristic DeviceType -QueryString
"Outlook" -AccessLevel Block
```

PowerShell

```
New-ActiveSyncDeviceAccessRule -Characteristic DeviceModel -QueryString
"Outlook for iOS and Android" -AccessLevel Block
```

Параметры по умолчанию для виртуальных каталогов Exchange в Exchange Server

Статья • 04.04.2023

Exchange Server 2016 и Exchange Server 2019 автоматически настраивают несколько виртуальных каталогов служб IIS во время установки сервера. В таблицах в следующих разделах показаны параметры служб клиентского доступа (внешний интерфейс) на серверах почтовых ящиков и параметры проверки подлинности IIS по умолчанию и ssl.

Службы клиентского доступа (внешний интерфейс) на серверах почтовых ящиков

В следующей таблице перечислены параметры по умолчанию в службах клиентского доступа (веб-сайте по умолчанию) на серверах почтовых ящиков Exchange.

Виртуальный каталог	**Метод проверки подлинности**	**Параметры SSL**	**Метод управления**
Веб-сайт по умолчанию	Анонимный	Обязательный	Консоль управления IIS
API[1]	Анонимная проверка подлинности Проверка подлинности Windows	Требуется SSL Требуется 128-разрядное шифрование	
aspnet_client	Анонимная проверка подлинности	Требуется SSL Требуется 128-разрядное шифрование	Консоль управления IIS
Автообнаружение	Анонимная проверка подлинности Обычная проверка подлинности Проверка подлинности Windows	Требуется SSL Требуется 128-разрядное шифрование	EAC или командная консоль Exchange

Виртуальный каталог	Метод проверки подлинности	Параметры SSL	Метод управления
ecp	Анонимная проверка подлинности Обычная проверка подлинности	Требуется SSL Требуется 128-разрядное шифрование	EAC или командная консоль Exchange
EWS	Анонимная проверка подлинности Проверка подлинности Windows	Требуется SSL Требуется 128-разрядное шифрование	EAC или командная консоль Exchange
MAPI	Проверка подлинности Windows	Требуется SSL Требуется 128-разрядное шифрование	EAC или командная консоль Exchange
Microsoft-Server-ActiveSync	Обычная проверка подлинности	Требуется SSL Требуется 128-разрядное шифрование	EAC или командная консоль Exchange
OAB	Проверка подлинности Windows	Требуется SSL Требуется 128-разрядное шифрование	EAC или командная консоль Exchange
owa	Обычная проверка подлинности	Требуется SSL Требуется 128-разрядное шифрование	EAC или командная консоль Exchange
PowerShell	По умолчанию все способы проверки подлинности отключены.	Не требуется	EAC или командная консоль Exchange
Rpc	Обычная проверка подлинности Проверка подлинности Windows	Не требуется	EAC или командная консоль Exchange

[1] Виртуальный каталог API доступен в Exchange 2016 CU3 или более поздней версии.

Серверные виртуальные каталоги на серверах почтовых ящиков

В следующей таблице перечислены параметры по умолчанию во внутренних службах на серверах почтовых ящиков Exchange.

Виртуальный каталог	**Метод проверки подлинности**	**Параметры SSL**	**Метод управления**
Серверная часть Exchange	Анонимная проверка подлинности	Требуется SSL Требуется 128-разрядное шифрование	Этот виртуальный каталог не должен быть настроен пользователем.
API[1]	Анонимная проверка подлинности Проверка подлинности Windows	Требуется SSL Требуется 128-разрядное шифрование	Этот виртуальный каталог не должен быть настроен пользователем.
Автообнаружение	Анонимная проверка подлинности Проверка подлинности Windows	Требуется SSL Требуется 128-разрядное шифрование	Этот виртуальный каталог не должен быть настроен пользователем.
ecp	Анонимная проверка подлинности Проверка подлинности Windows	Требуется SSL Требуется 128-разрядное шифрование	Этот виртуальный каталог не должен быть настроен пользователем.
EWS	Анонимная проверка подлинности Проверка подлинности Windows	Требуется SSL Требуется 128-разрядное шифрование	Этот виртуальный каталог не должен быть настроен пользователем.
Microsoft-Server-ActiveSync	Обычная проверка подлинности	Требуется SSL Требуется 128-разрядное шифрование	Этот виртуальный каталог не должен быть настроен пользователем.
OAB	Проверка подлинности Windows	Требуется SSL Требуется 128-разрядное шифрование	Этот виртуальный каталог не должен быть настроен пользователем.

Виртуальный каталог	Метод проверки подлинности	Параметры SSL	Метод управления
owa	Анонимная проверка подлинности Проверка подлинности Windows	Требуется SSL Требуется 128-разрядное шифрование	Этот виртуальный каталог не должен быть настроен пользователем.
PowerShell	Проверка подлинности Windows	Требуется SSL Требуется 128-разрядное шифрование	Этот виртуальный каталог не должен быть настроен пользователем.
Rpc	Проверка подлинности Windows	Не требуется	Этот виртуальный каталог не должен быть настроен пользователем.
RpcWithCert	Проверка подлинности Windows	Не требуется	Этот виртуальный каталог не должен быть настроен пользователем.

[1] Виртуальный каталог API доступен в Exchange 2016 CU3 или более поздней версии.

См. также

Управление виртуальным каталогом

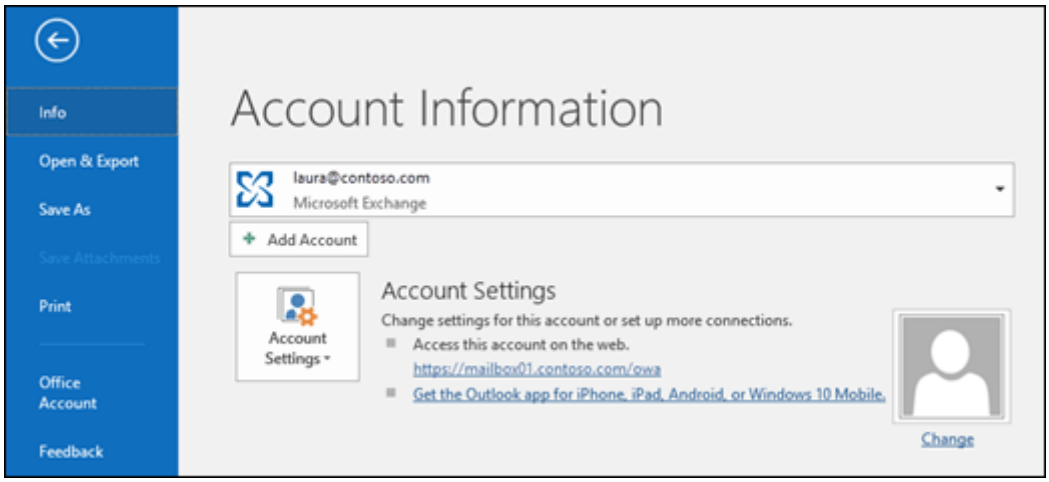
Outlook в Интернете в Exchange Server

Статья • 04.04.2023

Пользовательский интерфейс в Outlook в Интернете (ранее известный как Outlook Web App) для Exchange Server оптимизирован и упрощен для использования с телефонами и планшетами. Поддерживаемые веб-браузеры предоставляют пользователям доступ к дополнительным функциям Outlook. Неподдерживаемые веб-браузеры предоставляют пользователям облегченные версии Outlook в Интернете с меньшим количеством функций. Дополнительные сведения о функциях и поддерживаемых веб-браузерах см. в разделах Outlook в Интернете (ранее Outlook Web App) и Outlook в Интернете (ранее Outlook Web App).

При установке Exchange Server Outlook в Интернете автоматически становится доступным для внутренних пользователей по адресу `https://<ServerName>/owa` (например, `https://mailbox01.contoso.com/owa`). Но вы, скорее всего, захотите настроить Outlook в Интернете для внешнего доступа (например, `https://mail.contoso.com/owa`). Дополнительные сведения см. в разделе Шаг 4. Настройка внешних URL-адресовв статье Настройка потока обработки почты и клиентского доступа на серверах Exchange Server.

В установке Outlook 2010 или более поздней версии, подключенной к почтовому ящику Exchange, url-адрес Outlook в Интернете обычно отображается **в**> разделе Сведения**об**>**учетной записи** в разделе **Параметры учетной записи**.



Outlook в Интернете предоставляется службами клиентского доступа (внешний интерфейс) на серверах почтовых ящиков. В Exchange Server службы клиентского доступа являются частью сервера почтовых ящиков, поэтому вы не можете настроить автономный сервер клиентского доступа, как в предыдущих версиях Exchange. Дополнительные сведения см. в разделе Архитектура протокола клиентского доступа.

Сведения о Outlook в Интернете в Microsoft 365 или Office 365 см. в статье Использование электронной почты в Outlook в Интернете.

Задачи администрирования для управления Outlook в Интернете

В приведенной ниже таблице перечислены задачи настройки и управления, задокументированные для Outlook в Интернете в Outlook 2016.

Статья	Описание
Просмотр и настройка виртуальных каталогов Outlook в Интернете в Exchange Server	Просмотр и настройка свойств Outlook в Интернете для всех пользователей, которые подключаются к серверу.
Настройка перенаправления http-to https для Outlook в Интернете в Exchange Server	Перенаправление незашифрованных HTTP-запросов Outlook в Интернете на HTTPS.
Создание темы для Outlook в Интернете в Exchange Server	В состав Outlook в Интернете входят встроенные темы, которые определяют цвета и значки, используемые в Outlook в Интернете, но вы также можете создавать собственные темы.
Настройка Outlook в Интернете входа, выбора языка и страниц ошибок в Exchange Server	Настройка ключевых страниц в Outlook в Интернете.
Использование проверки подлинности на основе утверждений AD FS с Outlook в Интернете	Централизация проверки подлинности Outlook в Интернете с помощью службы федерации Active Directory (AD FS).

Включение или отключение Outlook в Интернете доступа к почтовым ящикам в Exchange Server

Статья • 04.04.2023

Администраторы могут включить или отключить доступ к почтовому ящику через Outlook в Интернете, используя Центр администрирования Exchange или командную консоль Exchange. По умолчанию доступ к почтовым ящикам через Outlook в Интернете разрешен. Если вы отключите доступ через Outlook в Интернете, пользователи по-прежнему смогут получить доступ к своим почтовым ящикам через Outlook или другие почтовые клиенты.

Дополнительные сведения об управлении доступом пользователей к почтовым ящикам см. в следующих статьях:

- Включение или отключение Exchange ActiveSync доступа к почтовым ящикам в Exchange Server
- Включение или отключение доступа по протоколу POP3 или IMAP4 к почтовым ящикам в Exchange Server
- Включение или отключение доступа MAPI к почтовым ящикам в Exchange Server

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Дополнительные сведения о доступе и использовании Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server.
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Параметры пользователя клиентского доступа" в разделе Разрешения клиентов и мобильных устройств .

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

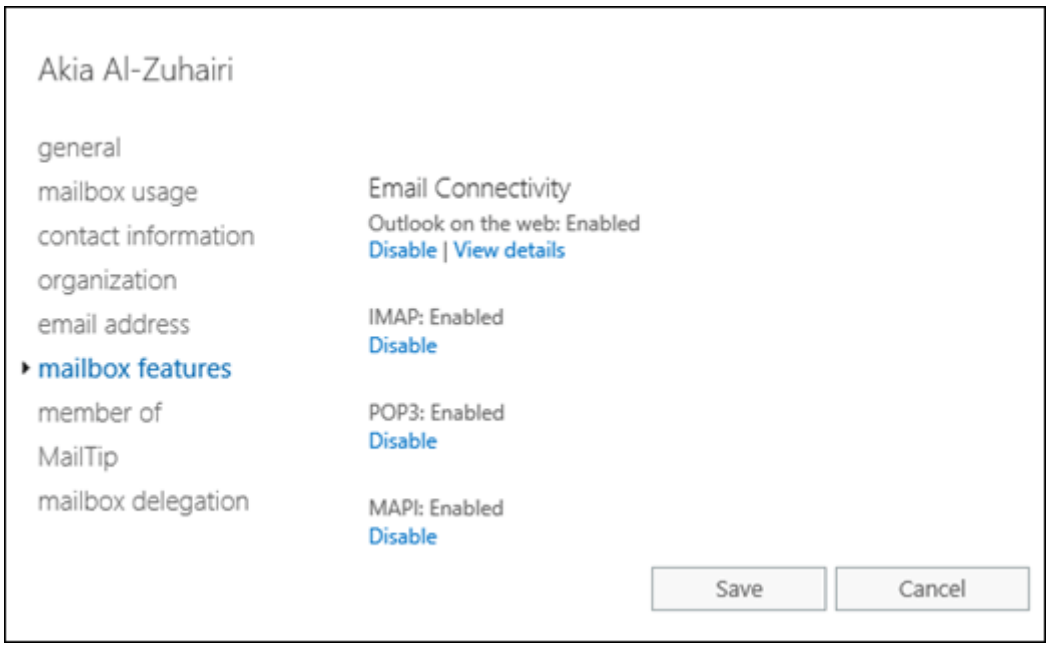
Включение и отключение доступа через Outlook в Интернете к одному почтовому ящику

Включение и отключение доступа через Outlook в Интернете к одному почтовому ящику в Центре администрирования Exchange

1. В EAC перейдите в раздел **Почтовые ящики получателей**>.
2. В списке почтовых ящиков найдите нужный почтовый ящик. Для этого выполните одно из следующих действий:
   - Прокрутите список почтовых ящиков.
   - Щелкните 🔎 введите часть имени пользователя, адреса электронной почты или псевдонима.
   - Щелкните **Значок Дополнительные параметры**••• > **Расширенный поиск** для поиска почтового ящика.

   Найдя почтовый ящик, который требуется изменить, выберите его и нажмите кнопку **Изменить**✏.
3. На открывшейся странице свойств выберите **Функции почтового ящика**.
4. В разделе **Возможность подключения электронной почты** настройте один из таких параметров:
   - Если вы видите **Outlook в Интернете: включено**, щелкните **Отключить**, а затем нажмите кнопку **Да** в появившемся предупреждении.

- Если вы видите **Outlook в Интернете: отключено**, щелкните **Включить**.



По завершении нажмите кнопку **Сохранить**.

Включение и отключение доступа к почтовому ящику через Outlook в Интернете с помощью командной консоли Exchange

Чтобы включить или отключить доступ через Outlook в Интернете к одному почтовому ящику, используйте такой синтаксис:

PowerShell

```
Set-CasMailbox -Identity <MailboxIdentity> -OWAEnabled <$true | $false>
```

В этом примере отключается доступ через Outlook в Интернете к почтовому ящику Yan Li.

PowerShell

```
Set-CasMailbox -Identity "Yan Li" -OWAEnabled $false
```

В этом примере включается доступ через Outlook в Интернете к почтовому ящику Elly Nkya.

PowerShell

```
Set-CasMailbox -Identity "Elly Nkya" -OWAEnabled $true
```

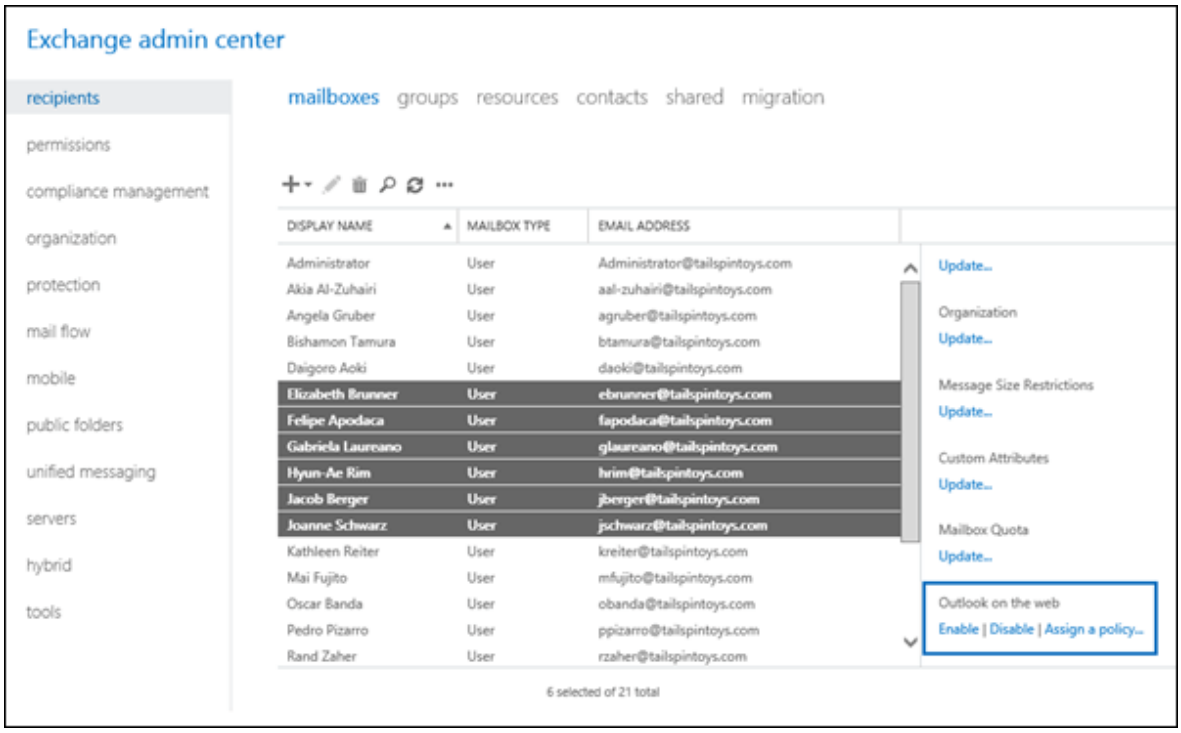
Дополнительные сведения о синтаксисе и параметрах см. в статье Set-CASMailbox.

Включение и отключение доступа через Outlook в Интернете к нескольким почтовым ящикам

Включение и отключение доступа через Outlook в Интернете к нескольким почтовым ящикам в Центре администрирования Exchange

1. В EAC перейдите в раздел **Почтовые ящики получателей**>.
2. В списке почтовых ящиков найдите нужные почтовые ящики. Для этого выполните одно из следующих действий:
   - Прокрутите список почтовых ящиков.
   - Щелкните 🔎 введите часть имени пользователя, адреса электронной почты или псевдонима.
   - Щелкните **Значок Дополнительные параметры**••• > **Расширенный поиск** для поиска почтового ящика.
3. В списке почтовых ящиков выберите несколько почтовых ящиков одного типа (например, **Пользователь**). Например:
   - Выберите почтовый ящик. Удерживая клавишу SHIFT, выберите другой ящик, расположенный ниже в списке.
   - Выберите нужные почтовые ящики, удерживая клавишу CTRL.

   После выбора нескольких почтовых ящиков одного типа заголовок области сведений изменится на **Массовое изменение**.
4. В области сведений найдите **Outlook в Интернете**, щелкните **Включить** или **Отключить**, а затем нажмите **ОК** в появившемся предупреждении.



Включение и отключение доступа через Outlook в Интернете к нескольким почтовым ящикам с помощью командной консоли Exchange

Чтобы указать нужные почтовые ящики, можно использовать командлеты **Get-Mailbox**, **Get-User** или **Get-Content**. Например:

- Используйте параметр *OrganizationalUnit* для фильтрации почтовых ящиков по подразделениям.
- Используйте параметр *Filter* для создания фильтров OPATH, определяющих почтовые ящики. Дополнительные сведения см. в статье Filterable Properties for the -Filter Parameter.
- Используйте текстовый файл для указания почтовых ящиков. В каждой строке текстового файла указан один почтовый ящик (адрес электронной почты, имя или другой уникальный идентификатор), например:

  > ebrunner@tailspintoys.com
  > fapodaca@tailspintoys.com
  > glaureano@tailspintoys.com
  > hrim@tailspintoys.com

В этом примере отключается доступ через Outlook в Интернете ко всем почтовым ящикам пользователей в североамериканском финансовом подразделении.

PowerShell

```
$NAFinance = Get-Mailbox -OrganizationalUnit "OU=Marketing,OU=North America,DC=contoso,DC=com" -Filter "RecipientTypeDetails -eq 'UserMailbox'" -ResultSize Unlimited; $NAFinance | foreach  {Set-CasMailbox  $_.Identity -OWAEnabled $false}
```

В этом примере отключается доступ через Outlook в Интернете ко всем почтовым ящикам пользователей в проектном отделе штата Вашингтон.

PowerShell

```
Get-User -Filter "RecipientType -eq 'UserMailbox' -and Department -like 'Engineering*' -and StateOrProvince -eq 'WA'" | Set-CasMailbox -OWAEnabled $false
```

В этом примере для отключения доступа через Outlook в Интернете к указанным почтовым ящикам используется текстовый файл C:\My Documents\Accounts.txt.

PowerShell

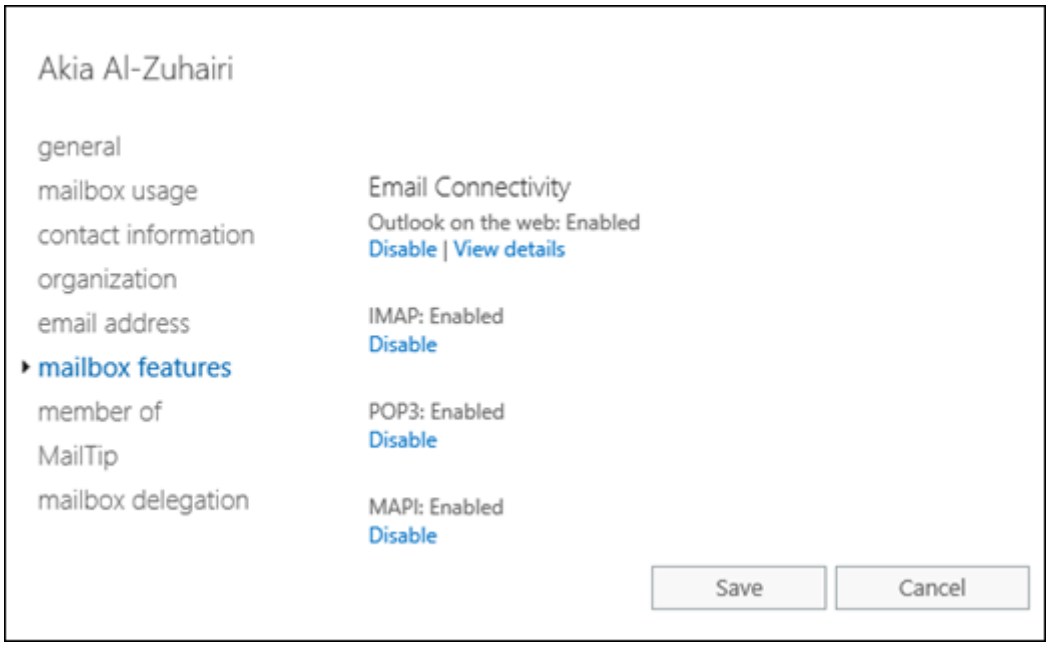
```
Get-Content "C:\My Documents\Accounts.txt" | foreach {Set-CasMailbox $_ -OWAEnabled $false}
```

Дополнительные сведения о синтаксисе и параметрах см. в статьях Get-Mailbox и Get-User.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно включили или отключили доступ к почтовому ящику через Outlook в Интернете, выполните одно из следующих действий:

- В EAC перейдите в раздел Почтовые**ящики**>**получателей**>, выберите почтовый ящик > щелкните ✎>**Функции почтового ящика** и проверьте значение **Outlook в Интернете** в разделе **подключение Email**.



- В командной консоли Exchange *замените*< *MailboxIdentity*> удостоверением почтового ящика (например, именем, псевдонимом или адресом электронной почты) и выполните следующую команду:

```
PowerShell

Get-CasMailbox -Identity "<MailboxIdentity>"
```

- Используйте тот же фильтр, что и для определения почтовых ящиков, но вместо командлета **Get-CasMailbox** используйте **Set-CasMailbox**. Например:

```
PowerShell

Get-User -Filter "RecipientType -eq 'UserMailbox' -and Department -like
'Engineering*' -and StateOrProvince -eq 'WA'" | Get-CasMailbox
```

- Чтобы увидеть все почтовые ящики, для которых отключен доступ по протоколу Outlook в Интернете, выполните следующую команду в командной консоли Exchange:

```
PowerShell

Get-CasMailbox -ResultSize unlimited -Filter "OWAEnabled -eq `$false"
```

Просмотр и настройка виртуальных каталогов Outlook в Интернете в Exchange Server

Статья • 04.04.2023

Для просмотра и изменения свойств виртуального каталога Outlook в Интернете (прежнее название — можно использовать Центр администрирования Exchange или командную консоль Exchange. Несмотря на то что название изменилось на Outlook в Интернете, имя виртуального каталога осталось прежним (owa).

Что нужно знать перед началом работы

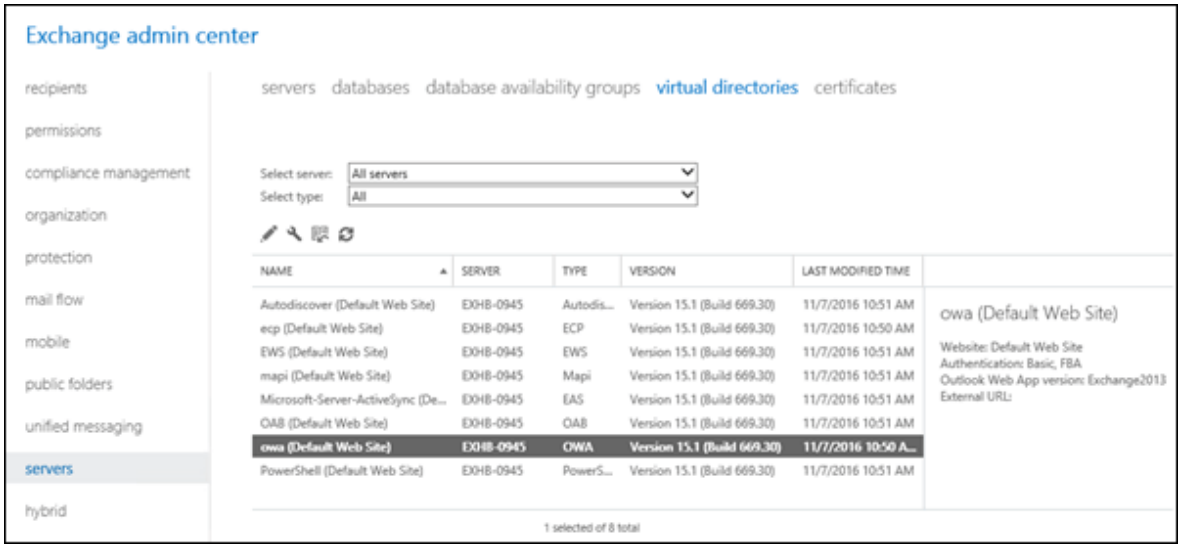
- Предполагаемое время для завершения каждой процедуры: 10 минут.
- Дополнительные сведения о EAC см. в разделе . Центр администрирования Exchange в Exchange Server. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Теперь для шифрования данных, которыми обмениваются компьютерные системы, используется протокол TLS вместо протокола SSL. Они настолько тесно связаны, что термины "SSL" и "TLS" (без версий) часто используются взаимозаменяемо. Из-за этого сходства ссылки на "SSL" в разделах Exchange, Центре администрирования Exchange и командной консоли Exchange часто используются для охвата протоколов SSL и TLS. Как правило, термин "SSL" обозначает именно протокол SSL только в тех случаях, когда указан номер версии (например, SSL 3.0). Чтобы узнать, почему следует отключить протокол SSL и переключиться на TLS, см. статью Защита от уязвимости SSL 3.0.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Outlook в Интернете виртуальных каталогов" в разделе Разрешения для клиентов и мобильных устройств.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Просмотр и настройка свойств виртуального каталога Outlook в Интернете в Центре администрирования Exchange

1. В EAC перейдите в раздел **Серверы**>**Виртуальные каталоги**.



2. Выберите нужный виртуальный каталог Outlook в Интернете.

   - С помощью раскрывающегося списка **Выбрать сервер** можно отфильтровать серверы Exchange Server по имени.
   - Чтобы отобразить только виртуальные каталоги Outlook в Интернете, выберите **OWA** в раскрывающемся списке **Выбрать тип**.

   После выбора виртуального каталога на панели функций можно увидеть следующие свойства и значения:

   - **Веб-сайт** (только для чтения). Веб-сайт по умолчанию называется **веб-сайтом по умолчанию**.
   - **Проверка подлинности**. По умолчанию используются методы проверки подлинности **Basic** и **FBA** (проверка подлинности на основе форм).
   - **версия Outlook в Интернете**: версия по умолчанию — `Exchange2013`.
   - **Внешний URL-адрес**: значение по умолчанию пустое (не настроено).

3. Чтобы просмотреть дополнительные свойства или изменить параметры, которые не доступны только для чтения, нажмите кнопку **Изменить** (✎ Доступные вкладки и параметры

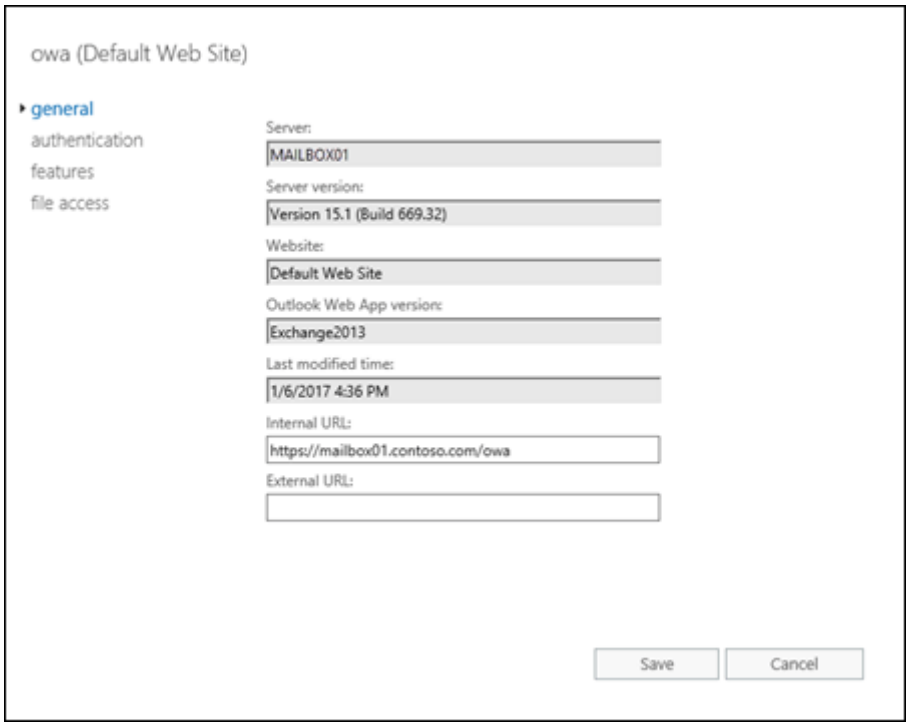
   - Вкладка **Общие**

     - **Внутренний URL-адрес**: URL-адрес, используемый для доступа к Outlook в Интернете из внутренней сети. Это значение настраивается автоматически во время настройки Exchange Server, а значение по умолчанию — `https:// _<Server FQDN>_/owa` (например, https://mailbox01.contoso.com/owa).

     - **Внешний URL-адрес**: URL-адрес, используемый для доступа к Outlook в Интернете из Интернета. Значение по умолчанию не задано.

       Для серверов Exchange Server с выходом в Интернет это значение, которое клиенты используют для доступа к Outlook в Интернете. Сведения о настройке этого параметра см. в разделе Настройка внешнего URL-адреса для Outlook в Интернете в Центре администрирования Exchange.

       Для серверов Exchange Server, не имеющих выхода в Интернет, значение параметра **Внешний URL-адрес** не указывается.



   - Вкладка **Проверка подлинности**

     - **Используйте один или несколько стандартных методов проверки подлинности**. Выберите этот параметр, чтобы использовать один или

несколько из следующих методов проверки подлинности:

- **Интегрированная проверка подлинности Windows**. Для этого метода требуется, чтобы у пользователей была действительная учетная запись пользователя Active Directory, а клиентский компьютер является членом того же домена, что и сервер Exchange Server (или домен, которому доверяет домен сервера Exchange Server). У пользователей не запрашиваются имена и пароли учетных записей. Вместо этого сервер согласовывает с пакетами безопасности Windows, установленными на клиентском компьютере. Незашифрованные данные не передаются по сети.

- **Дайджест-проверка подлинности для серверов домена Windows**. Для этого метода требуется, чтобы у пользователей была действительная учетная запись пользователя Active Directory. Пароли передаются по сети в виде значения хэша, что обеспечивает дополнительную безопасность.

- **Обычная проверка подлинности (пароль отправляется в виде ясного текста):** это значение по умолчанию. При использовании обычной проверки подлинности необходимо требовать зашифрованные подключения TLS между клиентскими компьютерами и сервером Exchange Server.

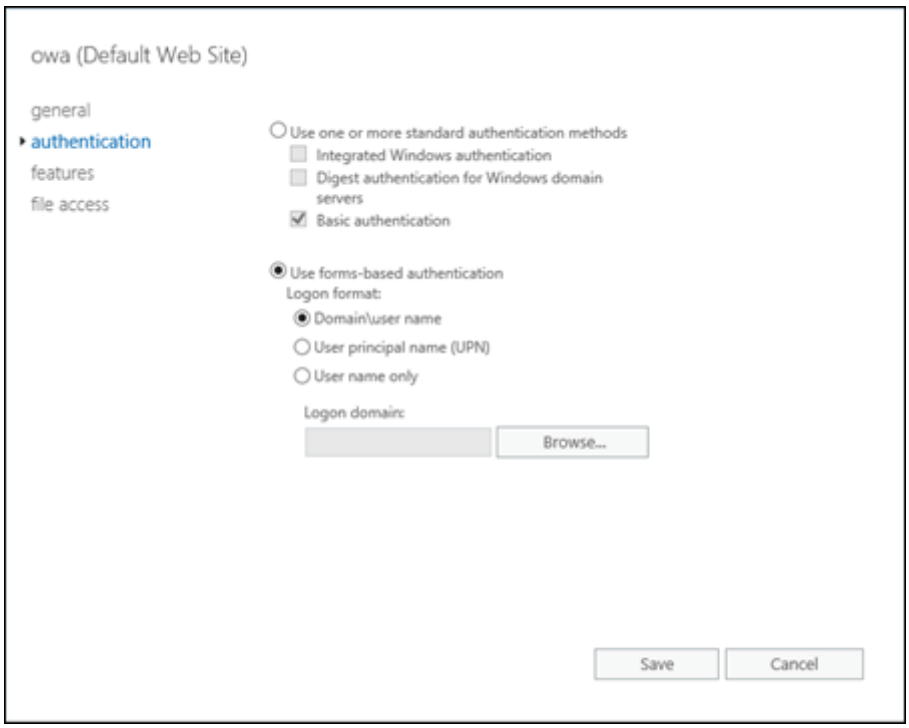
- **Использование проверки подлинности на основе форм**. Проверка подлинности на основе форм обеспечивает повышенную безопасность и позволяет настроить тип запроса, используемого для входа. Однако при проверке подлинности на основе форм безопасный канал не предоставляется, если не включен протокол TLS.

  Выберите один из приведенных ниже форматов входа, который будет использоваться при проверке подлинности на основе форм. В примерах используется учетная запись пользователя Мария Сазонова в домене contoso.com.

  - **Домен\имя пользователя** Например, CONTOSO\VBarrios. Это значение используется по умолчанию.

  - **Имя участника-пользователя (UPN)** Например, vbarrios@contoso.com. Обратите внимание, что если имя участника-пользователя не соответствует адресу электронной почты, пользователи не смогут получить доступ к Outlook в Интернете с помощью этого метода.

- **Только имя пользователя** Например, VBarrios. В этом случае необходимо настроить домен по умолчанию, используемый со всеми именами пользователей. Нажмите кнопку **Обзор** в свойстве **Домен входа** , чтобы выбрать домен Active Directory по умолчанию. Если пользователь не является членом указанного домена, он должен ввести домен и имя пользователя при входе.



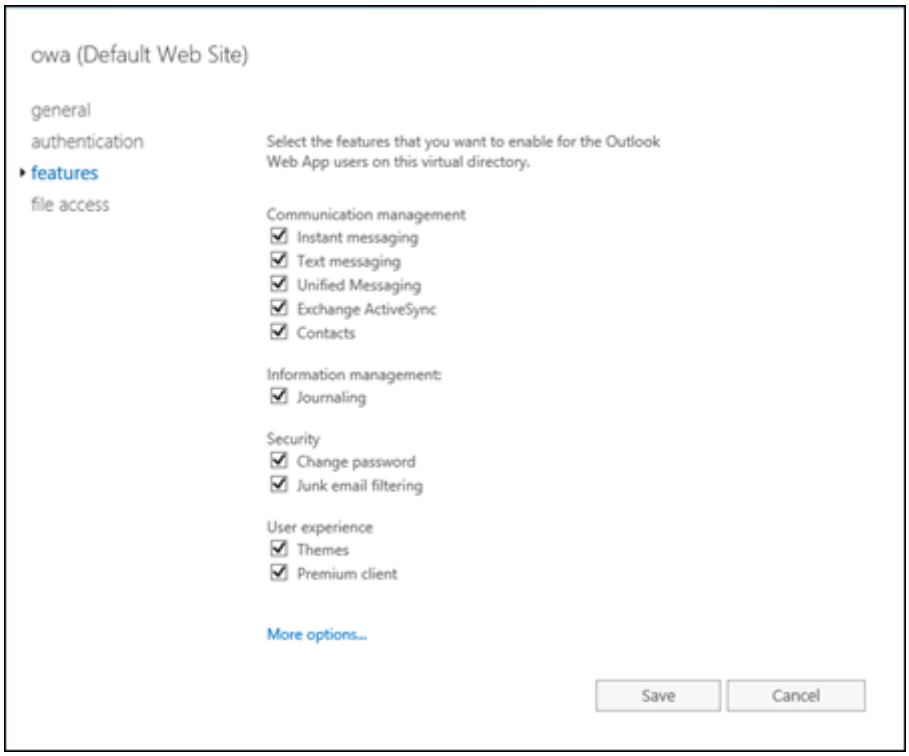
- Вкладка **Функции**

  Эти параметры влияют на всех пользователей, подключающихся к виртуальному каталогу Outlook в Интернете. Настраиваемые параметры Outlook в Интернете можно настроить для определенных пользователей или групп пользователей с помощью политик почтовых ящиков Outlook в Интернете. Дополнительные сведения см. в разделе Просмотр или настройка свойств политики почтовых ящиков Outlook в Интернете.

  - **Управление связью**
  - **Обмен мгновенными сообщениями**
  - **Обмен текстовыми сообщениями**
  - **Единая система обмена сообщениями**: (только в Exchange 2016; недоступно в Exchange 2019)
  - **Exchange ActiveSync**
  - **Контакты**

- **Все списки адресов***
- **Управление данными**
- **Ведение журнала**
- **Правила для папки "Входящие"***
- **Восстановление удаленных элементов***. Отключение этого параметра не влияет на хранение удаленных элементов для почтовых ящиков; пользователи не могут просматривать или восстанавливать удаленные элементы в Outlook в Интернете.
- **Безопасность**
- **Смена пароля**
- **Фильтрация нежелательной почты**: этот параметр не включает или отключает правило нежелательной почты в почтовых ящиках; он управляет *доступностью* параметров нежелательной почты для пользователей в Outlook в Интернете. Дополнительные сведения о правиле нежелательной почты и ее фильтрации в почтовых ящиках см. в статье Configure Exchange antispam settings on mailboxes.
- **Взаимодействие с пользователем**
- **Темы**
- **Клиент уровня "Премиум".** Если этот параметр снят, стандартная версия Outlook в Интернете (ранее известная как премиум-версия Outlook Web App) отключена, и все клиенты будут вынуждены использовать облегченные версии Outlook в Интернете.
- **Подпись электронной почты***
- **Управление временем***
- **Календарь***
- **Задачи***
- **Напоминания и уведомления***

* Эти параметры доступны после нажатия кнопки **Дополнительные параметры**.

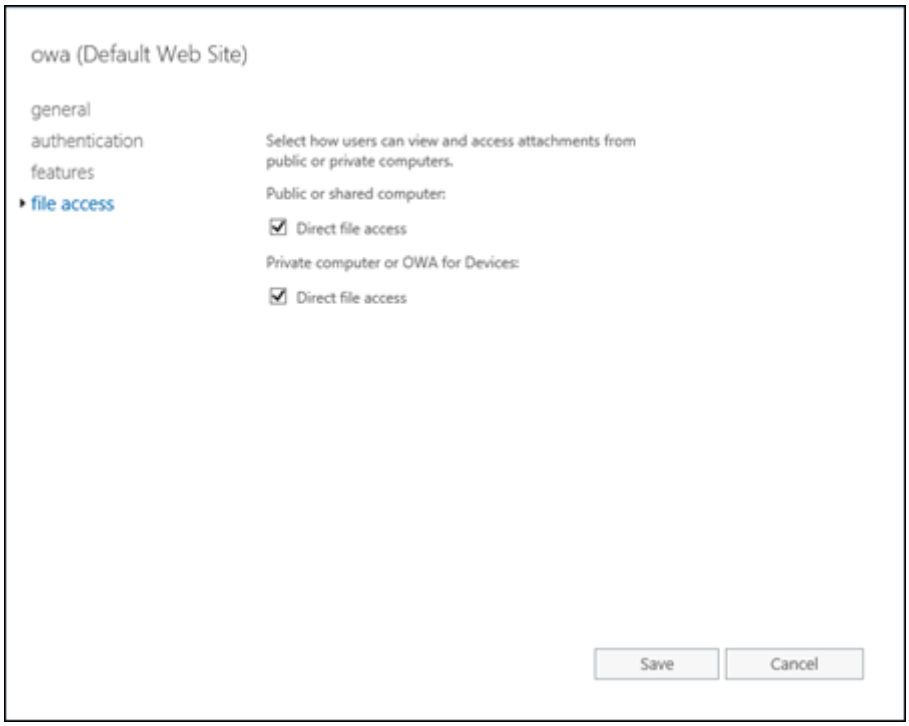


- Вкладка **Доступ к файлам**

  Параметры прямого доступа к файлам на этой странице влияют на обычные вложения, которые открываются или сохраняются щелчком, и MIME-файлы (обычно файлы изображений), внедренные в сообщение. Отключение прямого доступа к файлам не повлияет на доступ к файлам в других клиентах электронной почты (например, в Outlook) и в Outlook в Интернете при использовании других методов доступа (например, доступ к веб-документам, предоставляемый Office Online Server, и доступ по ссылкам на файлы в облаке).

  Обратите внимание: пользователи могут выбрать тип доступа в Outlook в Интернете (частный или общедоступный компьютер), только когда настроена проверка подлинности на основе форм. Все остальные способы проверки подлинности автоматически предполагают доступ с частного компьютера.

  - **Прямой доступ к файлам** для общедоступных компьютеров или компьютеров с общим доступом.
  - **Прямой доступ к файлам** для частных компьютеров.

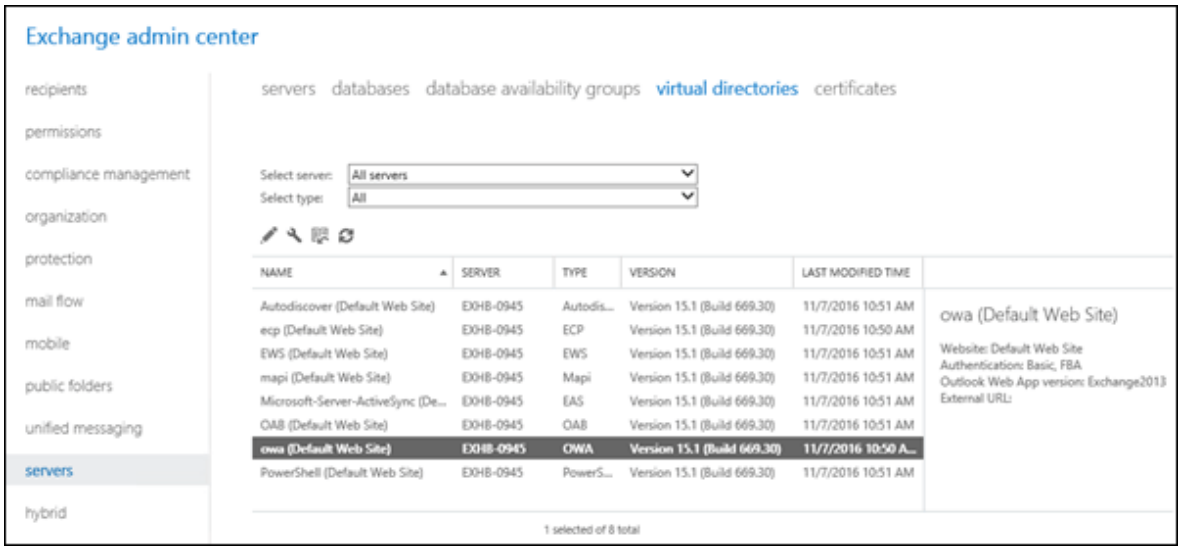


4. Если вы меняли какие-либо параметры виртуального каталога, нажмите **Сохранить**. Если вы просто просматривали их, нажмите **Отмена**.

Настройка внешнего URL-адреса для Outlook в Интернете в Центре администрирования Exchange

1. В EAC перейдите в раздел **Серверы**>**Виртуальные каталоги**, выберите Outlook в Интернете виртуальный каталог, который требуется просмотреть или настроить, а затем нажмите кнопку **Настроить** (🔧

    - С помощью раскрывающегося списка **Выбрать сервер** можно отфильтровать серверы Exchange Server по имени.
    - Чтобы отобразить только виртуальные каталоги Outlook в Интернете, выберите **OWA** в раскрывающемся списке **Выбрать тип**.

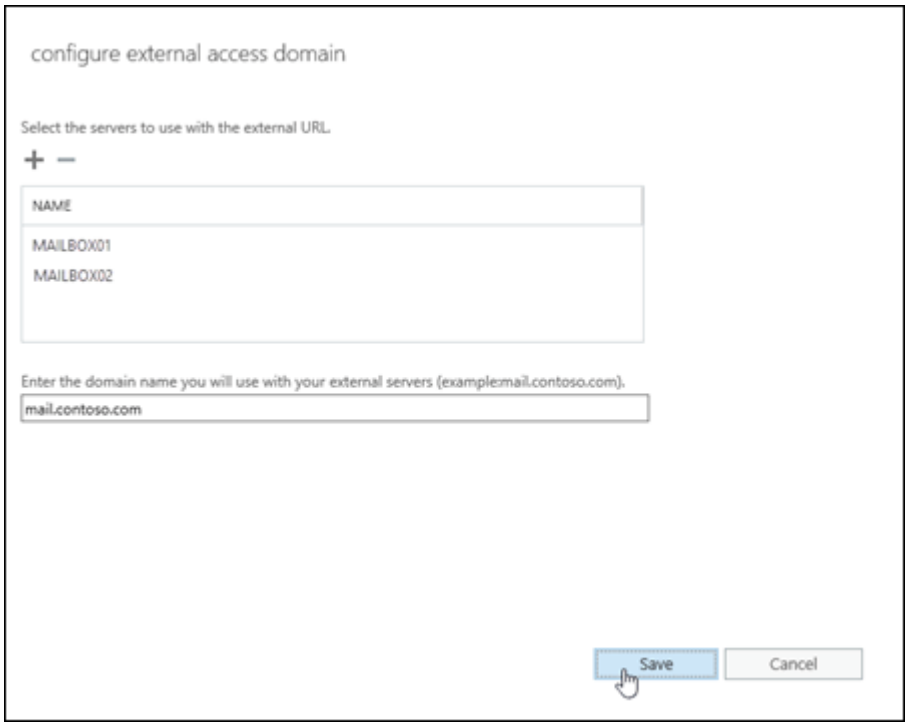


2. На открывшейся странице **Настроить домен внешнего доступа** настройте следующие параметры:

   - **Выберите серверы для использования с внешним URL-адресом**. Щелкните **Добавить** (➕ и выберите один или несколько серверов Exchange, которые внешние клиенты будут использовать для подключения к Outlook в Интернете (не выбирайте внутренние только серверы).

   - **Введите доменное имя, которое будет использоваться с внешними серверами**. Введите полное доменное имя, которое внешние клиенты будут использовать для подключения к Outlook в Интернете (например, mail.contoso.com). Обратите внимание: это значение должно быть настроено и разрешимо в общедоступном DNS вашей организации.

   По завершении нажмите кнопку **Сохранить**.



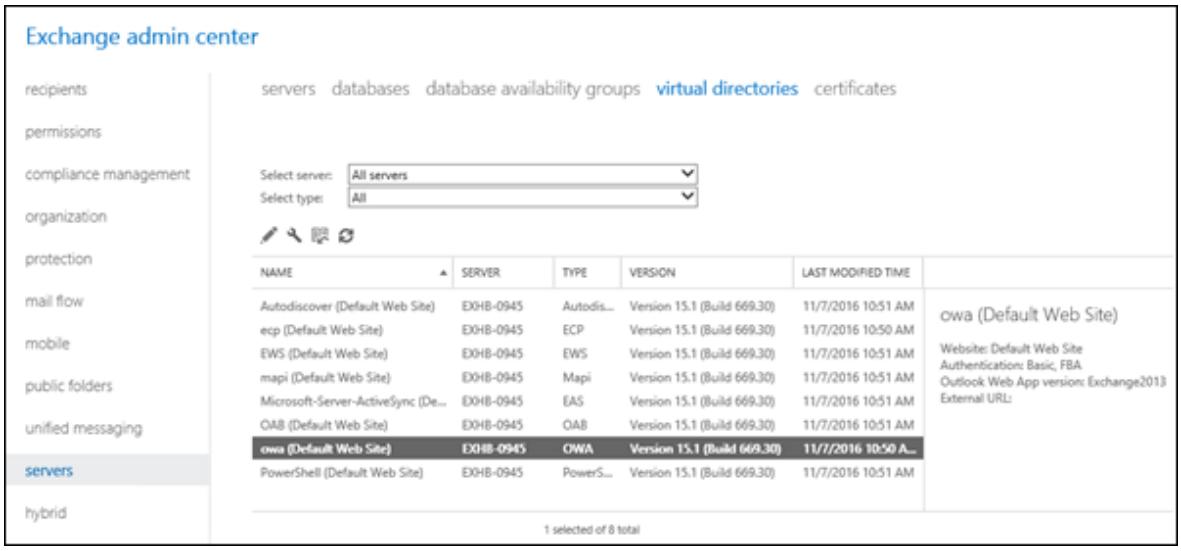
Сброс виртуального каталога Outlook в Интернете

Если вас не удовлетворяет работа виртуального каталога Outlook в Интернете, его можно сбросить. Виртуальный каталог удаляется, и создается новый каталог с параметрами по умолчанию. Несмотря на то что все настройки будут утрачены, необходимо выбрать расположение для текстового документа, в который будут скопированы текущие параметры.

1. В EAC перейдите в раздел **Серверы**>**Виртуальные каталоги**, выберите Outlook в Интернете виртуальный каталог, который требуется просмотреть или настроить, а затем нажмите кнопку **Сброс** (

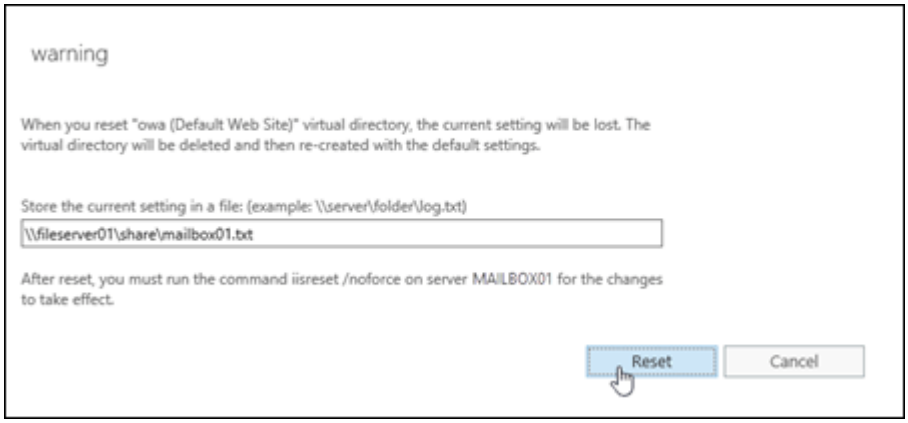
    - С помощью раскрывающегося списка **Выбрать сервер** можно отфильтровать серверы Exchange Server по имени.

    - Чтобы отобразить только виртуальные каталоги Outlook в Интернете, выберите **OWA** в раскрывающемся списке **Выбрать тип**.



2. На открывающейся странице **Предупреждение** укажите UNC-путь к файлу, чтобы сохранить текущие параметры виртуального каталога (например, \ <*Server*>\ <*Share*>\owavdir.txt или \ <*LocalServerName*>\c$\owavdir.txt).

   Когда закончите, нажмите **Сохранить**.



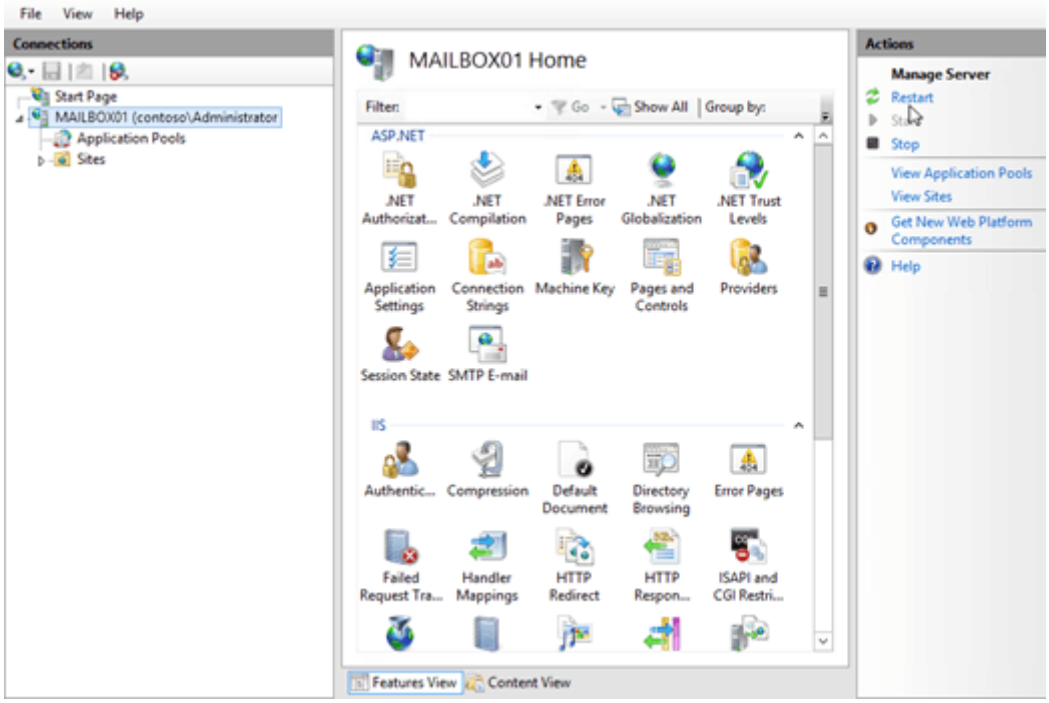
3. Перезапустите IIS одним из указанных ниже способов.

   - Диспетчер IIS

     a. Откройте диспетчер IIS на сервере Exchange Server. Простой способ сделать это в Windows Server 2012 или более поздней версии — нажать клавишу Windows + Q, ввести inetmgr и выбрать **Диспетчер служб IIS** в результатах.

     b. В диспетчере IIS выберите сервер.

     c. В области **Действия** выберите элемент **Перезапустить**.



- Командная строка

Откройте командную строку с повышенными привилегиями на сервере Exchange Server (открываемое окно командной строки, выбрав **Запуск от имени администратора**) и выполните следующие команды:

Консоль

```
net stop w3svc /y
```

Консоль

```
net start w3svc
```

Просмотр свойств виртуального каталога Outlook в Интернете с помощью командной консоли Exchange

Чтобы просмотреть свойства виртуальных каталогов Outlook в Интернете с помощью командной консоли Exchange, используйте следующий синтаксис:

PowerShell

```
Get-OWAVirtualDirectory [-Identity "<ExchangeServer>\owa <Website>"]
```

В этом примере возвращается сводный список всех Outlook в Интернете виртуальных каталогов на всех серверах Exchange в организации.

PowerShell

```
Get-OWAVirtualDirectory
```

В этом примере возвращаются подробные сведения о виртуальном каталоге Outlook в Интернете на веб-сайте по умолчанию на сервере Exchange Server Mailbox01.

PowerShell

```
Get-OWAVirtualDirectory -Identity "Mailbox01\owa (Default Web Site)" |
Format-List
```

В этом примере возвращаются настройки и способы проверки подлинности для того же виртуального каталога.

PowerShell

```
Get-OWAVirtualDirectory -Identity "Mailbox01\owa (Default Web Site)" |
Format-List *Authentication*
```

Примечание. Не все параметры применимы к Exchange 2016 или Exchange 2019 (например, **SpellCheckerEnabled**).

Дополнительные сведения о синтаксисе и параметрах см. в разделе Get-OWAVirtualDirectory.

Настройка параметров виртуальных каталогов Outlook в Интернете с помощью командной консоли Exchange

В командной консоли Exchange (командлет **Set-OwaVirtualDirectory**) доступно гораздо больше параметров конфигурации для виртуальных каталогов Outlook в Интернете, чем в Центре администрирования Exchange. Ниже перечислены параметры виртуального каталога Outlook в Интернете, доступные только в командной консоли Exchange.

Параметр	Функция

Параметр	Функция
AllowedFileTypes *BlockedFileTypes* *ForceSaveFileTypes* *AllowedMimeTypes* *BlockedMimeTypes* *ForceSaveMimeTypes* *ActionForUnknownFileAndMIMETypes*	Определение типов файлов для прямого доступа (обычные вложения и внедренные MIME-файлы) в Outlook в Интернете (но не в других клиентах электронной почты).
DefaultTheme	Определение темы по умолчанию, использующейся в Outlook в Интернете.
LogonAndErrorLanguage *OutboundCharset* *UseGB18030* *UseISO885915*	Настройка различных языковых параметров для Outlook в Интернете.
DisplayPhotosEnabled *SetPhotoEnabled* *SetPhotoURL*	Настройка параметров фотографий пользователя в Outlook в Интернете.

Примечание. Не все доступные параметры применяются к Exchange 2016 или Exchange 2019 (например, *SpellCheckerEnabled*).

Для настройки свойств виртуальных каталогов Outlook в Интернете с помощью командной консоли Exchange используйте следующий синтаксис:

PowerShell

```
Set-OWAVirtualDirectory -Identity "<ExchangeServer>\owa <Website>"
<Settings>
```

В этом примере настраивается блокировка файлов, типы которых не указаны в списке разрешений (действие по умолчанию — "разрешить").

PowerShell

```
Set-OwaVirtualDirectory -Identity "Contoso\owa (Default Web Site)" -
ActionForUnknownFileAndMIMETypes Block
```

Подробные сведения о синтаксисе и параметрах см. в статье Set-OwaVirtualDirectory.

Настройка перенаправления http-to https для Outlook в Интернете в Exchange Server

Статья • 04.04.2023

По умолчанию в Exchange Server URL-адрес `https://<ServerName>` перенаправляет пользователей на `https://<ServerName>/owa`. Но если кто-либо попытается получить доступ к Outlook в Интернете (ранее известной как Outlook Web App) с помощью `http://<ServerName>` или `http://<ServerName>/owa`, он получит ошибку.

Вы можете настроить перенаправление HTTP для Outlook в Интернете таким образом, чтобы запросы для `http://<ServerName>` или `http://<ServerName>/owa` автоматически перенаправлялись в `https://*<ServerName>*/owa`. Для этого в Службы IIS (IIS) необходимо выполнить приведенные ниже действия по настройке.

1. Удалите параметр **Требовать SSL** для веб-сайта по умолчанию.
2. Восстановите параметр **Требовать SSL** для других виртуальных каталогов на веб-сайте по умолчанию, где этот параметр был включен по умолчанию (кроме каталога /owa).
3. Настройте веб-сайт по умолчанию на перенаправление HTTP-запросов к виртуальному каталогу /owa.
4. Отключите перенаправление HTTP для всех виртуальных каталогов на веб-сайте по умолчанию (включая каталог /owa).
5. Чтобы изменения вступили в силу, перезагрузите службы IIS.

Параметры перенаправления SSL и HTTP по умолчанию для всех виртуальных каталогов на веб-сайте по умолчанию см. в разделе Требовать SSL и перенаправление HTTP по умолчанию на веб-сайте по умолчанию на сервере Exchange Server в конце этой статьи.

Что нужно знать перед началом работы

- Предполагаемое время выполнения процедуры: 15 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Диспетчер

IIS" в разделе Outlook в Интернете разрешений раздела Разрешения клиентов и мобильных устройств.

- Процедуры, описанные в этом разделе, могут привести к созданию файла web.config в папке `%ExchangeInstallPath%ClientAccess\OAB`. Если в дальнейшем отключить перенаправление HTTP для Outlook в Интернете, Outlook может зависать, когда пользователи выбирают команду **Отправка и получение**. Чтобы предотвратить замораживание Outlook после удаления перенаправления HTTP, удалите файл web.config в `%ExchangeInstallPath%ClientAccess\OAB`.

- Теперь для шифрования данных, которыми обмениваются компьютерные системы, используется протокол TLS вместо протокола SSL. Они настолько тесно связаны, что термины "SSL" и "TLS" (без версий) часто используются взаимозаменяемо. Из-за этого сходства ссылки на "SSL" в разделах Exchange, Центре администрирования Exchange и командной консоли Exchange часто используются для охвата протоколов SSL и TLS. Как правило, термин "SSL" обозначает именно протокол SSL только в тех случаях, когда указан номер версии (например, SSL 3.0). Чтобы узнать, почему следует отключить протокол SSL и переключиться на TLS, см. статью Защита от уязвимости SSL 3.0.

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

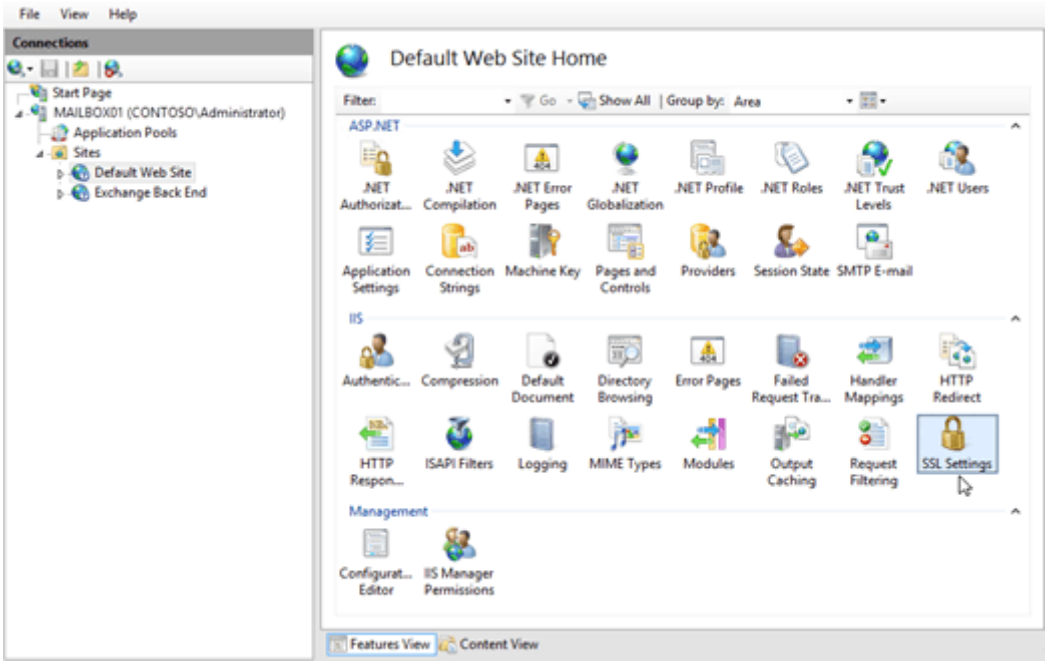
Этап 1. Удаление параметра "Требовать SSL" для веб-сайта по умолчанию с помощью диспетчера служб IIS

1. Откройте диспетчер IIS на сервере Exchange Server. Простой способ сделать это в Windows Server 2012 или более поздней версии — нажать клавишу Windows + Q, ввести inetmgr и выбрать **Диспетчер служб IIS** в результатах.

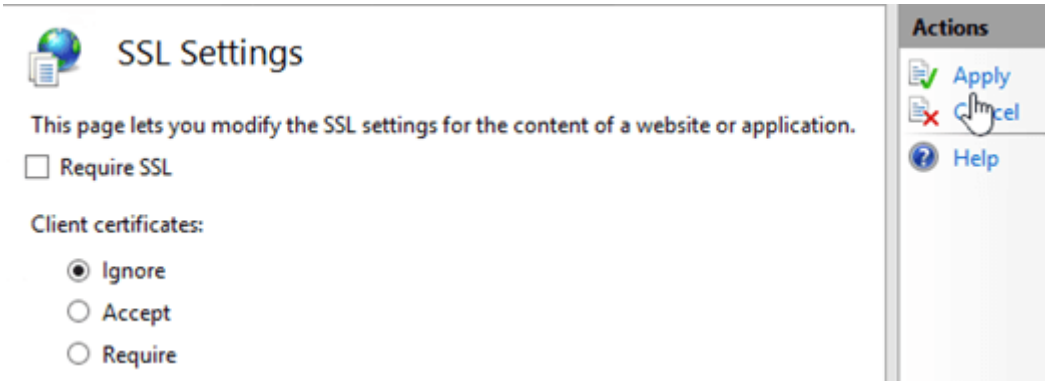
2. Разверните узел сервера, а затем — раздел **Сайты**.

3. Выберите **Веб-сайт по умолчанию**. и убедитесь, что в нижней части страницы выбран пункт **Представление функций** .

4. В разделе **IIS** дважды щелкните элемент **Параметры SSL**.



5. На странице **Параметры SSL** снимите флажок **Требовать SSL**, а затем на панели **Действия** нажмите кнопку **Применить**.



Примечание. Чтобы выполнить эту процедуру в командной строке, откройте командную строку с повышенными привилегиями на сервере Exchange Server (для этого выберите **Запуск от имени администратора**) и выполните следующую команду:

Консоль

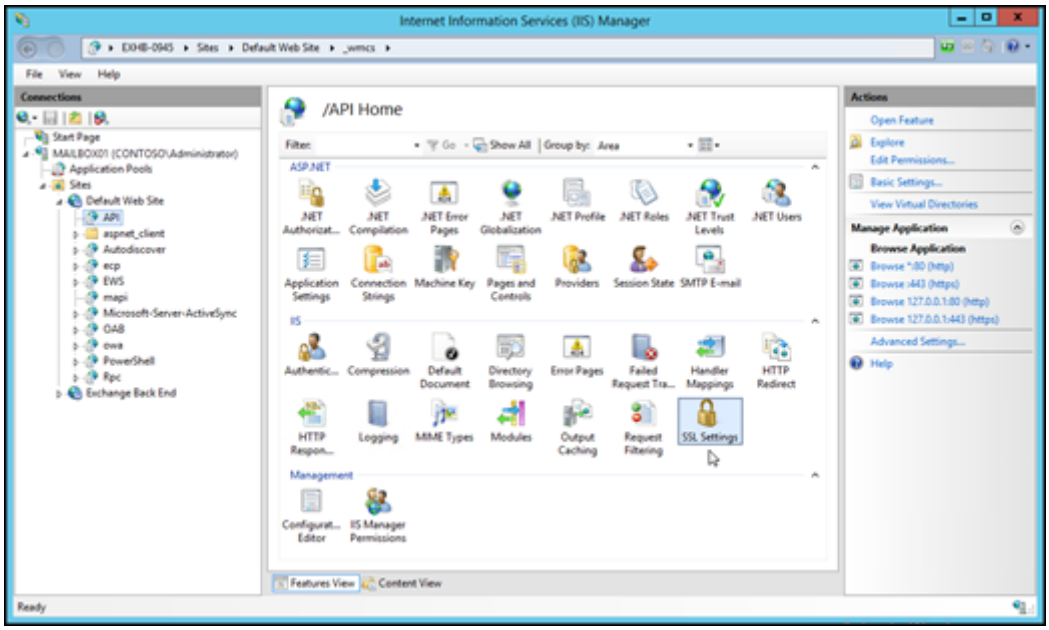
```
%windir%\system32\inetsrv\appcmd.exe set config "Default Web Site" -
section:access -sslFlags:None -commit:APPHOST
```

Этап 2. Восстановление параметра "Требовать SSL" для других виртуальных каталогов на веб-сайте по умолчанию с помощью диспетчера служб IIS

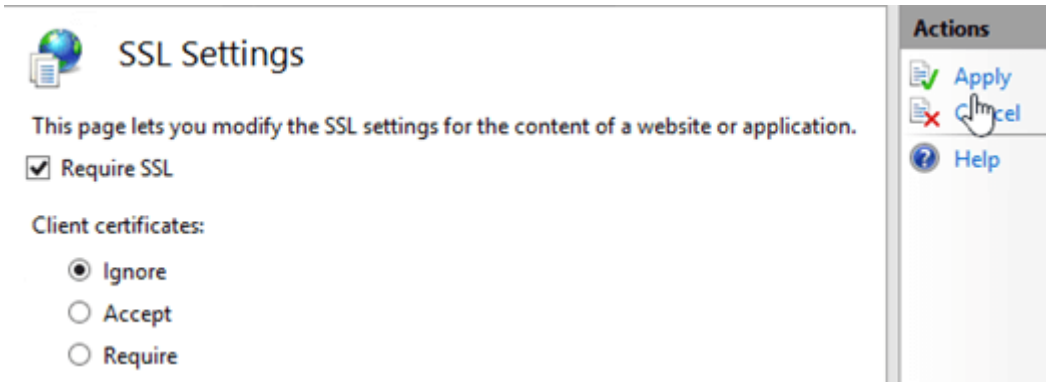
При изменении параметра **Требовать SSL** для веб-сайта в службах IIS этот параметр автоматически наследуется всеми виртуальными каталогами на веб-сайте. Так как нам нужно настроить только Outlook в Интернете, необходимо восстановить параметр **Требовать SSL** для других виртуальных каталогов, где он был включен по умолчанию.

На основе сведений, приведенных в разделе По умолчанию Требовать SSL и перенаправление HTTP в разделе веб-сайт по умолчанию на сервере Exchange Server, выполните следующую процедуру, чтобы восстановить параметр в других виртуальных каталогах, где по умолчанию включен **параметр Требовать SSL** :

1. In IIS Manager, expand the server, expand **Sites**, and expand **Default Web Site**.
2. Выберите виртуальный каталог и убедитесь, что в нижней части страницы включен параметр **Просмотр возможностей**.
3. В разделе **IIS** дважды щелкните элемент **Параметры SSL**.



4. На странице **Параметры SSL** установите флажок **Требовать SSL**, а затем на панели **Действия** нажмите кнопку **Применить**.



5. Повторите описанные выше действия для каждого виртуального каталога на веб-сайте по умолчанию, где параметр **Требовать SSL** был включен по умолчанию (кроме каталога /owa). Единственными виртуальными каталогами, для которых по умолчанию не включен **параметр Требовать SSL** , являются /PowerShell и /Rpc.

Примечание. Чтобы выполнить эти процедуры в командной строке, *замените*< *VirtualDirectory*> именем виртуального каталога и выполните следующую команду в командной строке с повышенными привилегиями:

Консоль

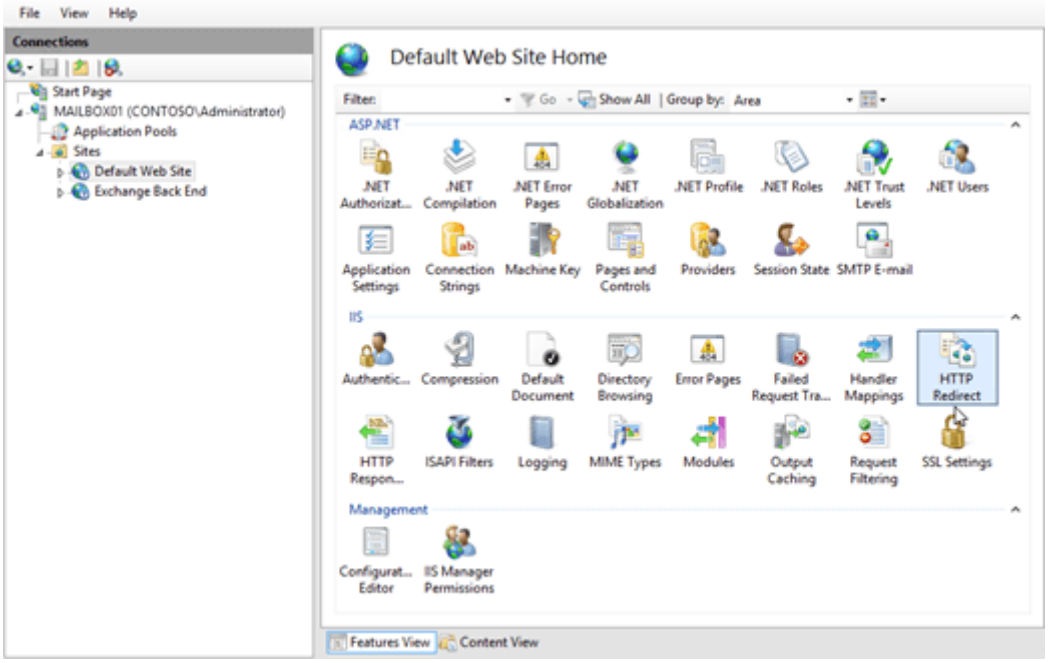
```
%windir%\system32\inetsrv\appcmd.exe set config "Default Web
Site/<VirtualDirectory>" -section:Access -sslFlags:Ssl,Ssl128 -
commit:APPHOST
```

Этап 3. Настройка веб-сайта по умолчанию на перенаправление к виртуальному каталогу /owa с помощью диспетчера служб IIS.

1. В диспетчере служб IIS разверните узел сервера и выберите **Сайты**.

2. Выберите **Веб-сайт по умолчанию**. и убедитесь, что в нижней части страницы выбран пункт **Представление функций** .

3. В разделе **IIS** дважды щелкните элемент **Перенаправление HTTP**.



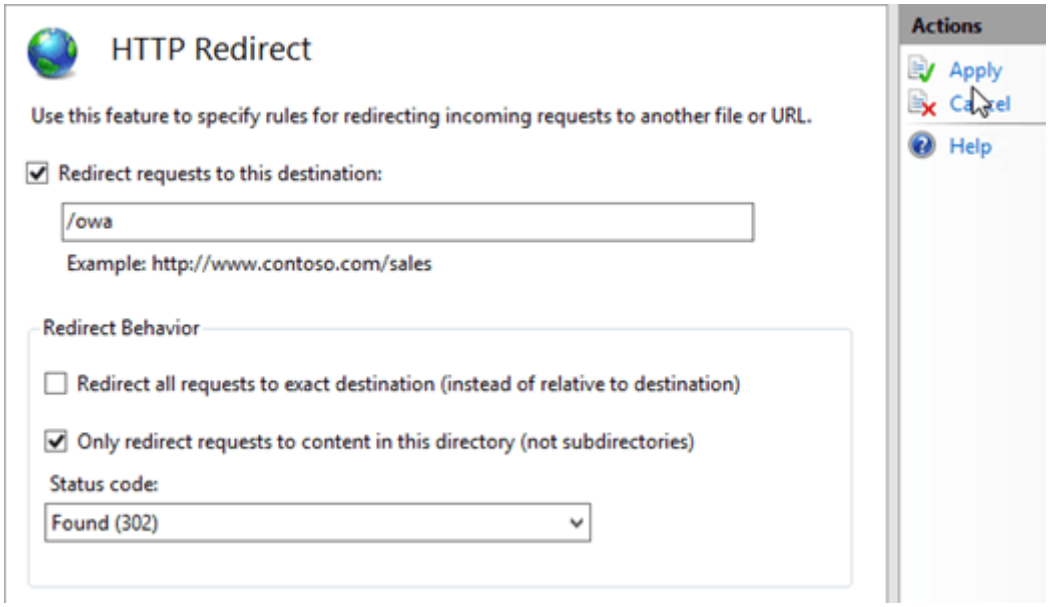
4. На странице **Перенаправление HTTP** настройте указанные ниже параметры.

5. Установите флажок **Перенаправить запросы в это назначение** и введите значение `https://*<OWAUrl>*/owa` (например, https://webmail.contoso.com/owa).

6. В разделе **Поведение при перенаправлении** установите флажок **Запросы на перенапр. содержимого этого каталога (без подкаталогов)**.

7. Убедитесь, что в списке **Код состояния** выбрано значение **Найдено (302)**.

   По завершении нажмите кнопку **Применить** на панели **Действия**.



Примечание. Чтобы выполнить эту процедуру в командной строке, замените *<OWAUrl>* URL-адресом виртуального каталога OWA, откройте командную строку с повышенными привилегиями и выполните следующую команду:

Консоль

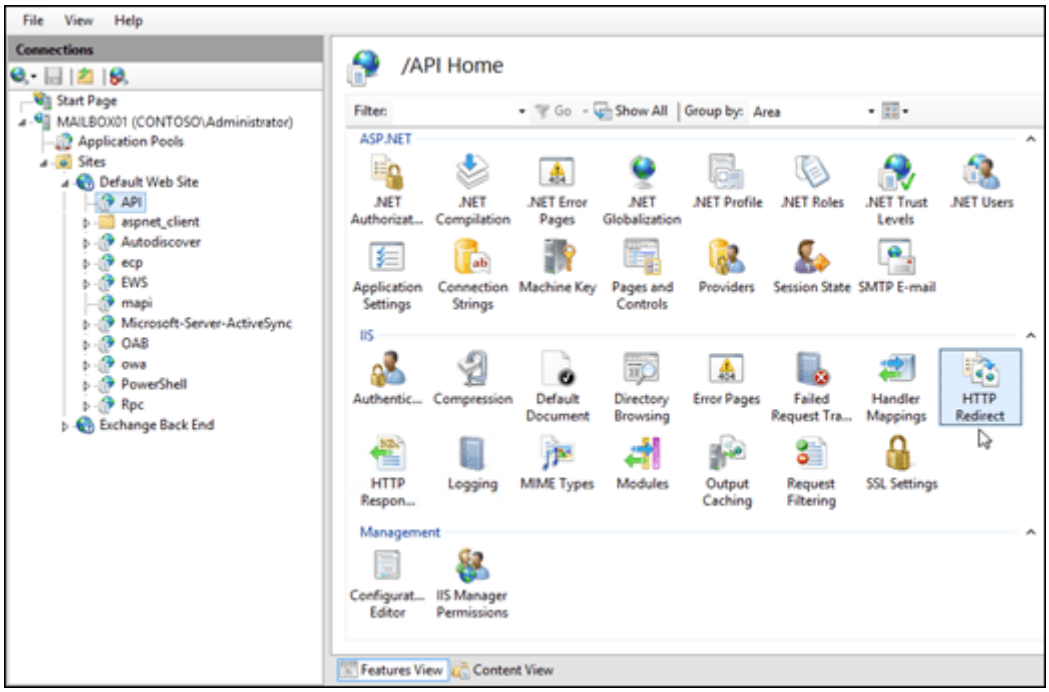
```
%windir%\system32\inetsrv\appcmd.exe set config "Default Web Site" -
section:httpredirect -enabled:true -destination:"https://<OWAUrl>/owa" -
childOnly:true
```

Этап 4. Отключение перенаправления HTTP для всех виртуальных каталогов на веб-сайте по умолчанию с помощью диспетчера служб IIS

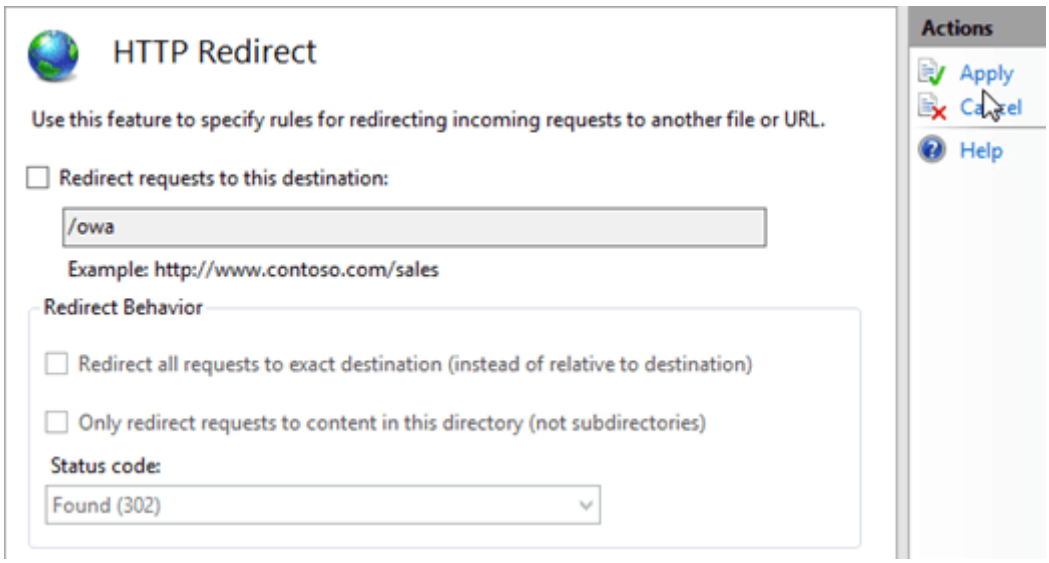
При включении перенаправления для веб-сайта в службах IIS этот параметр автоматически наследуется всеми виртуальными каталогами на веб-сайте. Так как нам нужно настроить перенаправление только для веб-сайта по умолчанию, необходимо удалить параметр перенаправления для всех виртуальных каталогов. По умолчанию перенаправление не включено для каталогов (в том числе виртуальных) на стандартном веб-сайте. Дополнительные сведения см. в разделе Требовать ssl и перенаправление HTTP по умолчанию на веб-сайте по умолчанию на сервере Exchange Server.

Чтобы удалить параметр перенаправления для всех виртуальных каталогов на веб-сайте по умолчанию (включая каталог /owa), выполните указанные ниже действия.

1. In IIS Manager, expand the server, expand **Sites**, and expand **Default Web Site**.
2. Выберите виртуальный каталог и убедитесь, что в нижней части страницы включен параметр **Просмотр возможностей**.
3. В разделе **IIS** дважды щелкните элемент **Перенаправление HTTP**.



4. На странице **Перенаправление HTTP** измените указанные ниже параметры.
5. Снимите флажок **Запросы на перенапр. содержимого этого каталога (без подкаталогов)**.
6. Снимите флажок **Запросы на перенаправление по следующему назначению**.
7. В области **Действия** нажмите кнопку **Применить**.



8. Повторите вышеуказанные действия для каждого виртуального каталога на веб-сайте по умолчанию.

Примечание. Чтобы выполнить эти процедуры в командной строке, *замените*<*VirtualDirectory*> именем виртуального каталога и выполните следующую команду в командной строке с повышенными привилегиями:

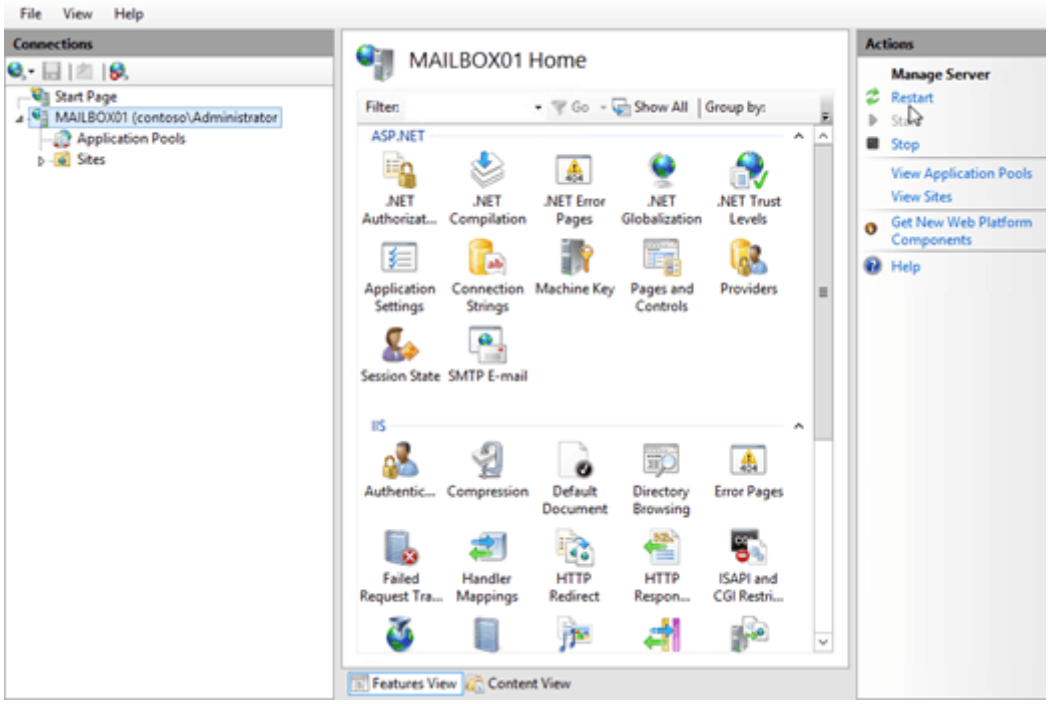
```
Консоль
```

```
%windir%\system32\inetsrv\appcmd.exe set config "Default Web
Site/<VirtualDirectory>" -section:httpredirect -enabled:false -
destination:"" -childOnly:false
```

Этап 5. Перезапуск служб IIS с помощью диспетчера IIS

1. В диспетчере IIS выберите сервер.

2. В области **Действия** выберите элемент **Перезапустить**.



Примечание. Чтобы выполнить эту процедуру в командной строке, откройте командную строку с повышенными привилегиями на сервере Exchange Server и выполните следующие команды:

Консоль

```
net stop w3svc /y
```

Консоль

```
net start w3svc
```

Как проверить, все ли получилось?

Чтобы убедиться, что перенаправление с HTTP на HTTPS для Outlook в Интернете успешно настроено, выполните следующие действия:

1. На клиентском компьютере откройте веб-браузер и введите URL-адрес `http://<ServerName>`. На локальном сервере можно использовать значение `http://127.0.0.1` или `http://localhost`.

2. Убедитесь, что вы перенаправлены на Outlook в Интернете по протоколу https, и убедитесь, что вы можете успешно войти в систему.

3. Откройте URL-адрес `http://<ServerName>/owa` (или `http://localhost/owa` `http://127.0.0.1/owa`).

4. Убедитесь, что вы перенаправлены на Outlook в Интернете по протоколу https, и убедитесь, что вы можете успешно войти в систему.

По умолчанию требовать параметры SSL и перенаправления HTTP на веб-сайте по умолчанию на сервере Exchange Server

Параметры по умолчанию **Требовать SSL** и **перенаправление HTTP** для веб-сайта по умолчанию и всех виртуальных каталогов на веб-сайте по умолчанию на сервере Exchange server описаны в следующей таблице.

Веб-сайт	**Виртуальный каталог**	**Требовать SSL**	**Перенаправление HTTP**
Веб-сайт по умолчанию	Н/д	да	Нет
Веб-сайт по умолчанию	API	да	Нет
Веб-сайт по умолчанию	aspnet_client (каталог)	Да	Нет
Веб-сайт по умолчанию	Autodiscover	да	Нет
Веб-сайт по умолчанию	ecp	да	Нет
Веб-сайт по умолчанию	EWS	да	Нет

Веб-сайт	Виртуальный каталог	Требовать SSL	Перенаправление HTTP
Веб-сайт по умолчанию	mapi	да	Нет
Веб-сайт по умолчанию	Microsoft-Server-ActiveSync	Да	Нет
Веб-сайт по умолчанию	OAB	да	Нет
Веб-сайт по умолчанию	owa	Да Подкаталоги: • auth — да; • Calendar — нет; • Integrated — да; • oma — да.	Нет
Веб-сайт по умолчанию	PowerShell	Нет	Нет
Веб-сайт по умолчанию	Rpc	нет	Нет

Просмотр или настройка свойств политики почтовых ящиков Outlook в Интернете

Статья • 04.04.2023

Политики почтовых ящиков можно настроить в Exchange Server для Outlook в Интернете с помощью Центра администрирования Exchange (EAC) или командной консоли Exchange. После создания политики почтовых ящиков Outlook в Интернете можно настроить различные параметры для управления функциями, доступными пользователям в Outlook в Интернете. Например, можно включить или отключить правила для папки входящих сообщений, либо создать список типов файлов, допустимых во вложениях.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 3 минуты.
- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "политики Outlook в Интернете почтовых ящиков" в разделе Разрешения клиентов и мобильных устройств.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование EAC для просмотра или настройки политик почтовых ящиков

Outlook в Интернете

1. В EAC щелкните **Разрешения**>**Outlook Web App политики**.

2. В области результатов щелкните для выбора политики почтовых ящиков, которую необходимо просмотреть или настроить.

3. Щелкните **Изменить**.

4. На вкладке **Общие** можно просмотреть и изменить имя политики.

5. На вкладке **Функции** включайте или отключайте функции с помощью флажков. По умолчанию отображаются наиболее часто используемые компоненты. Чтобы открыть весь список компонентов, которые можно включить или выключить, выберите команду **Дополнительные параметры**.

   Примечания.

   - Параметры компонентов для политик почтовых ящиков Outlook в Интернете переопределяют Outlook в Интернете параметры виртуального каталога. Параметры сегментации для отдельных пользователей можно изменить с помощью командлета **Set-CASMailbox** в командной консоли Exchange.

   - Параметр для включения или отключения стандартной версии Outlook в Интернете с помощью флажка **Клиента Уровня "Премиум"** не рекомендуется использовать и будет удален из параметров. Стандартная версия Outlook в Интернете всегда включена.

6. На вкладке **Доступ к файлам** установите флажки для настройки параметров доступа к файлам и просмотра для пользователей. Доступ к файлам позволяет пользователю открывать и просматривать содержимое файлов, вложенных в сообщение электронной почты.

   Доступ к файлам может контролироваться на основе того, вошел пользователь в систему на общедоступном или частном компьютере. Пользователи имеют возможность выбирать доступ к частному компьютеру или к общедоступному компьютеру только в случае использования проверки подлинности на основе форм. Все другие виды проверки подлинности по умолчанию относятся к доступу с частного компьютера.

   - **Прямой доступ к файлам**. Установите этот флажок, если вы хотите включить прямой доступ к файлам. С помощью прямого доступа к

файлам пользователи могут открывать файлы, вложенные в сообщения электронной почты.

- **Просмотр документов WebReady**. Установите этот флажок, если вы хотите включить преобразование поддерживаемых документов в HTML и отображение в веб-браузере.

- **Принудительное просмотр документов WebReady при наличии преобразователя**. Установите этот флажок, если вы хотите принудительно преобразовать документы в HTML и отобразить их в веб-браузере, прежде чем пользователи смогут открыть их в приложении для просмотра. Документы можно открыть с помощью программы просмотра, только если включен прямой доступ к файлам.

7. На вкладке **Автономный доступ** настройте доступность в автономном режиме с помощью переключателей.

8. Нажмите кнопку **Сохранить**, чтобы обновить политику.

Просмотр политик почтовых ящиков Outlook в Интернете с помощью командной консоли Exchange

В этом примере извлекаются свойства политики `Executives` почтовых ящиков Outlook в Интернете в организации `Fabrikam`.

PowerShell

```
Get-OwaMailboxPolicy -Identity Fabrikam\Executives
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе Get-OwaMailboxPolicy.

Настройка политик почтовых ящиков Outlook в Интернете с помощью командной консоли Exchange

В этом примере разрешается доступ к календарю в политике почтовых ящиков по умолчанию.

PowerShell

```
Set-OwaMailboxPolicy -Identity Default -CalendarEnabled $true
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе Set-OwaMailboxPolicy.

Как проверить, все ли получилось?

Чтобы убедиться, что политика почтовых ящиков Outlook в Интернете успешно изменена, выполните следующие действия:

1. В EAC щелкните **Разрешения**>**Outlook Web App Политики**, а затем выберите определенную политику почтовых ящиков Outlook в Интернете.
2. Щелкните **Изменить** , чтобы просмотреть свойства политики почтовых ящиков.
3. Нажмите кнопку **Отмена** или **Сохранить**, чтобы закрыть страницу свойств.

См. также

Outlook Web App процедур политики почтовых ящиков в Exchange 2013

Создание темы для Outlook в Интернете в Exchange Server

Статья • 04.04.2023

Тема определяет цвета, шрифты и изображения, отображаемые пользователям в Outlook в Интернете (ранее — Outlook Web App) в Exchange Server. Каждая тема представляет собой набор файлов, которые хранятся на сервере Exchange Server. Встроенные темы описаны в разделе По умолчанию Outlook в Интернете темы Exchange Server в конце этого раздела.

Чтобы создать тему для Outlook в Интернете:

1. Скопируйте папки и файлы из существующей темы и переименуйте копии.
2. Настройте отображаемое имя и порядок сортировки для новой темы.
3. Настройте новую тему.
4. (Необязательно) Установите новую тему по умолчанию и запретите пользователям выбирать темы.
5. (Необязательно) Разрешить пользователям просматривать и выбирать новую тему
6. Чтобы изменения вступили в силу, перезапустите службы IIS.

Если для клиентских подключений к Outlook в Интернете используются несколько серверов Exchange Server, скопируйте новую тему на каждый сервер. Также советуем создать резервную копию новой темы, чтобы вы могли скопировать файлы на сервер Exchange Server после переустановки или обновления.

После создания темы может потребоваться настроить элементы, общие для всех тем. Дополнительные сведения см. в статье Настройка Outlook в Интернете входа, выбора языка и страниц ошибок в Exchange Server.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 45 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Outlook в Интернете виртуальных каталогов" в разделе Разрешения для клиентов и

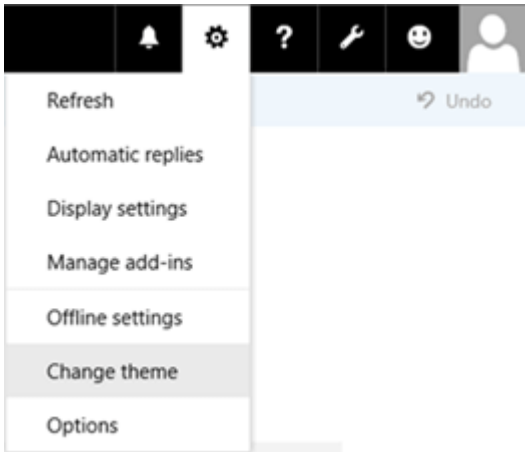
мобильных устройств. Используемая учетная запись также должна быть членом локальной группы администраторов на сервере Exchange Server.

- Облегченная версия Outlook в Интернете не поддерживает темы.
- Чтобы заменить существующий цвет, необходимо указать RGB-значение нового цвета в формате HTML. Эти значения можно найти в статье Таблица цветов. Если в ней нет нужного вам цвета, RGB-значение для него можно определить с помощью графического редактора или веб-сайта с кодами цветов HTML.
- Не удаляйте папку `%ExchangeInstallPath%ClientAccess\OWA\prem\<ExchangeVersion>\resources\themes\base` или файлы в ней.
- Прежде чем изменять существующую тему (а не ее копию), создайте резервную копию исходных файлов.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**.

Шаг 1. Используя проводник, скопируйте папки и файлы из существующей темы и переименуйте копии

Чтобы просмотреть встроенные темы, откройте почтовый ящик в Outlook в Интернете и выберите **Изменить тему** в меню **Параметры**.



Сведения, приведенные в разделе По умолчанию Outlook в Интернете темы Exchange Server в конце этого раздела, можно использовать для сопоставления отображаемого имени темы в Outlook в Интернете с именем папки темы на сервере Exchange Server.

Файлы и папки темы хранятся в таких расположениях:

- `%ExchangeInstallPath%ClientAccess\OWA\prem\<ExchangeVersion>\resources\themes\` содержит папку, в которой хранится изображение заголовка, изображение для предварительного просмотра и описание темы.
- `%ExchangeInstallPath%ClientAccess\OWA\prem\<ExchangeVersion>\resources\styles\` содержит `_fabric.color.variables.theme.<ThemeFolderName>.less` файлы и `fabric.color.theme.<ThemeFolderName>.css` , определяющие цвета, используемые в теме.

  Примечание. В *<подпапке ExchangeVersion>* используется синтаксис 15.1. *nnn*. *nn*, и указывает установленный накопительный пакет обновления (CU) Exchange.

Когда вы найдете наиболее подходящую тему (с изображением заголовка или без него), скопируйте папку темы и соответствующие файлы и переименуйте копии.

1. В проводник перейдите к `%ExchangeInstallPath%ClientAccess\OWA\prem\<ExchangeVersion>\resources\themes`.
2. Выберите существующую папку темы в папке `\themes` , скопируйте ее, а затем вставьте обратно в папку `\themes` . В результате создается новая папка с именем `<ThemeFolderName> - Copy`.

   Примечание. Чтобы быстро скопировать и вставить папку темы, выберите ее и нажмите клавиши CTRL+C, а затем CTRL+V.
3. Переименуйте новую папку темы, созданную на предыдущем шаге. Например, `fourthcoffee`.

   Примечание. Чтобы быстро переименовать папку, выберете ее и нажмите клавишу F2.
4. В проводник перейдите к `%ExchangeInstallPath%ClientAccess\OWA\prem\<ExchangeVersion>\resources\styles\`.

5. Найдите файлы с именем `_fabric.color.variables.theme.<ThemeFolderName>.less` и `fabric.color.theme.<ThemeFolderName>.css` , которые соответствуют папке темы, скопированной на шаге 2. Выделите каждый файл, скопируйте его и вставьте обратно в папку `\styles` . В результате появляются новые файлы с именами `_fabric.color.variables.theme.<ThemeFolderName> - Copy.less` и `fabric.color.theme.<ThemeFolderName> - Copy.css`.

6. Переименуйте новые файлы, созданные на предыдущем шаге. Значение *<ThemeFolderName>* должно соответствовать имени папки из шага 3. Например, `_fabric.color.variables.theme.fourthcoffee.less` и `fabric.color.theme.fourthcoffee.css`.

Шаг 2. Используя Блокнот, настройте для новой темы отображаемое имя и порядок сортировки

Для новой темы необходимо настроить уникальное отображаемое имя и порядок сортировки, так как они совпадают с именем и порядком сортировки темы, которую вы скопировали. Имя темы отображается на панели **Изменить тему** в приложении Outlook в Интернете. Порядок сортировки определяет расположение темы в списке тем.

1. Используйте Блокнот, чтобы открыть файл с именем `themeinfo.xml` в новой папке `%ExchangeInstallPath%ClientAccess\OWA\prem\<ExchangeVersion>\resources\themes\<NewThemeFolder>` theme, созданной на шаге 1. Содержимое файла будет выглядеть следующим образом:

   `<theme displayname="__<CopiedThemeName>__" sortorder="<CopiedThemeSortOrder>"/>`

2. Измените `displayname="__<CopiedThemeName>__"` значение на нужное значение. Например, `displayname = "Fourth Coffee Corporate Theme"`.

   Примечание. Значение `"__<ThemeName>__"` отображаемого имени темы — это строка кода, локализованная на разных языках. Текстовое значение, указанное для новой темы, не локализуется на разных языках.

3. Измените `sortorder="<CopiedThemeSortOrder>"` целочисленное значение на нужное уникальное значение. Чем ниже значение, тем выше в списке располагается тема. Чтобы найти значения порядка сортировки для

встроенных тем, можно использовать сведения, приведенные в разделе По умолчанию Outlook в Интернете темы Exchange Server в конце этого раздела. Тема по умолчанию содержит `sortorder="0"`, и отображается первой в списке.

- Если вы хотите вставить новую тему в список встроенных тем, укажите уникальное значение, которое еще не используется. Например, если вы хотите, чтобы новая тема отображалась в списке вторым, можно использовать значение `sortorder="5"`.

- Если вы хотите вставить новую тему *на место* встроенной, укажите такое же значение, как и у встроенной темы, а затем измените порядок сортировки для встроенной темы. Например, если вы хотите, чтобы новая тема отображалась первой в списке, необходимо задать для новой темы значение `sortorder="0"`. Но вам также нужно открыть `themeinfo.xml` файл в папке `\base` (тема по умолчанию), чтобы изменить значение `sortorder="0"` на что-то другое (например, `sortorder="5"`).

4. По завершении сохраните и закройте `themeinfo.xml` файл.

Шаг 3. Настройте новую тему

Файлы изображений

Файлы изображений темы хранятся в следующих папках в `%ExchangeInstallPath%ClientAccess\OWA\prem\<ExchangeVersion>\resources\themes\<ThemeFolderName>`:

- `\images\0`: эти файлы используются в языках слева направо.

- `\images\rtl`: эти файлы используются в языках справа налево. В зависимости от изображения этот файл может быть таким же, как и версия для языков с письмом справа налево, а может быть зеркально отраженным изображением.

Файлы изображений, которые находятся в этих папках, описаны в приведенной ниже таблице.

Имя файла	Размеры (ширина x высота в пикселях)	Разрядность	Описание

Имя файла	Размеры (ширина x высота в пикселях)	Разрядность	Описание
headerbgmaing2.png	2000 x 50	32	Изображение заголовка для тем, в которых используется статическое изображение заголовка. Размер файла варьируется. Если в теме не используется статическое изображение заголовка, размер файла — 1 x 1 пиксель (2815 байт).
headerbgmaing2.gif	2000 x 50	24	Изображение заголовка для тем, в которых используется анимированное изображение заголовка. Размер файла варьируется. Если в теме не используется анимированное изображение заголовка, размер файла — 1 x 1 пиксель (43 байта).
themepreview.png	64 x 64	24 или 8	Небольшое квадратное изображение, представляющее тему на панели **Изменить тему** в Outlook в Интернете. Для темы по умолчанию и черной темы размер файла — 1 x 1 пиксель, а изображение для предварительного просмотра представляет собой черный квадрат.

Существующий файл изображения можно изменить или заменить новым файлом с теми же именем и размерами.

цвета;

Цвета темы определяются в следующих файлах в папке `%ExchangeInstallPath%ClientAccess\OWA\prem\<ExchangeVersion>\resources\styles`:

- `fabric.color.theme.<ThemeFolderName>.css`

- `_fabric.color.variables.<ThemeFolderName>.less`

При изменении значения цвета необходимо изменить все ссылки на цвет в обоих файлах.

Шаг 4. (Необязательно) Установите тему по умолчанию и запретите пользователям выбирать тему

Установка новой темы по умолчанию затрагивает только тех пользователей, которые не выбрали тему вручную. Чтобы установить тему по умолчанию для всех пользователей, также необходимо отключить выбор темы в Outlook в Интернете. Эти настройки затрагивают всех пользователей, подключающихся к Outlook в Интернете через сервер Exchange Server.

Чтобы установить тему по умолчанию и запретить пользователям менять тему в Outlook в Интернете, используйте следующий синтаксис:

PowerShell

```
Set-OwaVirtualDirectory -Identity <VirtualDirectoryIdentity> -DefaultTheme
<ThemeFolderName> -ThemeSelectionEnabled $false
```

В этом примере папка темы с именем `fourthcoffee` в качестве темы по умолчанию настраивается в Outlook в Интернете для веб-сайта по умолчанию на сервере с именем Mailbox01.

PowerShell

```
Set-OwaVirtualDirectory -Identity "Mailbox01\owa (Default Web Site)" -
DefaultTheme fourthcoffee -ThemeSelectionEnabled $false
```

Примечания.

- По умолчанию значение параметра *DefaultTheme* пусто (`$null`). Это значение означает, что тема по умолчанию не задана, и если пользователь не выбрал тему вручную, используется "Тема по умолчанию".
- Exchange не проверяет значение, указанное для параметра *DefaultTheme* . Убедитесь, что такая тема существует.

- Чтобы указать тему по умолчанию для определенных пользователей, которая переопределяет параметр темы по умолчанию в виртуальном каталоге Outlook в Интернете, используйте параметр *DefaultTheme* в **командлете Set-OwaMailboxPolicy**.

Шаг 5. (Необязательно) Разрешить пользователям выбирать новую тему

Если вы не хотите заставлять всех пользователей использовать новую тему, необходимо добавить новую тему в `stylemanifest.xml` файл, чтобы пользователи могли найти и выбрать ее в списке тем. Файл `stylemanifest.xml` находится в `%ExchangeInstallPath%ClientAccess\OWA\prem\<ExchangeVersion>\manifests`.

В этом примере добавляется новая строка в `stylemanifest.xml` файл для новой `fourthcoffee` темы.

```
<themeVariables themeName="fourthcoffee"
fileName="_fabric.color.variables.theme.fourthcoffee.less" />
```

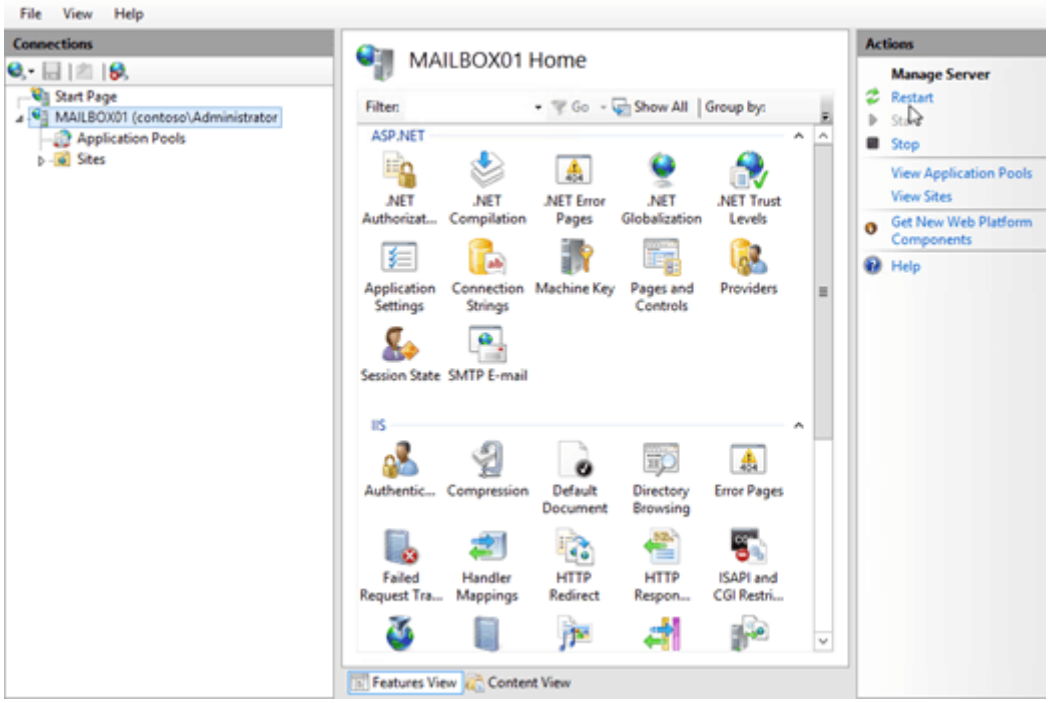
Шаг 6. Перезапуск СЛУЖБ IIS

Чтобы изменения вступили в силу, необходимо перезапустить службы IIS.

1. Откройте диспетчер IIS на сервере Exchange Server. Простой способ сделать это в Windows Server 2012 или более поздней версии — нажать клавишу Windows + Q, ввести inetmgr и выбрать **Диспетчер служб IIS** в результатах.

2. В диспетчере IIS выберите сервер.

3. В области **Действия** выберите элемент **Перезапустить**.



Примечание. Чтобы выполнить эту процедуру в командной строке, откройте командную строку с повышенными привилегиями на сервере Exchange Server (для этого выберите **Запуск от имени администратора**) и выполните следующую команду:

Консоль

```
net stop w3svc /y
```

Консоль

```
net start w3svc
```

Как проверить, все ли получилось?

Чтобы убедиться, что тема Outlook в Интернете успешно создана, выполните указанные ниже действия.

1. Откройте почтовый ящик в Outlook в Интернете. Чтобы проверить тему на сервере Exchange Server, откройте URL-адрес https://localhost/owa или https://127.0.0.1/owa.

2. В зависимости от настроенных параметров убедитесь, что новая тема используется по умолчанию, или убедитесь, что вы можете увидеть и выбрать новую тему в разделе **Параметры**>**Изменить тему**.

3. Если изменения не отображаются после перезапуска IIS, очистите журнал браузера (удалите временные файлы Интернета) и обновите окно браузера.

Темы Outlook в Интернете по умолчанию в Exchange Server

Встроенные темы Outlook в Интернете находятся в папке `%ExchangeInstallPath%ClientAccess\OWA\prem\<ExchangeVersion>\resources\themes` и описаны в следующей таблице.

Имя папки	Отображаемое имя в Outlook в Интернете	Порядок сортировки в Outlook в Интернете (чем ниже значение, тем выше в списке)	Тип изображения заголовка
angular	Косоугольник	110	Статическое
balloons	Воздушные шары	240	Статическое
base	Тема по умолчанию	0	Отсутствует
beach	Закат на пляже	40	Анимированное
black	Черная	670	Отсутствует
blueberry	Голубика	600	Отсутствует
blueprint	Копирка	120	Статическое
bricks	Кубики	20	Статическое
cats	Коты	300	Статическое
chevron	Зигзаги	80	Статическое
circuit	Канал	130	Статическое
comic	Книга комиксов	170	Статическое
contrast	Контраст	500	Отсутствует
cordovan	Коричневая	650	Отсутствует
crayon	Пастель	140	Статическое
cubes	3D-кубы	190	Статическое
cubism	Кубизм	310	Статическое

Имя папки	Отображаемое имя в Outlook в Интернете	Порядок сортировки в Outlook в Интернете (чем ниже значение, тем выше в списке)	Тип изображения заголовка
darkcordovan	Темно-коричневая	660	Отсутствует
darkorange	Темно-оранжевая	620	Отсутствует
diamonds	Плавающие ромбы	160	Статическое
far	Далекие края	150	Анимированное
grape	Виноград	610	Отсутствует
jelly	Медуза	70	Анимированное
lightblue	Светло-синяя	530	Отсутствует
lightgreen	Светло-зеленая	540	Отсутствует
lite	Lite	510	Отсутствует
mediumdarkblue	Темно-синяя	640	Отсутствует
minimal	Минимальная	520	Отсутствует
modern	Модерн 20-го века	280	Статическое
mountain	Вершина горы	50	Статическое
orange	Апельсин	580	Отсутствует
paint	Отпечатки пальцев	290	Статическое
pink	Розовая	550	Отсутствует
pixel	Pixel Pop	60	Статическое
polka	Узор в горошек	200	Статическое
pomegranate	Гранат	590	Отсутствует
primary	Основная	180	Статическое
raspberry	Малина	570	Отсутствует
robot	Робот	100	Анимированное
simple	Простые грани	230	Статическое

Имя папки	Отображаемое имя в Outlook в Интернете	Порядок сортировки в Outlook в Интернете (чем ниже значение, тем выше в списке)	Тип изображения заголовка
spectrum	Спектральные грани	90	Статическое
strawberry	Клубника	250	Статическое
super	Искрящаяся радость	10	Статическое
teagarden	Чайный сад	210	Статическое
teal	Сине-зеленая	550	Отсутствует
watermelon	Арбуз	630	Отсутствует
whale	Приятное время	30	Анимированное
whimsical	Прихотливая	220	Статическое
wntrlnd	Зимние мотивы	260	Статическое
wrld	Весь мир	270	Статическое

Настройка Outlook в Интернете входа, выбора языка и страниц ошибок в Exchange Server

Статья • 04.04.2023

Страницы Outlook в Интернете (прежнее название — Outlook Web App) для входа, выбора языка и ошибок основаны на файлах таблицы стилей изображений и содержимого (CSS) в папке ресурсов тем в службах клиентского доступа (интерфейсного интерфейса) на сервере Exchange Server 2016 или Exchange 2019. В Outlook в Интернете для всех тем используется единый набор страниц входа, выбора языка и ошибок. Любые изменения на этих страницах будут видны пользователям, подключающимся к Outlook в Интернете через сервер Exchange.

Примечания.

- Создайте резервную копию файлов по умолчанию Outlook в Интернете, прежде чем вносить изменения.
- Создайте резервную копию настроенных файлов, чтобы повторно их применить после переустановки или обновления сервера Exchange.
- Если для подключений Outlook в Интернете используется несколько серверов Exchange, скопируйте измененные файлы для каждого сервера.

Дополнительные сведения о Outlook в Интернете см. в разделе Outlook в Интернете в Exchange Server. Сведения о создании пользовательской темы см. в статье Создание темы для Outlook в Интернете в Exchange Server.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 30 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Редактор графики" в разделе "Разрешения Outlook в Интернете" раздела Разрешения клиентов и мобильных устройств.
- Чтобы заменить существующий цвет, необходимо для нового цвета указать RGB-значение в формате HTML. Эти значения можно найти в статье Таблица цветов. Если в ней нет нужного вам цвета, то RGB-значения в формате HTML для него можно определить с помощью графического редактора.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

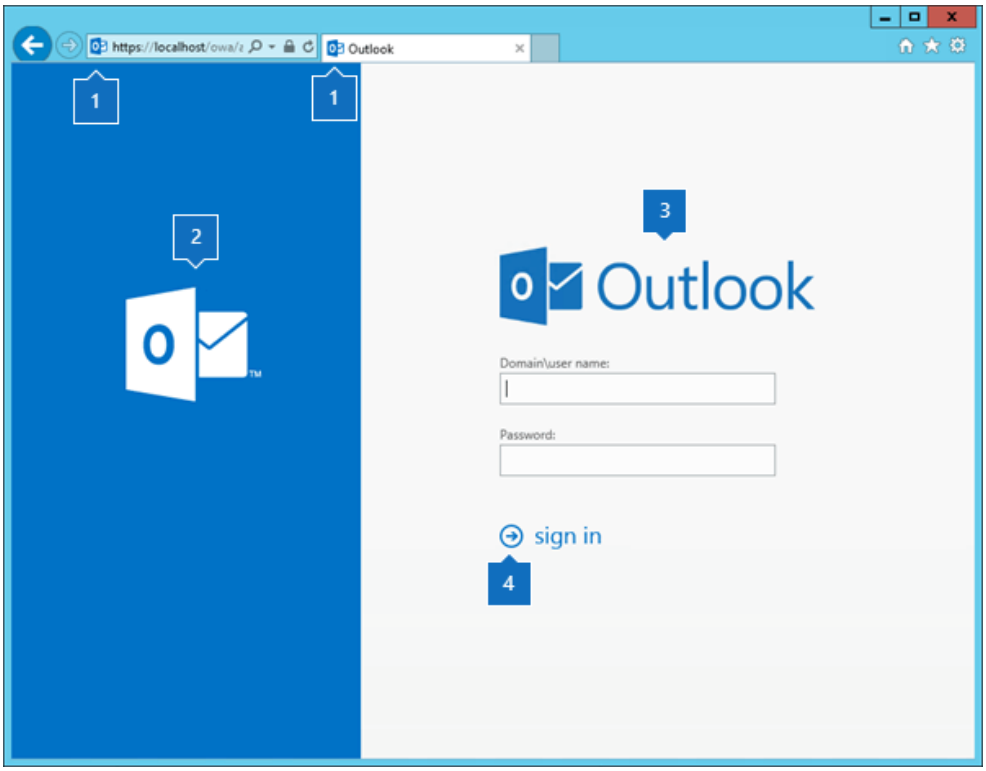
Настройка цвета страницы входа для Outlook в Интернете

1. Используйте Блокнот, чтобы открыть файл `%ExchangeInstallPath%FrontEnd\HttpProxy\owa\auth\<ExchangeVersion>\themes\resources\logon.css`.

   Примечание. В *<подпапке ExchangeVersion>* используется синтаксис 15.1. *nnn*. *nn* и изменяется при каждой установке накопительного обновления Exchange.

2. В файле замените `logon.css` значение синего цвета по умолчанию #0072c6 на HTML RGB-значение, которое вы хотите использовать.

3. По завершении сохраните и закройте файл.

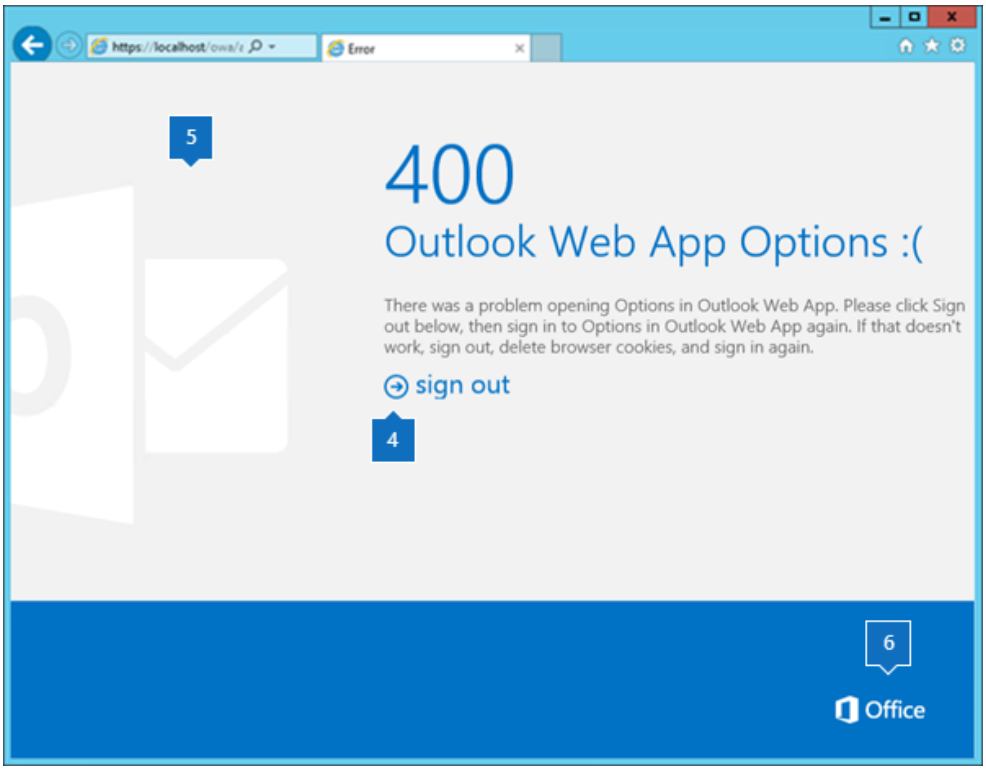


Настройка цветов страницы ошибок Outlook в Интернете

1. Используйте Блокнот, чтобы открыть файл `%ExchangeInstallPath%FrontEnd\HttpProxy\owa\auth\<ExchangeVersion>\themes\resources\errorFE.css`.

2. В файле замените `errorFE.css` значение синего цвета по умолчанию #0072c6 на HTML RGB-значение, которое вы хотите использовать.

3. По завершении сохраните и закройте файл.

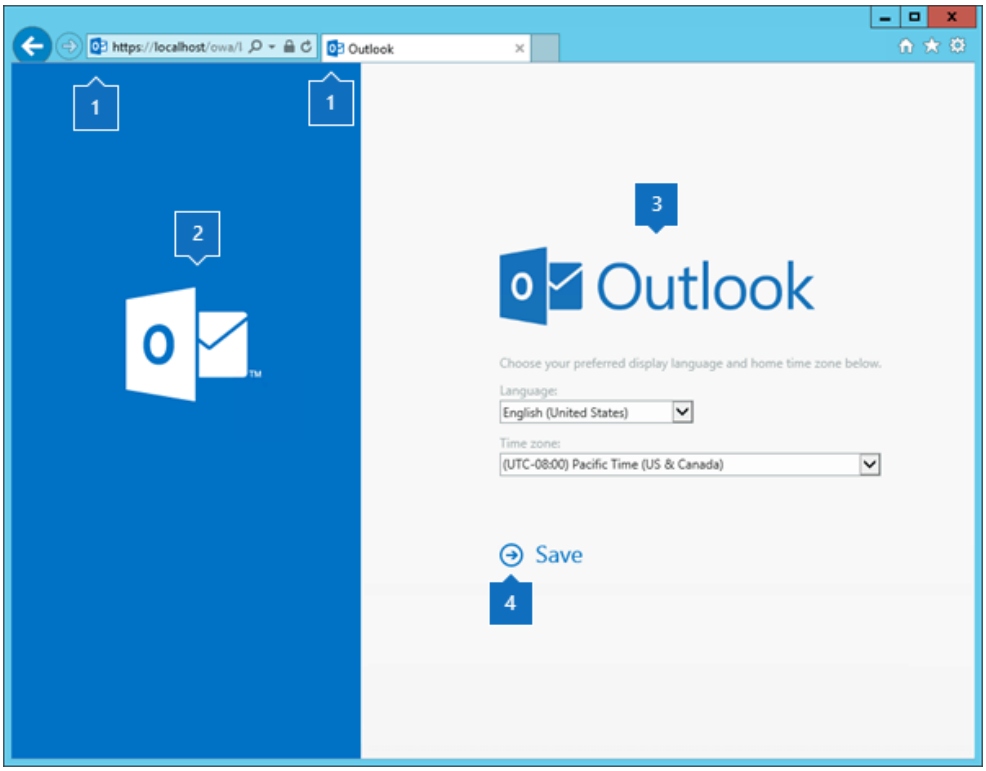


Настройка цвета страницы выбора языка Outlook в Интернете

1. Используйте Блокнот, чтобы открыть файл `%ExchangeInstallPath%ClientAccess\Owa\prem\<ExchangeVersion>\resources\styles\languageselection.css`.

2. В файле замените `languageselection.css` значение синего цвета по умолчанию #0072c6 на HTML RGB-значение, которое вы хотите использовать.

3. По завершении сохраните и закройте файл.



Настройка страниц входа, выбора языка и ошибок для Outlook в Интернете

Вы можете изменить существующие файлы или заменить их новыми, сохранив соответствующие имя и размеры. В таблице ниже содержится информация об изображениях.

Image	Имя файла	Расположение	Размеры (ширина x высота в пикселях)	Разрядность
1	Favicon.ico	`%ExchangeInstallPath%FrontEnd\HttpProxy\owa\auth\<ExchangeVersion>\themes\resources`	16 x 16	32
2	olk_logo_white.png	`%ExchangeInstallPath%ClientAccess\Owa\prem\<ExchangeVersion>\resources\images\0`	128 x 108	32
3	owa_text_blue.png	`%ExchangeInstallPath%ClientAccess\Owa\prem\<ExchangeVersion>\resources\images\0`	300 x 76	32
4	Sign_in_arrow.png (для языков с написанием слов слева направо) Sign_in_arrow_rtl.png (для языков с написанием слов справа налево)	`%ExchangeInstallPath%FrontEnd\HttpProxy\owa\auth\<ExchangeVersion>\themes\resources`	22 x 22	32
5	olk_logo_white_cropped.png	`%ExchangeInstallPath%FrontEnd\HttpProxy\owa\auth\<ExchangeVersion>\themes\resources`	265 x 310	32
6	office_logo_white_small.png	`%ExchangeInstallPath%ClientAccess\Owa\prem\<ExchangeVersion>\resources\images\0` (для языков с написанием слов слева направо) `%ExchangeInstallPath%ClientAccess\Owa\prem\<ExchangeVersion>\resources\images\rtl` (для языков справа налево)	81 x 26	8

Как проверить, все ли получилось?

Чтобы убедиться, что страницы входа, выбора языка и ошибок для Outlook в Интернете успешно настроены, выполните следующие действия:

1. Откройте в веб-браузере страницу входа в Outlook в Интернете. Чтобы проверить внесенные изменения, перейдите по URL-адресу https://localhost/owa или https://127.0.0.1/owa на сервере Exchange, на котором размещен виртуальный каталог Outlook в Интернете.

2. Если изменения не отображаются, очистите журнал браузера (удалите временные файлы Интернета) и обновите окно браузера.

   Примечание. Чтобы увидеть результаты изменений, вы можете оставить редактируемый файл CSS открытым и обновлять окно браузера после сохранения каждого изменения.

Использование проверки подлинности на основе утверждений AD FS с Outlook в Интернете

Статья • 04.04.2023

Установка и настройка службы федерации Active Directory (AD FS) (AD FS) в Exchange Server организациях позволяет клиентам использовать проверку подлинности на основе утверждений AD FS для подключения к Outlook в Интернете (ранее — Outlook Web App) и Центр администрирования Exchange (EAC). Удостоверение на основе утверждений — это еще один подход к проверке подлинности, который удаляет управление проверкой подлинности из приложения и упрощает управление учетными записями за счет централизованной проверки подлинности. Если включена проверка подлинности на основе утверждений, Outlook в Интернете и EAC не отвечают за проверку подлинности пользователей, хранение учетных записей пользователей и паролей, поиск сведений об удостоверениях пользователей или интеграцию с другими системами идентификации. Централизованная проверка подлинности упрощает обновление методов проверки подлинности в будущем.

Проверка подлинности на основе утверждений AD FS заменяет традиционные методы проверки подлинности, доступные для Outlook в Интернете и EAC. Например:

- проверка подлинности на основе клиентского сертификата Active Directory;
- Обычная проверка подлинности
- дайджест-проверка подлинности;
- проверка подлинности с помощью форм;
- Проверка подлинности Windows

Настройка проверки подлинности на основе утверждений AD FS для Outlook в Интернете и Центра администрирования Exchange в Exchange Server включает следующие дополнительные серверы:

- Контроллер домена Windows Server 2012 или более поздней версии (доменные службы Active Directory роль сервера).

- Сервер AD FS Windows Server 2012 или более поздней версии (службы федерации Active Directory (AD FS) роль сервера). Windows Server 2012 использует AD FS 2.1, а Windows Server 2012 R2 — AD FS 3.0. Для установки AD FS и создания необходимых правил доверия и утверждений проверяющей

стороны на сервере AD FS необходимо быть членом группы безопасности "Администраторы домена", "Администраторы предприятия" или "Локальные администраторы".

- При необходимости Windows Server 2012 R2 или более поздней версии веб-сервер Application Proxy (роль сервера удаленного доступа, служба роли веб-Application Proxy).
    - Веб-Application Proxy — это обратный прокси-сервер для веб-приложений, которые находятся в корпоративной сети. Веб-Application Proxy позволяет пользователям на многих устройствах получать доступ к опубликованным веб-приложениям за пределами корпоративной сети. Дополнительные сведения см. в статье Установка и настройка веб-Application Proxy для публикации внутренних приложений.
    - Хотя веб-Application Proxy обычно рекомендуется, когда СЛУЖБА AD FS доступна внешним клиентам, автономный доступ в Outlook в Интернете не поддерживается при использовании проверки подлинности AD FS через веб-Application Proxy.
    - Для установки веб-Application Proxy на сервере Windows Server 2012 R2 требуются разрешения локального администратора.
    - Перед настройкой сервера веб-Application Proxy необходимо развернуть и настроить сервер AD FS, и вы не сможете установить веб-Application Proxy на том же сервере, где установлена служба AD FS.

Что нужно знать перед началом работы

- Предполагаемое время выполнения этой процедуры: 45 минут.
- Процедуры в этом разделе основаны на Windows Server 2012 R2.
- Outlook в Интернете для устройств не поддерживает проверку подлинности, основанную на утверждениях AD FS.
- Для выполнения процедур в организации Exchange необходимо иметь разрешения на управление организацией.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Шаг 1. Проверка требований к сертификатам для AD FS

Для AD FS требуются два основных типа сертификатов:

- Обмен данными между службами SSL-сертификат для зашифрованного трафика веб-служб между сервером AD FS, клиентами, серверами Exchange и необязательным сервером веб-Application Proxy. Рекомендуется использовать сертификат, выданный внутренним или коммерческим центром сертификации (ЦС), так как все клиенты должны доверять этому сертификату.
- Сертификат подписи маркеров для зашифрованного обмена данными и проверки подлинности между сервером AD FS, контроллерами домена Active Directory и серверами Exchange. Рекомендуется использовать самозаверяющий сертификат подписи маркера AD FS по умолчанию.

Дополнительные сведения о создании и импорте SSL-сертификатов в Windows см. в разделе Серверные сертификаты.

Ниже приведена сводка сертификатов, которые мы будем использовать в этом сценарии:

Общее имя (CN) в сертификате (в поле Тема, Альтернативное имя субъекта или совпадение сертификата с подстановочными знаками)	**Тип**	**Требуется на серверах**	**Comments**
`adfs.contoso.com`	Выдано ЦС	Сервер AD FS Сервер веб-Application Proxy	Это имя узла, которое отображается клиентам, поэтому клиенты должны доверять издателю этого сертификата.
`ADFS Signing -`	Самозаверяющий	Сервер AD	Самозаверяющий сертификат по

Общее имя (CN) в сертификате (в поле Тема, Альтернативное имя субъекта или совпадение сертификата с подстановочными знаками)	Тип	Требуется на серверах	Comments
`adfs.contoso.com`		FS Серверы Exchange Сервер веб-Application Proxy	умолчанию автоматически копируется во время настройки дополнительного сервера веб-Application Proxy, но его необходимо импортировать вручную в хранилище доверенных корневых сертификатов на всех серверах Exchange в организации. По умолчанию самозаверяющий сертификат подписи маркеров действителен в течение одного года. Сервер AD FS настроен на автоматическое продление (замена) самозаверяемых сертификатов до истечения срока их действия, но вам потребуется повторно импортировать сертификат на серверы Exchange. Вы можете увеличить срок действия сертификата по умолчанию, выполнив следующую команду в Windows PowerShell на сервере AD FS: `Set-AdfsProperties -CertificateDuration <Days>` (значение по умолчанию — 365). Дополнительные сведения см. в разделе Set-AdfsProperties. Чтобы экспортировать сертификат из консоли управления AD FS, выберите**Сертификаты**>**службы**>, щелкните правой кнопкой мыши сертификат > для подписи маркера, выберите **Пункт Просмотр сертификата**>, перейдите на вкладку >**Сведения**, щелкните **Копировать в файл**.

Общее имя (CN) в сертификате (в поле Тема, Альтернативное имя субъекта или совпадение сертификата с подстановочными знаками)	Тип	Требуется на серверах	Comments
`mail.contoso.com`	Выдано ЦС	Серверы Exchange Сервер веб-Application Proxy	Это типичный сертификат, который используется для шифрования внешних клиентских подключений к Outlook в Интернете (и, вероятно, другим службам IIS Exchange). Дополнительные сведения см. в статье Требования к сертификатам для служб Exchange.

Дополнительные сведения см. в разделе "Требования к сертификатам" статьи Требования AD FS.

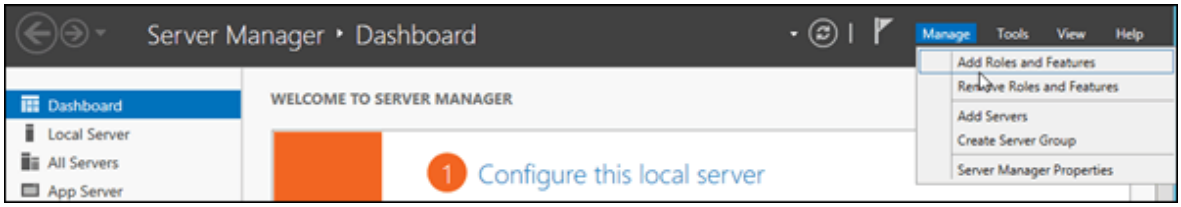
> ⓘ **Примечание**
>
> Теперь для шифрования данных, которыми обмениваются компьютерные системы, используется протокол TLS вместо протокола SSL. Они настолько тесно связаны, что термины "SSL" и "TLS" (без версий) часто используются взаимозаменяемо. Из-за этого сходства ссылки на "SSL" в разделах Exchange, Центре администрирования Exchange и командной консоли Exchange часто используются для охвата протоколов SSL и TLS. Как правило, термин "SSL" обозначает именно протокол SSL только в тех случаях, когда указан номер версии (например, SSL 3.0). Чтобы узнать, почему следует отключить протокол SSL и переключиться на TLS, см. **статью Защита от уязвимости SSL 3.0** .

Шаг 2. Развертывание сервера AD FS

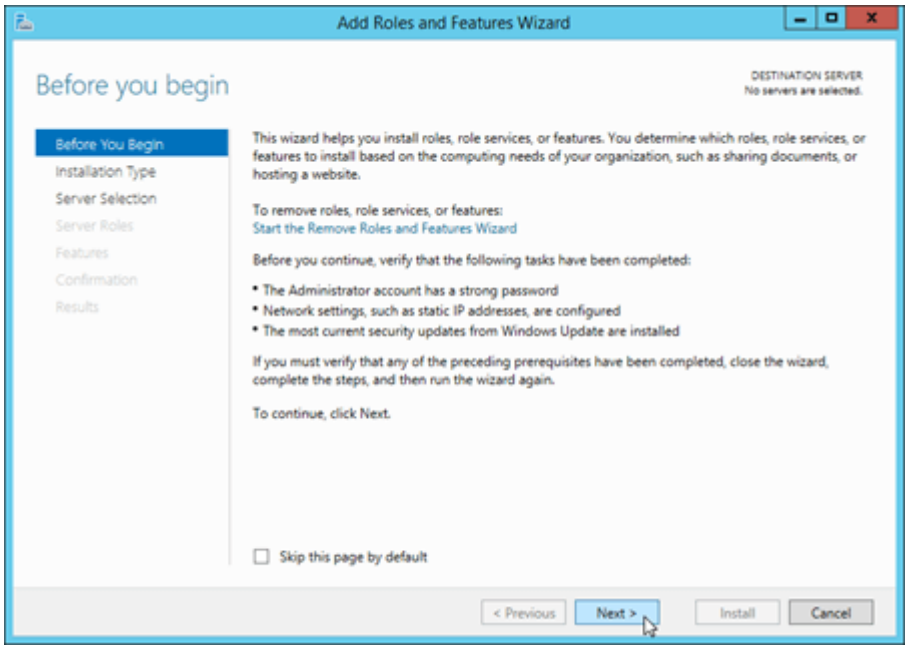
Для установки службы роли службы федерации Active Directory (AD FS) на целевом сервере можно использовать диспетчер сервера или Windows PowerShell.

Чтобы использовать диспетчер сервера для установки AD FS, выполните следующие действия.

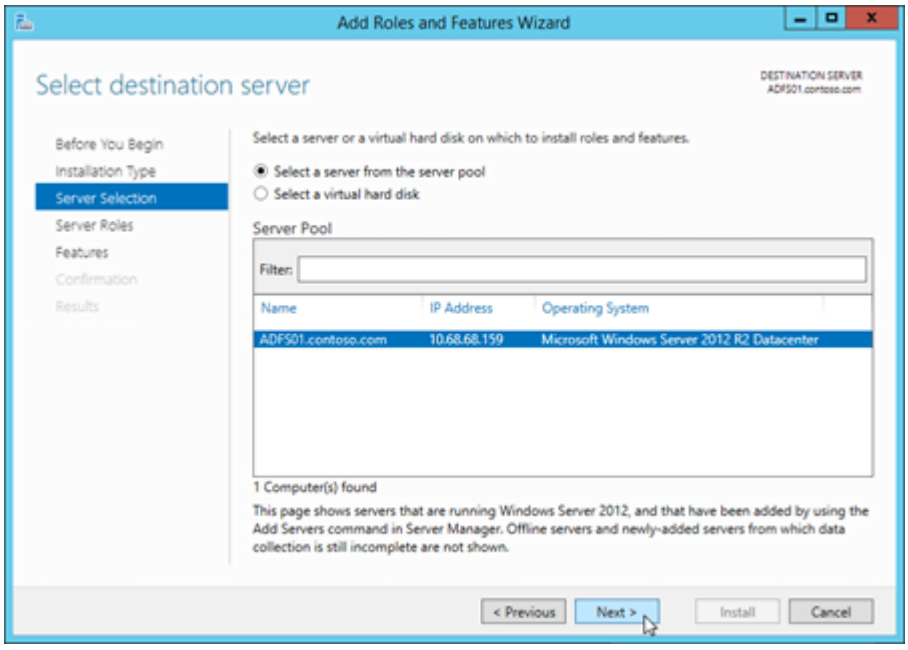
1. На целевом сервере откройте **диспетчер сервера**, щелкните **Управление**, а затем выберите **Добавить роли и компоненты**.



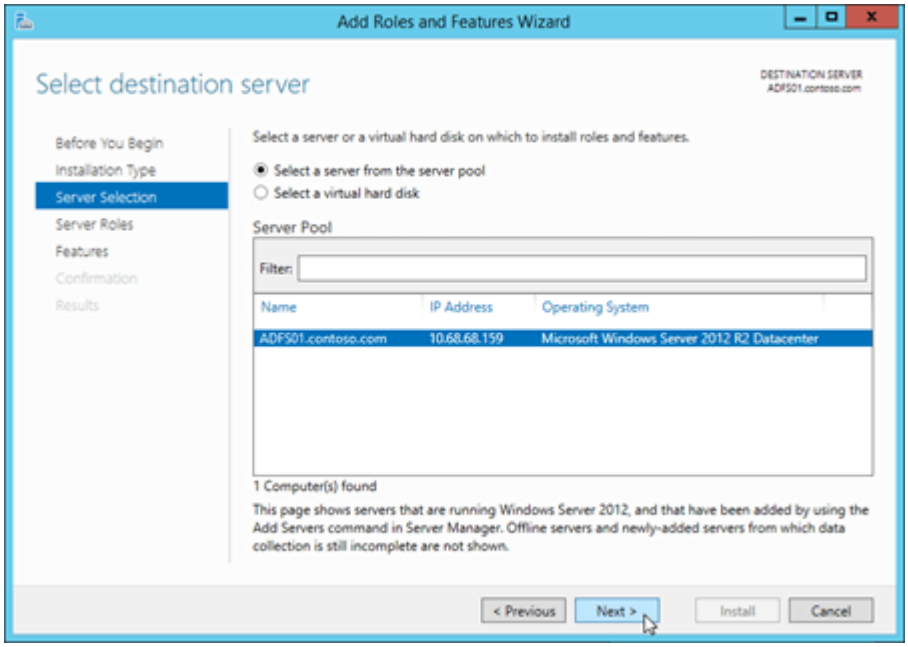
2. Откроется **мастер добавления ролей и компонентов** . Вы будете начинать с страницы **Перед началом работы** , если вы не выбрали **пропустить эту страницу по умолчанию**. Нажмите кнопку **Далее**.



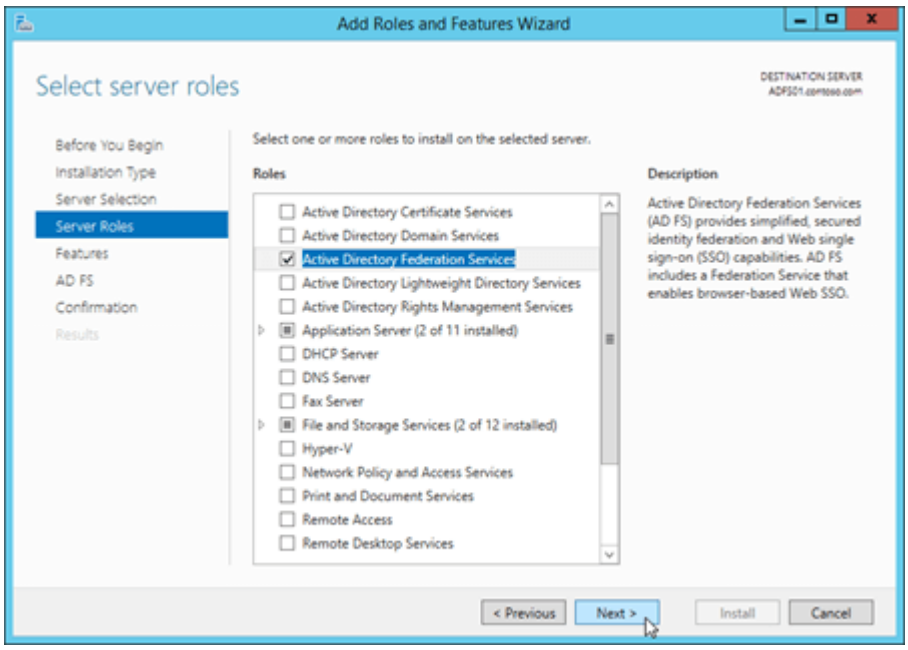
3. На странице **Выбор типа установки** убедитесь, что выбран параметр **Установка на основе ролей или компонентов** , а затем нажмите кнопку **Далее**.



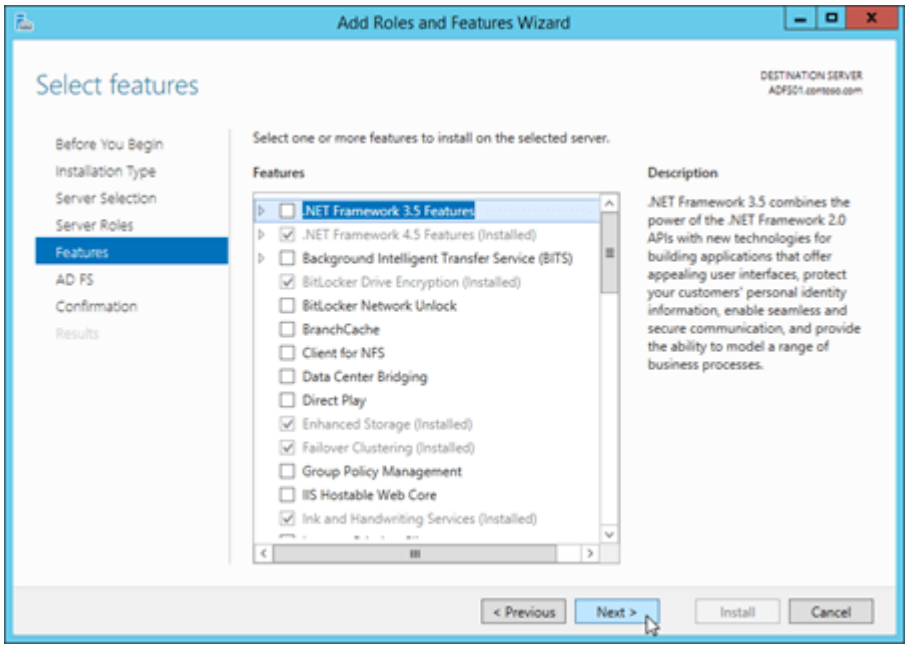
4. На странице **Выбор целевого сервера** проверьте выбор сервера и нажмите кнопку **Далее**.



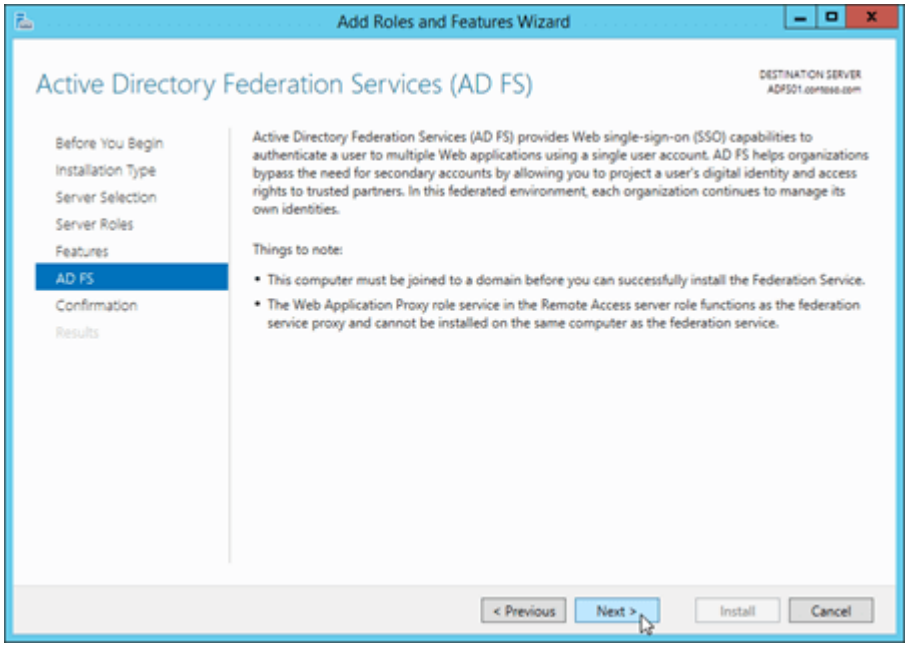
5. На странице **Выбор ролей сервера** выберите **службы федерации Active Directory (AD FS)** в списке и нажмите кнопку **Далее**.



6. На странице **Выбор компонентов** нажмите кнопку **Далее** (примите выбранные функции по умолчанию).

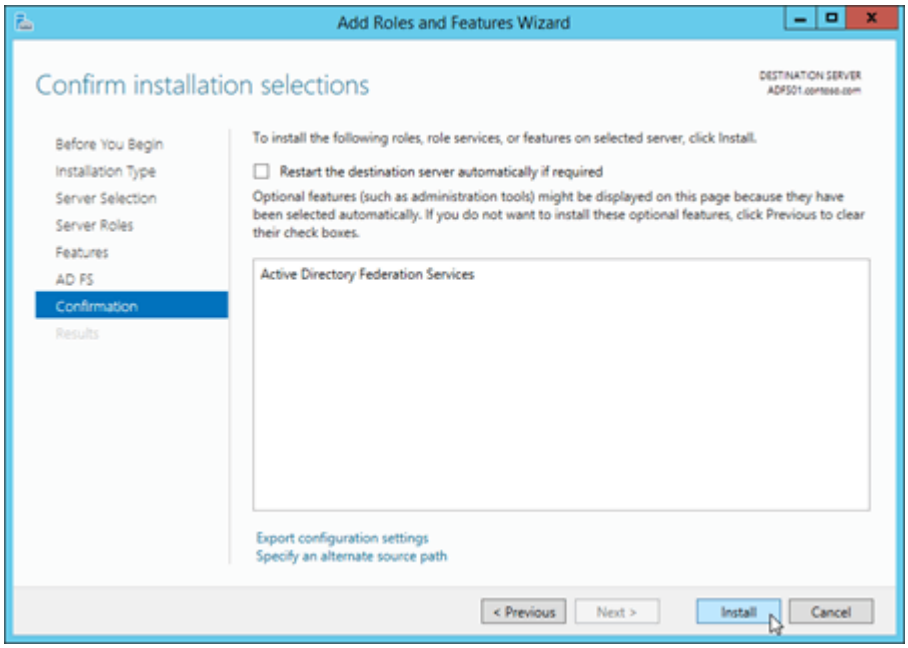


7. На странице **службы федерации Active Directory (AD FS) (AD FS)** нажмите кнопку **Далее**.

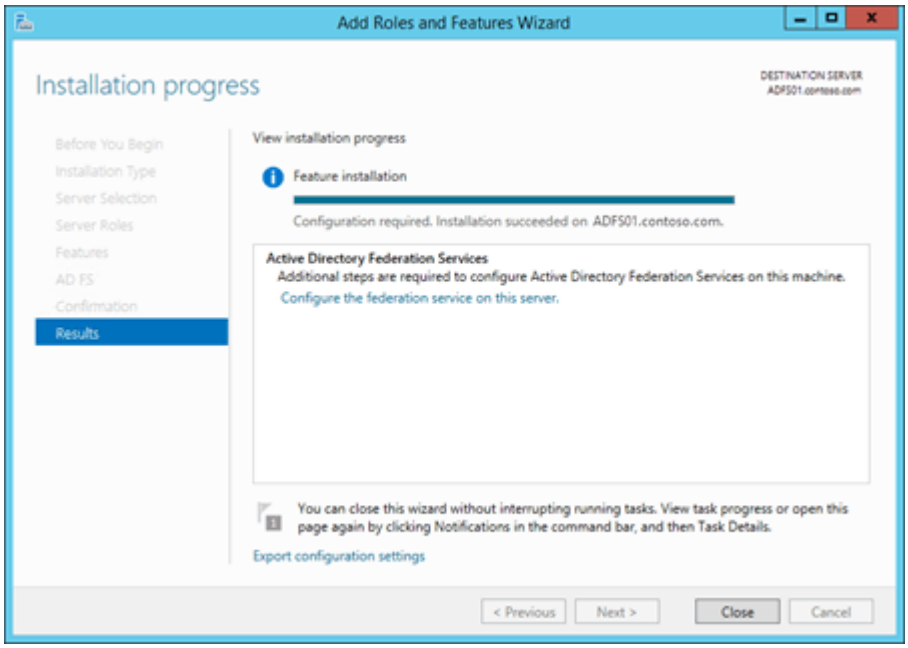


8. **только Windows Server 2012**. На странице **Выбор служб ролей** нажмите кнопку **Далее** (примите выбранные по умолчанию службы ролей).

9. На странице **Подтверждение выбранных вариантов установки** нажмите кнопку **Установить**.



10. На странице **Ход установки** можно просмотреть индикатор выполнения, чтобы убедиться, что установка прошла успешно. По завершении установки оставьте мастер открытым, чтобы щелкнуть **Настроить службу федерации на этом сервере** в разделе Шаг 3b. Настройка сервера AD FS.



Чтобы использовать Windows PowerShell для установки AD FS, выполните следующую команду:

PowerShell

```
Install-WindowsFeature ADFS-Federation -IncludeManagementTools
```

Шаг 3. Настройка и проверка сервера AD FS

Вы также можете ознакомиться с этим контрольным списком, чтобы помочь вам настроить AD FS : Контрольный список: Настройка сервера федерации.

Шаг 3a. Создание gMSA на контроллере домена

Перед настройкой сервера AD FS необходимо создать групповую управляемую учетную запись службы (gMSA) на контроллере домена Windows Server 2012 или более поздней версии. Это можно сделать в окне с повышенными привилегиями Windows PowerShell на контроллере домена (окно Windows PowerShell, открываемое путем выбора **запуска от имени администратора**).

1. Выполните следующую команду:

   ```
   PowerShell

   Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)
   ```

   Если команда выполнена успешно, возвращается значение GUID. Например:

   ```
   Guid
   ----
   2570034b-ab50-461d-eb80-04e73ecf142b
   ```

2. Чтобы создать учетную запись gMSA для сервера AD FS, используйте следующий синтаксис:

   ```
   PowerShell

   New-ADServiceAccount -Name <AccountName> -DnsHostName
   <FederationServiceName> -ServicePrincipalNames
   http/<FederationServiceName>
   ```

   В этом примере создается учетная запись gMSA с именем FSgMSA для службы федерации с именем adfs.contoso.com. Имя службы федерации — это значение, видимое для клиентов.

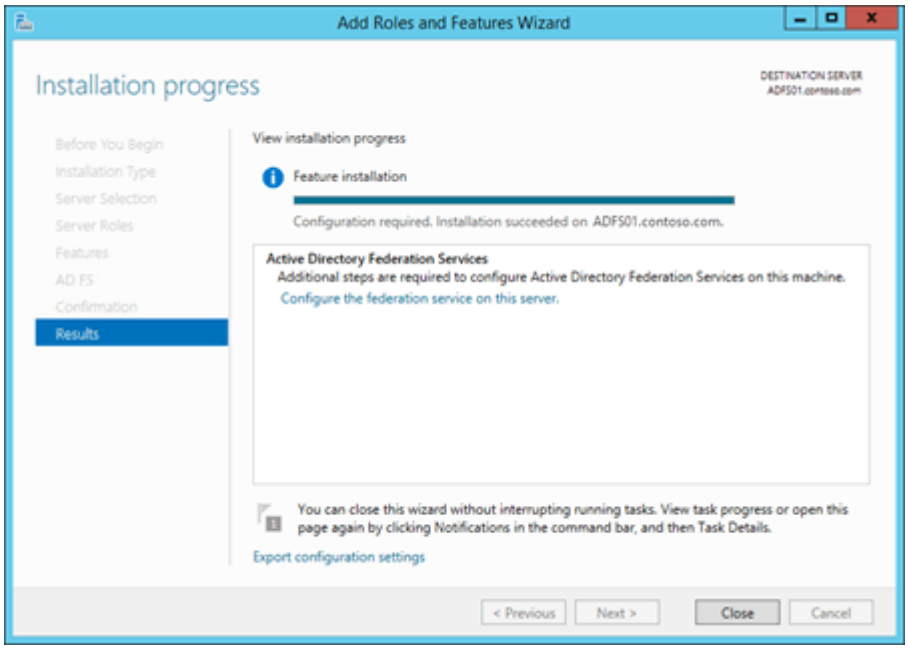
   ```
   PowerShell

   New-ADServiceAccount -Name FSgMSA -DnsHostName adfs.contoso.com -
   ServicePrincipalNames http/adfs.contoso.com
   ```

Шаг 3b. Настройка сервера AD FS

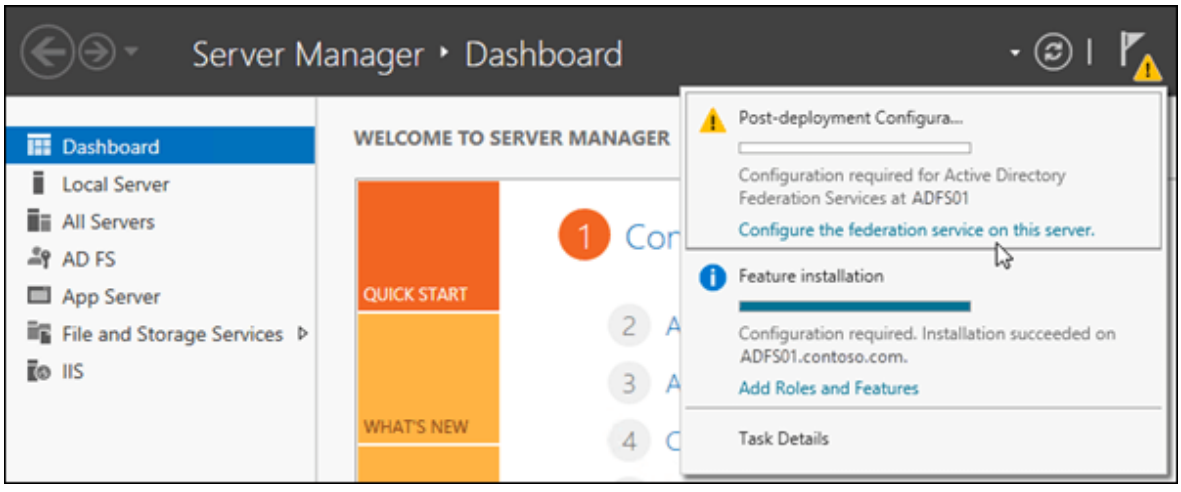
Чтобы настроить сервер AD FS, можно использовать диспетчер сервера или Windows PowerShell.

Чтобы использовать диспетчер сервера, выполните следующие действия.

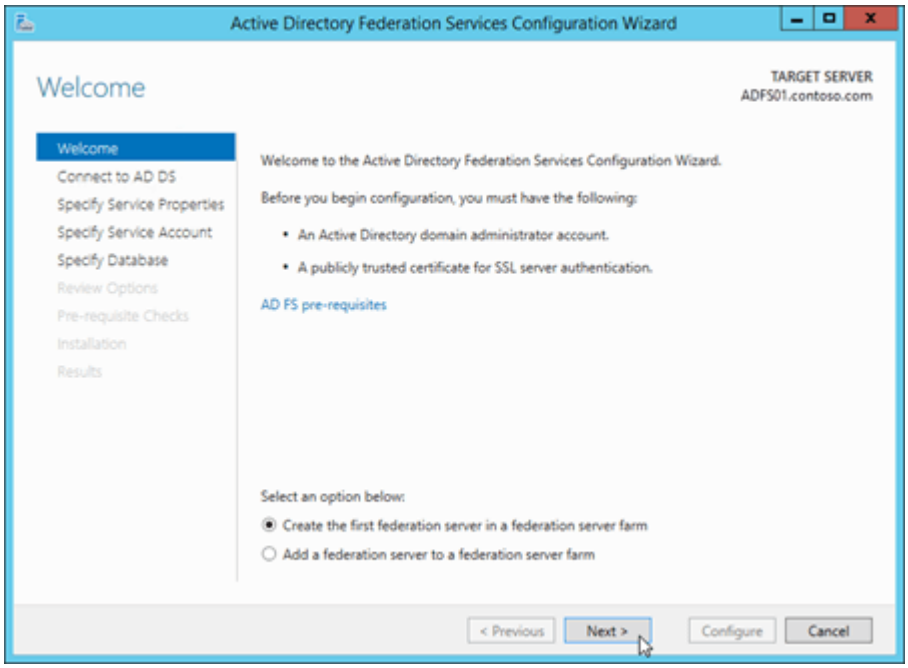
1. Если вы оставили **мастер добавления ролей и компонентов** открытым на сервере AD FS из шага 2. Развертывание сервера AD FS, щелкните ссылку **Настройка службы федерации на этом сервере** на странице **Ход установки** .



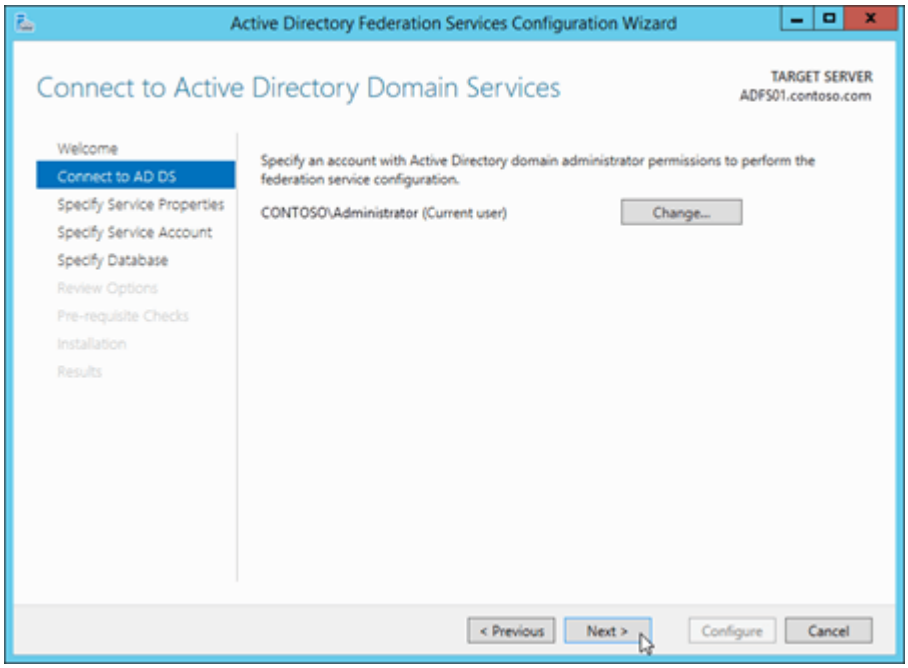
Если вы закрыли **мастер добавления ролей и компонентов** или использовали Windows PowerShell для установки AD FS, вы можете перейти к тому же месту в диспетчер сервера, щелкнув **Уведомления**, а затем выбрав **Настроить службу федерации на этом сервере** в **предупреждении Конфигурация после развертывания**.



2. Откроется **мастер службы федерации Active Directory (AD FS)**. На странице **Приветствие** убедитесь, что выбран пункт **Создать первый сервер федерации в ферме серверов федерации** , а затем нажмите кнопку **Далее**.



3. На странице **Подключение к службы федерации Active Directory (AD FS)** выберите учетную запись администратора домена в домене, где находится сервер AD FS (текущие учетные данные выбраны по умолчанию). Если необходимо выбрать другого пользователя, нажмите кнопку **Изменить**. По завершении нажмите кнопку **Далее**.



4. На странице **Указание свойств службы** настройте следующие параметры:

   - **SSL-сертификат**. Импортируйте или выберите SSL-сертификат, содержащий имя службы федерации, настроенное на шаге 3a. Создание gMSA на контроллере домена (например `adfs.contoso.com`,). При импорте сертификата, который еще не установлен на сервере, необходимо импортировать PFX-файл (скорее всего, защищенный

паролем файл, содержащий закрытый ключ сертификата). Здесь отображается значение общего имени (CN) в поле Subject сертификата.

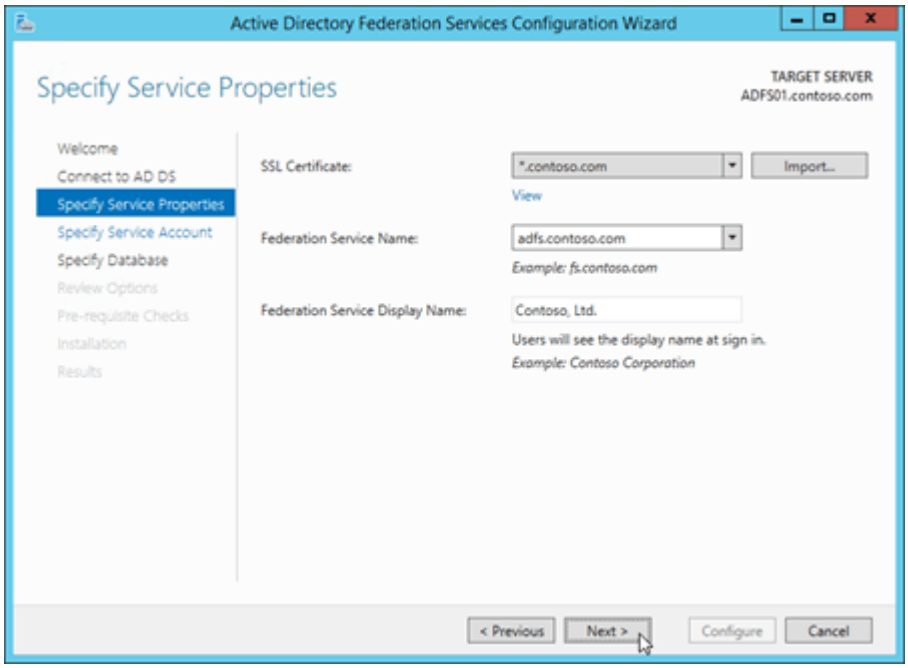
- **Имя службы федерации**. Это поле заполняется автоматически в зависимости от типа выбранного или импортируемого SSL-сертификата:
  - **Сертификат с одним субъектом**: отображается значение CN в поле Subject сертификата, и его нельзя изменить (например, `adfs.contoso.com`).
  - **Сертификат SAN**. Если сертификат содержит требуемое имя службы федерации, отображается это значение (например, `adfs.contoso.com`). Вы можете использовать раскрывающийся список, чтобы просмотреть другие значения CN в сертификате.
  - **Сертификат с подстановочным знаком**: отображается значение CN в поле Subject сертификата (например, `*.contoso.com`), но его необходимо изменить на обязательное имя службы федерации (например, `adfs.contoso.com`).

  Примечание. Если выбираемый сертификат не содержит требуемого имени службы федерации (поле **Имя службы федерации** не содержит обязательного значения), вы получите следующую ошибку:

  `The federation service name does not match any of the subject names found in the certificate.`

- **Отображаемое имя службы федерации**. Введите название организации. Например, Contoso, Ltd..

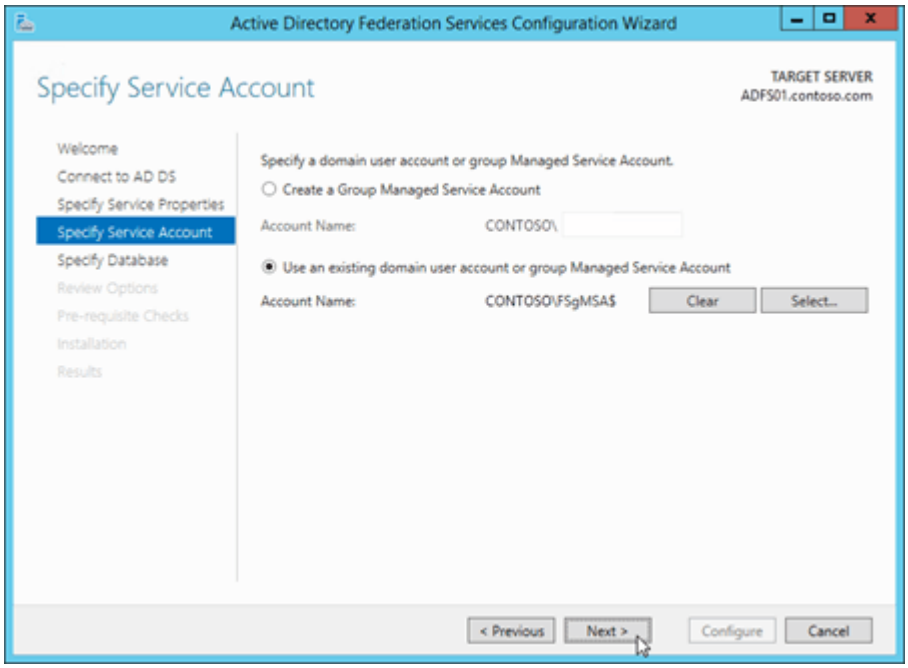
По завершении нажмите кнопку **Далее**.



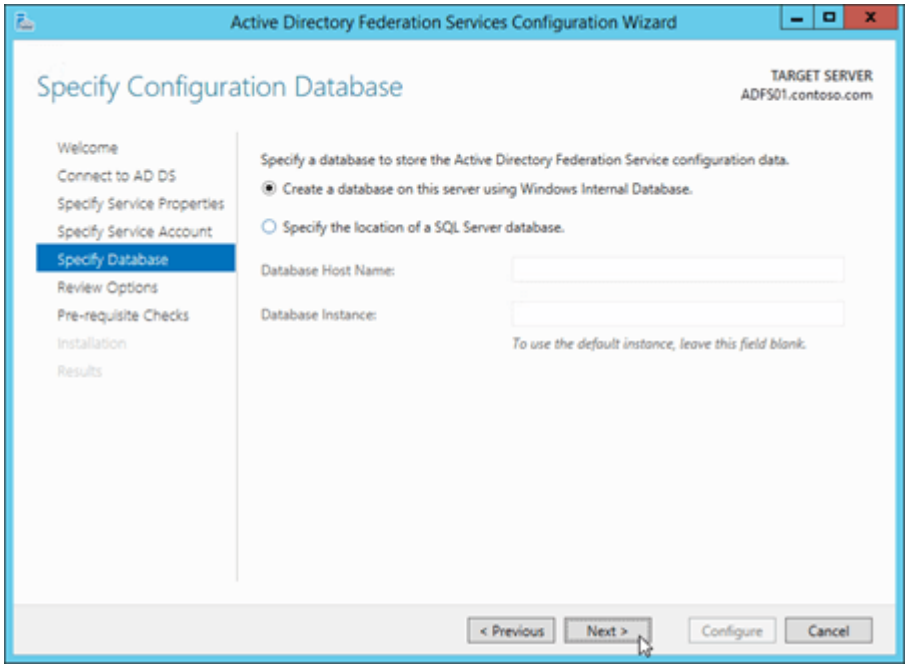
5. На странице **Указание учетной записи службы** настройте следующие параметры:

   - Выберите **Использовать существующую учетную запись пользователя домена или групповую управляемую учетную запись службы**.
   - **Имя учетной записи**. Щелкните **Выбрать** и введите учетную запись gMSA, созданную на шаге 3a. Создание gMSA на контроллере домена (например, `FSgMSA`). Обратите внимание, что после его выбора отображается `<Domain>\<gMSAAccountName>$` значение (например, `CONTOSO\FSgMSA$`).

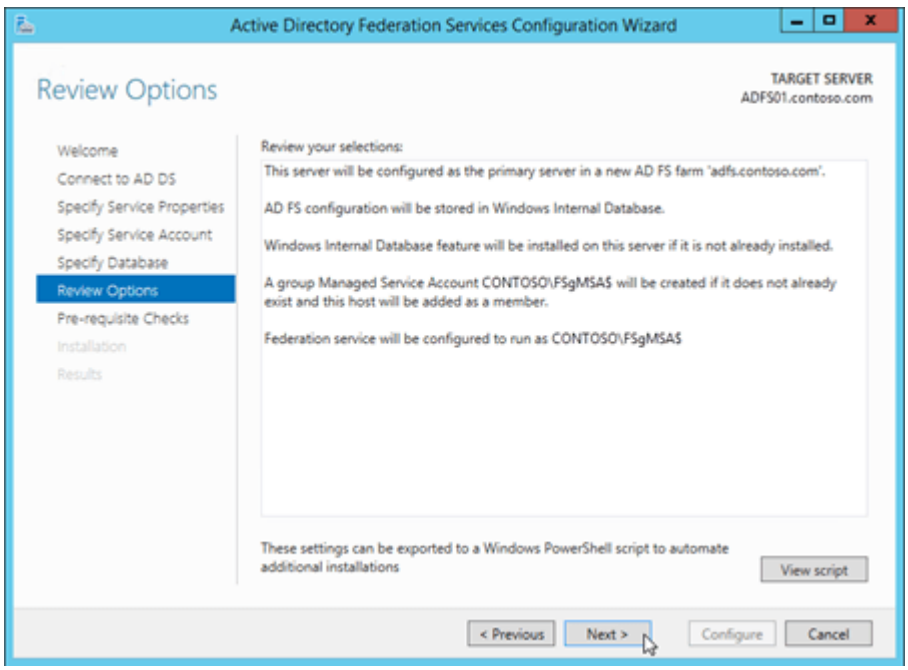
   По завершении нажмите кнопку **Далее**.



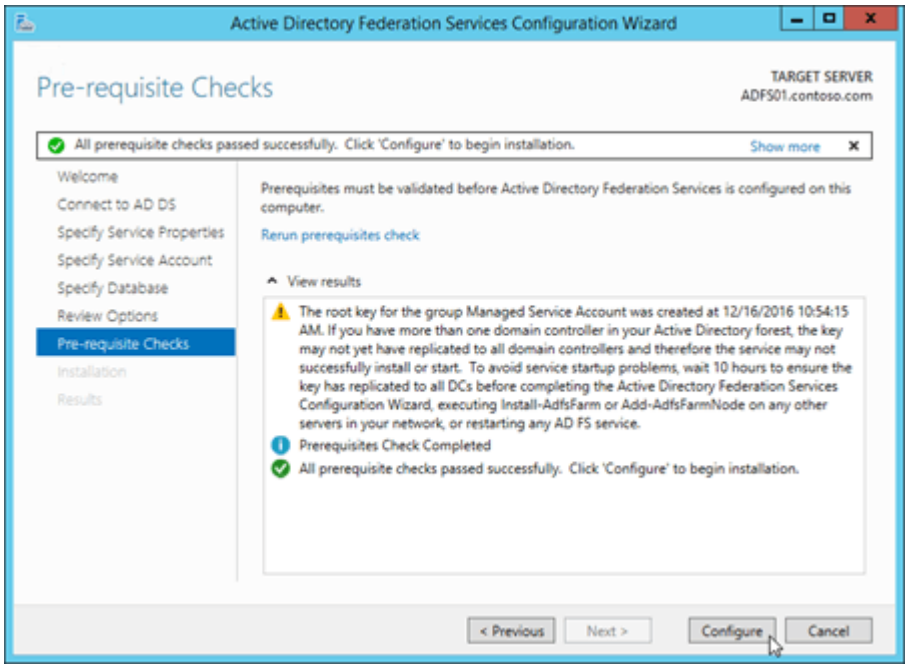
6. На странице **Укажите базу данных конфигурации** убедитесь, что выбран параметр **Создать базу данных на этом сервере с помощью внутренняя база данных Windows**, а затем нажмите кнопку **Далее**.



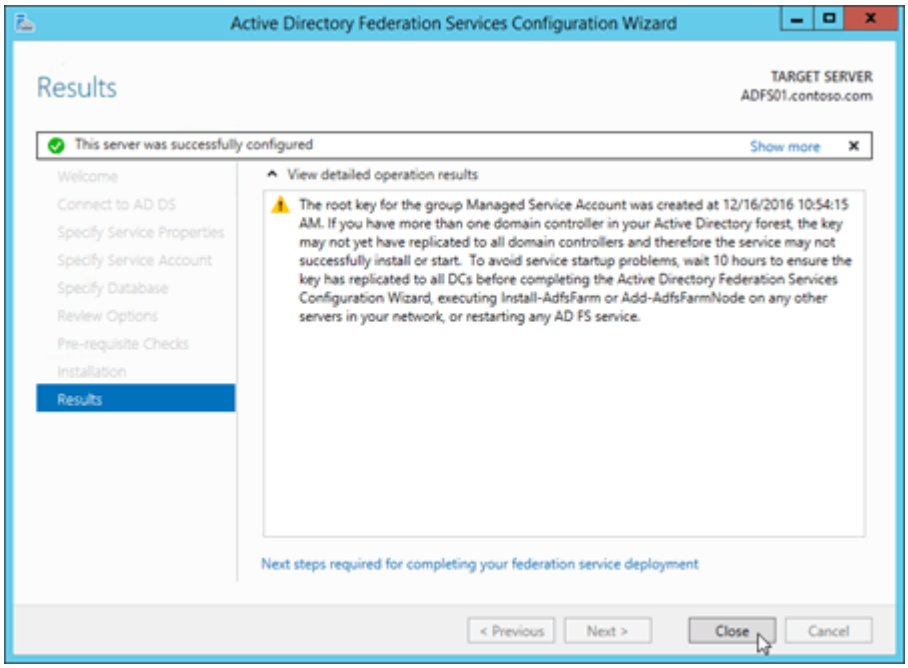
7. На странице **Параметры проверки** проверьте выбранные параметры. Вы можете нажать кнопку **Просмотреть скрипт**, чтобы скопировать Windows PowerShell эквивалент выбранных для использования в будущем. По завершении нажмите кнопку **Далее**.



8. На странице **Предварительные проверки** убедитесь, что все проверки необходимых компонентов успешно завершены, и нажмите кнопку **Настроить**.



9. На странице **Результаты** просмотрите результаты и убедитесь, что настройка успешно завершена. Если вы хотите прочитать о следующих шагах (например, настройка DNS), щелкните **Дальнейшие действия, необходимые для завершения развертывания службы федерации** . Когда закончите, нажмите кнопку **Закрыть**.



Чтобы использовать Windows PowerShell для настройки AD FS, выполните следующие действия.

1. Выполните следующую команду на сервере AD FS, чтобы найти значение отпечатка установленного сертификата, содержащего `adfs.contoso.com`:

```
PowerShell
```

```
Set-Location Cert:\LocalMachine\My; Get-ChildItem | Format-List
FriendlyName,Subject,Thumbprint
```

2. Выполните следующую команду:

```
PowerShell

Import-Module ADFS
```

3. Используйте следующий синтаксис.

```
PowerShell

Install-AdfsFarm -CertificateThumbprint <ThumbprintValue> -
FederationServiceName <FederationServiceName> -
FederationServiceDisplayName <FederationServiceDisplayName> -
GroupServiceAccountIdentifier <gMSA>
```

В этом примере ad FS настраивается со следующими параметрами:

- **adfs.contoso.com отпечаток сертификата**: `*.contoso.com` сертификат, имеющий значение `5AE82C737900B29C2BAC3AB6D8C44D249EE05609` отпечатка .
- **Имя службы федерации**: `adfs.contoso.com`
- **Отображаемое имя службы федерации**: `Contoso, Ltd.`
- **Имя учетной записи и домен sam федерации gMSA**. Например, для учетной записи gMSA с именем `FSgMSA` в `contoso.com` домене обязательное значение равно `contoso\FSgMSA$`.

```
PowerShell

Install-AdfsFarm -CertificateThumbprint
5AE82C737900B29C2BAC3AB6D8C44D249EE05609 -FederationServiceName
adfs.contoso.com -FederationServiceDisplayName "Contoso, Ltd." -
GroupServiceAccountIdentifier "contoso\FSgMSA`$"
```

Примечания.

- При создании gMSA автоматически добавляется к значению **Name**, `$` чтобы создать значение **SamAccountName**, которое здесь требуется.
- Escape-символ (''') требуется для `$` в **SamAccountName**.

Дополнительные сведения и синтаксис см. в статье Install-AdfsFarm.

Шаг 3c. Тестирование сервера AD FS

После настройки AD FS можно проверить установку на сервере AD FS, успешно открыв URL-адрес метаданных федерации в веб-браузере. В URL-адресе используется синтаксис `https://<FederationServiceName>/federationmetadata/2007-06/federationmetadata.xml`. Например, `https://adfs.contoso.com/federationmetadata/2007-06/federationmetadata.xml`.

Шаг 4. Создание правил доверия проверяющей стороны и настраиваемых утверждений в AD FS для Outlook в Интернете и EAC

- На сервере Exchange server Outlook в Интернете использует виртуальный каталог с именем `owa`, а EAC — виртуальный каталог с именем `ecp`.
- Косая черта (`/`), используемая в значениях URL-адреса Outlook в Интернете и EAC, является преднамеренным. Важно, чтобы отношения доверия проверяющей стороны AD FS и URI аудитории Exchange **были идентичными**. Они **оба должны иметь** или **оба должны пропускать** конечные косые черты в своих URL-адресах. Примеры в этом разделе содержат конечные косые черты после URL-адресов owa и ecp (`owa/` и `ecp/`).
- В организациях с несколькими сайтами Active Directory, которые используют отдельные пространства имен (например, и `na.contoso.com`), необходимо настроить отношения доверия с проверяющей стороной для каждого пространства имен как для Outlook в Интернете, `eu.contoso.com` так и для центра администрирования EAC.

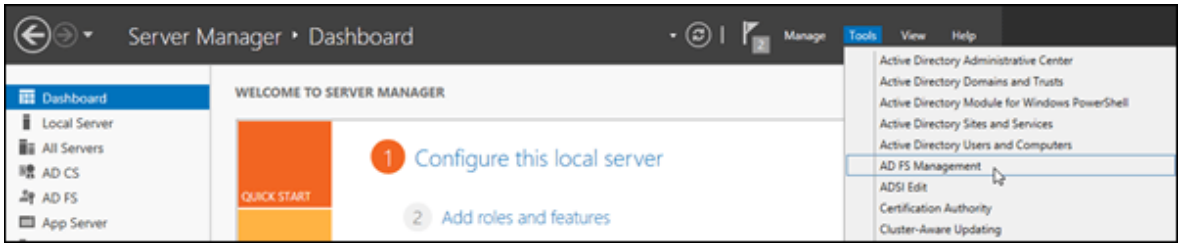
Шаг 4a. Создание отношений доверия с проверяющей стороной в AD FS для Outlook в Интернете и EAC

Чтобы создать отношения доверия с проверяющей стороной на сервере AD FS, можно использовать консоль управления AD FS или Windows PowerShell.

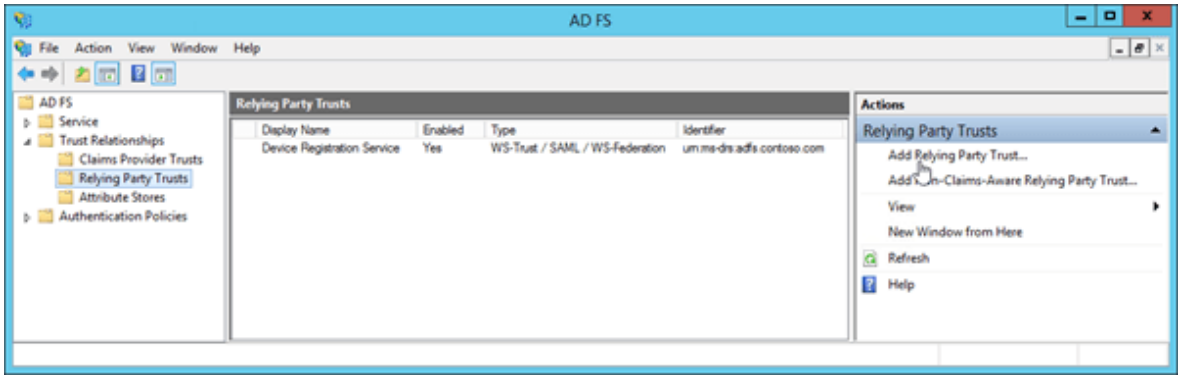
Чтобы использовать консоль управления AD FS для создания отношений доверия с проверяющей стороной, выполните следующие действия.

Примечание. Эти действия необходимо выполнить дважды: один раз для Outlook в Интернете и один раз для EAC. Единственное различие заключается в значениях, которые вы вводите на шагах 5 и 8 (страницы **Указание отображаемого имени** и **Настройка URL-адреса** в мастере).

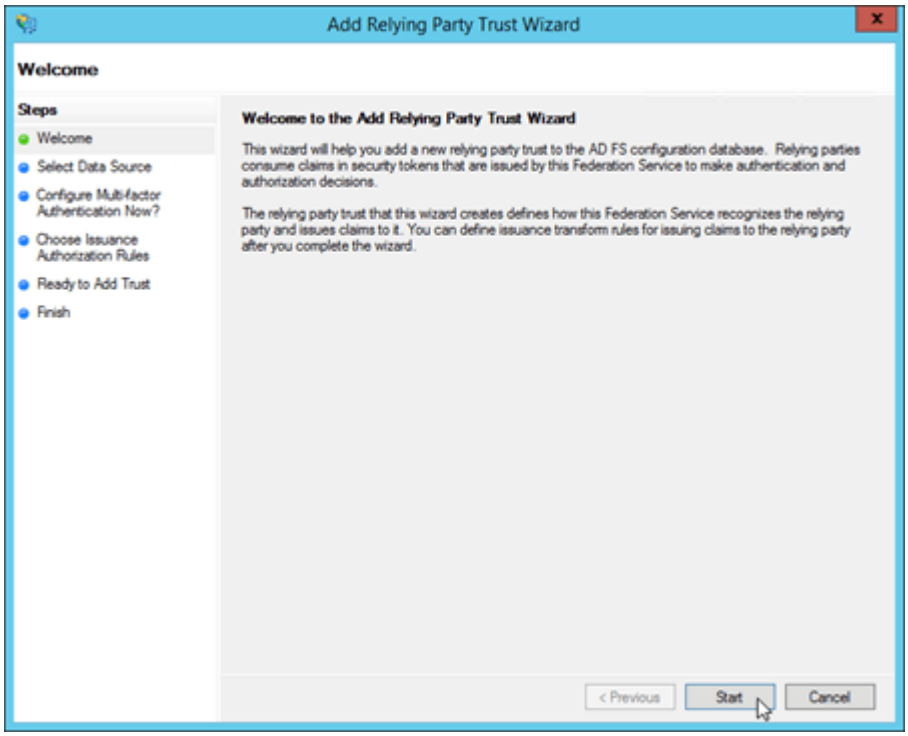
1. В окне **Диспетчер серверов** выберите **Средства**, а затем выберите **Управление AD FS**.



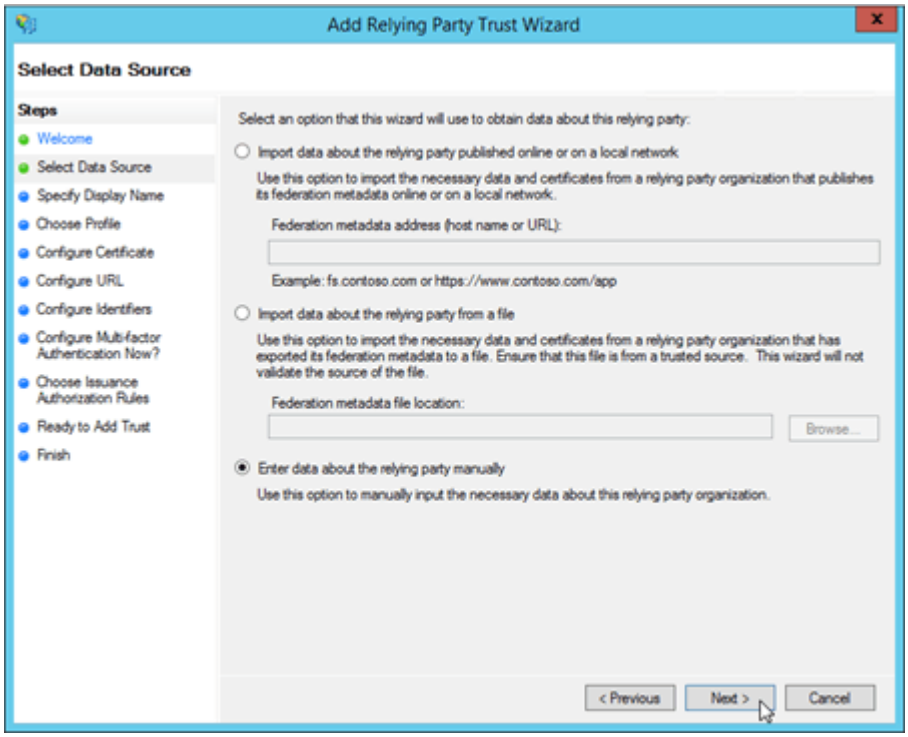
2. В консоли управления AD FS разверните узел **Отношения доверия** , а затем выберите **Отношения доверия проверяющей стороны**. В области **Действия** выберите **Добавить доверие проверяющей стороны**.



3. **Откроется мастер добавления доверия проверяющей стороны**. На странице **Добро пожаловать** нажмите кнопку **Пуск**.

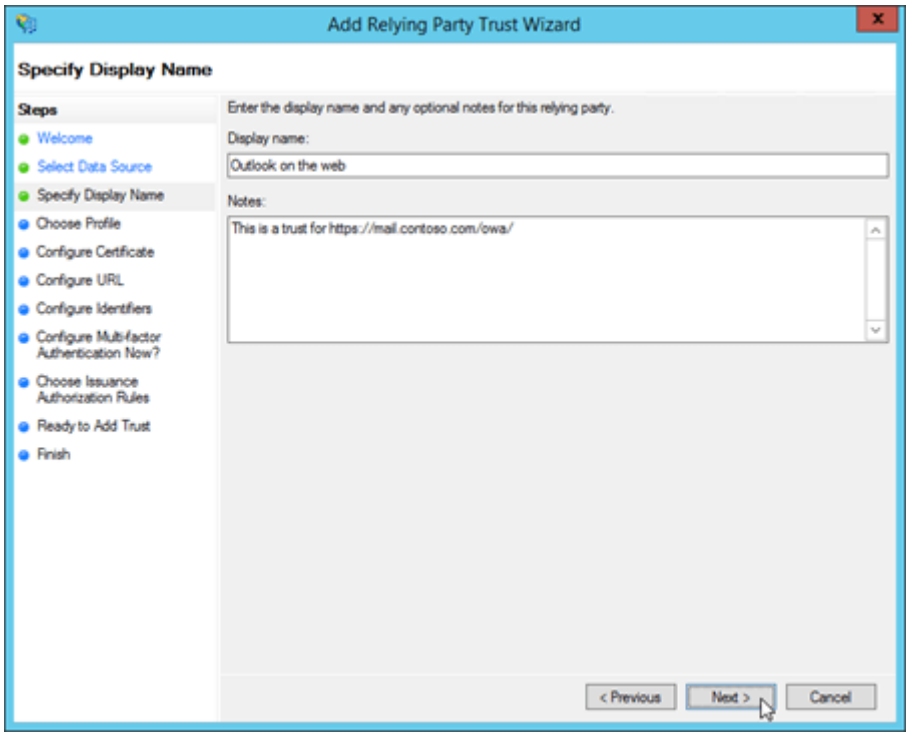


4. На странице **Выбор источника данных** выберите **Ввести данные о проверяющей стороне вручную** и нажмите кнопку **Далее**.

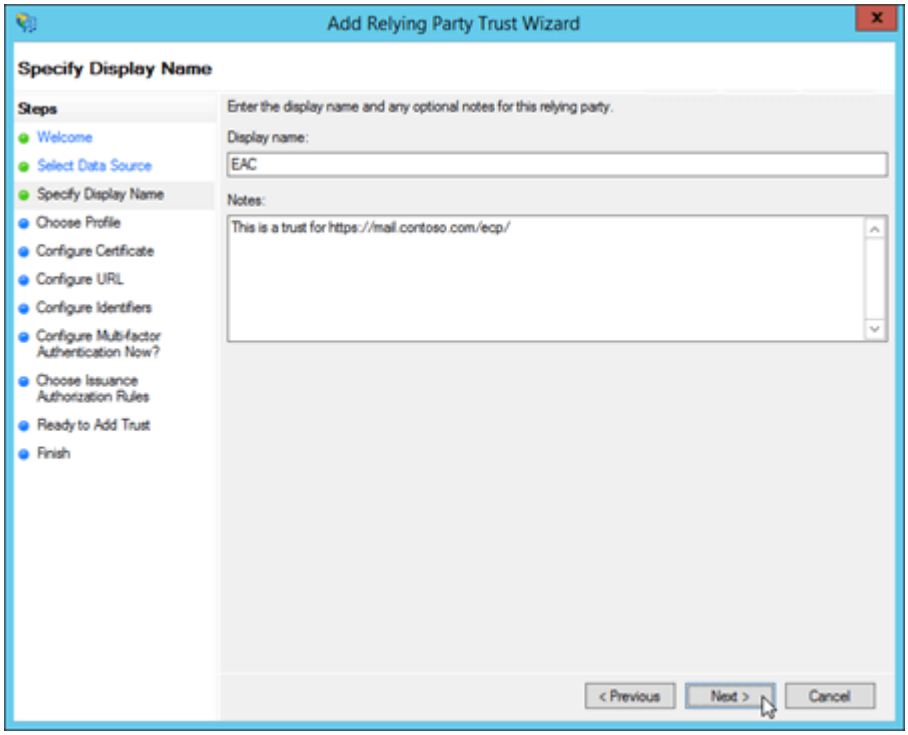


5. На странице **Указание отображаемого имени** настройте следующие параметры:

   - **Для Outlook в Интернете**:
   - **Отображаемое имя**: введите Outlook в Интернете.
   - **Примечания**. Введите описание. Например, это доверие для https://mail.contoso.com/owa/ .

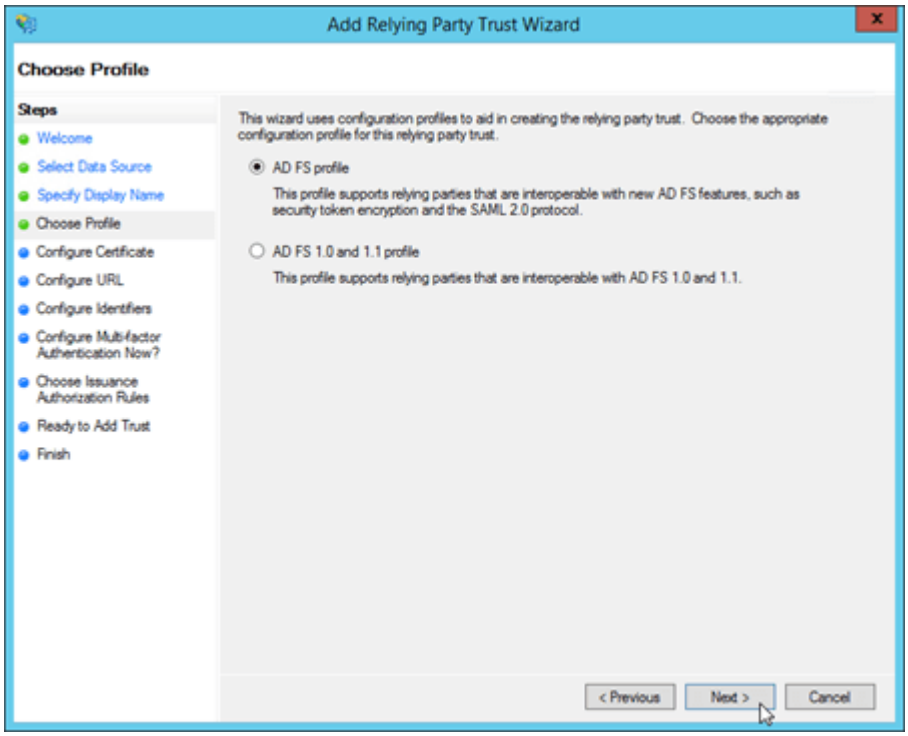


- **Для Центра администрирования EAC**:
- **Отображаемое имя**: введите EAC.
- **Примечания**. Введите описание. Например, это доверие для https://mail.contoso.com/ecp/ .

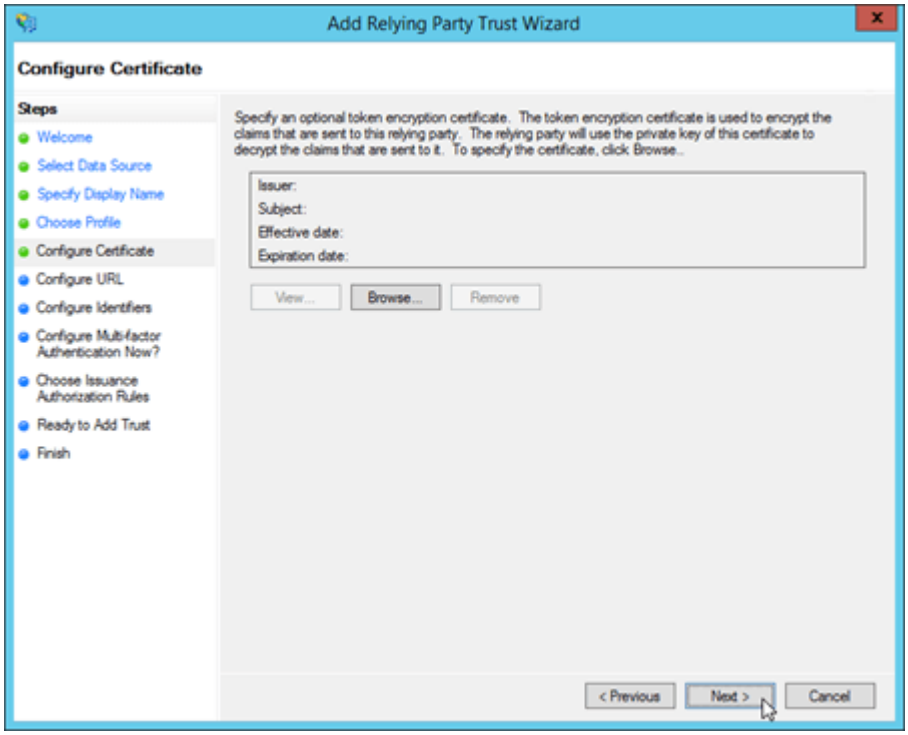


По завершении нажмите кнопку **Далее**.

6. На странице **Выбор профиля** убедитесь, что выбран **профиль AD FS** и нажмите кнопку **Далее**.

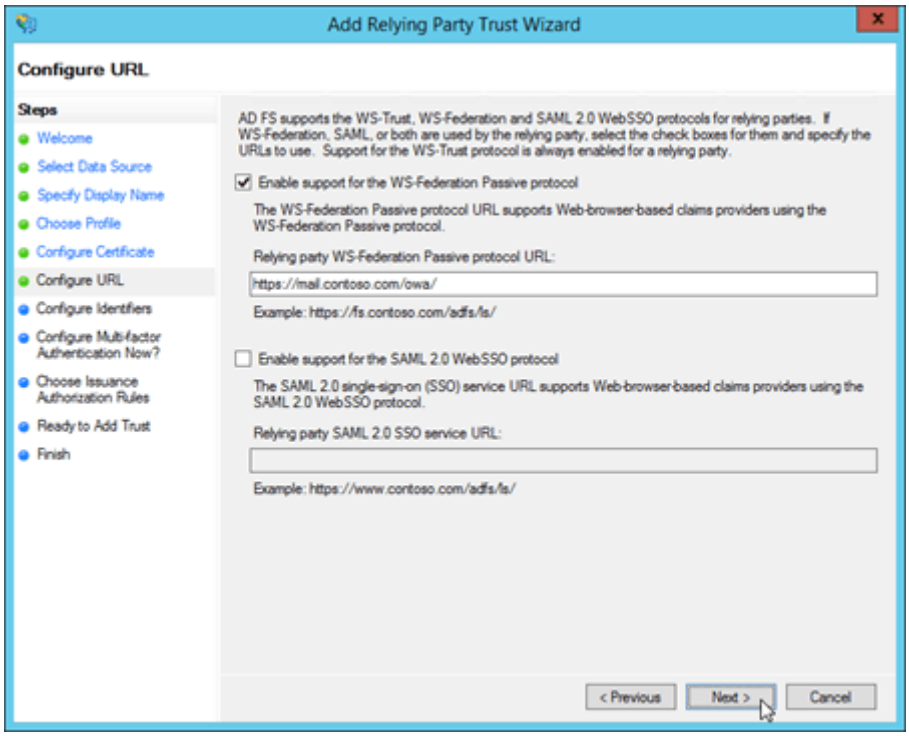


7. На странице **Настройка сертификата** нажмите кнопку **Далее** (не указывайте необязательный сертификат шифрования маркеров).



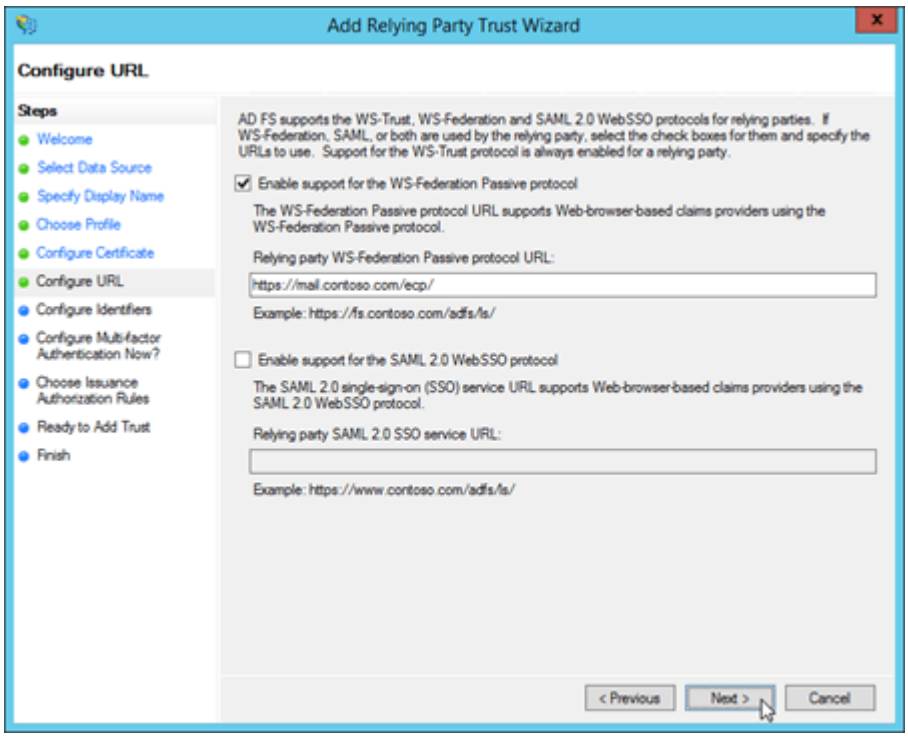
8. На странице **Настройка URL-адреса** выберите **Включить поддержку пассивного протокола WS-Federation** и в поле **Url-адрес пассивного протокола проверяющей стороны WS-Federation введите** следующие сведения:

   - **Outlook в Интернете**: введите URL-адрес внешнего Outlook в Интернете (например, https://mail.contoso.com/owa/).

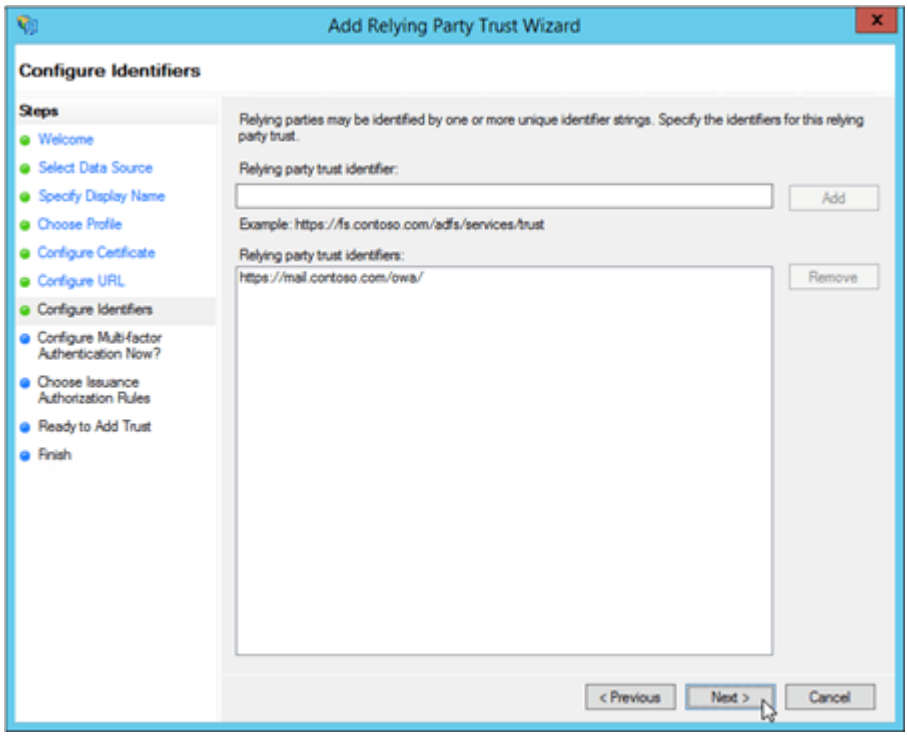


- **EAC**: введите внешний URL-адрес EAC (например, https://mail.contoso.com/ecp/).

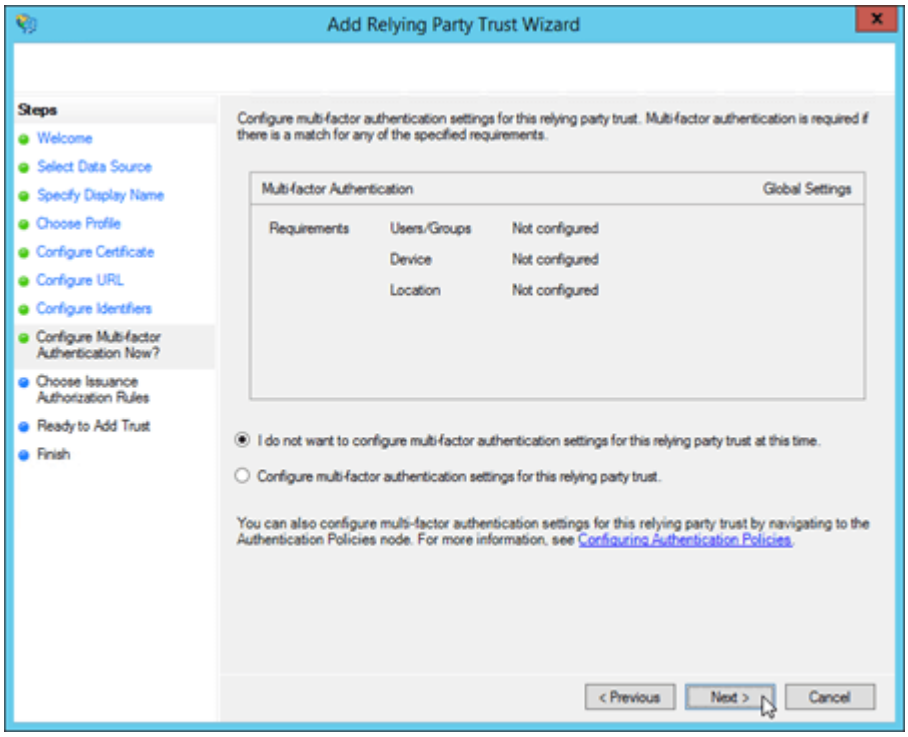
По завершении нажмите кнопку **Далее**.



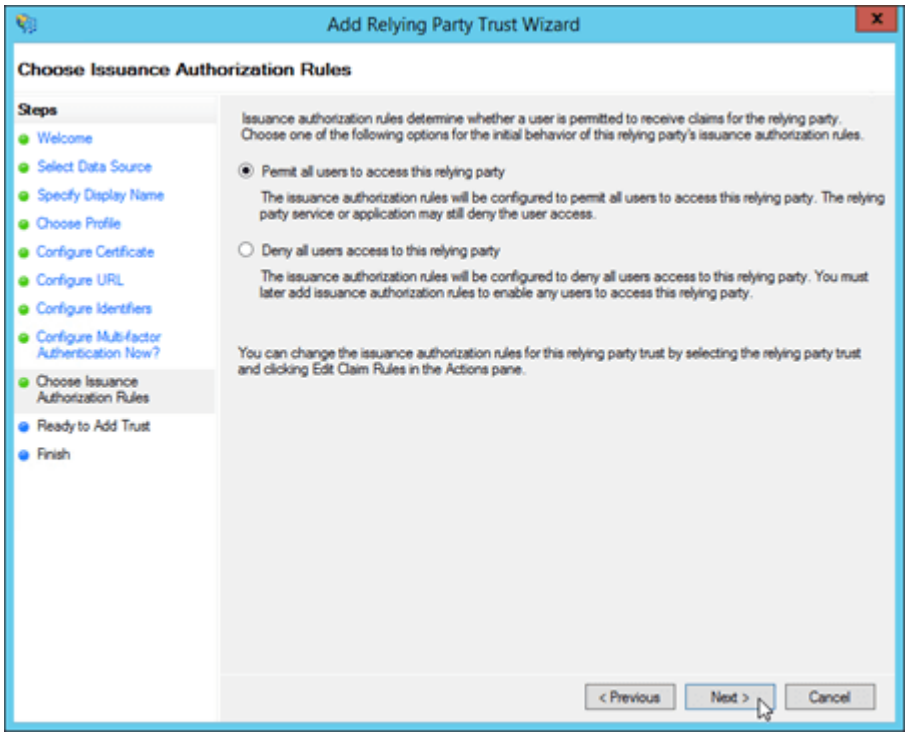
9. На странице **Настройка идентификаторов** нажмите кнопку **Далее** (URL-адрес из предыдущего шага указан в разделе **Идентификаторы доверия проверяющей стороны**).



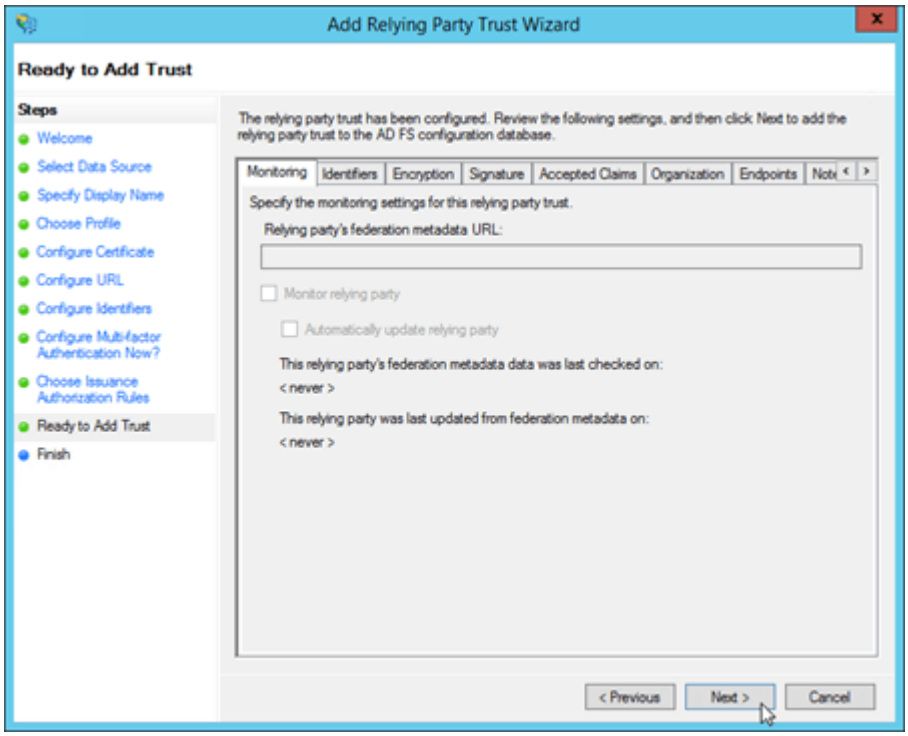
10. На странице **Настройка многофакторной идентификации сейчас?** убедитесь, что **я не хочу настраивать параметры многофакторной проверки подлинности для этого отношения доверия с проверяющей стороной** , и нажмите кнопку **Далее**.



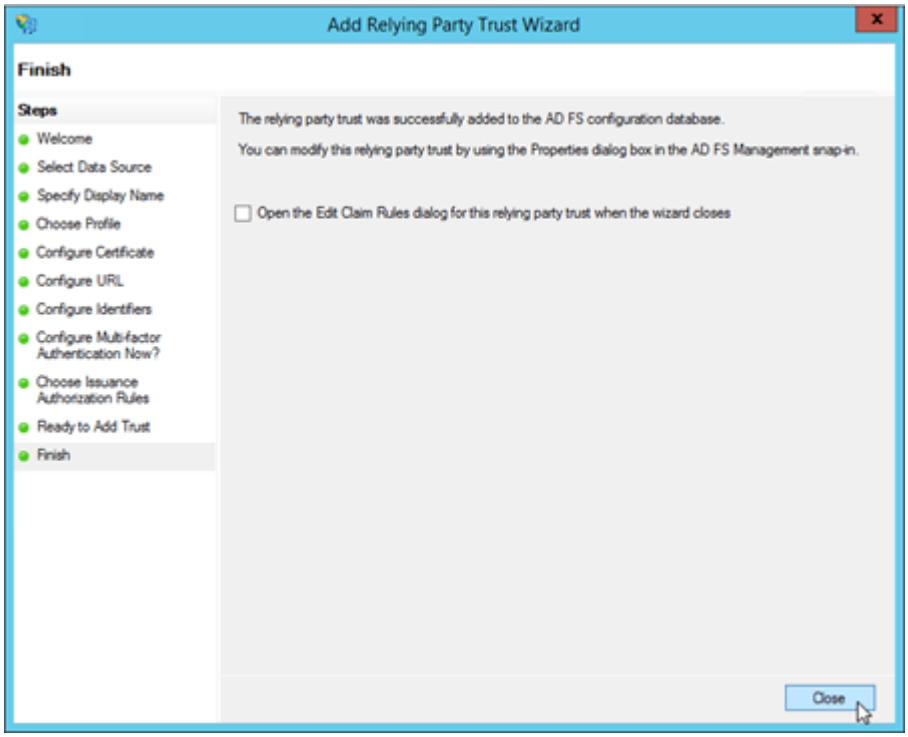
11. На странице **Выбор правил авторизации выдачи** установите **флажок Разрешить всем пользователям доступ к этой проверяющей стороне** выбран, а затем нажмите кнопку **Далее**.



12. На странице **Готово для добавления доверия** проверьте настройки, а затем нажмите кнопку **Далее**, чтобы сохранить сведения об отношении доверия с проверяющей стороной.



13. На странице **Готово** снимите флажок **Открыть диалоговое окно Изменение правил утверждений для этого отношения доверия проверяющей стороны при закрытии мастера**, а затем нажмите кнопку **Закрыть**.



Чтобы использовать Windows PowerShell запрос на создание отношений доверия с проверяющей стороной, выполните следующие действия.

1. В окне Windows PowerShell с повышенными привилегиями выполните следующую команду:

```
PowerShell

Import-Module ADFS
```

2. Используйте следующий синтаксис.

```
PowerShell

Add-AdfsRelyingPartyTrust -Name <"Outlook on the web" | EAC> -Notes
"This is a trust for <OotwURL | EACURL>" -Identifier <OotwURL | EACURL>
-WSFedEndpoint <OotwURL | EACURL> -IssuanceAuthorizationRules
'@RuleTemplate = "AllowAllAuthzRule" => issue(Type =
"http://schemas.microsoft.com/authorization/claims/permit", Value =
"true");' -IssueOAuthRefreshTokensTo NoDevice
```

В этом примере создается доверие проверяющей стороны для Outlook в Интернете с использованием следующих значений:

- **Имя**: Outlook в Интернете
- **Примечания**. Это доверие для https://mail.contoso.com/owa/
- **Идентификатор**: https://mail.contoso.com/owa/
- **WSFedEndpoint**: https://mail.contoso.com/owa/

PowerShell

```
Add-AdfsRelyingPartyTrust -Name "Outlook on the web" -Notes "This is a trust
for https://mail.contoso.com/owa/" -Identifier https://mail.contoso.com/owa/
-WSFedEndpoint https://mail.contoso.com/owa/ -IssuanceAuthorizationRules
'@RuleTemplate = "AllowAllAuthzRule" => issue(Type =
"http://schemas.microsoft.com/authorization/claims/permit", Value =
"true");' -IssueOAuthRefreshTokensTo NoDevice
```

В этом примере создается доверие проверяющей стороны для центра администрирования EAC, используя следующие значения:

- **Имя**: EAC
- **Примечания**. Это доверие для https://mail.contoso.com/ecp/
- **Идентификатор**: https://mail.contoso.com/ecp/
- **WSFedEndpoint**: https://mail.contoso.com/ecp/

PowerShell

```
Add-AdfsRelyingPartyTrust -Name EAC -Notes "This is a trust for
https://mail.contoso.com/ecp/" -Identifier https://mail.contoso.com/ecp/ -
WSFedEndpoint https://mail.contoso.com/ecp/ -IssuanceAuthorizationRules
'@RuleTemplate = "AllowAllAuthzRule" => issue(Type =
"http://schemas.microsoft.com/authorization/claims/permit", Value =
"true");' -IssueOAuthRefreshTokensTo NoDevice
```

Шаг 4b. Создание настраиваемых правил утверждений в AD FS для Outlook в Интернете и EAC

Для Outlook в Интернете и EAC необходимо создать два правила утверждений:

- ИД безопасности пользователя Active Directory
- UPN Active Directory

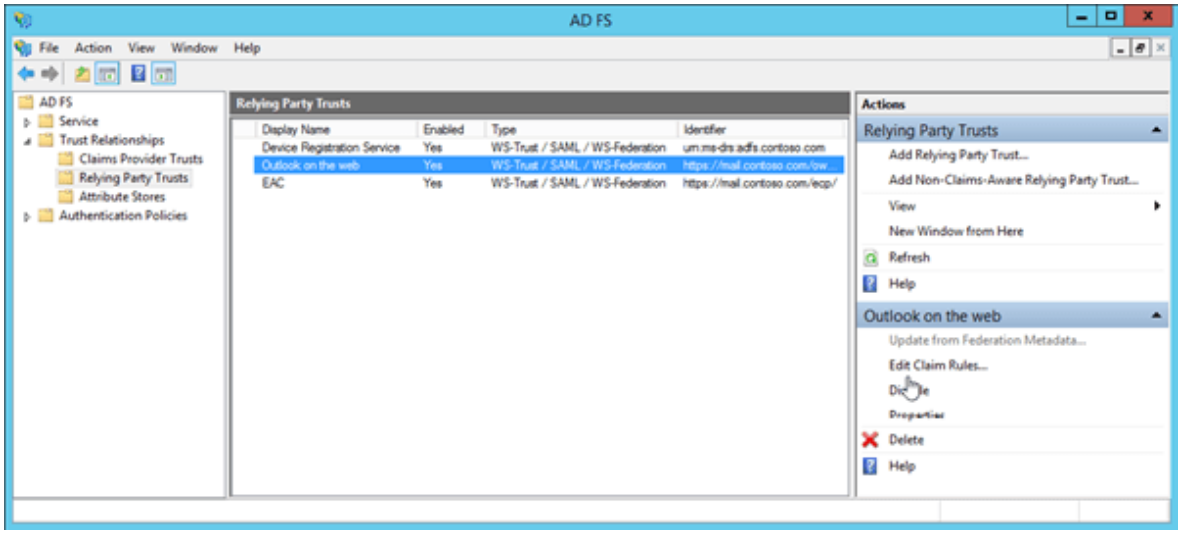
Чтобы создать правила утверждений на сервере AD FS, можно использовать консоль управления AD FS или Windows PowerShell.

Чтобы использовать консоль управления AD FS для создания правил утверждений, выполните следующие действия.

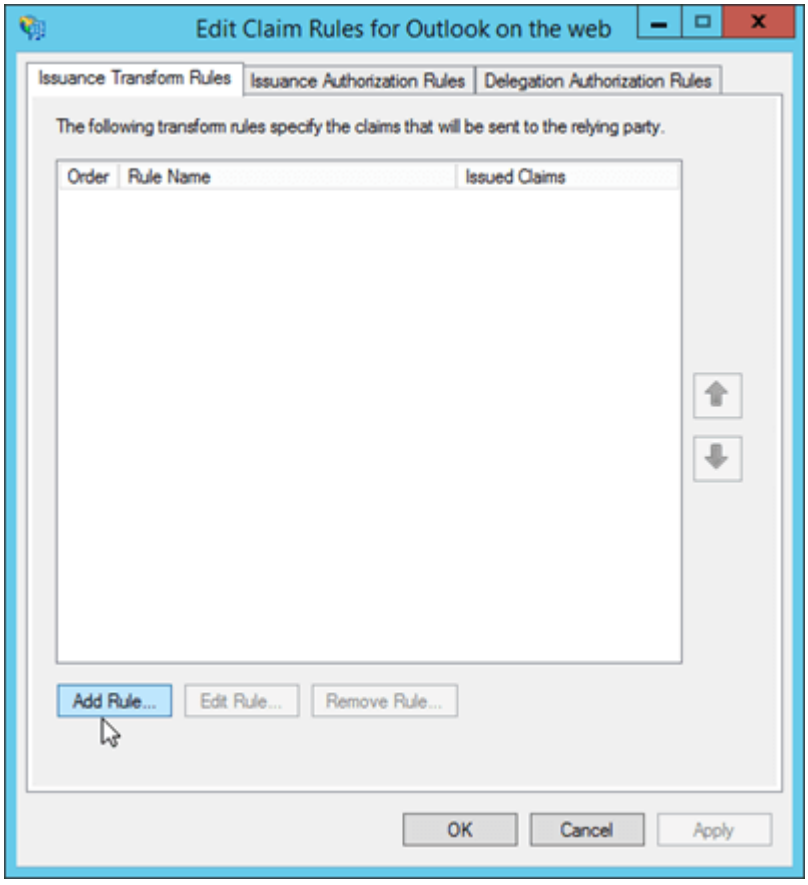
Примечание. Эти действия необходимо выполнить дважды: один раз для Outlook в Интернете и один раз для EAC. Единственным отличием является доверие проверяющей стороны, выбранное на первом шаге. Все остальные значения в процедуре идентичны.

Чтобы добавить необходимые правила утверждений:

1. В консоли управления AD FS разверните узел **Отношения доверия**, выберите **Отношения доверия с проверяющей стороной**, а затем выберите Outlook в Интернете или доверие проверяющей стороны EAC. В области **Действия** выберите **Изменить правила утверждений**.

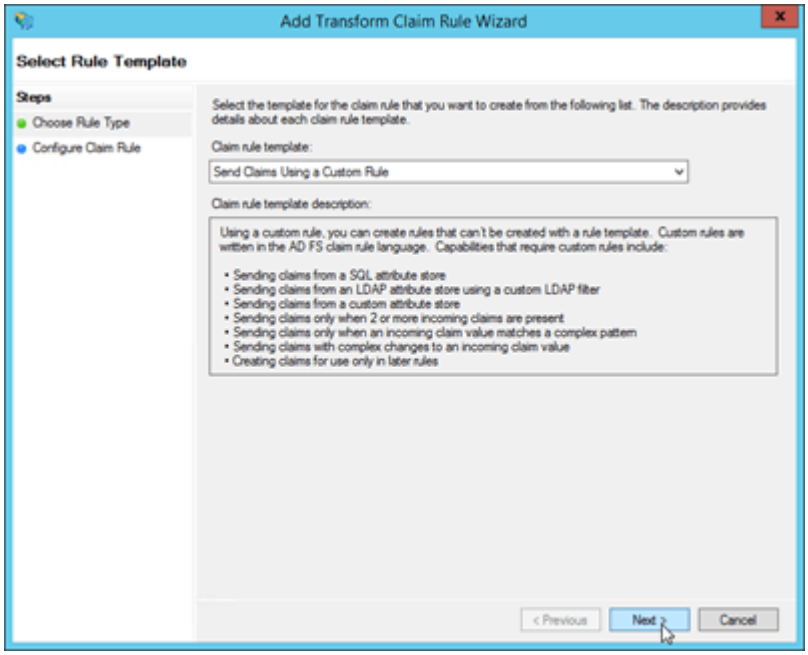


2. В открывавшемся окне **Изменение правил утверждений для <ruleName>** убедитесь, что выбрана **вкладка Правила преобразования выдачи** , а затем нажмите кнопку **Добавить правило**.



3. Откроется **мастер добавления правила утверждения преобразования** . На странице **Выбор шаблона правила** щелкните раскрывающийся список

Шаблон правила утверждения и выберите **Отправить утверждения с помощью настраиваемого правила**. По завершении нажмите кнопку **Далее**.

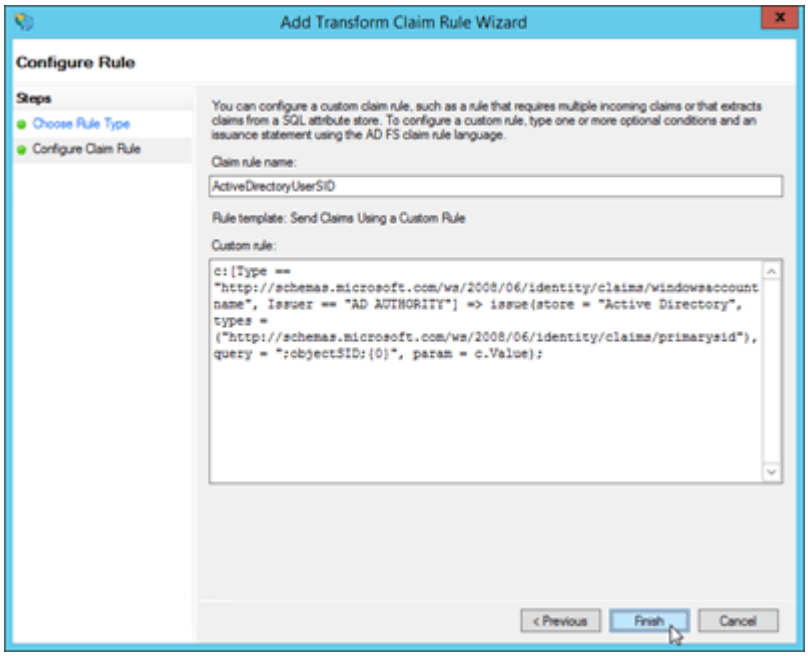


4. На странице **Настройка правила** введите следующие сведения:

   - **Имя правила утверждения**. Введите описательное имя правила утверждения. Например, ActiveDirectoryUserSID.

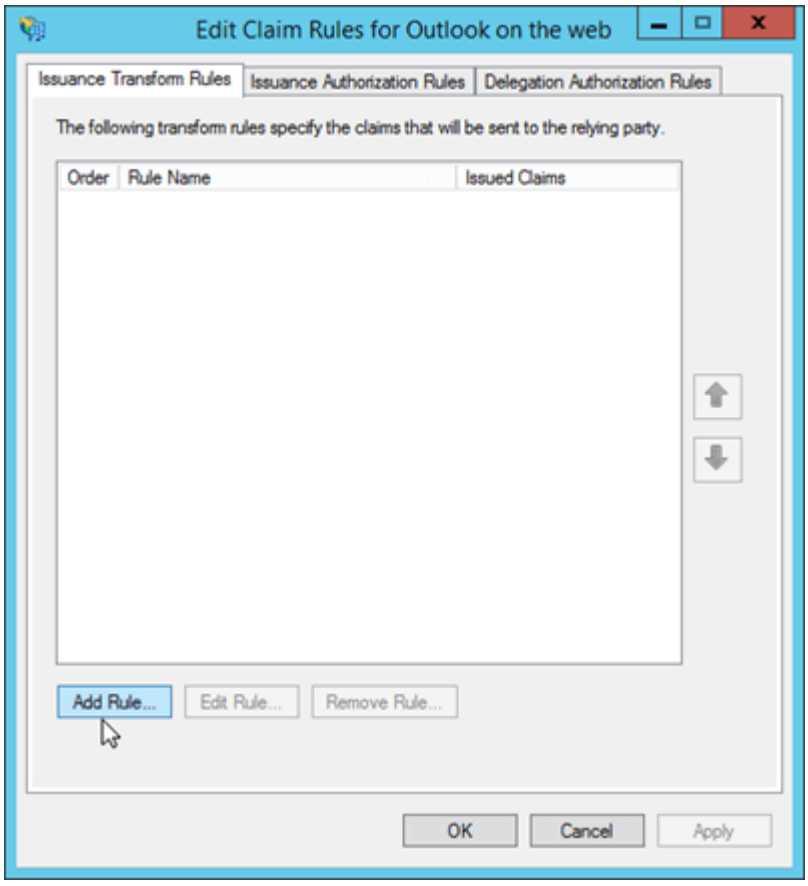
   - **Пользовательское правило**: скопируйте и вставьте следующий текст:

     ```
     c:[Type ==
     "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsac
     countname", Issuer == "AD AUTHORITY"] => issue(store = "Active
     Directory", types =
     ("http://schemas.microsoft.com/ws/2008/06/identity/claims/primarys
     id"), query = ";objectSID;{0}", param = c.Value);
     ```

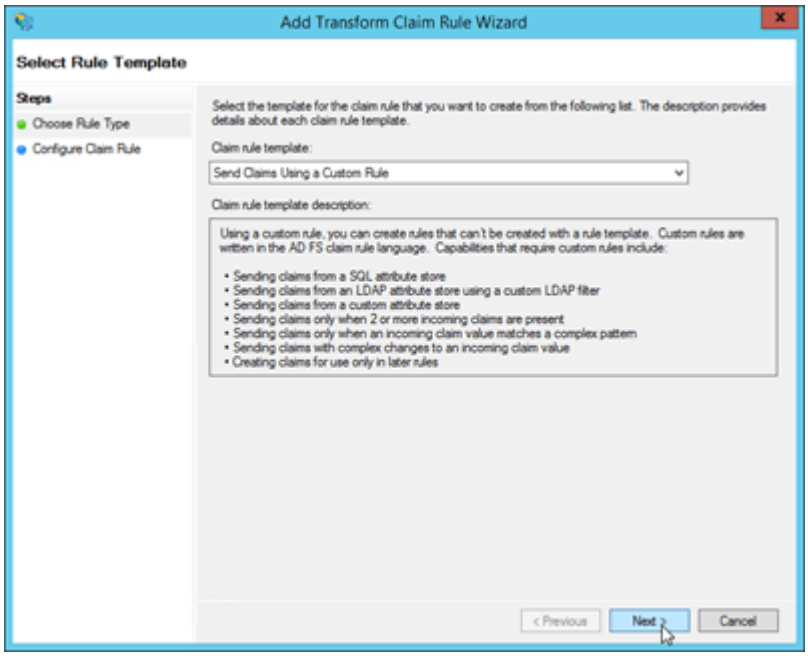


Закончив, нажмите кнопку **Готово**.

5. Вернитесь в окно **Изменение правил утверждений для <ruleName>** , убедитесь, что выбрана **вкладка Правила преобразования выдачи** , а затем нажмите кнопку **Добавить правило**.



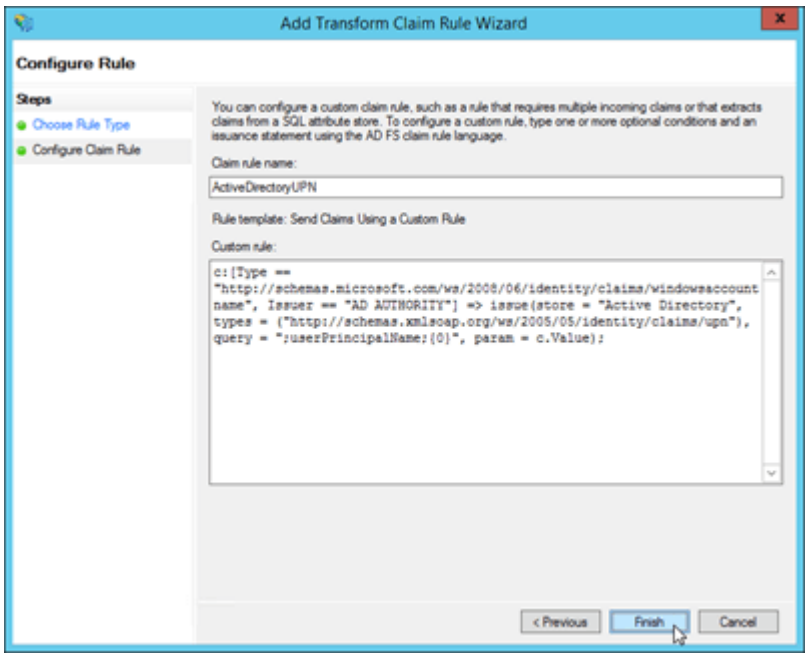
6. Откроется **мастер добавления правила утверждения преобразования** . На странице **Выбор шаблона правила** щелкните раскрывающийся список **Шаблон правила утверждения** и выберите **Отправить утверждения с помощью настраиваемого правила**. По завершении нажмите кнопку **Далее**.



7. На странице **Настройка правила** введите следующие сведения:

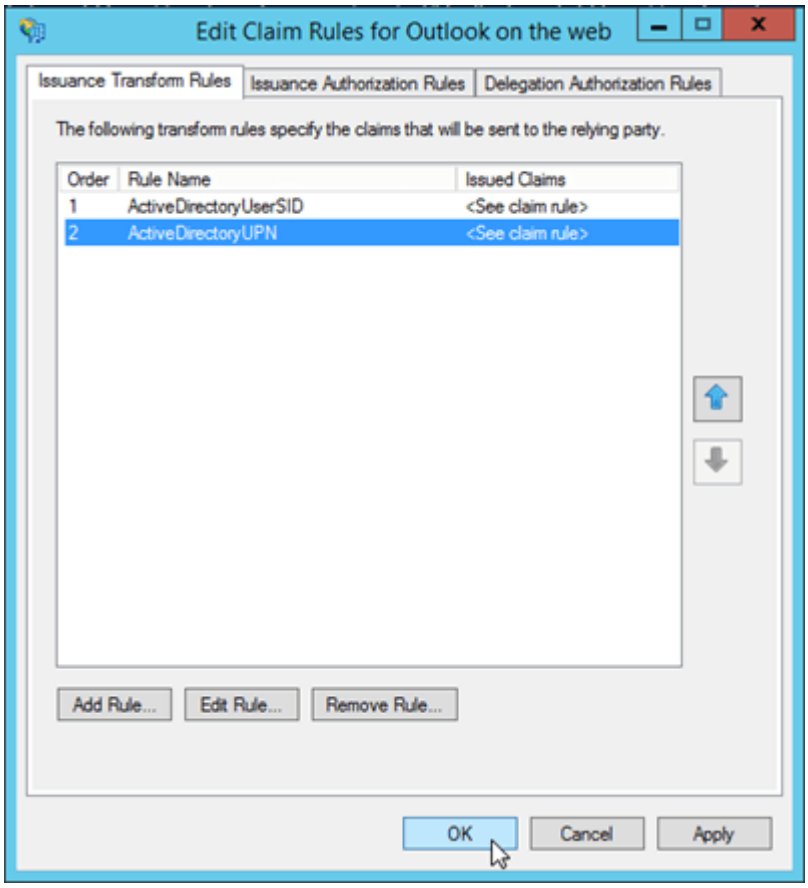
   - **Имя правила утверждения**. Введите описательное имя правила утверждения. Например, ActiveDirectoryUPN.
   - **Пользовательское правило**: скопируйте и вставьте следующий текст:

```text
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsac
countname", Issuer == "AD AUTHORITY"] => issue(store = "Active
Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"),
query = ";userPrincipalName;{0}", param = c.Value);
```



Закончив, нажмите кнопку **Готово**.

8. В окне **Изменение правил утверждений для <ruleName>** нажмите кнопку **OK**.



Чтобы использовать Windows PowerShell для создания настраиваемых правил утверждений, выполните следующие действия.

1. Откройте окно Windows PowerShell с повышенными привилегиями и выполните следующую команду:

```
PowerShell

Import-Module ADFS
```

2. Используйте следующий синтаксис.

```
PowerShell

Set-AdfsRelyingPartyTrust -TargetName <OotwRelyingPartyTrust |
EACRelyingPartyTrust> -IssuanceTransformRules '@RuleName =
"ActiveDirectoryUserSID" c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount
name", Issuer == "AD AUTHORITY"] => issue(store = "Active Directory",
types =
("http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"),
query = ";objectSID;{0}", param = c.Value); @RuleName =
```

```
"ActiveDirectoryUPN" c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount
name", Issuer == "AD AUTHORITY"] => issue(store = "Active Directory",
types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"),
query = ";userPrincipalName;{0}", param = c.Value);'
```

Чтобы создать настраиваемые правила утверждений в существующем доверии проверяющей стороны с именем Outlook в Интернете, выполните следующую команду:

PowerShell

```
Set-AdfsRelyingPartyTrust -TargetName "Outlook on the web" -
IssuanceTransformRules '@RuleName = "ActiveDirectoryUserSID" c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
, Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types =
("http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"),
query = ";objectSID;{0}", param = c.Value); @RuleName = "ActiveDirectoryUPN"
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
, Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);'
```

Чтобы создать настраиваемые правила утверждений в существующем доверии проверяющей стороны с именем EAC, выполните следующую команду:

PowerShell

```
Set-AdfsRelyingPartyTrust -TargetName EAC -IssuanceTransformRules '@RuleName
= "ActiveDirectoryUserSID" c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
, Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types =
("http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"),
query = ";objectSID;{0}", param = c.Value); @RuleName = "ActiveDirectoryUPN"
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
, Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);'
```

Шаг 5. Развертывание и настройка сервера веб-Application Proxy Windows Server 2012 R2 (необязательно)

Действия, описанные в этом разделе, необходимы только в том случае, если вы хотите опубликовать Outlook в Интернете и EAC с помощью веб-Application Proxy, а веб-Application Proxy выполнить проверку подлинности AD FS. Помните:

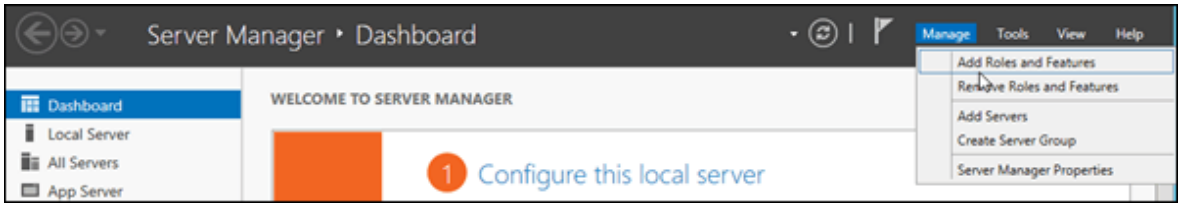
- Вы не можете использовать автономный доступ в Outlook в Интернете, если используете проверку подлинности AD FS через веб-Application Proxy.
- Невозможно установить веб-Application Proxy на том же сервере, где установлена служба AD FS.

Если вы не собираетесь использовать веб-Application Proxy, перейдите к шагу 6.

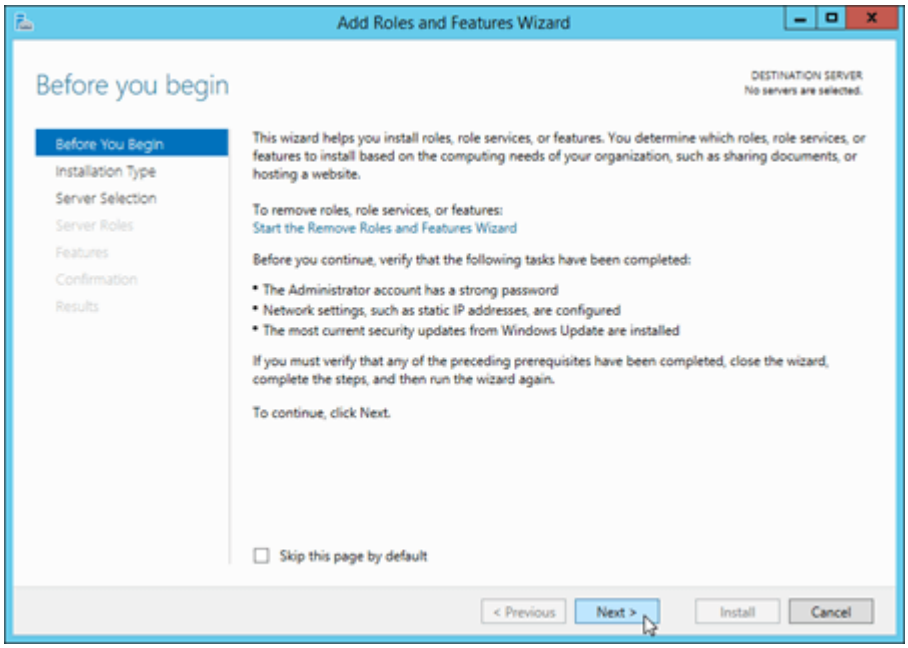
Шаг 5a. Установка веб-Application Proxy

Чтобы использовать диспетчер сервера для установки веб-Application Proxy, выполните следующие действия.

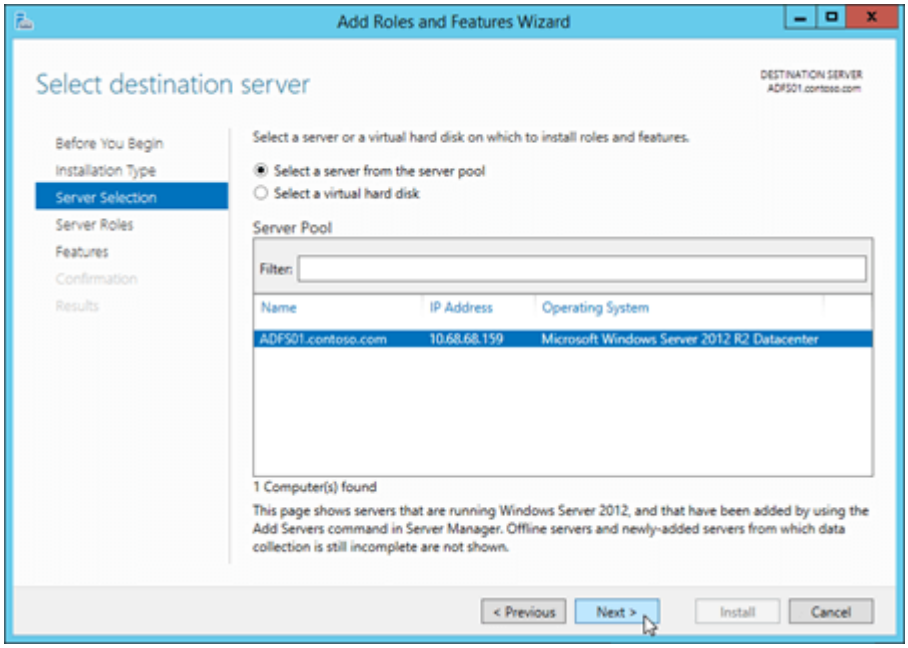
1. На целевом сервере откройте **диспетчер сервера**, щелкните **Управление**, а затем выберите **Добавить роли и компоненты**.



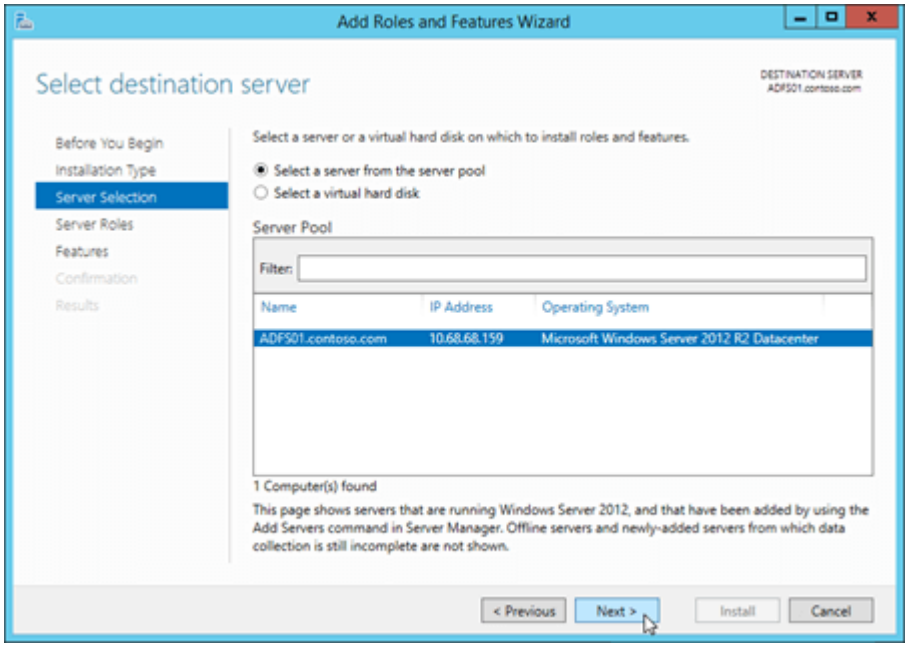
2. Откроется **мастер добавления ролей и компонентов** . Вы будете начинать с страницы **Перед началом работы** , если вы не выбрали **пропустить эту страницу по умолчанию**. Нажмите кнопку **Далее**.



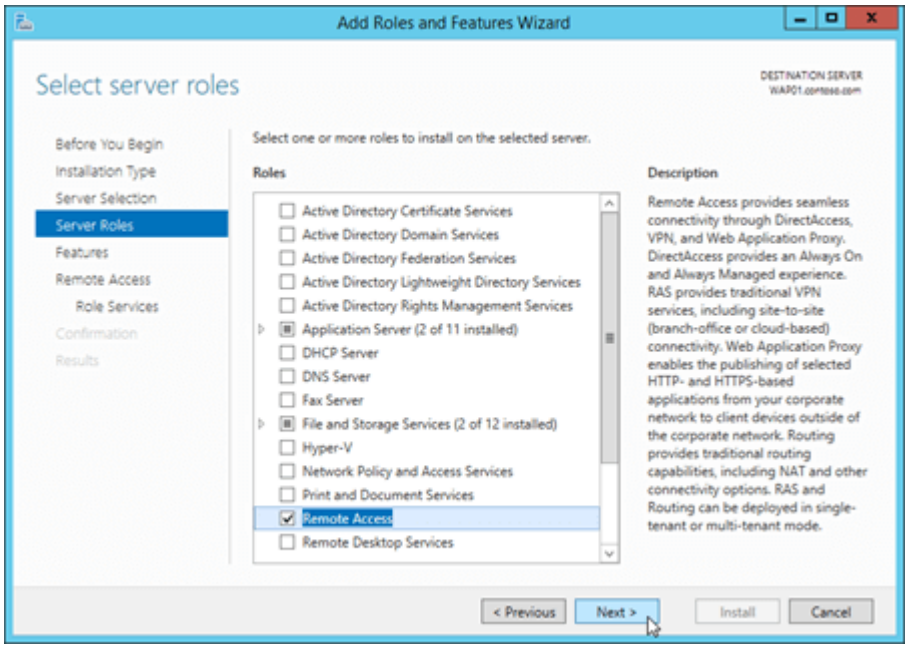
3. На странице **Выбор типа установки** убедитесь, что выбран параметр **Установка на основе ролей или компонентов** , а затем нажмите кнопку **Далее**.



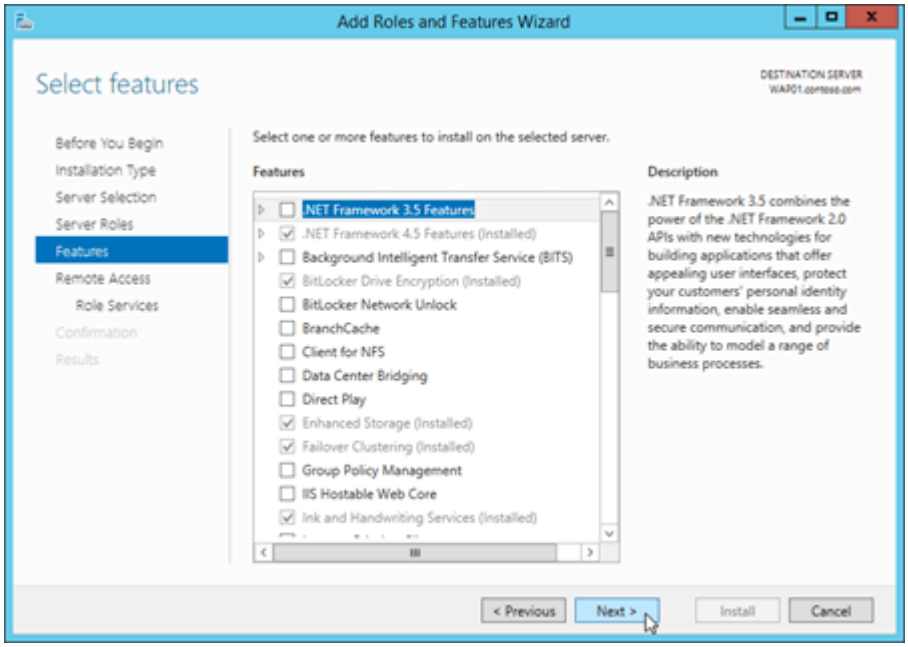
4. На странице **Выбор целевого сервера** проверьте выбор сервера и нажмите кнопку **Далее**.



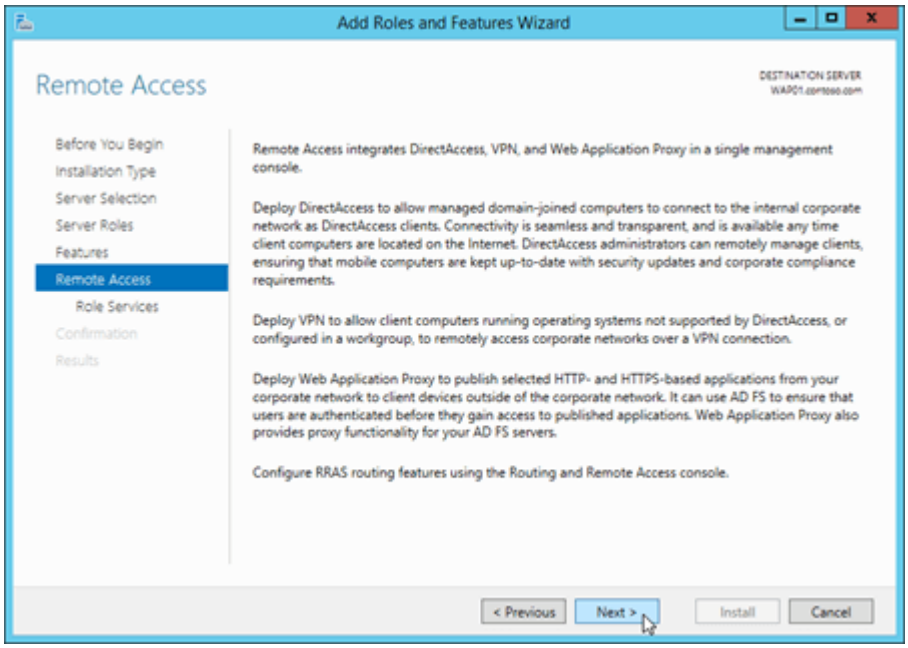
5. На странице **Выбор ролей сервера** выберите **Удаленный доступ** в списке ролей и нажмите кнопку **Далее**.



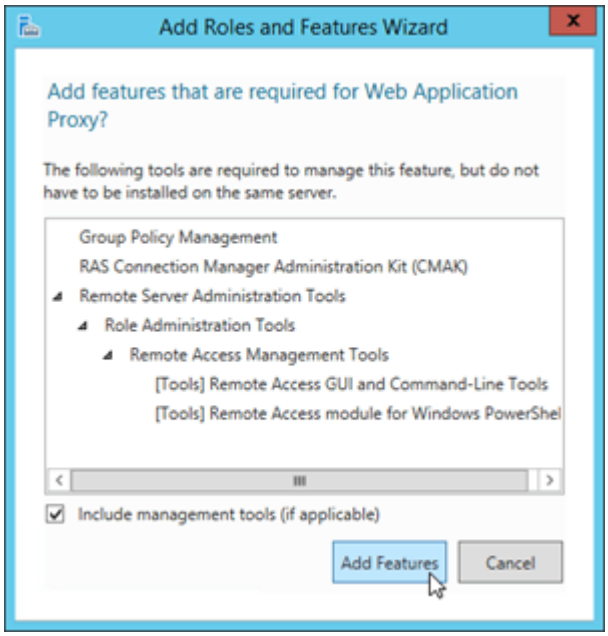
6. На странице **Компоненты** нажмите кнопку **Далее** (примите выбранные по умолчанию функции).

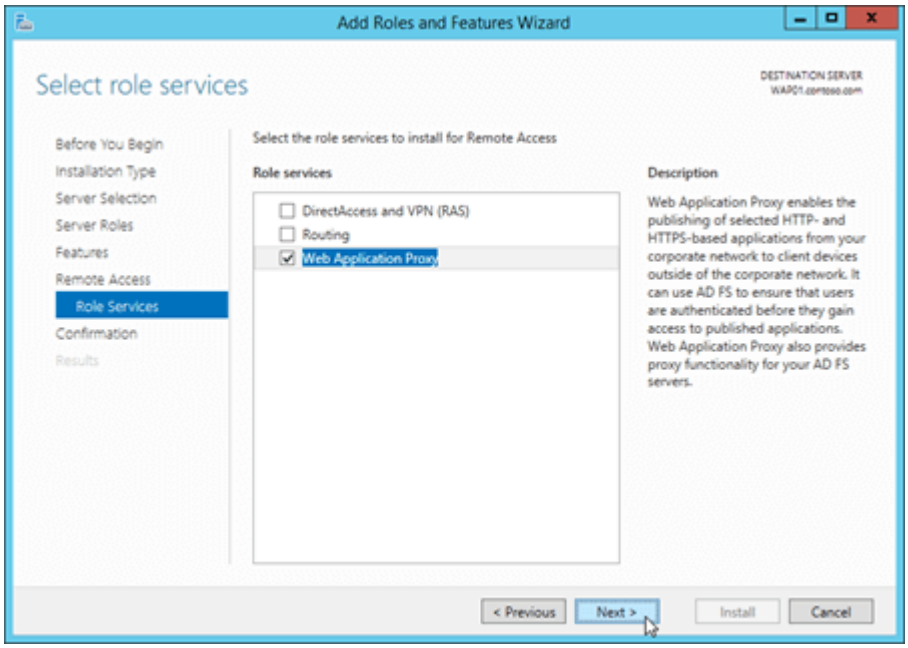


7. На странице **Удаленный доступ** прочтите сведения, а затем нажмите кнопку **Далее**.

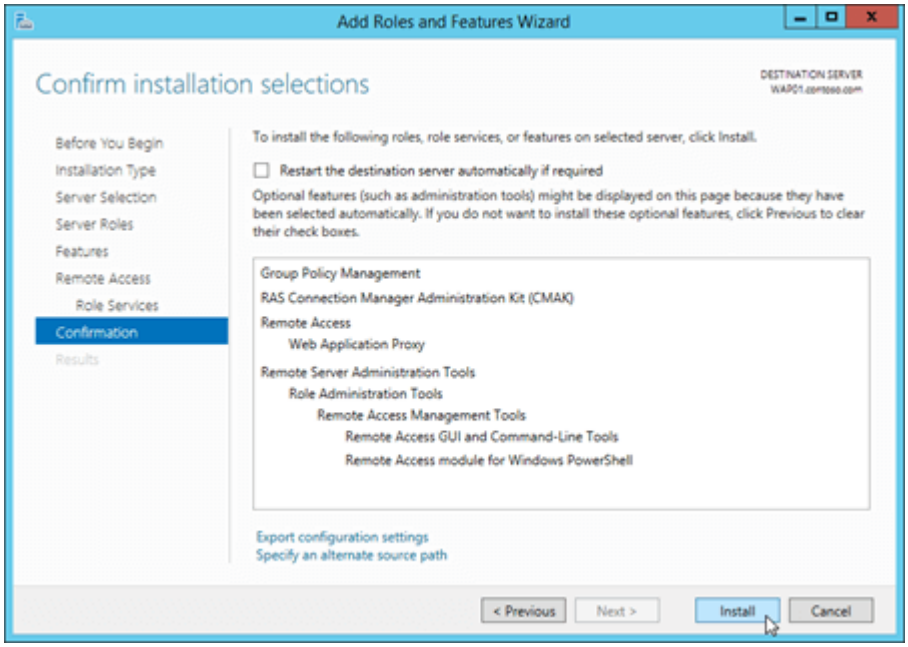


8. На странице **Выбор служб ролей** выберите **Веб-Application Proxy**. В открывшемся диалоговом окне Добавление компонентов щелкните **Добавить компоненты** , чтобы принять значения по умолчанию и закрыть диалоговое окно. На странице **Выбор служб ролей** нажмите кнопку **Далее**.

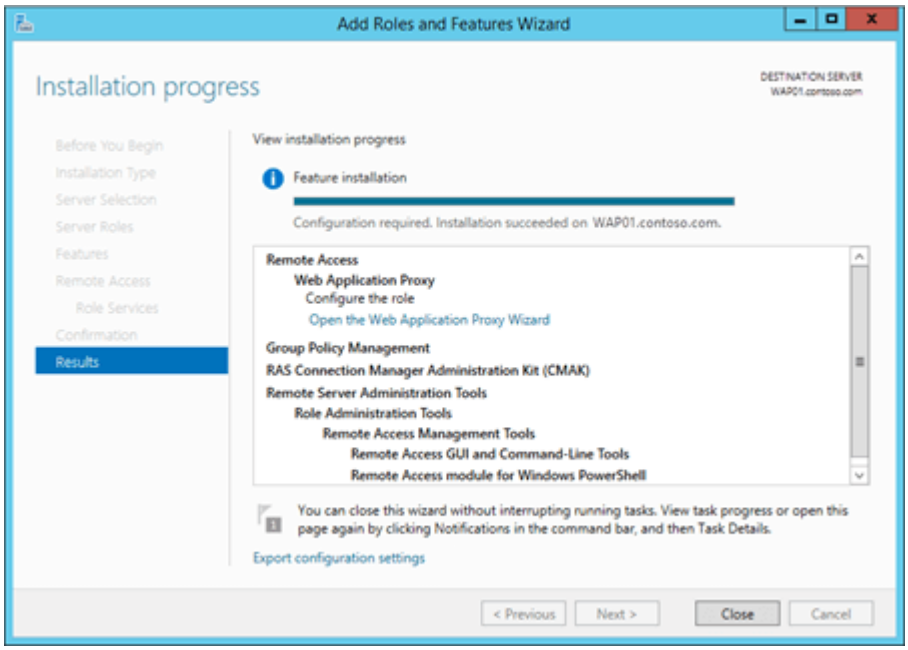




9. На странице **Подтверждение выбранных вариантов установки** нажмите кнопку **Установить**.



10. На странице **Ход установки** просмотрите индикатор выполнения, чтобы убедиться, что установка прошла успешно. По завершении установки оставьте мастер открытым, чтобы на следующем шаге (5b) нажать кнопку **Открыть мастер веб-Application Proxy**.



Чтобы использовать Windows PowerShell для установки веб-Application Proxy, выполните следующую команду:

```PowerShell
Install-WindowsFeature Web-Application-Proxy -IncludeManagementTools
```

Шаг 5b. Настройка сервера веб-Application Proxy

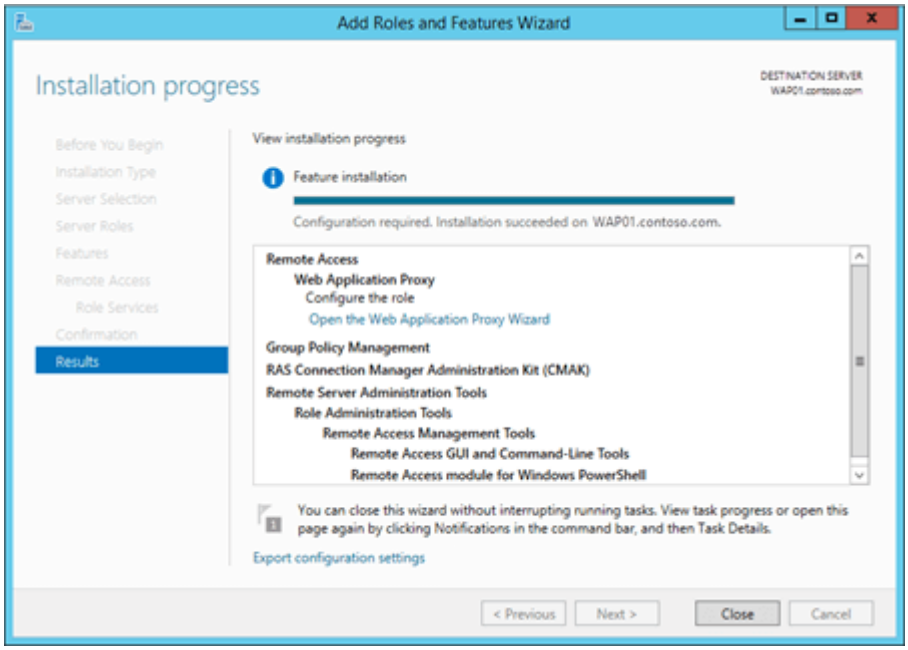
После развертывания сервера веб-Application Proxy необходимо настроить следующие параметры веб-Application Proxy:

- **Имя службы федерации**: например, `adfs.contoso.com`.
- **Учетные данные доверия службы федерации**. Имя пользователя и пароль учетной записи локального администратора на сервере AD FS.
- **Сертификат прокси-сервера AD FS**: сертификат, установленный на сервере веб-Application Proxy, который определяет сервер для клиентов в качестве прокси-сервера для службы федерации и, следовательно, содержит имя службы федерации (например, `adfs.contoso.com`). Кроме того, имя службы федерации должно быть доступно для веб-сервера Application Proxy (разрешается в DNS).

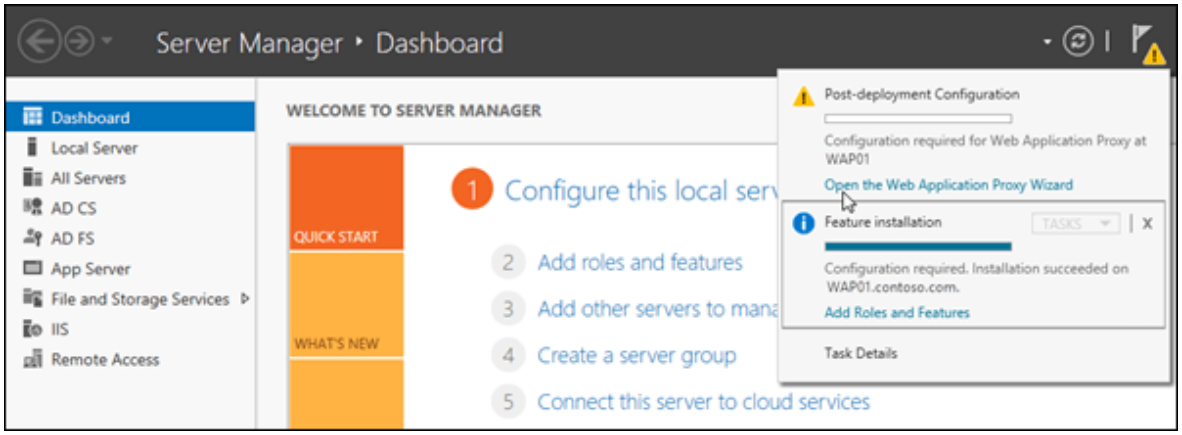
Для настройки сервера веб-Application Proxy можно использовать диспетчер сервера или Windows PowerShell.

Чтобы использовать диспетчер сервера для настройки веб-Application Proxy, выполните следующие действия.

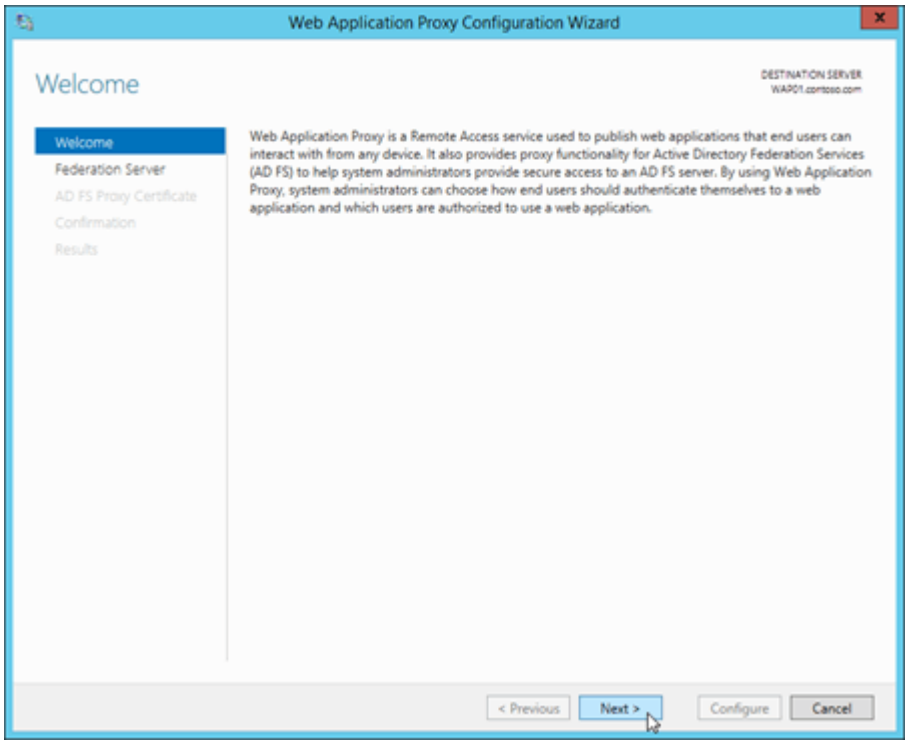
1. Если вы оставили **мастер добавления ролей и компонентов** открытым на веб-сервере Application Proxy на предыдущем шаге, можно щелкнуть ссылку **Открыть мастер веб-Application Proxy** на странице **Ход установки**.



Если вы закрыли **мастер добавления ролей и компонентов** или использовали Windows PowerShell для установки веб-Application Proxy, вы можете перейти к тому же месту, щелкнув **Уведомления**, а затем **щелкнув Открыть мастер веб-Application Proxy** в **предупреждении Конфигурация после развертывания**.



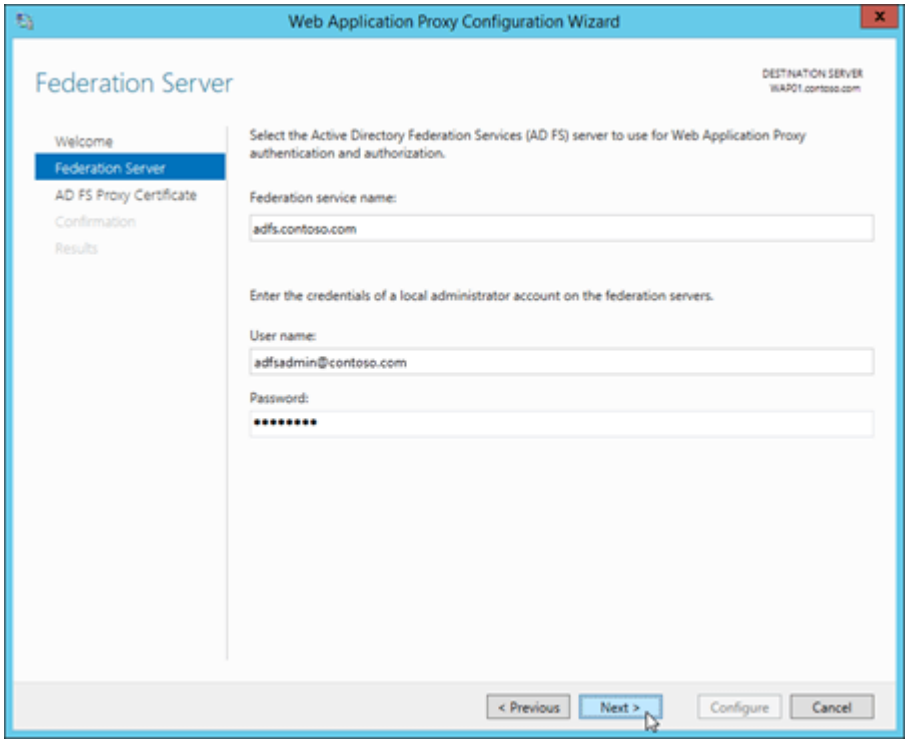
2. Откроется **мастер настройки веб-Application Proxy**. На странице **приветствия** нажмите кнопку **Далее**.



3. На странице **Сервер федерации** введите следующие сведения:

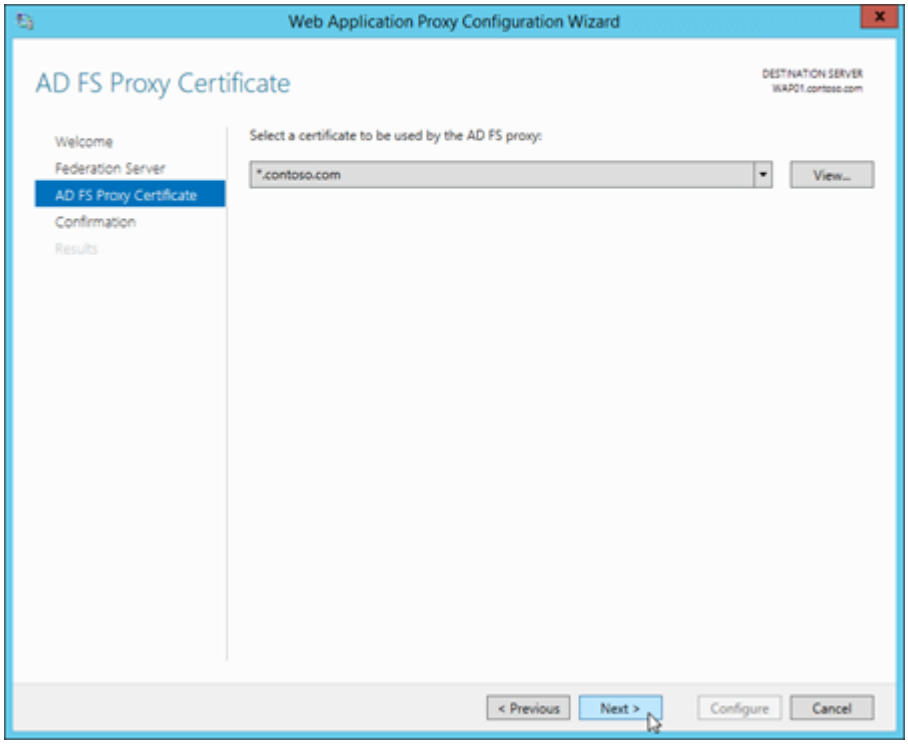
   - **Имя службы федерации**: например, `adfs.contoso.com`.
   - **Имя пользователя** и **пароль**. Введите учетные данные учетной записи локального администратора на сервере AD FS.

   По завершении нажмите кнопку **Далее**.

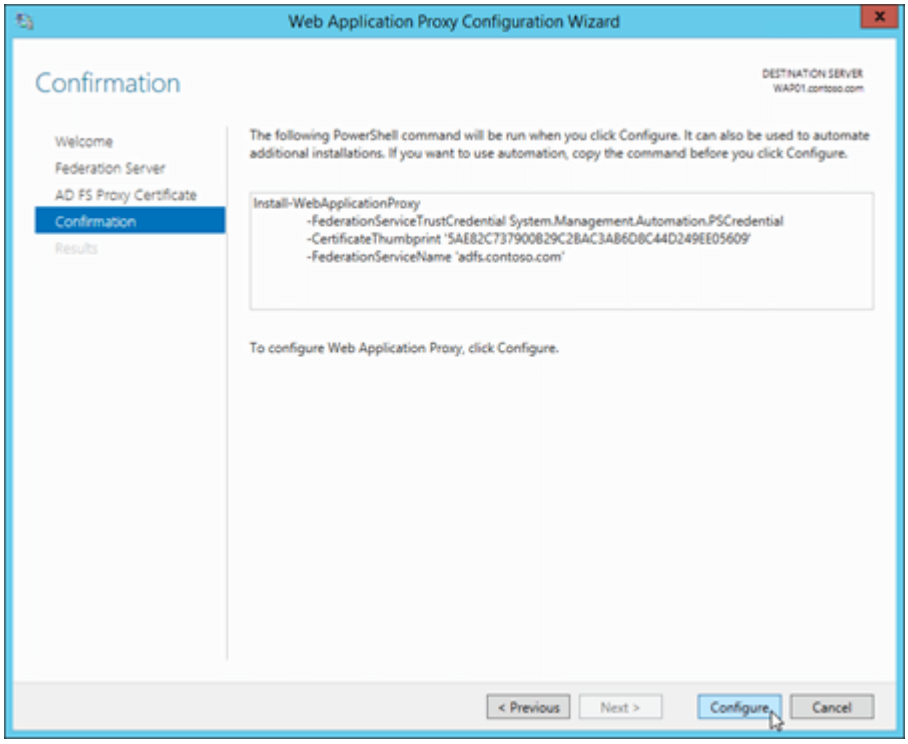


4. На странице **Сертификат прокси-сервера AD FS** выберите установленный сертификат, содержащий имя службы федерации (например `adfs.contoso.com`,

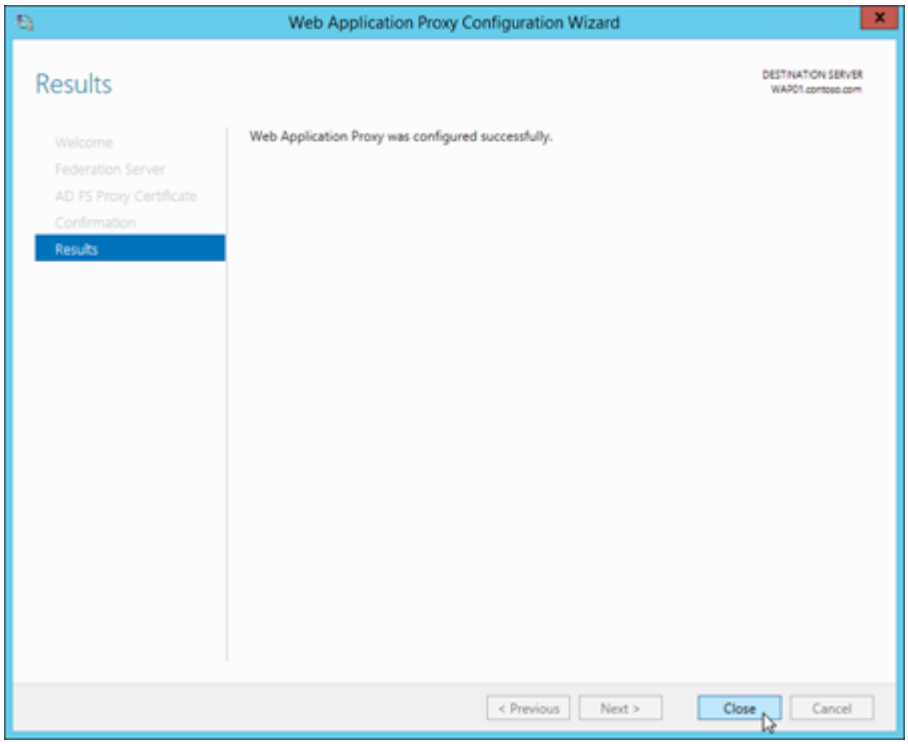
). Вы можете выбрать сертификат в раскрывающемся списке, а затем нажать кнопку **Просмотреть**>**сведения** , чтобы просмотреть дополнительные сведения о сертификате. По завершении нажмите кнопку **Далее**.



5. На странице **Подтверждение** просмотрите параметры. Команду Windows PowerShell можно скопировать, чтобы автоматизировать дополнительные установки (в частности, значение отпечатка сертификата). По завершении нажмите кнопку **Настроить**.



6. На странице **Результаты** убедитесь, что конфигурация прошла успешно, и нажмите кнопку **Закрыть**.



Чтобы использовать Windows PowerShell для настройки веб-Application Proxy, выполните следующие действия.

1. Выполните следующую команду на сервере веб-Application Proxy, чтобы найти значение отпечатка установленного сертификата, содержащего `adfs.contoso.com`:

   PowerShell

   ```
   Set-Location Cert:\LocalMachine\My; Get-ChildItem | Format-List
   FriendlyName,Subject,Thumbprint
   ```

2. Выполните следующую команду и введите имя пользователя и пароль учетной записи локального администратора на сервере AD FS.

   PowerShell

   ```
   $ADFSServerCred = Get-Credential
   ```

3. Используйте следующий синтаксис.

   PowerShell

   ```
   Install-WebApplicationProxy -FederationServiceName
   <FederationServiceName> -FederationServiceTrustCredential
   $ADFSServerCred -CertificateThumprint <ADFSCertThumbprint>
   ```

В этом примере настраивается сервер веб-Application Proxy со следующими параметрами:

- **Имя службы федерации**: `adfs.contoso.com`
- **Отпечаток SSL-сертификата AD FS**: `*.contoso.com` сертификат, имеющий значение `5AE82C737900B29C2BAC3AB6D8C44D249EE05609` отпечатка .

PowerShell

```
Install-WebApplicationProxy -FederationServiceName adfs.contoso.com -
FederationServiceTrustCredential $ADFSServerCred -CertificateThumprint
5AE82C737900B29C2BAC3AB6D8C44D249EE05609
```

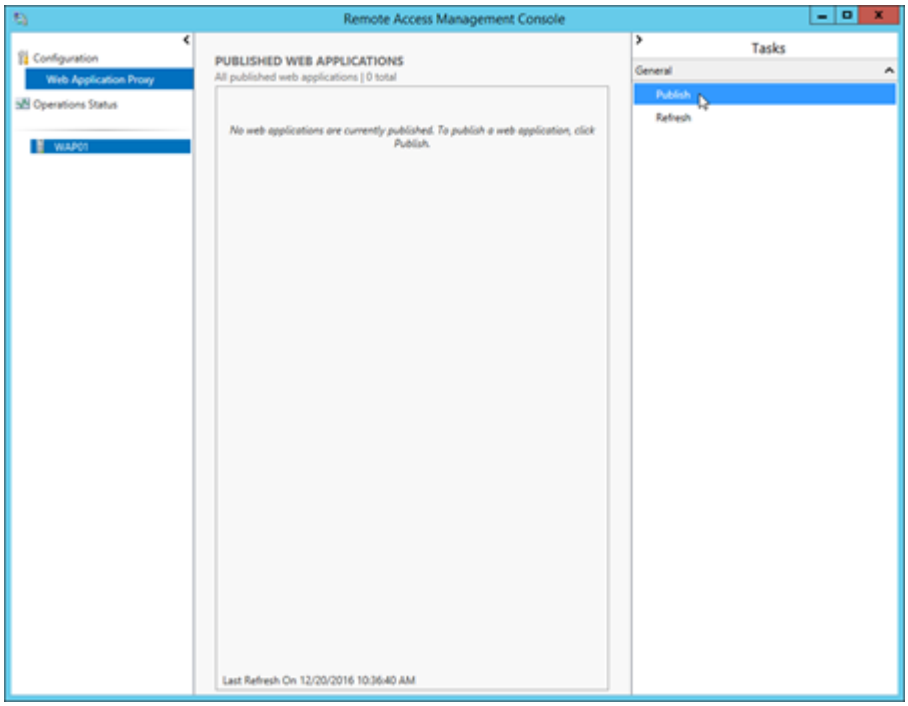
Шаг 5c. Публикация утверждений доверия с проверяющей стороной для Outlook в Интернете и EAC в веб-Application Proxy

Чтобы опубликовать отношения доверия с проверяющей стороной в веб-Application Proxy, можно использовать консоль управления удаленным доступом или Windows PowerShell.

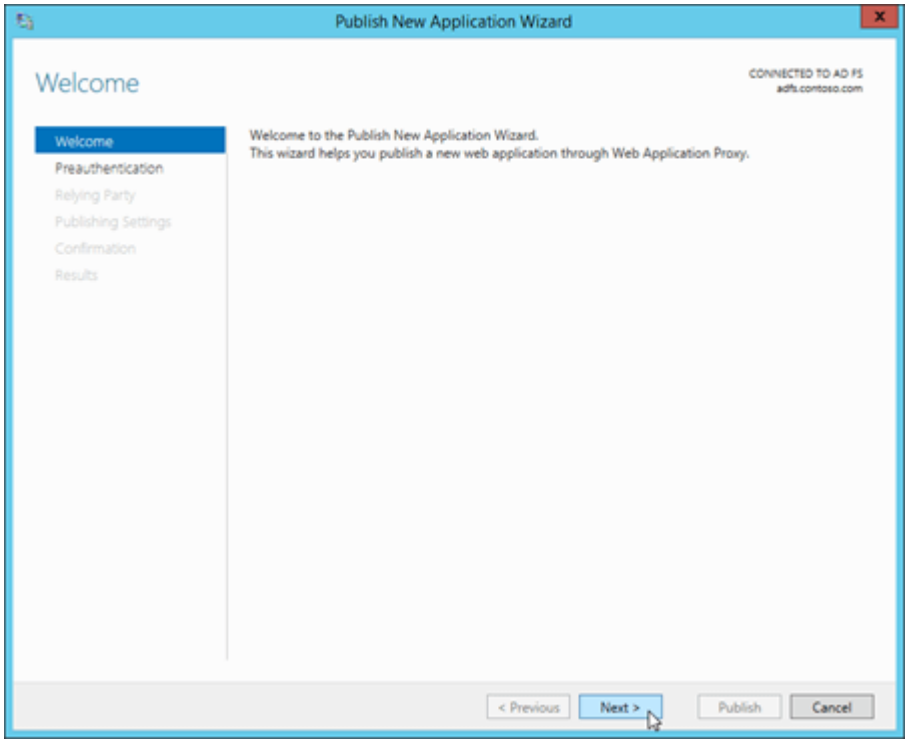
Чтобы использовать консоль управления удаленным доступом, выполните следующие действия.

Примечание. Эти действия необходимо выполнить дважды: один раз для Outlook в Интернете и один раз для EAC. Необходимые параметры описаны в процедуре.

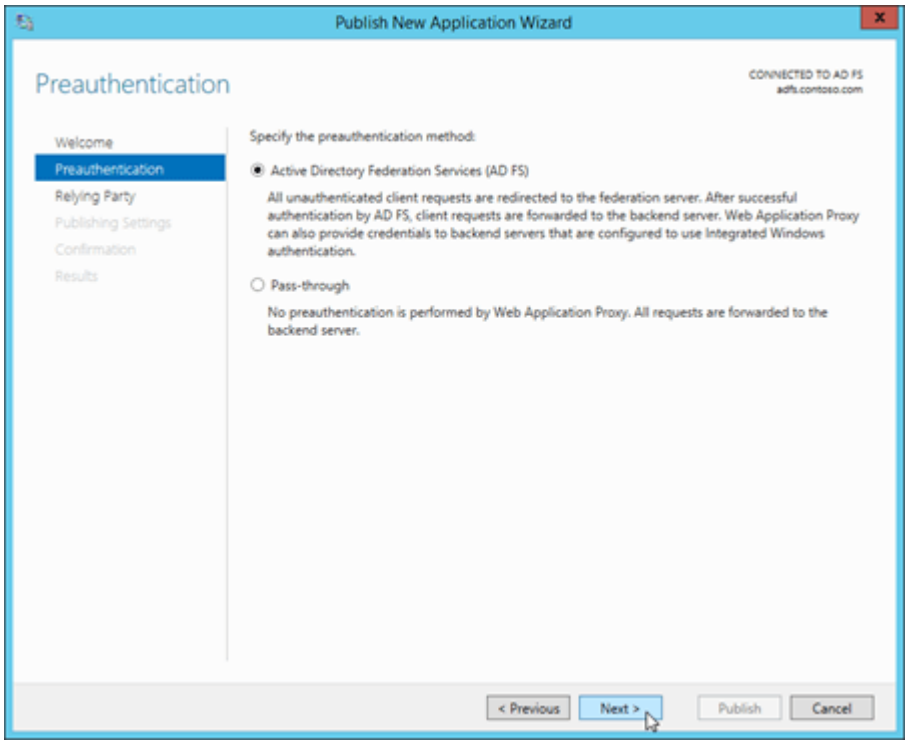
1. Откройте консоль управления удаленным доступом на сервере веб-Application Proxy: в диспетчер сервера щелкните **Инструменты**>**удаленного управления доступом**.
2. В консоли управления удаленным доступом в разделе **Конфигурация** щелкните **Веб-Application Proxy**, а затем в области **Задачи** щелкните **Опубликовать**.



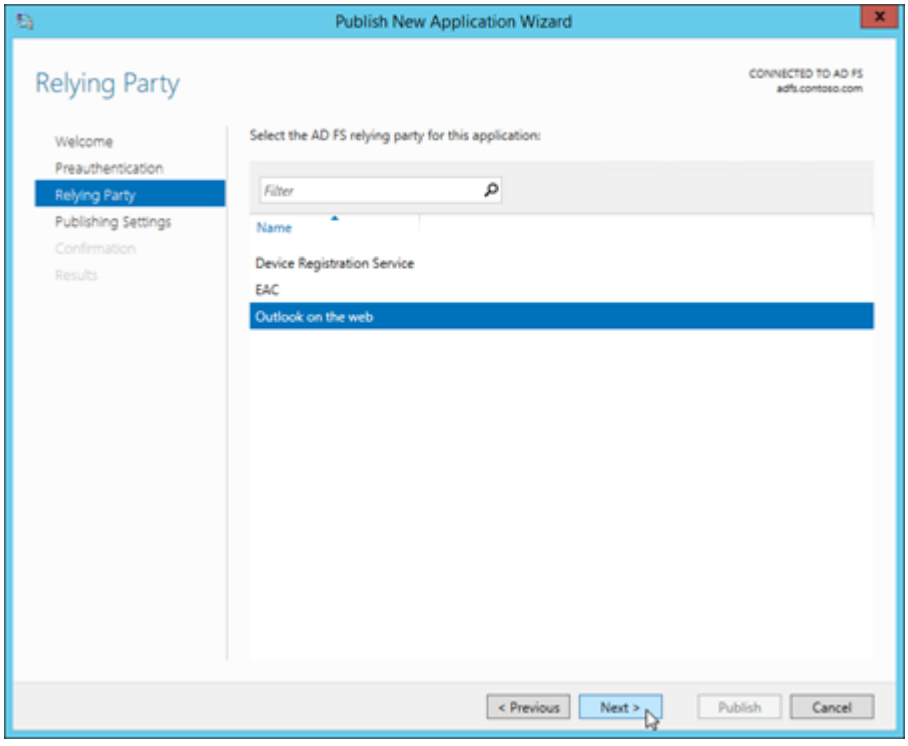
3. Откроется **мастер публикации нового приложения** . На странице **приветствия** нажмите кнопку **Далее**.



4. На странице **Предварительная проверка подлинности** убедитесь, **что выбрано службы федерации Active Directory (AD FS) (AD FS),** а затем нажмите кнопку **Далее**.



5. На странице **Проверяющая сторона выберите проверяющую** сторону, созданную на сервере AD FS в разделе Шаг 4. Создание правил доверия проверяющей стороны и настраиваемых правил утверждений в AD FS для Outlook в Интернете и EAC:

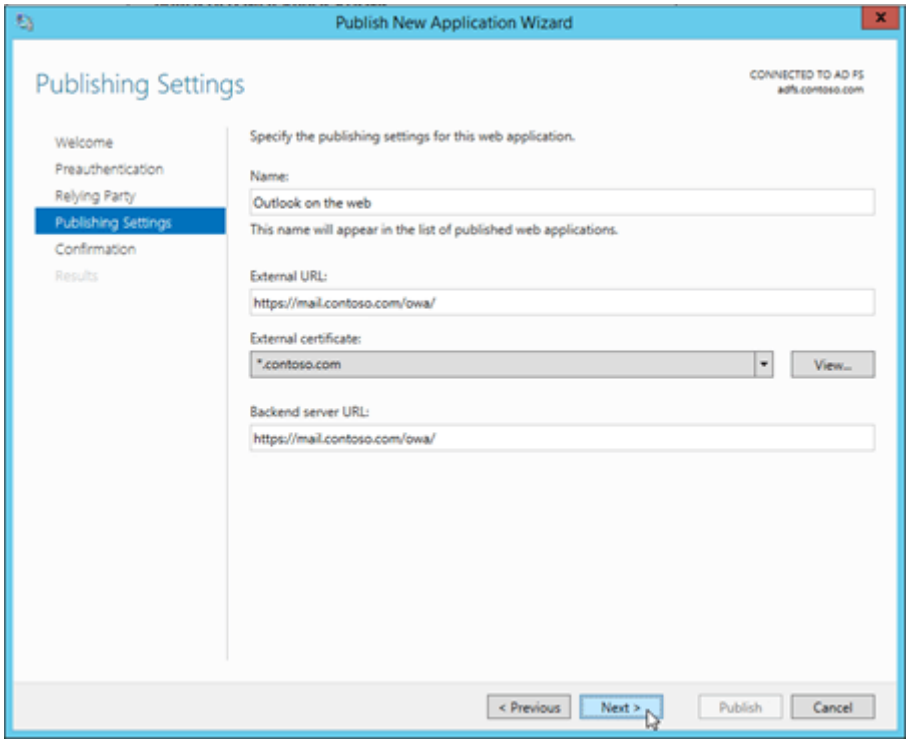


- **Для Outlook в Интернете** выберите Outlook в Интернете.
- **Для EAC**: выберите EAC.

По завершении нажмите кнопку **Далее**.

6. На странице **Параметры публикации** введите следующие сведения:

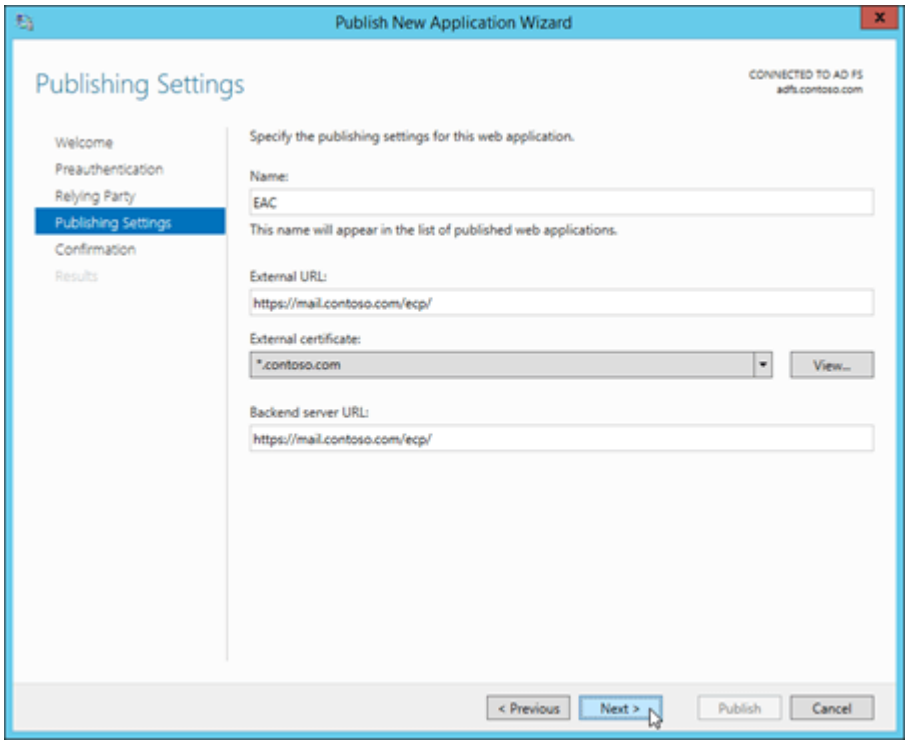
- **Для Outlook в Интернете**
  - **Имя**: например, `Outlook on the web`. Это имя отображается только в консоли управления удаленным доступом.
  - **Внешний URL-адрес**: например, `https://mail.contoso.com/owa/`.
  - **Внешний сертификат**. Выберите установленный сертификат, содержащий имя узла внешнего URL-адреса для Outlook в Интернете (например, `mail.contoso.com`). Вы можете выбрать сертификат в раскрывающемся списке, а затем нажать кнопку **Просмотреть**>**сведения** , чтобы просмотреть дополнительные сведения о сертификате.
  - **URL-адрес внутреннего сервера**. Это значение автоматически заполняется **внешним URL-адресом**. Изменить его нужно только в том случае, если URL-адрес внутреннего сервера отличается от внешнего URL-адреса. Например, `https://server01.contoso.com/owa/`. Обратите внимание, что пути во внешнем URL-адресе и URL-адресе внутреннего сервера должны соответствовать (`/owa/`), но значения имени узла могут отличаться (например, `mail.contoso.com` и `server01.contoso.com`).



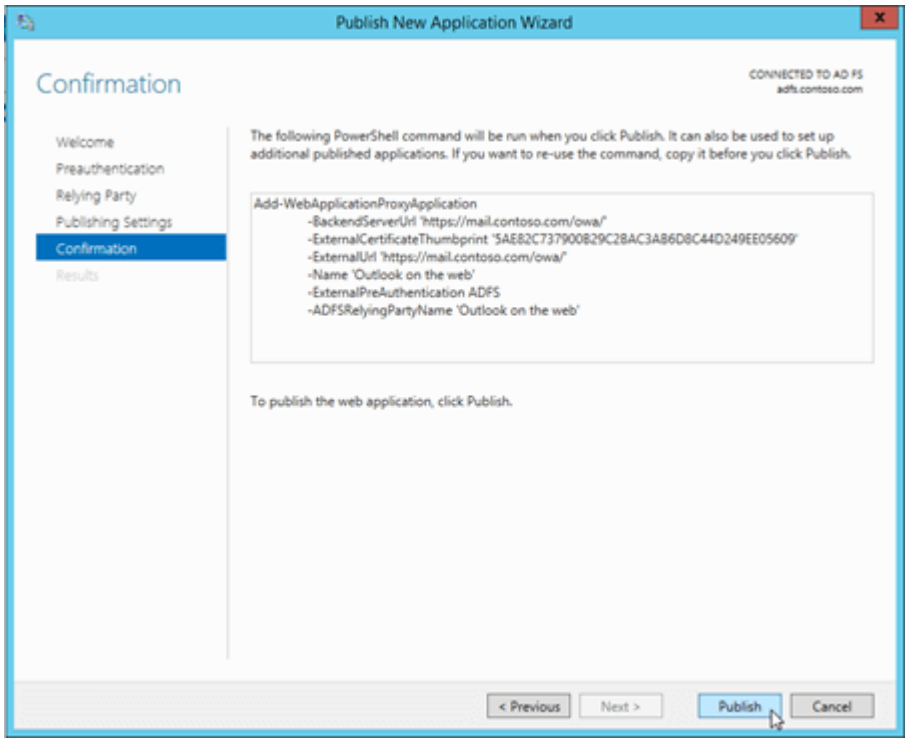
- **Для EAC**
  - **Имя**: например, `EAC`. Это имя отображается только в консоли управления удаленным доступом.

- **Внешний URL-адрес**: внешний URL-адрес центра администрирования EAC. Например, https://mail.contoso.com/ecp/ .
- **Внешний сертификат**. Выберите установленный сертификат, содержащий имя узла внешнего URL-адреса центра администрирования (например, `mail.contoso.com`). Сертификат, скорее всего, является подстановочным сертификатом или сертификатом SAN. Вы можете выбрать сертификат в раскрывающемся списке, а затем нажать кнопку **Просмотреть**>**сведения** , чтобы просмотреть дополнительные сведения о сертификате.
- **URL-адрес внутреннего сервера**. Это значение автоматически заполняется **внешним URL-адресом**. Изменить его нужно только в том случае, если URL-адрес внутреннего сервера отличается от внешнего URL-адреса. Например, `https://server01.contoso.com/ecp/`. Обратите внимание, что пути во внешнем URL-адресе и URL-адресе внутреннего сервера должны соответствовать (`/ecp/`), но значения имени узла могут отличаться (например, `mail.contoso.com` и `server01.contoso.com`).

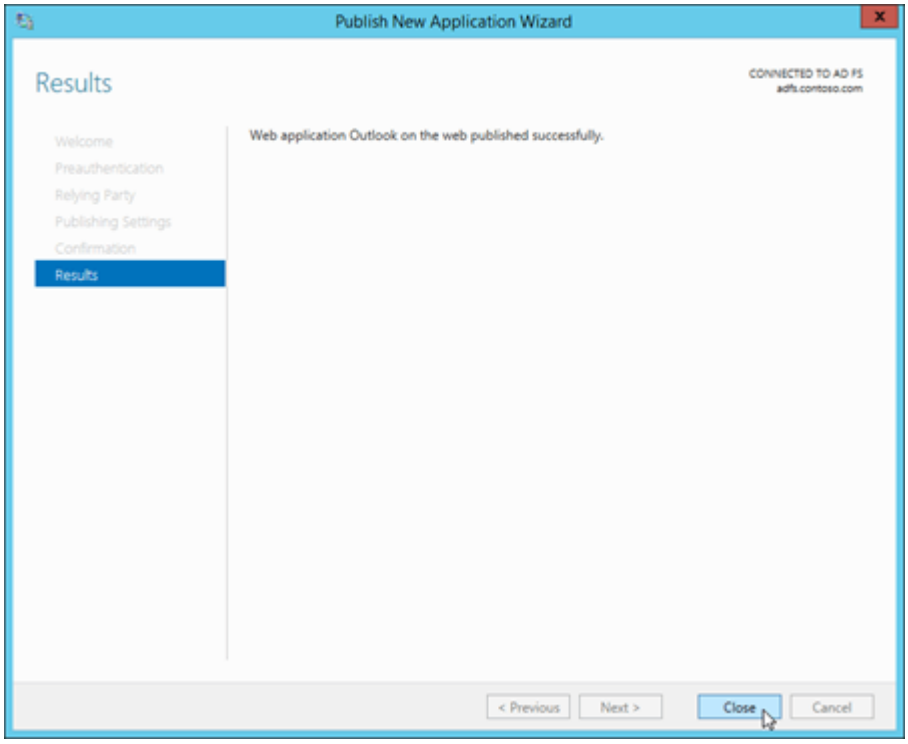
По завершении нажмите кнопку **Далее**.



7. На странице **Подтверждение** просмотрите параметры. Команду Windows PowerShell можно скопировать, чтобы автоматизировать дополнительные установки (в частности, значение отпечатка сертификата). По завершении нажмите кнопку **Опубликовать**.



8. На странице **Результаты** убедитесь, что приложение успешно опубликовано, и нажмите кнопку **Закрыть**.



Чтобы использовать Windows PowerShell для публикации отношений доверия с проверяющей стороной, выполните следующие действия.

1. Выполните следующую команду на сервере веб-Application Proxy, чтобы найти отпечаток установленного сертификата, содержащего имя узла Outlook в Интернете и URL-адреса EAC (например, `mail.contoso.com`):

```
PowerShell
```

```
Set-Location Cert:\LocalMachine\My; Get-ChildItem | Format-List
FriendlyName,Subject,Thumbprint
```

2. Используйте следующий синтаксис.

PowerShell

```
Add-WebApplicationProxyApplication -ExternalPreAuthentication ADFS -
ADFSRelyingPartyName <OotwRelyingParty | EACRelyingParty> -Name "
<Outlook on the web  | EAC>" -ExternalUrl <OotwURL | EACURL> -
ExternalCertificateThumbprint <Thumbprint> -BackendServerUrl <OotwURL |
EACURL>
```

В этом примере Outlook в Интернете публикуется в веб-Application Proxy со следующими параметрами:

- **Проверяющая сторона AD FS**: Outlook в Интернете
- **Имя**: Outlook в Интернете
- **Внешний URL-адрес**: https://mail.contoso.com/owa/
- **Отпечаток внешнего сертификата**: `*.contoso.com` сертификат, имеющий значение `5AE82C737900B29C2BAC3AB6D8C44D249EE05609`отпечатка .
- **URL-адрес внутреннего сервера**: https://mail.contoso.com/owa/

PowerShell

```
Add-WebApplicationProxyApplication -ExternalPreAuthentication ADFS -
ADFSRelyingPartyName "Outlook on the web" -Name "Outlook on the web" -
ExternalUrl https://mail.contoso.com/owa/ -
ExternalCertificateThumbprint 5AE82C737900B29C2BAC3AB6D8C44D249EE056093
-BackendServerUrl https://mail.contoso.com/owa/
```

В этом примере EAC публикуется в веб-Application Proxy со следующими параметрами:

- **Имя**: EAC
- **Внешний URL-адрес**: https://external.contoso.com/ecp/
- **Отпечаток внешнего сертификата**: `*.contoso.com` сертификат, имеющий значение `5AE82C737900B29C2BAC3AB6D8C44D249EE05609`отпечатка .
- **URL-адрес внутреннего сервера**: https://mail.contoso.com/ecp/

PowerShell

```
Add-WebApplicationProxyApplication -ExternalPreAuthentication ADFS -
ADFSRelyingPartyName EAC -Name EAC -ExternalUrl
https://external.contoso.com/ecp/ -ExternalCertificateThumbprint
```

```
5AE82C737900B29C2BAC3AB6D8C44D249EE05609 -BackendServerUrl
https://mail.contoso.com/ecp/
```

Примечание. Все конечные точки AD FS, которые нужно опубликовать через веб-Application Proxy, должны быть включены прокси-серверы. Это можно сделать в консоли управления AD FS на**конечных точкахслужбы**> (убедитесь, что для указанной конечной точки **включено прокси-сервер имеет** значение **Да**).

Шаг 6. Настройка организации Exchange для использования проверки подлинности AD FS

Чтобы настроить организацию Exchange для использования проверки подлинности AD FS, необходимо использовать командную консоль Exchange. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

1. Выполните следующую команду, чтобы найти значение отпечатка импортированного сертификата подписи маркера AD FS:

   PowerShell

   ```
   Set-Location Cert:\LocalMachine\Root; Get-ChildItem | Sort-Object
   Subject
   ```

   Найдите значение `CN=ADFS Signing - <FederationServiceName>` Subject (например, `CN=ADFS Signing - adfs.contoso.com`).

   Это значение отпечатка можно подтвердить на сервере AD FS в окне с повышенными Windows PowerShell, выполнив команду `Import-Module ADFS`, а затем команду `Get-AdfsCertificate -CertificateType Token-Signing`.

2. Используйте следующий синтаксис.

   PowerShell

   ```
   Set-OrganizationConfig -AdfsIssuer
   https://<FederationServiceName>/adfs/ls/ -AdfsAudienceUris "
   <OotwURL>","<EACURL>" -AdfsSignCertificateThumbprint "<Thumbprint>"
   ```

   В этом примере используются следующие значения:

   - **URL-адрес AD FS**: `https://adfs.contoso.com/adfs/ls/`

- **URL-адрес Outlook в Интернете**: `https://mail.contoso.com/owa/`
- **URL-адрес EAC**: `https://mail.contoso.com/ecp/`
- **Отпечаток сертификата для подписи маркера AD FS**: `ADFS Signing - adfs.contoso.com` сертификат, имеющий значение `88970C64278A15D642934DC2961D9CCA5E28DA6B` отпечатка .

PowerShell

```
Set-OrganizationConfig -AdfsIssuer https://adfs.contoso.com/adfs/ls/ -
AdfsAudienceUris
"https://mail.contoso.com/owa/","https://mail.contoso.com/ecp/" -
AdfsSignCertificateThumbprint
"88970C64278A15D642934DC2961D9CCA5E28DA6B"
```

Примечание. Параметр *AdfsEncryptCertificateThumbprint* не поддерживается в этих сценариях.

Шаг 7. Настройка проверки подлинности AD FS в виртуальных каталогах Outlook в Интернете и EAC

Для виртуальных каталогов Outlook в Интернете и EAC необходимо настроить проверку подлинности AD FS как единственный доступный метод проверки подлинности, отключив все остальные методы проверки подлинности.

- Перед настройкой виртуального каталога Outlook в Интернете необходимо настроить виртуальный каталог EAC.
- Скорее всего, вам потребуется настроить проверку подлинности AD FS только на серверах Exchange с выходом в Интернет, которые клиенты используют для подключения к Outlook в Интернете и EAC.
- По умолчанию для виртуальных каталогов Outlook в Интернете и EAC включена только обычная проверка подлинности и проверка подлинности с помощью форм.

Чтобы использовать командную консоль Exchange для настройки EAC или Outlook в Интернете виртуального каталога только для принятия проверки подлинности AD FS, используйте следующий синтаксис:

PowerShell

```
Set-EcpVirtualDirectory -Identity <VirtualDirectoryIdentity> -
AdfsAuthentication $true -BasicAuthentication $false -DigestAuthentication
$false -FormsAuthentication $false -OAuthAuthentication $false -
WindowsAuthentication $false
```

В этом примере настраивается виртуальный каталог EAC на веб-сайте по умолчанию на сервере Mailbox01:

PowerShell

```
Set-EcpVirtualDirectory -Identity "Mailbox01\ecp (Default Web Site)" -
AdfsAuthentication $true -BasicAuthentication $false -DigestAuthentication
$false -FormsAuthentication $false -OAuthAuthentication $false -
WindowsAuthentication $false
```

В этом примере настраивается виртуальный каталог Outlook в Интернете на сайте по умолчанию на сервере Mailbox01:

PowerShell

```
Set-OwaVirtualDirectory -Identity "Mailbox01\owa (Default Web Site)" -
AdfsAuthentication $true -BasicAuthentication $false -DigestAuthentication
$false -FormsAuthentication $false -OAuthAuthentication $false -
WindowsAuthentication $false
```

Примечание. Чтобы настроить все виртуальные каталоги EAC и Outlook в Интернете на каждом сервере Exchange в организации, выполните следующие команды:

PowerShell

```
Get-EcpVirtualDirectory | Set-EcpVirtualDirectory -AdfsAuthentication $true
-BasicAuthentication $false -DigestAuthentication $false -
FormsAuthentication $false -OAuthAuthentication $false -
WindowsAuthentication $false
```

PowerShell

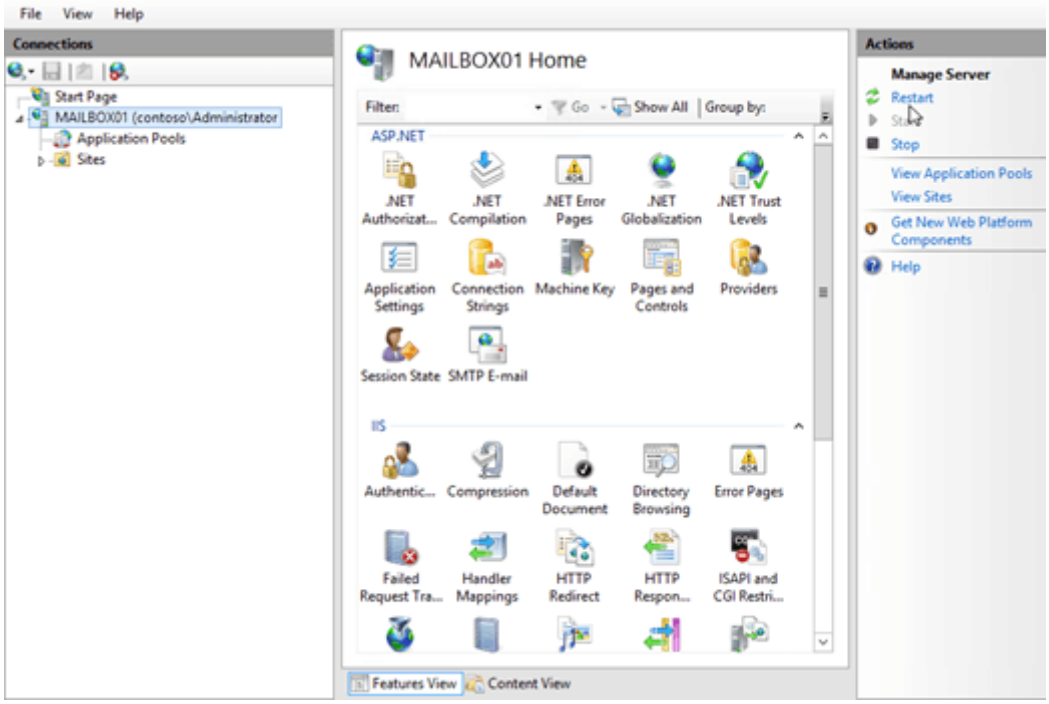
```
Get-OwaVirtualDirectory | Set-OwaVirtualDirectory -AdfsAuthentication $true
-BasicAuthentication $false -DigestAuthentication $false -
FormsAuthentication $false -OAuthAuthentication $false -
WindowsAuthentication $false
```

Шаг 8. Перезапуск СЛУЖБ IIS на сервере Exchange Server

1. Откройте диспетчер IIS на сервере Exchange Server. Простой способ сделать это в Windows Server 2012 или более поздней версии — нажать клавишу Windows + Q, ввести inetmgr и выбрать **Диспетчер служб IIS** в результатах.

2. В диспетчере IIS выберите сервер.

3. В области **Действия** выберите элемент **Перезапустить**.



Примечание. Чтобы выполнить эту процедуру в командной строке, откройте командную строку с повышенными привилегиями на сервере Exchange (открываемое окно командной строки, выбрав **Запуск от имени администратора**) и выполните следующие команды:

Консоль

```
net stop w3svc /y
```

Консоль

```
net start w3svc
```

Как проверить, все ли получилось?

Чтобы протестировать утверждения AD FS для Outlook в Интернете:

1. В веб-браузере откройте Outlook в Интернете (например, https://mail.contoso.com/owa).
2. Если в веб-браузере появляется ошибка сертификата, просто перейдите на сайт Outlook в Интернете. Вы должны быть перенаправлены на страницу входа AD FS или запрос ad FS на ввод учетных данных.
3. Введите имя пользователя (домен\пользователя) и пароль, а затем нажмите кнопку **Войти**.
4. Outlook в Интернете загрузится в окне.

Чтобы проверить утверждения AD FS для EAC, сделайте следующее.

1. В веб-браузере откройте EAC (например, https://mail.contoso.com/ecp).
2. Если в веб-браузере появляется ошибка сертификата, просто перейдите на веб-сайт EAC. Вы должны быть перенаправлены на страницу входа AD FS или запрос ad FS на ввод учетных данных.
3. Введите имя пользователя (домен\пользователя) и пароль, а затем нажмите кнопку **Войти**.
4. EAC загрузится в окне.

Дополнительные сведения

Многофакторная проверка подлинности

Развертывание и настройка AD FS для проверки подлинности на основе утверждений позволяет Outlook в Интернете и EAC поддерживать многофакторную проверку подлинности, например проверку подлинности на основе сертификата, проверку подлинности или маркеры безопасности и проверку подлинности по отпечатку пальца. Для многофакторной проверки подлинности требуются два из следующих трех факторов:

- То, что знает только пользователь (например, пароль, ПИН-код или шаблон).
- Что-то только у пользователя (например, карточка банкомата, маркер безопасности, смарт-карта или мобильный телефон).

- Что-то есть только у пользователя (например, биометрическая характеристика, например отпечаток пальца).

Например, пароль и код безопасности, отправленные на мобильный телефон, или ПИН-код и отпечаток пальца.

Дополнительные сведения о многофакторной проверке подлинности в Windows Server 2012 R2 см. в статьях Обзор: управление рисками для уязвимых приложений с помощью дополнительной многофакторной проверки подлинности и Пошаговое руководство: управление рисками для уязвимых приложений с помощью дополнительной многофакторной проверки подлинности.

На сервере AD FS служба федерации функционирует как служба маркеров безопасности и предоставляет маркеры безопасности, используемые с утверждениями. Служба федерации издает маркеры на основе предоставленных учетных данных. После того как хранилище учетных записей проверит учетные данные пользователя, в соответствии с правилами политики доверия для этого пользователя создаются утверждения, которые затем добавляются к маркеру безопасности, выданному клиенту. Дополнительные сведения о утверждениях см. в разделе Основные сведения о утверждениях.

Сосуществование с другими версиями Exchange

Вы можете использовать проверку подлинности AD FS для Outlook в Интернете и Центра администрирования Exchange, если в вашей организации развернуто несколько версий Exchange. Этот сценарий поддерживается только в том случае, если все клиенты подключаются через серверы Exchange **и** все эти серверы настроены для проверки подлинности AD FS.

В организациях Exchange 2016 пользователи с почтовыми ящиками на серверах Exchange 2010 могут получить доступ к своим почтовым ящикам через сервер Exchange 2016, настроенный для проверки подлинности AD FS. При первоначальном подключении клиента к серверу Или Exchange 2016 используется проверка подлинности AD FS. Однако прокси-подключение к Exchange 2010 использует Kerberos. Не поддерживается способ настройки Exchange 2010 для прямой проверки подлинности AD FS.

Правила клиентского доступа в Exchange 2019

Статья • 04.04.2023

Правила доступа клиентов помогают управлять доступом к организации Exchange 2019 в Центре администрирования Exchange (EAC) и удаленном PowerShell на основе свойств клиента или запросов на доступ клиента. Правила доступа клиента — это правила потока обработки почты (также известные как правила транспорта) для EAC и удаленных подключений PowerShell к организации Exchange. Вы можете запретить подключение EAC и удаленных клиентов PowerShell к Exchange на основе их IP-адреса (IPv4 и IPv6), типа проверки подлинности и значений свойств пользователя. Например:

- Запретите клиентский доступ с помощью удаленной оболочки PowerShell (которая также включает в себя командную консоль Exchange).
- Блокировка доступа к EAC для пользователей в определенной стране или регионе.

Процедуры правил клиентского доступа см. в разделе Процедуры для правил клиентского доступа в Exchange Server.

Компоненты правил клиентского доступа

Правило состоит из условий, исключений, действия и значения приоритета.

- **Условия**. Определите клиентские подключения, к которому нужно применить действие. Полный список условий см. в разделе Условия и исключения правила клиентского доступа далее в этом разделе. Если клиентское подключение соответствует условиям правила, действие применяется к клиентскому подключению, и оценка правила останавливается (больше к подключению не применяются правила).

- **Исключения**. При необходимости определите клиентские подключения, к которым не должно применяться действие. Исключения переопределяют условия и запрещают применение действий правила к подключению, даже если оно соответствует всем настроенным условиям. Оценка правила продолжается для клиентских подключений, разрешенных исключением, но последующее правило по-прежнему может повлиять на подключение.

- **Действие**. Указывает, что следует делать с клиентскими подключениями, которые соответствуют условиям в правиле и не соответствуют ни одному из исключений. Допустимые действия:

  - Разрешить подключение (`AllowAccess` значение параметра *Action*).

  - Блокировать подключение (`DenyAccess` значение параметра *Action*).

    Примечание. Блокировка подключений по определенному протоколу может повлиять на другие приложения, использующие этот протокол.

- **Приоритет**: указывает порядок применения правил к клиентским подключениям (меньшее число указывает на более высокий приоритет). Приоритет, заданный по умолчанию, зависит от времени создания правила (чем старше правило, тем выше приоритет), а проверка в случае правил с высоким приоритетом выполняется раньше, чем в случае правил с низким приоритетом. Помните, что если клиентское подключение соответствует условиям правила, обработка правил останавливается.

  Дополнительные сведения о настройке значения приоритета для правил см. в разделе Использование командной консоли Exchange для задания приоритета правил доступа клиентов.

Как оцениваются правила клиентского доступа

В приведенной ниже таблице описывается оценка нескольких правил, включающих одно и то же условие, а также правил с несколькими условиями, значениями условий и исключениями.

Компонент	Логический оператор	Комментарии
Несколько правил, содержащих одно условие	Первое правило применяется, а последующие пропускаются	Например, если правило с наивысшим приоритетом блокирует удаленные подключения PowerShell и вы создаете другое правило, разрешающее удаленные подключения PowerShell для определенного диапазона IP-адресов, все удаленные подключения PowerShell по-прежнему блокируются первым правилом. Вместо создания другого правила для удаленного powerShell необходимо добавить исключение в существующее удаленное правило PowerShell, чтобы разрешить подключения из указанного диапазона IP-адресов.

Компонент	Логический оператор	Комментарии
Несколько условий в одном правиле	И	Клиентское подключение должно соответствовать всем условиям правила. Например, подключения EAC от пользователей в отделе бухгалтерского учета.
Одно условие с несколькими значениями в правиле	ИЛИ	Для условий, в которых разрешено несколько значений, подключение должно соответствовать одному (не всем) из указанных условий. Например, EAC или удаленные подключения PowerShell.
Несколько исключений в одном правиле	ИЛИ	Если клиентское подключение соответствует какому-либо из исключений, то к нему не применяются действия. Подключению не обязательно соответствовать всем исключениям. Примеры: IP-адрес 19.2.168.1.1 или обычная проверка подлинности.

Вы можете проверить, как правила клиентского доступа повлияют на то или иное клиентское подключение (какие правила будут к нему применяться). Дополнительные сведения см. в статье Использование командной консоли Exchange для проверки правил доступа клиентов.

Важные замечания

Клиентские подключения из внутренней сети

Подключениям из локальной сети не разрешается автоматически обходить правила клиентского доступа. Поэтому при создании правил клиентского доступа, которые блокируют клиентские подключения к Exchange, необходимо учитывать, как это может повлиять на подключения из внутренней сети. Предпочитаемый способ разрешить внутренним клиентским подключениям обходить правила клиентского доступа — создать правило с самым высоким приоритетом, которое разрешает клиентские подключения из внутренней сети (со всех или только с определенных IP-адресов). Таким образом, клиентские подключения всегда разрешены, независимо от того, какие блокирующие правила будут созданы в будущем.

Правила клиентского доступа и приложения среднего уровня

Многие приложения, которые обращаются к Exchange, используют архитектуру среднего уровня (клиенты обращаются к приложению среднего уровня, а приложение среднего уровня взаимодействует с Exchange). Правило клиентского доступа, разрешающее доступ только из локальной среды, может блокировать приложения среднего уровня. Таким образом, правила должны разрешать доступ с IP-адресов приложений среднего уровня.

Приложения среднего уровня, принадлежащие корпорации Майкрософт (например, Outlook для iOS и Android), будут обходить блокировку правилами доступа клиентов и всегда будут разрешены. Чтобы предоставить дополнительный контроль над этими приложениями, необходимо использовать доступные в них возможности управления.

Время изменения правил

Для повышения общей производительности правила клиентского доступа используют кэш, поэтому изменения правил вступают в силу не сразу. Чтобы первое правило, созданное в организации, вступило в силу, может потребоваться до 24 часов. После этого изменение, добавление и удаление правил может занимать до одного часа.

Администрирование

Вы можете использовать командную консоль Exchange (удаленную оболочку PowerShell) только для управления правилами доступа клиентов, поэтому необходимо быть осторожными с правилами, которые блокируют доступ к удаленному PowerShell.

Рекомендуется создать правило клиентского доступа с наивысшим приоритетом, чтобы сохранить доступ к удаленной оболочке PowerShell. Например:

PowerShell

```
New-ClientAccessRule -Name "Always Allow Remote PowerShell" -Action Allow -AnyOfProtocols RemotePowerShell -Priority 1
```

Типы и протоколы проверки подлинности

Не все типы проверки подлинности поддерживаются для всех протоколов. Поддерживаемые типы проверки подлинности для каждого протокола в Exchange Server описаны в следующей таблице:

Протокол	AdfsAuthentication	BasicAuthentication	CertificateBasedAuthentication	NonBasicAuthentication	OAuthAuthentication
`ExchangeAdminCenter`	поддерживается	поддерживается	н/д	н/д	н/д
`RemotePowerShell`	н/д	поддерживается	н/д	поддерживается	н/д

Условия и исключения для правил клиентского доступа

Условия и исключения в правилах клиентского доступа определяют, к каким клиентским подключениям правило применяется, а к каким — нет. Например, если правило блокирует доступ удаленных клиентов PowerShell, можно настроить правило так, чтобы разрешить удаленные подключения PowerShell из определенного диапазона IP-адресов. В условии и соответствующем исключении используется один и тот же синтаксис. Единственное отличие заключается в том, что условия указывают, к каким клиентским подключениям правило применяется, а исключения — наоборот.

В приведенной ниже таблице описываются условия и исключения, доступные в правилах клиентского доступа.

Параметр Condition в командной консоли Exchange	Параметр exception в командной консоли Exchange	Описание
AnyOfAuthenticationTypes	*ExceptAnyOfAuthenticationTypes*	Допустимые значения в Exchange Server: • Для EAC: `AdfsAuthentication` и `BasicAuthentication` • Для удаленной оболочки PowerShell: `BasicAuthentication` и `NonBasicAuthentication` Вы можете указать несколько значений, разделив их запятыми. Можно использовать кавычки вокруг каждого отдельного значения ("*value1*","*value2*"), но не для всех значений (не используйте "*value1,value2*").
AnyOfClientIPAddressesOrRanges	*ExceptAnyOfClientIPAddressesOrRanges*	Поддерживаются адреса IPv4 и IPv6. Допустимые значения: • **Один IP-адрес**: например, 192.168.1.1 или 2001:DB8:2AA:FF:C0A8:640A. • **Диапазон IP-адресов**: например, 192.168.0.1-192.168.0.254 или 2001:DB8:2AA:FF:C0A8:640A-2001:DB8:2AA:FF:C0A8:6414. • **IP-адрес маршрутизации Inter-Domain (CIDR):** например, 192.168.3.1/24 или 2001:DB8:2AA:FF:C0A8:640A/64. Вы можете указать несколько значений, разделив их запятыми. Дополнительные сведения об IPv6-адресах и синтаксисе см. в разделе Exchange 2013: IPv6-адреса основы.
AnyOfProtocols	*ExceptAnyOfProtocols*	Допустимые значения в Exchange Server: • `ExchangeAdminCenter` • `RemotePowerShell` Вы можете указать несколько значений, разделив их запятыми. Можно использовать кавычки вокруг каждого отдельного значения ("*value1*","*value2*"), но не вокруг всех значений (не используйте "*value1,value2*"). **Примечание**. Если это условие не используется в правиле, правило применяется к обоим протоколам.
Scope	н/д	Задает тип подключений, к которым применяется правило. Допустимые значения: • `Users`: правило применяется только к подключениям конечных пользователей. • `All`: правило применяется ко всем типам подключений (конечным пользователям и приложениям среднего уровня).

Параметр Condition в командной консоли Exchange	Параметр exception в командной консоли Exchange	Описание
UsernameMatchesAnyOfPatterns	*ExceptUsernameMatchesAnyOfPatterns*	Принимает текст и подстановочный знак (*) для идентификации имени учетной записи пользователя в формате `<Domain>\<UserName>` (например, `contoso.com\jeff` или `*jeff*`, но не `jeff*`). Для символов, не являющихся буквенно-цифровыми, не требуются escape-символы. Вы можете указать несколько значений, разделив их запятыми.
UserRecipientFilter	н/д	Указывает пользователя, к которому применяется правило, с помощью синтаксиса фильтра OPath. Например, `"City -eq 'Redmond'"`. Фильтруемые атрибуты: • `City` • `Company` • `CountryOrRegion` • `CustomAttribute1` меняется на `CustomAttribute15` • `Department` • `Office` • `PostalCode` • `StateOrProvince` • `StreetAddress` Для критериев поиска используется следующий синтаксис: `"<Property> -<Comparison operator> '<Value>'"`. • `<Property>` является фильтруемым свойством. • `-<Comparison Operator>` — оператор сравнения OPATH. Например, `-eq` для точных совпадений (подстановочные знаки не поддерживаются) и `-like` для сравнения строк (для которого требуется по крайней мере один подстановочный знак в значении свойства). Подробнее об операторах сравнения см. в статье about_Comparison_Operators. • `<Value>` — это значение свойства. Текстовые значения с пробелами или без нее или значения с подстановочными знаками (*) должны быть заключены в кавычки (например, `'<Value>'` или `'*<Value>'`). Не используйте кавычки с системным значением `$null` (для пустых значений). Можно связать несколько условий поиска вместе с помощью логических операторов `-and` и `-or`. Например, `"<Criteria1> -and <Criteria2>"` или `"(<Criteria1> -and <Criteria2>) -or <Criteria3>"`. Дополнительные сведения о синтаксисе фильтра OPATH см. в разделе Дополнительные сведения о синтаксисе OPATH.

Процедуры для правил доступа клиентов в Exchange 2019

Статья • 04.04.2023

Правила клиентского доступа разрешают или блокируют подключения Центра администрирования Exchange (EAC) или удаленного подключения PowerShell к организации Exchange 2019 в зависимости от свойств подключения. Дополнительные сведения о правилах клиентского доступа см. в разделе Правила клиентского доступа в Exchange Server.

> **Совет**
>
> Убедитесь, что правила работают надлежащим образом. Тщательно тестируйте все правила и взаимодействия между ними. Дополнительные сведения см. в разделе **Использование командной консоли Exchange для проверки правил доступа клиентов** далее в этом разделе.

Что нужно знать перед началом работы

- Предполагаемое время выполнения каждой процедуры: менее 5 минут.
- Процедуры, описанные в этом разделе, доступны только в командной консоли Exchange. Дополнительные сведения см. в разделе Открытие командной консоли Exchange или Подключение к серверам Exchange с помощью удаленной оболочки PowerShell.
- Правила доступа клиентов поддерживают адреса IPv4 и IPv6. Дополнительные сведения об IPv6-адресах и синтаксисе см. в разделе Exchange 2013: IPv6-адреса основы.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Поток обработки почты" в разделе Разрешения потока обработки почты.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по **адресу Exchange Server**.

Использование командной консоли Exchange для просмотра правил доступа клиентов

Следующая команда возвращает сводный список всех правил клиентского доступа:

```
PowerShell

Get-ClientAccessRule
```

Чтобы получить подробные сведения об определенном правиле, используйте следующий синтаксис:

```
PowerShell

Get-ClientAccessRule -Identity "<RuleName>" | Format-List [<Specific
properties to view>]
```

В этом примере возвращаются значения всех свойств правила "Block Client Connections from 192.168.1.0/24".

```
PowerShell

Get-ClientAccessRule -Identity "Block Client Connections from
192.168.1.0/24" | Format-List
```

В этом примере возвращаются только указанные свойства правила.

```
PowerShell

Get-ClientAccessRule -Identity "Block Client Connections from
192.168.1.0/24" | Format-List Name,Priority,Enabled,Scope,Action
```

Подробные сведения о синтаксисе и параметрах см. в статье Get-ClientAccessRule.

Создание правил клиентского доступа с помощью командной консоли Exchange

Чтобы создать правила клиентского доступа в командной консоли Exchange, используйте следующий синтаксис:

```
```

PowerShell

```
New-ClientAccessRule -Name "<RuleName>" [-Priority <PriorityValue>] [-
Enabled <$true | $false>] -Action <AllowAccess | DenyAccess> [<Conditions>]
[<Exceptions>]
```

В этом примере создается новое правило клиентского доступа с именем Block PowerShell, которое блокирует удаленный доступ к PowerShell, за исключением клиентов в диапазоне IP-адресов 192.168.10.1/24.

PowerShell

```
New-ClientAccessRule -Name "Block PowerShell" -Action DenyAccess -
AnyOfProtocols RemotePowerShell -ExceptAnyOfClientIPAddressesOrRanges
192.168.10.1/24
```

Примечания.

- Рекомендуется создать правило клиентского доступа с наивысшим приоритетом, чтобы сохранить доступ администратора к удаленной оболочке PowerShell. Пример: `New-ClientAccessRule -Name "Always Allow Remote PowerShell" -Action Allow -AnyOfProtocols RemotePowerShell -Priority 1`.
- Для правила задано значение приоритета по умолчанию, так как мы не использовали параметр *Priority*. Дополнительные сведения см. в разделе Использование командной консоли Exchange для задания приоритета правил доступа клиентов далее в этом разделе.
- Правило включено, так как мы не использовали параметр *Enabled* , а значение по умолчанию — `$true`.

В этом примере создается новое правило клиентского доступа с именем Restrict EAC Access, которое блокирует доступ для Центра администрирования Exchange, за исключением случаев, когда клиент поступает с IP-адреса в диапазоне 192.168.10.1/24 или если имя учетной записи пользователя содержит "tanyas".

PowerShell

```
New-ClientAccessRule -Name "Restrict EAC Access" -Action DenyAccess -
AnyOfProtocols ExchangeAdminCenter -ExceptAnyOfClientIPAddressesOrRanges
192.168.10.1/24 -ExceptUsernameMatchesAnyOfPatterns *tanyas*
```

Подробные сведения о синтаксисе и параметрах см. в статье New-ClientAccessRule.

Как проверить, все ли получилось?

Чтобы убедиться, что правило клиентского доступа успешно создано, выполните одно из указанных ниже действий.

- Выполните следующую команду в командной консоли Exchange, чтобы увидеть новое правило в списке правил:

  PowerShell

  ```
  Get-ClientAccessRule
  ```

- Замените <*RuleName*> именем правила и выполните следующую команду, чтобы просмотреть сведения о правиле:

  PowerShell

  ```
  Get-ClientAccessRule -Identity "<RuleName>" | Format-List
  ```

- Узнайте, какие правила клиентского доступа повлияют на определенное клиентское подключение к Exchange, с помощью командлета **Test-ClientAccessRule** . Дополнительные сведения см. в разделе Использование командной консоли Exchange для проверки правил доступа клиентов далее в этом разделе.

Изменение правил доступа клиентов с помощью командной консоли Exchange

При изменении правила клиентского доступа никакие дополнительные параметры не используются. В этом случае доступны те же параметры, что и при создании правила.

Чтобы изменить правило клиентского доступа в командной консоли Exchange, используйте следующий синтаксис:

PowerShell

```
Set-ClientAccessRule -Identity "<RuleName>" [-Name "<NewName>"] [-Priority
<PriorityValue>] [-Enabled <$true | $false>] -Action <AllowAccess |
DenyAccess> [<Conditions>] [<Exceptions>]
```

В этом примере отключается существующее правило клиентского доступа с именем Allow EAC.

PowerShell

```
Set-ClientAccessRule -Identity "Allow EAC" -Enabled $false
```

При изменении правил клиентского доступа обратите особое внимание на изменение условий или исключений, которые принимают несколько значений:

- Указанные вами значения *заменят* существующие значения.
- Чтобы добавить или удалить значения без влияния на другие существующие значения, используйте следующий синтаксис: `@{Add="<Value1>","<Value2>"...; Remove="<Value1>","<Value2>"...}`

В этом примере диапазон IP-адресов 172.17.17.27/16 добавляется в существующее правило клиентского доступа с именем Разрешить EAC, не затрагивая существующие значения IP-адресов.

PowerShell

```
Set-ClientAccessRule -Identity "Allow EAC" -AnyOfClientIPAddressesOrRanges
@{Add="172.17.17.27/16"}
```

Подробные сведения о синтаксисе и параметрах см. в статье Set-ClientAccessRule.

Как проверить, все ли получилось?

Чтобы убедиться, что правило клиентского доступа успешно изменено, выполните одно из указанных ниже действий.

- Замените <*RuleName*> именем правила и выполните следующую команду, чтобы просмотреть сведения о правиле:

  PowerShell

  ```
  Get-ClientAccessRule -Identity "<RuleName>" | Format-List
  ```

- Узнайте, какие правила клиентского доступа повлияют на определенное клиентское подключение к Exchange, с помощью командлета **Test-ClientAccessRule** . Дополнительные сведения см. в разделе Использование командной консоли Exchange для проверки правил доступа клиентов далее в этом разделе.

Использование командной консоли Exchange для задания приоритета правил доступа клиентов

По умолчанию правилам клиентского доступа присваивается приоритет, основанный на порядке их создания (новые правила имеют более низкий приоритет, чем старые). Более низкий приоритет указывает на более высокий приоритет правила, а правила обрабатываются в порядке приоритета (правила с более высоким приоритетом обрабатываются перед правилами с более низким приоритетом). Два правила не могут иметь одинаковый приоритет.

Максимальный приоритет, который можно задать для правила, — 1. Минимальное значение зависит от количества правил. Например, если у вас есть пять правил, вы можете использовать значения 1-5. Изменение приоритета существующего правила оказывает каскадное влияние на другие правила. Например, если вы замените приоритет правила 5 приоритетом 2, когда у вас есть пять правил (с приоритетами от 1 до 5), то для существующего правила с приоритетом 2 будет задан приоритет 3, для правила с приоритетом 3 — приоритет 4, а для правила с приоритетом 4 — приоритет 5.

Чтобы задать приоритет правила клиентского доступа в командной консоли Exchange, используйте следующий синтаксис:

PowerShell

```
Set-ClientAccessRule -Identity "<RuleName>" -Priority <Number>
```

В этом примере для правила с именем Disable PowerShell задается приоритет 3. Все существующие правила, приоритет которых меньше или равен 3, уменьшаются на 1 (их приоритеты увеличиваются на 1).

PowerShell

```
Set-ClientAccessRule -Identity "Disable PowerShell" -Priority 4
```

Примечание. Чтобы задать приоритет нового правила при его создании, используйте параметр *Priority* командлета **New-ClientAccessRule**.

Как проверить, все ли получилось?

Чтобы убедиться, что приоритет правила клиентского доступа успешно задан, выполните одно из указанных ниже действий.

- Выполните следующую команду в командной консоли Exchange, чтобы просмотреть список правил и их значения **Priority** :

```
PowerShell

Get-ClientAccessRule
```

- Замените <*RuleName*> именем правила и выполните следующую команду:

```
PowerShell

Get-ClientAccessRule -Identity "<RuleName>" | Format-List Name,Priority
```

Удаление правил клиентского доступа с помощью командной консоли Exchange

Чтобы удалить правила клиентского доступа в командной консоли Exchange, используйте следующий синтаксис:

```
PowerShell

Remove-ClientAccessRule -Identity "<RuleName>"
```

В этом примере удаляется правило клиентского доступа с именем Block EAC.

```
PowerShell

Remove-ClientAccessRule -Identity "Block EAC"
```

Примечание. Чтобы отключить правило клиентского доступа, не удаляя его, используйте параметр *Enabled* со значением `$false` в командлете **Set-ClientAccessRule** .

Подробные сведения о синтаксисе и параметрах см. в статье Remove-ClientAccessRule.

Как проверить, все ли получилось?

Чтобы убедиться, что правило клиентского доступа успешно удалено, выполните следующую команду в командной консоли Exchange, чтобы убедиться, что правило больше не указано в списке:

PowerShell

```
Get-ClientAccessRule
```

Проверка правил клиентского доступа с помощью командной консоли Exchange

Чтобы узнать, какие правила клиентского доступа повлияют на определенное клиентское подключение к Exchange, используйте следующий синтаксис:

PowerShell

```
Test-ClientAccessRule -User <MailboxIdentity> -AuthenticationType
<AuthenticationType> -Protocol <Protocol> -RemoteAddress <ClientIPAddress> -
RemotePort <TCPPortNumber>
```

В этом примере возвращаются правила клиентского доступа, которые будут соответствовать клиентскому подключению к Exchange со следующими свойствами:

- **Тип проверки подлинности**: "Базовый"
- **Протокол**: `ExchangeAdminCenter`
- **Удаленный адрес**: 172.17.17.26
- **Удаленный порт**: 443
- **Пользователь**: julia@contoso.com

PowerShell

```
Test-ClientAccessRule -User julia@contoso.com -AuthenticationType
BasicAuthentication -Protocol ExchangeAdminCenter -RemoteAddress
172.17.17.26 -RemotePort 443
```

Подробные сведения о синтаксисе и параметрах см. в статье Test-ClientAccessRule.

Поток обработки почты и транспортный конвейер

Статья • 04.04.2023

В Exchange Server поток почты проходит через транспортный конвейер. *Транспортный конвейер* — это коллекция служб, соединений, компонентов и очередей, которые совместно направляют все сообщения в классификатор в транспортной службе на сервере почтовых ящиков Exchange в организации.

Сведения о настройке потока обработки почты в новой организации Exchange 2016 или Exchange 2019 см. в статье Настройка потока обработки почты и клиентского доступа.

Общие сведения о транспортном конвейере

Транспортный конвейер состоит из следующих служб:

- **Транспортная служба переднего плана на серверах почтовых ящиков**. Эта служба выступает в качестве прокси-сервера без отслеживания состояния для всего входящего и (при необходимости) исходящего внешнего SMTP-трафика для Exchange Server организации. Внешняя служба транспорта не проверяет содержимое сообщений, не обменивается данными со службой транспорта почтовых ящиков и не ставит сообщения в локальную очередь.

- **Транспортная служба на серверах почтовых ящиков**. Эта служба практически идентична роли транспортного сервера-концентратора в Exchange Server 2010 г. Служба транспорта обрабатывает весь поток обработки почты SMTP для организации, выполняет классификацию сообщений и проверку их содержимого. В отличие от Exchange 2010, транспортная служба никогда не взаимодействует напрямую с базами данных почтовых ящиков. Эту задачу теперь выполняет служба транспорта почтовых ящиков. Служба транспорта передает сообщения между службой транспорта почтовых ящиков, службой транспорта, внешней службой транспорта и (в зависимости от вашей конфигурации) службой транспорта на пограничных транспортных серверах. В этой статье более подробно описывается служба транспорта на серверах почтовых ящиков.

- **Служба транспорта почтовых ящиков на серверах почтовых ящиков**. Эта служба состоит из двух отдельных служб:

- **Служба отправки транспорта почтовых ящиков**. Эта служба подключается к локальной базе данных почтовых ящиков с помощью удаленного вызова процедуры Exchange (RPC) для получения сообщений. Служба отправляет сообщения по протоколу SMTP службе транспорта на локальном (или другом) сервере почтовых ящиков. Службе отправки транспорта почтовых ящиков доступны те же данные о топологии маршрутизации, что и службе транспорта.

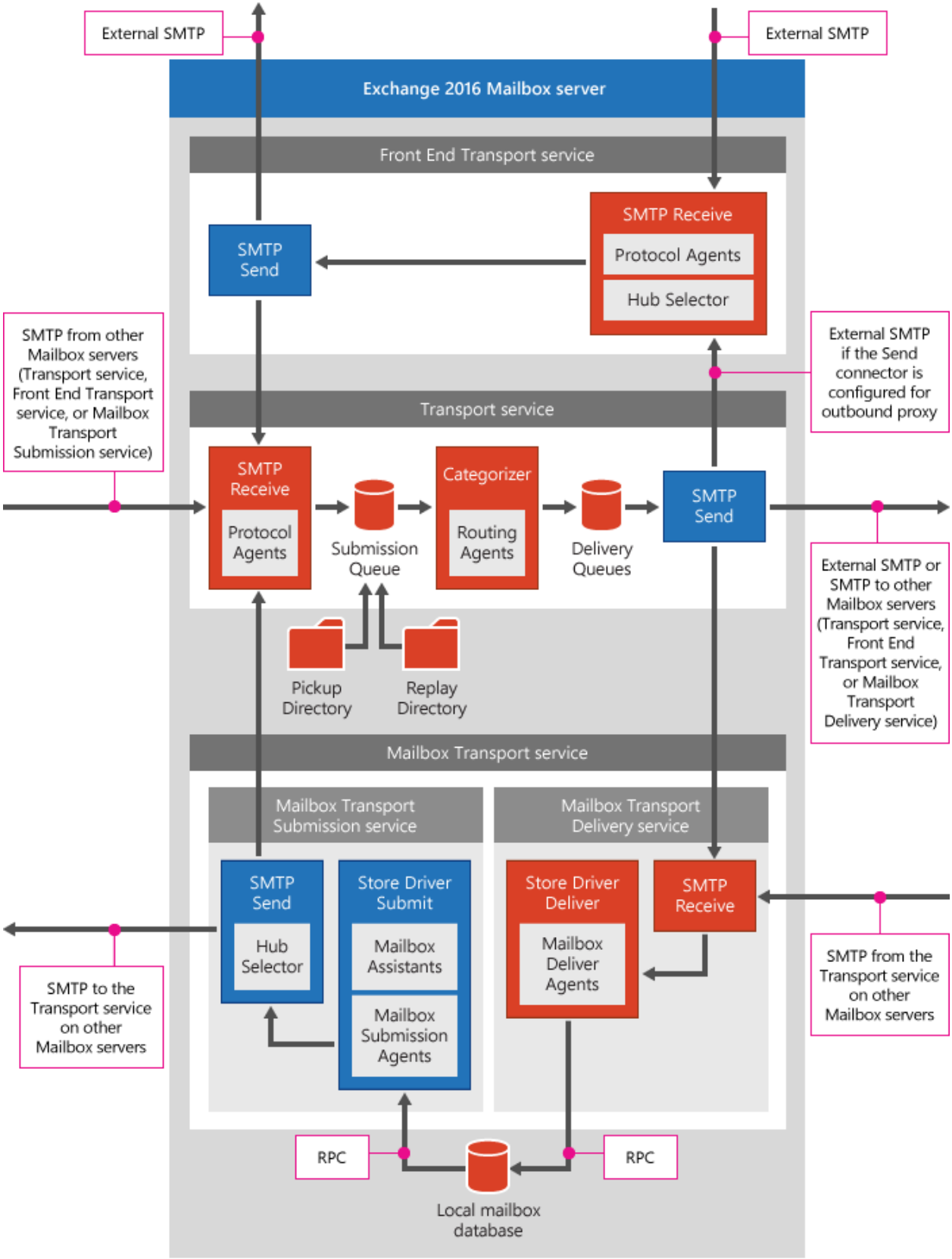
- **Служба доставки транспорта почтовых ящиков**. Эта служба получает SMTP-сообщения от службы транспорта на локальном сервере почтовых ящиков или на других серверах почтовых ящиков и подключается к локальной базе данных почтовых ящиков с помощью RPC для доставки сообщений.

  Служба транспорта почтовых ящиков не взаимодействует со внешней службой транспорта, службой транспорта почтовых ящиков и базами данных почтовых ящиков на других серверах почтовых ящиков. Кроме того, она не ставит сообщения в локальную очередь.

- **Транспортная служба на пограничных транспортных серверах**. Эта служба очень похожа на транспортную службу на серверах почтовых ящиков. Если в сети периметра установлен пограничный транспортный сервер, вся входящая и исходящая почта Интернета проходит через пограничный транспортный сервер транспортной службы. Эта служба описана более подробно далее в этом разделе.

На следующей схеме показаны связи между компонентами в конвейере транспорта Exchange.

> ⓘ **Примечание**
>
> Хотя на схемах в этом разделе показаны компоненты на одном сервере Exchange Server, взаимодействие также происходит между этими компонентами на разных серверах Exchange. Единственное взаимодействие, которое всегда происходит на локальном сервере Exchange Server, — это между транспортной службой почтовых ящиков и локальной базой данных почтовых ящиков.



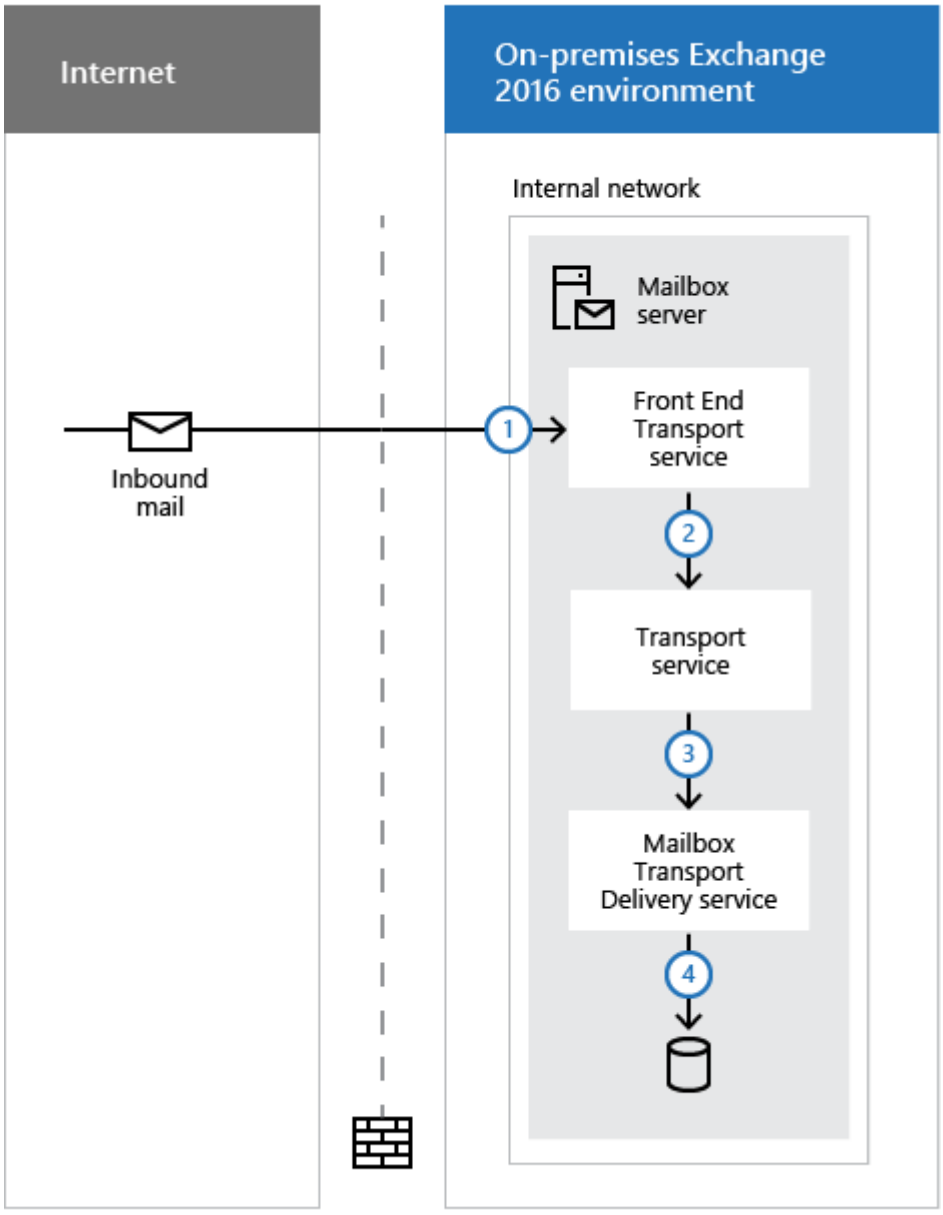
Как сообщения от внешних отправителей поступают в транспортный конвейер

Способ поступления сообщений из-за пределов организации Exchange в транспортный конвейер зависит от того, развернут ли в сети периметра

подписанный пограничный транспортный сервер.

Поток обработки входящей почты (без пограничных транспортных серверов)

На следующей схеме и списке описывается поток входящей почты только с серверами почтовых ящиков Exchange.



1. Сообщение извне организации входит в транспортный конвейер через соединитель получения по умолчанию с именем "*Имя> сервера внешних< почтовых ящиков* по умолчанию" в транспортной службе переднего плана.

2. Сообщение отправляется службе транспорта на локальном (или другом) сервере почтовых ящиков. Транспортная служба прослушивает сообщения в

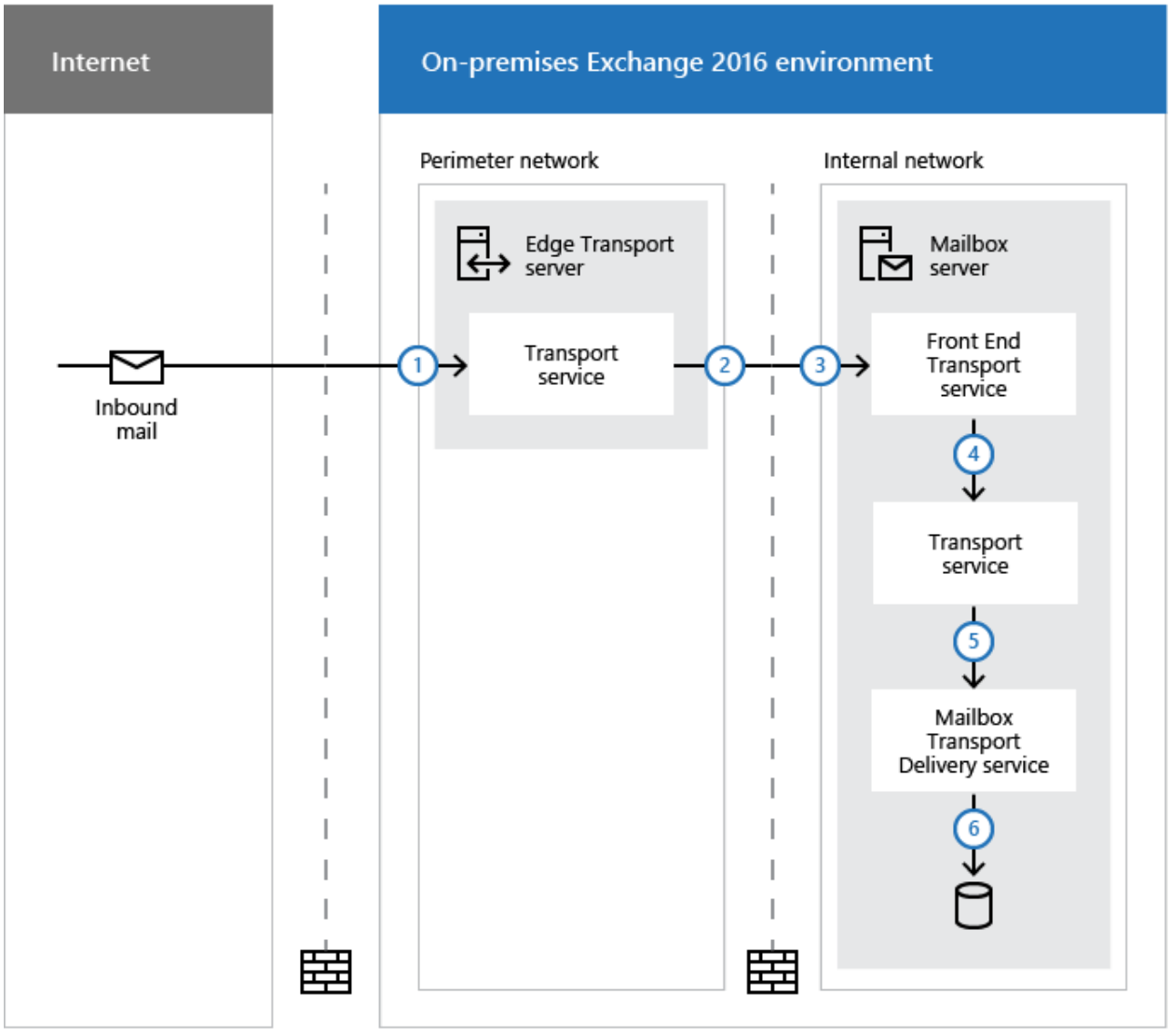
соединителе получения по умолчанию с именем "*Имя> сервера почтовых ящиков по умолчанию<*".

3. Сообщение отправляется из транспортной службы в службу доставки транспорта почтовых ящиков на локальном сервере почтовых ящиков или на другом сервере почтовых ящиков.

4. Затем служба доставки транспорта почтовых ящиков использует RPC для доставки сообщения в локальную базу данных почтовых ящиков.

Поток обработки входящей почты с пограничными транспортными серверами

На приведенной ниже схеме и в представленном ниже списке описывается поток обработки почты с пограничным транспортным сервером, установленным в сети периметра



1. Сообщение из-за пределов организации Exchange поступает в транспортный конвейер через соединитель получения по умолчанию с именем "*Имя> пограничного транспортного сервера внутреннего соединителя<* получения" в транспортной службе на пограничном транспортном сервере.

2. В транспортной службе на пограничном транспортном сервере соединитель отправки по умолчанию с именем "EdgeSync — входящий в *<Active Directory имя> сайта*" отправляет сообщение на сервер почтовых ящиков на сайте Active Directory с подпиской.

3. В транспортной службе переднего плана на сервере почтовых ящиков соединитель получения по умолчанию с именем "*Имя> сервера внешних< почтовых ящиков* по умолчанию" принимает сообщение.

4. Сообщение отправляется из внешней службы транспорта в службу транспорта на локальном (или другом) сервере почтовых ящиков. Транспортная служба прослушивает сообщения в соединителе получения по умолчанию с именем "*Имя> сервера почтовых ящиков по умолчанию<*".

5. Сообщение отправляется из транспортной службы в службу доставки транспорта почтовых ящиков на локальном сервере почтовых ящиков или на другом сервере почтовых ящиков.

6. Затем служба доставки транспорта почтовых ящиков использует RPC для доставки сообщения в локальную базу данных почтовых ящиков.

Как сообщения от внутренних отправителей поступают в транспортный конвейер

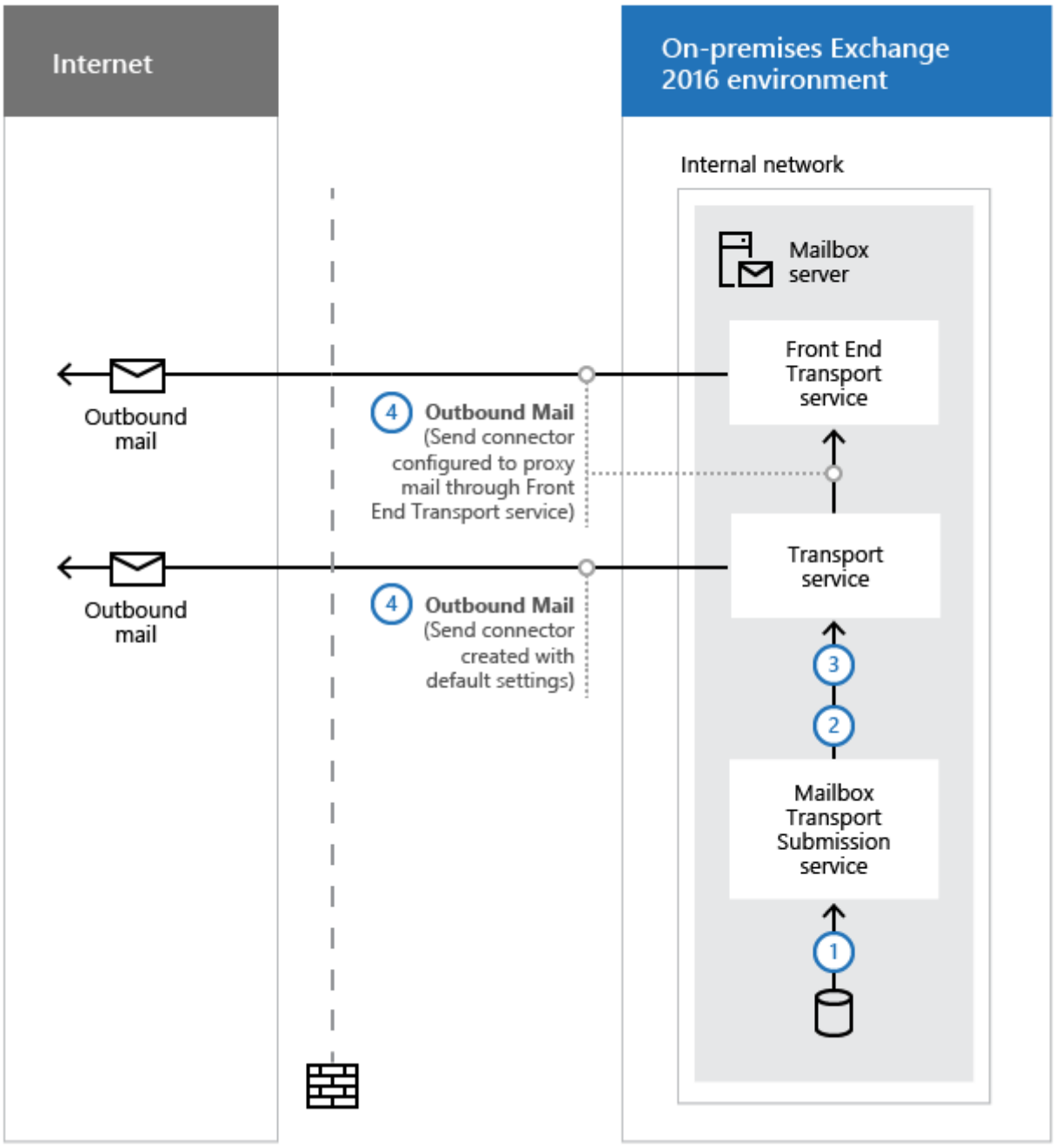
SMTP-сообщения внутри организации попадают на транспортный конвейер через транспортную службу на сервере почтовых ящиков одним из указанных ниже способов.

- Через соединитель приема.
- Из каталога раскладки или преобразования.
- Из службы отправки транспорта почтовых ящиков.
- Через агент доставки.

Сообщение направляется в соответствии с назначением маршрутизации или группой доставки.

Поток обработки исходящей почты (без пограничных транспортных серверов)

По умолчанию в новой организации Exchange Server нет соединителя отправки, настроенного для отправки сообщений в Интернет. Соединитель отправки необходимо создать самостоятельно. После этого поток обработки исходящей почты работает так, как показано на представленной ниже схеме и в приведенном списке.



1. Служба отправки транспорта почтовых ящиков использует RPC для получения исходящего сообщения из локальной базы данных почтовых ящиков.

2. Служба отправки транспорта почтовых ящиков использует ПРОТОКОЛ SMTP для отправки сообщения в транспортную службу на локальном сервере почтовых ящиков или на другом сервере почтовых ящиков.

3. В транспортной службе соединитель получения по умолчанию с именем "*Имя> сервера почтовых ящиков по умолчанию<*" принимает сообщение.

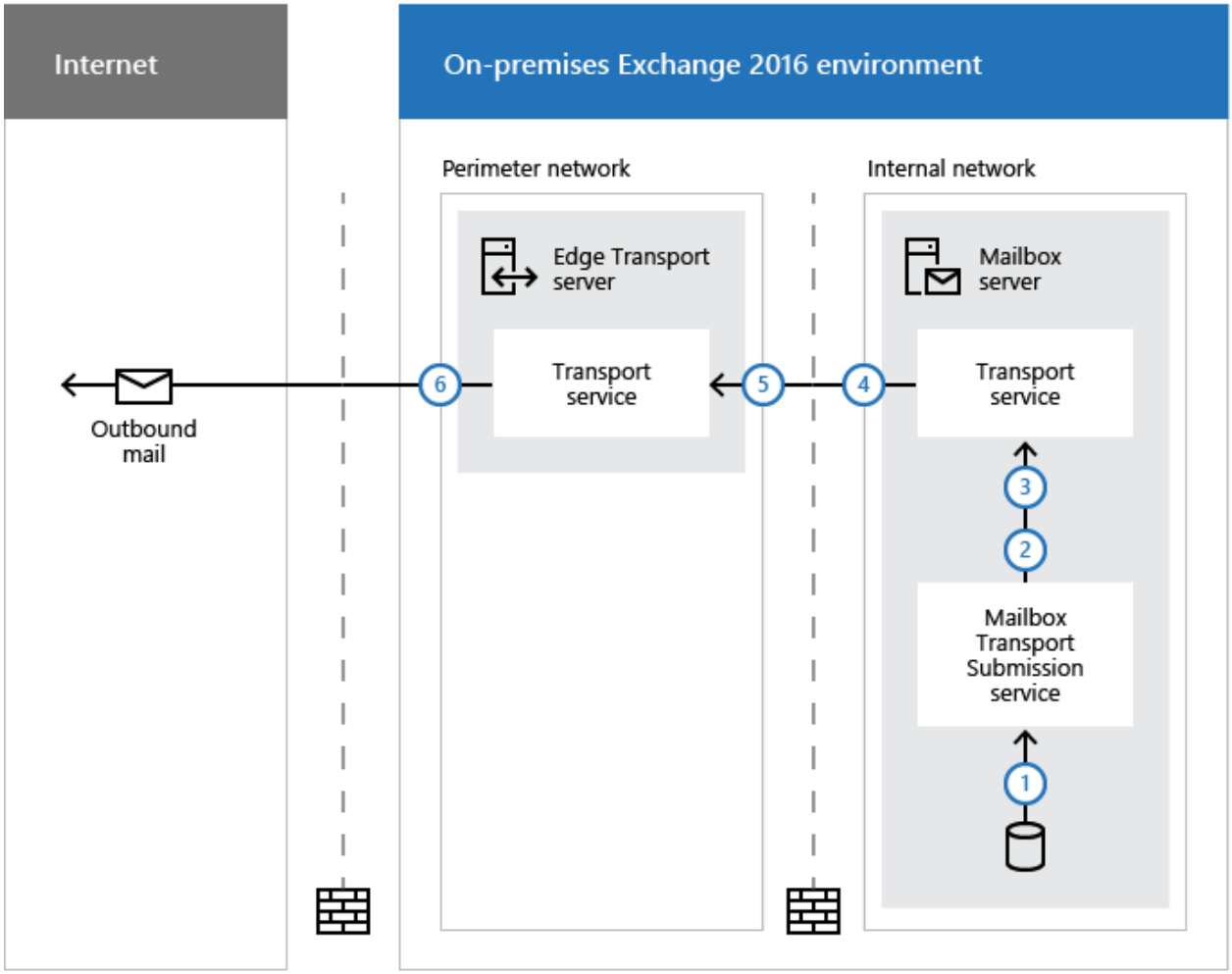
4. Дальнейшие действия зависят от конфигурации соединителя отправки:

    - **По умолчанию**: служба транспорта использует созданный соединитель отправки для отправки сообщения в Интернет.

    - **Исходящий прокси-сервер**. Транспортная служба использует созданный соединитель отправки для отправки сообщения в службу внешнего транспорта на локальном сервере почтовых ящиков или на удаленном сервере почтовых ящиков. В транспортной службе переднего плана соединитель получения по умолчанию с именем "*Имя> внешнего почтового ящика исходящего прокси-сервера<*" принимает сообщение. Внешняя служба транспорта отправляет сообщение в Интернет.

Поток обработки исходящей почты с пограничными транспортными серверами

Если в сети периметра установлен пограничный транспортный сервер, исходящая почта никогда не проходит через внешнюю службу транспорта. Поток обработки исходящей почты с пограничным транспортным сервером описывается на представленной ниже схеме и в приведенном списке.



1. Служба отправки транспорта почтовых ящиков использует RPC для получения исходящего сообщения из локальной базы данных почтовых ящиков.

2. Служба отправки транспорта почтовых ящиков использует ПРОТОКОЛ SMTP для отправки сообщения в транспортную службу на локальном сервере почтовых ящиков или на другом сервере почтовых ящиков.

3. В транспортной службе на сервере почтовых ящиков на сайте Active Directory с подпиской соединитель получения по умолчанию с именем "*Имя> сервера почтовых ящиков по умолчанию*<" принимает сообщение.

4. Сообщение отправляется на пограничный транспортный сервер с помощью неявного и невидимого соединителя отправки внутри организации, который автоматически отправляет почту между серверами Exchange в той же организации.

5. В транспортной службе на пограничном транспортном сервере соединитель получения по умолчанию с именем "*Имя> пограничного транспортного сервера внутреннего соединителя*< получения по умолчанию" принимает сообщение.

6. В транспортной службе на пограничном транспортном сервере соединитель отправки по умолчанию с именем "EdgeSync — *<имя> сайта Active Directory* в Интернет" отправляет сообщение в Интернет.

Общие сведения о службе транспорта на серверах почтовых ящиков

Каждое сообщение, отправленное или полученное в Exchange Server организации, должно быть классифицировано в транспортной службе на сервере почтовых ящиков, прежде чем его можно будет перенаправить и доставить. После классификации сообщения оно помещается в очередь доставки в целевую базу данных почтовых ящиков, группу доступности целевой базы данных (DAG), сайт Active Directory или лес Active Directory или в целевой домен за пределами организации.

Транспортная служба на сервере почтовых ящиков состоит из следующих компонентов и процессов.

- **Получение SMTP**: при получении сообщений транспортной службой выполняется проверка содержимого сообщений и проверка против спама, если включена. В сеансе SMTP имеется ряд событий, совместно работающих в определенном порядке для проверки содержимого сообщения перед его принятием. После того как сообщение полностью прошло через получение SMTP и не было отклонено событиями получения или агентом защиты от нежелательной почты, оно помещается в очередь отправки.

- **Отправка**. Отправка — это процесс помещения сообщений в очередь отправки. После этого классификатор берет по одному сообщению для классификации. Отправки осуществляются тремя способами:
  - От получателя SMTP через соединитель приема.
  - Через каталог раскладки или преобразования. Эти каталоги существуют на серверах почтовых ящиков и пограничных транспортных серверах. Файлы сообщений правильного формата, скопированные в каталог раскладки или в каталог преобразования, напрямую помещаются в очередь отправки.
  - Через агента транспорта.

- **Классификатор**. Классификатор за раз выбирает одно сообщение из очереди отправки. Классификатор выполняет следующие действия:

  - Разрешение получателей, включающее адресацию верхнего уровня, расширение группы рассылки и развертывание сообщения.

- Разрешение маршрутизации.
- Преобразование содержимого.

  Кроме того, применяются правила потока почты, определяемые организацией. После классификации сообщения помещаются в очередь доставки в зависимости от назначения сообщения. Сообщения помещаются в очередь целевой базой данных почтовых ящиков, daG, сайтом Active Directory, лесом Active Directory или внешним доменом.

- **Отправка SMTP**. Маршрутизация сообщений из службы транспорта зависит от расположения получателей сообщений относительно сервера почтовых ящиков, на котором была выполнена классификация. Сообщение может быть направлено в одно из указанных ниже расположений.
  - В службу доставки транспорта почтовых ящиков на том же сервере почтовых ящиков.
  - В службу доставки транспорта почтовых ящиков на другом сервере почтовых ящиков, который входит в ту же группу обеспечения доступности баз данных.
  - В транспортную службу на сервере почтовых ящиков в другой daG, на сайте Active Directory или в лесу Active Directory.
  - Для доставки в Интернет через:
    - соединитель отправки на том же сервере почтовых ящиков;
    - службу транспорта на другом сервере почтовых ящиков;
    - внешнюю службу транспорта на том же сервере почтовых ящиков или на другом сервере почтовых ящиков (если настроен исходящий прокси-сервер);
    - службу транспорта на пограничном транспортном сервере в сети периметра.

Общие сведения о службе транспорта на пограничных транспортных серверах

Компоненты транспортной службы на пограничных транспортных серверах не отличаются от компонентов транспортной службы на серверах почтовых ящиков. Однако отличаются действия, выполняемые на всех этапах обработки на пограничных транспортных серверах. Эти отличия описаны в приведенном ниже списке.

- **Получение SMTP**. Если пограничный транспортный сервер подписан на внутренний сайт Active Directory, соединитель получения по умолчанию с

именем "Имя> пограничного транспортного сервера по умолчанию<" автоматически настраивается для приема почты с внутренних серверов почтовых ящиков и из Интернета. Когда интернет-сообщения поступают на пограничный транспортный сервер, агенты защиты от спама фильтруют подключения и содержимое сообщений и помогают идентифицировать отправителя и получателя во время принятия сообщения в организацию. Агенты антиспамов устанавливаются и включены по умолчанию. Доступны дополнительные функции фильтрации вложений и подключений, но встроенной функция фильтрации вредоносных программ не существует. Кроме того, правила потока обработки почты (также известные как правила транспорта) управляются агентом правил Edge. По сравнению с агентом правил транспорта на серверах почтовых ящиков на пограничных транспортных серверах доступно только небольшое подмножество правил потока обработки почты. Но существуют уникальные действия правил потока обработки почты, связанные с SMTP-подключениями, которые доступны только на пограничных транспортных серверах.

- **Отправка**. На пограничном транспортном сервере сообщения обычно поступают в очередь отправки через соединитель получения. Однако также доступны каталоги раскладки и преобразования.

- **Классификатор**. На пограничном транспортном сервере классификация — это короткий процесс, в котором сообщение помещается непосредственно в очередь доставки для доставки внутренним или внешним получателям.

- **Отправка SMTP**. Когда пограничный транспортный сервер подписан на внутренний сайт Active Directory, автоматически создаются и настраиваются два соединителя отправки. Один с именем "EdgeSync — <имя> сайта Active Directory в Интернет" отвечает за отправку исходящей почты получателям Из Интернета, а другой с именем "EdgeSync — входящий <в Active Directory имя> сайта" отвечает за отправку входящей почты из Интернета внутренним получателям. Входящая почта отправляется в службу транспорта переднего плана на доступном сервере почтовых ящиков на сайте Active Directory с подпиской.

Регулярные выражения, используемые в правилах транспорта

Статья • 24.03.2023

Область применения: *Exchange Server 2013 г., Exchange Server 2016 г., Exchange Server 2019 г., Exchange Online*

Регулярные выражения можно использовать в предикатах правил транспорта Microsoft Exchange Server 2016 и 2019 для сопоставления текстовых шаблонов в разных частях сообщения (например, заголовки сообщений, отправитель, получатели, тема сообщения и текст). Предикаты используются в условиях и ограничениях для определения возможности применения настроенного действия к сообщению электронной почты.

> ⓘ **Примечание**
>
> Из-за отклонений в клиентских средах службы поддержки майкрософт (CSS) не могут участвовать в разработке или тестировании пользовательских скриптов регулярных выражений ("скрипты регулярных выражений"). Для разработки, тестирования и отладки пользовательских скриптов RegEX Office 365 клиентам потребуется использовать внутренние ИТ-ресурсы. Пользователи Office 365 могут также обратиться во внешнюю консультационную службу, такую как Microsoft Consulting Services (MCS). Независимо от ресурса разработки скриптов инженеры службы поддержки CSS EXO и EOP не могут помочь клиентам с пользовательскими запросами к скриптам RegEx.

Ищете задачи управления, связанные с правилами транспорта? См. раздел Управление правилами транспорта.

Содержание

Содержание

- Простые и регулярные выражения
- Регулярные выражения в Exchange Server 2016 и 2019
- Создание правила транспорта, использующего регулярное выражение

Простые и регулярные выражения

Чтобы разобраться с регулярными выражениями, необходимо начать с простых. Простое выражение — это определенное значение, которое необходимо найти в сообщении. Предикаты с помощью простых выражений находят определенные слова или строки. Примером простого выражения является название документа, который ваша организация не хочет распространять за пределами организации, например **Yearly Sales Forecast.doc**. Фрагмент данных в сообщении электронной почты должен точно соответствовать простому выражению для удовлетворения условия или исключения в правилах транспорта.

Регулярное выражение — это лаконичная и гибкая запись, предназначенная для обнаружения шаблонных элементов текста в сообщении. Эта запись выполняется с использованием двух базовых типов символов:

- **Литеральные символы**: текст, который должен существовать в целевой строке. Эти символы являются обычными символами, как типизированные.
- **Метачары**: один или несколько специальных символов, которые не интерпретируются буквально. Эти символы указывают, как текст может отличаться в целевой строке.

Регулярные выражения можно использовать для быстрого анализа сообщений электронной почты для поиска определенных текстовых шаблонов. Эти выражения позволяют обнаруживать сообщения с определенными типами содержимого, например номерами социального страхования (SSN), номерами патентов и номерами телефонов.

Такие данные нельзя логично сопоставить с простым выражением, так как в простом выражении требуется вводить каждый вариант нужного значения. Во многих случаях использование простых выражений для таких приложений становится сложной задачей, и сопоставление большого количества простых выражений в содержимом сообщения может быть ресурсоемким. Использование регулярных выражений является более эффективным. Вместо указания всех возможных вариантов можно настроить предикат правила транспорта на поиск текстовых шаблонов.

Регулярные выражения в Exchange Server 2016 и 2019

В командной консоли Exchange можно использовать регулярные выражения в любом предикате, который принимает свойство **предиката Patterns** . В консоли управления Exchange можно использовать регулярные выражения с любым условием или исключением, содержащим слова с текстовыми шаблонами. Дополнительные сведения о предикатах см. в разделе Transport Rule Predicates.

> ⚠ **Предупреждение**
>
> Необходимо тщательно протестировать создаваемые регулярные выражения, чтобы убедиться, что они дают ожидаемые результаты. Неправильное регулярное выражение может привести к неожиданным совпадениям и вызвать нежелательное поведение правила транспорта. Эти последствия могут привести к нежелательным действиям в отношении сообщений и содержимого сообщений, что может привести к потере данных при использовании таких действий, как отклонение или отказ сообщения. Кроме того, сложные регулярные выражения могут повлиять на производительность транспорта электронной почты. Регулярные выражения следует проверять в лабораторной среде до их внедрения в производство.

В следующей таблице перечислены строки шаблонов, которые можно использовать для создания регулярного выражения, соответствующего шаблону, в Exchange Server 2016 и 2019:

Строка шаблона	**Описание**
\S	Строка шаблона \S соответствует любому единичному символу, который не является пробелом.
\s	Строка шаблона \s соответствует единичному символу пробела.
\D	Строка шаблона \D соответствует любой цифре, которая не является числом.
\d	Строка шаблона \d соответствует любой одной цифре.
\w	Строка шаблона \w соответствует любому символу Юникода, классифицированным как буква или десятичная цифра.
\W	Строка шаблона \W соответствует любому символу Юникода, который не является буквой или цифрой.
*	Звездочка (*) соответствует отсутствию предыдущего символа или одному либо нескольким его вхождениям. Например, ab*c соответствует следующим строкам: ac, abc и abbbbc.
( )	Скобки выступают в роли группирующего разделителя. Например, a(bc)* соответствует следующим строкам: a, abc, abcbc, abcbcbc и так далее.

Строка шаблона	Описание
\	Обратная косая черта используется в качестве escape-символа перед специальным символом. Специальные символы — это символы, используемые в строках шаблона: обратная косая черта (\ ); Трубы; Звездочка (*); Открываемая скобка (( ); Закрывающая скобка ( )); Курсор (^); Знак доллара ($). Например, если требуется сопоставить строку, содержащую (525), введите (525).
^	Символ «крышка» (^) указывает, что следующая за этим символом строка шаблона должна располагаться в начале сопоставляемой текстовой строки. Например, ^fred@contoso соответствует и fred@contoso.co.ukalfred@contoso.comне соответствует fred@contoso.com .
$	Символ символа `$` доллара указывает, что предыдущая строка шаблона должна существовать в конце соответствующей текстовой строки. Например, contoso.com$ соответствует adam@contoso.com и kim@research.contoso.com, но не соответствует kim@contoso.com.au.

Создание регулярных выражений

С помощью предыдущей таблицы можно создать регулярное выражение, которое соответствует нужному шаблону данных. В порядке следования слева направо изучите отдельные символы или группы символов в данных, которые нужно сопоставить. Прочтите описание каждой из строк шаблона, чтобы определить, как он будет применяться к сопоставляемым данным. Затем определите, какая строка из приведенных в таблице соответствует данному символу или группе символов, и добавьте ее в регулярное выражение. По завершении этой работы будет получено полностью готовое регулярное выражение.

Например, данное регулярное выражение соответствует телефонным номерам в Северной Америке в форматах 425 555-0100 и 425.555.0100.

PowerShell

```
425(\s|.)\d\d\d(-|.)\d\d\d\d
```

Можно развернуть этот пример, добавив формат телефонного номера (425) 555-0100, в котором код региона заключен в скобки. В этом примере регулярное выражение соответствует всем трем форматам телефонных номеров.

\d\d\d((\s|.| -|)|) \s)\d\d\d(\s|.| -)\d\d\d\d

Разберем приведенный выше пример:

- **\d\d\d\d**: для этой части требуется, чтобы в первую очередь появились ровно три цифры.
- **((\s|.| -|)|) \s)**: для этой части требуется, чтобы после трехзначного числа существовал пробел, точка или дефис. Каждая строка сопоставления символов заключена в группирующие разделители и отделена вертикальной чертой. Это разделение означает, что в этом расположении в сопоставляемой строке может существовать только один из указанных символов внутри разделителей группирования. Для разделения между кодом области и следующими тремя цифрами он также ищет закрытую скобку или замкнутую скобку и пробел.
- **\d\d\d\d**: для этой части требуется, чтобы рядом отображалось ровно три числовые цифры.
- **(\s|.| -)**: для этой части требуется, чтобы после трехзначного числа существовал пробел, точка или дефис.
- **\d\d\d\d\d**: для этой части требуется, чтобы рядом появились ровно четыре числовые цифры.

Выше регулярного выражения располагаются следующие примеры значений:

- (425)555.0100
- 425 555 0100
- 425 555 0100
- (425) 555-0100
- 425-555-0100
- (425) 555-0100

Создание правила транспорта, использующего регулярное выражение

В этом примере создается правило транспорта в PowerShell, которое использует регулярные выражения для сопоставления имен SSN в теме сообщения электронной почты.

PowerShell

```
   New-TransportRule -Name "Social Security Number Block Rule" -
SubjectOrBodyMatchesPatterns '\d\d\d-\d\d-\d\d\d\d' -
RejectMessageEnhancedStatusCode "5.7.1" -RejectMessageReasonText "This
message has been rejected because of content restrictions"
```

В этом примере показано, как можно просмотреть новые правила транспорта.

PowerShell

```
Get-TransportRule "Social Security Number Block Rule" | Format-List
```

Обслуживаемые домены в Exchange Server

Статья • 04.04.2023

Обслуживаемые домены — это пространства имен SMTP (также известные как адресные пространства), которые вы настраиваете в организации Exchange для получения сообщений электронной почты. Например, если ваша компания зарегистрировала домен contoso.com и вы настроили запись обмена почтой (MX) в DNS через Интернет для contoso.com, необходимо настроить contoso.com в качестве принятого домена в организации Exchange для приема сообщений, адресованных @contoso.com получателям.

Обслуживаемые домены в Exchange 2016 и Exchange 2019 практически не изменились по сравнению с Exchange Server 2010 года и состоят из следующих типов:

- **Полномочные домены**. Получатели (в частности, почтовые ящики) настраиваются с адресами электронной почты в этих доменах. Организация Exchange принимает сообщения, адресованные получателям в этих доменах, и отвечает за создание отчетов о недоставке (также известных как недоставка или отказ сообщений) для несуществующих получателей.

- **Домены ретранслятора**. Организация Exchange принимает сообщения, адресованные получателям в доменах ретранслятора, но не отвечает за создание NDR для несуществующих получателей. Вместо этого Exchange (с дополнительной конфигурацией) передает сообщения на серверы обмена сообщениями, которые являются внешними для организации Exchange. Домены ретрансляции могут быть **внутренними** (для контролируемых вами доменов) или **внешними** (для доменов, которыми вы не управляете).

Обслуживаемый домен может быть отдельным доменом (contoso.com) или включать поддомены (*.contoso.com). Обслуживаемые домены — это глобальный параметр организации Exchange, и вы можете использовать несколько обслуживаемых доменов одного или разных типов.

Сведения о настройке принятых доменов см. в разделе Процедуры для принятых доменов в Exchange Server.

> ⓘ **Примечание**

Если в сети периметра существует подписанный пограничный транспортный сервер, можно настроить обслуживаемые домены на сервере почтовых ящиков в своей организации Exchange. Конфигурация обслуживаемых доменов реплицируется на пограничный транспортный сервер в процессе синхронизации EdgeSync. Дополнительную информацию см. в статье **Edge Subscriptions**.

Уполномоченные домены

Обслуживаемый домен настраивается как уполномоченный, если все получатели в нем есть в организации Exchange.

По умолчанию при установке первого сервера почтовых ящиков Exchange полное доменное имя (FQDN) корневого домена леса в Active Directory настраивается как уполномоченный домен. Если вы не хотите использовать этот домен для электронной почты, необходимо добавить другой уполномоченный домен. Инструкции см. в статье Создание обслуживаемых доменов.

В организации можно настроить несколько уполномоченных доменов. Домены электронной почты, используемые в организации, являются уполномоченными доменами. Вы можете использовать уполномоченные домены в политиках электронных адресов, а Exchange отвечает за создание отчетов о недоставке для несуществующих получателей в уполномоченных доменах.

Домены ретрансляции

Вы настраиваете принятый домен в качестве домена ретранслятора (также известного как неавторитетный домен), если в вашей организации Exchange существуют некоторые или нет получателей в этом домене (например, партнеры или дочерние компании). Exchange не отвечает за создание NDR для несуществующих получателей в домене ретрансляции. Вместо этого соединитель отправки настраивается на использование диапазона адресов домена ретрансляции и маршрутизацию через промежуточный узел для ретрансляции сообщений в место назначения (непосредственной или до следующего прыжка). Дополнительные сведения о создании соединителей отправки, использующих маршрутизацию через промежуточный узел, см. в статье Create a Send connector to route outbound mail through a smart host.

Домен ретрансляции можно настроить в качестве домена внутренней или внешней ретрансляции. Различия между ними описаны в приведенном ниже списке.

- **Домены внутренней ретрансляции**
  - Некоторых получателей в домене внутренней ретрансляции нет в организации Exchange. Ниже представлены примеры.
    - Домен совместно используется организацией Exchange и сторонней системой обмена сообщениями.
    - Домен совместно используется несколькими организациями Exchange из разных лесов Active Directory.
  - Получатели в домене внутренней ретрансляции могут быть представлены как почтовые контакты или почтовые пользователи в организации Exchange (созданные вручную или автоматически, путем синхронизации службы каталогов).
  - Соединитель отправки, настраиваемый для домена внутренней ретрансляции, находится на внутреннем сервере почтовых ящиков.

    Примечание. По умолчанию вы не можете настроить соединитель отправки для домен внутренней ретрансляции на подписанном пограничном транспортном сервере. Сообщения, отправляемые получателям в домен внутренней ретрансляции, автоматически перенаправляются на внутренние серверы почтовых ящиков на сайте Active Directory с подпиской с помощью соединителя отправки по умолчанию EdgeSync — inbound to <*Active Directory site name*>. Этот соединитель отправки автоматически настраивается для маршрутизации почты для всех полномочных доменов и внутренних доменов ретранслятора (значение адресного пространства равно `--`). Дополнительные сведения см. в статье Отправка соединителей, автоматически созданных подпиской Edge.
  - Вы можете использовать домены внутренней ретрансляции в политиках электронных адресов.
- **Домены внешней ретрансляции**
  - Ни один получатель в домене внешней ретрансляции не существует в организации Exchange (включая почтовые контакты и почтовых пользователей). Например, ваша организация Exchange является центральным местом для приема электронной почты в Интернете для группы отдельных организаций.

- Соединитель отправки, настраиваемый для домена внешней ретрансляции, находится на пограничном транспортном сервере или сервере почтовых ящиков с выходом в Интернет.
- В политиках электронных адресов невозможно использовать домены внешней ретрансляции.

Обслуживаемые домены и политики электронных адресов

Политики электронных адресов назначают электронные адреса получателям. Чтобы использовать домен внутренней ретрансляции или уполномоченный домен в политике электронных адресов, необходимо добавить его. Дополнительные сведения о политиках адресов электронной почты см. в разделе политики адресов Email в Exchange Server.

Поиск получателей в обслуживаемых доменах

Фильтрация получателей на подписанном пограничном транспортном сервере может блокировать сообщения, адресованные несуществующим получателям в организации Exchange. Эта функция называется *поиском получателей*. Дополнительные сведения о фильтрации получателей см. в разделе Фильтрация получателей на пограничных транспортных серверах.

Вы можете включить или отключить поиск получателей для принятого домена с помощью параметра *AddressBookEnabled* командлета **Set-AcceptedDomain** . В приведенной ниже таблице указаны значения по умолчанию для каждого типа обслуживаемых доменов.

Тип обслуживаемых доменов	**Значение по умолчанию для поиска получателей (параметр *AddressBookEnabled*)**	**Comments**
Уполномоченный домен	Включено (`$true`)	Все получатели в уполномоченном домене существуют в организации Exchange, поэтому поиск получателей для домена включен по умолчанию.

Тип обслуживаемых доменов	Значение по умолчанию для поиска получателей (параметр ***AddressBookEnabled***)	Comments
Домен внутренней ретрансляции	Отключено (`$false`)	Если все получатели в домене внутренней ретрансляции существуют в организации Exchange (включая почтовые контакты и почтовых пользователей), вы можете включить поиск получателей для домена. Если не все получатели в домене внутренней ретрансляции существуют в организации Exchange, то для домена не следует включать поиск получателей.
Домен внешней ретрансляции	Отключено (`$false`)	Получателей в уполномоченном домене нет в организации Exchange, поэтому для домена не следует включать поиск получателей.

Инструкции по настройке см. в статье Изменение обслуживаемых доменов.

Домен по умолчанию

FQDN корневого домена леса автоматически настраивается в качестве первого обслуживаемого домена в организации, поэтому он также указывается как *домен по умолчанию*. Однако после добавления других обслуживаемых доменов вы можете сделать один из них доменом по умолчанию. Ниже перечислены некоторые особенности домена по умолчанию.

- Домен по умолчанию невозможно удалить. Для использования по умолчанию можно настроить другой обслуживаемый домен (один из обслуживаемых доменов всегда настраивается как домен по умолчанию).
- Домен по умолчанию используется во внешнем адресе postmaster: `postmaster@<default domain>`.
- Домен по умолчанию используется в инкапсулированных электронных адресах, к которым не применяется протокол SMTP (метод Internet Mail Connector Encapsulated Address, или IMCEA).
- Первый домен по умолчанию используется в качестве основного адреса всех получателей в заданной по умолчанию политике электронных адресов. Если задать другой обслуживаемый домен для использования по умолчанию, то стандартная политика электронных адресов не обновится автоматически.

- Вы можете настроить любой обслуживаемый домен для использования по умолчанию, но обычно указывается уполномоченный домен.

Процедуры для принятых доменов в Exchange Server

Статья • 04.04.2023

Обслуживаемые домены — это пространства имен SMTP (также известные как адресные пространства), которые можно настроить в организации Exchange, чтобы получать сообщения электронной почты. Для настройки обслуживаемых доменов в Exchange Server используется Центр администрирования Exchange (EAC) или командная консоль Exchange.

Дополнительные сведения о принятых доменах см. в разделе Принятые домены в Exchange Server. В следующем списке перечислены типы обслуживаемых доменов:

- **Заслуживающие доверия домены**
  - Все получатели в заслуживающем доверия домене существуют в организации Exchange.
  - Exchange отвечает за создание отчетов о недоставке (также известных как сообщения возврата) для несуществующих получателей в заслуживающем доверия домене.
- **Домены внутренней ретрансляции**
  - Некоторые получатели в домене внутренней ретрансляции могут существовать в организации Exchange.
  - Exchange не отвечает за создание отчетов о недоставке для несуществующих получателей в домене внутренней ретрансляции. Вместо этого необходимо создать соединитель отправки с адресным пространством домена внутренней ретрансляции. В качестве источника для такого соединителя отправки используется внутренний сервер почтовых ящиков, чтобы ретранслировать сообщения для несуществующих получателей в домене.
- **Домены внешней ретрансляции**
  - Ни один получатель в домене внешней ретрансляции не существует в организации Exchange.
  - Exchange не отвечает за создание отчетов о недоставке для несуществующих получателей в домене внешней ретрансляции. Вместо этого необходимо создать соединитель отправки с адресным

пространством домена внешней ретрансляции. В качестве источника для такого соединителя отправки используется пограничный транспортный сервер, чтобы ретранслировать сообщения для всех получателей в домене.

Что нужно знать перед началом работы

- Предполагаемое время для выполнения каждой процедуры составляет 5 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Принятые домены" в разделе Разрешения потока обработки почты и в записи "политики Email адресов" в разделе Разрешения получателей.
- Если в сети периметра существует подписанный пограничный транспортный сервер, можно настроить обслуживаемые домены на сервере почтовых ящиков в своей организации Exchange. Конфигурация обслуживаемых доменов реплицируется на пограничный транспортный сервер в процессе синхронизации EdgeSync. Дополнительную информацию см. в статье Edge Subscriptions.
- Если Exchange принимает почту из Интернета для получателей в обслуживаемом домене, необходимо настроить запись MX для домена на общедоступных DNS-серверах (с выходом в Интернет). Каждая запись MX должна указывать на сервер с выходом в Интернет, который получает электронную почту для организации.
- Необходимо создать соединитель отправки, чтобы направлять почту для несуществующих получателей в доменах внутренней или внешней ретрансляции. Дополнительные сведения см. в статье Create a Send connector to route outbound mail through a smart host.
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online**

или **Exchange Online Protection**.

Создание обслуживаемых доменов

Создав обслуживаемый домен, вы не можете изменить его значение (например, с contoso.com на *.contoso.com или наоборот).

Создание обслуживаемых доменов с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел **Поток**> обработки**почты Принятые домены** и нажмите кнопку **Добавить** (➕

2. В открывшемся окне **Новый обслуживаемый домен** настройте следующие параметры:

   - **Имя**. Введите уникальное описательное имя.
   - **Обслуживаемый домен**. Введите один домен (например, contoso.com) или домен с поддоменами (например, *.contoso.com).
   - **Этот домен:** выберите **Полномочный**, **Внутренний ретранслятор** или **Внешний ретранслятор**.

   По завершении нажмите кнопку **Сохранить**.

Создание обслуживаемых доменов с помощью командной консоли Exchange

Чтобы создать обслуживаемый домен, используйте указанный ниже синтаксис.

PowerShell

```
New-AcceptedDomain -Name <Name> -DomainName <DomainOrDomainWithSubdomains> -
DomainType <Authoritative | InternalRelay | ExternalRelay>
```

В этом примере создается заслуживающий доверия домен корпорации Contoso для адреса contoso.com.

PowerShell

```
New-AcceptedDomain -Name "Contoso Corp" -DomainName contoso.com
```

Примечание. Нам не нужно использовать параметр *DomainType* , так как по умолчанию используется `Authoritative` значение .

Подробные сведения о синтаксисе и параметрах см. в разделе New-AcceptedDomain.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли создан обслуживаемый домен, следуйте одной из перечисленных процедур:

- В EAC перейдите в раздел **Поток**> обработки**почты Принятые домены**, убедитесь, что в списке указан обслуживаемый домен и указаны правильные сведения.
- В командной консоли Exchange выполните следующую команду, чтобы проверить значения свойств:

```
PowerShell

Get-AcceptedDomain | Format-Table -Auto
Name,DomainName,DomainType,Default,AddressBookEnabled
```

Изменение обслуживаемых доменов

- Вы можете только *заменить* домен по умолчанию на новый домен по умолчанию (один обслуживаемый домен всегда настраивается как домен по умолчанию). Дополнительные сведения см. в разделе, посвященном домену по умолчанию.
- Вы можете включить и отключить поиск получателей для принятого домена только в командной консоли Exchange. Дополнительные сведения см. в разделе Подстановка получателей в обслуживаемых доменах.

Использование Центра администрирования Exchange для изменения обслуживаемых доменов

1. В EAC перейдите в раздел **Поток**> обработки**почты Принятые домены**, выберите в списке обслуживаемый домен и нажмите кнопку **Изменить** (✎
2. В открывшемся окне свойств можно настроить следующие параметры:

- **Имя**
- **Это домен**: "Полномочный", "Внутренний ретранслятор" или "Внешний ретранслятор".
- **Сделайте этот домен доменом по умолчанию**. Если флажок снят, установите его, чтобы настроить обслуживаемый домен в качестве домена по умолчанию.

По завершении нажмите кнопку **Сохранить**.

Использование командной консоли Exchange для изменения обслуживаемых доменов

Чтобы изменить обслуживаемый домен, используйте приведенный ниже синтаксис.

PowerShell

```
Set-AcceptedDomain -Identity <AcceptedDomainIdentity> [-Name <Name>]  [-
DomainType <Authoritative | InternalRelay | ExternalRelay>] [-
AddressBookEnabled <$true | $false>] [-MakeDefault $true]
```

В этом примере описана настройка заслуживающего доверия домена корпорации Contoso в качестве домена по умолчанию.

PowerShell

```
Set-AcceptedDomain -Identity "Contoso Corp" -MakeDefault $true
```

В примере ниже описано включение просмотра получателей на пограничном транспортном сервере для домена внутренней ретрансляции корпорации Fabrikam. Все внешние получатели в домене fabrikam.com представлены в качестве получателей почты Exchange.

PowerShell

```
Set-AcceptedDomain -Identity "Fabrikam Corp" -AddressBookEnabled $true
```

Подробные сведения о синтаксисе и параметрах см. в разделе Set-AcceptedDomain.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли изменен обслуживаемый домен, следуйте одной из перечисленных процедур:

- В EAC перейдите в раздел **Поток**> обработки**почты Принятые домены** и проверьте значения свойств.

  Примечания.

  - Чтобы убедиться, что принятый домен является доменом по умолчанию, необходимо выбрать обслуживаемый домен в списке, а затем нажать кнопку **Изменить** (✎ Этот домен задан по умолчанию, если установлен флажок **Сделать доменом по умолчанию**.
  - В Центре администрирования Exchange нельзя проверить, включен или выключен просмотр получателей для обслуживаемого домена. Для этого нужна Командная консоль Exchange.

- В командной консоли Exchange выполните следующую команду, чтобы проверить значения свойств:

```
PowerShell

Get-AcceptedDomain | Format-Table -Auto
Name,DomainName,DomainType,Default,AddressBookEnabled
```

Удаление обслуживаемых доменов

- Невозможно удалить домен по умолчанию. Сначала необходимо настроить в качестве домена по умолчанию другой обслуживаемый домен.

- Вам не удастся удалить обслуживаемый домен, указанный в политике адресов электронной почты (в том числе в отключенных шаблонах адресов электронной почты). Чтобы просмотреть все домены, используемые в политиках адресов электронной почты, выполните в командной консоли Exchange следующую команду:

```
PowerShell

Get-EmailAddressPolicy | Format-List Name,*EmailAddressTemplate*
```

  Дополнительные сведения об изменении политик адресов электронной почты см. в разделе Изменение политик адресов электронной почты[Изменение политик адресов электронной почты]).

Использование Центра администрирования Exchange для удаления обслуживаемых доменов

1. В EAC перейдите в раздел **Поток**> обработки**почты Принятые домены**, выберите в списке обслуживаемый домен и нажмите кнопку **Удалить** (━).
2. В появившемся диалоговом окне **Предупреждение** выберите **Да** для подтверждения.

Использование командной консоли Exchange для удаления обслуживаемых доменов

Чтобы удалить обслуживаемый домен, используйте приведенный ниже синтаксис.

```
PowerShell

Remove-AcceptedDomain -Identity <AcceptedDomainIdentity>
```

В этом примере показано, как удалить обслуживаемый домен корпорации Fabrikam.

```
PowerShell

Remove-AcceptedDomain -Identity "Fabrikam Corp"
```

Дополнительные сведения о синтаксисе и параметрах см. в статье remove-AcceptedDomain.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли удален обслуживаемый домен, следуйте одной из перечисленных процедур:

- В EAC перейдите в раздел **Поток**> обработки**почты Принятые домены** и убедитесь, что обслуживаемый домен больше не указан.
- Чтобы убедиться, что обслуживаемый домен не указан в списке, в командной консоли Exchange выполните следующую команду:

  ```
  PowerShell

  Get-AcceptedDomain
  ```

Настройка Exchange для приема почты для нескольких доменов, заслуживающих доверия

Ниже приведены некоторые сценарии, для которых требуется несколько заслуживающих доверия доменов:

- Ваша организация меняет свое имя домена SMTP.
- Вам необходимо назначить разные адреса электронной почты для различных подразделений вашей организации.
- Вы предоставляете услуги по размещению электронной почты и вам необходимо получать электронную почту для нескольких доменных имен SMTP.

После настройки одного или нескольких заслуживающих доверия доменов вам необходимо решить, как использовать эти домены в вашей организации. Например:

- Вы хотите заменить существующий основной (**Reply-To:**) адрес для получателей или добавить новый адрес электронной почты в качестве прокси-адреса?
- Вы хотите сохранить в качестве прокси-адресов старые адреса электронной почты, чтобы получатели могли по-прежнему получать отправленную на них почту?
- Вы хотите, чтобы адреса электронной почты в новом заслуживающем доверия домене применялись ко всем получателям и их типам? Или же эти адреса должны применяться к определенным типам получателей или конкретным получателям в зависимости от их свойств (например, только к пользователям в отделе финансов)?

Ниже описаны действия, необходимые, чтобы настроить Exchange для получения почты на несколько заслуживающих доверия доменов.

1. Создайте один или несколько заслуживающих доверия доменов, как описано в разделе Создание обслуживаемых доменов.

   Например, если вы уже настроили contoso.com в качестве заслуживающего доверия домена, добавьте в качестве такого же домена fourthcoffee.com.

2. Создайте или измените политику адресов электронной почты, в которой используются заслуживающие доверия домены, в соответствии с вашими потребностями. Пример

   - Измените политику адресов электронной почты по умолчанию, чтобы у всех получателей были необходимые основной и прокси-адрес электронной почты.

   Например, измените политику по умолчанию, чтобы *<псевдоним>*@fourthcoffee.com был основным SMTP-адресом электронной *почты>*, *а< псевдоним*@contoso.com хранится в качестве прокси-адреса. Инструкции см. в статье Изменение политик адресов электронной почты.

   - Создайте политику адресов электронной почты, в соответствии с которой основной и прокси-адрес электронной почты применяются для отфильтрованного набора получателей.

   Например, создайте политику под именем «Получатели Fourth Coffee», используя указанные параметры:

   - **Предустановленный фильтр получателей**: все пользователи с почтовыми ящиками, где значение **Company** — Fourth Coffee.
   - **Основной SMTP-адрес электронной почты**: <*alias*>@fourthcoffee.com.
   - **Дополнительные адреса электронной почты прокси-сервера**: нет. Затронутые получатели больше не могут получать сообщения, отправляемые на свой старый @contoso.com основной адрес электронной почты.
   - **Приоритет**: 1. Первая политика адресов электронной почты, в которой определяется получатель, настраивает адреса электронной почты получателя. Все остальные политики игнорируются, даже если первая политика не применяется и не может настраивать электронные адреса получателя.

     Инструкции см. в статье Создание политик адресов электронной почты.

3. Примените новую или обновленную политику адресов электронной почты к получателям, которых это касается. Инструкции см. в статье Применение политик адресов электронной почты к получателям.

Чтобы убедиться, что служба Exchange настроена для получения почты на несколько заслуживающих доверия доменов, следуйте указанным ниже процедурам.

1. Отправьте тестовые сообщения получателю, которого это касается, из почтового ящика за пределами организации Exchange и просмотрите, какие адреса электронной почты принимают или отклоняют сообщения.

2. Отправьте тестовые сообщения из соответствующего почтового внешнему получателю и проверьте адрес отправителя в сообщении.

Соединители на серверах Exchange

Статья • 04.04.2023

Exchange использует соединители для включения потока обработки входящей и исходящей почты на серверах Exchange, а также между службами в транспортном конвейере на локальном сервере Exchange.

Ниже приведены типы соединителей, доступных в Exchange.

Connector	**Описание**
Соединители получения	Соединители получения управляют потоком входящей почты SMTP. Они ожидают входящие подключения, которые соответствуют конфигурации соединителя. При установке Exchange по умолчанию создается множество соединителей получения. Подробнее см. в статье Соединители получения.
Соединители отправки	Соединители отправки управляют потоком исходящей почты SMTP. Соединитель отправки выбирается в зависимости от получателей сообщений и конфигурации соединителя. Для потока обработки внешней почты по умолчанию не создаются соединители отправки при установке Exchange, но неявные и невидимые соединители отправки существуют и используются для маршрутизации почты между внутренними серверами Exchange. Дополнительные сведения см. в разделе Отправка соединителей.
Агенты доставки и соединители агентов доставки	Агенты доставки и их соединители управляют потоком обработки исходящей почты, которая направляется в системы, не использующие протокол SMTP. Исходящие сообщения помещаются в очереди для доставки в систему, не использующую протокол SMTP. Службы доставки и их соединители предпочтительнее, чем внешние соединители, из-за более удобного управления и более высокой производительности. Дополнительные сведения см. в разделе Агенты доставки и соединители агентов доставки.
Внешние соединители	Внешние соединители управляют потоком обработки исходящей почты, которая направляется в системы, не использующие протокол SMTP. Исходящие сообщения записываются в файлы в расположении, которое называется транзитным каталогом, а потом передаются в систему, не использующую протокол SMTP. Дополнительные сведения см. в разделе Внешние соединители.

Получение соединителей в Exchange Server

Статья • 04.04.2023

Серверы Exchange используют соединители получения для управления входящими SMTP-подключениями из:

- от серверов обмена сообщениями, не входящих в организацию Exchange;
- служб в транспортном конвейере на локальном сервере Exchange Server или удаленных серверах Exchange Server;
- почтовых клиентов, которым необходимо использовать для отправки сообщений протокол SMTP с проверкой подлинности.

Соединители получения можно создавать в службе транспорта на серверах почтовых ящиков, во внешней службе транспорта на серверах почтовых ящиков, а также на пограничных транспортных серверах. По умолчанию соединители получения, необходимые для входящего потока почты, создаются автоматически при установке сервера почтовых ящиков Exchange и при подписке на пограничный транспортный сервер в организации Exchange.

Соединитель получения связан с сервером почтовых ящиков или пограничным транспортным сервером, на котором он создан, и определяет, как этот сервер прослушивает SMTP-подключения. На серверах почтовых ящиков соединитель получения хранится в Active Directory как дочерний объект сервера. На пограничных транспортных серверах соединитель получения хранится в службах Active Directory облегченного доступа к каталогу (AD LDS).

Ниже перечислены важные параметры соединителей получения.

- **Привязки локальных адаптеров**. Настройте сочетание локальных IP-адресов и TCP-портов, которые соединитель получения использует для приема подключений.
- **Параметры удаленной сети**. Настройте исходные IP-адреса, которые соединитель получения прослушивает для подключений.
- **Тип использования**. Настройте группы разрешений по умолчанию и механизмы проверки подлинности интеллектуальных узлов для соединителя получения.
- **Группы разрешений**. Настройте, кому разрешено использовать соединитель получения, и разрешения, которые они получают.

Каждый соединитель получения ищет входящие подключения, соответствующие параметрам конфигурации этого соединителя. Каждый соединитель получения на сервере Exchange Server использует уникальное сочетание привязок локальных IP-адресов, TCP-портов и диапазонов удаленных IP-адресов, определяющих, будут ли приниматься подключения от клиентов и серверов SMTP и каким образом это будет происходить.

В большинстве случаев достаточно заданных по умолчанию соединителей получения, но вы можете создавать собственные соединители получения для определенных сценариев. Например, вы можете:

- применять специальные свойства к источнику электронной почты, например увеличивать максимальный размер сообщения, количество получателей на сообщение или количество одновременных входящих подключений;
- принимать зашифрованные сообщения с помощью определенного сертификата TLS.

На серверах почтовых ящиков вы можете создавать соединители получения и управлять ими с помощью Центра администрирования Exchange (EAC) или командной консоли Exchange. На пограничных транспортных серверах доступна только командная консоль Exchange.

Получение изменений соединителя в Exchange Server

Ниже приведены важные изменения в соединителях получения в Exchange 2016 и Exchange 2019 по сравнению с Exchange 2010:

- Параметр *TlsCertificateName* позволяет указать издателя сертификата и субъекта сертификата. Это помогает защититься от поддельных сертификатов.
- Параметр *TransportRole* позволяет различать внешние (клиентский доступ) и внутренние соединители на серверах почтовых ящиков.

Соединители приема по умолчанию, созданные во время установки

По умолчанию при установке Exchange создается несколько разных соединителей получения. По умолчанию эти соединители включены, а ведение журнала протоколов для большинства из них отключено. Дополнительные сведения о ведении журнала протокола в соединителях получения см. в разделе Ведение журнала протоколов.

Соединители получения по умолчанию во внешней службе транспорта на серверах почтовых ящиков

Основная функция соединителей получения во внешней службе транспорта — принимать анонимные и проверенные SMTP-подключения в организацию Exchange. Значение свойства **TransportRole** для этих соединителей — `FrontendTransport`. Служба внешнего транспорта ретранслирует или *прокси-серверы* этих подключений к транспортной службе для классификации и маршрутизации в конечное место назначения.

В приведенной ниже таблице представлены соединители получения по умолчанию, создаваемые во внешней службе транспорта на серверах почтовых ящиков.

Имя	Описание	Ведение журнала протокола	TCP-порт	Привязки к локальным IP-адресам	Диапазоны удаленных IP-адресов	Механизмы проверки подлинности	Группы разрешений
Имя внешнего *<сервера>* клиента	Принимает подключения от клиентов SMTP, прошедших проверку подлинности.	Нет	587	Все доступные адреса IPv4 и IPv6 (`0.0.0.0` и `[::]:`)	`{::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff, 0.0.0.0-255.255.255.255}` (все IPv4- и IPv6-адреса)	`TLS` `BasicAuth` `BasicAuthRequireTLS` `Integrated`	`ExchangeUsers`
Имя внешнего *<сервера>* по умолчанию	Принимает анонимные подключения от внешних серверов SMTP. Это распространенная точка входа сообщений в организацию Exchange.	Подробное	25	Все доступные адреса IPv4 и IPv6 (`0.0.0.0` и `[::]:`)	`{::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff, 0.0.0.0-255.255.255.255}` (все IPv4- и IPv6-адреса)	`TLS` `BasicAuth` `BasicAuthRequireTLS` `ExchangeServer` `Integrated`	`AnonymousUsers` `ExchangeLegacyServers` `ExchangeServers`
Исходящий прокси-сервер внешнего *сервера<>*	Принимает проверенные подключения от службы транспорта на серверах почтовых ящиков. Для шифрования подключений используется самозаверяющий сертификат сервера Exchange Server. Этот соединитель используется только в том случае, если соединитель отправки настроен для использования исходящего прокси-сервера. Дополнительные сведения см. в статье Configure Send connectors to proxy outbound mail.	Нет	717	Все доступные адреса IPv4 и IPv6 (`0.0.0.0` и `[::]:`)	`{::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff, 0.0.0.0-255.255.255.255}` (все IPv4- и IPv6-адреса)	`TLS` `BasicAuth` `BasicAuthRequireTLS` `ExchangeServer` `Integrated`	`ExchangeServers`

Соединители получения по умолчанию в службе транспорта на серверах почтовых ящиков

Основная функция соединителей получения в службе транспорта — принимать проверенные и зашифрованные SMTP-подключения от других служб транспорта на локальном сервере почтовых ящиков или удаленных серверах почтовых ящиков в

организации. Значение свойства **TransportRole** в этих соединителях равно `HubTransport`. Клиенты не подключаются к таким соединителям напрямую.

В приведенной ниже таблице представлены соединители получения по умолчанию, создаваемые в службе транспорта на серверах почтовых ящиков.

Имя	Описание	Ведение журнала протокола	TCP-порт	Привязки к локальным IP-адресам	Диапазоны удаленных IP-адресов	Механизмы проверки подлинности	Группы разрешен
Имя *прокси-сервера< >* клиента	Принимает проверенные клиентские подключения, переданные через прокси-сервер из внешней службы транспорта.	Нет	465	Все доступные адреса IPv4 и IPv6 (`0.0.0.0` и `[::]:`)	`{::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff, 0.0.0.0-255.255.255.255}` (все IPv4- и IPv6-адреса)	`TLS` `BasicAuth` `BasicAuthRequireTLS` `ExchangeServer` `Integrated`	`ExchangeServers` `ExchangeUsers`
Имя *сервера> по умолчанию<*	Принимает проверенные подключения: • от внешней службы транспорта на локальных или удаленных серверах почтовых ящиков; • службы транспорта на удаленных серверах почтовых ящиков; • службы транспорта почтовых ящиков на локальных или удаленных серверах почтовых ящиков. • Пограничные транспортные серверы Для шифрования подключений используется самозаверяющий сертификат сервера Exchange Server.	Нет	2525	Все доступные адреса IPv4 и IPv6 (`0.0.0.0` и `[::]:`)	`{::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff, 0.0.0.0-255.255.255.255}` (все IPv4- и IPv6-адреса)	`TLS` `BasicAuth` `ExchangeServer` `Integrated`	`ExchangeLegacyServ` `ExchangeServers` `ExchangeUsers`

Соединители получения по умолчанию в службе транспорта на пограничных транспортных серверах

Основная функция соединителя получения на пограничных транспортных серверах — принимать почту из Интернета. При подписке на пограничный транспортный сервер в организацию Exchange автоматически настраиваются разрешения соединителя и механизмы проверки подлинности, необходимые для передачи почты через Интернет в вашу организацию и из нее. Дополнительные сведения см. в разделе Пограничные транспортные серверы.

В приведенной ниже таблице представлен соединитель получения по умолчанию, создаваемый в службе транспорта на пограничных транспортных серверах.

Имя	Описание	Ведение журнала протокола	TCP-порт	Привязки к локальным IP-адресам	Диапазоны удаленных IP-адресов	Механизмы проверки подлинности	Группы разрешений
Имя *сервера*> *внутреннего соединителя*< получения по умолчанию	Принимает анонимные подключения от внешних серверов SMTP.	Нет	25	Все доступные IPv4-адреса (`0.0.0.0`)	`{0.0.0.0-255.255.255.255}` (все IPv4-адреса)	`TLS` `ExchangeServer`	`AnonymousUsers` `ExchangeServers` `Partners`

Скрытые соединители получения в службе доставки транспорта почтовых ящиков на серверах почтовых ящиков

Помимо соединителей получения, создаваемых во время установки серверов Exchange, в службе доставки транспорта почтовых ящиков на серверах почтовых ящиков есть специальный *неявный соединитель получения* . Этот скрытый соединитель получения автоматически доступен, не виден и не требует управления. Основная функция этого соединителя — принимать почту из службы транспорта на локальном сервере почтовых ящиков или удаленных серверах почтовых ящиков в организации.

В приведенной ниже таблице описывается скрытый соединитель получения, который находится в службе доставки транспорта почтовых ящиков на серверах почтовых ящиков.

Имя	Описание	Ведение журнала протокола	TCP-порт	Привязки к локальным IP-адресам	Диапазоны удаленных IP-адресов	Механизмы проверки подлинности	Группы разрешений
Соединитель получения для доставки почты в почтовые ящики	Принимает проверенные подключения от службы транспорта на локальных или удаленных серверах почтовых ящиков.	Нет	475	Все доступные адреса IPv4 и IPv6 (`0.0.0.0` и `[::]:`)	`{::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff, 0.0.0.0-255.255.255.255}` (все IPv4- и IPv6-адреса)	`ExchangeServer`	`ExchangeServers`

Привязки локальных адресов для соединителей получения

Привязки локальных адресов ограничивают соединитель получения для прослушивания SMTP-подключений по определенному локальному IP-адресу (сетевому адаптеру) и TCP-порту. Как правило, сочетание локального IP-адреса и TCP-порта является уникальным для каждого соединителя получения на сервере. Однако несколько соединителей получения на сервере могут иметь одни и те же локальные IP-адреса и TCP-порты, если диапазоны удаленных IP-адресов отличаются. Дополнительные сведения см. в разделе Удаленные адреса соединителя получения .

По умолчанию соединитель получения прослушивает подключения по всем доступным локальным адресам IPv4 и IPv6 (`0.0.0.0` и `[::]:`). Если на сервере несколько сетевых адаптеров, вы можете настроить соединители получения так, чтобы они принимали подключения только с тех IP-адресов, которые указаны для определенного сетевого адаптера. Например, на сервере Exchange Server с доступом к Интернету можно настроить соединитель получения, привязанный к IP-адресу внешнего сетевого адаптера, для прослушивания анонимных подключений к Интернету. У вас может быть отдельный соединитель получения, привязанный к IP-адресу внутреннего сетевого адаптера, для прослушивания проверенных подключений со внутренних серверов Exchange Server.

> ⓘ **Примечание**
>
> Привязывая соединитель получения к определенному IP-адресу, убедитесь, что этот адрес настроен на локальном сетевом адаптере. Если указать недействительный локальный IP-адрес, служба транспорта Microsoft Exchange может не запуститься при перезагрузке сервера или перезапуске службы.

В Центре администрирования Exchange вы можете настроить привязки локальных адресов в поле **Привязки сетевого адаптера** мастера создания соединителей получения или на вкладке **Определение области** в свойствах имеющихся соединителей получения. В командной консоли Exchange параметр *Bindings* используется в командлетах **New-ReceiveConnector** и **Set-ReceiveConnector** . В зависимости от выбранного типа использования, у вас может отсутствовать возможность настраивать привязки локальных адресов при создании соединителя получения, но вы можете изменить эти привязки после его создания. Соответствующие типы использования определены в разделе Типы использования соединителей получения.

Удаленные адреса соединителей получения

Удаленные адреса определяют, откуда соединитель получения принимает SMTP-подключения. По умолчанию соединители получения прослушивают подключения со всех IPv4- и IPv6-адресов (0.0.0.0-255.255.255.255 и ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff). Создавая пользовательский соединитель получения, чтобы принимать почту из определенного источника, настройте его на прослушивание подключений только от определенного IP-адреса или диапазона адресов.

Допустимо пересечение диапазонов удаленных IP-адресов для нескольких соединителей получения на сервере при условии, что такое пересечение является полным. Когда диапазоны удаленных IP-адресов пересекаются, используется тот диапазон, который содержит наиболее точное совпадение с IP-адресом подключающегося сервера.

Например, рассмотрим следующие соединители получения во внешней службе транспорта на сервере Exchange01:

- **Имя соединителя**: клиентский интерфейс Exchange01
  - **Привязки сетевых адаптеров**: все доступные IPv4 через порт 25.
  - **Параметры удаленной сети**: 0.0.0.0-255.255.255.255.255
- **Имя соединителя**: Настраиваемый соединитель A
  - **Привязки сетевых адаптеров**: все доступные IPv4 через порт 25.
  - **Параметры удаленной сети**: 192.168.1.0-192.168.1.255
- **Имя соединителя**: Пользовательский соединитель B
  - **Привязки сетевых адаптеров**: все доступные IPv4 через порт 25.
  - **Параметры удаленной сети**: 192.168.1.75

SMTP-подключения с адреса 192.168.1.75 принимает "Пользовательский соединитель Б", так как его совпадение с IP-адресом наиболее точное.

SMTP-подключения с адреса 192.168.1.100 принимает "Пользовательский соединитель А", так как его совпадение с IP-адресом наиболее точное.

В Центре администрирования Exchange вы можете настроить удаленные IP-адреса в поле **Настройки удаленной сети** мастера создания соединителя получения или на вкладке **Определение области** в свойствах имеющихся соединителей получения. В командной консоли Exchange параметр *RemoteIPRanges* используется в командлетах **New-ReceiveConnector** и **Set-ReceiveConnector** .

Типы использования соединителей получения

Тип использования определяет параметры безопасности по умолчанию для этого соединителя получения. Тип использования указывает, кому разрешено использовать соединитель, какие разрешения получают эти пользователи и какие способы проверки подлинности поддерживаются.

При создании соединителей получения в Центре администрирования Exchange мастер предлагает выбрать значение **Тип** для соединителя. При использовании командлета **New-ReceiveConnector** в командной консоли Exchange используется параметр *Usage* с одним из доступных значений (например, `-Usage Custom`), или назначенный параметр для типа использования (например, `-Custom`).

Тип использования можно указать только при создании соединителей получения. Создав соединитель, вы можете изменить доступные механизмы проверки подлинности и группы разрешений в Центре администрирования Exchange или с помощью командлета **Set-ReceiveConnector** в командной консоли Exchange.

Доступные типы использования представлены в приведенной ниже таблице.

Тип использования	Назначенные группы разрешений	Доступные механизмы проверки подлинности	Comments

Тип использования	Назначенные группы разрешений	Доступные механизмы проверки подлинности	Comments
Client	**Пользователи Exchange** (`ExchangeUsers`)	**Безопасность транспортного уровня** (`TLS`) **Обычная проверка подлинности** (`BasicAuth`) **Предлагать обычную проверку подлинности только после запуска TLS** (`BasicAuthRequireTLS`) **Интегрированные проверка подлинности Windows** (`Integrated`)	Используется клиентами POP3 и IMAP4, которым требуется отправлять электронные сообщения по протоколу SMTP с проверкой подлинности. При создании соединителя получения с этим типом использования в Центре администрирования Exchange или командной консоли Exchange невозможно выбрать привязки локальных IP-адресов и TCP-порт. По умолчанию этот тип использования привязан ко всем локальным IPv4- и IPv6-адресам для TCP-порта 587. Вы можете изменить эти привязки после создания соединителя. Этот тип использования недоступен на пограничных транспортных серверах.
Пользовательские	Не выбрано (`None`)	**Безопасность транспортного уровня** (`TLS`)	Используется в сценариях с несколькими лесами для получения почты от сторонних серверов обмена сообщениями, а также для внешней ретрансляции. Создав соединитель получения с этим типом использования, необходимо добавить группы разрешений в Центре администрирования Exchange или командной консоли Exchange.
Внутренний	**Устаревшие серверы Exchange** (`ExchangeLegacyServers`) **Серверы Exchange** (`ExchangeServers`)	**Безопасность транспортного уровня** (`TLS`) **проверка подлинности Exchange Server** (`ExchangeServers`)	Используется в сценариях с несколькими лесами для получения почты от предыдущих версий Exchange или от сторонних серверов обмена сообщениями либо на пограничных транспортных серверах для получения исходящей почты из внутренней организации Exchange. При создании соединителя получения с этим типом использования в Центре администрирования Exchange или командной консоли Exchange невозможно выбрать привязки локальных IP-адресов и TCP-порт. По умолчанию соединитель привязан ко всем локальным IPv4- и IPv6-адресам для TCP-порта 25. Вы можете изменить эти привязки после создания соединителя. Группа `ExchangeLegacyServers` разрешений недоступна на пограничных транспортных серверах.
Интернет	**Анонимные пользователи** (`AnonymousUsers`)	**Безопасность транспортного уровня** (`TLS`)	Используется для получения почты из Интернета. При создании соединителя получения с этим типом использования в Центре администрирования Exchange или командной консоли Exchange невозможно выбрать удаленные IP-адреса. По умолчанию соединитель принимает удаленные подключения со всех IPv4-адресов (0.0.0.0-255.255.255.255). Вы можете изменить эти привязки после создания соединителя.
Партнер	**Партнеры** (`Partners`)	**Безопасность транспортного уровня** (`TLS`)	Используется для настройки защищенного соединения с внешним партнером (взаимная проверка подлинности TLS, также называемая защитой на уровне домена).

Механизмы проверки подлинности соединителя получения

Механизмы проверки подлинности задают параметры входа и шифрования, используемые для входящих SMTP-подключений. Для соединителя получения можно настроить несколько механизмов проверки подлинности. В Центре администрирования Exchange механизмы проверки подлинности доступны на вкладке **Безопасность** в окне свойств соединителя получения. В командной консоли Exchange группы разрешений доступны в *параметре AuthMechanisms командлетов***New-ReceiveConnector** и **Set-ReceiveConnector** .

Доступные механизмы проверки подлинности описаны в таблице ниже.

Механизм проверки подлинности	Описание
Не выбрано (`None`)	Проверка подлинности не выполняется.
Безопасность на уровне транспорта (TLS) (`TLS`)	Объявление **STARTTLS** в ответе EHLO. Для зашифрованных подключений TLS требуется сертификат сервера, содержащий имя, которое соединитель получения объявляет в ответе EHLO. Дополнительные сведения см. в разделе Изменение баннера SMTP на соединителях получения. Другие серверы Exchange в вашей организации доверяют самозаверяющий сертификат сервера, но клиенты и внешние серверы обычно используют доверенный сторонний сертификат.

Механизм проверки подлинности	Описание
Обычная проверка подлинности (`BasicAuth`)	Обычная проверка подлинности (открытый текст).
Предлагать обычную проверку подлинности только после запуска TLS (`BasicAuthRequireTLS`)	Обычная проверка подлинности с шифрованием TLS.
Интегрированные проверка подлинности Windows (`Integrated`)	Проверка подлинности NTLM и Kerberos.
проверка подлинности Exchange Server (`ExchangeServer`)	Программный интерфейс универсальных служб защиты (GSSAPI) и взаимная проверка подлинности GSSAPI.
Внешняя защита (`ExternalAuthoritative`)	Предполагается, что используется внешний механизм защиты соединения, не входящий в состав Exchange. Подключение может быть связью IPsec или виртуальной частной сетью. Кроме того, серверы могут находиться в доверенной, физически контролируемой сети. Для этого механизма проверки подлинности требуется `ExchangeServers` группа разрешений. Такое сочетание механизма проверки подлинности и группы безопасности обеспечивает поддержку разрешения электронных адресов анонимных отправителей для сообщений, получаемых через соединитель.

Группы разрешений соединителя получения

Группа разрешений — это предопределенный набор разрешений, который предоставляется известным субъектам безопасности и назначается соединителю получения. Субъекты безопасности включают учетные записи пользователей, учетные записи компьютеров и группы безопасности (объекты, идентифицируемые идентификатором безопасности или идентификатором безопасности, которым могут быть назначены разрешения). Группы разрешений определяют, кто может использовать соединитель получения, и разрешения, которые они получают. Вы не можете создавать группы разрешений, а также изменять членов группы разрешений или разрешения по умолчанию группы разрешений.

В Центре администрирования Exchange группы разрешений доступны на вкладке **Безопасность** в свойствах соединителя получения. В командной консоли Exchange группы разрешений доступны в *параметре PermissionGroups командлетов***New-ReceiveConnector** и **Set-ReceiveConnector** .

Доступные группы разрешений представлены в приведенной ниже таблице.

Группа разрешений	Связанные субъекты безопасности	Предоставляемые разрешения

Анонимные пользователи (`Anonymous`)	`NT AUTHORITY\ANONYMOUS LOGON`	`ms-Exch-Accept-Headers-Routing`
		`ms-Exch-SMTP-Accept-Any-Sender`
		`ms-Exch-SMTP-Accept-Authoritative-Domain-Sender`
		`ms-Exch-SMTP-Submit`

Пользователи Exchange (`ExchangeUsers`)	`NT AUTHORITY\Authenticated Users`	`ms-Exch-Accept-Headers-Routing`
		`ms-Exch-Bypass-Anti-Spam`
		`ms-Exch-SMTP-Accept-Any-Recipient`
		`ms-Exch-SMTP-Submit`

Группа разрешений	Связанные субъекты безопасности	Предоставляемые разрешения

Серверы Exchange (`ExchangeServers`)	`<Domain>\Exchange Servers`
	`MS Exchange\Edge Transport Servers`
	`MS Exchange\Hub Transport Servers`
	Примечание: Этим субъектам безопасности также назначены другие внутренние разрешения. Дополнительные сведения см. в конце раздела Получение разрешений соединителя .
		`ms-Exch-Accept-Headers-Forest`
		`ms-Exch-Accept-Headers-Organization`
		`ms-Exch-Accept-Headers-Routing`
		`ms-Exch-Bypass-Anti-Spam`
		`ms-Exch-Bypass-Message-Size-Limit`
		`ms-Exch-SMTP-Accept-Any-Recipient`
		`ms-Exch-SMTP-Accept-Any-Sender`
		`ms-Exch-SMTP-Accept-Authentication-Flag`
		`ms-Exch-SMTP-Accept-Authoritative-Domain-Sender`
		`ms-Exch-SMTP-Accept-Exch50`
		`ms-Exch-SMTP-Submit`

Серверы Exchange (`ExchangeServers`)	`MS Exchange\Externally Secured Servers`	`ms-Exch-Accept-Headers-Routing`
		`ms-Exch-Bypass-Anti-Spam`
		`ms-Exch-Bypass-Message-Size-Limit`
		`s-Exch-SMTP-Accept-Any-Recipient`
		`ms-Exch-SMTP-Accept-Any-Sender`
		`ms-Exch-SMTP-Accept-Authentication-Flag`
		`ms-Exch-SMTP-Accept-Authoritative-Domain-Sender`
		`ms-Exch-SMTP-Accept-Exch50`
		`ms-Exch-SMTP-Submit`

Устаревшие серверы Exchange (`ExchangeLegacyServers`)	`<Domain>\ExchangeLegacyInterop`	`ms-Exch-Accept-Headers-Routing`
		`ms-Exch-Bypass-Anti-Spam`
		`ms-Exch-Bypass-Message-Size-Limit`
		`ms-Exch-SMTP-Accept-Any-Recipient`
		`ms-Exch-SMTP-Accept-Any-Sender`
		`ms-Exch-SMTP-Accept-Authentication-Flag`
		`ms-Exch-SMTP-Accept-Authoritative-Domain-Sender`
		`ms-Exch-SMTP-Accept-Exch50`
		`ms-Exch-SMTP-Submit`

Партнеры (`Partner`)	`MS Exchange\Partner Servers`	`ms-Exch-Accept-Headers-Routing` `ms-Exch-SMTP-Submit`

Разрешения описаны в разделе Разрешения соединителя получения далее в этой статье.

Разрешения соединителя получения

Как правило, разрешения применяются к соединителям получения с помощью групп разрешений. Однако вы можете настраивать детализированные разрешения для соединителя получения с помощью командлетов **Add-ADPermission** и **Remove-ADPermission**.

Разрешения соединителя получения назначаются субъектам безопасности с помощью групп разрешений для соединителя. Когда клиент или сервер SMTP создает подключение к соединителю получения, разрешения этого соединителя определяют, принимается ли соединение и как оно обрабатывается.

Доступные разрешения соединителя получения представлены в приведенной ниже таблице.

Разрешение соединителя получения	**Описание**
`ms-Exch-Accept-Headers-Forest`	Управляет хранением заголовков лесов Exchange в сообщениях. Имена заголовков лесов начинаются с **X-MS-Exchange-Forest-**. Если разрешение не предоставлено, все заголовки лесов удаляются из сообщений.
`ms-Exch-Accept-Headers-Organization`	Управляет сохранением заголовков организаций Exchange в сообщениях. Имена заголовков организаций начинаются с **X-MS-Exchange-Organization-**. Если это разрешение не предоставлено, все заголовки организаций удаляются из сообщений.
`ms-Exch-Accept-Headers-Routing`	Управляет сохранением заголовков **Received** и **Resent-*** в сообщениях. Если разрешение не предоставлено, все эти заголовки удаляются из сообщений.
`ms-Exch-Bypass-Anti-Spam`	Позволяет клиентам и серверам SMTP обходить фильтрацию спама.
`ms-Exch-Bypass-Message-Size-Limit`	Позволяет клиентам и серверам SMTP отправлять сообщения больше максимального размера, настроенного для соединителя получения.
`ms-Exch-SMTP-Accept-Any-Recipient`	Позволяет клиентам и серверам SMTP ретранслировать сообщения через соединитель получения. Если это разрешение не предоставлено, соединитель получения принимает только те сообщения, которые отправлены получателям в обслуживаемых доменах, настроенных для организации Exchange.
`ms-Exch-SMTP-Accept-Any-Sender`	Позволяет клиентам и серверам SMTP обходить проверку адреса отправителя на спуфинг, для которой обычно требуется, чтобы электронный адрес отправителя находился на обслуживаемом домене, настроенном для организации Exchange.
`ms-Exch-SMTP-Accept-Authentication-Flag`	Указывает, будут ли сообщения от клиентов и серверов SMTP рассматриваться как прошедшие проверку подлинности. Если это разрешение не предоставлено, то сообщения из этих источников определяются как внешние (непроверенные). Этот параметр важен для групп рассылки, настроенных для приема почты только от внутренних получателей (например, параметр *RequireSenderAuthenticationEnabled* для группы имеет `$true`значение).
`ms-Exch-SMTP-Accept-Authoritative-Domain-Sender`	Разрешает доступ к соединителю получения для отправителей, электронные адреса которых находятся на уполномоченных доменах, настроенных для организации Exchange.
`ms-Exch-SMTP-Accept-Exch50`	Позволяет клиентам и серверам SMTP отправлять команды **XEXCH50** соединителю отправки. Большой двоичный объект **X-EXCH50** использовался старыми версиями Exchange (Exchange 2003 и более ранними) для хранения данных Exchange в сообщениях (например, о вероятности нежелательной почты).
`ms-Exch-SMTP-Submit`	Это разрешение необходимо для отправки сообщений соединителям получения. Если это разрешение не предоставлено, команды **MAIL FROM** и **AUTH** не будут выполняться.

Примечания.

- Помимо задокументированных разрешений, существуют разрешения, которые назначаются всем субъектам безопасности в группе разрешений **серверов Exchange** (`ExchangeServers`), кроме `MS Exchange\Externally Secured Servers`. Эти разрешения зарезервированы для внутреннего использования в корпорации Майкрософт и представлены здесь исключительно в справочных целях.
  - `ms-Exch-SMTP-Accept-Xattr`
  - `ms-Exch-SMTP-Accept-XProxyFrom`
  - `ms-Exch-SMTP-Accept-XSessionParams`
  - `ms-Exch-SMTP-Accept-XShadow`

- `ms-Exch-SMTP-Accept-XSysProbe`
- `ms-Exch-SMTP-Send-XMessageContext-ADRecipientCache`
- `ms-Exch-SMTP-Send-XMessageContext-ExtendedProperties`
- `ms-Exch-SMTP-Send-XMessageContext-FastIndex`

- Имена разрешений, содержащиеся `ms-Exch-Accept-Headers-` в составе функции *брандмауэра заголовков* . Дополнительные сведения см. в разделе Брандмауэр заголовков.

Действия с разрешениями соединителей получения

Чтобы просмотреть разрешения, назначенные субъектам безопасности соединителя получения, используйте следующий синтаксис в командной консоли Exchange:

```
PowerShell

Get-ADPermission -Identity <ReceiveConnector> [-User <SecurityPrincipal>] | where {($_.Deny -eq $false) -and
($_.IsInherited -eq $false)} | Format-Table User,ExtendedRights
```

Например, чтобы просмотреть разрешения, назначенные всем субъектам безопасности соединителя получения Client Frontend Mailbox01, выполните следующую команду:

```
PowerShell

Get-ADPermission -Identity "Client Frontend Mailbox01" | where {($_.Deny -eq $false) -and ($_.IsInherited -eq $false)} |
Format-Table User,ExtendedRights
```

Чтобы просмотреть разрешения, назначенные только субъекту `NT AUTHORITY\Authenticated Users` безопасности в соединителе получения с именем Default Mailbox01, выполните следующую команду:

```
PowerShell

Get-ADPermission -Identity "Default Mailbox01" -User "NT AUTHORITY\Authenticated Users" | where {($_.Deny -eq $false) -and
($_.IsInherited -eq $false)} | Format-Table User,ExtendedRights
```

Чтобы добавить разрешения для субъекта безопасности, используйте следующий синтаксис:

```
PowerShell

Add-ADPermission -Identity <ReceiveConnector> -User <SecurityPrincipal> -ExtendedRights "<Permission1>","<Permission2>"...
```

Чтобы удалить разрешения субъекта безопасности, используйте следующий синтаксис:

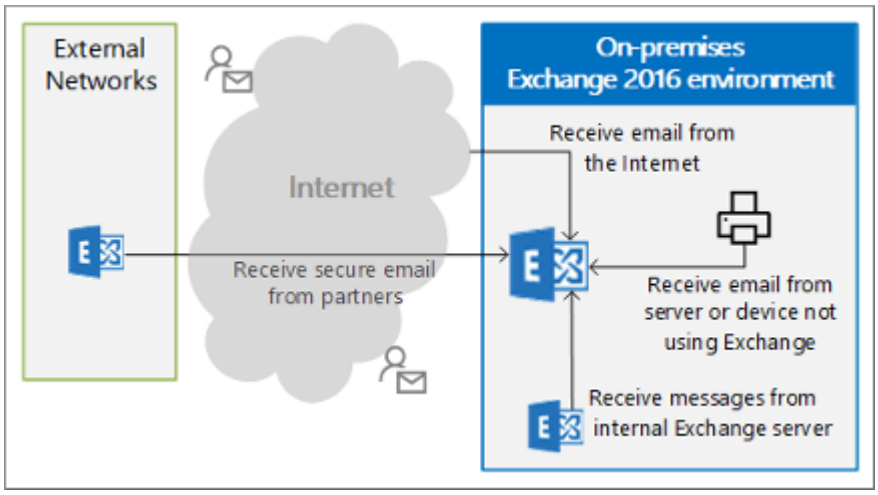
```
PowerShell

Remove-ADPermission -Identity <ReceiveConnector> -User <SecurityPrincipal> -ExtendedRights "<Permission1>","
<Permission2>"...
```

Сценарии для настраиваемых соединителей получения в Exchange Server

Статья • 04.04.2023

По умолчанию Exchange Server поставляется со многими различными соединителями получения, настроенными для наиболее распространенных сценариев потока обработки почты. Дополнительные сведения об этих соединителях см. в статье Соединители получения, создаваемые по умолчанию во время установки.

Вам может понадобиться обработать сообщения из другой системы обмена сообщениями, в которой нет Exchange. Кроме того, если у вас есть сетевое устройство, которое выполняет проверки на базе политик и пересылает сообщения на сервер Exchange Server, вам понадобится вручную настроить соединитель получения.



Если необходимо создать настраиваемый соединитель получения, следует принять во внимание приведенные ниже аспекты.

- Настраиваемые соединители получения можно создать в следующих службах на серверах Exchange:
  - **Серверы почтовых ящиков**: служба транспорта (концентратор) и служба транспорта переднего плана.
  - **Пограничные транспортные серверы**: транспортная служба.
- Для каждого соединителя получения на сервере Exchange Server требуется уникальное сочетание привязок сетевого адаптера (сочетание **локального IP-**

адреса и **TCP-порта**) и **параметров удаленной сети** (удаленных IP-адресов).

- Соединитель получения по умолчанию, который прослушивает все доступные локальные IP-адреса на порту 25, проверяя наличие подключений со всех удаленных IP-адресов, уже существует на всех серверах почтовых ящиков и пограничных транспортных серверах.

- Если вы создаете настраиваемый соединитель получения, который прослушивает все доступные локальные IP-адреса на порту 25, но для которого предусмотрен ограниченный диапазон *удаленных* IP-адресов, этот новый соединитель не будет конфликтовать ни с одним из соединителей получения по умолчанию на сервере. Дополнительные сведения см. в статье Удаленные адреса соединителей получения.

  Если не удается ограничить диапазон удаленных IP-адресов для настраиваемого соединителя получения, единственным вариантом является ограничение локального IP-адреса, используемого соединителем для порта 25. Необходимо изменить локальный IP-адрес для конфликтующего стандартного соединителя получения, а затем указать другой локальный IP-адрес при создании настраиваемого соединителя получения.

- В случае серверов почтовых ящиков необходимо создать настраиваемые соединители получения, для которых используется порт 25, во внешней службе транспорта, а не в службе транспорта (концентратора). Соединители получения в службе транспорта на серверах почтовых ящиков принимают зашифрованные SMTP-подключения, для которых предусмотрена проверка подлинности, от других служб транспорта на локальном сервере или других серверах почтовых ящиков в организации. Клиенты не подключаются к таким соединителям напрямую. Этот способ отличается от того, что предусмотрено в Exchange 2010, так как соединители получения можно создать только на транспортных серверах-концентраторах (не на серверах клиентского доступа).

Дополнительные сведения о соединителях получения см. в статье Соединители получения в Exchange Server.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 10 минут

- Процедуры Центра администрирования Exchange (EAC) доступны только на серверах почтовых ящиков. Дополнительные сведения о EAC см. в разделе

Центр администрирования Exchange в Exchange Server.

- Процедуры командной консоли Exchange доступны на серверах почтовых ящиков и пограничных транспортных серверах. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Получение соединителей" в разделе Разрешения потока обработки почты .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Сценарий 1. Получение почты из Интернета

В этом сценарии соединитель получения прослушивает анонимные SMTP-подключения через порт 25 со всех удаленных IP-адресов. Как правило, вам не нужно вручную настраивать соединитель получения для получения почты из Интернета. Соединитель получения с этими параметрами автоматически создается при установке сервера почтовых ящиков или пограничного транспортного сервера:

- Соединитель получения с именем Frontend <*ServerName*> по умолчанию в транспортной службе переднего плана на серверах почтовых ящиков.
- Соединитель получения с именем *ServerName*> *внутреннего соединителя*< получения по умолчанию на пограничных транспортных серверах.

Если один из этих соединителей существует, при попытке создания настраиваемого соединителя получения на сервере, который также прослушивает порт 25 на наличие анонимных SMTP-подключений со всех удаленных IP-адресов, появится сообщение об ошибке. Потребуется изменить привязку сетевого адаптера для конфликтующего соединителя получения, указав определенный локальный IP-адрес. При создании настраиваемого соединителя получения сообщений из Интернета нужно указать другую привязку сетевого адаптера.

Создание соединителя получения сообщений из Интернета на серверах почтовых ящиков с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел**Соединители получения** потока >**обработки почты**и нажмите кнопку Добавить (+

2. Откроется мастер **создания соединителей получения**. На первой странице настройте указанные ниже параметры.

   - **Имя**: введите описательное значение. Например, Соединитель получения сообщений из Интернета.
   - **Роль**. Выберите **Внешний транспорт**.
   - **Тип**: выберите **Интернет**.

   По завершении нажмите кнопку **Далее**.

3. В разделе **Привязки сетевого адаптера** на последней странице мастера выполните одно из приведенных ниже действий.

   - Если вы воссоздаете соединитель получения через Интернет, чтобы заменить отсутствующий соединитель получения по умолчанию с именем Default Frontend <*ServerName*> на сервере почтовых ящиков, оставьте значения по умолчанию **IP-адреса: (Все доступные IPv4)** и **Порт: 25** (при нажатии кнопки **Готово** сообщение об ошибке не появится).
   - Если вы создаете соединитель получения через Интернет, а соединитель получения по умолчанию с именем Default Frontend <*ServerName*> по-прежнему существует на сервере почтовых ящиков, выполните следующие действия.

     a. Выберите **IP-адреса** записи по умолчанию**(Все доступные IPv4)** и **Порт**: **25**, а затем нажмите кнопку **Изменить** (✎

     b. В открывшемся диалоговом окне **Изменить IP-адрес** настройте приведенные ниже параметры.

        - **Адрес**. Выберите **Укажите IPv4-адрес или IPv6-адрес** и введите допустимый локальный IP-адрес для соединителя.
        - **Порт**. Оставьте значение по умолчанию **25** .

По завершении нажмите кнопку **Сохранить**.

> ⓘ **Примечание**
>
> После создания нового соединителя получения Через Интернет на сервере почтовых ящиков обязательно измените параметры локального IP-адреса в свойствах соединителя получения по умолчанию с именем Default Frontend <*ServerName*>. Вам потребуется перейти к **разделу Определениепривязок сетевого адаптера**> в свойствах соединителя, а затем выбрать другой локальный IP-адрес, чтобы заменить **ip-адреса** по умолчанию: **(Все доступные IPv4)** и **Порт**: **25**.

Закончив, нажмите кнопку **Готово**.

Создание соединителя получения сообщений из Интернета с помощью командной консоли Exchange

Для создания соединителя получения сообщений из Интернета используйте приведенный ниже синтаксис.

PowerShell

```
New-ReceiveConnector -Name <UniqueName> [-TransportRole Frontend] -Internet
-Bindings <UniqueValidLocalIPAddress>
```

Приведенный ниже пример кода создает соединитель получения с названием "Internet Receive Connector" (Соединитель получения сообщений из Интернета) на сервере почтовых ящиков, который прослушивает локальный IP-адрес 10.1.15 на порту 25, проверяя наличие подключений со всех удаленных IP-адресов.

PowerShell

```
New-ReceiveConnector -Name "Internet Receive Connector" -TransportRole
Frontend -Internet -Bindings 10.10.1.1:25
```

Примечания.

- Чтобы выполнить эту команду на пограничном транспортном сервере, опустите параметр *TransportRole* .
- Если другой соединитель получения настроен для прослушивания через порт 25, используя все доступные локальные IP-адреса на сервере, вам потребуется

использовать параметр *Bindings* в **командлете Set-ReceiveConnector** , чтобы указать уникальный локальный IP-адрес для другого соединителя после создания нового соединителя получения Через Интернет.

Приведенный ниже пример кода создает соединитель получения с названием "Internet Receive Connector" (Соединитель получения сообщений из Интернета), который прослушивает все доступные локальные IP-адреса на порту 25, проверяя наличие подключений со всех удаленных IP-адресов. Эту команду можно выполнить, только если на сервере нет других соединителей получения, прослушивающих все доступные локальные IP-адреса на порту 25.

PowerShell

```
New-ReceiveConnector -Name "Internet Receive Connector" -TransportRole
Frontend -Internet -Bindings "0.0.0.0","[::]:"
```

Примечание. Чтобы выполнить эту команду на пограничном транспортном сервере, опустите параметр *TransportRole* .

Дополнительные сведения о синтаксисе и параметрах см. в статье New-ReceiveConnector.

Как проверить, все ли получилось?

Чтобы убедиться в том, что вы успешно создали соединитель получения сообщений из Интернета, выполните одно из приведенных ниже действий.

- В EAC перейдите к **разделу Соединители получения** потока >**обработки почты**, выберите соединитель получения, выберите Изменить (✎) и проверьте значения свойств.
- В командной консоли Exchange выполните указанную ниже команду на сервере и проверьте значения свойств.

  PowerShell

  ```
  Get-ReceiveConnector | where {$_.Bindings -like '*25' -AND
  $_.PermissionGroups -like '*AnonymousUsers*'} | Format-List
  Identity,Bindings,RemoteIPRanges,PermissionGroups
  ```

- Включите для соединителя получения ведение журнала протокола. Дополнительные сведения см. в разделе Настройка ведения журнала протокола.

- Отправьте из внешнего клиента тестовое сообщение другому пользователю в вашей организации. Кроме того, вы можете с помощью Telnet подключиться к соединителю получения. Дополнительные сведения см. в статье Проверка связи по протоколу SMTP на серверах Exchange с помощью Telnet.

Сценарий 2. Получение электронной почты от партнера

В этом сценарии соединитель получения прослушивает SMTP-подключения, прошедшие проверку подлинности TLS, через порт 25, но только с определенных IP-адресов партнерской организации. Для этого сценария не подходит соединитель получения по умолчанию. необходимо создать пользовательский соединитель получения.

Примечание. Создание специального соединителя получения — это только одно действие из всех тех, которые нужны для обеспечения связи с поддержкой шифрования TLS между вашей организацией и доверенным партнером (например, нужно еще создать и установить сертификаты).

Создание соединителя получения для шифрования сообщений от партнера на серверах почтовых ящиков с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел**Соединители получения** потока >**обработки почты**и нажмите кнопку Добавить (➕

2. Откроется мастер **создания соединителей получения**. На первой странице настройте указанные ниже параметры.

   - **Имя**: введите описательное значение. Например, Зашифрованные с помощью TLS сообщения от Fabrikam.com.

   - **Роль**. Выберите **Внешний транспорт**.

   - **Тип**: выберите **Партнер**.

   По завершении нажмите кнопку **Далее**.

3. В разделе **Привязки сетевого адаптера** на второй странице мастера выполните одно из приведенных ниже действий.

- Для параметра **IP-адреса** оставьте значение **(Все доступные IPv4)**, для параметра **Порт** — **25**.
- Вы можете ограничить ряд допустимых локальных IP-адресов для соединителя получения на сервере, указав всего один, если этого требует ваш сценарий.

  a. Выберите **IP-адреса** записи по умолчанию**(Все доступные IPv4)** и **Порт**: **25**, а затем нажмите кнопку **Изменить** (✎

  b. В открывшемся диалоговом окне **Изменить IP-адрес** настройте приведенные ниже параметры.

  - **Адрес**. Выберите **Укажите IPv4-адрес или IPv6-адрес** и введите допустимый локальный IP-адрес для соединителя.
  - **Порт**. Оставьте значение по умолчанию **25** .

  По завершении нажмите кнопку **Сохранить**.

Закончив, нажмите кнопку **Далее**.

4. В разделе **Настройки удаленной сети** на последней странице мастера настройте указанные ниже параметры.

   a. Выберите запись по умолчанию **0.0.0.0-255.255.255.255** и нажмите кнопку **Изменить** (✎

   b. В открывшемся диалоговом окне **Изменить IP-адрес** введите IP-адрес или диапазон IP-адресов удаленной партнерской организации.

   Закончив, нажмите кнопку **Сохранить**.

Закончив, нажмите кнопку **Готово**.

Создание соединителя получения для шифрования сообщений от партнера с помощью командной консоли Exchange

Синтаксис для создания соединителя получения, использующего TLS для шифрования сообщений от партнера:

```
PowerShell
```

```
New-ReceiveConnector -Name <UniqueName> [-TransportRole Frontend] -Partner
-Bindings <0.0.0.0:25 | LocalIPAddress:25> -RemoteIPRanges
<RemoteIPAddresses>
```

Приведенный ниже пример кода создает на сервере почтовых ящиков соединитель получения, названный "Fabrikam.com TLS", который принимает сообщения только с IP-адресов 17.17.17.1/24, используя все доступные локальные IP-адреса.

PowerShell

```
New-ReceiveConnector -Name "Fabrikam.com TLS" -TransportRole Frontend -
Partner -RemoteIPRanges 17.17.17.1/24 -Bindings 0.0.0.0:25
```

Примечание. Чтобы выполнить эту команду на пограничном транспортном сервере, опустите параметр *TransportRole* .

Дополнительные сведения о синтаксисе и параметрах см. в статье New-ReceiveConnector.

Как проверить, все ли получилось?

Чтобы убедиться в том, что вы успешно создали соединитель получения сообщений от партнера, зашифрованных с использованием TLS, выполните одно из приведенных ниже действий.

- В EAC перейдите к **разделу Соединители получения** потока >**обработки почты**, выберите соединитель получения, выберите Изменить (✎) и проверьте значения свойств.
- В командной консоли Exchange выполните указанную ниже команду на сервере и проверьте значения свойств.

  PowerShell

  ```
  Get-ReceiveConnector | where {$_.Bindings -like '*25' -AND
  $_.PermissionGroups -like '*Partners*'} | Format-List
  Identity,Bindings,RemoteIPRanges,PermissionGroups
  ```

- Включите для соединителя получения ведение журнала протокола. Дополнительные сведения см. в разделе Настройка ведения журнала протокола.

- Попросите представителя партнерской организации отправить тестовое сообщение пользователю в вашей организации. Убедитесь, что сообщение зашифровано с использованием TLS, просмотрев заголовок сообщения.

Сценарий 3. Получение сообщений с сервера, устройства или из службы, если отправитель не использует Exchange

В этом сценарии соединитель получения прослушивает порт 25 на наличие подключений с определенного IP-адреса службы или устройства. Для этого сценария может потребоваться определенный тип проверки подлинности (обратитесь к документации по службе или устройству).

Создание соединителя получения, который принимает сообщения только от определенной службы или устройства, на серверах почтовых ящиков с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел**Соединители получения** потока >**обработки почты**и нажмите кнопку Добавить (**+**

2. Откроется мастер **создания соединителей получения**. На первой странице настройте указанные ниже параметры.

   - **Имя**: введите описательное значение. Например, Входящая почта из безопасного устройства.

   - **Роль**. Выберите **Внешний транспорт**.

   - **Тип**: выберите **Пользовательский**.

   По завершении нажмите кнопку **Далее**.

3. В разделе **Привязки сетевого адаптера** на второй странице мастера выполните одно из приведенных ниже действий.

   - Для параметра **IP-адреса** оставьте значение **(Все доступные IPv4)**, для параметра **Порт** — **25**.

   - Вы можете ограничить ряд допустимых локальных IP-адресов для соединителя получения на сервере, указав всего один, если этого требует ваш сценарий.

a. Выберите **IP-адреса** записи по умолчанию**(Все доступные IPv4)** и **Порт**: **25**, а затем нажмите кнопку **Изменить** (✏️

b. В открывшемся диалоговом окне **Изменить IP-адрес** настройте приведенные ниже параметры.

- **Адрес**. Выберите **Укажите IPv4-адрес или IPv6-адрес** и введите допустимый локальный IP-адрес для соединителя.
- **Порт**. Оставьте значение по умолчанию **25** .

По завершении нажмите кнопку **Сохранить**.

Закончив, нажмите кнопку **Далее**.

4. В разделе **Настройки удаленной сети** на последней странице мастера настройте указанные ниже параметры.

a. Выберите запись по умолчанию **0.0.0.0-255.255.255.255** и нажмите кнопку **Изменить** (✏️

b. В открывшемся диалоговом окне **Изменить IP-адрес** введите IP-адрес или диапазон IP-адресов службы или устройства.

Закончив, нажмите кнопку **Сохранить**.

Закончив, нажмите кнопку **Готово**.

5. Вернитесь в раздел**Соединители получения** потока >**обработки почты**, выберите только что созданный соединитель и нажмите кнопку Изменить (✏️

6. На вкладке **Безопасность** настройте сочетание методов проверки подлинности и групп разрешений, необходимых для службы или устройства. Пример:

- Оставьте параметр **Протокол TLS** выбранным, выберите параметр **Обычная проверка подлинности**, а затем выберите группу разрешений **Анонимные пользователи**.
- Clear **Transport Layer Security (TLS)**, select **Basic authentication** and **Exchange server authentication**, and then select the **Exchange users** and **Legacy Exchange servers** permission group.

  Дополнительные сведения о группах разрешений см. в статье Группы разрешений соединителя получения.

> ⊗ **Внимание!**
>
> Будьте очень осторожны, используя метод проверки подлинности **Внешняя защита** с группой разрешений **Серверы Exchange Server**. Это сочетание позволяет удаленным IP-адресам, указанным в разделе **Параметры удаленной сети** на вкладке **Определение** области, анонимно передавать сообщения через сервер Exchange Server. Дополнительные сведения см. в статье **Allow anonymous relay on Exchange servers**.

> ⚠ **Предупреждение**
>
> При использовании механизма проверки подлинности **Обычная проверка подлинности** или **Предложение обычной проверки подлинности только после запуска TLS** без группы разрешений **Анонимные пользователи** в качестве соединителя ретранслятора, прошедших проверку подлинности, маршрутизация почты всегда будет пытаться выбрать пользователя, прошедшего проверку подлинности, или активный почтовый сервер почтового ящика организации.

По завершении нажмите кнопку **Сохранить**.

Создание соединителя получения, который принимает сообщения только от определенной службы или устройства, с помощью командной консоли Exchange

Синтаксис для создания соединителя получения, принимающего сообщения только от определенной службы или устройства:

PowerShell

```
New-ReceiveConnector -Name <UniqueName> [-TransportRole Frontend] -Custom -
Bindings <0.0.0.0:25 | LocalIPAddress:25> -RemoteIPRanges
<RemoteIPAddresses> -AuthMechanism <AuthMechanism1>,<AuthMechanism2>... -
PermissionGroups <PermissionGroup1>,<PermissionGroup2>...
```

Приведенный ниже пример кода создает соединитель получения с названием "Inbound From Service" (Входящие сообщения из службы) на сервере почтовых ящиков.

- **Привязки**: все доступные локальные IP-адреса.
- **Диапазоны удаленных IP-адресов**: 192.168.5.1/24.
- **Механизмы проверки подлинности**: обычная проверка подлинности.
- **Группы разрешений**: анонимные пользователи.

PowerShell

```
New-ReceiveConnector -Name "Inbound From Service" -TransportRole Frontend -
Custom -Bindings 0.0.0.0:25 -RemoteIPRanges 192.168.10.5 -AuthMechanism
BasicAuth -PermissionGroups AnonymousUsers
```

Примечание. Чтобы выполнить эту команду на пограничном транспортном сервере, опустите параметр *TransportRole* .

Дополнительные сведения о синтаксисе и параметрах см. в статье New-ReceiveConnector.

Как проверить, все ли получилось?

Чтобы убедиться в том, что вы успешно создали соединитель получения, который принимает сообщения только от определенной службы или устройства, выполните одно из приведенных ниже действий.

- В EAC перейдите к разделу**Соединители получения** потока >**обработки почты**, выберите соединитель Получения, выберите Изменить (✎ и проверьте значения свойств.
- В командной консоли Exchange выполните указанную ниже команду на сервере и проверьте значения свойств.

  PowerShell

  ```
  Get-ReceiveConnector | where {$_.Bindings -like '*25'} | Format-List
  Identity,RemoteIPRanges,PermissionGroups,AuthMechanism
  ```

- Включите для соединителя получения ведение журнала протокола. Дополнительные сведения см. в разделе Настройка ведения журнала протокола.
- Отправьте тестовое сообщение или подключитесь к соединителю получения с помощью Telnet с сервера или устройства. Дополнительные сведения см. в

статье Проверка связи по протоколу SMTP на серверах Exchange с помощью Telnet.

Сценарий 4. Получение сообщений с внутренних серверов Exchange Server

Настраиваемые соединители получения не нужно настраивать для потока обработки внутренней почты между серверами почтовых ящиков. Но для получения сообщений с серверов почтовых ящиков может потребоваться создание настраиваемого соединителя получения на пограничном транспортном сервере без подписки. В этом сценарии пограничный транспортный сервер прослушивает порт 25 на наличие подключений только с IP-адреса указанных серверов почтовых ящиков.

Создание соединителя получения, принимающего сообщения только с внутреннего сервера Exchange Server, с помощью командной консоли Exchange

Синтаксис для создания соединителя получения, принимающего сообщения только с внутреннего сервера Exchange Server:

PowerShell

```
New-ReceiveConnector -Name <UniqueName> [-TransportRole Frontend] -Internal
-RemoteIPRanges <RemoteIPAddress>
```

Приведенный ниже пример кода создает соединитель получения с названием "Inbound From Organization" (Входящие сообщения от организации) на пограничном транспортном сервере без подписки, который прослушивает IP-адреса 10.1.2.10, 10.1.2.15 и 10.1.2.20 на наличие входящих сообщений с внутренних серверов почтовых ящиков.

PowerShell

```
New-ReceiveConnector -Name "Inbound From Organization" -Internal -
RemoteIPRanges 10.1.2.10,10.1.2.15,10.1.2.20
```

Примечание. Если пограничный транспортный сервер использует разные сетевые адаптеры для внутренних и внешних сетей, обязательно используйте параметр

Bindings в командлете **Set-ReceiveConnector после создания соединителя** , чтобы указать правильный локальный IP-адрес соединителя.

Дополнительные сведения о синтаксисе и параметрах см. в статье New-ReceiveConnector.

Как проверить, все ли получилось?

Чтобы убедиться в том, что вы успешно создали соединитель получения, который принимает сообщения только с внутреннего сервера Exchange Server, выполните одно из приведенных ниже действий.

- В EAC перейдите к разделу**Соединители получения** потока >**обработки почты**, выберите соединитель Получения, выберите Изменить (✎ и проверьте значения свойств.
- В командной консоли Exchange выполните указанную ниже команду на сервере и проверьте значения свойств.

  PowerShell

  ```
  Get-ReceiveConnector | where {$_.Bindings -like '*25'} | Format-List Identity,RemoteIPRanges,PermissionGroups,AuthMechanism
  ```

- Включите для соединителя получения ведение журнала протокола. Дополнительные сведения см. в разделе Настройка ведения журнала протокола.
- Отправьте тестовое сообщение или подключитесь к соединителю получения с помощью Telnet с удаленного сервера Exchange Server. Дополнительные сведения см. в статье Проверка связи по протоколу SMTP на серверах Exchange с помощью Telnet.

Изменение заголовка SMTP в соединителе получения

Статья • 04.04.2023

Баннер SMTP — это начальный ответ smtp-подключения, который сервер обмена сообщениями получает после подключения к серверу Exchange Server. В частности, сервер обмена сообщениями подключается к соединителю получения, настроенным на сервере Exchange Server. Для серверов почтовых ящиков Exchange внешние серверы обмена сообщениями подключаются через соединители получения, настроенные в службе внешнего транспорта. Соединитель получения по умолчанию, настроенный для приема анонимных SMTP-подключений, называется Frontend <*ServerName*> по умолчанию. Для пограничных транспортных серверов соединитель получения по умолчанию в транспортной службе с именем По умолчанию внутренний соединитель <*получения ServerName*>> настроен для приема анонимных SMTP-подключений. Дополнительные сведения см. в разделах Как сообщения от внешних отправителей поступают в транспортный конвейер и Соединители приема по умолчанию, созданные во время установки.

По умолчанию отклик подключения выглядит вот так:

```
220 <ServerName> Microsoft ESMTP MAIL service ready at <RegionalDay-Date-24HourTimeFormat><RegionalTimeZoneOffset>
```

Ниже перечислены причины, по которым вам, возможно, потребуется изменить заголовок SMTP, используемый по умолчанию.

- Вы не хотите раскрывать имя сервера Exchange или внутреннего сервера Exchange внешним серверам обмена сообщениями в отклике подключения.
- Вы хотите, чтобы отклик подключения включал ваше доменное имя для проверок, выполняемых системами защиты от нежелательной почты, или обратного поиска DNS для заголовков SMTP.
- Вы хотите, чтобы отклик подключения включал имя соединителя получения для упрощения устранения неполадок, связанных с подключением.

Что нужно знать перед началом работы?

- Предполагаемое время для завершения: 5 минут.

- Для выполнения этой процедуры можно использовать только PowerShell. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Замещающая строка баннера SMTP всегда должна начинаться с `220` (по умолчанию код ответа SMTP "Готово к обслуживанию" — 220).
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Получение соединителей" в разделе Разрешения потока обработки почты .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование Командная консоль Exchange для изменения заголовка SMTP в соединителе получения

Используйте следующий синтаксис.

PowerShell

```
Set-ReceiveConnector -Identity <ConnectorIdentity> -Banner "220 <Banner Text>"
```

В этом примере показано, как изменить заголовок SMTP в соединителе получения с именем Default Frontend Mailbox01 и присвоить ему значение 220 contoso.com.

PowerShell

```
Set-ReceiveConnector -Identity "Default Frontend Mailbox01" -Banner "220 consoso.com"
```

В этом примере показано, как удалить настраиваемый заголовок SMTP, который задает для заголовка SMTP значение, используемое по умолчанию.

PowerShell

```
Set-ReceiveConnector -Identity "Default Frontend Mailbox01" -Banner $null
```

Как проверить, что все получилось?

Чтобы убедиться, что вы успешно изменили заголовок SMTP на соединителе получения, выполните указанные ниже действия.

1. Откройте клиент Telnet на компьютере, с помощью которого можно получить доступ к соединителю получения, и выполните следующую команду:

   ```
   open <Connector FQDN or IP address><TCPPort>
   ```

2. Убедитесь, что в отклике имеется настроенный вами заголовок SMTP.

Обратите внимание, что данная процедура работает только на соединителях получения, которые разрешают анонимную или обычную проверку подлинности. Дополнительные сведения см. в статье Проверка связи по протоколу SMTP на серверах Exchange с помощью Telnet.

Включение анонимной ретрансляции на серверах Exchange

Статья • 04.04.2023

Открытая ретрансляция не подходит для серверов обмена сообщениями в Интернете. Открытая ретрансляция позволяет прозрачно перенаправлять почту из любого источника через сервер открытой ретрансляции. Такое поведение маскирует источник сообщений, создавая впечатление, что почта отправлена с сервера открытой ретрансляции. Серверы открытой ретрансляции пользуются большой популярностью у рассылающих нежелательную почту, поэтому никогда не настраивайте свои серверы обмена сообщениями на открытую ретрансляцию.

С другой стороны, *анонимная ретрансляция* — обычное требование для многих компаний с внутренними веб-серверами, серверами баз данных, приложениями мониторинга и другими сетевыми устройствами, которые создают сообщения электронной почты, но не могут их отправлять.

В Exchange Server можно создать выделенный соединитель получения в транспортной службе переднего плана на сервере почтовых ящиков, который разрешает анонимный ретранслятор из определенного списка узлов внутренней сети. Ниже приведены основные моменты, которые следует учесть при настройке соединителя получения для анонимной ретрансляции.

- Необходимо создать выделенный соединитель получения, чтобы указать сетевые узлы, которым разрешено анонимно ретранслировать сообщения, чтобы вы могли исключить из использования соединителя кого-либо или что-либо еще. Не пытайтесь добавить возможность анонимного ретранслятора в соединители получения по умолчанию, созданные Exchange. Ограничение доступа к соединителю получения имеет решающее значение, так как вы не хотите настраивать сервер в качестве открытого ретранслятора.

- Выделенный соединитель получения нужно создавать во внешней службе транспорта, а не в службе транспорта. В Exchange Server служба транспорта переднего плана и транспортная служба всегда находятся вместе на серверах почтовых ящиков. Служба внешнего транспорта имеет соединитель получения по умолчанию с именем Default Frontend *<ServerName>* , настроенный для прослушивания входящих SMTP-подключений из любого источника через TCP-порт 25. Вы можете создать еще один соединитель получения во внешней службе транспорта, который также прослушивает TCP-порт 25 в ожидании входящих SMTP-подключений, но необходимо указать IP-

адреса, которым разрешено использовать этот соединитель. Выделенный соединитель получения всегда будет использоваться для входящих подключений из этих конкретных узлов сети (соединитель получения, в конфигурации которого указано наиболее точное соответствие IP-адресу подключающегося сервера, имеет приоритет).

В отличие от этого, в транспортной службе есть соединитель получения по умолчанию с именем Default <*ServerName*> , который также настроен для входящих SMTP-подключений из любого источника, но этот соединитель прослушивает TCP-порт 2525, чтобы он не конфликтовал с соединителем Receive в транспортной службе переднего плана. Кроме того, в вашей организации этот соединитель получения должны использовать только другие службы транспорта и серверы Exchange, так как методы проверки подлинности и шифрования настроены соответствующим образом.

Дополнительные сведения см. в разделах Mail flow and the transport pipeline и Соединители получения по умолчанию, созданные во время установки.

- После того как вы создали выделенный соединитель получения, необходимо изменить его разрешения, чтобы разрешить анонимную ретрансляцию определенным узлам сети. Для анонимной ретрансляции сообщений узлам сети необходимы как минимум следующие разрешения на уровне соединителя получения:
  - `ms-Exch-Accept-Headers-Routing`
  - `ms-Exch-SMTP-Accept-Any-Recipient`
  - `ms-Exch-SMTP-Accept-Any-Sender`
  - `ms-Exch-SMTP-Accept-Authoritative-Domain-Sender`
  - `ms-Exch-SMTP-Submit`

    Дополнительные сведения о разрешениях на уровне соединителей получения см. в разделах Группы разрешений соединителя получения и Разрешения соединителя получения.

    Настроить разрешения на уровне соединителя получения, необходимые для анонимной ретрансляции, можно двумя способами. Эти способы описаны в приведенной ниже таблице.

Метод	Предоставляемые разрешения	Достоинства	Недостатки

Метод	Предоставляемые разрешения	Достоинства	Недостатки
Добавьте группу разрешений **Анонимные пользователи** (`Anonymous`) в соединитель получения и добавьте `Ms-Exch-SMTP-Accept-Any-Recipient` разрешение субъекту `NT AUTHORITY\ANONYMOUS LOGON` безопасности на соединителе получения.	Подключения используют `NT AUTHORITY\ANONYMOUS LOGON` субъект безопасности со следующими разрешениями: • `ms-Exch-Accept-Headers-Routing` • `ms-Exch-SMTP-Accept-Any-Recipient` • `ms-Exch-SMTP-Accept-Any-Sender` • `ms-Exch-SMTP-Accept-Authoritative-Domain-Sender` • `ms-Exch-SMTP-Submit`	Предоставляет минимальный объем разрешений, необходимый для анонимной ретрансляции.	Сложнее настроить (необходимо использовать Командная консоль Exchange). Сетевые узлы считаются анонимными отправителями. Сообщения не обходят проверки антиспама или ограничения размера сообщений, и адрес электронной почты отправителя не может быть разрешен в соответствующее отображаемое имя (если оно есть) в глобальном списке адресов.

Метод	Предоставляемые разрешения	Достоинства	Недостатки
Добавьте группу разрешений **серверов Exchange** (`ExchangeServers`) и механизм проверки **подлинности для внешней защиты** (`ExternalAuthoritative`) в соединитель получения.	Подключения используют `MS Exchange\Externally Secured Servers` субъект безопасности со следующими разрешениями: • `ms-Exch-Accept-Headers-Routing` • `ms-Exch-Bypass-Anti-Spam` • `ms-Exch-Bypass-Message-Size-Limit` • `ms-Exch-SMTP-Accept-Any-Recipient` • `ms-Exch-SMTP-Accept-Any-Sender` • `ms-Exch-SMTP-Accept-Authentication-Flag` • `ms-Exch-SMTP-Accept-Authoritative-Domain-Sender` • `ms-Exch-SMTP-Accept-Exch50` • `ms-Exch-SMTP-Submit`	Проще настроить (все можно сделать в Центр администрирования Exchange). Узлы сети считаются отправителями, прошедшими проверку подлинности. Сообщения обходят проверки антиспамов и ограничения размера сообщений, и адрес электронной почты отправителя может быть разрешен в соответствующее отображаемое имя в глобальном списке адресов.	Разрешает отправлять сообщения от имени пользователей организации Exchange. Узлы сети считаются полностью надежными, независимо от объема, размера и содержания отправляемых сообщений.

Вам необходимо выбрать способ, наиболее подходящий для вашей организации. Мы покажем, как настроить разрешения обоими способами. Помните: использовать можно только один способ, а не два одновременно.

Что нужно знать перед началом работы?

- Предполагаемое время выполнения задачи: 10 минут.
- Для некоторых из этих процедур требуется командная консоль Exchange. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Получение соединителей" в разделе Разрешения потока обработки почты .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Шаг 1. Создайте выделенный соединитель получения для анонимной ретрансляции

Вы можете создать соединитель получения в EAC или в Командная консоль Exchange.

Создание выделенного соединителя получения для анонимной ретрансляции с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел**Соединители полученияпотока**> обработки почты и нажмите кнопку **Добавить**➕ Запустится мастер **создания соединителя получения**.
2. На первой странице укажите следующие сведения:
   - **Имя**. Введите описательное имя соединителя получения, например Анонимный ретранслятор.
   - **Роль**. Выберите **Внешний транспорт**.
   - **Тип**: выберите **Пользовательский**.

По завершении нажмите кнопку **Далее**.

3. На следующей странице, в разделе **Привязки сетевого адаптера**, выполните одно из указанных ниже действий.

   - Если у сервера Exchange один сетевой адаптер, а внешний и внутренний трафик не разделены с помощью разных подсетей, примите существующую запись **(Все доступные IPv4)** на порте 25.

   - Если у сервера Exchange есть внутренний и внешний сетевой адаптер, а внутренний и внешний сетевой трафик разделены с помощью разных подсетей, безопасность можно улучшить, ограничив использование соединителя запросами, исходящими от внутреннего сетевого адаптера. Выполните следующие действия:

     a. Выберите существующую **запись (Все доступные IPv4),** щелкните **удалить**━ а затем щелкните **Добавить**✚.

     b. В появившемся диалоговом окне **Привязки сетевого адаптера** выберите параметр **Указать адрес IPv4 или IPv6**, введите доступный IP-адрес, настроенный на внутреннем сетевом адаптере, и нажмите кнопку **Сохранить**.

   По завершении нажмите кнопку **Далее**.

4. На следующей странице в разделе **Параметры удаленной сети** выполните следующие действия.

   a. Выберите существующую запись **0.0.0.0-255.255.255.255,** а затем нажмите кнопку **Удалить**━ нажмите кнопку **Добавить**✚

   b. В появившемся диалоговом окне **Параметры удаленного адреса** введите IP-адрес или диапазон IP-адресов, указанных для узлов сети, которым разрешено использовать этот соединитель, и нажмите кнопку **Сохранить**. Вы можете повторить этот шаг, чтобы добавить несколько IP-адресов или диапазонов IP-адресов. Не используйте общие конструкции: максимально точно укажите узлы сети, которым разрешено использовать этот соединитель.

   Закончив, нажмите кнопку **Готово**.

Создание выделенного соединителя получения для анонимной ретрансляции с помощью Командная

консоль Exchange

Чтобы создать такой же соединитель получения в Командная консоль Exchange, используйте следующий синтаксис:

```
PowerShell

New-ReceiveConnector -Name <ConnectorName> -TransportRole FrontendTransport
-Custom -Bindings <LocalIPAddresses>:25 -RemoteIpRanges <RemoteIPAddresses>
```

В этом примере создается соединитель получения со следующими параметрами:

- **Имя**: Анонимный ретранслятор
- **Роль транспорта**: `FrontEndTransport`
- **Тип использования**: Пользовательский
- **Привязки**: `0.0.0.0:25` (прослушивание входящих сообщений на всех IP-адресах, настроенных на всех сетевых адаптерах на сервере Exchange Server через TCP-порт 25.)
- **Удаленные IP-адреса, которым разрешено использовать этот соединитель**: 192.168.5.10 и 192.168.5.11

```
PowerShell

New-ReceiveConnector -Name "Anonymous Relay" -TransportRole
FrontendTransport -Custom -Bindings 0.0.0.0:25 -RemoteIpRanges
192.168.5.10,192.168.5.11
```

Примечания:

- Параметр *Bindings* является обязательным при указании настраиваемого типа использования.
- Параметр *RemoteIpRanges* принимает отдельный IP-адрес, диапазон IP-адресов (например, `192.168.5.10-192.168.5.20`) или межклассовую маршрутизацию (CIDR) (например, `192.168.5.1/24`). Вы можете указать несколько значений, разделив их запятыми.

Шаг 2. Настройте разрешения для анонимной ретрансляции на уровне

выделенного соединителя получения

Как отмечалось выше, настроить необходимые разрешения на уровне соединителя получения можно двумя разными способами:

- настройка анонимных соединений;
- настройка соединений с внешней защитой.

Выберите один из этих способов. В примерах используется соединитель получения Anonymous Relay, созданный на шаге 1.

Настройка анонимных соединений

Выполните следующие команды в Командная консоль Exchange:

1.

PowerShell

```
Set-ReceiveConnector "Anonymous Relay" -PermissionGroups AnonymousUsers
```

2.

PowerShell

```
Get-ReceiveConnector "Anonymous Relay" | Add-ADPermission -User "NT
AUTHORITY\ANONYMOUS LOGON" -ExtendedRights "Ms-Exch-SMTP-Accept-Any-
Recipient"
```

Настройка соединений с внешней защитой

1. В EAC перейдите в раздел**Соединители получения** потока >**обработки почты**, выберите соединитель Анонимный ретранслятор и щелкните ✎
2. В окне свойств соединителя откройте вкладку **Безопасность** и сделайте следующее:
   - **Проверка подлинности**. Снимите флажок **TLS** и выберите **Внешняя защита (например, с помощью IPsec).**
   - **Группы разрешений**. Выберите **Серверы Exchange**.

   По завершении нажмите кнопку **Сохранить**.

Чтобы выполнить те же действия в Командная консоль Exchange, запустите следующую команду:

```
PowerShell

Set-ReceiveConnector "Anonymous Relay" -AuthMechanism ExternalAuthoritative
-PermissionGroups ExchangeServers
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно настроили анонимный ретранслятор, выполните следующие действия.

- Проверьте настройки выделенного соединителя получения.

  ```
  PowerShell

  Get-ReceiveConnector "Anonymous Relay" | Format-List
  Enabled,TransportRole,Bindings,RemoteIPRanges
  ```

- Проверьте разрешения выделенного соединителя получения.

  ```
  PowerShell

  Get-ADPermission "Anonymous Relay" -User "NT AUTHORITY\ANONYMOUS LOGON"
  | where {($_.Deny -eq $false) -and ($_.IsInherited -eq $false)} |
  Format-Table User,ExtendedRights
  ```

  Или

  ```
  PowerShell

  Get-ADPermission "Anonymous Relay" -User "MS Exchange\Externally
  Secured Servers" | where {($_.Deny -eq $false) -and ($_.IsInherited -eq
  $false)} | Format-Table User,ExtendedRights
  ```

- Используйте Telnet, чтобы проверить подключение одного или нескольких указанных узлов сети к выделенному соединителю получения и анонимную ретрансляцию почты через соединитель. По умолчанию клиент Telnet не устанавливается в большинстве клиентских или серверных версий Microsoft Windows. Сведения об установке см. в статье Установка клиента Telnet.

  Дополнительные сведения см. в статье Проверка связи по протоколу SMTP на серверах Exchange с помощью Telnet.

Если узел сети — устройство без Telnet, вы можете временно добавить IP-адрес компьютера в соединитель получения, а после проверки удалить его.

Для проверки потребуются следующие значения:

- **Назначение**. Это IP-адрес или полное доменное имя, которое используется для подключения к выделенному соединителю получения. Скорее всего, это IP-адрес сервера почтовых ящиков, на котором задан соединитель получения. Это значение связано со свойством **Привязки сетевого адаптера** (или параметром *Bindings*), которое вы настроили на уровне соединителя. Используйте значение, допустимое для вашей среды. В этом примере мы используем значение 10.1.1.1.
- **Адрес электронной почты отправителя**. Вероятно, вы настроите серверы или устройства, которые анонимно ретранслируют почту, чтобы использовать адрес электронной почты для отправки, который находится в авторитетном домене вашей организации. В этом примере мы будем использовать chris@contoso.com.
- **Адрес электронной почты получателя**. Используйте допустимый адрес электронной почты. В этом примере мы будем использовать kate@fabrikam.com.
- **Тема сообщения**: Тест
- **Текст сообщения**: это тестовое сообщение

1. В командной строке введите telnet и нажмите клавишу ВВОД.
2. Введите set localecho и нажмите клавишу ВВОД.
3. Введите OPEN 10.1.1.1 25 и нажмите клавишу ВВОД.
4. Введите EHLO и нажмите клавишу ВВОД.
5. Введите MAIL FROM:chris@contoso.com, а затем нажмите клавишу ВВОД.
6. Введите RCPT TO:kate@fabrikam.com, а затем нажмите клавишу ВВОД.
    - При получении ответа `250 2.1.5 Recipient OK` соединитель получения разрешает анонимный ретранслятор с сетевого узла. Перейдите к следующему шагу, чтобы закончить отправку проверочного сообщения.
    - Если вы получили ответ `550 5.7.1 Unable to relay`, соединитель получения не разрешает анонимный ретранслятор с сетевого узла. В

этом случае сделайте следующее:

- Убедитесь, что вы подключаетесь к правильному IP-адресу или полному доменному имени для выделенного соединителя получения.
- Убедитесь, что компьютеру, на котором запущен Telnet, разрешено использовать соединитель получения.
- Проверьте разрешения на уровне соединителя получения.

7. Введите DATA и нажмите клавишу ВВОД.

   Вы должны получить приблизительно такой ответ:

   ```
   354 Start mail input; end with <CLRF>.<CLRF>
   ```

8. Введите Subject: Test и нажмите клавишу ВВОД.
9. Еще раз нажмите клавишу ВВОД.
10. Введите This is a test message и нажмите клавишу ВВОД.
11. Нажмите клавишу ВВОД, введите точку (.) и нажмите клавишу ВВОД.

    Вы должны получить приблизительно такой ответ:

    ```
    250 2.6.0 <GUID> Queued mail for delivery
    ```

12. Чтобы отключиться от сервера SMTP, введите QUIT и нажмите клавишу ВВОД.

    Вы должны получить приблизительно такой ответ:

    ```
    221 2.0.0 Service closing transmission channel
    ```

13. Чтобы закрыть сеанс Telnet, введите quit и нажмите клавишу ВВОД.

- Если анонимная ретрансляция работает с перебоями, возможно, необходимо изменить частоту отправки сообщений и ограничения по умолчанию на уровне соединителя получения. Дополнительные сведения см. в разделе Регулирование количества сообщений на соединителях получения.

Отправка соединителей в Exchange Server

Статья • 04.04.2023

Exchange использует соединители отправки для исходящих SMTP-подключений с исходных серверов Exchange на конечные почтовые серверы. Соединитель, используемый для отправки сообщений получателю, выбирается на этапе сопоставления маршрутизации. Дополнительные сведения см. в разделе Маршрутизация почты.

Соединители отправки можно создать в транспортной службе на серверах почтовых ящиков и на пограничных транспортных серверах. Соединители отправки хранятся в Active Directory и (по умолчанию) видны всем серверам почтовых ящиков в организации.

> ⓘ **Важно!**
>
> По умолчанию соединители отправки для внешнего потока обработки почты при установке Exchange не существуют. Чтобы включить исходящий поток обработки почты в Интернете, необходимо создать соединитель отправки или подписать пограничный транспортный сервер в организации Exchange. Дополнительные сведения см. в статье **Создание соединителя отправки для отправки почты на интернет-серверы** и **пограничные транспортные серверы**.

Вам не нужно настраивать соединители отправки для обмена почтой между серверами Exchange в одном лесу Active Directory. Для отправки почты на внешние серверы Exchange доступны неявные и невидимые соединители отправки, которые полностью совместимы с топологией сервера Exchange. Эти соединители описаны в разделе Неявные соединители отправки.

Основные параметры соединителей отправки:

- **Тип использования**
- **Параметры сети**. Настройте способ отправки соединителя почты: с помощью DNS или автоматической пересылки всей почты на смарт-узел.
- **Адресные пространства**. Настройте конечные домены, за которые отвечает соединитель отправки.

- **Область.** Настраивает видимость соединителя отправки на другие серверы Exchange в организации.
- **Исходные серверы**. Настройте серверы Exchange, на которых размещен соединитель отправки. Почта, которая должна быть доставлена соединителем отправки, направляется на один из исходных серверов.

На серверах почтовых ящиков для создания соединителей отправки и управления ими можно использовать Центр администрирования Exchange или командную консоль Exchange. На пограничных транспортных серверах можно использовать только командную консоль Exchange.

Отправка изменений соединителя в Exchange Server

Ниже приведены важные изменения отправки соединителей в Exchange 2016 или Exchange 2019 по сравнению с Exchange 2010:

- Вы можете настроить соединители отправки, чтобы перенаправлять исходящую почту через внешнюю службу транспорта. Дополнительные сведения см. в статье Configure Send connectors to proxy outbound mail.
- Параметр *IsCoexistenceConnector* больше недоступен.
- Параметр *LinkedReceiveConnector* больше недоступен.
- Максимальный размер сообщения по умолчанию увеличен до 35 МБ (приблизительно 25 МБ из-за кодировки Base64). Дополнительные сведения см. в статье Размер сообщений и ограничения получателей в Exchange Server.
- Параметр *TlsCertificateName* позволяет указать издателя сертификата и субъекта сертификата. Это помогает защититься от поддельных сертификатов.

Неявные соединители отправки

Хотя соединители отправки не создаются во время установки серверов Exchange, существует специальный *неявный соединитель отправки* с именем соединитель отправки внутри организации. Этот неявный соединитель отправки автоматически доступен, не виден и не требует управления. Соединитель отправки Intra-Organization существует в службах транспорта для отправки почты между службами на локальном сервере Exchange или в службы на отдаленных серверах Exchange в организации. Например:

- Из внешней службы транспорта в службу транспорта.
- Из службы транспорта в службу транспорта на других серверах.
- Из службы транспорта на включенные пограничные транспортные серверы.
- Из службы транспорта в службу транспортной доставки почтовых ящиков.
- Из службы транспортной отправки почтовых ящиков к службе передачи.

Дополнительные сведения см. в статье Mail flow and the transport pipeline.

Типы использования соединителей отправки

Тип использования указывает, для чего используется соединитель отправки. Все типы использования получают одинаковые разрешения.

Тип использования можно указать только при создании соединителя отправки. При использовании Центра администрирования Exchange необходимо выбрать значение **Тип**. Но при использовании командлета **New-SendConnector** в командной консоли Exchange тип использования не требуется (с помощью `-Usage <UsageType>` или `-<UsageType>`).

Тип использования определяет максимальный размер сообщения по умолчанию, который вы можете изменить после создания соединителя.

Доступные типы использования описаны в таблице ниже.

Тип использования	**Максимальный размер сообщения**	**Comments**
Пользовательские	35 МБ	Нет
Internal;	неограниченно	When you create a Send connector of this usage type in the EAC, you can't select **MX record associated with recipient domain**. After you create the connector, you can go to the **Delivery** tab in the properties of the Send connector and select **MX record associated with recipient domain**. Это ограничение отсутствует в командной консоли Exchange. Можно использовать *внутренний* коммутатор и задать *для DNSRoutingEnabled* значение в `$true` командлете **New-SendConnector** .
Интернет	35 МБ	Нет

Тип использования	Максимальный размер сообщения	Comments
Партнер	35 МБ	When you create a Send connector of this usage type in the EAC, you can't select **Route mail through smart hosts** or a smart host authentication mechanism. After you create the connector, you can go to the **Delivery** tab in the properties of the Send connector and select **Route mail through smart hosts** and the smart host authentication mechanism. Это ограничение отсутствует в командной консоли Exchange. Вы можете использовать параметр *Partner* и задать *для DNSRoutingEnabled* `$false` значение и использовать параметры *SmartHosts* и *SmartHostAuthMechanism* в командлете **New-SendConnector** .

Сетевые параметры соединителей отправки

Для каждого соединителя отправки необходимо выбрать один из этих параметров:

- Использовать DNS для маршрутизации почты.
- Использовать один или несколько промежуточных узлов для маршрутизации почты.

Использование DNS для маршрутизации почты.

Если для доставки почты выбрано сопоставление DNS, исходный сервер Exchange соединителя отправки должен сопоставлять записи MX для адресных пространств, настроенных в соединителе. В зависимости от характера соединителя и количества сетевых адаптеров на сервере, соединителю отправки может требоваться доступ к внутреннему или внешнему (общедоступному) DNS-серверу. Вы можете настроить сервер для использования отдельных DNS-серверов для внутренних и внешних DNS-запросов.

- В центре администрирования Exchange в разделе **Серверы**>> выберите сервер и нажмите кнопку **Изменить**✎>**Вкладка подстановки DNS**.
- В командной консоли Exchange используйте параметры *ExternalDNS** и *InternalDNS** в командлете **Set-TransportService** .

Если вы уже настроили отдельные DNS-серверы для внутренних и внешних DNS-запросов, а соединитель отправки направляет почту во внешнее адресное пространство, вам нужно настроить соединитель отправки для использования внешнего DNS-сервера:

- В Центре администрирования Exchange выберите **Использовать параметры внешних DNS-запросов на серверах с ролью транспорта** (в мастере создания соединителя отправки или на вкладке **Доставка** в свойствах существующих соединителей).
- В командной консоли Exchange используйте параметр *UseExternalDNSServersEnabled* в командлетах **New-SendConnector** и **Set-SendConnector** .

Использование промежуточных узлов для маршрутизации почты

При маршрутизации почты через промежуточный узел соединитель отправки пересылает почту на промежуточный узел, который в свою очередь направляет ее на следующий транзитный участок. Маршрутизация через промежуточный узел позволяет отправлять исходящую почту через службу или устройство защиты от спама.

Чтобы добавить один или несколько промежуточных узлов, нужно указать IP-адрес (например, 10.1.1.1), полное доменное имя (FQDN) (например, spamservice.contoso.com) или оба типа значений. Если вы укажете FQDN, исходный сервер Exchange соединителя отправки должен сопоставлять полные доменные имена (записи MX или записи A), используя DNS.

Важной составляющей маршрутизации через промежуточные узлы является используемый ими механизм проверки подлинности. Доступные механизмы проверки подлинности описаны в таблице ниже.

Механизм проверки подлинности	**Описание**
Нет (`None`)	Проверка подлинности не выполняется. Например, доступ к промежуточному узлу ограничен исходным IP-адресом.
Обычная проверка подлинности (`BasicAuth`)	Обычная проверка подлинности. Требуется имя пользователя и пароль. Имя пользователя и пароль отправляются в виде ясного текста.

Механизм проверки подлинности	Описание
Предлагать обычную проверку подлинности только после запуска TLS (`BasicAuthRequireTLS`)	Обычная проверка подлинности с шифрованием TLS. Сертификат сервера на промежуточном узле должен содержать полное доменное имя промежуточного узла, указанное в соединителе отправки. Соединитель отправки устанавливает сеанс TLS, отправляя команду **STARTTLS** на промежуточный узел, и только после этого выполняет обычную проверку подлинности. Для взаимной проверки подлинности TLS также необходим сертификат клиента.
проверка подлинности Exchange Server (`ExchangeServer`)	Программный интерфейс универсальных служб защиты (GSSAPI) и взаимная проверка подлинности GSSAPI.
Внешняя защита (`ExternalAuthoritative`)	Предполагается, что используется внешний механизм защиты соединения, не входящий в состав Exchange. Подключение может быть связью IPsec или виртуальной частной сетью. Кроме того, серверы могут находиться в доверенной, физически контролируемой сети.

Адресные пространства соединителей отправки

Адресное пространство определяет конечные домены, которые обслуживает соединитель отправки. Только в эти домены почта направляется через соединитель отправки.

Доступные адресные пространства SMTP описаны в таблице ниже.

Адресное пространство	Объяснение
`*`	Почта направляется через соединитель отправки во все домены.
Домен (например, `contoso.com`)	Почта направляется через соединитель отправки в указанный домен, но не в дочерние домены.

Адресное пространство	Объяснение
Домен и поддомены (например, `*.contoso.com`)	Почта направляется через соединитель отправки в указанный и все дочерние домены.
`--`	Почта направляется через соединитель отправки во все обслуживаемые домены в организации Exchange. Это значение доступно только для соединителей отправки на пограничных транспортных серверах, которые отправляют почту во внутреннюю организацию Exchange.

Вы также можете настроить значения **Тип** и **Стоимость** адресного пространства.

На пограничных транспортных серверах значение **Type** должно иметь значение `SMTP`. На серверах почтовых ящиков можно также использовать типы пространства адресов, отличные от SMTP, например `X400` или любую другую текстовую строку. Адреса X.400 должны быть совместимыми с RFC 1685 (например, `o=MySite;p=MyOrg;a=adatum;c=us`), но другие значения **type** принимают любое текстовое значение для адресного пространства. If you specify a non-SMTP address space type, the Send connector must use smart host routing, and SMTP is used to send messages to the smart host. Delivery Agent connectors and Foreign connectors send non-SMTP messages to non-SMTP servers without using SMTP. Дополнительные сведения см. в разделе Агенты доставки и соединители агента доставки и внешние соединители.

Значение **Стоимость** адресного пространства используется для оптимизации потока обработки почты и отказоустойчивости, когда одинаковые адресные пространства настроены для нескольких соединителей отправки на разных исходных серверах. Чем ниже значение приоритета, тем предпочтительнее соединитель отправки.

Соединитель, используемый для отправки сообщений получателю, выбирается на этапе сопоставления маршрутизации. Выбирается соединитель отправки, адресное пространство которого максимально соответствует адресу электронной почты получателя и значение приоритета которого наиболее низкое.

Например, предположим, что получатель имеет значение julia@marketing.contoso.com. Если для домена *.contoso.com настроен соединитель отправки, сообщение направляется через этот соединитель. В противном случае сообщение направляется через соединитель, настроенный для *. Если несколько соединителей отправки на одном сайте Active Directory настроены для *.contoso.com, выбран соединитель со значением более низкого приоритета.

Область действия соединителя отправки

Исходные серверы для соединителя отправки определяют конечный сервер Exchange для почты, которая должна быть направлена через соединитель отправки. Область действия определяет видимость соединителя в организации Exchange.

По умолчанию соединители отправки видны всем серверам Exchange во всем лесу Active Directory и используются при принятии решений о маршрутизации. Однако можно ограничить область соединителя отправки, чтобы он был виден только для других серверов Exchange на том же сайте Active Directory. Соединитель отправки невидим для серверов Exchange на других сайтах Active Directory и не используется в их решениях о маршрутизации. Соединитель отправки, ограниченный таким образом, называется *областью действия*.

Чтобы настроить область действия соединителя отправки в Центре администрирования Exchange, выберите **Соединитель отправки с заданной областью** в разделе **Адресное пространство** мастера создания соединителя отправки или на вкладке **Определение области** в свойствах существующих соединителей отправки. В командной консоли Exchange параметр *IsScopedConnector используется* в командлетах **New-SendConnector** и **Set-SendConnector** .

Разрешения соединителя отправки

Когда соединитель отправки устанавливает соединение с целевым почтовым сервером, разрешения на отправку соединителя определяют типы заголовков, которые можно отправлять в сообщениях. Недопустимые заголовки удаляются из сообщений.

Разрешения на отправку соединителей назначаются известными субъектами безопасности. Субъекты безопасности включают учетные записи пользователей, учетные записи компьютеров и группы безопасности (объекты, идентифицируемые идентификатором безопасности или идентификатором безопасности, которым могут быть назначены разрешения). По умолчанию одни и те же субъекты безопасности с одинаковыми разрешениями назначаются всем соединителям отправки независимо от типа использования, выбранного при создании соединителя. Чтобы изменить разрешения по умолчанию для соединителя отправки, необходимо использовать **командлеты Add-ADPermission** и **Remove-ADPermission** в командной консоли Exchange.

Доступные разрешения соединителей отправки описаны в таблице ниже.

Разрешение	Кому назначено	Описание

`ms-Exch-Send-Headers-Forest`	`<Domain>\Exchange Servers`
	
	`MS Exchange\Edge Transport Servers`
	
	`MS Exchange\Hub Transport Servers`
		Управляет хранением заголовков лесов Exchange в сообщениях. Имена заголовков лесов начинаются с **X-MS-Exchange-Forest-**. Если разрешение не предоставлено, все заголовки лесов удаляются из сообщений.

`ms-Exch-Send-Headers-Organization`	`<Domain>\Exchange Servers`
	
	`MS Exchange\Edge Transport Servers`
	
	`MS Exchange\Hub Transport Servers`
		Управляет сохранением заголовков организаций Exchange в сообщениях. Имена заголовков организаций начинаются с **X-MS-Exchange-Organization-**. Если разрешение не предоставлено, все заголовки организации удаляются из сообщений.

`ms-Exch-Send-Headers-Routing`	`NT AUTHORITY\ANONYMOUS LOGON`
	
	`<Domain>\Exchange Servers`
	
	`MS Exchange\Edge Transport Servers`
	
	`MS Exchange\Externally Secured Servers`
	
	`MS Exchange\Hub Transport Servers`
	
	`MS Exchange\Legacy Exchange Servers`
	
	`MS Exchange\Partner Servers`
		Управляет сохранением заголовков **RECEIVED** в сообщениях. Если разрешение не предоставлено, все полученные заголовки удаляются из сообщений.

Разрешение	Кому назначено	Описание

`ms-Exch-SMTP-Send-Exch50`	`<Domain>\Exchange Servers`
	
	`MS Exchange\Edge Transport Servers`
	
	`MS Exchange\Externally Secured Servers`
	
	`MS Exchange\Hub Transport Servers`
	
	`MS Exchange\Legacy Exchange Servers`
		Позволяет исходному серверу Exchange отправлять команды **XEXCH50** через соединитель отправки. Большой двоичный объект **X-EXCH50** использовался старыми версиями Exchange (Exchange 2003 и более ранними) для хранения данных Exchange в сообщениях (например, вероятности нежелательной почты).
		
		If this permission isn't granted, and messages contain the **X-EXCH50** BLOB, the Exchange server sends the message without the **X-EXCH50** BLOB.

`ms-Exch-SMTP-Send-XShadow`	`<Domain>\Exchange Servers`
	
	`MS Exchange\Edge Transport Servers`
	
	`MS Exchange\Hub Transport Servers`
		Это разрешение зарезервировано для внутреннего использования в корпорации Майкрософт.

Примечание. Имена разрешений, содержащиеся `ms-Exch-Send-Headers-` в составе функции *брандмауэра заголовков* . Дополнительные сведения см. в разделе Брандмауэр заголовков.

Действия с разрешениями соединителя отправки

Чтобы просмотреть разрешения, назначенные субъектам безопасности соединителя отправки, используйте следующий синтаксис в командной консоли Exchange:

PowerShell

```
Get-ADPermission -Identity <SendConnector> [-User <SecurityPrincipal>] |
where {($_.Deny -eq $false) -and ($_.IsInherited -eq $false)} | Format-Table
User,ExtendedRights
```

Например, чтобы просмотреть разрешения, назначенные всем субъектам безопасности соединителя отправки To Fabrikam.com, выполните следующую

команду:

```
PowerShell

Get-ADPermission -Identity "To Fabrikam.com" | where {($_.Deny -eq $false) -
and ($_.IsInherited -eq $false)} | Format-Table User,ExtendedRights
```

Чтобы просмотреть разрешения, назначенные только субъекту `NT AUTHORITY\ANONYMOUS LOGON` безопасности в соединителе Отправки с именем Fabrikam, выполните следующую команду:

```
PowerShell

Get-ADPermission -Identity "To Fabrikam.com" -User "NT AUTHORITY\ANONYMOUS
LOGON" | where {($_.Deny -eq $false) -and ($_.IsInherited -eq $false)} |
Format-Table User,ExtendedRights
```

Чтобы добавить разрешения для субъекта безопасности, используйте следующий синтаксис:

```
PowerShell

Add-ADPermission -Identity <SendConnector> -User <SecurityPrincipal> -
ExtendedRights "<Permission1>","<Permission2>"...
```

Чтобы удалить разрешения субъекта безопасности, используйте следующий синтаксис:

```
PowerShell

Remove-ADPermission -Identity <SendConnector> -User <SecurityPrincipal> -
ExtendedRights "<Permission1>","<Permission2>"...
```

Создание соединителя отправки в Exchange Server для отправки почты в Интернет

Статья • 04.04.2023

При установке первого сервера Exchange Server 2016 или Exchange 2019 сервер не может отправлять почту за пределы организации Exchange. Чтобы отправлять почту за пределы своей организации Exchange, необходимо создать соединитель отправки.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Отправка соединителей" в разделе Разрешения потока обработки почты .
- Если вы начинаете установку, см. статью Развертывание новой установки Exchange Server. После установки можно выполнить действия, описанные в этом разделе, чтобы создать соединитель отправки через Интернет.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Создание соединителя отправки для отправки почты в Интернет

Пока вы не создадите соединитель отправки, почта не сможет передаваться из Exchange в Интернет. Исключением является установка пограничного транспорта в

сети периметра и подписка на пограничный транспорт в организации Exchange. Дополнительные сведения см. в разделе Пограничные транспортные серверы.

Дополнительные сведения о соединителях, а также подходящих и неподходящих случаях для их использования вместо пограничных транспортных серверов см. в статье Соединители отправки.

Создание соединителя отправки через Интернет с помощью EAC

1. В EAC перейдите к разделу**Отправка соединителей** потока >**обработки почты**и нажмите кнопку Добавить ➕ Запустится мастер **создания соединителя отправки**.

2. На первой странице укажите следующие сведения:

   - **Имя**. Введите описательное имя соединителя отправки (например, в Интернет).

   - **Тип**: выберите **Интернет**.

   По завершении нажмите кнопку **Далее**.

3. Убедитесь, что на следующей странице выбран параметр **Запись MX, связанная с доменом получателя**. Это означает, что соединитель использует DNS в Интернете для маршрутизации почты, в отличие от маршрутизации всей исходящей почты на интеллектуальный узел. Сведения о создании соединителя отправки, использующего маршрутизацию интеллектуальных узлов, см. в статье Создание соединителя отправки для маршрутизации исходящей почты через интеллектуальный узел.

   По завершении нажмите кнопку **Далее**.

4. На следующей странице введите указанные ниже сведения.

   - В разделе **Адресное пространство** нажмите кнопку **Добавить**➕ В появившемся диалоговом окне **Добавление домена** в поле **Полное доменное имя (FQDN)** введите звездочку (*) и нажмите кнопку **Сохранить**. Это значение указывает, что соединитель отправки применяется к сообщениям, которые адресованы всем внешним доменам.

   - Параметр **Соединитель отправки с заданной областью** важен, если серверы Exchange в вашей организации установлены на нескольких

сайтах Active Directory:

- Если не выбрать **соединитель отправки с областью** действия, соединитель можно использовать на всех транспортных серверах (серверах почтовых ящиков Exchange 2013 или более поздних версий и транспортных серверах концентратора Exchange 2010) во всем лесу Active Directory. Это значение используется по умолчанию.
- Если включить параметр **Соединитель отправки с заданной областью**, соединитель смогут использовать только другие транспортные серверы на том же сайте Active Directory.

По завершении нажмите кнопку **Далее**.

5. На следующей странице в разделе **Исходный сервер** нажмите кнопку **Добавить**➕ В появившемся диалоговом окне **Выбор сервера** выберите один или несколько серверов почтовых ящиков, которые нужно использовать для отправки почты в Интернет. Если в вашей среде несколько серверов почтовых ящиков, выберите те, которые могут маршрутизировать почту в Интернет. Если у вас только один сервер почтовых ящиков, выберите его. Выбрав по крайней мере один сервер почтовых ящиков, нажмите кнопку **Добавить**, кнопку **ОК**, а затем — кнопку **Готово**.

Созданный соединитель появится в списке соединителей отправки. Сведения о том, как настроить соединитель отправки, чтобы он передавал исходящую почту через внешнюю службу транспорта, используя прокси-сервер, см. в статье Configure Send connectors to proxy outbound mail.

Создание соединителя отправки через Интернет с помощью командной консоли Exchange

1. Запустите командную консоль Exchange. Дополнительные сведения см. в разделе Открытие командной консоли Exchange.
2. Используйте следующий синтаксис.

```
PowerShell

New-SendConnector -Name <Name> -AddressSpaces * -Internet [-
SourceTransportServer <fqdn1>,<fqdn2>...]
```

В этом примере создается соединитель отправки через Интернет с именем "В Интернет" со следующими свойствами:

- Тип использования — "Интернет".
- Соединитель отправки использует маршрутизацию DNS. Мы не используем параметр *DNSRoutingEnabled* , и значение по умолчанию — `$true`.
- Соединитель отправки предназначен для всех внешних доменов (*).
- Исходным сервером является локальный сервер Exchange. Мы не используем параметр *SourceTransportServer* , а значением по умолчанию является локальный сервер Exchange Server.
- Область соединителя отправки не ограничена локальным сайтом Active Directory. Мы не используем параметр *IsScopedConnector* , а значение по умолчанию — `$false`.

PowerShell

```
New-SendConnector -Name "To internet" -AddressSpaces * -Internet
```

Дополнительные сведения о других параметрах см. в статье New-SendConnector.

> ⓘ **Примечание**
>
> Чтобы настроить отправку соединителя для прокси-сервера исходящей почты через службу транспорта переднего плана, добавьте `-FrontEndProxyEnabled $true` в команду . Дополнительные сведения см. в статье **Configure Send connectors to proxy outbound mail**.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно создали соединитель отправки, который отправляет почту в Интернет, создайте и отправьте сообщение из внутреннего почтового ящика внешнему получателю, а затем убедитесь, что получатель получает сообщение.

Вы также можете включить ведение журнала протокола для соединителя отправки и просматривать сведения в журнале. Дополнительные сведения см. в разделе Ведение журнала протокола.

Создание соединителя отправки для маршрутизации исходящей почты через промежуточный узел

Статья • 04.04.2023

Вместо того чтобы направлять все исходящие сообщения непосредственно в Интернет, вам может потребоваться направлять исходящую почту организации через сторонний промежуточный узел. Например, в вашей организации может использоваться прибор, сканирующий исходящую почту на спам и вредоносные программы.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Если вы начинаете установку, см. статью Развертывание новой установки Exchange Server. После установки можно выполнить действия, описанные в этом разделе, чтобы создать исходящий соединитель.
- Промежуточный узел, описываемый в этой статье, должен использовать протокол SMTP для передачи сообщений. Если это не так, необходимо использовать соединитель агента доставки или внешний соединитель. Дополнительные сведения см. в статьях Delivery Agents and Delivery Agent Connectors и Foreign Connectors.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Отправка соединителей" в разделе Разрешения потока обработки почты .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Создание соединителя отправки, использующего маршрутизацию через промежуточный узел, с помощью Центра администрирования Exchange

1. В EAC перейдите к разделу**Отправка соединителей** потока >**обработки почты**и нажмите кнопку Добавить ➕ Запустится мастер **создания соединителя отправки**.

2. На первой странице укажите следующие сведения:

   - **Имя**. Введите описательное имя соединителя отправки, например Интеллектуальный узел в Интернет.

   - **Тип**: выберите описательное значение. Пример: **Интернет** или **Настраиваемый**. Дополнительные сведения о типах использования соединителей отправки см. в разделе Типы использования соединителей отправки.

   По завершении нажмите кнопку **Далее**.

3. На следующей странице выберите **Маршрутизировать почту через смарт-узлы** и нажмите кнопку **Добавить**➕ В открывшемся диалоговом окне **Добавление промежуточного узла** определите промежуточный узел, используя одно из следующих значений:

   - **IP-адрес**: например, 192.168.3.2.

   - **Полное доменное имя (FQDN):** например, securitydevice01.contoso.com. Обратите внимание, что исходные серверы Exchange для соединителя отправки должны иметь возможность разрешать интеллектуальный узел в DNS с помощью этого полного доменного имени.

   По завершении нажмите кнопку **Сохранить**.

4. Вы можете указать несколько промежуточных узлов, повторив этап 3. По завершении нажмите кнопку **Далее**.

5. На следующей странице, в разделе **Перенаправлять почту через промежуточные узлы**, выберите способ проверки подлинности, необходимый промежуточному узлу. Допустимые значения:

Механизм проверки подлинности	Описание
Нет	Проверка подлинности не выполняется. Например, доступ к промежуточному узлу ограничен исходным IP-адресом.
Обычная проверка подлинности	Обычная проверка подлинности. Требуется имя пользователя и пароль. Имя пользователя и пароль отправляются в виде ясного текста.
Предлагать обычную проверку подлинности только после запуска TLS	Обычная проверка подлинности с шифрованием TLS. Сертификат сервера на промежуточном узле должен содержать полное доменное имя промежуточного узла, указанное в соединителе отправки.
Проверка подлинности Exchange Server	Программный интерфейс универсальных служб защиты (GSSAPI) и взаимная проверка подлинности GSSAPI.
Внешняя защита	Предполагается, что используется внешний механизм защиты соединения, не входящий в состав Exchange. Подключение может быть связью IPsec или виртуальной частной сетью. Кроме того, серверы могут находиться в доверенной, физически контролируемой сети.

По завершении нажмите кнопку **Далее**.

6. На следующей странице в разделе **Адресное пространство** нажмите кнопку **Добавить**➕ В открывшемся диалоговом окне **Добавление домена** введите следующие сведения:

   - **Тип**: убедитесь, что smtp введен.
   - **Полное доменное имя (FQDN).** Введите звездочку (*), чтобы указать, что соединитель отправки применяется к сообщениям, адресованным всем внешним доменам. Вы также можете указать определенный внешний домен (например, contoso.com) либо домен и все его поддомены (например, *.contoso.com).
   - **Затраты**: убедитесь, что введено значение 1. Чем ниже значение, тем предпочтительнее будет этот маршрут для указанных доменов.

   По завершении нажмите кнопку **Сохранить**.

7. На предыдущей странице имеется параметр **Соединитель отправки с заданной областью**, который важен, если серверы Exchange установлены на нескольких сайтах Active Directory в организации:

   - Если не выбрать **соединитель отправки с областью** действия, соединитель можно использовать на всех транспортных серверах (серверах почтовых ящиков Exchange 2013 или более поздних версий и транспортных серверах концентратора Exchange 2010) во всем лесу Active Directory. Это значение используется по умолчанию.

   - Если включить параметр **Соединитель отправки с заданной областью**, соединитель смогут использовать только другие транспортные серверы на том же сайте Active Directory.

   По завершении нажмите кнопку **Далее**.

8. На следующей странице в разделе **Исходный сервер** нажмите кнопку **Добавить**➕ В открывшемся диалоговом окне **Выбор сервера** выберите один или несколько серверов почтовых ящиков, которые вы хотите использовать для отправки исходящей почты на промежуточный узел. Если в вашей среде несколько серверов почтовых ящиков, выберите те из них, которые могут направлять почту на промежуточный узел. Если у вас только один сервер почтовых ящиков, выберите его. Выбрав по крайней мере один сервер почтовых ящиков, нажмите кнопку **Добавить**, кнопку **ОК**, а затем — кнопку **Готово**.

Созданный соединитель появится в списке соединителей отправки.

Создание соединителя отправки, использующего маршрутизацию через промежуточный узел, с помощью командной консоли Exchange

1. Запустите командную консоль Exchange. Дополнительные сведения см. в разделе Открытие командной консоли Exchange.

2. Используйте следующий синтаксис:

```
PowerShell

New-SendConnector -Name <Name> -AddressSpaces * -Custom -
DnsRoutingEnabled $false -SmartHosts <SmartHost1>[,<SmartHost2>...] [-
```

```
SourceTransportServer <fqdn1>,<fqdn2>...]
```

В этом примере создается соединитель отправки в Интернет с именем Smart host to Internet и следующими свойствами:

- Тип использования — "Настраиваемый".
- Соединитель отправки использует маршрутизацию интеллектуальных узлов (параметр *DNSRoutingEnabled* имеет значение `$false`). IP-адрес промежуточного узла — 192.168.3.2, а проверка подлинности не выполняется, так как промежуточный узел прослушивает подключения только от ограниченного списка исходных серверов.
- Соединитель отправки предназначен для всех внешних доменов (*). Значение `*` эквивалентно значению `"SMTP:*;1"`, где тип адресного пространства — `SMTP`, а значение стоимости адресного пространства — `1`.
- Исходным сервером является локальный сервер Exchange. Мы не используем параметр *SourceTransportServer* , а значением по умолчанию является локальный сервер Exchange Server.
- Область соединителя отправки не ограничена локальным сайтом Active Directory. Мы не используем параметр *IsScopedConnector* , а значение по умолчанию — `$false`. Соединитель отправки могут использовать все транспортные серверы Exchange в лесу Active Directory.

PowerShell

```
New-SendConnector -Name "Smart host to Internet" -AddressSpaces * -
Custom -DNSRoutingEnabled $false -SmartHosts 192.168.3.2 -
SmartHostAuthMechanism None
```

Дополнительные сведения о других параметрах см. в статье New-SendConnector.

Как проверить, все ли получилось?

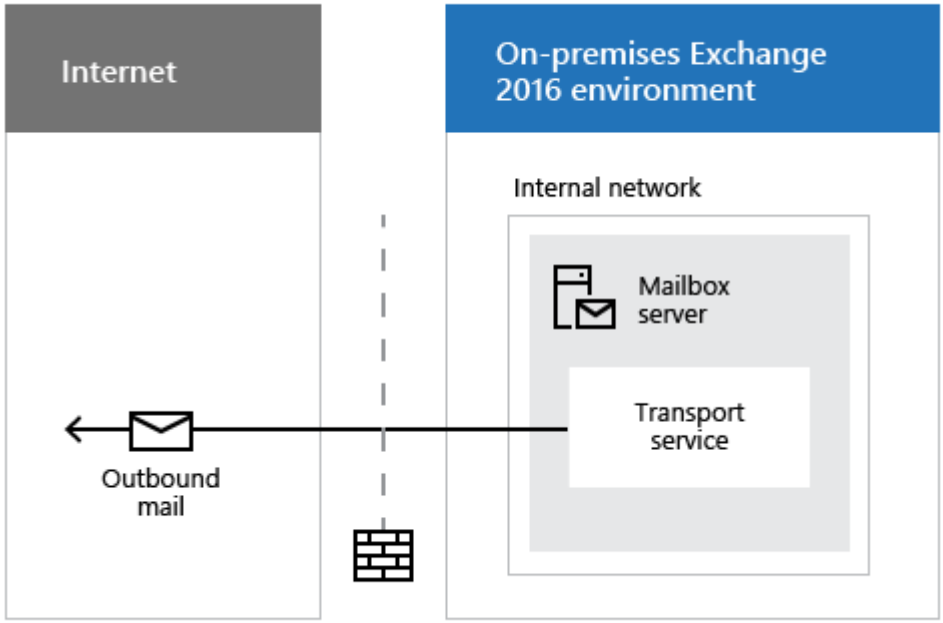
Чтобы убедиться, что вы успешно создали соединитель отправки, направляющий исходящую почту через промежуточный узел, отправьте сообщение от пользователя в организации на внешний домен, обслуживаемый соединителем отправки.

Вы также можете включить ведение журнала протокола для соединителя отправки и просматривать сведения в журнале. Дополнительные сведения см. в разделе Ведение журнала протокола.

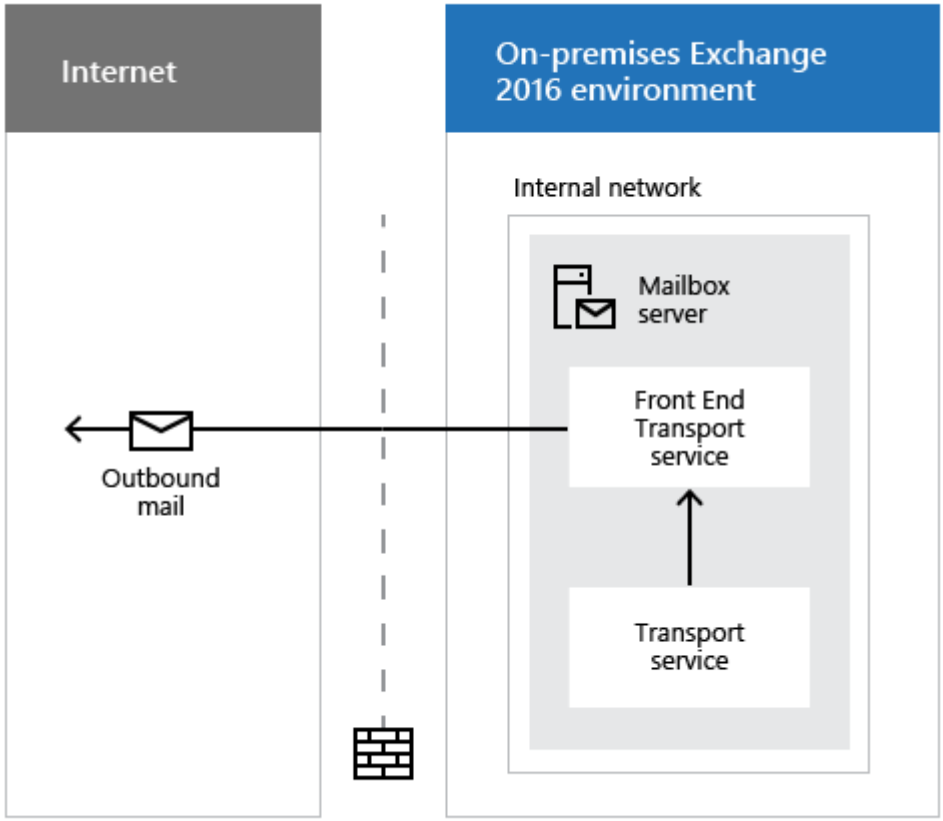
Настройка соединителей отправки на проксирование исходящей почты

Статья • 04.04.2023

При создании соединителей отправки исходящая почта проходит через соединитель отправки в службе транспорта на серверах почтовых ящиков, как показано ни приведенной ниже схеме.



Однако вы можете настроить соединитель отправки так, чтобы он ретранслировал, или *передавал с помощью прокси-сервера*, исходящую почту через внешнюю транспортную службу на сервере почтовых ящиков, как показано на приведенной ниже схеме.



По умолчанию вся входящая почта поступает в организацию Exchange через транспортную службу переднего плана, а служба транспорта переднего плана отправляет входящую почту в транспортную службу. Дополнительные сведения см. в разделе Поток обработки почты и конвейер транспорта.

При настройке соединителя отправки для прокси-сервера исходящей почты через службу транспорта переднего плана соединитель получения с именем "*Имя> сервера внешнего< почтового ящика* исходящего прокси-сервера" в службе внешнего транспорта прослушивает эти исходящие сообщения из транспортной службы, а затем служба внешнего транспорта отправляет сообщения в Интернет.

Что нужно знать перед началом работы?

- Предполагаемое время для завершения: менее пяти минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Отправка соединителей" в разделе Разрешения потока обработки почты .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Настройка соединителей отправки на передачу исходящей почты через внешнюю службу транспорта с использованием прокси-сервера

Настройка соединителей отправки на использование прокси-сервера для передачи исходящей почты с помощью Центра администрирования Exchange

В Центре администрирования Exchange можно настраивать только существующие соединители отправки на передачу исходящей почты с использованием прокси-сервера.

1. В EAC перейдите к разделу Отправка**соединителей** потока >**обработки почты**, выберите соединитель Отправить и щелкните ✎

2. На вкладке **Общие**, в разделе **Состояние соединителя**, выберите параметр **Прокси через сервер клиентского доступа**, а затем нажмите кнопку **Сохранить**.

Настройка соединителей отправки на использование прокси-сервера для передачи исходящей почты с помощью PowerShell

В командной консоли Exchange можно настраивать как новые, так и существующие соединители отправки на передачу исходящей почты с использованием прокси-сервера.

Сведения о том, как открыть командную консоль Exchange, см. в статье Open the Exchange Management Shell.

- Чтобы настроить новый соединитель отправки для исходящей почты прокси-сервера, добавьте `-FrontEndProxyEnabled $true` в команду **New-SendConnector** .

- Чтобы настроить существующий соединитель отправки на передачу исходящей почты с использованием прокси-сервера, выполните следующую команду:

  PowerShell

  ```
  Set-SendConnector <Send connector identity>  -FrontEndProxyEnabled $true
  ```

  В этом примере показано, как настроить существующий соединитель отправки с именем Contoso.com Outbound на передачу исходящей почты с использованием прокси-сервера.

  PowerShell

  ```
  Set-SendConnector "Contoso.com Outbound" -FrontendProxyEnabled $true
  ```

Как проверить, что все получилось?

Чтобы убедиться, что соединитель отправки настроен на передачу исходящей почты с использованием прокси-сервера, выполните одну из следующих процедур:

- В EAC перейдите к разделу Отправка**соединителей** потока >**обработки почты**, выберите соединитель Отправить и щелкните ✎ Убедитесь, что на вкладке **Общие**, в разделе **Состояние соединителя** выбран параметр **Прокси через сервер клиентского доступа**.

- В командной консоли Exchange выполните следующую команду:

  PowerShell

  ```
  Get-SendConnector | Format-Table -Auto Name,FrontEndProxyEnabled
  ```

  Убедитесь, что значение **FrontEndProxyEnabled** равно `True` соединителю Отправки.

Ведение журнала протокола в Exchange Server

Статья • 04.04.2023

При ведении журнала протокола записываются разговоры SMTP между серверами обмена сообщениями и службами Exchange в транспортном конвейере в рамках доставки сообщений. Ведение журнала протокола можно использовать для диагностики неполадок, связанных с потоком обработки почты. Разговоры SMTP, которые могут быть записаны в журнале протокола, происходят в:

- соединителях отправки и получения в службе транспорта на серверах почтовых ящиков;
- соединителях отправки и получения в службе транспорта на пограничных транспортных серверах;
- соединителях получения во внешней службе транспорта на серверах почтовых ящиков;
- неявном и невидимом соединителе отправки внутри организации в службе транспорта на серверах почтовых ящиков;
- неявном и невидимом соединителе отправки внутри организации во внешней службе транспорта на серверах почтовых ящиков;
- неявном и невидимом соединителе отправки внутри организации в службе отправки транспорта почтовых ящиков на серверах почтовых ящиков;
- неявном и невидимом соединителе получения доставки в почтовые ящики в службе доставки транспорта почтовых ящиков на серверах почтовых ящиков.

По умолчанию ведение журнала протокола включено для:

- Соединитель получения по умолчанию с именем Default Frontend *<ServerName>* в транспортной службе переднего плана на серверах почтовых ящиков.
- неявного и невидимого соединителя отправки во внешней службе транспорта на серверах почтовых ящиков.

Для всех остальных соединителей ведение журнала протокола отключено по умолчанию. Его потребуется включить отдельно для каждого соединителя. Вы можете настраивать остальные параметры ведения журнала протокола для всех

соединителей получения или отправки в каждой отдельной службе транспорта на сервере Exchange. Все соединители получения в службе транспорта используют одни и те же файлы и параметры журнала протокола. Эти файлы и параметры отделены от файлов и параметров журнала протокола для соединителя отправки в той же службе транспорта на сервере Exchange.

По умолчанию Exchange использует циклическое ведение журнала, чтобы ограничить журнал протокола в зависимости от размера файла и возраста файла, чтобы контролировать место на жестком диске, используемое файлами журнала. Сведения о настройке ведения журнала протокола см. в разделе Настройка ведения журнала протокола.

Структура файлов журнала протокола

По умолчанию файлы протокола размещаются в следующих папках:

- Внешняя служба транспорта на серверах почтовых ящиков:
  - **Соединители получения**: `%ExchangeInstallPath%TransportRoles\Logs\FrontEnd\ProtocolLog\SmtpReceive`
  - **Отправка соединителей**: `%ExchangeInstallPath%TransportRoles\Logs\FrontEnd\ProtocolLog\SmtpSend`
- Транспортная служба на серверах почтовых ящиков:
  - **Соединители получения**: `%ExchangeInstallPath%TransportRoles\Logs\Hub\ProtocolLog\SmtpReceive`
  - **Отправка соединителей**: `%ExchangeInstallPath%TransportRoles\Logs\Hub\ProtocolLog\SmtpSend`
- Служба доставки транспорта почтовых ящиков на серверах почтовых ящиков (**соединители получения**): `%ExchangeInstallPath%TransportRoles\Logs\Mailbox\ProtocolLog\SmtpReceive\Delivery`
- Служба отправки транспорта почтовых ящиков на серверах почтовых ящиков (**соединители отправки**): `%ExchangeInstallPath%TransportRoles\Logs\Mailbox\ProtocolLog\SmtpSend\Submission`

Примечание. Ведение журнала протоколов для сообщений о побочных эффектах, которые отправляются после доставки сообщений в почтовые ящики, происходит в `%ExchangeInstallPath%TransportRoles\Logs\Mailbox\ProtocolLog\SmtpSend\Delivery`. Например, сообщение, доставленное в почтовый ящик, активирует правило папки "Входящие", которое перенаправляет сообщение другому получателю.

- Транспортная служба на пограничных транспортных серверах:
  - **Соединители получения**: `%ExchangeInstallPath%TransportRoles\Logs\Edge\ProtocolLog\SmtpReceive`
  - **Отправка соединителей**: `%ExchangeInstallPath%TransportRoles\Logs\Edge\ProtocolLog\SmtpSend`

Соглашение об именовании для файлов журнала — для `SENDyyyymmddhh-nnnn.log` соединителей отправки и `RECVyyyymmddhh-nnnn.log` для соединителей получения. Заполнители обозначают следующее:

- *yyymmddhh* — это дата создания файла журнала в формате UTC. *гггг* = год, *мм* = месяц, *дд* = день и *чч* = час.
- *nnnn* — это номер экземпляра, начинающийся со значения 1 каждый час.

Данные записываются в файл журнала, пока не будет достигнут его максимальный размер. Затем открывается новый файл журнала с увеличенным номером экземпляра (-1 для первого, -2 для второго и т. д.) При циклическом ведении журнала самые старые файлы журнала удаляются при соблюдении любого из следующих условий:

- достигнут максимальный срок хранения файла журнала;
- достигнут максимальный размер папки журнала протокола.

Файлы журнала протокола представляют собой текстовые файлы в формате данных с разделителями-запятыми (CSV). Каждый файл журнала протокола снабжен заголовком, содержащим следующие сведения:

- **#Software**: значение равно `Microsoft Exchange Server`.
- **#Version**: номер версии сервера Exchange Server, создавшего файл журнала отслеживания сообщений. Значение использует формат `15.01.nnnn.nnn`.
- **#Log-Type**: значение равно `SMTP Receive Protocol Log` или `SMTP Send Protocol Log`.

- **#Date**: дата и время создания файла журнала в формате UTC. Дата-время в формате UTC представлено в формате даты и времени ISO 8601: *гггг-мм-дд*T*чч:мм:ss.fff*Z, где *гггг* = год, *мм* = месяц, *дд* = день, T указывает начало компонента времени, *чч* = час, *мм* = минута, *ss* = секунда, *fff* = доли секунды, а Z обозначает Zulu, что является еще одним способом обозначения UTC.
- **#Fields**: имена полей с разделителями-запятыми, используемые в файлах журнала протокола.

Поля журнала протокола

В каждой строке журнала протокола хранится одно событие протокола SMTP. Данные в каждой строке сгруппированы по полям, а поля разделены запятыми. В приведенной ниже таблице представлены поля, используемые в журнале протокола.

Имя поля	Описание
date-time	Дата и время события протокола в формате UTC. Дата-время в формате UTC представлено в формате даты и времени ISO 8601: *гггг-мм-дд*T*чч:мм:ss.fff*Z, где *гггг* = год, *мм* = месяц, *дд* = день, T указывает начало компонента времени, *чч* = час, *мм* = минута, *ss* = секунда, *fff* = доли секунды, а Z обозначает Zulu, что является еще одним способом обозначения UTC.
connector-id	Различающееся имя (DN) соединителя, связанного с событием SMTP.
session-id	Значение GUID, уникальное для каждого сеанса SMTP, но одинаковое для каждого события, связанного с этим сеансом.
sequence-number	Значение счетчика, которое начинается с 0 и увеличивается на единицу для каждого события в рамках одного SMTP-сеанса.
local-endpoint	Локальная конечная точка SMTP-сеанса. Он состоит из IP-адреса и номера TCP-порта, отформатированного как <*IP-адрес*>: <*порт*>.
remote-endpoint	Удаленная конечная точка SMTP-сеанса. Он состоит из IP-адреса и номера TCP-порта, отформатированного как <*IP-адрес*>: <*порт*>.
event	Одиночный символ, представляющий событие протокола. Допустимые значения: `+`:Подключения `-`:Отключите `>`:Отправить `<`:Получить `*`:Информация

Имя поля	Описание
data	Текстовые данные, связанные с SMTP-событием.
context	Дополнительные содержательные сведения, которые могут быть связаны с SMTP-событием.

Один разговор SMTP, представляющий отправку или получение одного электронного сообщения, создает несколько событий SMTP. Каждое событие записывается в отдельной строке журнала протокола. В любой момент на сервере Exchange происходит множество разговоров SMTP. При этом в журнале протокола попеременно создаются записи из разных разговоров SMTP. С помощью полей **session-id** и **sequence-number** можно отсортировать записи в журнале протокола по разговорам SMTP.

Настройка ведения журнала протокола в Exchange Server

Статья • 04.04.2023

При ведении журнала протокола записываются разговоры SMTP между серверами обмена сообщениями и службами Exchange в транспортном конвейере в рамках доставки сообщений.

Для журналов протокола всех соединителей отправки и получения на сервере Exchange доступны следующие параметры:

- Указание расположения файлов журнала протокола. Расположения по умолчанию:
  - Внешняя служба транспорта на серверах почтовых ящиков:
  - **Соединители получения**: `%ExchangeInstallPath%TransportRoles\Logs\FrontEnd\ProtocolLog\SmtpReceive`
  - **Отправка соединителей**: `%ExchangeInstallPath%TransportRoles\Logs\FrontEnd\ProtocolLog\SmtpSend`
  - Транспортная служба на серверах почтовых ящиков:
  - **Соединители получения**: `%ExchangeInstallPath%TransportRoles\Logs\Hub\ProtocolLog\SmtpReceive`
  - **Отправка соединителей**: `%ExchangeInstallPath%TransportRoles\Logs\Hub\ProtocolLog\SmtpSend`
  - Служба доставки транспорта почтовых ящиков на серверах почтовых ящиков (**соединители получения**): `%ExchangeInstallPath%TransportRoles\Logs\Mailbox\ProtocolLog\SmtpReceive\Delivery`
  - Служба отправки транспорта почтовых ящиков на серверах почтовых ящиков (**соединители отправки**): `%ExchangeInstallPath%TransportRoles\Logs\Mailbox\ProtocolLog\SmtpSend\Submission`

    Примечание. Ведение журнала протоколов для сообщений о побочных эффектах, которые отправляются после доставки сообщений в почтовые

ящики, происходит в `%ExchangeInstallPath%TransportRoles\Logs\Mailbox\ProtocolLog\SmtpSend\Delivery`. Например, сообщение, доставленное в почтовый ящик, активирует правило папки "Входящие", которое перенаправляет сообщение другому получателю.

    - Транспортная служба на пограничных транспортных серверах:

    - **Соединители получения**: `%ExchangeInstallPath%TransportRoles\Logs\Edge\ProtocolLog\SmtpReceive`

    - **Отправка соединителей**: `%ExchangeInstallPath%TransportRoles\Logs\Edge\ProtocolLog\SmtpSend`

- Указание максимального размера для файлов журнала протокола. Значение по умолчанию — 10 мегабайт (МБ).

- Указание максимального размера для файлов журнала протокола. Значение по умолчанию — 250 МБ.

- Указание максимального возраста для файлов журнала протокола. Значение по умолчанию —— 30 дней.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записях "Транспортная служба", "Транспортная служба переднего плана", "Транспортная служба почтовых ящиков", "Получение соединителей" и "Отправка соединителей" в разделе Разрешения потока обработки почты .

- С помощью Центра администрирования Exchange (EAC) можно включить или отключить ведение журнала протоколов для соединителей получения и отправки соединителей на серверах почтовых ящиков. Вы также можете использовать EAC для настройки путей к журналам протокола только для транспортной службы. Для всех остальных параметров ведения журнала протоколов необходимо использовать командную консоль Exchange. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

- Вы можете включать и выключать ведение журнала протокола на каждом соединителе по отдельности. Остальные параметры ведения журнала протокола настраиваются для всех соединителей получения или всех соединителей отправки, влияющих на каждую отдельную службу транспорта на сервере Exchange. Все соединители получения в службе транспорта используют одни и те же файлы и параметры журнала протокола. Эти файлы и параметры отделены от файлов и параметров журнала протокола для соединителя отправки в той же службе транспорта.

  > **⊗ Внимание!**
  >
  > Не выполняйте эту процедуру на пограничном транспортном сервере, который подписан на организацию Exchange с помощью EdgeSync. Вместо этого внесите изменения в транспортной службе на сервере почтовых ящиков. Затем изменения реплицируются на пограничный транспортный сервер при следующей синхронизации EdgeSync.

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Настройка ведения журнала протокола с помощью Центра администрирования Exchange

Включение и выключение ведения журнала протокола для соединителя с помощью Центра администрирования Exchange

Выполните указанные ниже действия, чтобы включить или выключить ведение журнала протокола для соединителя отправки или получения в службе транспорта на серверах почтовых ящиков либо соединителя получения во внешней службе транспорта на серверах почтовых ящиков.

1. Откройте Центр администрирования Exchange и перейдите к одному из следующих разделов:

    - Поток >**обработки почтыОтправка соединителей**.

    - Поток >**обработки почтыСоединители получения**.

2. Выберите соединитель, который требуется настроить, и нажмите кнопку **Изменить**.✎

3. На вкладке **Общие** в разделе **Уровень ведения журнала протокола** выберите один из следующих параметров.

    - **Нет**: ведение журнала протокола отключено на соединителе.

    - **Подробно.** Ведение журнала протокола включено в соединителе.

4. По завершении нажмите кнопку **Сохранить**.

Настройка расположения журналов протокола на сервере Exchange с помощью Центра администрирования Exchange

Выполните указанные ниже действия, чтобы настроить расположение журналов протокола для всех соединителей отправки или всех соединителей получения в службе транспорта на серверах почтовых ящиков.

1. Откройте EAC и перейдите в раздел **Серверы**>.

2. Выберите сервер почтовых ящиков, который требуется настроить, и нажмите кнопку **Изменить**.✎

3. На странице свойств сервера нажмите кнопку **Журналы транспорта**. В разделе **Журнал протокола** измените следующие параметры:

    - **Путь к журналу протокола отправки**

    - **Путь к журналу протокола приема**

    Укажите расположение на локальном сервере Exchange. Если такой папки не существует, она будет создана при нажатии кнопки **Сохранить**.

4. По завершении нажмите кнопку **Сохранить**.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно настроили ведение журнала протокола с помощью Центра администрирования Exchange, перейдите к указанному расположению журналов протокола для соединителей отправки или получения. Если вы включили ведение журнала протокола, убедитесь, что файл журнала существует и обновляется для соединителя. Если же вы отключали ведение журнала протокола, убедитесь, что последний файл журнала больше не обновляется для соединителя.

Включение и отключение ведения журнала протокола для соединителя с помощью командной консоли Exchange

Включение и отключение ведения журнала протокола для соединителей отправки и получения с помощью командной консоли Exchange

Выполните указанные ниже действия, чтобы включить или отключить ведение журнала протокола для:

- соединителя отправки или получения в службе транспорта на серверах почтовых ящиков;
- соединителя получения во внешней службе транспорта на серверах почтовых ящиков;
- соединителя отправки или получения в службе транспорта на пограничных транспортных серверах.

Чтобы включить или отключить ведение журнала протокола для соединителя отправки или получения, используйте следующий синтаксис в командной консоли Exchange:

PowerShell

```
<Set-SendConnector | Set-ReceiveConnector> <ConnectorIdentity> -
ProtocolLoggingLevel <Verbose | None>
```

В этом примере показано, как включить ведение журнала протокола для соединителя получения Connection from Contoso.com на сервере Mailbox01.

PowerShell

```
Set-ReceiveConnector "Mailbox01\Connection from Contoso.com" -
ProtocolLoggingLevel Verbose
```

В этом примере показано, как отключить ведение журнала протокола для соединителя отправки Connection to Internet.

PowerShell

```
Set-ReceiveConnector "Connection to Internet" -ProtocolLoggingLevel None
```

Включение и отключение ведения журнала протокола для соединителя отправки внутри организации с помощью командной консоли Exchange

Используйте эту процедуру, чтобы включить или отключить ведение журнала протоколов в неявном и невидимом соединителе отправки внутри организации, который существует в транспортной службе, интерфейсной транспортной службе и службе отправки транспорта почтовых ящиков на серверах почтовых ящиков. Дополнительные сведения об этих соединителях см. в разделе Соединители неявной отправки.

Ведение журнала протокола для соединителя отправки внутри организации происходит в журналах протокола соединителя отправки для указанной службы транспорта. Обратите внимание, что параметр службы транспорта управляет ведением журнала протокола для соединителя отправки внутри организации в службе транспорта, а также в службе отправки транспорта почтовых ящиков.

Чтобы включить или отключить ведение журнала протокола для соединителя отправки внутри организации, используйте следующий синтаксис в командной консоли Exchange:

PowerShell

```
<Set-TransportService | Set-FrontEndTransportService> <ServerIdentity> -
IntraOrgConnectorProtocolLoggingLevel <Verbose | None>
```

В этом примере показано, как включить ведение журнала протокола для соединителя отправки внутри организации в службе транспорта и службе отправки транспорта почтовых ящиков на сервере Mailbox01.

PowerShell

```
Set-TransportService Mailbox01 -IntraOrgConnectorProtocolLoggingLevel
Verbose
```

В этом примере показано, как отключить ведение журнала протокола для соединителя отправки внутри организации во внешней службе транспорта на том же сервере.

PowerShell

```
Set-FrontEndTransportService Mailbox01 -
IntraOrgConnectorProtocolLoggingLevel None
```

Включение или выключение ведения журнала протокола для соединителя получения доставки в почтовые ящики с помощью командной консоли Exchange

Используйте эту процедуру, чтобы включить или отключить ведение журнала протокола в неявном и невидимом соединителе получения почтовых ящиков, существующем в службе доставки транспорта почтовых ящиков. Ведение журнала протокола для этого соединителя происходит в журналах протокола соединителя получения для службы доставки транспорта почтовых ящиков. Дополнительные сведения об этом соединителе см . в разделе Соединители неявного получения в службе доставки транспорта почтовых ящиков на серверах почтовых ящиков.

Чтобы включить или отключить ведение журнала протокола для соединителя отправки доставки в почтовые ящики, используйте следующий синтаксис в командной консоли Exchange:

PowerShell

```
Set-MailboxTransportService <ServerIdentity> -
MailboxDeliveryConnectorProtocolLoggingLevel <Verbose | None>
```

В этом примере показано, как включить ведение журнала протокола для соединителя получения доставки в почтовые ящики на сервере Mailbox01.

PowerShell

```
Set-MailboxTransportService Mailbox01 -
MailboxDeliveryConnectorProtocolLoggingLevel Verbose
```

В этом примере показано, как отключить ведение журнала протокола для соединителя получения доставки в почтовые ящики на том же сервере.

PowerShell

```
Set-MailboxTransportService Mailbox01 -
MailboxDeliveryConnectorProtocolLoggingLevel None
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно включили или отключили ведение журнала протокола для соединителя с помощью командной консоли Exchange, сделайте следующее:

1. Выполните следующую команду в командной консоли Exchange, чтобы проверить, удалось ли вам включить или отключить ведение журнала протокола для всех соединителей на сервере Exchange:

   PowerShell

   ```
   Write-Host "Send Connectors:" -ForegroundColor yellow; Get-
   SendConnector | Format-List Name,ProtocolLoggingLevel; Write-Host
   "Receive Connectors:" -ForegroundColor yellow; Get-ReceiveConnector |
   Format-List Name,TransportRole,ProtocolLoggingLevel; Write-Host
   "Mailbox Transport Delivery service:" -ForegroundColor yellow; Get-
   MailboxTransportService | Format-List *ProtocolLoggingLevel; Write-Host
   "Front End Transport service:" -ForegroundColor yellow; Get-
   FrontEndTransportService | Format-List *ProtocolLoggingLevel; Write-
   Host "Transport service and Mailbox Transport Submission service:" -
   ForegroundColor yellow; Get-TransportService | Format-List
   *ProtocolLoggingLevel
   ```

2. Перейдите к расположению журнала протокола. Если вы включили ведение журнала протокола, убедитесь, что файл журнала существует и обновляется для соединителя. Если же вы отключали ведение журнала протокола, убедитесь, что последний файл журнала больше не обновляется для соединителя.

Настройка параметров журнала протокола на сервере Exchange с помощью командной консоли Exchange

Выполните указанные ниже действия, чтобы настроить параметры журнала протокола для всех соединителей отправки или получения в службе транспорта на сервере почтовых ящиков, а также в службе транспорта на пограничном транспортном сервере.

Чтобы настроить параметры журнала протокола в командной консоли Exchange, используйте следующий синтаксис:

PowerShell

```
<Set-FrontEndTransportService | Set-MailboxTransportService | Set-
TransportService> <ServerIdentity> -ReceiveProtocolLogPath <LocalFilePath> -
ReceiveProtocolLogMaxFileSize <Size> -ReceiveProtocolLogMaxDirectorySize
<Size> -ReceiveProtocolLogMaxAge <dd.hh:mm:ss> -SendProtocolLogPath
<LocalFilePath> -SendProtocolLogMaxFileSize <Size> -
SendProtocolLogMaxDirectorySize <Size> -SendProtocolLogMaxAge <dd.hh:mm:ss>
```

В этом примере показано, как задать следующие параметры журнала протокола в службе транспорта на сервере Mailbox01:

- расположение журнала протокола для всех соединителей получения — D:\Hub SMTP Receive Log, а для всех соединителей отправки — D:\Hub SMTP Send Log. Если такой папки не существует она создается автоматически;
- максимальный размер файла журнала протокола для соединителей получения и отправки — 20 МБ;
- максимальный размер папки журнала протокола для соединителей получения и отправки — 400 МБ;
- максимальный возраст файла журнала протокола для соединителей получения и отправки — 45 дней.

PowerShell

```
Set-TransportService Mailbox01 -ReceiveProtocolLogPath "D:\Hub SMTP Receive
Log" -ReceiveProtocolLogMaxFileSize 20MB -ReceiveProtocolLogMaxDirectorySize
400MB -ReceiveProtocolLogMaxAge 45.00:00:00 -SendProtocolLogPath "D:\Hub
SMTP Send Log" -SendProtocolLogMaxFileSize 20MB -
SendProtocolLogMaxDirectorySize 400MB -SendProtocolLogMaxAge 45.00:00:00
```

Примечания.

- Установка значения `$null` для параметров *SendProtocolLogPath* или *ReceiveProtocolLogPath* фактически отключает ведение журнала протокола для всех соединителей отправки или соединителей получения на сервере. Однако

при установке значения `$null` в журнал событий возникают ошибки журнала событий, если протоколирование включено для любого соединителя отправки или соединителя получения на сервере, включая соединитель отправки внутри организации или соединитель получения доставки почтового ящика.

- Установка значения `00:00:00` для параметров *ReceiveProtocolLogMaxAge* или *SendProtocolLogMaxAge* предотвращает автоматическое удаление файлов журнала протокола из-за их возраста.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно настроили параметры ведения журнала протокола на сервере Exchange с помощью командной консоли Exchange, сделайте следующее:

1. Выполните следующую команду в командной консоли Exchange и проверьте параметры журнала протокола на сервере Exchange:

```
PowerShell
```

```
Write-Host "Front End Transport service:" -ForegroundColor yellow; Get-
FrontEndTransportService | Format-List
ReceiveProtocolLog*,SendProtocolLog*; Write-Host "Mailbox Transport
Submission and Mailbox Transport Delivery services:" -ForegroundColor
yellow; Get-MailboxTransportService | Format-List
ReceiveProtocolLog*,SendProtocolLog*; Write-Host "Transport service:" -
ForegroundColor yellow; Get-TransportService | Format-List
ReceiveProtocolLog*,SendProtocolLog*
```

2. Откройте расположение журнала протокола в проводнике, чтобы убедиться, что файлы журнала существуют, в них записываются данные и они удаляются в соответствии с заданными максимальными размерами файлов и папок.

Маршрутизация почты в Exchange Server

Статья • 04.04.2023

Основная задача службы транспорта, которая существует на серверах почтовых ящиков в организации Exchange, — маршрутизация сообщений, полученных от пользователей и из внешних источников, в конечные пункты доставки. Решения о маршрутизации принимаются во время классификации сообщений. Классификатор — это компонент службы транспорта, который обрабатывает все входящие сообщения и определяет, как поступить с сообщением, на основе сведений о пункте доставки.

Маршрутизация в Exchange 2016 и Exchange 2019 практически не изменилась по сравнению с Exchange 2013. Ниже приведены важные изменения в маршрутизации по сравнению с Exchange 2010:

- Маршрутизация полностью учитывает группы доступности баз данных (DAG) и может использовать членство DAG в решениях о маршрутизации, даже если члены DAG находятся на разных сайтах Active Directory. Для серверов почтовых ящиков, которые не относятся к daG, и для взаимодействия с предыдущими версиями Exchange членство на сайте Active Directory по-прежнему используется в решениях о маршрутизации.

- Служба транспорта не взаимодействует напрямую с базой данных почтовых ящиков. Вместо этого она взаимодействует со службой транспорта почтовых ящиков, размещенной локально или на удаленном сервере почтовых ящиков. Только служба транспорта почтовых ящиков взаимодействует с локальной базой данных почтовых ящиков. Если сервер почтовых ящиков является участником группы DAG, только служба транспорта почтовых ящиков на сервере почтовых ящиков, на котором хранится активная копия базы данных почтовых ящиков, принимает сообщения для конечного получателя.

- Удаленные вызовы процедур (RPC) используются только службой транспорта почтовых ящиков для отправки и получения сообщений из локальной базы данных почтовых ящиков. Когда сервер почтовых ящиков входит в группу DAG, RPC используется только для локальной связи между службой транспорта почтовых ящиков и активными копиями базы данных почтовых ящиков. Другими словами, RPC никогда не используется для связи между серверами или службами. Связь между службой транспорта почтовых ящиков и службой транспорта всегда осуществляется по протоколу SMTP.

- Exchange теперь использует более точные очереди для удаленных назначений. Вместо того чтобы использовать одну очередь для всех назначений на удаленном сайте Active Directory, Exchange теперь помещает в очередь сообщения для определенных назначений на сайте Active Directory, например для отдельных соединителей отправки.

- Связанные соединители больше не доступны. Связанный соединитель — это соединитель получения, связанный с соединителем отправки. Все сообщения, полученные соединителем получения, автоматически переадресовывались соединителю отправки.

Компоненты маршрутизации

Когда сообщение получено службой транспорта на сервере почтовых ящиков, его необходимо классифицировать. Первый этап классификации сообщения — это разрешение получателя. После этого можно определить конечный адрес доставки. На следующем этапе — этапе маршрутизации — определяется оптимальный маршрут. Маршрутизация в Exchange обобщена для повышения гибкости и уменьшения сложности за счет использования концепций *назначения маршрутизации* и *групп доставки*.

Места назначения

Конечный адрес доставки сообщения называется *целью маршрутизации*. Независимо от сложности организации Exchange, существует на удивление мало целей маршрутизации. Они указаны ниже.

- **База данных почтовых ящиков**. Это назначение маршрутизации для любого получателя с почтовым ящиком в организации Exchange. В Exchange 2013 или более поздней версии общедоступные папки являются типом почтовых ящиков, поэтому маршрутизация сообщений получателям общедоступных папок аналогична маршрутизации сообщений получателям почтовых ящиков.

- **Соединитель**. Соединитель отправки используется в качестве назначения маршрутизации для сообщений SMTP в зависимости от конфигурации соединителя отправки (адресные пространства, области или нет и т. д.). Аналогичным образом, соединитель агента доставки или внешний соединитель используется в качестве цели маршрутизации сообщений, не использующих SMTP.

- **Сервер расширения группы рассылки**. Это место назначения маршрутизации, когда группа рассылки имеет назначенный сервер

расширения (сервер, отвечающий за расширение списка участников группы). Сервер расширения группы рассылки — это сервер почтовых ящиков Exchange 2013 или более поздней версии или транспортный сервер-концентратор Exchange 2010.

Обратите внимание, что эти цели маршрутизации существовали в предыдущих версиях Exchange, но они не назывались целями маршрутизации.

Группы доставки

За доставку почты в каждую цель маршрутизации отвечает коллекция из одного или нескольких транспортных серверов. Эта коллекция транспортных серверов называется *группой доставки*. Термин *транспортные серверы* используется, так как они могут быть смесью серверов почтовых ящиков Exchange 2013 или более поздней версии (транспортной службы) или транспортных серверов концентратора Exchange 2010. Отношение между целями маршрутизации и группами доставки описывается в следующей таблице:

Цель маршрутизации	**Группа доставки**
Базы данных почтовых ящиков Exchange 2013 или более поздней версии	Серверы почтовых ящиков Exchange 2013 или более поздней версии.
Базы данных почтовых ящиков Exchange 2010 в организациях Exchange 2016	Только транспортные серверы-концентраторы Exchange 2010.
Connectors	Серверы почтовых ящиков Exchange 2013 или более поздней версии или транспортные серверы-концентратор Exchange 2010.
Серверы расширения групп рассылки	Серверы почтовых ящиков Exchange 2013 или более поздней версии или транспортные серверы-концентратор Exchange 2010.

Маршрутизация сообщения зависит от отношений между исходной и целевой группами доставки:

- Если исходная и целевая группы доставки совпадают, никаких решений по маршрутизации не требуется. Цель маршрутизации — это следующий прыжок для сообщения.
- Если исходная группа доставки находится за пределами целевой, требуется принять решения по маршрутизации. Сообщение передается в целевую

группу доставки по пути маршрутизации с наименьшей стоимостью. В зависимости от размера и сложности среды Exchange, для доставки в целевую группу доставки и достижения цели маршрутизации сообщение может быть передано через множество транспортных серверов.

В приведенной ниже таблице перечислены различные типы групп доставки Exchange 2016.

Тип группы доставки	**Группа доставки**	**Цель маршрутизации**	**Comments**
Маршрутизируемая группа обеспечения доступности баз данных	• Серверы почтовых ящиков Exchange 2019, принадлежащие группе daG Exchange 2019. • Серверы почтовых ящиков Exchange 2016, которые относятся к группе обеспечения доступности баз данных Exchange 2016. • Серверы почтовых ящиков Exchange 2013, которые относятся к группе обеспечения доступности баз данных Exchange 2013.	Базы данных почтовых ящиков в DAG	После того как сообщение поступает на сервер почтовых ящиков в DAG, служба транспорта передает его в службу доставки транспорта почтовых ящиков в участнике DAG, который содержит активную копию целевой базы данных почтовых ящиков. Затем служба доставки транспорта почтовых ящиков доставляет сообщение в локальную базу данных почтовых ящиков. Хотя DAG может содержать серверы почтовых ящиков, расположенные на разных сайтах Active Directory, DAG определяет группу доставки, а не сайт Active Directory.
Группа доставки почтовых ящиков (Exchange 2013 или более поздней версии)	Серверы почтовых ящиков Exchange 2013 или более поздней версии на сайте Active Directory.	Базы данных почтовых ящиков на серверах Exchange 2013 или более поздних версий	Базы данных почтовых ящиков, расположенные на серверах, которые не относятся к DAG, обслуживаются транспортной службой на серверах почтовых

Тип группы доставки	Группа доставки	Цель маршрутизации	Comments
		на сайте Active Directory, которые не относятся к daG.	ящиков на том же сайте Active Directory. После поступления сообщения на сервер почтовых ящиков на сайте Active Directory транспортная служба использует ПРОТОКОЛ SMTP для передачи сообщения в службу доставки транспорта почтовых ящиков на сервере почтовых ящиков, на котором хранится база данных почтовых ящиков. Затем служба доставки транспорта почтовых ящиков доставляет сообщение в локальную базу данных почтовых ящиков с помощью RPC. Другими словами, между разными версиями Exchange поддерживаются следующие пути доставки почты: • Транспортная служба Exchange 2019 в службу доставки транспорта почтовых ящиков Exchange 2016 в базу данных почтовых ящиков Exchange 2016. • Транспортная служба Exchange 2019 в службу доставки транспорта почтовых ящиков Exchange 2013 в

Тип группы доставки	Группа доставки	Цель маршрутизации	Comments
			базу данных почтовых ящиков Exchange 2013. • Транспортная служба Exchange 2016 — служба доставки транспорта почтовых ящиков Exchange 2019 в базу данных почтовых ящиков Exchange 2019. • Exchange 2016 Transport service to Exchange 2013 Mailbox Transport Delivery service to Exchange 2013 mailbox database. • Транспортная служба Exchange 2013 — служба доставки транспорта почтовых ящиков Exchange 2019 в базу данных почтовых ящиков Exchange 2019. • Exchange 2013 Transport service to Exchange 2016 Mailbox Transport Delivery service to Exchange 2016 mailbox database.

Тип группы доставки	Группа доставки	Цель маршрутизации	Comments
Группа доставки почтовых ящиков (Exchange 2010)	Транспортные серверы-концентраторы Exchange 2010 на сайте Active Directory.	Базы данных почтовых ящиков на серверах почтовых ящиков Exchange 2010 на сайте Active Directory.	Базы данных почтовых ящиков, расположенные на серверах почтовых ящиков Exchange 2010, обслуживаются транспортными серверами-концентраторами Exchange 2010 на том же сайте Active Directory. p> После поступления сообщения на случайный транспортный сервер-концентратор Exchange 2010 на сайте Active Directory драйвер хранилища на транспортном сервере-концентраторе использует RPC для записи сообщения в базу данных почтовых ящиков.
Исходный сервер соединителя	Сочетание любых серверов почтовых ящиков Exchange 2013 или более поздних версий или транспортных серверов-концентраторов Exchange 2010, которые определены как исходные транспортные серверы для соединителя.	Соединитель отправки, соединитель агента доставки или внешний соединитель.	Если область действия соединителя ограничена транспортными серверами на одном сайте Active Directory, то только другие транспортные серверы на этом сайте могут использовать соединитель для маршрутизации почты. Если область действия соединителя не ограничена, то все транспортные серверы в лесу Active Directory могут использовать соединитель для маршрутизации почты.

Тип группы доставки	Группа доставки	Цель маршрутизации	Comments
Список серверов	Сервер почтовых ящиков Exchange 2013 или более поздней версии или транспортный сервер-концентратор Exchange 2010, определенный как сервер расширения для группы рассылки.	Сервер расширения группы рассылки.	Нет

Тип группы доставки	Группа доставки	Цель маршрутизации	Comments
Сайт Active Directory	Любое сочетание серверов почтовых ящиков Exchange 2013 или более поздней версии или транспортных серверов концентратора Exchange 2010, которые существуют в: • сайтах Active Directory, настроенных в качестве узловых сайтов; • сайтах Active Directory, у которых есть подписанные пограничные транспортные серверы.	Нет. Сообщение должно пройти через сайт Active Directory на пути к фактической цели маршрутизации.	Этот тип группы доставки является единственным сценарием маршрутизации в Exchange 2013 или более поздних версий, где *по-прежнему используется отложенное отключение* . Задержка развертывания призвана уменьшить количество передач сообщений при наличии общего пути маршрутизации с наименьшей стоимостью у нескольких целей маршрутизации. Узловые сайты используются только при наличии сайта Active Directory на пути маршрутизации с наименьшей стоимостью. br/> Для пограничных транспортных серверов служба транспорта на любом сервере почтовых ящиков на сайте Active Directory с подпиской может отправлять сообщения на пограничный транспортный сервер независимо от того, участвует ли этот сервер в синхронизации EdgeSync. Дополнительные сведения см. в разделе Пограничные транспортные серверы.

ⓘ Примечание

Членство в группе доставки не является взаимоисключающим. Например, сервер почтовых ящиков, который является членом DAG, также может быть исходным транспортным сервером соединителя отправки. Сервер почтовых ящиков относится к маршрутизируемой группе доставки DAG для баз данных почтовых ящиков в DAG, а также группе доставки исходного сервера соединителя для соединителя отправки.

Очереди

С точки зрения отправляющего транспортного сервера каждая очередь доставки сообщения представляет собой адрес доставки конкретного сообщения. Когда служба транспорта выбирает адрес доставки сообщения, он записывается в атрибуте **NextHopSolutionKey** получателя. Если одно сообщение отправляется нескольким получателям, у каждого из них есть атрибут **NextHopSolutionKey**. Принимающий транспортный сервер также выполняет классификацию сообщения и помещает его в очередь на доставку. После помещения сообщения в очередь можно просмотреть ее тип доставки, чтобы определить, будет ли сообщение снова передаваться, когда оно достигнет следующего пункта прыжка. Каждое уникальное значение атрибута **NextHopSolutionKey** соответствует отдельной очереди доставки сообщения.

Дополнительные сведения см. в разделе NextHopSolutionKey.

Маршрутизация сообщений

Если сообщение должно быть доставлено в удаленную группу доставки, необходимо определить для него путь маршрутизации. Exchange использует следующую логику для выбора пути маршрутизации сообщения. Эта логика практически не изменилась по сравнению с Exchange 2010:

1. Сначала рассчитывается маршрут с наименьшей стоимостью путем сложения стоимости связей сайтов IP, которые необходимо пройти для достижения сервера назначения. Если назначением является соединитель, стоимость, назначенная адресному пространству, добавляется к стоимости достижения указанного соединителя. Если возможно несколько путей маршрутизации, используется только путь маршрутизации с наименьшей совокупной стоимостью.

   Примечание. Ограничения размера соединителей здесь являются фактором. Соединители, настроенные с ограничениями на размер сообщения, меньше размера сообщения, исключаются из рассмотрения. Дополнительные

сведения см. в разделе Выбор соединителя при маршрутизации внешних сообщений.

2. Если существует несколько путей маршрутизации с одинаковой совокупной стоимостью, оценивается количество прыжков в каждом пути. Используется путь маршрутизации с наименьшим количеством прыжков.

3. Если доступно несколько путей маршрутизации, учитывается имя, присвоенное сайтам Active Directory перед пунктом доставки. Используется путь маршрутизации, в котором ближайший к пункту доставки сайт Active Directory является последним по буквенно-цифровому порядку. Если ближайшим к пункту доставки для всех путей маршрутизации оказывается один и тот же сайт, рассматриваются имена предыдущих сайтов.

В Exchange 2010 каждый получатель сообщения связан только с одним сайтом Active Directory, а между исходным сайтом Active Directory и целевым сайтом имеется только один маршрут с наименьшей стоимостью. В Exchange 2013 или более поздней версии группа доставки может охватывать несколько сайтов Active Directory, а также несколько путей маршрутизации с наименьшими затратами на эти сайты. Exchange назначает один сайт Active Directory в целевой группе доставки в качестве *основного сайта*. Основной сайт — это ближайший сайт Active Directory согласно описанной ранее логике маршрутизации. Для успешной маршрутизации сообщений между группами доставки Exchange учитывает следующие проблемы:

- **Наличие одного или нескольких центральных сайтов по пути маршрутизации с наименьшей стоимостью**. Если путь маршрутизации с наименьшей стоимостью к основному сайту содержит какие-либо центральные сайты, сообщение должно быть перенаправлено через центральные сайты. Ближайший сайт-концентратор на пути маршрутизации с наименьшей стоимостью будет выбран в качестве новой группы доставки — **AD site**, в которую входят все транспортные серверы на этом сайте. После прохода сайта-концентратора маршрутизация сообщения по пути маршрутизации с наименьшей стоимостью продолжается. Если основной сайт оказался сайтом-концентратором, то он все же считается сайтом-концентратором по следующим причинам:

    - Если целевая группа доставки охватывает несколько сайтов Active Directory, исходный сервер должен подключаться только к серверам на узловом сайте.

    - Серверы на узловом сайте, которые относятся к целевой группе доставки, являются предпочтительными.

Как и в предыдущей версии Exchange, все узловые сайты не на пути маршрутизации с наименьшей стоимостью к основному сайту игнорируются.

- **Целевой сервер Exchange Server для выбора в целевой группе маршрутизации. Если целевая** группа доставки охватывает несколько сайтов Active Directory, путь маршрутизации к определенным серверам в группе доставки может иметь разные затраты. Серверы, расположенные на ближайшем сайте Active Directory, выбираются в качестве целевых серверов для группы доставки на основе пути маршрутизации с наименьшей стоимостью, а сайт Active Directory, на который находятся эти серверы, выбирается в качестве основного сайта.

- **Резервные параметры при попытке подключения ко всем серверам в целевой группе маршрутизации сбой**. Если целевая группа доставки охватывает несколько сайтов Active Directory, первым резервным вариантом являются все остальные серверы в целевой группе доставки на других сайтах Active Directory, которые не выбраны в качестве целевых серверов. Выбор сервера основан на наименее затратном пути маршрутизации к другим сайтам Active Directory. Если в целевой группе доставки есть какие-либо серверы на локальном сайте Active Directory, другие резервные варианты отсутствуют, так как сообщение уже находится как можно ближе к целевому назначению маршрутизации. Если целевая группа доставки содержит серверы на удаленных сайтах Active Directory, можно попытаться подключиться ко всем остальным серверам на первичном сайте.

Routing messages between Active Directory sites

Способ маршрутизации сообщений между сайтами Active Directory практически не отличается от Exchange 2010. Дополнительные сведения см. в статье Route Mail Between Active Directory Sites.

Маршрутизация во внешней службе транспорта на серверах почтовых ящиков

Служба внешнего транспорта выступает в качестве прокси-сервера без отслеживания состояния для всего входящего и (при необходимости) исходящего внешнего SMTP-трафика для организации Exchange. Служба транспорта взаимодействует со внешней службой транспорта для отправки сообщений, только если она настроена соответствующим образом. Дополнительные сведения см. в статье Configure Send connectors to proxy outbound mail.

Внешняя служба транспорта должна быстро найти одну работоспособную службу транспорта, чтобы получить передаваемое сообщение, независимо от количества и типа получателей. При несоблюдении этого требования служба электронной почты будет восприниматься сервером-отправителем как недоступная. Как и служба транспорта, внешняя служба транспорта загружает таблицы маршрутизации на основе сведений из Active Directory и использует группы доставки для маршрутизации сообщений. Тем не менее таблицы маршрутизации, используемые внешней службой транспорта, имеют следующие уникальные характеристики:

- Служба транспорта переднего плана никогда не считается членом группы доставки, даже если сервер почтовых ящиков и сервер клиентского доступа установлены на одном физическом сервере (что всегда происходит в Exchange 2016 или более поздней версии). Это принуждает внешнюю службу транспорта взаимодействовать только со службой транспорта.
- Таблицы маршрутизации не содержат маршрутов соединителей отправки.
- Таблицы маршрутизации содержат специальный список серверов почтовых ящиков на локальном сайте Active Directory для быстрой отработки отказа.

Маршрутизация в транспортной службе переднего плана разрешает получателей сообщений в базы данных почтовых ящиков. Список серверов почтовых ящиков, используемых службой транспорта переднего плана, основан на базах данных почтовых ящиков получателей сообщений. Обратите внимание, что ни у одного из получателей нет почтовых ящиков, например, если получатель является группой рассылки или почтовым пользователем. Для каждой базы данных почтовых ящиков служба транспорта переднего плана ищет группу доставки и связанные с ней сведения о маршрутизации. Группами доставки, используемыми службой внешнего транспорта, являются:

- Маршрутизируемая группа обеспечения доступности баз данных
- Группа доставки в почтовые ящики
- Сайт Active Directory

В зависимости от числа и типа получателей служба транспорта переднего плана выполняет одно из следующих действий:

- Для сообщений с одним получателем выберите сервер почтовых ящиков в целевой группе доставки в зависимости от расстояния до сайта Active Directory. Передача сообщения получателю может включать маршрутизацию через узловой сайт.

- Для сообщений с несколькими получателями используйте первых 20 получателей для выбора сервера почтовых ящиков в ближайшей группе доставки, в зависимости от расстояния до сайта Active Directory. Обратите внимание, что развертывание сообщений не выполняется во внешней службе транспорта, поэтому в конечном счете выбирается только один сервер почтовых ящиков, независимо от количества получателей сообщения.

- Если среди получателей сообщения нет почтовых ящиков, выберите произвольный сервер почтовых ящиков на локальном сайте Active Directory.

Маршрутизация в транспортной службе почтовых ящиков на серверах почтовых ящиков

Служба транспорта почтовых ящиков состоит из двух отдельных служб: службы отправки транспорта почтовых ящиков и службы доставки транспорта почтовых ящиков. Служба доставки транспорта почтовых ящиков получает сообщения SMTP из службы транспорта и подключается к локальной базе данных почтовых ящиков с помощью RPC для доставки сообщения. Служба отправки транспорта почтовых ящиков подключается к локальной базе данных почтовых ящиков с помощью RPC для извлечения сообщений и передает сообщения через SMTP в службу транспорта. Служба транспорта почтовых ящиков — это служба без отслеживания состояния, она не использует очереди доставки сообщений.

Как и служба транспорта, служба транспорта почтовых ящиков загружает таблицы маршрутизации на основе сведений из Active Directory и использует группы доставки для маршрутизации сообщений. Тем не менее есть аспекты маршрутизации, уникальные для службы транспорта почтовых ящиков:

- Так как служба транспорта и служба транспорта почтовых ящиков размещаются на одном сервере почтовых ящиков, служба транспорта почтовых ящиков всегда относится к той же группе доставки, что и сервер почтовых ящиков. Это группа доставки называется *локальной*.

- Служба отправки транспорта почтовых ящиков не отправляет сообщения автоматически в службу транспорта на локальном сервере почтовых ящиков или на других серверах почтовых ящиков в своей локальной группе доставки. Служба отправки транспорта почтовых ящиков имеет доступ к тем же сведениями о топологии маршрутизации, что и служба транспорта, так что служба отправки транспорта почтовых ящиков может отправлять сообщения в службу транспорта на серверах почтовых ящиков за пределами группы доставки. Серверы почтовых ящиков в локальной группе доставки

используются как резервные варианты, а также для доставки получателям без почтовых ящиков.

- Служба транспорта почтовых ящиков взаимодействует только со службой транспорта на серверах почтовых ящиков.
- Служба транспорта почтовых ящиков взаимодействует только с локальными базами данных почтовых ящиков. Служба транспорта почтовых ящиков не взаимодействует с базами данных почтовых ящиков на других серверах почтовых ящиков.

Когда пользователь отправляет сообщение из своего почтового ящика, служба отправки транспорта почтовых ящиков разрешает получателей сообщений в базы данных почтовых ящиков. Список серверов почтовых ящиков, используемых службой отправки транспорта почтовых ящиков, основан на базах данных почтовых ящиков получателей сообщений. Обратите внимание, что ни у одного из получателей нет почтовых ящиков, например, если получатель является группой рассылки или почтовым пользователем. Для каждой базы данных почтовых ящиков служба отправки транспорта почтовых ящиков ищет группу доставки и связанные сведения о маршрутизации. Ниже перечислены группы доставки, используемые службой отправки транспорта почтовых ящиков.

- Маршрутизируемая группа обеспечения доступности баз данных
- Группа доставки в почтовые ящики
- Сайт Active Directory

В зависимости от числа и типа получателей служба отправки транспорта почтовых ящиков выполняет одно из следующих действий:

- Для сообщений с одним получателем выберите сервер почтовых ящиков в целевой группе доставки в зависимости от расстояния до сайта Active Directory. Передача сообщения получателю может включать маршрутизацию через узловой сайт.
- Для сообщений с несколькими получателями используйте первых 20 получателей для выбора сервера почтовых ящиков в ближайшей к сайту Active Directory группе доставки.
- Если сообщение не имеет получателей с почтовыми ящиками, выбирается сервер почтовых ящиков в локальной группе доставки.

Если служба доставки транспорта почтовых ящиков получает сообщение от службы транспорта, она принимает либо отклоняет его для доставки в локальную

базу данных почтовых ящиков. Служба доставки транспорта почтовых ящиков может доставить сообщение в том случае, если получатель находится в активной копии локальной базы данных почтовых ящиков. Если же получатель отсутствует в активной копии локальной базы данных почтовых ящиков, служба доставки транспорта почтовых ящиков не может доставить сообщение и должна сообщить о недоставке в службу транспорта. Например, если активная копия базы данных почтовых ящиков недавно перемещена на другой сервер, служба транспорта может ошибочно передать сообщение на сервер почтовых ящиков, который теперь содержит неактивную копию базы данных почтовых ящиков. Среди ответов о недоставке, которые служба доставки транспорта почтовых ящиков возвращает службе транспорта, могут быть следующие:

- Повторная попытка доставки
- Создание отчета о недоставке
- Сообщение перенаправляется

Маршрутизация в транспортной службе на пограничных транспортных серверах

Служба транспорта на пограничных транспортных серверах обеспечивает ретрансляцию SMTP и работу служб промежуточных узлов для всего потока обработки почты в Интернете. Входящие и исходящие сообщения Интернета помещаются в очереди доставки сообщений на пограничном транспортном сервере. Очереди соответствуют внешним доменам или соединителям отправки. Дополнительные сведения см. в разделе NextHopSolutionKey.

Как правило, устанавливая пограничный транспортный сервер в своей сети периметра, вы подписываете пограничный транспортный сервер на сайт Active Directory. Сайт Active Directory содержит серверы почтовых ящиков, которые будут ретранслировать сообщения на пограничный транспортный сервер и обратно. В процессе пограничной подписки создается членство на сайте Active Directory для пограничного транспортного сервера. Это членство позволяет серверам почтовых ящиков на сайте Active Directory ретранслировать сообщения на пограничный транспортный сервер без настройки явных соединителей отправки.

В организациях с серверами Exchange Server на нескольких сайтах Active Directory исходящая почта от внутренних получателей к внешним получателям сначала направляется на сайт Active Directory с подпиской. Транспортные серверы на целевом сайте Active Directory являются группой доставки. Назначением маршрутизации является соединитель отправки внутри организации в

транспортной службе на любом из серверов почтовых ящиков на сайте Active Directory с подпиской. *Соединитель отправки внутри организации* — это специальный соединитель отправки, который существует в транспортной службе на каждом сервере почтовых ящиков. Этот соединитель отправки неявно создается, невидим, не требует управления и используется для ретрансляции сообщений между серверами Exchange.

Дополнительные сведения о маршрутизации входящей и исходящей почты на пограничных транспортных серверах см. в статье Mail flow and the transport pipeline.

Выбор соединителей для маршрутизации внешних сообщений

Статья • 04.04.2023

Как и в предыдущих версиях Exchange, Exchange Server 2016 и Exchange Server 2019 используют соединители для доставки сообщений внешним получателям (получателям, которых нет в организации Exchange). Exchange использует соединители отправки для маршрутизации сообщений на внешние домены SMTP. Если внешний получатель не находится в системе обмена сообщениями SMTP, Exchange использует соединители агента доставки или внешние соединители.

Дополнительные сведения о разных типах соединителей см. в статье Connectors. Дополнительные сведения о том, как Exchange принимает решения о маршрутизации, см. в статье Маршрутизация почты.

Выбор соединителей для маршрутизации сообщений

Параметры, настраиваемые для соединителей, могут исключить доступный соединитель из процесса маршрутизации. Эти параметры перечислены в приведенной ниже таблице.

Параметр соединителя	**Comments**
Состояние (включен или отключен)	Только включенные соединители используются для маршрутизации. Если соединитель отключен, он не учитывается при маршрутизации сообщений.

Параметр соединителя	Comments
Адресное пространство	Адресные пространства определяют целевые домены или другие адресные пространства, обслуживаемые соединителем. Выбирая соединитель для маршрутизации, Exchange учитывает только те соединители, у которых есть соответствующее адресное пространство. Если целевому адресному пространству соответствуют несколько соединителей, выбирается соединитель с более точным соответствием адреса. Например, предположим, что получатель — julia@marketing.contoso.com, а отдельные соединители отправки настроены для *, *.contoso.com и marketing.contoso.com. Порядок выбора соединителя, основанного исключительно на адресном пространстве, будет следующим: 1. marketing.contoso.com 2. *.contoso.com 3. *
тип адресного пространства;	По умолчанию для нового соединителя отправки используется адресное пространство SMTP. Если вы укажете другое адресное пространство, сообщения по-прежнему будут отправляться по назначению (на промежуточный узел) с помощью протокола SMTP. Для маршрутизации сообщений на серверы обмена сообщениями без использования протокола SMTP необходимо создать соединитель агента доставки или внешний соединитель.
Стоимость адресного пространства	Вы можете использовать значение стоимости адресного пространства для оптимизации потока обработки почты и повышения отказоустойчивости при настройке одного и того же адресного пространства для нескольких соединителей. Чем ниже стоимость, тем предпочтительнее соединитель.
Исходный сервер	Для размещения соединителя необходимо настроить по крайней мере один сервер почтовых ящиков или пограничный транспортный сервер. Вы можете настроить несколько исходных серверов, обеспечивающих балансировку нагрузки и отказоустойчивость для адресных пространств, определенных в соединителе.
Область	Область действия соединителя управляет его видимостью в организации Exchange. По умолчанию соединители видны всем серверам Exchange в лесу Active Directory. Однако вы можете ограничить область действия соединителя, чтобы он был виден только остальным серверам Exchange на локальном сайте Active Directory. Соединитель не виден серверам Exchange на остальных сайтах Active Directory и не используется для маршрутизации. Ограниченный таким образом соединитель называется *соединителем с заданной областью действия*.

Параметр соединителя	Comments
Ограничения на размер сообщений	Из-за ограничения на размер сообщений соединитель может не учитываться при выборе, если размер сообщения превышает максимальный размер, разрешенный в соединителе. Дополнительные сведения об ограничениях на размер сообщений в соединителях см. в разделе Ограничения для соединителя.

Выбор соединителя для внешнего получателя

Для маршрутизации сообщений, отправляемых внешним получателям, Exchange должен выбрать наиболее подходящий соединитель. Необходимые для этого решения перечислены в следующем списке:

1. Exchange исключает все соединители, в которых ограничение на размер сообщений меньше размера сообщения.
2. Exchange ограничивает список оставшихся соединителей согласно всем следующим условиям:
    - Областью действия соединителя является сервер Exchange на локальном сайте Active Directory, либо у него нет области действия (соединитель доступен всем серверам Exchange в лесу Active Directory).
    - Соединитель включен.
    - Для соединителя настроено адресное пространство, соответствующее электронному адресу получателя.
3. Из полученного списка Exchange выбирает соединитель с наиболее точным соответствием адресного пространства. Если для нескольких соединителей настроено одно и то же адресное пространство, Exchange использует для выбора соединителя следующие условия:
    a. **Совокупная стоимость**. Это сумма затрат, назначаемых всем IP-соединениям между исходным сайтом Active Directory и сайтом Active Directory, содержащим исходные серверы соединителя, и затраты, назначенные адресному пространству соединителя (затраты на подключение к IP-сайту + стоимость соединителя). Выбирается соединитель с наименьшей совокупной стоимостью. Если у нескольких

соединителей одинаковая совокупная стоимость, выполняется следующий этап выбора.

b. **Количество прыжков**. Выбран исходный сервер для соединителя, к которому можно получить наименьшее число прыжков. Как правило, это означает, что используется следующий порядок выбора:

   i. Локальный сервер Exchange.

   ii. Сервер Exchange на том же сайте Active Directory.

   iii. Сервер Exchange на удаленном сайте Active Directory.

   Если нескольких соединителей можно достичь за одинаковое число прыжков, выполняется следующий этап выбора.

c. **Имя соединителя**. Если несколько путей маршрутизации имеют одинаковые совокупные затраты и количество прыжков, выбирается соединитель с именем с наименьшим буквенно-цифровым значением.

Обработка сообщений, которые невозможно маршрутизировать

Если ни один из соединителей не удовлетворяет условиям выбора, выполняется одно из следующих действий:

- При отсутствии подходящего соединителя для адресного пространства SMTP получатель помечается как недоступный, а сообщение перенаправляется в очередь недоступных сообщений. Дополнительные сведения об этой очереди см. в разделе Типы очередей.
- При отсутствии подходящего соединителя для адресного пространства, не использующего протокол SMTP, отправителю возвращается отчет о недоставке.
- Если размер сообщения превышает ограничение на размер для всех соединителей, отправителю возвращается отчет о недоставке.

Разрешение получателей в Exchange Server

Статья • 04.04.2023

Разрешение получателей — это, когда сервер Exchange Server развертывает и разрешает всех получателей в сообщении. При разрешении получателей выполняются указанные ниже действия.

- Сопоставление получателя с соответствующим объектом Active Directory.
- Разворачивание групп рассылки в список отдельных получателей.
- Применение ограничений для сообщений и альтернативных получателей к каждому получателю.

Разрешение получателей в Exchange 2016 или Exchange 2019 практически не изменилось по сравнению с Exchange 2013. Разрешение получателей выполняет классификатор в службе транспорта на серверах почтовых ящиков. Классификатор обрабатывает каждое сообщение после того, как оно добавляется в очередь передачи, но до того, как оно будет добавлено в очередь доставки. Компонент классификатора, который отвечает за разрешение получателей, часто называют *сопоставителем*. Дополнительные сведения о классификаторе и очереди передачи см. в разделе Общие сведения о службе транспорта на серверах почтовых ящиков.

В этой статье описаны различные этапы и компоненты разрешения получателей на сервере Exchange Server.

разрешение верхнего уровня;

Разрешение верхнего уровня — это первый этап разрешения получателей, который связывает каждого получателя во входящем сообщении с соответствующим объектом получателя в Active Directory. Классификатор создает список, содержащий отправителя и исходные (неразвернутые) электронные адреса получателей из сообщения, а затем использует этот список в запросе к Active Directory. При обнаружении совпадения в свойствах электронных адресов для объектов Active Directory, поддерживающих почту, классификатор кэширует свойства объектов и применяет ограничения для отправителей сообщений.

Адреса электронной почты получателей

Разрешение верхнего уровня начинается с обработки сообщения и первоначального (неразвернутого) списка получателей из *конверта сообщения*. Конверт сообщения содержит команды SMTP, которые используются для передачи сообщений между серверами.

- Электронный адрес отправителя указывается в команде **MAIL FROM**.
- Электронный адрес каждого получателя указывается в отдельной команде **RCPT TO**.

Отправитель и получатели конверта обычно создаются из отправителя и получателей в `To:` полях заголовка , `From:`, `Cc:` и `Bcc:` в заголовке сообщения. Однако эти поля заголовка легко

подделать, и они могут не соответствовать действительным электронным адресам отправителя и получателей, которые использовались для передачи сообщения.

Инкапсулированные электронные адреса

Стандартные SMTP-адреса соответствуют спецификациям в RFC 5321 и RFC 5322 (например chris@contoso.com). Однако электронный адрес также может не являться SMTP-адресом и быть инкапсулированным в SMTP-адрес. Exchange поддерживает метод инкапсуляции IMCEA, заменяющий символы, не поддерживаемые в SMTP-адресах, на допустимые символы.

Адреса IMCEA используют синтаксис `IMCEA<Type>-<address>@<domain>`:

- <*Тип*> определяет тип адреса, отличного от SMTP (например `EX`, , `X400`или `FAX`). Хотя `SMTP` и `X500` являются теоретически допустимыми значениями для <*типа*>, разрешение получателей Exchange отклоняет все адреса в кодировке IMCEA, использующие любой из этих типов.
- <*address*> — это закодированный вариант первоначального адреса:
  - буквенно-цифровые символы, знак равенства (=) и дефис (-) не заменяются;
  - косая черта (/) заменяется на символ подчеркивания (_);
  - Другие символы US-ASCII заменяются знаком плюса (+) и двумя цифрами значения ASCII в шестнадцатеричном формате (например, пробел имеет закодированное значение `+20`).
- <*domain*> — это домен SMTP, используемый для инкапсуляции адреса, не являющегося SMTP-адресом (например, contoso.com).

Адреса IMCEA возвращаются к исходным значениям (неинкапсулированным) только в том случае, если домен соответствует принятому домену по умолчанию в организации Exchange. Дополнительные сведения см. в разделе Домен по умолчанию.

Максимальная длина SMTP-адреса электронной почты в Exchange составляет 571 символов. Этот предел включает:

- 315 символов для части адреса, относящейся к имени;
- 255 символов для имени домена;
- символ "@", отделяющий имя от домена.

Exchange не поддерживает сообщения в кодировке IMCEA, где длина части адреса, относящейся к имени, превышает 315 символов, даже если полная длина электронного адреса меньше 571 символов.

Способ разрешения адресов

Электронные адреса отправителя и всех получателей каждого сообщения добавляются в список, который используется в случае запроса для Active Directory. Перед добавлением в список отменяется инкапсуляция всех инкапсулированных адресов. Отправка запроса Active Directory может выполняться для 20 электронных адресов за один раз. Если в запросе возникают временные ошибки, сообщение возвращается в очередь отправки и откладывается на время, указанное ключом *ResolverRetryInterval* в

`%ExchangeInstallPath%Bin\EdgeTransport.exe.config` XML-файле конфигурации приложения, связанном со службой транспорта. Значение по умолчанию — 30 минут.

Объекты получателей Active Directory, используемые Exchange, описаны в следующей таблице. Дополнительные сведения о типах получателей Exchange см. в разделе Получатели.

Тип получателя Active Directory	**Описание**
DistributionGroup	Любой объект группы, поддерживающий почту. Объекты групп рассылки могут относиться к указанным ниже типам. • **MailUniversalDistributionGroup**: объект универсальной группы рассылки • **MailUniversalSecurityGroup**: объект универсальной группы безопасности (USG), имеющий адрес электронной почты.
DynamicDistributionGroup	Объект, имеющий класс Active Directory **msExchDynamicDistributionList**. Дополнительные сведения см. в разделе Управление динамическими группами рассылки.
Mailbox	Объект с адресом электронной почты и определенным параметром *Database* .
MailUser	Объект пользователя, для которого назначен адрес электронной почты и не определен параметр *Database*. Дополнительные сведения см. в разделе Управление пользователями почты.
MailContact	Объект контакта, которому назначен электронный адрес. Как правило, почтовый контакт используется для получателей за пределами организации Exchange. Почтовый контакт также используется в средах Exchange между лесами. Дополнительные сведения см. в разделе Управление почтовыми контактами.
MailPublicFolder	Объект общей папки, который имеет адрес электронной почты. Дополнительные сведения см. в разделе Общедоступные папки.
MicrosoftExchangeRecipient	Объект, имеющий класс Active Directory **msExchExchangeServerRecipient**. Дополнительные сведения об объекте получателя Exchange см. в разделе Recipients.
Systemmailbox	Объект пользователя, которому назначен электронный адрес и который находится в контейнере системных объектов Microsoft Exchange. В организации Exchange должно быть по одному системному почтовому ящику для каждой базы данных почтовых ящиков.

Запрос Active Directory классифицирует объект, в котором отсутствуют или неправильно отформатированы критически важные свойства, как недопустимый (например, объект динамической группы рассылки без электронного адреса). Для сообщений, отправленных получателям, классифицируемым как недопустимые объекты, создается отчет о недоставке (также называемый сообщением возврата).

Для каждого электронного адреса классификатор отправляет по одному первоначальному запросу возможных свойств получателей (например, их идентификаторов, типов, электронных адресов, альтернативных получателей и ограничений для сообщений). Применимые свойства

получателей кэшируются для дальнейшего использования. При разрешении получатели классифицируются на основе сходства способов их разрешения и применимых свойств.

То, какой фильтр LDAP используется для разрешения адресов, зависит от электронного адреса получателя:

- Фильтр LDAP для типа электронного адреса **EX** основан на атрибуте **legacyExchangeDN** получателя (более высокая важность) или его атрибуте **proxyAddresses** (более низкая важность).
- Для других типов адресов электронной почты в качестве фильтра LDAP используется атрибут **proxyAddresses** получателя.

Если электронный адрес не совпадает с основным SMTP-адресом получателя, классификатор перезаписывает электронный адрес сообщения так, чтобы он соответствовал основному SMTP-адресу. Исходный адрес электронной почты сохраняется в `ORCPT=` записи в команде **RCPT TO** в конверте сообщения.

Ограничения для отправителя сообщения

Размер сообщения может меняться из-за преобразования содержимого, кодирования или обработки агентом. Когда сообщение поступает в организацию Exchange, его исходный размер записывается в поле **X-MS-Exchange-Organization-OriginalSize:** заголовка сообщения. Размер текущего или исходного сообщения (смотря что меньше) используется в качестве ограничения на размер сообщений. Если поле заголовка с размером исходного сообщения не существует, оно создается с использованием текущего размера сообщения. Если размер сообщения слишком большой, отправителю возвращается отчет о недоставке, а дальнейшая обработка сообщения прекращается.

Ограничение на количество отправителей применяется только в службе транспорта на первом сервере почтовых ящиков, обрабатывающем сообщение. Количество получателей исходного (неразвернутого) конверта сообщения сравнивается с ограничением на количество отправителей.

Отправитель и все получатели сообщения помечаются как разрешенные путем установки развернутого свойства сообщения. Это расширенное свойство позволяет сообщению обходить разрешение верхнего уровня, если сообщение снова проходит через разрешение получателей (например, из-за перезапуска транспортной службы Exchange).

Разворачивание

Разворачивание выполняется после разрешения верхнего уровня. При этом вложенные уровни получателей полностью разворачиваются в отдельных получателей. Для разворачивания всех получателей может потребоваться выполнить разворачивание несколько раз. Не всех получателей можно развернуть. Но все получатели проходят через этот процесс, чтобы ограничения для получателей сообщений применялись к получателям всех типов.

В приведенном ниже списке описаны типы получателей, для которых требуется разворачивание.

- **Группы рассылки и динамические группы рассылки**. Группы рассылки развертываются на основе свойства **memberOf** Active Directory. Динамические группы рассылки расширяются с помощью определения запроса Active Directory. Если параметр *ExpansionServer* задан для группы в командной консоли Exchange, группа направляется на указанный сервер для расширения.

  Примечание: При указании сервера расширения для группы группа становится зависимой от доступности сервера расширения (сообщения не могут быть доставлены в группу, если сервер расширения недоступен). Следовательно, рекомендуем реализовывать решения с высоким уровнем доступности для серверов разворачивания.

- **Альтернативные получатели**. Вы можете настроить почтовые ящики и общедоступные папки с поддержкой почты для пересылки сообщений другим получателям:

  - **Почтовые ящики**. Переадресацию можно настроить другому получателю в организации Exchange или на внешний адрес электронной почты. Дополнительные сведения см. в статье Настройка переадресации электронной почты для почтового ящика.

  - **Общедоступные папки с поддержкой почты**. Вы можете настроить переадресацию другому получателю в организации Exchange.

    Вы можете настроить почтовый ящик или общедоступную папку, поддерживающую почту, чтобы сообщения отправлялись только на адрес переадресации либо как исходному получателю, так и на адрес переадресации.

- **Цепочки контактов**. *Цепочка контактов* — это почтовый пользователь или почтовый контакт, где для внешнего адреса электронной почты задан адрес электронной почты другого получателя в организации Exchange.

Обнаружение зацикливания получателей

При разворачивании групп, альтернативных получателей и цепочек контактов классификатор проверяет, есть ли *зацикливание получателей*. Зацикливание получателей — это проблема конфигурации, которая приводит к доставке сообщения одним и тем же получателям в бесконечном цикле. В приведенном ниже списке представлены различные типы зацикливания получателей.

- **Безвредный цикл получателя**. Это два сценария, когда могут возникать циклы безвредных получателей:
  - если две группы рассылки являются членами друг друга;
  - если почтовые ящики или общедоступные папки, поддерживающие почту, настроены на доставку и переадресацию сообщений друг другу (сообщение доставляется исходному получателю и переадресуется).

  Когда классификатор обнаруживает безвредное зацикливание получателей, сообщение доставляется получателю, но дополнительные попытки доставки сообщения тому же получателю не предпринимаются.

- **Цикл неработающего получателя**: если почтовые ящики или общедоступные папки с поддержкой почты перенаправляются друг другу (сообщения перенаправляются только).

  Прерванное зацикливание получателей не может привести к успешной доставке сообщения. Когда классификатор обнаруживает такое зацикливание, разворачивание для текущего получателя прекращается и создается отчет о недоставке.

Обнаружение зацикливания получателей не препятствует доставке сообщений. Рассмотрим следующую ситуацию:

- группа рассылки A включает группы рассылки B и C в качестве членов;
- группа рассылки C также является членом группы рассылки B.

В этом случае в группу рассылки C будут доставляться повторяющиеся сообщения.

Перенаправление отчетов о доставке для групп

При разворачивании группы происходит проверка того, является ли сообщение отчетом о доставке. Если это так, параметры перенаправления группы проверяются на предмет того, требуется ли перенаправление отчета о доставке. Возможно, следует запретить отправку отчетов о доставке для группы, так как они могут содержать конфиденциальные сведения о членах группы.

В приведенном ниже списке перечислены параметры перенаправления отчетов о доставке, доступные в командной строке Exchange для обычных и динамических групп рассылки.

- **Параметр ReportToManagerEnabled**: включает или отключает отправку отчетов о доставке диспетчеру групп. Допустимые значения: `$true` или `$false`. Значение по умолчанию — `$false`. Для группы рассылки диспетчер управляется параметром *ManagedBy* в командлетах **Set-Group** (группы рассылки) или **Set-DynamicDistributionGroup** (динамические группы рассылки).

- **Параметр ReportToOriginatorEnabled**: включает или отключает отправку отчетов о доставке отправителю сообщений для сообщений, отправляемых в группу. Допустимые значения: `$true` или `$false`. Значение по умолчанию — `$true`.

  Примечание. Значения параметра *ReportToManagerEnabled* и *ReportToOriginatorEnabled* не могут быть `$true`одновременно . Если для одного параметра задано значение `$true`, для другого необходимо задать значение `$false`. Значения обоих параметров могут иметь значение `$false`, что подавляет перенаправление всех сообщений отчета о доставке для группы.

В приведенном ниже списке представлены различные типы отчетов о доставке, на которые может повлиять перенаправление отчетов о доставке для групп.

- **Уведомление о доставке (DR)**: подтверждает, что сообщение было доставлено предполагаемому получателю.

- **Уведомление о состоянии доставки (DSN):** описывает результат попытки доставки сообщения, которая не привела к возврату сообщения отправителю в отчете о недоставке (NDR). Дополнительные сведения о сообщениях DSN см. в разделе DSN и NDR в Exchange Server.

- **Уведомление о ликвидации сообщения (MDN):** описывает состояние сообщения после его успешной доставки получателю. Как уведомления о прочтении (RN), так и уведомления о непрочтении (NRN) относятся к сообщениям MDN. Сообщения MDN определены в стандарте RFC 2298, и ими управляет поле **Disposition-Notification-To:** заголовка сообщения. Параметры MDN, в которых используется это поле заголовка, совместимы с различными типами серверов обмена сообщениями. Параметры MDN также можно определить с помощью свойств MAPI в Outlook и Exchange.

- **Отчет о недоставках (NDR)**: указывает отправителю сообщения о том, что сообщение не удалось доставить указанным получателям. Сообщение возвращается отправителю в отчете о недоставке.

- **Уведомление о нечитаемом состоянии (NRN).** Указывает, что сообщение было удалено перед чтением.

- **Нет на месте (OOF):** указывает, что получатель не будет отвечать на сообщения электронной почты. Аббревиатура OOF восходит к исходной системе обмена сообщениями Майкрософт, где соответствующее уведомление было названо "out of facility".

- **Уведомление о прочтении (RN):** указывает, что сообщение было прочитано.

- **Отчет об отзыве**. Указывает состояние запроса на отзыв для определенного получателя (отправитель пытался отозвать отправленное сообщение с помощью Outlook).

Сообщения отчетов о доставке удаляются при их отправке в группу, если используются указанные ниже параметры.

- Для группы не настроено перенаправление отчетов, либо задано перенаправление отправителю сообщения.
- Отчет перенаправляется руководителю группы, а сообщение отчета о доставке не является отчетом о недоставке.

Если задано перенаправление отчетов руководителю группы, а сообщение отчета о доставке является отчетом о недоставке, то сообщение доставляется руководителю группы.

В приведенном ниже списке указано, как параметры перенаправления отчетов о доставке в группы влияют на обычные сообщения, содержащие запросы отчетов.

- Если задано перенаправление отчетов отправителю сообщения, параметры запрашивания отчетов не меняются.
- Если перенаправление отчетов не настроено для группы, все запросы отчетов отклоняются. Запись `NOTIFY=NEVER` добавляется в **RCPT TO** для каждого получателя в конверте сообщения.

- Если задано перенаправление отчетов руководителю группы, то отчеты о недоставке отправляются руководителю группы, но все остальные запросы отчетов отклоняются.

Ограничения для получателей сообщения

При разворачивании также применяются все ограничения для получателей сообщения. Их можно настраивать отдельно для каждого получателя либо для всех серверов в организации Exchange.

Дополнительные сведения об ограничениях на размер сообщений см. в разделах Ограничения для получателей и Ограничения для организации.

Restriction	**Настройка в Центре администрирования Exchange**	**Настройка с помощью командной консоли Exchange**	**Описание**
Максимальный размер принимаемых сообщений	Организация: **поток**> обработки**почты Получать соединители**>**Дополнительные параметры**•••>**Параметры**> транспорта организации **Вкладка "Ограничения"** >**Максимальный размер сообщения о получении (МБ)** Почтовые ящики. **ПолучателиПочтовые ящики**>> выберите ✎ >**редактированияпочтового ящика**> Функции > раздела >**Ограниченияразмера сообщений** раздела >**Просмотр сведений**>**о полученных сообщениях** в разделе >**Максимальный размер сообщения (КБ)** Пользователи **почты: Получатели**>**Контакты**> выберите почтовый пользователь >**Изменить**.✎ >**потока почты**> Ограничения**размера** сообщений раздел >**Просмотр сведений**>**О полученных сообщениях** раздел >**Максимальный размер сообщения (КБ)**	Командлет для организаций: **Set-TransportConfig** Командлеты для получателей: **Set-DistributionGroup**, **Set-DynamicDistributionGroup**, **Set-Mailbox**, **Set-MailContact**, **Set-MailPublicFolder** и **Set-MailUser** Параметр: *MaxReceiveSize*	Задает максимальный размер сообщения, включая заголовок, текст и все вложения. Когда Exchange проверяет размер сообщения, используется размер текущего или исходного сообщения (заголовок сообщения **X-MS-Exchange-Organization-OriginalSize:**), смотря что меньше. Размер сообщения может меняться из-за преобразования содержимого, кодировки и обработки агентом транспорта. **Примечание.** Заданный максимальный размер сообщения сокращается примерно на 33

Restriction	Настройка в Центре администрирования Exchange	Настройка с помощью командной консоли Exchange	Описание
			%, чтобы учесть кодировку Base64 (например, если задано значение 64 МБ, то на самом деле максимальный размер сообщения будет составлять приблизительно 48 МБ). Дополнительные сведения см. в статье Размер сообщений и ограничения получателей в Exchange Server.

Restriction	Настройка в Центре администрирования Exchange	Настройка с помощью командной консоли Exchange	Описание
Получатель может принимать сообщения только от внутренних отправителей и должен отклонять сообщения от внешних отправителей	Почтовые ящики: **получатели**>**Почтовые ящики**> щелкните значок **изменить**.✎ >> Функции >**почтового ящика** Раздел >"**Поток обработки почты**" Раздел **Ограничения доставки сообщений** в разделе >**Просмотр сведений**>**О принятии сообщений из** раздела > проверка или **снятие флажка Требовать проверки подлинности всех отправителей** Удаленные почтовые ящики: **получатели Почтовые ящики**>> выбирают Microsoft 365 или Office 365 почтовый ящик >**Изменить**.✎ >>**Потокобработки сообщений в разделе Ограничения доставки сообщений** раздел >**Просмотр сведений**>**Принять сообщения из** раздела > флажок или снять флажок **Требовать, чтобы все отправители прошли проверку подлинности** Пользователи **почты: Получатели**>**Контакты**> выберите почтового пользователя >**Изменить**.✎> Параметры**потока почты**> Ограничения**доставки сообщений** раздел >**Просмотр сведений**>**О приеме сообщений из** раздела > проверка или отмена флажка **Требовать проверки подлинности всех отправителей** Группы: **Получатели**>**Группы**> выберите группу >**Изменить**.✎ >**редактирования Управление**> доставкой выберите **Только отправители внутри моей организации** или **Отправители внутри и за ее пределами**	Командлеты: **New-DistributionGroup**, **Set-DistributionGroup**, **Set-DynamicDistributionGroup**, **Set-Mailbox**, **Set-MailContact**, **Set-MailPublicFolder**, **Set-MailUser** и **Set-RemoteMailbox** Параметр: *RequireSenderAuthenticationEnabled*	Вы можете сделать так, чтобы получатель принимал сообщения только от отправителей, прошедших проверку подлинности (внутренних), или также принимал сообщения от пользователей, не прошедших проверку подлинности (внешних).
Отправители, которым	Почтовые ящики: **получатели**>**Почтовые ящики**>	Командлеты: **Set-DistributionGroup**, **Set-DynamicDistributionGroup**, **Set-Mailbox**,	Классификатор проверяет

Restriction	Настройка в Центре администрирования Exchange	Настройка с помощью командной консоли Exchange	Описание
разрешено или запрещено отправлять сообщения получателю	щелкните значок **изменить**. >> Функции >**почтового ящика** Раздел >**Поток обработкипочты Раздел Ограничения доставки сообщений** раздел >**Просмотр сведений**>**О принятии сообщений из** раздела: **Все отправители** или **Только отправители в следующем списке** или **Отклонение сообщений из** раздела: **Нет отправителей** или **Отправителей в следующем списке** Удаленные почтовые ящики: **Получатели**>**Почтовые ящики**> выберите Microsoft 365 или Office 365 почтовый ящик >**Изменить**. >>**Потокаобработки сообщений** раздел >**Просмотр сведений**>**. Принять сообщения из** раздела: **Все отправители** или **Только отправители в следующем списке** или **Отклонить сообщения из** раздела: **Нет отправителей** или **Отправители в следующем списке** Пользователи **почты: Получатели**>**Контакты**> Выберите почтовый пользователь >**Изменить**.> Параметры**потока почты**> Раздел**Ограничения доставки** сообщений Просмотр >**сведений**>**Принять сообщения из** раздела: **Все отправители** или **Только отправители в следующем списке** или **Отклонить сообщения из** раздела: **Нет отправителей** или **Отправителей в следующем списке** Группы: **Получатели**>**Группы**> выберите группу >**Изменить**. >**редактирования. Управление**> доставкой нажмите кнопку **Добавить**	**Set-MailContact**, **Set-MailPublicFolder**, **Set-MailUser** и **Set-RemoteMailbox** Принять параметры: *AcceptMessagesOnlyFromSendersOrMembers* (или *AcceptMessagesOnlyFrom* только для отдельных получателей и *AcceptMessagesOnlyFromDLMembers* только для членов группы) Отклонить параметры: *RejectMessagesFromSendersOrMembers* (или *RejectMessagesOnlyFrom* только для отдельных получателей и *RejectMessagesOnlyFromDLMembers* только для членов группы)	разрешения получателей в два этапа. На первом этапе он определяет, присутствует ли отправитель в списках приема или отклонения. Если отправитель не найден ни в одном из списков, группы рассылки в этих параметрах полностью разворачиваются. Полное разворачивание группы может занять некоторое время, поэтому рекомендуем свести к минимуму иерархию вложенных групп в списках приема и отклонения.

Restriction	Настройка в Центре администрирования Exchange	Настройка с помощью командной консоли Exchange	Описание
	или **Удалить**, чтобы указать пользователей или участников группы, которые могут отправлять в группу (сообщения от других отправителей отклоняются).		

Ограничения не распространяются на некоторые типы сообщений, отправляемых прошедшими проверку отправителями. Такие виды сообщений описаны ниже.

- **Сообщения, отправляемые получателем Microsoft Exchange**. К ним относятся dsn и NDR, отчеты журналов, сообщения о квотах и другие системные сообщения, отправляемые внутренним отправителям сообщений. Дополнительные сведения о получателе Microsoft Exchange см. в разделе Получатели.
- **Сообщения, отправляемые по внешнему адресу postmaster**. К ним относятся dsn и NDR, а также другие системные сообщения, отправляемые внешним отправителям сообщений. Дополнительные сведения о внешнем адресе администратора почты см. в статье Managing the External Postmaster Address.

Exchange блокирует определенные типы сообщений, отправляемых во внешние домены (например, внутренние сообщения OOF, автоматические ответы и уведомления о переадресации собраний). Эти параметры настраиваются в удаленных доменах (в стандартном домене или удаленных доменах для определенных внешних доменов). Дополнительные сведения см. в статье Managing Remote Domains.

Развертывание и контроль разворачивания получателей

Так как при разрешении получателей разворачивается и разрешается полный список получателей сообщения, в некоторых случаях необходимо создать несколько копий одного сообщения.

- **Получателям требуются другие параметры сообщения**. Создание новой версии сообщения с немного отличающимися от свойств исходного называется *бифуркацией*. Например, Exchange может потребоваться бифуркировать сообщение, если уведомления о прочтении включены для одних получателей и заблокированы для других.
- **Ограничьте число получателей конвертов в одном сообщении**. Расширение большой группы может создать тысячи отдельных получателей. Вместо создания одной копии сообщения с тысячами получателей конвертов Exchange создает несколько копий одного сообщения с ограниченным числом получателей в конверте сообщения.

Развертывание

Развертывание происходит при разрешении получателей, если выполняются указанные ниже условия.

- При обновлении отправителя сообщения в **mail from** в конверте сообщения (например, если параметр *ReportToManagerEnabled* в группе имеет значение `$true`).
- Требуется запретить сообщения автоматического ответа (например, уведомления о доставке, уведомления о недоставке, сообщения OOF и отчеты об отзыве).
- Разворачиваются альтернативные получатели.
- Поле заголовка **Resent-From:** добавляется в заголовок сообщения. Поля заголовков Resent — это информационные поля заголовков, по которым можно определить, было ли сообщение переадресовано пользователем. Поля Resent применяются для того, чтобы сообщение выглядело так, как если бы оно было отправлено непосредственно исходным отправителем. Просмотрев заголовок сообщения, получатель может узнать, кто переадресовал сообщение. Поля заголовков Resent определяются в разделе 3.6.6 документа RFC 5322.
- Требуется передать журнал разворачивания группы.

Управление разворачиванием получателей

Если количество получателей после разворачивания слишком большое, классификатор делит сообщение на несколько копий, чтобы снизить уровень использования системных ресурсов при разворачивании сообщения. Максимальное число получателей конверта в сообщении управляется ключом *ExpansionSizeLimit* в `%ExchangeInstallPath%Bin\EdgeTransport.exe.config` файле конфигурации приложения. Значение по умолчанию — 1000.

> ⊗ **Внимание!**
>
> Не рекомендуется изменять значение ключа *ExpansionSizeLimit* на транспортном сервере Exchange в рабочей среде.

Диагностика разрешения получателей

Exchange предоставляет сведения об отчетах и диагностике для разрешения получателей в счетчиках производительности, записях журнала отслеживания сообщений и журналах разрешения получателей. Эти источники могут быть полезны для определения и диагностики проблем с разрешением получателей.

Счетчики производительности разрешения получателей

В приведенной ниже таблице описаны счетчики производительности, доступные для разрешения получателей.

Имя счетчика	Отображаемое имя	Описание

Имя счетчика	Отображаемое имя	Описание
AmbiguousRecipientsTotal	Неоднозначных получателей	Общее количество неоднозначных получателей, обнаруженных при разрешении. Неоднозначные получатели — это разные получатели, у которых совпадают **legacyExchangeDN** Active Directory или **proxyAddresses** Active Directory.
AmbiguousSendersTotal	Неоднозначных отправителей	Количество неоднозначных отправителей, обнаруженных в ходе разрешения получателей. Неоднозначные отправители — это разные отправители, у которых совпадают атрибуты **legacyExchangeDN** Active Directory или **proxyAddresses** Active Directory.
FailedRecipientsTotal	Неудачных получателей	Общее количество обнаруженных получателей, разрешение которых не удалось.
LoopRecipientsTotal	Зацикленных получателей	Общее количество получателей, разрешение которых не удалось из-за зацикливания получателей.
MessagesChippedTotal	Усеченных сообщений	Общее количество копий одного сообщения, созданных при разрешении получателей для контроля числа получателей конверта одного сообщения. Этот процесс называется *усечением*.
MessagesCreatedTotal	Создано сообщений	Количество сообщений, созданных при разрешении получателей.
MessagesRetriedTotal	Повторных попыток доставки сообщений	Количество сообщений, для которых была запланирована повторная попытка при разрешении получателей.
НеразрешенныйOrgRecipientsTotal	Получателей с нераспознанной организацией	Количество неразрешенных получателей из уполномоченного домена, обнаруженных при разрешении получателей.
НеразрешенныйOrgSendersTotal	Отправителей с нераспознанной организацией	Количество неразрешенных отправителей из уполномоченного домена, обнаруженных при разрешении получателей.

События разрешения получателей в журнале отслеживания сообщений

В приведенной ниже таблице описаны события разрешения получателей, которые заносятся в журнал отслеживания сообщений.

Событие отслеживания сообщений	Описание
EXPAND	Была расширена группа рассылки.

Событие отслеживания сообщений	Описание
REDIRECT	Сообщение было переслано на адрес переадресации, настроенный для почтового ящика или общедоступной папки, поддерживающей почту.
RESOLVE	Электронный адрес получателя был заменен на основной SMTP-адрес электронной почты соответствующего объекта получателя Active Directory (другими словами, сообщение было отправлено на прокси-адрес получателя).
TRANSFER	Произошло развертывание или усечение сообщения (например, из-за преобразования содержимого, ограничений на количество получателей или агентов транспорта).

Дополнительные сведения об отслеживании сообщений см. в разделе Отслеживание сообщений.

Ведение журнала разрешения получателей

Ведение журнала разрешения получателей управляется ключом *ResolverLogLevel* в `%ExchangeInstallPath%Bin\EdgeTransport.exe.config` файле конфигурации приложения. Допустимые значения этого параметра:

- `Disabled`: данные разрешения получателей не регистрируются. Это значение используется по умолчанию.
- `Enabled`: регистрируются только данные конверта сообщения.
- `FullContent`: регистрируются данные конверта сообщения и данные заголовка сообщения.

Файлы журнала хранятся по адресу `%ExchangeInstallPath%Logging\Resolver`.

> ⓘ **Примечание**
>
> Все настраиваемые параметры Exchange или IIS, внесенные в файлы конфигурации приложения Exchange XML на сервере Exchange Server (например, web.config файлы или EdgeTransport.exe.config файл), **будут перезаписаны** при установке exchange CU. Обязательно сохраните эти сведения, чтобы можно было легко повторно применить параметры после установки. После установки exchange CU необходимо повторно настроить эти параметры.

Агенты транспорта в Exchange Server

Статья • 04.04.2023

Агенты транспорта позволяют установить пользовательское программное обеспечение, созданное корпорацией Майкрософт, сторонними поставщиками или специалистами вашей организации, на сервер Exchange. Это программное обеспечение может обрабатывать сообщения электронной почты, которые проходят через транспортный конвейер. В Microsoft Exchange Server 2016 или 2019 г. транспортный конвейер состоит из следующих процессов:

- Транспортная служба переднего плана на серверах почтовых ящиков
- транспортная служба на серверах почтовых ящиков;
- транспортная служба почтовых ящиков на серверах почтовых ящиков;
- транспортная служба на пограничных транспортных серверах.

Дополнительные сведения о транспортном конвейере см. в разделе Поток обработки почты и конвейер транспорта.

Транспорт Exchange обеспечивает расширяемость с помощью пакета SDK Microsoft Exchange Server транспортных агентов. Версия пакета SDK для Exchange позволяет сторонним организациям реализовать следующие предопределенные классы:

- **SmtpReceiveAgent**
- **RoutingAgent**
- **DeliveryAgent**

При соблюдении требований к библиотекам в пакете SDK результирующие сборки регистрируются в Exchange, который загружает агенты и вызывает их обработчики событий на определенных этапах сеансов SMTP или обработки сообщений. Эти стадии, или события, являются частью определений агентов. Регистрационные данные агента хранятся в файле конфигурации XML.

В следующем списке описаны требования к использованию агентов транспорта в Exchange.

- Транспортная служба на серверах почтовых ящиков и пограничных транспортных серверах полностью поддерживает все предопределенные классы в пакете SDK.
- Служба внешнего транспорта поддерживает только класс **SmtpReceiveAgent** в пакете SDK, а сторонние агенты не могут работать с событием SMTP **OnEndOfData** .

- Транспортная служба почтовых ящиков вообще не поддерживает пакет SDK, поэтому в транспортной службе почтовых ящиков нельзя использовать сторонние агенты.

Управление агентом транспорта

Командлеты агента транспорта должны различать транспортную службу и транспортную службу переднего плана. Командлеты управления агентом транспорта управляют файлом `agents.config` конфигурации, расположенным по адресу `%ExchangeInstallPath%TransportRoles\Shared`.

Дополнительные сведения см. в статье Управление агентами транспорта в Exchange Server.

Агенты транспорта и события SMTP

Агенты транспорта используют события SMTP. Такие события возникают при передаче сообщений через транспортный конвейер. События SMTP предоставляют агентам транспорта доступ к сообщениям в особых точках в процессе сеансов связи SMTP и при маршрутизации сообщений через организацию.

Получение SMTP существует в службе внешнего транспорта на серверах почтовых ящиков, транспортной службе на серверах почтовых ящиков и пограничных транспортных серверах, а также в службе доставки транспорта почтовых ящиков на серверах почтовых ящиков. Классификатор существует только в транспортной службе на серверах почтовых ящиков и пограничных транспортных серверах. Дополнительные сведения о транспортных службах и классификаторе см. в статье Маршрутизация почты в Exchange Server.

В следующих таблицах приведены события SMTP, предоставляющие доступ к сообщениям в конвейере транспорта.

События приема SMTP

Sequence	событие SMTP	Описание
1	**OnConnectEvent**	Это событие инициируется первоначальным подключением удаленного узла SMTP.
2	**OnHeloCommand**	Это событие активируется при выполнении `HELO` команды удаленным узлом SMTP.

Sequence	событие SMTP	Описание
3	**OnEhloCommand**	Это событие активируется при выполнении `EHLO` команды удаленным узлом SMTP.
4	**OnStartTlsCommand**	Это событие активируется при выполнении `STARTTLS` команды удаленным узлом SMTP.
5	**OnAuthCommand**	Это событие активируется при выполнении `AUTH` команды удаленным узлом SMTP.
6	**OnProcessAuthentication**	Это событие инициируется, когда выполняется обработка проверки подлинности с помощью удаленного узла SMTP.
7	**OnEndOfAuthentication**	Это событие инициируется, когда удаленный узел SMTP завершил проверку подлинности.
8	**OnXSessionParamsCommand**	Это событие активируется при выполнении `XSESSIONPARAMS` команды удаленным узлом SMTP.
9	**OnMailCommand**	Это событие активируется при выполнении `MAIL FROM` команды удаленным узлом SMTP.
10	**OnRcptToCommand**	Это событие активируется при выполнении `RCPT TO` команды удаленным узлом SMTP.
11	**OnDataCommand**	Это событие активируется, когда удаленный `DATA` узел SMTP выдает команду (text) или `BDAT` (двоичные данные).
12	**OnEndOfHeaders**	Это событие инициируется, когда удаленный узел SMTP завершает передачу заголовков сообщений электронной почты. На это указывает пустая строка (`<CRLF>`), разделяющая заголовки сообщения и текст сообщения.
13	**OnProxyInboundMessage**	Это событие активируется при ретрансляции входящего сеанса SMTP или *передачи прокси-сервера* службой внешнего транспорта в транспортную службу на сервере почтовых ящиков.

Sequence	событие SMTP	Описание
14	**OnEndOfData**	Это событие активируется, когда удаленный узел SMTP выдает команду конца данных: • Для текстовых сеансов, запускаемых командой `DATA` , конец индикатора данных — `<CRLF>.<CRLF>`. • Для двоичных сеансов, запускаемых командой `BDAT` , конец индикатора данных — `BDAT LAST`.
**	**OnHelpCommand**	Это событие активируется, `HELP` если команда выдана удаленным узлом SMTP.
**	**OnNoopCommand**	Это событие активируется, `NOOP` если команда выдана удаленным узлом SMTP.
**	**OnReject**	Это событие активируется, если получающий узел SMTP выдает временное или постоянное уведомление о состоянии доставки (также известное как DSN, отчет о недоставке, NDR или сообщение о отказе) на отправляющий узел SMTP.
**	**OnRsetCommand**	Это событие активируется, `RSET` если команда выдана отправляемым узлом SMTP.
15	**OnDisconnectEvent**	Это событие инициируется при прекращении сеанса связи SMTP узлом-отправителем или узлом-получателем SMTP. Как правило, это происходит, когда `QUIT` команда выполняется удаленным узлом SMTP.

** Эти события могут возникать в любое время между событиями **OnConnectEvent** и **OnDisconnectEvent**.

Классификатор событий

Sequence	Событие классификатора	Описание
1	**OnSubmittedMessage**	Это событие активируется при поступлении сообщения в очередь отправки в транспортной службе на принимающем сервере Exchange Server.

Sequence	Событие классификатора	Описание
2	**OnResolvedMessage**	Это событие возникает после разрешения всех получателей, но до определения следующего перехода для каждого получателя. Событие маршрутизации **OnResolvedMessage** позволяет последующим событиям переопределять способ маршрутизации по умолчанию с помощью метода **SetRoutingOverride**, выполняемого для отдельных получателей.
3	**OnRoutedMessage**	Это событие инициируется после завершения классификации сообщений, расширения списков рассылки и разрешения получателей.
4	**OnCategorizedMessage**	Это событие инициируется, когда классификатор завершает обработку сообщения.

Приоритет агентов транспорта

Два фактора определяют порядок действий агентов транспорта с сообщениями в конвейере транспорта:

1. Событие SMTP, в котором зарегистрирован агент транспорта, и момент, когда такое событие SMTP обнаруживает сообщения.
2. Значение приоритета, назначенное агенту транспорта, если в одном событии SMTP зарегистрировано несколько агентов. Самый высокий приоритет — 1. Чем больше значение, тем ниже приоритет агента.

Например, предположим, что настроены следующие агенты транспорта:

- В событии SMTP **OnEndOfHeaders** зарегистрированы агент транспорта А с приоритетом 1 и агент транспорта В с приоритетом 2.
- В событии SMTP **OnMailCommand** зарегистрирован агент транспорта Б с приоритетом 4.

Сначала к сообщениям применяется агент транспорта Б, так как событие **OnMailCommand** обнаруживает сообщения раньше, чем событие **OnEndOfHeaders**. Когда сообщения достигают события **OnEndOfHeaders**, сначала применяется агент транспорта А, а затем — В, так как у первого из них приоритет выше (целое значение меньше).

Встроенные агенты транспорта

Exchange Server включает множество встроенных агентов транспорта, которые предоставляют такие функции, как защита от нежелательной почты, правила транспорта и ведение журнала. Большинство встроенных агентов транспорта на серверах почтовых ящиков Exchange недоступны командлетам управления агентами транспорта и не могут контролироваться с их помощью. Практически все встроенные агенты транспорта, которые являются видимыми и управляемыми, находятся в транспортной службе на серверах почтовых ящиков и пограничных транспортных серверах.

Более интересные встроенные агенты транспорта на серверах почтовых ящиков описаны в таблице ниже. Обратите внимание, что в таблицу не включены многие невидимые агенты транспорта, которыми невозможно управлять.

Интересные встроенные агенты транспорта на серверах почтовых ящиков

Имя агента	**Управляемость**	**Приоритет**	**События SMTP или классификатора**
Агент правил транспорта	Да	1	**OnResolvedMessage**
Агент политики защиты от потери данных	Да	2	**OnResolvedMessage**
Агент политики хранения	Да	3	**OnResolvedMessage**
Агент надзорной проверки	Да	4	**OnResolvedMessage**
Агент защиты от вредоносных программ	Да	5	**OnSubmittedMessage**
Агент маршрутизации обмена текстовыми сообщениями	Да	6	**OnSubmittedMessage**
Агент доставки обмена текстовыми сообщениями	Да	7	н/д
Агент SMTP для удаления пробы системы	Да	8	**OnEndOfHeaders**
Агент маршрутизации удаления пробы системы	Да	9	**OnCategorizedMessage**
Агент ведения журнала	Нет	Не настраивается	**OnRoutedMessage**

Имя агента	Управляемость	Приоритет	События SMTP или классификатора
Агент расшифровки отчетов журнала	Нет	Не настраивается	**OnCategorizedMessage**
Агент расшифровки RMS	Нет	Не настраивается	**OnSubmittedMessage**
Агент шифрования RMS	Нет	Не настраивается	**OnSubmittedMessage** **OnRoutedMessage**
Агент расшифровки протокола RMS	Нет	Не настраивается	**OnEndOfData**

Интересные встроенные агенты транспорта на пограничных транспортных серверах

На пограничных транспортных серверах большинство встроенных агентов транспорта доступны для командлетов агентов транспорта и других командлетов и могут контролироваться с их помощью.

Другие интересные встроенные агенты транспорта на пограничных транспортных серверах описаны в таблице ниже. Обратите внимание, что в таблицу не включены невидимые агенты транспорта, которыми невозможно управлять.

Имя агента	Управляемость	Приоритет	События SMTP или классификатора
Агент фильтрации подключений	Да	1	**OnConnectEvent** **OnMailCommand** **OnRcptCommand** **OnEndOfHeaders**
Агент переопределения адресов входящих сообщений	Да	2	**OnRcptCommand** **OnEndOfHeaders**
Агент пограничных правил	Да	3	**OnEndOfData**
Агент фильтра содержимого*	Да	4	**OnEndOfData**
Агент идентификации отправителей*	Да	5	**OnEndOfHeaders**

Имя агента	Управляемость	Приоритет	События SMTP или классификатора
Агент фильтра отправителей*	Да	6	**OnMailCommand** **OnEndOfHeaders**
Агент фильтра получателей	Да	7	**OnRcptCommand**
Агент анализа протоколов*	Да	8	**OnConnectEvent** **OnEndOfHeaders** **OnEndOfData** **OnReject** **OnRsetCommand** **OnDisconnectEvent**
Агент фильтрации вложений	Да	9	**OnEndOfData**
Агент переопределения адресов исходящих сообщений	Да	10	**OnSubmittedMessage** **OnRoutedMessage**

* Вы также можете установить и настроить эти агенты защиты от нежелательной почты на серверах почтовых ящиков. Дополнительные сведения см. в разделе Включение функций защиты от нежелательной почты на серверах почтовых ящиков.

Устранение неполадок агентов транспорта

Устранить неполадки агентов транспорта можно с помощью следующих функций:

- **Get-TransportPipeline**: этот командлет показывает события SMTP и соответствующие агенты транспорта, которые сталкиваются с сообщениями на сервере Exchange Server. Дополнительные сведения см. в разделе Просмотр агентов транспорта в конвейере транспорта в Exchange Server.
- **Трассировка конвейера**. Трассировка конвейера создает точный моментальный снимок сообщения до и после обнаружения каждого агента транспорта. Это позволяет обнаружить агент транспорта, который приводит к неожиданным результатам. Дополнительные сведения см. в разделе Трассировка конвейера.

Управление агентами транспорта в Exchange Server

Статья • 04.04.2023

Агенты транспорта используют события SMTP для обработки сообщений, когда они проходят через транспортный конвейер. Большинство встроенных транспортных агентов, включенных в Microsoft Exchange Server 2016 или 2019 годах, невидимы и неуправляемы. Однако на серверах Exchange в организации можно установить и настроить сторонние агенты транспорта. Дополнительные сведения об агентах транспорта см. в разделе Транспортные агенты в Exchange Server.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 10 минут
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Агенты транспорта" в разделе Разрешения потока обработки почты .
- Для выполнения этой процедуры можно использовать только командную консоль Exchange.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**.

Установка агента транспорта с помощью командной консоли Exchange

При установке агента транспорта Exchange регистрирует только те библиотеки DLL, которые относятся к агенту транспорта. Поэтому все файлы, разделы реестра и другие объекты, влияющие на работу агента транспорта, должны быть установлены и правильно настроены. После загрузки библиотек DLL Exchange продолжает ссылаться на них после завершения выполнения команды.

Агенты транспорта имеют полный доступ ко всем сообщениям электронной почты, которые они обнаруживают. Приложение Exchange не накладывает ограничений на поведение агентов транспорта. Нестабильные агенты транспорта или с недостатками в системе безопасности могут повлиять на стабильность и безопасность Exchange. Поэтому устанавливать следует только те агенты транспорта, которые заслуживают полного доверия и были испытаны в лабораторной среде.

Чтобы исключить влияние не настроенных агентов транспорта на передачу почтовых сообщений, после установки они находятся в отключенном состоянии. Поэтому после правильной настройки агента транспорта его необходимо включить.

Чтобы установить агент транспорта, используйте следующий синтаксис.

PowerShell

```
Install-TransportAgent -Name <TransportAgentIdentity> -TransportAgentFactory
<"TransportAgentFactory"> -AssemblyPath <"FilePath">
```

В этом примере устанавливается вымышленный транспортный агент с именем Contoso Transport Agent в транспортной службе.

PowerShell

```
Install-TransportAgent -Name "Contoso Transport Agent" -
TransportAgentFactory "vendor.exchange.ContosoTransportAgentfactory" -
AssemblyPath "C:\Program
Files\Vendor\TransportAgent\ContosoTransportAgentFactory.dll"
```

Как проверить, что все получилось?

Чтобы убедиться, что агент транспорта успешно установлен, выполните команду `Get-TransportAgent` и убедитесь, что агент транспорта указан в списке.

Включение агента транспорта с помощью командной консоли Exchange

Чтобы включить агент транспорта, используйте следующий синтаксис.

PowerShell

```
Enable-TransportAgent <TransportAgentIdentity>
```

В этом примере агент транспорта с именем Contoso Transport Agent включается в транспортной службе.

```
PowerShell

Enable-TransportAgent "Contoso Transport Agent"
```

Как проверить, что все получилось?

Чтобы убедиться, что агент транспорта включен, выполните команду `Get-TransportAgent | Format-List Name,Enabled` и убедитесь, что агент транспорта включен.

Отключение агента транспорта с помощью командной консоли Exchange

Чтобы отключить агент транспорта, используйте следующий синтаксис:

```
PowerShell

Disable-TransportAgent <TransportAgentIdentity>
```

В этом примере агент транспорта с именем Fabrikam Transport Agent отключается в транспортной службе.

```
PowerShell

Disable-TransportAgent "Fabrikam Transport Agent"
```

Как проверить, что все получилось?

Чтобы убедиться, что агент транспорта успешно отключен, выполните команду `Get-TransportAgent | Format-List Name,Enabled` и убедитесь, что агент транспорта отключен.

Использование командной консоли Exchange для просмотра агентов транспорта

Чтобы просмотреть сводный список всех агентов транспорта, выполните следующую команду:

PowerShell

```
Get-TransportAgent
```

Чтобы просмотреть подробные сведения о конфигурации определенного агента транспорта, выполните следующую команду:

PowerShell

```
Get-TransportAgent <TransportAgentIdentity> | Format-List
```

В этом примере представлена подробная конфигурация агента транспорта с именем "Агент правил транспорта".

PowerShell

```
Get-TransportAgent "Transport Rule Agent" | Format-List
```

Настройка приоритета агента транспорта с помощью командной консоли Exchange

Агенты транспорта, для которых значение приоритета близко к нулю, обрабатывают сообщения электронной почты в первую очередь. Однако событие SMTP в транспортном конвейере, где зарегистрирован агент транспорта, может стать причиной того, что агенты с низким приоритетом будут обрабатывать сообщения раньше агентов с высоким приоритетом.

Чтобы изменить приоритет существующего агента транспорта, выполните следующую команду:

PowerShell

```
Set-TransportAgent <TransportAgentIdentity> -Priority <Integer>
```

В этом примере устанавливается значение агента приоритета 3 для существующего агента транспорта Contoso в транспортной службе.

PowerShell

```
Set-TransportAgent "Contoso Transport Agent" -Priority 3
```

Как проверить, что все получилось?

Чтобы убедиться, что приоритет агента транспорта успешно настроен, выполните команду `Get-TransportAgent | Format-List Name,Priority` и подтвердите значение приоритета агента транспорта.

Удаление агента транспорта с помощью командной консоли Exchange

При удалении агента транспорта Exchange отменяет регистрацию используемых агентом файлов DLL. При этом файлы, разделы реестра или другие объекты, добавляемые при установке агента транспорта, Exchange не удаляет.

Для удаления агента транспорта выполните следующую команду:

PowerShell

```
Uninstall-TransportAgent <TransportAgentIdentity>
```

В этом примере агент транспорта с именем Fabrikam Transport Agent удаляется из транспортной службы.

PowerShell

```
Uninstall-TransportAgent "Fabrikam Transport Agent"
```

Как проверить, что все получилось?

Чтобы убедиться, что агент транспорта успешно удален, выполните команду `Get-TransportAgent` и убедитесь, что агент транспорта отсутствует в списке.

Просмотр агентов транспорта в конвейере транспорта в Exchange Server

Статья • 04.04.2023

С помощью командной консоли Exchange можно просмотреть список агентов транспорта в конвейере транспорта Microsoft Exchange Server 2016 или 2019 годах. А именно, командлет **Get-TransportPipeline** показывает информацию о следующих типах агентов транспорта в конвейере транспорта.

- Агенты на основе классов **SmtpReceiveAgent**, **RoutingAgent**, **DeliveryAgent** и **StorageAgent** в транспортной службе.
- Агенты на основе **smtpReceiveAgentClass** в транспортной службе переднего плана.

Можно просмотреть список всех включенных агентов транспорта, обнаруживших сообщения в транспортном конвейере, и события SMTP, в которых зарегистрированы эти агенты. Дополнительные сведения об агентах транспорта см. в разделе Транспортные агенты в Exchange Server.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Агенты транспорта" в разделе Разрешения потока обработки почты .
- Для выполнения этой процедуры можно использовать только командную консоль Exchange.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**.

Использование командной консоли Exchange для просмотра списка агентов транспорта в конвейере транспорта

Чтобы при помощи командной консоли просмотреть список агентов транспорта в конвейере транспорта на сервере Exchange Server, выполните следующую команду:

```
PowerShell

Get-TransportPipeline | Format-List
```

Чтобы экспортировать результаты в текстовый файл с именем C:\My Documents\Transport Agents.txt, выполните следующую команду:

```
PowerShell

Get-TransportPipeline | Format-List > "C:\My Documents\Transport Agents.txt"
```

Как проверить, все ли получилось?

Командлет **Get-TransportPipeline** выводит только те агенты транспорта, которые обнаружили сообщения в конвейере транспорта в момент времени между запуском службы транспорта и запуском этого командлета. Агент транспорта, который не обнаружил сообщение в транспортном конвейере, не будет отображаться в результатах, отображаемых командлетом **Get-TransportPipeline** , даже если этот агент транспорта включен.

Высокий уровень доступности транспорта в Exchange Server

Статья • 04.04.2023

В Exchange Server высокий уровень доступности транспорта отвечает за хранение избыточных копий сообщений до и после успешной доставки сообщений. Эти функции появились в Exchange 2013 как усовершенствования функций высокого уровня доступности транспорта в Exchange 2010 (например, теневой избыточности и контейнер транспорта), чтобы гарантировать, что сообщения не будут потеряны при передаче.

Ниже представлены основные функции, повышающие высокий уровень доступности транспорта в Exchange 2013, Exchange 2016 и Exchange 2019 по сравнению с Exchange 2010.

- Функция теневого резервирования создает резервную копию сообщения на другом сервере до принятия или подтверждения сообщения. Поддержка сервера отправителя или ее отсутствие не имеет значения для теневого резервирования.

- Функция теневого резервирования распознает группы доступности баз данных и сайты Active Directory как границы высокого уровня доступности транспорта. Это позволяет сократить количество серверов, которые могут содержать резервные копии сообщений, а также устраняет ненужный трафик обслуживания резервных сообщений через группы доступности баз данных или сайты Active Directory.

  Дополнительные сведения см. в разделе Теневая избыточность в Exchange Server.

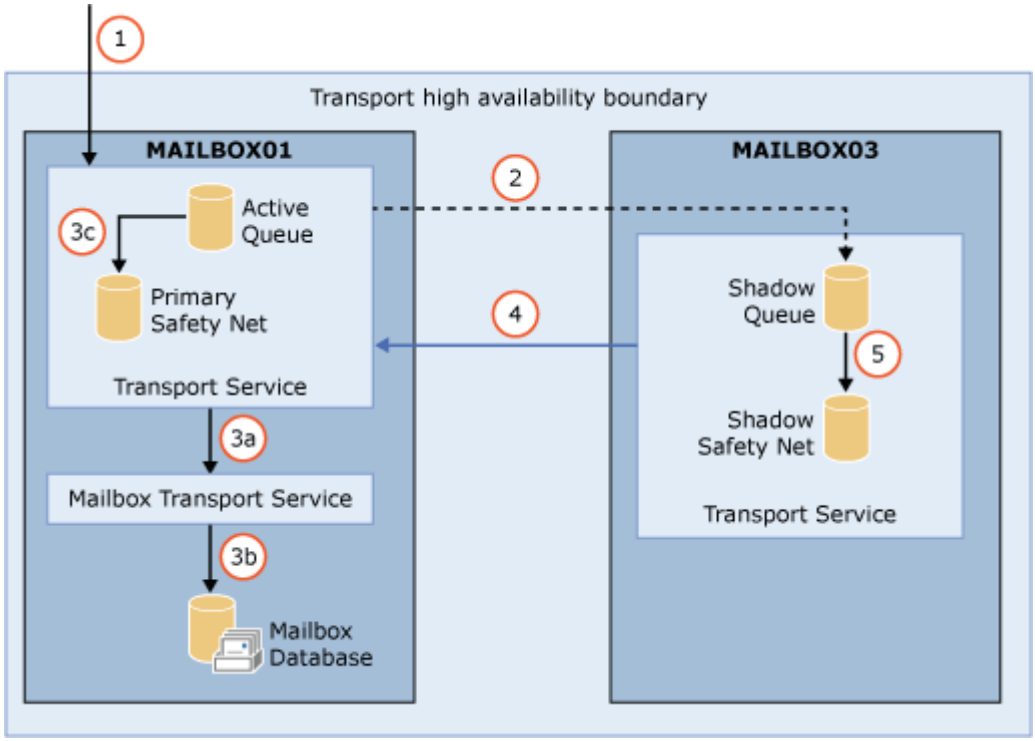
- Транспортная корзина была улучшена и теперь называется *сеть безопасности*. Сеть безопасности хранит сообщения, которые были успешно обработаны службой транспорта на серверах почтовых ящиков. Сеть безопасности лучше всего подходит для серверов почтовых ящиков в группе доступности баз данных, но также работает на нескольких серверах почтовых ящиков на одном сайте Active Directory, не принадлежащих к группе доступности баз данных.

- Теперь резервная копия сети безопасности хранится на другом сервере. Это необходимо, чтобы избежать единой точки отказа, потому что и служба

транспорта, и базы данных почтовых ящиков расположены на сервере почтовых ящиков.

Дополнительные сведения см. в разделе Safety Net в Exchange Server.

На этой схеме представлен общий обзор принципов высокой доступности транспорта в Exchange Server.



1. Сервер почтовых ящиков Exchange с именем Mailbox01 получает сообщение от SMTP-сервера, который находится за пределами границы высокой доступности транспорта. *Граница высокого уровня доступности транспорта* — это daG или сайт Active Directory в средах, отличных от DAG. Сообщение может поступить от:

    - стороннего внутреннего сервера обмена сообщениями;
    - сервера обмена сообщениями в Интернете через прокси-сервер внешней службы транспорта на сервере почтовых ящиков;
    - Другой сервер Exchange в вашей организации.

2. Перед подтверждением получения сообщения Mailbox01 инициирует новый сеанс SMTP на другом сервере почтовых ящиков Exchange с именем Mailbox03, который находится в пределах границы высокой доступности транспорта, и Mailbox03 создает теневой копии сообщения. В средах групп доступности баз данных предпочтителен теневой сервер на удаленном сайте Active Directory. Mailbox01 — это основной сервер, хранящий основное сообщение, а Mailbox03 — теневой сервер, хранящий теневое сообщение.

3. Служба транспорта на Mailbox01 обрабатывает основное сообщение.

   А. В этом примере почтовый ящик получателя находится на Mailbox01, поэтому служба транспорта передает сообщение в локальную службу транспорта почтовых ящиков.

   Б. Транспортная служба почтовых ящиков доставляет сообщение в локальную базу данных почтовых ящиков.

   с. Mailbox01 ставит в очередь статус удаления для Mailbox03, что указывает на то, что основное сообщение было успешно обработано, и Mailbox01 перемещает копию основного сообщения в локальную основную сеть безопасности. Обратите внимание, что сообщение перемещается между очередями в пределах одной и той же базы данных очередей.

4. Mailbox03 периодически опрашивает Mailbox01 о состоянии удаления основного сообщения.

5. Когда Mailbox03 определяет, что Mailbox01 успешно обработал основное сообщение, Mailbox03 перемещает теневое сообщение в локальную теневую сеть безопасности. Обратите внимание, что сообщение перемещается между очередями в пределах одной и той же базы данных очередей.

Сообщение сохраняется в основной и теневой сетях безопасности до истечения срока действия сообщения, в зависимости от настраиваемого значения времени ожидания. Если отработка отказа базы данных почтовых ящиков происходит до истечения срока действия сообщения, основная сеть безопасности на Mailbox01 повторно отправляет сообщение. Если Mailbox01 недоступен, теневая сеть безопасности на Mailbox03 активируется и повторно отправляет сообщение.

Резервирование сообщений во внешней службе транспорта на серверах почтовых ящиков

Внешняя служба транспорта на сервере почтовых ящиков (часть служб клиентского доступа) не имеет очередей сообщений. Это прокси-сервер с неизменным состоянием, принимающий входящие SMTP-подключения и представляющий их службе транспорта на сервере почтовых ящиков. Внешняя служба транспорта поддерживает открытым сеанс SMTP с отправляющим сервером, пока:

- основное сообщение передается в службу транспорта на сервере почтовых ящиков;

и

- служба транспорта создает теневую копию сообщения на другом сервере почтовых ящиков в границах высокого уровня доступности транспорта (группа обеспечения доступности баз данных или сайт Active Directory).

Команда SMTP об окончании передачи данных отправляется обратно отправляющему SMTP-серверу через внешнюю службу транспорта только после того, как основное и теневое сообщения успешно созданы.

Теневая избыточность в Exchange Server

Статья • 04.04.2023

Теневая избыточность была введена в Exchange 2010 для предоставления избыточных копий сообщений перед их доставкой в почтовые ящики. В Exchange 2010 теневая избыточность отложила удаление сообщения из базы данных очереди на транспортном сервере-концентраторе до тех пор, пока сервер не проверит доставку следующего прыжка в пути доставки сообщений. Если следующий прыжок завершился сбоем, прежде чем сообщить об успешной доставке обратно на транспортный сервер-концентратор, сервер повторно перенаправил сообщение на следующий прыжок. Транспортные серверы-концентратор Exchange 2010 использовали команду **XSHADOW** для объявления поддержки теневой избыточности. Если исходный сервер обмена сообщениями не поддерживал теневой избыточности, Exchange 2010 использовал отложенное подтверждение на основе заданного интервала времени в соединителе получения для создания избыточной копии сообщения.

В Exchange 2016 и Exchange 2019 реализованы те же улучшения, которые были внесены в теневой избыточности в Exchange 2013: служба транспорта на сервере почтовых ящиков теперь создает избыточное копирование любого сообщения, которое она получает, прежде чем подтверждает получение сообщения на сервер отправки. Поддержание избыточных копий сообщений при передаче — это не просто лучшие усилия, которые могут или не могут работать, так как теперь теневая избыточность не зависит от поддерживаемых функций отправляющего сервера (поддержка или отсутствие поддержки теневой избыточности не имеет значения). Это гарантирует, что пока все сообщения в конвейере транспорта находятся в пути, для них имеются резервные копии. Если Exchange определяет, что исходное сообщение было потеряно при передаче, избыточное копирование сообщения будет повторно выполнено.

Дополнительные сведения о функциях высокого уровня доступности транспорта в Exchange Server см. в статье Высокий уровень доступности транспорта в Exchange Server. Дополнительные сведения об избыточности сообщений после успешной доставки сообщения см. в разделе Safety Net в Exchange Server.

Компоненты теневого резервирования

В таблице ниже описаны компоненты системы теневого резервирования в службе транспорта на сервере почтовых ящиков. Эти термины используются во всей статье.

Термин	Описание
Граница высокой доступности транспорта	Группа доступности базы данных (DAG) в средах DAG или сайт Active Directory в средах, отличных от DAG. Для групп доступности баз данных, охватывающих несколько сайтов Active Directory, само DAG по-прежнему является границей (а не сайтом). Когда сообщение поступает на сервер почтовых ящиков в пределах границы высокой доступности транспорта, Exchange пытается сохранить две избыточные копии сообщения на серверах почтовых ящиков в пределах границы. Когда сообщение покидает границу высокого уровня доступности транспорта, Exchange прекращает обслуживание избыточных копий сообщения.
Основное сообщение	Сообщение, отправленное в транспортный конвейер для доставки.
Теневое сообщение	Избыточная копия сообщения, которую теневой сервер сохраняет, пока не убедится, что основное сообщение было успешно обработано основным сервером.
Основной сервер	Сервер почтовых ящиков, который в настоящее время обрабатывает основное сообщение.
Теневой сервер	Сервер почтовых ящиков, хранящий теневое сообщение для основного сервера. Сервер почтовых ящиков может одновременно быть основным сервером для некоторых сообщений и теневым сервером для других сообщений.
Теневая очередь	Очередь доставки, где теневой сервер хранит теневые сообщения. Для сообщений с несколькими получателями каждый следующий прыжок для основного сообщения требует отдельной теневой очереди.
Состояние удаления	Информация, которую сервер почтовых ящиков хранит для теневых сообщений, указывающая на то, что основное сообщение было успешно обработано.
Уведомление об удалении	Ответ, который теневой сервер получает от основного сервера, и который указывает, что теневое сообщение готово к отклонению.
Сеть безопасности	Улучшенная версия контейнерной корзины транспорта в Exchange 2013 или более поздней версии. Сообщения, которые были успешно обработаны или доставлены в почтовый ящик получателя транспортной службой на сервере почтовых ящиков, перемещаются в сеть безопасности. Дополнительные сведения см. в разделе Safety Net в Exchange Server.

Термин	Описание
Диспетчер теневой избыточности	Компонент транспорта, управляющий теневой избыточностью.
Пульс	Процесс, который позволяет основным серверам и теневым серверам проверять доступность друг друга.

Требования для теневого резервирования

Хотя это может показаться очевидным, для теневой избыточности требуется несколько серверов почтовых ящиков:

- Если сервер почтовых ящиков не является членом daG, другие серверы почтовых ящиков должны находиться на локальном сайте Active Directory.
- Если сервер почтовых ящиков является участником DAG, другие серверы почтовых ящиков должны принадлежать той же самой DAG. Другие члены DAG могут находиться на локальном сайте Active Directory или на удаленном сайте. По умолчанию, если DAG охватывает несколько сайтов Active Directory, теневая избыточность предпочитает создание избыточной копии сообщения на удаленном сайте для обеспечения устойчивости сайта.

Ниже указаны ситуации, в которых системе теневого резервирования не удается защитить сообщения, находящиеся в пути.

- В средах с одним сервером Exchange.
- В DAG, подготовка которых не завершена.
- При одновременном отказе двух или большего количества серверов почтовых ящиков, участвующих в работе функции теневого резервирования сообщения.

Теневое резервирование включено по умолчанию

По умолчанию теневое резервирование включено глобально в службе транспорта на всех серверах почтовых ящиков. В таблице ниже описаны параметры, которые позволяют использовать теневое резервирование.

Параметр	Значение по умолчанию	Описание
ShadowRedundancyEnabled по **Set-TransportConfig**	`$true`	`$true`: на всех серверах почтовых ящиков в организации включена теневая избыточность. `$false`: Теневая избыточность отключена на всех серверах почтовых ящиков в организации.
RejectMessageOnShadowFailure в **Set-TransportConfig**	`$false`	`$false`: если теневая копия сообщения не может быть создана, основное сообщение в любом случае принимается серверами почтовых ящиков в организации. Когда эти сообщения находятся в пути, их резервные копии не сохраняются. `$true`: ни один сервер почтовых ящиков в организации не принимает или не подтверждает сообщение до тех пор, пока не будет успешно создана теневая копия сообщения. Если не удается создать теневую копию сообщения, основное сообщение будет отклонено с временной ошибкой, но отправляющий сервер может еще раз передать сообщение. Код ответа SMTP — `451 4.4.0 Message failed to be made redundant`. Для всех сообщений в организации, находящихся в пути, сохраняются резервные копии. **Примечание**. Используйте `$true` только в том случае, если на одном сайте DAG или Active Directory имеется несколько серверов почтовых ящиков, чтобы можно было создать теневые копии сообщения. Этот параметр имеет смысл только в том случае, если *ShadowRedundancyEnabled* имеет значение `$true`.

Порядок создания теневых сообщений

Главная цель теневого резервирования состоит в том, чтобы всегда хранить две копии сообщения в пределах границы высокой доступности транспорта, пока сообщение находится в пути. Место и время создания резервной копии сообщения

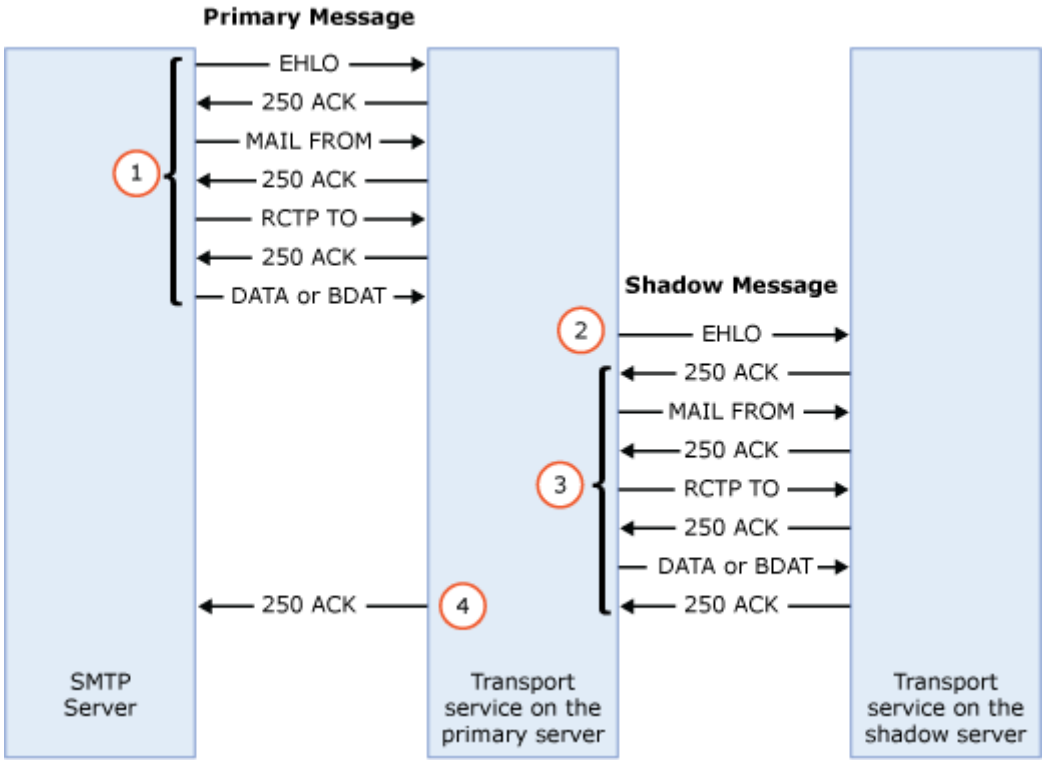
зависит от того, откуда прибыло сообщение и куда оно направляется. Существует три указанных ниже определяющих фактора, используемых при создании теневых сообщений.

- Сообщения, полученные за пределами границы высокого уровня доступности транспорта (daG или сайта Active Directory в средах, отличных от DAG).
- Сообщения, отправленные за пределы границы высокой доступности транспорта.
- Сообщения, полученные от службы отправки транспорта почтовых ящиков с сервера почтовых ящиков в пределах границы высокой доступности.

Теневая избыточность никогда не отслеживает теневые сообщения через границу высокой доступности транспорта. Когда сообщение пересекает границу высокой доступности транспорта, начинается или перезапускается теневая избыточность. Это сокращает трафик обслуживания теневых сообщений и предотвращает повторную отправку теневых сообщений через границу высокого уровня доступности транспорта. Транспортные серверы-концентратор Exchange 2010 — это особый случай, который рассматривается далее в этом разделе.

Сообщения, полученные из-за границы высокой доступности транспорта

Когда служба транспорта на сервере почтовых ящиков получает сообщение из-за границы высокой доступности транспорта, то для этого сервера почтовых ящиков неважно наличие поддержки теневого резервирования на отправляющем сервере. Пока теневое резервирование включено, сервер почтовых ящиков, принимающий сообщение, создает резервную копию сообщения на другом сервере почтовых ящиков в пределах границы высокой доступности транспорта, прежде чем отправить подтверждение получения сообщения на отправляющий сервер. Ниже показан пример такого процесса.



1. Отправляющий сервер передает сообщение в службу транспорта на сервере почтовых ящиков. Сервер почтовых ящиков является основным сервером, а сообщение — основным сообщением.

2. Если исходный сеанс SMTP с сервером обмена сообщениями все еще активен, служба транспорта на основном сервере открывает новый параллельный сеанс SMTP со службой транспорта на другом сервере почтовых ящиков в организации, чтобы создать резервную копию сообщения.

    - Если основной сервер является участником DAG, он подключается к другому серверу почтовых ящиков в той же DAG. Если daG охватывает несколько сайтов Active Directory, по умолчанию предпочтителен сервер почтовых ящиков на другом сайте Active Directory (значение по умолчанию параметра *ShadowMessagePreferenceSetting* в **командлете Set-TransportConfig** — `PreferRemote`, но его можно изменить на `RemoteOnly` или `LocalOnly`).

    - Если сервер-источник не является членом DAG, сервер-источник подключается к другому серверу почтовых ящиков на том же сайте Active Directory (независимо от значения параметра *ShadowMessagePreferenceSetting*).

3. Основной сервер передает копию сообщения в службу транспорта на другом сервере почтовых ящиков, а служба транспорта на другом сервере почтовых ящиков подтверждает, что копия сообщения успешно создана. Копия сообщения является теневым сообщением, и сервер почтовых ящиков, на

котором она находится, является теневым сервером по отношению к основному серверу. Сообщение присутствует в теневой очереди на теневом сервере.

4. После того как основной сервер получает подтверждение от теневого сервера, он отправляет подтверждение получения основного сообщения на исходный сервер обмена сообщениями в исходном сеансе SMTP, и сеанс SMTP будет закрыт.

Сообщения, отправленные за пределы границы высокой доступности транспорта

Когда сервер почтовых ящиков передает сообщение за границу высокой доступности транспорта, сервер обмена сообщениями на другой стороне подтверждает успешное получение сообщения, и сервер почтовых ящиков перемещает это сообщение в сеть безопасности. После успешной передачи основного сообщения через границу высокой доступности транспорта повторная отправка сообщения из сети безопасности не выполняется. Дополнительные сведения о Safety Net см. в разделе Safety Net в Exchange Server.

Сообщения, передаваемые внутри границы высокой доступности транспорта

Маршрутизация сообщений оптимизирована таким образом, что, когда конечное место назначения находится на сайте DAG или Active Directory, несколько прыжков между серверами в целевом DAG или сайте обычно не требуются. После того как сообщение будет принято службой транспорта на сервере почтовых ящиков в целевой DAG или Active Directory, следующий прыжок сообщения обычно является конечным назначением (например, сервер почтовых ящиков, на котором хранится активная копия целевого почтового ящика). Цель теневой избыточности, связанная с сохранением двух копий сообщения при передаче, выполняется, если одна теневая копия сообщения существует в *любом месте* сайта DAG или Active Directory. Обычно несколько прыжков в пределах одной и той же границы высокой доступности транспорта требуются только в сценариях отработки отказа в DAG, для которой необходимо, чтобы командлет **Redirect-Message** опустошал очереди активных сообщений.

Теневая избыточность с помощью транспортных серверов-концентраторов Exchange 2010 на том же

сайте Active Directory в организациях Exchange 2016

Когда транспортный сервер-концентратор Exchange 2010 передает сообщение на сервер почтовых ящиков Exchange 2016 на том же сайте Active Directory, транспортный сервер концентратора Exchange 2010 объявляет о поддержке теневой избыточности с помощью команды XSHADOW, но сервер почтовых ящиков не объявляет поддержку теневой избыточности. Это предотвращает создание теневой копии сообщения на сервере почтовых ящиков Exchange 2016 на сервере почтовых ящиков Exchange 2010.

Когда транспортная служба на сервере почтовых ящиков Exchange 2016 передает сообщение транспорту-концентратору Exchange 2010 на том же сайте Active Directory, сервер почтовых ящиков Exchange 2016 затеняет сообщение для транспортного сервера концентратора Exchange 2010. После того как сервер почтовых ящиков Exchange 2016 получит подтверждение от транспортного сервера концентратора Exchange 2010 о том, что сообщение было успешно получено, сервер почтовых ящиков Exchange 2016 перемещает успешно обработанное сообщение в Safety Net. Однако успешно обработанные сообщения, хранящиеся в Safety Net почтовым ящиком Exchange 2016, никогда не отправляются повторно на транспортные серверы концентратора Exchange 2010.

Время ожидания SMTP

Во время попытки создания резервной копии сообщения может истечь время ожидания для соединения SMTP между серверами (между передающим и основным серверами либо между основным и теневым серверами). Соединители получения и соединители отправки имеют параметр *ConnectionInactivityTimeOut*, указывающий на фактическую передачу данных через соединитель. Соединители получения также имеют абсолютный параметр *ConnectionTimeOut*.

Если какой-либо из сеансов SMTP истекает до успешного создания и подтверждения теневой копии сообщения, результат управляется параметром *RejectMessageOnShadowFailure* в **командлете Set-TransportConfig** . По умолчанию значение этого параметра равно `$false`, что означает, что основное сообщение принимается без создания теневой копии. Если значение этого параметра равно `$true` , основное сообщение отклоняется с временной ошибкой `451 4.4.0`.

Если теневая копия сообщения успешно создана, но истекло время ожидания для сеанса SMTP между отправляющим и основным серверами, основной сервер принимает и обрабатывает основное сообщение. Отправляющий сервер повторно доставит неподтвержденное сообщение, но функция обнаружения дублирующихся

сообщений не позволит отобразить дублирующиеся сообщения для пользователей почтовых ящиков Exchange. Когда отправляющий сервер повторно передает сообщение, основной сервер создает еще одну теневую копию сообщения. При этом нет никакой связи между теневыми сообщениями, созданными во время повторных отправок сообщений с отправляющего сервера.

В таблице ниже описаны параметры, управляющие процессом создания теневых сообщений

Source	**Значение по умолчанию**	**Описание**
ShadowMessagePreferenceSetting в **Set-TransportConfig**	`PreferRemote`	Этот параметр используется только в том случае, если сервер-источник, который пытается создать теневую копию сообщения, является членом daG, охватывающего несколько сайтов Active Directory. • `PreferRemote`: попробуйте создать теневой копии сообщения на члене DAG на другом сайте Active Directory в зависимости от количества попыток, указанного параметром *MaxRetriesForRemoteSiteShadow* . Если операция завершается неудачно, попробуйте создать теневое копирование сообщения в члене DAG на локальном сайте Active Directory на основе количества попыток, указанного параметром *MaxRetriesForLocalSiteShadow* . • `LocalOnly`: попробуйте создать теневые копии сообщения только для члена DAG на локальном сайте Active Directory на основе количества попыток, указанного параметром *MaxRetriesForLocalSiteShadow* . • `RemoteOnly`: попробуйте создать теневое копирование сообщения только для члена DAG на другом сайте Active Directory в зависимости от количества попыток, указанного параметром *MaxRetriesForRemoteSiteShadow* .

Source	Значение по умолчанию	Описание
MaxRetriesForRemoteSiteShadow в **Set-TransportConfig**	4	Этот параметр указывает максимальное число попыток создания теневой копии сообщения на другом сервере в DAG, если значение параметра *ShadowMessagePreferenceSetting* равно `PreferRemote` (значение по умолчанию) или `RemoteOnly`. Этот параметр используется только в том случае, если сервер почтовых ящиков является членом daG, охватывающего несколько сайтов Active Directory. Если не удалось создать теневую копию сообщения после указанного количества попыток, результат зависит от параметра *RejectMessageOnShadowFailure*. • `$true`: основное сообщение отклоняется с временной ошибкой. • `$false`: основное сообщение в любом случае принимается, но не сохраняется избыточно.

Source	Значение по умолчанию	Описание
MaxRetriesForLocalSiteShadow в **Set-TransportConfig**	2	Этот параметр указывает максимальное число попыток создания теневой копии сообщения на другом сервере почтовых ящиков на локальном сайте Active Directory в следующих случаях: • Сервер почтовых ящиков является членом daG, охватывающего несколько сайтов Active Directory, а параметр *ShadowMessagePreferenceSetting* имеет `PreferRemote` значение (значение по умолчанию) или `LocalOnly`. • Сервер почтовых ящиков является членом группы доступности, которая находится на одном сайте Active Directory. • Сервер почтовых ящиков не является участником DAG. Если не удалось создать теневую копию сообщения после указанного количества попыток, результат зависит от параметра *RejectMessageOnShadowFailure*. • `$true`: основное сообщение отклоняется с временной ошибкой. • `$false`: основное сообщение в любом случае принимается, но не сохраняется избыточно.
ConnectionInactivityTimeout в **Set-ReceiveConnector**	5 минут для соединителей получения в службе транспорта на серверах почтовых ящиков	Этот параметр указывает максимальное время, в течение которого открытое подключение SMTP к исходному серверу обмена сообщениями может находиться в состоянии бездействия, прежде чем оно будет закрыто. Значение данного параметра должно быть больше значения параметра *ConnectionTimeout*.

Source	Значение по умолчанию	Описание
ConnectionTimeout в **Set-ReceiveConnector**	10 минут для соединителей получения в службе транспорта на серверах почтовых ящиков	Этот параметр указывает максимальное время, в течение которого подключение SMTP к исходному серверу обмена сообщениями может оставаться открытым, даже если сервер передает данные. Значение данного параметра должно быть больше значения параметра *ConnectionInactivityTimeout*.
ConnectionInactivityTimeOut в **Set-SendConnector**	10 минут	Этот параметр задает максимальное количество времени, в течение которого подключение по протоколу SMTP к конечному серверу обмена сообщениями может оставаться открытым при его бездействии.

Как хранятся теневые сообщения

После успешного создания теневого сообщения работа теневой избыточности только начинается. Основной и теневой серверы должны постоянно находиться в контакте друг с другом, чтобы отслеживать ход сообщения.

Когда основной сервер успешно передает сообщение для следующего прыжка и следующий прыжок подтверждает прием сообщения, основной сервер обновляет *состояние удаления* сообщения, указывая, что оно доставлено. Состояние удаления по сути представляет собой сообщение, содержащее список отслеживаемых сообщений. Успешно доставленное сообщение не обязано находиться в теневой очереди, поэтому когда теневой сервер узнает, что основной сервер успешно передал сообщение для следующего прыжка, теневой сервер перемещает теневое сообщение из теневой очереди в систему безопасности.

Теневой сервер определяет состояние удаления теневых сообщений в теневой очереди путем опроса основного сервера. Если теневой сервер создает сеанс SMTP с основным сервером по какой-либо причине (в том числе при передаче других несвязанных сообщений), теневой сервер отправляет команду **XQDISCARD**, чтобы определить состояние удаления основного сообщения. В противном случае теневой сервер автоматически откроет сеанс SMTP с основным сервером после предварительно настроенного интервала времени (параметр *ShadowHeartbeatFrequency* в **командлете Set-TransportConfig** ; значение по умолчанию — 2 минуты).

После того как теневой сервер откроет сеанс SMTP с основным сервером, основной сервер отвечает *уведомлениями об удалении* для сообщений, относящихся к запрашивающему теневому серверу. Уведомления об отмене хранятся на диске (не в памяти), поэтому при перезапуске службы транспорта Microsoft Exchange уведомления об отмене сохраняются. После запуска службы основной сервер по-прежнему знает о сообщениях, которые он успешно обработал, и эти сведения доступны теневому серверу.

SMTP-связь между теневым сервером и основным сервером используется в качестве *пульса*, определяющего доступность серверов. Если теневому серверу не удается открыть сеанс SMTP с основным сервером после предварительно заданного интервала времени (параметр *ShadowResubmitTimeSpan* в командлете **Set-TransportConfig**; значение, используемое по умолчанию: 3 часа), теневой сервер объявит себя основным сервером, объявит теневые сообщения основными сообщениями и передаст сообщения в следующий прыжок. Но каждый раз, когда теневой сервер обнаруживает, что идентификатор базы данных очереди основного сервера изменился, теневой сервер также объявляет себя основным сервером, объявляет теневые сообщения основными сообщениями и передает сообщения в следующий прыжок. Это может произойти перед передачей значения параметра *ShadowResubmitTimeSpan*.

Диспетчер теневого резервирования — это основной компонент сервера почтовых ящиков, отвечающего за управление теневым резервированием. Диспетчер теневого резервирования отвечает за хранение указанных ниже сведений для всех основных сообщений, обрабатываемых в настоящее время сервером.

- Теневой сервер для каждого обрабатываемого основного сообщения.
- Состояние удаления, которое необходимо отправить на теневые серверы.

Диспетчер теневого резервирования отвечает за следующие действия для всех теневых сообщений, находящихся в теневых очередях теневого сервера:

- сохранение списка основных серверов для каждого теневого сообщения;
- сравнение исходного идентификатора базы данных и текущего идентификатора базы данных очереди, где хранится основная копия сообщения;
- проверка доступности каждого основного сервера, в очередь для которого помещено теневое сообщение;
- обработка уведомлений об удалении для основных серверов.

- удаление теневых сообщений из теневых очередей после получения всех ожидаемых уведомлений об удалении;
- принятие решений о том, когда теневой сервер должен вступить во владение теневыми сообщениями и стать основным сервером.
- Отслеживание развертываний сообщений и других побочных эффектов, например уведомлений о состоянии доставки (отчетов или сообщений о недоставке), а также отчетов журнала, чтобы гарантировать, что резервная копия сообщения не будет выпущена до полной обработки всех ветвлений сообщения.

В таблице ниже описаны параметры, управляющие порядком хранения теневых сообщений.

Параметр	**Значение по умолчанию**	**Описание**
ShadowHeartbeatFrequency в **Set-TransportConfig**	2 минуты	Максимальный период времени, в течение которого теневой сервер ждет перед открытием SMTP-подключения к основному серверу, чтобы проверить состояние удаления из сообщения.
ShadowResubmitTimeSpan в **Set-TransportConfig**	3 часа	Время ожидания сервера до принятия решения о том, что на основном сервере произошел сбой, и присвоения владения теневыми сообщениями в теневой очереди для недоступного основного сервера. Обратите внимание, что теневой сервер также может объявлять себя основным сервером до изменения значения этого параметра, когда обнаруживается, что база данных очереди основного сервера имеет другой идентификатор базы данных.

Параметр	Значение по умолчанию	Описание
ShadowMessageAutoDiscardInterval в **Set-TransportConfig**	2 дня	Время, в течение которого сервер сохраняет события удаления для успешно доставленных сообщений. Основной сервер ставит события удаления в очередь, пока не получит запрос от теневого сервера. Тем не менее если теневой сервер не запрашивает основной сервер в течение периода, указанного в этом параметре, основной сервер удаляет события удаления, поставленные в очередь.
SafetyNetHoldTime по **Set-TransportConfig**	2 дня	Время, в течение которого успешно обработанные сообщения хранятся в сети безопасности. Неподтвержденные теневые сообщения в конечном итоге будут удалены сети безопасности после истечении определенного срока — суммы значений параметров *SafetyNetHoldTime* и *MessageExpirationTimeout* в командлете **Set-TransportService**.
MessageExpirationTimeout по **Set-TransportService**	2 дней	Как долго сообщение может оставаться в очереди до истечения срока его действия.

Обработка сообщений после сбоев

В таблице ниже содержатся сводные сведения о том, как теневое резервирование сводит к минимуму потерю сообщений из-за сбоев на серверах. Для определенности допустим, что сбой произошел на сервере Mailbox01.

Сценарий восстановления	Выполняемые действия

Сценарий восстановления	Выполняемые действия
Сервер Mailbox01 возобновляет работу с использованием новой базы данных очереди до того как было передано значение параметра *ShadowResubmitTimeSpan* (по умолчанию 3 часа). Этот сценарий возможен, если не удается восстановить очередь базы данных из-за сбоя оборудования или повреждения данных.	При обнаружении нового идентификатора базы данных очереди на сервере Mailbox01 каждый сервер, поместивший теневые сообщения в очередь для сервера Mailbox01, признает себя владельцем этих сообщений и повторно отправит их. После этого сообщения будут доставлены по назначению. Максимальная задержка при отправке сообщений после обнаружения новой базы данных очереди определяется значением параметра *ShadowHeartbeatFrequency* (по умолчанию 2 минуты).
Mailbox01 возвращается к сети с той же базой данных после прохождения значения параметра *ShadowResubmitTimeSpan* (по умолчанию 3 часа). Этот сценарий возможен после сбоя сетевого адаптера или продолжительного сеанса технического обслуживания на сервере.	После того как сервер Mailbox01 возобновит работу, он доставит сообщения, находящиеся в его очередях, которые уже были доставлены серверами, хранящими теневые копии сообщений для сервера Mailbox01. Это приведет к дублированию всех таких сообщений. Пользователи почтовых ящиков Exchange не будут видеть повторяющиеся сообщения из-за обнаружения повторяющихся сообщений. Тем не менее для получателей в других системах обмена сообщениями дублирующиеся сообщения, возможно, будут отображены. Максимальная задержка отправки сообщения — это значение параметра *ShadowResubmitTimeSpan* .

Сеть безопасности в Exchange Server

Статья • 04.04.2023

В Exchange 2010 *контейнер транспорта* помог защититься от потери данных, поддерживая очередь успешно доставленных сообщений, которые не реплицировались в пассивные копии базы данных почтовых ящиков в группе доступности баз данных (DAG). Когда при сбое сервера или базы данных почтовых ящиков требовалось продвижение устаревшей копии базы данных почтовых ящиков, сообщения в транспортной корзине автоматически повторно отправлялись в новую активную копию базы данных почтовых ящиков.

Контейнер транспорта был улучшен в Exchange 2013 и теперь называется *Safety Net*. В Exchange 2016 и Exchange 2019 есть те же улучшения.

Чем сеть безопасности похожа на транспортную корзину в Exchange 2010.

- Сеть безопасности — это очередь, связанная с транспортной службой на сервере почтовых ящиков. В этой очереди хранятся копии сообщений, успешно обработанных сервером.
- Вы можете указать срок хранения сетью безопасности копий успешно обработанных сообщений до их автоматического удаления. Значение по умолчанию — 2 дней.

Чем сеть безопасности лучше транспортной корзины в Exchange 2010:

- **Safety Net не требует daG**. Для серверов почтовых ящиков, которые не принадлежат к daG, Safety Net сохраняет копии доставленных сообщений на других серверах почтовых ящиков на локальном сайте Active Directory.
- **Сеть безопасности сама по себе не является единственной точкой отказа**: избыточность обеспечивается с помощью *основной сети безопасности* и *теневой сети безопасности*. Если основная сеть безопасности недоступна более 12 часов, запросы на повторную отправку становятся запросами на теневую повторную отправку и сообщения повторно доставляются из теневой сети безопасности.
- **Safety Net берет на себя некоторую ответственность от теневой избыточности в средах DAG**. Теневая избыточность не требует хранить другую копию доставленного сообщения в теневой очереди, пока она ожидает репликации доставленного сообщения в пассивные копии базы данных почтовых ящиков. Копия доставленного сообщения уже хранится в

сети безопасности, следовательно, в случае необходимости сообщение может быть повторно отправлено из сети безопасности.

- **Safety Net пытается гарантировать избыточность сообщений**: Safety Net — это больше, чем просто лучший способ обеспечения избыточности сообщений, поэтому невозможно указать максимальный размер для Safety Net. Вы можете задать только длительность хранения сообщений в сети безопасности перед их автоматическим удалением.

Дополнительные сведения о функциях высокого уровня доступности транспорта в Exchange Server см. в статье Высокий уровень доступности транспорта в Exchange Server. Дополнительные сведения об избыточности сообщений при передаче см. в разделе Теневая избыточность в Exchange Server.

Принцип работы сети безопасности

Теневое резервирование хранит резервную копию сообщения на протяжении его передачи. Сеть безопасности хранит резервную копию сообщения после его успешной обработки. Таким образом, сеть безопасности начинается там, где заканчивается теневое резервирование. К сети безопасности применимы те же понятия, что и к теневому резервированию, а именно "граница высокого уровня доступности транспорта", "основные сообщения", "основные серверы", "теневые сообщения", "теневые серверы". Дополнительные сведения см. в разделе Теневая избыточность в Exchange Server.

Основная сеть безопасности существует на сервере почтовых ящиков, где основное сообщение хранится до того, как будет успешно обработано транспортной службой. Это может означать, что сообщение было доставлено в службу доставки транспорта почтовых ящиков по пути к серверу почтовых ящиков. Или могло быть ретранслировано через сервер почтовых ящиков на сайт Active Directory, который был назначен концентратором на пути к конечной группе обеспечения доступности баз данных почтовых ящиков или сайту Active Directory. После обработки основного сообщения основным сервером оно перемещается из активной очереди доставки в основную сеть безопасности на том же сервере.

Теневая сеть безопасности существует на сервере почтовых ящиков, удерживающем теневое сообщение. После того как теневой сервер определяет, что основной сервер успешно обработал основное сообщение, он перемещает теневое сообщение из теневой очереди в теневую сеть безопасности на том же сервере. Конечно же, существование теневой сети безопасности требует включенного теневого резервирования (включено по умолчанию).

В приведенной ниже таблице описаны параметры, используемые в сети безопасности.

Параметр	Значение по умолчанию	Описание
SafetyNetHoldTime по **Set-TransportConfig**	2 дней	Временной период, на протяжении которого успешно обработанные основные сообщения хранятся в основной сети безопасности, а подтвержденные теневые сообщения хранятся в теневой сети безопасности. Это значение также можно указать в Центре администрирования Exchange (EAC) на странице**Соединители получения**потока >**почты**>**Дополнительные параметры**••• >**Параметры**> транспорта организации **Safety Net**>**Время удержания в сети безопасности**. Срок хранения неподтвержденных теневых сообщений в теневой сети безопасности истекает после сложения значений параметров *SafetyNetHoldTime* и *MessageExpirationTimeout*. Чтобы избежать потери данных во время повторной отправки Safety Net, значение этого параметра должно быть больше или равно значению *ReplayLagTime* в **Set-MailboxDatabaseCopy** для отстающей копии базы данных почтового ящика.
Параметр *ReplayLagTime* в командлете **Set-MailboxDatabaseCopy**	Не настроено	Время ожидания службы репликации Microsoft Exchange перед воспроизведением файлов журнала, скопированных в пассивную копию базы данных. Если для данного параметра установлено значения больше 0, создается изолированная копия базы данных почтовых ящиков. Наибольшее значение — 14 дней. Чтобы избежать потери данных во время повторной отправки Safety Net, значение этого параметра для отстающей копии базы данных почтовых ящиков должно быть меньше или равно значению *SafetyNetHoldTime* в **Set-TransportConfig**.
MessageExpirationTimeout по **Set-TransportService**	2 дней	Как долго сообщение может оставаться в очереди до истечения срока его действия.

Параметр	Значение по умолчанию	Описание
ShadowRedundancyEnabled по **Set-TransportConfig**	`$true`	`$true`: на всех серверах почтовых ящиков в организации включена теневая избыточность. `$false`: Теневая избыточность отключена на всех транспортных серверах в организации. Резервирование сети безопасности требует включенного теневого резервирования.

Максимальные поддерживаемые размеры в Safety Net

В Microsoft Exchange Server 2019 и 2016 годах максимальный поддерживаемый размер базы данных Safety Net JET для транспорта составляет 2 ТБ.

При использовании звездообразной топологии транспортная база данных Safety Net JET может превысить 2 ТБ. Чтобы не превышать поддерживаемое ограничение в 2 ТБ, следуйте приведенным ниже рекомендациям.

- Серверы-концентраторы, используемые для ретрансляции сообщений, не могут быть настроены для доставки сообщений в почтовые ящики.
- Отключите Safety Net на центральных серверах, используемых для ретрансляции сообщений. Для этого выполните следующие действия:

    1. В окне командной строки откройте файл EdgeTransport.exe.config в **Блокноте** , выполнив на сервере следующую команду:

        DOS

        ```
        Notepad %ExchangeInstallPath%Bin\EdgeTransport.exe.config
        ```

    2. Добавьте следующий ключ в раздел **appSettings** .

        XML

        ```
        <add key="SafetyNetHoldTimeInterval" value="0.00:00:15" />
        ```

        Закончив, сохраните и закройте файл EdgeTransport.exe.config.

3. Перезапустите службу Транспорт Exchange, выполнив следующую команду:

```
DOS

net stop MSExchangeTransport && net start MSExchangeTransport
```

Повторная отправка сообщений из сети безопасности

Компонент Active Manager службы репликации Microsoft Exchange (MSExchangeRepl.exe) управляет dag и копиями базы данных почтовых ящиков. Повторная отправка сообщений из сети безопасности не требует действий, выполняемых вручную, и запускается компонентом Active Manager. Дополнительные сведения о компоненте Active Manager см. в разделе Active Manager.

Существует два основных сценария повторной отправки сообщения из сети безопасности.

- После автоматической или ручной отработки отказа баз данных почтовых ящиков в группе обеспечения доступности баз данных.
- После активации изолированной копии базы данных почтовых ящиков.

Изолированная копия базы данных почтовых ящиков или *изолированная копия* — это пассивная копия базы данных почтовых ящиков, где обновления базы данных намеренно откладываются для защиты базы данных почтовых ящиков от логического повреждения. Дополнительные сведения см. в разделе Управление копиями базы данных почтовых ящиков.

Единственная существенная разница между этими двумя сценариями — значение задержки для повторной отправки сообщений из сети безопасности. Как правило, для отработки отказа базы данных в группе обеспечения доступности баз данных разница во времени между новой и старой активными копиями баз данных почтовых ящиков составляет от нескольких минут до нескольких часов. Изолированная копия базы данных почтовых ящиков обычно отстает от старой активной копии на несколько дней.

Главное требование для успешной повторной отправки изолированной копии из сети безопасности — время хранения сообщений в сети безопасности должно превышать или быть равным интервалу задержки изолированной копии. Другими

словами, для изолированной копии значение параметра *SafetyNetHoldTime* в **Set-TransportConfig** должно превышать значение параметра *ReplayLagTime* (или быть равным ему) в **Set-MailboxDatabaseCopy**.

Повторная отправка сообщений из теневой сети безопасности

Как и в случае с основной сетью безопасности, повторная отправка сообщений из теневой сети безопасности полностью автоматическая и не требует ручного вмешательства. Этот сценарий описывает взаимодействие основной и теневой сетей безопасности в процессе повторной отправки сообщений.

1. Active Manager запрашивает повторную отправку сообщений из сети безопасности для базы данных почтовых ящиков за определенный временной интервал (например, 05:00–09:00). Однако на сервере почтовых ящиков, хранящем основную сеть безопасности, произошел сбой из-за сбоя оборудования. В течение следующих 12 часов Active Manager безуспешно пытается установить связь с основной сетью безопасности.

2. По прошествии 12 часов Active Manager отправляет широковещательное сообщение в транспортную службу на всех серверах почтовых ящиков в границах высокого уровня доступности транспорта (группа обеспечения доступности баз данных или сайт Active Directory в средах без таких групп) в поисках сетей безопасности, содержащих сообщения для целевой базы данных почтовых ящиков за указанный интервал времени. Ответом теневой сети безопасности служит повторная отправка сообщений для базы данных почтовых ящиков за период времени с 05:00 до 09:00.

Когда теневая сеть безопасности отвечает, она повторно отправляет сообщения для требуемой базы данных почтовых ящиков только на протяжении требуемого периода времени. Это ограничение по базе данных почтовых ящиков и временному интервалу помогает уменьшить количество таких потенциальных проблем:

- Повторная отправка сообщений из сети безопасности может привести к дублирующимся сообщениям. Это не проблема для почтовых ящиков в организации Exchange, поскольку система определения повторяющихся сообщений скрывает дублирующиеся сообщения от пользователя почтового ящика. Однако внешние пользователи могут увидеть несколько одинаковых повторяющихся сообщений.

- Теневые сообщения, повторно отправленные из теневой сети безопасности, требуют полной классификации и обработки через службу транспорта на сервере почтовых ящиков. Повторная отправка большого количества теневых сообщений может быть дорогой в плане ресурсов сервера почтовых ящиков.

Необходимо учесть несколько важных рекомендаций относительно теневых сообщений, хранящихся в теневой сети безопасности.

- Теневая сеть безопасности не владеет информацией о том, куда основной сервер передал основное сообщение.

- Теневые сообщения в теневой сети безопасности содержат только получателей конверта исходного сообщения, а не фактических получателей, которым было доставлено основное сообщение (например, получателем конверта сообщения может быть группа рассылки, требующая развертывания).

- В сообщениях теневой сети безопасности нет обновлений сообщения, появившихся после его обработки основным сервером (например, шифрования сообщения или преобразования содержимого).

Этот сценарий описывает, что происходит, если основная сеть безопасности работает автономно во время запрошенного интервала на повторную отправку:

1. База данных очереди на сервере почтовых ящиков, хранящем основную сеть безопасности, повреждена, а новая база данных очереди создана в 07:00. Все основные сообщения, которые хранились в основной сети безопасности с 01:00 до 07:00, утеряны, но сервер способен хранить копии успешно доставленных сообщений в сети безопасности, начиная с 07:00.

2. Active Manager запрашивает повторную отправку сообщений из сети безопасности для базы данных почтовых ящиков за временной интервал 01:00–09:00.

3. Основная сеть безопасности повторно оправляет сообщения за временной интервал 07:00–09:00.

4. Поскольку основная сеть безопасности не содержит необходимых сообщений с 1:00 до 7:00. Основная сеть безопасности отправляет широковещательное сообщение в транспортную службу на всех серверах почтовых ящиков в пределах границы высокой доступности транспорта в поисках других сетей безопасности, содержащих необходимые сообщения. Shadow Safety Net создает второй запрос на повторную отправку от имени основной сети

безопасности для повторной отправки теневых сообщений для целевой базы данных почтовых ящиков за интервал времени с 1:00 до 7:00.

При повторной отправке сообщений из сети безопасности также следует принимать во внимание и другие аспекты:

- **Все уведомления о состоянии доставки (также известные как dsn, отчеты о недоставке, недоставки или сообщения о недоставке) подавляются для повторной отправки сообщений Safety Net**. Например, если основное сообщение привело к недоставке, недоставка для повторно отправленного сообщения не будет доставлена.

- **Пользователи, удаленные из группы рассылки, могут не получить повторно отправленное сообщение, когда Shadow Safety Net повторно отправляет сообщение**: например, сообщение отправляется группе, содержащей пользователей A и пользователя B, и оба получателя получают это сообщение. Пользователь B впоследствии удаляется из группы. Позже для базы данных почтовых ящиков, в которой хранится почтовый ящик пользователя B, будет выполнен запрос на повторную отправку из основной сети Safety Net. Однако основная сеть безопасности недоступна более 12 часов, поэтому сервер Shadow Safety Net отвечает и повторно отправляет затронутое сообщение. Во время повторной отправки сообщения при развертывании группы рассылки пользователь Б больше не является членом группы и не получит копию повторно отправленного сообщения.

- **Новые пользователи, добавленные в группу рассылки, могут получать старое повторно отправленное сообщение, когда теневая сеть безопасности повторно отправляет сообщение**: например, сообщение отправляется группе, содержащей пользователя A и пользователя B, и оба получателя получают сообщение. Пользователь C впоследствии добавляется в группу. Позже для базы данных почтовых ящиков, в которой хранится почтовый ящик пользователя C, будет выполнен запрос на повторную отправку из основной сети Safety Net. Однако основной сервер Safety Net недоступен более 12 часов, поэтому сервер Shadow Safety Net отвечает и повторно отправляет затронутые сообщения. Во время повторной отправки сообщения при развертывании группы рассылки пользователь C теперь является членом группы и получит копию повторно отправленного сообщения.

- **Развертывание Safety Net в звездообразной топологии**: Safety Net предназначена для защиты доставки сообщений на серверах Exchange Server, на которые размещаются почтовые ящики конечных пользователей. Клиенты, которые развернули топологию звездообразной маршрутизации, должны

отключить Safety Net на транспортных серверах на центральных сайтах, чтобы избежать значительного увеличения размера транспортной базы данных в расположениях концентраторов.

Журналы транспорта в Exchange Server

Статья • 04.04.2023

Журналы транспорта предоставляют сведения о том, что происходит в транспортном конвейере. Дополнительные сведения о транспортном конвейере см. в статье Mail flow and the transport pipeline.

Журналы транспорта в Exchange Server описаны в следующих разделах.

Ведение журнала агентов

Ведение журнала агента записывает действия, выполняемые с сообщениями определенными агентами транспорта защиты от спама на сервере Exchange Server. Дополнительные сведения см. в следующих статьях:

- Ведение журнала агента антиспамов
- Настройка ведения журнала агента antispam
- Включение функций защиты от нежелательной почты на серверах почтовых ящиков

Включено по умолчанию?: Да

Расположение файлов журнала по умолчанию. Обратите внимание, что папка не создается до тех пор, пока агент не попытается записать сведения в журнал.

- **Серверы почтовых ящиков**:
  - **Транспортная служба переднего плана**: `%ExchangeInstallPath%TransportRoles\Logs\FrontEnd\AgentLog`
  - **Транспортная служба**: `%ExchangeInstallPath%TransportRoles\Logs\Hub\AgentLog`
- **Служба транспорта на пограничных транспортных серверах**: `%ExchangeInstallPath%TransportRoles\Logs\Edge\AgentLog`

Ведение журнала подключений

Ведение журнала подключений регистрирует действия передачи исходящих сообщений транспортными службами на сервере Exchange Server. Дополнительные сведения см. в следующих статьях:

- Ведение журнала подключений в Exchange Server
- Настройка ведения журнала подключений в Exchange Server

Включено по умолчанию?: Да

Расположение файлов журнала по умолчанию:

- **Серверы почтовых ящиков**:
  - **Транспортная служба переднего плана**: `%ExchangeInstallPath%TransportRoles\Logs\FrontEnd\Connectivity`
  - **Транспортная служба**: `%ExchangeInstallPath%TransportRoles\Logs\Hub\Connectivity`
  - **Служба доставки транспорта почтовых ящиков**: `%ExchangeInstallPath%TransportRoles\Logs\Mailbox\Connectivity\Delivery`
  - **Служба отправки транспорта почтовых ящиков**:
- **Служба транспорта на пограничных транспортных серверах**: `%ExchangeInstallPath%TransportRoles\Logs\Edge\Connectivity`

Отчеты об отслеживании и доставке сообщений для администраторов

Отслеживание сообщений — это подробная запись обо всех действиях сообщений при прохождении почты через транспортный конвейер на сервере Exchange Server. Дополнительные сведения см. в следующих статьях:

- Отслеживание сообщений
- Настройка отслеживания сообщений
- Поиск в журналах отслеживания сообщений

Отчеты о доставке для администраторов — это целевой поиск журнала отслеживания сообщений, отправленных в указанный почтовых ящик или из него. Дополнительные сведения см. в следующих статьях:

- Отчеты о доставке для администраторов
- Отслеживание сообщений при помощи отчетов о доставке

Включено по умолчанию?: Да

Расположение файлов журнала по умолчанию:

- **Серверы почтовых ящиков**: `%ExchangeInstallPath%TransportRoles\Logs\MessageTracking`:
  - Файлы `MSGTRK` для службы транспорта.
  - Файлы `MSGTRMD` для службы доставки транспорта почтовых ящиков.
  - Файлы `MSGTRMS` для службы отправки транспорта почтовых ящиков.
- **Служба транспорта на пограничных транспортных серверах**: `%ExchangeInstallPath%TransportRoles\Logs\MessageTracking`

Трассировка конвейера

При трассировке конвейера записываются моментальные снимки сообщений до и после их обработки агентами транспорта в транспортном конвейере. Дополнительные сведения см. в следующих статьях:

- Конвейерная трассировка
- Настройка трассировки конвейера

Включено по умолчанию?: Нет

Расположение файлов журнала по умолчанию. Обратите внимание, что папка не создается, пока не будет включена трассировка конвейера.

- **Серверы почтовых ящиков**:
  - **Транспортная служба**: `%ExchangeInstallPath%TransportRoles\Logs\Hub\PipelineTracing`
  - **Транспортная служба почтовых ящиков**: `%ExchangeInstallPath%TransportRoles\Logs\Mailbox\PipelineTracing`
- **Служба транспорта на пограничных транспортных серверах**: `%ExchangeInstallPath%TransportRoles\Logs\Edge\PipelineTracking`

Ведение журнала протокола

Ведение журнала протокола содержит сведения о связи через SMTP в случае соединителей отправки и получения во время доставки сообщений. Дополнительные сведения см. в следующих статьях:

- Ведение журнала протокола
- Настройка ведения журнала протокола

Включено по умолчанию?: только на следующих соединителях:

- Соединитель получения по умолчанию с именем Default Frontend *<ServerName>* в транспортной службе переднего плана на серверах почтовых ящиков.
- неявного и невидимого соединителя отправки во внешней службе транспорта на серверах почтовых ящиков.

Дополнительные сведения об этих соединителях см. в разделах Соединители приема по умолчанию, созданные во время установки и Неявные соединители отправки.

Расположение файлов журнала по умолчанию:

- **Серверы почтовых ящиков**:
  - **Внешняя служба транспорта**:
  - **Соединители получения**: `%ExchangeInstallPath%TransportRoles\Logs\FrontEnd\ProtocolLog\SmtpReceive`
  - **Отправка соединителей**: `%ExchangeInstallPath%TransportRoles\Logs\FrontEnd\ProtocolLog\SmtpSend`
  - **Служба транспорта**:
  - **Соединители получения**: `%ExchangeInstallPath%TransportRoles\Logs\Hub\ProtocolLog\SmtpReceive`
  - **Отправка соединителей**: `%ExchangeInstallPath%TransportRoles\Logs\Hub\ProtocolLog\SmtpSend`
  - **Служба доставки транспорта почтовых ящиков (соединители получения):** `%ExchangeInstallPath%TransportRoles\Logs\Mailbox\ProtocolLog\SmtpReceive\Delivery`

    - **Служба отправки транспорта почтовых ящиков**:
    - **Отправка соединителей**: `%ExchangeInstallPath%TransportRoles\Logs\Mailbox\ProtocolLog\SmtpSend\Submission`
    - **Сообщения о побочных эффектах**: `%ExchangeInstallPath%TransportRoles\Logs\Mailbox\ProtocolLog\SmtpSend\Delivery`
- **Служба транспорта на пограничных транспортных серверах**:
    - **Соединители получения**: `%ExchangeInstallPath%TransportRoles\Logs\Edge\ProtocolLog\SmtpReceive`
    - **Отправка соединителей**: `%ExchangeInstallPath%TransportRoles\Logs\Edge\ProtocolLog\SmtpSend`

Ведение журнала таблицы маршрутизации

Примечание. Средство просмотра журналов маршрутизации больше не доступно на панели элементов Exchange.

Ведение журнала таблицы маршрутизации периодически записывает моментальные снимки таблицы маршрутизации, которую серверы Exchange server используют для доставки сообщений. Дополнительные сведения см. в следующих статьях:

- Общие сведения о ведении журнала таблицы маршрутизации
- Настройка ведения журнала таблицы маршрутизации

Включено по умолчанию?: Да

Расположение файлов журнала по умолчанию:

- **Серверы почтовых ящиков**:
    - **Транспортная служба переднего плана**: `%ExchangeInstallPath%TransportRoles\Logs\FrontEnd\Routing`
    - **Транспортная служба**: `%ExchangeInstallPath%TransportRoles\Logs\Hub\Routing`
    - **Транспортная служба почтовых ящиков**:`%ExchangeInstallPath%TransportRoles\Logs\Mailbox\Routing` :

    - Файлы `MDRoutingConfig` для службы доставки транспорта почтовых ящиков.
    - Файлы `MSRoutingConfig` для службы отправки транспорта почтовых ящиков.
- **Служба транспорта на пограничных транспортных серверах**: `%ExchangeInstallPath%TransportRoles\Logs\Edge\Routing`

Отслеживание сообщений

Статья • 04.04.2023

Журнал отслеживания сообщений — это подробная запись обо всех действиях, когда почта проходит через транспортный конвейер на серверах почтовых ящиков и пограничных транспортных серверах. Вы можете использовать отслеживание сообщений для криминалистической экспертизы сообщений, анализа потока почты, составления отчетов и устранения неполадок.

По умолчанию Exchange использует циклическое ведение журнала, чтобы ограничить журнал отслеживания сообщений в зависимости от размера файла и возраста файла, чтобы управлять местом на жестком диске, используемым файлами журнала. Сведения о настройке журнала отслеживания сообщений см. в разделе Настройка отслеживания сообщений.

Поиск в журнале отслеживания сообщений

Журналы отслеживания сообщений содержат огромные объемы данных при перемещении сообщений через сервер почтовых ящиков или пограничный транспортный сервер. Когда дело доходит до поиска журналов отслеживания сообщений, у вас есть варианты:

- **Get-MessageTrackingLog**. Администраторы могут использовать этот командлет командной консоли Exchange для поиска в журнале отслеживания сообщений на наличие сведений о сообщениях с использованием широкого спектра условий фильтра. Дополнительные сведения см. в разделе Журналы отслеживания сообщений поиска.

- **Отчеты о доставке для администраторов**. Администраторы могут использовать вкладку **Отчеты о доставке** в Центре администрирования Exchange или базовые командлеты **Search-MessageTrackingReport** и **Get-MessageTrackingReport** в командной консоли Exchange, чтобы найти в журналах отслеживания сообщений сведения о сообщениях, отправленных или полученных определенным почтовым ящиком в организации. Дополнительные сведения см. в статье Отчеты о доставке для администраторов.

Структура файлов журналов отслеживания сообщений

По умолчанию файлы журнала отслеживания сообщений существуют в `%ExchangeInstallPath%TransportRoles\Logs\MessageTracking`. Папка содержит файлы журналов с разными именами, но все они следуют соглашению `MSGTRKServiceyyyymmdd-nnnn.log` об именовании . Различные имена файлов журнала описаны в следующей таблице.

Имя файла	Серверы	Описание
`MSGTRK`	Серверы почтовых ящиков и пограничные транспортные серверы	Файлы журнала для службы транспорта.
`MSGTRKMA`	Серверы почтовых ящиков	Файлы журнала для утверждений и отклонений в модерируемом транспорте. Дополнительные сведения см. в разделе Управление утверждением сообщений.
`MSGTRKMD`	Серверы почтовых ящиков	Файлы журналов для сообщений, доставленных в почтовые ящики службой доставки транспорта почтовых ящиков.
`MSGTRKMS`	Серверы почтовых ящиков	Файлы журналов для сообщений, отправленных из почтовых ящиков службой отправки транспорта почтовых ящиков.

Другие заполнители в именах файлов журнала представляют следующие сведения:

- *yyyymmdd* — это дата создания файла журнала (в формате UTC). *гггг* = год, *мм* = месяц, и *дд* = день.
- *nnnn* — это номер экземпляра, который начинается со значения 1 каждый день для каждого журнала.

Данные записываются в файл журнала, пока не будет достигнут его максимальный размер. Затем открывается новый файл журнала с увеличенным номером экземпляра (-1 для первого, -2 для второго и т. Циклическое ведение журнала удаляет самые старые файлы журнала для службы при выполнении любого из следующих условий:

- достигнут максимальный срок хранения файла журнала;
- Папка журнала отслеживания сообщений достигает максимального размера.

  Примечания.

- Максимальный размер папки журнала отслеживания сообщений вычисляется как общий размер всех файлов журнала с одинаковым префиксом имени. Другие файлы, которые не соответствуют соглашению о префиксе имени, не учитываются при вычислении общего размера папки. Переименование старых файлов журнала или копирование других файлов в папку журнала отслеживания сообщений может привести к превышению указанного максимального размера папки.
- На серверах почтовых ящиков максимальный размер папки журнала отслеживания сообщений в три раза больше указанного значения. Несмотря на то, что файлы журнала отслеживания сообщений создаются четырьмя разными службами и имеют четыре разных префикса имен, объем и частота записи данных в журнал транспорта с модерированием (`MSGTRKMA`) незначительно по сравнению с тремя другими журналами.

Файлы журналов отслеживания сообщений представляют собой текстовые файлы с данными в формате CSV. Каждый файл журнала отслеживания сообщений имеет заголовок, содержащий следующие сведения:

- **#Software**: значение равно `Microsoft Exchange Server`.
- **#Version**: номер версии сервера Exchange Server, создавшего файл журнала отслеживания сообщений. Значение использует формат `15.01.nnnn.nnn`.
- **#Log-Type**: значение равно `Message Tracking Log`.
- **#Date**: дата и время создания файла журнала в формате UTC. Дата-время в формате UTC представлено в формате даты и времени ISO 8601: *гггг-мм-дд*T*чч:мм:ss.fff*Z, где *гггг* = год, *мм* = месяц, *дд* = день, T указывает начало компонента времени, *чч* = час, *мм* = минута, *ss* = секунда, *fff* = доли секунды, а Z обозначает Zulu, что является еще одним способом обозначения UTC.
- **#Fields**: имена полей с разделителями-запятыми, которые используются в файлах журнала отслеживания сообщений.

Поля в файлах журналов отслеживания сообщений

В журнале отслеживания сообщений каждое событие, связанное с сообщением, заносится в отдельную строку. Информация о событиях с сообщениями упорядочена по полям, разделенным запятыми. Обычно имя поля достаточно полно характеризует информацию, которая в нем хранится. Однако некоторые

поля могут быть пустыми, или тип сведений в поле может меняться в зависимости от типа события сообщения и службы, записавшей событие. В следующей таблице приводятся общие описания полей, которые используются для классификации каждого события отслеживания сообщений.

Имя поля	Описание
date-time	Дата и время события отслеживания сообщений в формате UTC. Дата-время в формате UTC представлено в формате даты и времени ISO 8601: *гггг-мм-ддТчч:мм:ss.fffZ*, где *гггг* = год, *мм* = месяц, *дд* = день, T указывает начало компонента времени, *чч* = час, *мм* = минута, *ss* = секунда, *fff* = доли секунды, а Z обозначает Zulu, что является еще одним способом обозначения UTC.
client-ip	Адрес IPv4 или IPv6 сервера или клиента, который отправил сообщение.
client-hostname	Имя узла или полное доменное имя сервера или клиента обмена сообщениями , который отправил сообщение.
server-ip	IPv4- или IPv6-адрес исходного или целевого сервера.
server-hostname	Имя узла или полное доменное имя сервера назначения.
source-context	Дополнительная информация, относящаяся к полю **источника**. Например: `CatContentConversion` `250 2.0.0 OK;ClientSubmitTime:<UTC>`
connector-id	Имя соединителя отправки или соединителя получения, которые приняли сообщение. Например, *serverName*\ *ConnectorName* или *ConnectorName*.
источник	Транспортный компонент Exchange, отвечающий за событие. Эти значения описаны в разделе Исходные значения в журнале отслеживания сообщений далее в этом разделе.
event-id	Тип события. Эти значения описаны в разделе Типы событий в журнале отслеживания сообщений далее в этом разделе.
internal-message-id	Идентификатор сообщения, назначенный сервером Exchange Server, который в настоящее время обрабатывает сообщение. **Внутренний идентификатор сообщения** отличается в журнале отслеживания сообщений на каждом сервере Exchange Server, который участвует в передаче сообщения. Пример значения — `73014444033`.
message-id	Значение поля заголовка **Message-Id:** в заголовке сообщения. Если поле заголовка **Message-Id:** не существует или пустое, Exchange присваивает произвольное значение. Это значение не изменяется на протяжении всего времени жизни сообщения. Для сообщений, созданных в Exchange, значение имеет формат `<GUID@ServerFQDN>`, включая угловые скобки (`< >`). Например, `<4867a3d78a50438bad95c0f6d072fca5@mailbox01.contoso.com>`. В других системах обмена сообщениями могут использоваться другие значения или синтаксис.

Имя поля	Описание
network-message-id	Уникальное значение идентификатора сообщения, которое сохраняется в различных копиях сообщения, которые могут создаваться в связи с развертыванием или расширением группы рассылки. Пример значения — `1341ac7b13fb42ab4d4408cf7f55890f`.
recipient-address	Адрес электронной почты получателя сообщения. Если указано несколько адресов, то они отделяются друг от друга точкой с запятой (;).

recipient-status	Состояние получателя для каждого получателя, разделенное символом с запятой (;). Значения состояния представляются получателям в таком же порядке, как и значения в поле **recipient-address**. Примеры значений состояния:
	`To`, `Cc` или `Bcc`
	`250 2.1.5 Recipient OK`
	`550 4.4.7 QUEUE.Expired;<ErrorText>`

total-bytes	Общий размер сообщения в байтах, включая все вложения.
recipient-count	Общее число получателей в сообщении.
related-recipient-address	Это поле используется с событиями **EXPAND**, **REDIRECT** и **RESOLVE** для отображения других адресов электронной почты получателей, связанных с сообщением.
reference	В этом поле содержится дополнительная информация о конкретных типах событий. Например: **DSN**: содержит ссылку на отчет, которая является значением **Message-Id** связанного уведомления о состоянии доставки (также известного как DSN, сообщение о отказе, отчет о недоставке или NDR), если dsN создается после этого события. Если это сообщение DSN, поле **Reference** содержит значение **Message-Id** исходного сообщения, для чего было создано DSN. **EXPAND**: содержит значение **адреса связанного получателя** для связанных сообщений. **RECEIVE**: может содержать значение **Message-Id** связанного сообщения, если сообщение было создано другими процессами, например правилами генерации журналов или папки "Входящие". **SEND**: содержит значение **Internal-Message-Id** всех сообщений DSN. **THROTTLE**: содержит причину регулирования сообщения. **TRANSFER**: содержит значение **Internal-Message-Id** вилки сообщения. **Сообщение, созданное правилами папки "Входящие**". Содержит значение **Internal-Message-Id** входящего сообщения, которое привело к созданию исходящего сообщения правилом папки "Входящие". **Вилки сообщений**: может содержать значение **Internal-Message-Id** . Для других типов событий это поле обычно пустое.

Имя поля	Описание
message-subject	Тема сообщения указывается в поле заголовка **Subject:**. Отслеживание тем сообщений управляется параметром *MessageTrackingLogSubjectLoggingEnabled* командлета **Set-TransportService** . По умолчанию отслеживание тем сообщений включено.
sender-address	Адрес электронной почты, указанный в поле **заголовка Sender:** или Поле заголовка **From:** , если поле **Sender:** не существует.
return-path	Возвращаемый адрес электронной почты, указанный командой **MAIL FROM** , отправляющей сообщение. Хотя это поле никогда не является пустым, оно может иметь значение null отправителя, представленное как `<>`.
message-info	Дополнительные сведения о сообщении. Например: Дата и время возникновения сообщения в формате UTC для событий **DELIVER** и **SEND** . Это дата и время первоначального поступления сообщения в организацию Exchange. Дата-время в формате UTC представлено в формате даты и времени ISO 8601: *гггг-мм-дд*T*чч:мм:ss.fff*Z, где *гггг* = год, *мм* = месяц, *дд* = день, T указывает начало компонента времени, *чч* = час, *мм* = минута, *ss* = секунда, *fff* = доли секунды, а Z обозначает Zulu, что является еще одним способом обозначения UTC. Ошибки проверки подлинности. Например, вы можете увидеть значение `11a` и тип проверки подлинности, которые использовались при возникновении ошибки проверки подлинности.
directionality	Направление сообщения. Примеры значений: `Incoming`, `Undefined` и `Originating`.
tenant-id	Это поле не используется в локальных организациях Exchange.
original-client-ip	Адрес IPv4 или IPv6 исходного клиента.
original-server-ip	Адрес IPv4 или IPv6 исходного сервера.
custom-data	Это поле содержит данные, связанные с определенными типами событий. Например, агент правил транспорта использует это поле для записи GUID правила потока обработки почты (также известного как правило транспорта) или политики защиты от потери данных, которая действовала в сообщении. Дополнительные сведения см. в разделе Просмотр отчетов об обнаружении политики защиты от потери данных.
transport-traffic-type	В локальной среде Exchange это поле пустое или имеет значение `Email`.
log-id	Уникальный идентификатор строки в журнале отслеживания сообщений. Это поле не важно в локальных организациях Exchange.

Имя поля	Описание
schema-version	Номер версии сервера Exchange Server, создавшего запись в журнале отслеживания сообщений. Значение использует формат `15.01.nnnn.nnn`.

Типы событий в журнале отслеживания сообщений

Различные типы событий в поле **event-id** используются для классификации событий, связанных с сообщениями, в журнале отслеживания сообщений. Некоторые события, связанные с сообщениями, отображаются только в одном типе файлов журнала отслеживания сообщений, а некоторые — во всех типах файлов. Типы событий, используемые для классификации каждого события, приведены в следующей таблице.

Имя события	Описание
AGENTINFO	Это событие используется агентами транспорта для журналирования пользовательских данных.
BADMAIL	Сообщение отправлено каталогом раскладки или каталогом преобразования и не может быть доставлено и возвращено.
CLIENTSUBMISSION	Сообщение отправлено из папки "Исходящие" почтового ящика.
DEFER	Доставка сообщения отложена.
DELIVER	Сообщение было доставлено в локальный почтовый ящик.
DELIVERFAIL	Агент пытался доставить сообщение в папку, которая не существует в почтовом ящике.
DROP	Сообщение было отклонено без уведомления о доставке (также называемого сообщением возврата или отчетом о недоставке). Например: • сообщения о выполненных запросах для утверждения; • нежелательные сообщения, удаленные автоматически без отчета о недоставке.
DSN	Создано уведомление о доставке.

Имя события	Описание
DUPLICATEDELIVER	Сообщение было доставлено получателю повторно. Повторная доставка сообщений может происходить в том случае, если получатель входит в несколько вложенных групп рассылки. Банк данных обнаруживает и удаляет дубликаты сообщений.
DUPLICATEEXPAND	При расширении группы рассылки обнаружен повторяющийся получатель.
DUPLICATEREDIRECT	Альтернативный получатель сообщения уже являлся получателем.
EXPAND	Была расширена группа рассылки.
FAIL	Не удается доставить сообщение. Источники: **SMTP**, **DNS**, **QUEUE** и **ROUTING**.
HADISCARD	Теневое сообщение было отвергнуто, после того как основная копия была доставлена на следующий узел. Дополнительные сведения см. в разделе Теневая избыточность в Exchange Server.
HARECEIVE	Теневое сообщение было получено сервером в локальной группе обеспечения доступности баз данных или на сайте Active Directory.
HAREDIRECT	Создано теневое сообщение.
HAREDIRECTFAIL	Не удалось создать теневое сообщение. Сведения сохранены в поле **source-context**.
INITMESSAGECREATED	Сообщение отправлено контролируемому получателю, поэтому оно отправлено в почтовый ящик вынесения решения для утверждения. Дополнительные сведения см. в разделе Управление утверждением сообщений.
LOAD	Сообщение успешно загружено при загрузке.
MODERATIONEXPIRE	Модератор контролируемого получателя не утвердил и не отклонил сообщение, поэтому для него истек срок ожидания. Дополнительные сведения о получателях с модерированием см. в разделе Управление утверждением сообщений.
MODERATORAPPROVE	Модератор контролируемого получателя утвердил сообщение, поэтому оно было доставлено контролируемому получателю.

Имя события	Описание
MODERATORREJECT	Модератор контролируемого получателя отклонил сообщение, поэтому оно не было доставлено контролируемому получателю.
MODERATORSALLNDR	Все запросы на утверждение, отправленные всем модераторам модерированного получателя, были недоступны и привели к отчетам о недоставке (также известных как недоставка или отказ сообщений).
NOTIFYMAPI	Сообщение было обнаружено в папке "Исходящие" почтового ящика на локальном сервере.
NOTIFYSHADOW	Сообщение было обнаружено в папке "Исходящие" почтового ящика на локальном сервере, и необходимо создать теневую копию сообщения.
POISONMESSAGE	Сообщение помещено в очередь сообщений о сбое или удалено из нее.
PROCESS	Сообщение успешно обработано.
PROCESSMEETINGMESSAGE	Сообщение о собрании обработано службой транспортной доставки почтовых ящиков.
RECEIVE	Сообщение было получено компонентом получения SMTP службы транспорта или из каталогов Pickup или Replay (источник: `SMTP`), либо сообщение было отправлено из почтового ящика в службу отправки транспорта почтовых ящиков (источник: `STOREDRIVER`).
REDIRECT	Сообщение перенаправлено другому получателю в результате поиска в Active Directory.
RESOLVE	В результате поиска в Active Directory для получателей сообщения был найден другой адрес электронной почты.
RESUBMIT	Сообщение было автоматически повторно отправлено из сети безопасности. Дополнительные сведения см. в разделе Safety Net в Exchange Server.
RESUBMITDEFER	Сообщение, повторно отправленное из сети безопасности, было отложено.
RESUBMITFAIL	Сообщение, повторно отправленное из сети безопасности, не удалось отправить.
SEND	Сообщение было отправлено протоколом SMTP между службами транспорта.

Имя события	Описание
SUBMIT	Служба отправки почтовых ящиков успешно передала сообщение службе транспорта. Для событий **SUBMIT** свойство **source-context** содержит следующие данные: • **MDB**: GUID базы данных почтовых ящиков. • **Mailbox**: GUID почтового ящика. • **Event**: порядковый номер события. • **MessageClass**: тип сообщения. Например, `IPM.Note`. • **CreationTime**: дата отправки сообщения. • **ClientType**: например, `User`, `OWA` или `ActiveSync`.
SUBMITDEFER	Передача сообщения из службы доставки почты в почтовый ящик в службу транспорта была отложена.
SUBMITFAIL	Передача сообщения из службы доставки почты в почтовый ящик в службу транспорта не была выполнена.
SUPPRESSED	Передача сообщения была отменена.
THROTTLE	Сообщение было отрегулировано.
TRANSFER	В результате преобразования содержимого, ограничения числа получателей или работы агентов получатели были перемещены в сообщение с ветвлением. Источники: **ROUTING** или **QUEUE**.

Значения источника в журнале отслеживания сообщений

Значения в поле **source** в журнале отслеживания сообщений указывает на компонент транспорта, ответственный за событие отслеживания сообщений. В следующей таблице описаны значения поля **source**.

Значение источника	Описание
ADMIN	Источник события был введен пользователем. Например, администратор использовал средство просмотра, чтобы удалить сообщение, или отправил файлы сообщений с помощью каталога воспроизведения.
AGENT	Источником события был агент транспорта.

Значение источника	Описание
APPROVAL	Источником события была платформа утверждения, используемая для контролируемых получателей. Дополнительные сведения см. в разделе Управление утверждением сообщений.
BOOTLOADER	Источником события были необработанные сообщения, которые присутствовали на сервере на момент загрузки. Это относится к типу событий **LOAD**.
DNS	Источником события было DNS.
DSN	Источником события было уведомление о состоянии доставки (также известное как DSN, сообщение о отказе, отчет о недоставке или NDR).
GATEWAY	Источником события был внешний соединитель. Подробнее см. в разделе Foreign Connectors.
MAILBOXRULE	Источником события было правило для папки "Входящие". Дополнительные сведения см. в разделе Правила папки "Входящие".
MEETINGMESSAGEPROCESSOR	Источником события был обработчик сообщения о собрании, который обновляет календари в соответствии с обновлениями собрания.
ORAR	Источником события был альтернативный получатель, запрошенный отправителем (ORAR). Вы можете включить или отключить поддержку ORAR в соединителях получения с помощью параметра *OrarEnabled* в командлетах **New-ReceiveConnector** или **Set-ReceiveConnector** .
PICKUP	Источником события был каталог раскладки. Подробнее см. в разделе Pickup Directory and Replay Directory.
POISONMESSAGE	Источником события был идентификатор сообщения о сбое. Дополнительные сведения о подозрительных сообщениях и очереди подозрительных сообщений см. в разделе Очереди и сообщения в очередях.
PUBLICFOLDER	Источником события была общедоступная папка, поддерживающая почту.
QUEUE	Источником события была очередь.
REDUNDANCY	Источником события было избыточное теневое копирование. Дополнительные сведения см. в разделе Теневая избыточность в Exchange Server.

Значение источника	Описание
РАСПОЗНАВАТЕЛЯ	Источником события был компонент разрешения получателей классификатора в транспортной службе. Дополнительные сведения см. в разделе Разрешение получателей в Exchange Server.
ROUTING	Источником события был компонент разрешения маршрутизации классификатора в службе транспорта.
SAFETYNET	Источником события была сеть безопасности. Дополнительные сведения см. в разделе Safety Net в Exchange Server.
SMTP	Сообщение было отправлено компонентом отправки или получения SMTP службы транспорта.
STOREDRIVER	Источником события была MAPI-отправка из почтового ящика на локальном сервере.

Примеры записей в журнале отслеживания сообщений

Не вызвавшее событий сообщение, отправленное между двумя пользователями, создает несколько записей в журнале отслеживания сообщений. Результаты можно просмотреть с помощью командлета **Get-MessageTrackingLog**. Дополнительные сведения см. в разделе Журналы отслеживания сообщений поиска.

Это пример записей журнала отслеживания сообщений, созданных при успешной отправке пользователем chris@contoso.com тестового сообщения пользователю michelle@contoso.com. У обоих пользователей есть почтовые ящики на одном и том же сервере.

```
EventId    Source      Sender            Recipients
MessageSubject
-------    ------      ------            ----------              ------------
--
NOTIFYMAPI STOREDRIVER                   {}
RECEIVE    STOREDRIVER chris@contoso.com {michelle@contoso.com} test
SUBMIT     STOREDRIVER chris@contoso.com {michelle@contoso.com} test
HAREDIRECT SMTP        chris@contoso.com {michelle@contoso.com} test
RECEIVE    SMTP        chris@contoso.com {michelle@contoso.com} test
AGENTINFO  AGENT       chris@contoso.com {michelle@contoso.com} test
SEND       SMTP        chris@contoso.com {michelle@contoso.com} test
DELIVER    STOREDRIVER chris@contoso.com {michelle@contoso.com} test
```

Журнал отслеживания сообщений и вопросы безопасности

В журнале отслеживания сообщений не хранится содержимое сообщений. По умолчанию в этот журнал заносятся темы сообщений электронной почты. В соответствии с повышенными требованиями к безопасности или конфиденциальности может потребоваться отключить ведение журнала субъектов. Инструкции по отключению ведения журнала тем см. в разделе Настройка отслеживания сообщений.

Настройка отслеживания сообщений в Exchange Server

Статья • 04.04.2023

В журнал отслеживания сообщений записывается информация о потоке обработки почты на серверах почтовых ящиков и пограничных транспортных серверах. Журналы отслеживания можно использовать для исследования сообщений, анализа потока обработки почты, создания отчетов и устранения неполадок.

Используйте командлет **Set-TransportService** в командной консоли Exchange на серверах почтовых ящиков и пограничных транспортных серверах для любых задач настройки отслеживания сообщений. Примеры использования:

- Включение и отключение отслеживания сообщений. По умолчанию регистрация включена.
- Выбор расположения файлов журналов отслеживания сообщений. Расположение по умолчанию — `%ExchangeInstallPath%TransportRoles\Logs\MessageTracking`.
- Задание максимального размера отдельных файлов журналов отслеживания сообщений. Значение по умолчанию — 10 МБ.
- Задание максимального размера каталога, который содержит файлы журналов отслеживания сообщений. Значение по умолчанию — 1 000 МВ.
- Задание максимального времени хранения файлов журналов отслеживания сообщений. Значение по умолчанию — 30 дней.
- Включение и отключение регистрации темы сообщений в журналах отслеживания сообщений. По умолчанию регистрация включена.

> ⓘ **Примечание**
>
> На серверах почтовых ящиков можно использовать Центр администрирования Exchange (EAC), чтобы включать и отключать отслеживание сообщений, а также указывать расположение файлов журнала отслеживания сообщений.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записях "Транспортная служба" в разделе Разрешения потока обработки почты .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Настройка отслеживания сообщений на серверах почтовых ящиков с помощью Центра администрирования Exchange

1. Откройте EAC и **перейдите в раздел Серверы**>,> выберите сервер почтовых ящиков, который нужно настроить>, и нажмите кнопку **Изменить**.
2. На странице свойств сервера нажмите кнопку **Журналы транспорта**. В разделе **Журнал отслеживания сообщений** измените следующие параметры:
   - **Включить журнал отслеживания сообщений**. Чтобы отключить отслеживание сообщений на сервере, снимите флажок. Чтобы включить отслеживание сообщений на сервере, установите этот флажок.
   - **Путь к журналу отслеживания сообщений**. Указанное значение должно находиться на локальном сервере Exchange Server. Если папка не существует, она будет создана после нажатия кнопки **Сохранить**.
3. По завершении нажмите кнопку **Сохранить**.

Настройка отслеживания сообщений с помощью командной консоли Exchange

Как указывалось ранее, с помощью командлета **Set-TransportService** можно выполнить любые задачи по настройке отслеживания сообщений на серверах почтовых ящиков и пограничных транспортных серверах. Чтобы настроить отслеживание сообщений в командной консоли Exchange, используйте следующий синтаксис:

PowerShell

```
Set-TransportService [<ServerIdentity>] -MessageTrackingLogEnabled <$true | $false> -MessageTrackingLogMaxAge <dd.hh:mm:ss> -MessageTrackingLogMaxDirectorySize <Size> -MessageTrackingLogMaxFileSize <Size> -MessageTrackingLogPath <LocalFilePath> -MessageTrackingLogSubjectLoggingEnabled <$true | $false>
```

Обратите внимание, что не требуется указывать сервер Exchange при выполнении команды на сервере, который нужно настроить.

В этом примере показано, как настроить следующие параметры журнала на сервере с именем Mailbox01:

- Задает для файлов журнала отслеживания сообщений расположение D:\Message Tracking Log. Обратите внимание, что если папка не существует, она будет создана.
- Задает максимальный размер файла журнала отслеживания сообщений равным 20 МБ.
- Задает максимальный размер каталога журнала отслеживания сообщений равным 1,5 ГБ.
- Задает максимальный срок хранения файла журнала отслеживания сообщений равным 45 дням.

PowerShell

```
Set-TransportService Mailbox01 -MessageTrackingLogPath "D:\Message Tracking Log" -MessageTrackingLogMaxFileSize 20MB -MessageTrackingLogMaxDirectorySize 1.5GB -MessageTrackingLogMaxAge 45.00:00:00
```

ⓘ Примечание

- При установке для параметра *MessageTrackingLogPath* значения `$null` фактически отключается отслеживание сообщений. Однако если

значение параметра *MessageTrackingLogEnabled* равно `$true`, создаются ошибки журнала событий.

- Если *параметру MessageTrackingLogMaxAge* присвоено значение , `00:00:00` это предотвращает автоматическое удаление файлов журнала отслеживания сообщений из-за их возраста.
- Максимальный размер каталога журнала отслеживания сообщений в три раза больше значения параметра *MessageTrackingLogMaxDirectorySize*. Несмотря на то что файлы журнала отслеживания сообщений, создаваемые четырьмя различными службами, имеют четыре различных префикса имен, количество и частота данных, записываемых в журнал управляемого транспорта (**MSGTRKMA**), являются незначительными по сравнению с тремя другими журналами. Дополнительные сведения см. **в разделе Структура файлов журнала отслеживания сообщений**.

В этом примере показано, как отключить ведение журнала темы сообщений в журнале отслеживания сообщений на сервере с именем Mailbox01.

PowerShell

```
Set-TransportService Mailbox01 -MessageTrackingLogSubjectLoggingEnabled $false
```

В этом примере показано, как выключить отслеживание сообщений на сервере почтовых ящиков с именем Mailbox01.

PowerShell

```
Set-TransportService Mailbox01 -MessageTrackingLogEnabled $false
```

Как проверить, что все получилось?

Чтобы убедиться, что отслеживание сообщений настроено успешно, выполните следующую команду в командной консоли Exchange:

PowerShell

```
Get-TransportService [<ServerIdentity>] | Format-List MessageTrackingLog*
```

Кроме того, вы можете открыть расположение журнала отслеживания сообщений в проводнике, чтобы убедиться, что файлы журнала существуют, в них

записываются данные и они удаляются в соответствии с заданными максимальными размерами файлов и папок.

Exchange Server: журналы отслеживания сообщений поиска

Статья • 04.04.2023

В журнал отслеживания сообщений записывается информация о потоке обработки почты на серверах почтовых ящиков и пограничных транспортных серверах. Командлет **Get-MessageTrackingLog** в командной консоли Exchange позволяет искать записи в журнале отслеживания сообщений, используя определенные условия поиска. Например, вы можете:

- узнать, что произошло с сообщением, отправленным пользователем определенному получателю;
- Узнайте, действовало ли на сообщение правило обработки почты (также известное как правило транспорта).
- узнать, поступило ли в вашу организацию Exchange сообщение, отправленное из Интернета;
- найти все сообщения, отправленные пользователем за определенный период.

Что нужно знать перед началом работы

- Предполагаемое время выполнения: 10 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Отслеживание сообщений" в разделе Разрешения потока обработки почты .
- Для поиска в журналах отслеживания сообщений должна быть запущена служба поиска журналов транспорта Microsoft Exchange. Если вы отключите или остановите эту службу, то не сможете выполнять поиск в журналах отслеживания сообщений или создавать отчеты о доставке. Однако остановка этой службы не затрагивает другие функции Exchange.
- Имена полей в результатах командлета **Get-MessageTrackingLog** похожи на имена полей в файлах журнала отслеживания сообщений. Ниже приведены основные различия.
  - Из имен полей удаляются дефисы. Например, **internal-message-id** отображается как `InternalMessageId`.

- Поле **даты и времени** отображается как `Timestamp`.
- Поле **адреса получателя** отображается как `Recipients`.
- Поле **отправителя-адреса** отображается как `Sender`.

- В поле **date-time** журнала отслеживания сообщений информация хранится в формате UTC. Однако необходимо ввести критерии поиска даты и времени для параметров *Start* или *End* в формате регионального времени даты и времени компьютера, который вы используете для поиска.
- Нельзя скопировать файлы журнала отслеживания сообщений с другого сервера Exchange, а затем выполнить в них поиск с помощью командлета **Get-MessageTrackingLog**. Кроме того, если вручную сохранить файл журнала отслеживания сообщений, изменение метки даты и времени в файле нарушит логику запросов, используемую в Exchange для поиска данных в журналах отслеживания сообщений.
- В Exchange 2016 командлет **Get-MessageTrackingLog** позволяет выполнять поиск журналов отслеживания сообщений на серверах почтовых ящиков Exchange 2013 и транспортных серверах-концентраторах Exchange 2010 на том же сайте Active Directory. В Exchange 2019 командлет **Get-MessageTrackingLog** позволяет выполнять поиск журналов отслеживания сообщений на серверах почтовых ящиков Exchange 2016 и Exchange 2013 на одном сайте Active Directory.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Поиск в журналах отслеживания сообщений с помощью командной консоли Exchange

При поиске записей об определенных событиях в журналах отслеживания сообщений введите команду в следующем формате.

```
```

PowerShell

```
Get-MessageTrackingLog [-Server <ServerIdentity>] [-ResultSize <Integer> |
Unlimited] [-Start <DateTime>] [-End <DateTime>] [-EventId <EventId>] [-
InternalMessageId <InternalMessageId>] [-MessageId <MessageId>] [-
MessageSubject <Subject>] [-Recipients
<RecipientAddress1,RecipientAddress2...>] [-Reference <Reference>] [-Sender
<SenderAddress>]
```

Чтобы просмотреть 1000 последних записей в журнале отслеживания сообщений на сервере, выполните следующую команду.

PowerShell

```
Get-MessageTrackingLog
```

В этом примере выполняется поиск всех записей в журналах отслеживания сообщений на локальном сервере с 28.03.2015 с 8:00 по 28.03.2015 17:00 для всех событий **FAIL** , в которых отправитель сообщения был pat@contoso.com.

PowerShell

```
Get-MessageTrackingLog -ResultSize Unlimited -Start "3/28/2015 8:00AM" -End
"3/28/2015 5:00PM" -EventId "Fail" -Sender "pat@contoso.com"
```

Управление форматом вывода результатов поиска в журналах отслеживания сообщений с помощью командной консоли Exchange

Введите команду в следующем формате.

PowerShell

```
Get-MessageTrackingLog <SearchFilters> | <Format-Table | Format-List>
[<FieldNames>] [<OutputFileOptions>]
```

В этом примере в журналах отслеживания сообщений выполняется поиск со следующими условиями.

- Возвращаются результаты для первых 1000 событий с меткой **Send**.

- Результаты отображаются в формате списка.
- Отображение только тех имен полей, которые начинаются с `Send` или `Recipient`.
- Запись выходных данных в новый файл с именем `D:\Send Search.txt`

PowerShell

```
Get-MessageTrackingLog -EventId Send | Format-List Send*,Recipient* | Set-Content -Path "D:\Send Search.txt"
```

Поиск записей сообщений в журналах отслеживания сообщений на нескольких серверах с помощью командной консоли Exchange

Обычно значение в поле заголовка **MessageID:** остается неизменным по мере продвижения сообщения в организации Exchange. В программах просмотра очереди это свойство называется **InternetMessageId**, а в программах просмотра журнала отслеживания сообщений — **MessageId**. Определив значение поля **MessageID:** для конкретного сообщения, вы можете искать информацию о нем в журналах отслеживания сообщений на каждом сервере почтовых ящиков в своей организации Exchange.

Для поиска определенного сообщения во всех записях журнала отслеживания сообщений на всех серверах почтовых ящиков и транспортных серверах-концентраторах Exchange 2010 используйте такой синтаксис:

PowerShell

```
$Servers = Get-ExchangeServer;  $Servers | where {$_.isHubTransportServer -eq $true -or $_.isMailboxServer -eq $true} | Get-MessageTrackingLog -MessageId <MessageID>  | Select-Object <CommaSeparatedFieldNames>  | Sort-Object -Property <FieldName>
```

В этом примере в журналах отслеживания сообщений на всех серверах почтовых ящиков и транспортных серверах-концентраторах Exchange 2010 выполняется поиск с указанными ниже условиями.

- Найдите все записи, связанные с сообщением, которое имеет **MessageID:** значение `<ba18339e-8151-4ff3-aeea-87ccf5fc9796@mailbox01.contoso.com>`. Обратите внимание, что знаки угловой скобки (`< >`) можно опустить. Если не сделать этого, все значение поля **MessageID:** необходимо заключить в кавычки.

- Для каждой записи отображаются поля **date-time**, **server-hostname**, **client-hostname**, **source**, **event-id** и **recipient-address**.

- Результаты сортируются по полю **date-time**.

PowerShell

```
$Servers = Get-ExchangeServer; $Servers | where {$_.isHubTransportServer -eq $true -or $_.isMailboxServer -eq $true} | Get-MessageTrackingLog -MessageId ba18339e-8151-4ff3-aeea-87ccf5fc9796@mailbox01.contoso.com | Select-Object Timestamp,ServerHostname,ClientHostname,Source,EventId,Recipients | Sort-Object -Property Timestamp
```

Использование Центра администрирования Exchange для поиска данных в журналах отслеживания сообщений

Вы можете использовать функцию "Отчеты о доставке для администраторов" в Центре администрирования Exchange (EAC) для поиска в журналах отслеживания сообщений на наличие сведений о сообщениях, отправленных или полученных определенным почтовым ящиком в вашей организации. Дополнительные сведения см. в разделе Отслеживание сообщений с помощью отчетов о доставке.

Отчеты о доставке для администраторов в Exchange Server

Статья • 04.04.2023

С помощью отчетов о доставке для администраторов можно отслеживать сведения о доставке сообщений, отправленных или полученных с определенного почтового ящика в организации. В частности, функция составления отчетов о доставке для администраторов использует Центр администрирования Exchange для выполнения целенаправленного поиска журналов отслеживания сообщений. Область поиска всегда ограничена конкретным почтовым ящиком. Вы можете искать сообщения, отправленные с почтового ящика или на почтовый ящик, а также фильтровать результаты поиска по теме сообщения.

Содержимое тела сообщения не возвращается в отчете о доставке, но в результатах отображается поле темы. Если вы хотите найти в почтовых ящиках организации определенные сообщения электронной почты на основе содержимого сообщений, см. статью Обнаружение электронных данных на месте в Exchange Server.

Отчеты о доставке удобны в следующих ситуациях.

- Руководитель дает плохой отзыв об обучаемом, так как последний не вернул назначение в срок. Обучаемый утверждает, что он отправил письмо с присоединенным назначением. Руководитель просит вас проверить состояние сообщения.
- Пользователям был отправлен бюллетень безопасности с запросом о немедленном ответе, но никто не ответил. Они не стали отвечать на сообщение или не получили его?
- Пользователи утверждают, что они не получали сообщение. Они проверяют состояние почты, но не могут понять, что происходит. Это может произойти из-за правила, применяемого к сообщениям на уровне организации.

После создания отчета о доставке в результате поиска будут отображаться следующие сведения: кому и куда было отправлено сообщение, строка темы и время отправки сообщения. В отчете о доставке также отображается состояние доставки сообщений и причины задержки или сбоя доставки.

Дополнительные сведения об отчетах о доставке

- Вот как администраторы в локальных организациях Exchange создают отчеты о доставке: Отслеживание сообщений с помощью отчетов о доставке.
- Более эффективным вариантом для администраторов в локальных организациях Exchange является использование командной консоли Exchange для непосредственного запроса журналов отслеживания сообщений. Дополнительные сведения см. в разделе Журналы отслеживания сообщений поиска.
- Отчеты о доставке Exchange 2016 или Exchange 2019 могут отслеживать сообщения на серверах Exchange 2019, Exchange 2016 и Exchange 2013 на одном сайте Active Directory.

Exchange Server: отслеживание сообщений с помощью отчетов о доставке

Статья • 04.04.2023

Отчеты о доставке — это средство отслеживания сообщений в Центре администрирования Exchange, которое можно использовать для определения состояния доставки электронных сообщений, отправленных пользователями или адресованных пользователям в адресной книге организации. Вы можете отслеживать сведения о доставке сообщений, отправленных или полученных с определенного почтового ящика в организации. Содержимое сообщения не возвращается в отчете о доставке, но в результатах отображается строка темы. Вы можете отслеживать сообщения до 14 дней после того, как они были отправлены или получены.

> **Примечание**
>
> Отчеты о доставке отслеживают сообщения, отправленные пользователями с помощью Microsoft Outlook или Outlook в Интернете. Они не позволяют отслеживать сообщения, отправленные из почтовых клиентов, использующих протоколы POP3 или IMAP4, таких как "Почта Windows Live" и Mozilla Thunderbird.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: Время выполнения зависит от области поиска.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Отслеживание сообщений" в разделе Разрешения потока обработки почты .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.
- Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server, Exchange Online или Exchange Online Protection.

Использования EAC для отслеживания сообщений

1. В EAC перейдите к разделу**Отчеты о доставке** потока >**почты**.

2. Введите следующие сведения.

    - **Почтовый ящик для поиска**. Нажмите кнопку **Обзор** , чтобы выбрать почтовый ящик из адресной книги, а затем нажмите кнопку **OK**. Выбирать почтовый ящик для поиска обязательно.

    - Выберите один из приведенных ниже параметров:

    - **Поиск сообщений, отправленных** в: используйте этот параметр для поиска сообщений, отправленных определенным пользователям из почтового ящика, выбранного в **поле Почтовый ящик для поиска**. Щелкните **Выбор пользователей**, а затем выберите пользователей в адресной книге — для этого нужно выбрать пользователя в списке и нажать кнопку **Добавить**. Допускается выбор нескольких пользователей. После выбора пользователей нажмите кнопку **OK**, чтобы вернуться на страницу **Отчеты о доставке**. При выборе этого параметра можно оставить поле пустым, чтобы искать сообщения, отправленные всем пользователям.

    - **Поиск сообщений, полученных из**: используйте этот параметр для поиска сообщений, отправленных определенным пользователем в почтовый ящик, выбранный в **поле Почтовый ящик для поиска**. Снова выберите пользователя из адресной книги и нажмите кнопку **OK**, чтобы вернуться на страницу **Отчеты о доставке**. При выборе этого параметра необходимо указать отправителя.

    - **Найдите эти слова в строке темы**. Введите здесь сведения о строке темы или оставьте их пустыми.

3. По завершении нажмите кнопку **Поиск**. Чтобы начать настройку с начала, нажмите кнопку **Очистить**.

Использование EAC для просмотра отчетов о доставке

Чтобы просмотреть сведения о доставке, выберите сообщение в области **Результаты поиска** и щелкните **Значок**✎.

Отчет о доставке содержит состояние доставки, а также подробные сведения о доставке сообщения, выбранного в области **Результаты поиска**. В верхней части отчета расположены следующие поля.

- **Тема**: строка темы сообщения отображается в качестве заголовка отчета.
- **От**: псевдоним, отображаемое имя или адрес электронной почты пользователя, отправившего сообщение.
- **По** адресу: псевдоним, отображаемое имя или адрес электронной почты для каждого получателя сообщения.
- **Отправлено**: дата и время отправки сообщения.

Раздел "Сводка на текущий момент"

Этот раздел отображается в отчете о доставке в том случае, если сообщение было отправлено нескольким получателям. В верхней части этого раздела указано общее количество получателей, которым было отправлено сообщение, а также краткое состояние доставки по каждому получателю.

- **Сводка по дате**: отображает общее число получателей и при наличии сообщений **Pending**, **Delivered** или **Неудачно**. Щелкните гиперссылки, чтобы выполнить сортировку по состоянию доставки.
- **Поле поиска**. Поле поиска полезно, если вы отправили сообщение группе из более чем 30 получателей. В поле поиска введите адрес электронной почты, по которому вы хотите получить сведения о доставке, и щелкните 🔎 лупы.
- **По адресу**: отображает адрес электронной почты получателя.
- **Состояние**. В этом столбце отображается состояние сообщения для каждого получателя.

Удаление сведений отчета

В этом разделе содержатся сведения о доставке сообщения, отправленного получателю, который был выбран в разделе **Общие сведения на текущий момент**.

- **Отчет о доставке для**: адрес электронной почты выбранного получателя показан здесь.
- **Отправлено**: дата и время отправки сообщения для доставки системой.

В зависимости от состояния доставки сообщения вы можете видеть ряд состояний, в том числе:

- **Доставлено**: указывает на успешную доставку.
- **Отложено**: указывает, что сообщение отложено.
- **Ожидание**. Если доставка сообщения ожидается, так как сообщение соответствует критериям правила или политики в масштабах организации или из-за того, что оно подлежит утверждению сообщения, в сообщении о состоянии объясняется, какое действие выполняет правило или что сообщение должно быть утверждено модератором перед доставкой.
- **Moderator**: состояние указывает, было ли сообщение утверждено или отклонено модератором.
- **Развернутые группы**. Если сообщение было отправлено группе, отдельные пользователи отображаются в разделе **Сводка по дате** , чтобы вы могли видеть состояние доставки для каждого получателя. Если необходимо удалить или добавить пользователя или группу при ознакомлении с отчетом о доставке, можно изменить группу, нажав кнопку **Изменить группы**.
- **Сбой**: показывает дату, время и причину сбоя доставки сообщения. For example, an organization-wide rule may be blocking message delivery or the message couldn't be delivered.

По завершении просмотра отчета нажмите кнопку **Закрыть**. Отчеты о доставке не сохраняются, однако их можно снова создать в любое время. Помните, что поиск возможен в пределах двухнедельного окна.

Как проверить, что все получилось?

Если поиск выполнен успешно, то сообщения, соответствующие условиям поиска, отображаются в области **Результаты поиска**. Чтобы просмотреть сведения о доставке для определенного сообщения, выберите его и щелкните **значок Изменения**. Если сообщения не отображаются в области **Результаты поиска**, измените условия поиска, а затем повторите поиск.

Ведение журнала подключений в Exchange Server

Статья • 04.04.2023

В журнале подключения записываются действия подключения для передачи исходящих сообщений на серверы Exchange. В Exchange Server следующие службы передают сообщения, поэтому у них есть журналы подключения:

- Служба транспорта на серверах почтовых ящиков и пограничных транспортных серверах.
- Внешняя служба транспорта на серверах почтовых ящиков.
- Служба отправки транспорта почтовых ящиков на серверах почтовых ящиков.
- Служба доставки транспорта почтовых ящиков на серверах почтовых ящиков.

Дополнительные сведения об этих службах транспорта, а также о том, куда они могут передавать сообщения, см. в разделе Mail flow and the transport pipeline.

Журнал подключения не отслеживает передачу отдельных сообщений. Вместо этого он отслеживает число и размер сообщений, переданных через подключение, сведения о разрешении DNS для назначения, а также информационные сообщения, имеющие отношение к подключению.

Функция ведения журнала подключения включена по умолчанию, а для облегчения контроля за расходованием места на жестком диске, где хранятся файлы журналов подключений, Exchange использует циклическое ведение журнала, чтобы ограничивать количество файлов журнала, исходя из их размера и срока хранения. Сведения о настройке ведения журнала подключений см. в статье Настройка ведения журнала подключений в Exchange Server.

Примечание. Если вам необходимо подробно записать всю беседу по протоколу SMTP от начала до конца, см. раздел Ведение журнала протокола.

Структура файлов журнала подключения

По умолчанию файлы журнала подключения размещаются в следующих папках:

- **Серверы почтовых ящиков**:

    - **Транспортная служба**: `%ExchangeInstallPath%TransportRoles\Logs\Hub\Connectivity`
    - **Транспортная служба переднего плана**: `%ExchangeInstallPath%TransportRoles\Logs\FrontEnd\Connectivity`
    - **Служба доставки транспорта почтовых ящиков**: `%ExchangeInstallPath%TransportRoles\Logs\Mailbox\Connectivity\Delivery`
    - **Служба отправки транспорта почтовых ящиков**: `%ExchangeInstallPath%TransportRoles\Logs\Mailbox\Connectivity\Submission`
- **Пограничные транспортные серверы**

Соглашение об именовании для файлов журнала подключения — `CONNECTLOGyyymmdd-nnnn.log`. Заполнители обозначают следующее:

- *yyyymmdd* — это дата создания файла журнала (в формате UTC). *гггг* = год, *мм* = месяц, и *дд* = день.
- *nnnn* представляет собой номер экземпляра, который каждый день начинается со значения 1.

Данные записываются в файл журнала, пока не будет достигнут его максимальный размер. Затем открывается новый файл журнала с увеличенным номером экземпляра (1 для первого файла, 2 для второго и т. д.) При циклическом ведении журнала самые старые файлы журнала удаляются при соблюдении любого из следующих условий:

- достигнут максимальный срок хранения файла журнала;
- достигнут максимальный размер папки журнала подключений.

Файлы журнала подключения представляют собой текстовые файлы с разделителями-запятыми в формате CSV. Каждый файл журнала подключения снабжен заголовком, содержащим следующие сведения:

- **#Software**: значение равно `Microsoft Exchange Server`.
- **#Version**: значение равно `15.0.0.0`.
- **#Log-Type**: значение равно `Transport Connectivity Log`.
- **#Date**: дата и время создания файла журнала в формате UTC. Дата-время в формате UTC представлено в формате даты и времени ISO 8601: *гггг-мм-*

*дд*T*чч:мм:ss.fffZ*, где *гггг* = год, *мм* = месяц, *дд* = день, T указывает начало компонента времени, *чч* = час, *мм* = минута, *ss* = секунда, *fff* = доли секунды, а Z обозначает Zulu, что является еще одним способом обозначения UTC.

- **#Fields**: имена полей с разделителями-запятыми, которые используются в файлах журнала подключения. Эти значения описаны в следующем разделе.

Поля в файлах журнала подключения

В журнале подключения каждое событие исходящего подключения хранится отдельной строкой. Сведения по каждой строке сгруппированы по полям, разделенным запятыми. В приведенной ниже таблице описаны поля, используемые для классификации каждого события исходящего подключения.

Имя поля	Описание
date-time	Дата и время события подключения в формате UTC. Дата-время в формате UTC представлено в формате даты и времени ISO 8601: *гггг-мм-дд*T*чч:мм:ss.fffZ*, где *гггг* = год, *мм* = месяц, *дд* = день, T указывает начало компонента времени, *чч* = час, *мм* = минута, *ss* = секунда, *fff* = доли секунды, а Z обозначает Zulu, что является еще одним способом обозначения UTC.
session	Значение GUID. Значение GUID одинаковое для каждого события, связанного с одним и тем же сеансом, но уникальное для каждого сеанса.
source	Одно из этих значений: • **SMTP** для SMTP-подключений. • **MapiDelivery** для подключений от локальной базы данных почтовых ящиков с помощью службы доставки транспорта почтовых ящиков. • **MapiSubmission** для подключений от локальной базы данных почтовых ящиков с помощью службы отправки транспорта почтовых ящиков.

Имя поля	Описание

destination	Вот некоторые примеры значений, которые вы увидите здесь:
	• **В транспортной службе**:
	  ○ FQDN для целевого сервера обмена сообщениями
	  ○ `shadowredundancy` (только на серверах почтовых ящиков)
	• **В службе внешнего транспорта**:
	  ○ `internalproxy`
	  ○ `client proxy`
	• **В службе доставки транспорта почтовых ящиков** выполните следующие действия.
	  ○ Значение GUID для целевой базы данных почтовых ящиков.
	• **В службе отправки транспорта почтовых ящиков выполните следующие действия**.
	  ○ Значение GUID для целевой базы данных почтовых ящиков.
	  ○ `mailboxtransportsubmissioninternalproxy`

direction	Одиночный символ, указывающий начало, середину или завершение подключения. Здесь вы можете увидеть следующие значения: • `+`:Подключения • `-`:Отключите • `>`:Отправить
description	Текстовая информация, относящаяся к событию подключения. Например: • количество и размер отправленных сообщений; • информация о разрешении DNS почтового обменника для целевых доменов; • информация о разрешении DNS для целевых серверов почтовых ящиков; • сообщения об установлении подключения; • сообщения об ошибке подключения.

Транспортные службы подключаются и отправляют сообщения к нескольким назначениям одновременно. Записи различных событий подключения в файле журнала чередуются (обычно они не группируются вместе как непрерывный ряд событий подключения). Однако, чтобы упорядочивать и сортировать записи журнала для каждого отдельного подключения от начала до конца, можно использовать поля (в частности, уникальное значение поля **session** для подключения).

Настройка ведения журнала подключений в Exchange Server

Статья • 04.04.2023

Журнал подключений записывает действия исходящего подключения (источник, назначение, количество и размер сообщений, а также сведения о подключении) для транспортных служб на серверах Exchange. Дополнительные сведения о ведении журнала подключений см. в разделе Ведение журнала подключений в Exchange Server.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 15 минут.
- Вы можете использовать Центр администрирования Exchange (EAC), чтобы включить или отключить ведение журнала подключений и задать путь к журналу для транспортной службы только на серверах почтовых ящиков. Для всех остальных параметров ведения журнала подключений в других транспортных службах необходимо использовать командную консоль Exchange. Дополнительные сведения о EAC см. в разделе Центр администрирования Exchange в Exchange Server. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Папке для ведения журнала подключений нужны такие разрешения:
  - Сетевая служба: полный доступ
  - Система: полный доступ
  - Администраторы: полный доступ

  Если такой папки нет, но эти разрешения есть у родительской папки, новая папка создается автоматически.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записях "Транспортная служба", "Транспортная служба переднего плана" и "Транспортная служба почтовых ящиков" в разделе Разрешения потока обработки почты .

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Настройка ведения журнала подключений в транспортной службе на серверах почтовых ящиков в Центре администрирования Exchange

1. В EAC перейдите в раздел **Серверы**>.
2. Выберите сервер почтовых ящиков, который требуется настроить, и нажмите кнопку **Изменить**.
3. На открывшейся странице свойств сервера нажмите **Журналы транспорта**.
4. В разделе **Журнал подключений** измените один из указанных ниже параметров.

    - **Включить журнал подключений**. Чтобы отключить ведение журнала подключений для транспортной службы на сервере, снимите флажок. Чтобы включить ведение журнала подключений для транспортной службы на сервере, установите его.
    - **Путь к журналу подключения**. Указанное значение должно находиться на локальном сервере Exchange Server. Если папка не существует, она будет создана автоматически, если у родительской папки есть необходимые разрешения.

    По завершении нажмите кнопку **Сохранить**.

Настройка ведения журнала подключений с помощью командной консоли Exchange

На серверах почтовых ящиков ведение журнала подключений доступно для таких транспортных служб:

- транспортная служба (используйте командлет **Set-TransportService**);
- внешняя служба транспорта (используйте командлет **Set-FrontEndTransportService**);
- транспортные службы доставки и отправки почтовых ящиков (используйте командлет **Set-MailboxTransportService** для настройки обеих служб).

На пограничных транспортных серверах ведение журнала подключений доступно для транспортной службы (используйте командлет **Set-TransportService**).

Чтобы настроить ведение журнала подключений, используйте такой синтаксис:

PowerShell

```
<Set-TransportService | Set-MailboxTransportService | Set-
FrontEndTransportService> -Identity <ServerIdentity> -ConnectivityLogEnabled
<$true | $false> -ConnectivityLogMaxAge <dd.hh:mm:ss> -
ConnectivityLogMaxDirectorySize <Size> -ConnectivityLogMaxFileSize <Size> -
ConnectivityLogPath <LocalFilePath>
```

В этом примере показана установка следующих параметров журнала подключения в службе транспорта на сервере почтовых ящиков с именем Mailbox01.

- **Расположение журнала подключения**: D:\Connectivity Log\Hub. Обратите внимание: если папка не существует, она будет создана, если у родительской папки есть необходимые разрешения.
- **Максимальный размер файла журнала подключения**. Задает максимальный размер файла журнала подключения в 20 МБ.
- **Максимальный размер папки журнала подключения**. Задает максимальный размер каталога журнала подключения в 1,5 ГБ.
- **Максимальный возраст файла журнала подключения**. Задает максимальный возраст файла журнала подключений в 45 дней.

PowerShell

```
Set-TransportService -Identity Mailbox01 -ConnectivityLogPath
"D:\Connectivity Log\Hub" -ConnectivityLogMaxFileSize 20MB -
ConnectivityLogMaxDirectorySize 1.5GB -ConnectivityLogMaxAge 45.00:00:00
```

Дополнительные сведения о синтаксисе и параметрах см. в статьях Set-TransportService, Set-FrontendTransportService и Set-MailboxTransportService.

Примечания.

- Установка параметра *ConnectivityLogPath* значения `$null` фактически отключает ведение журнала подключений. Однако это значение создает ошибки журнала событий, если значение параметра *ConnectivityLogEnabled* также `$true` имеет значение .
- При использовании параметра *ConnectivityLogPath* в командлете **Set-MailboxTransportService** в указанной папке автоматически создаются две вложенные папки:
  - `Delivery` для транспортной службы доставки почтового ящика;
  - `Submission` для транспортной службы отправки почтового ящика.
- Установка значения параметра `00:00:00` *ConnectivityLogMaxAge* предотвращает автоматическое удаление файлов журнала подключения из-за их возраста.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно настроили ведение журнала подключений, сделайте следующее:

1. Выполните следующую команду в командной консоли Exchange, чтобы проверить параметры журнала подключений на серверах Exchange Server:

```
PowerShell
```

```
Write-Host "Front End Transport service:" -ForegroundColor yellow; Get-FrontEndTransportService | Format-List Name,ConnectivityLog*; Write-Host "Mailbox Transport Submission and Mailbox Transport Delivery services:" -ForegroundColor yellow; Get-MailboxTransportService | Format-List Name,ConnectivityLog*; Write-Host "Transport service:" -ForegroundColor yellow; Get-TransportService | Format-List Name,ConnectivityLog*
```

2. Откройте расположение журнала подключений в проводнике, чтобы убедиться, что файлы журнала существуют, в них записываются данные и они удаляются в соответствии с заданными максимальными размерами файлов и папок. Если вы отключили ведение журнала подключений, убедитесь, что файлы журнала не обновляются.

Трассировка конвейера

Статья • 04.04.2023

Трассировка конвейера захватывает копии сообщений электронной почты от определенного отправителя при их перемещении через транспортную службу на серверах почтовых ящиков, службу доставки транспорта почтовых ящиков на серверах почтовых ящиков и через пограничные транспортные серверы. Функция конвейерной трассировки также отвечает за захват подробных сведений об изменениях, которые применяет каждый агент транспорта к сообщениям в транспортном конвейере, с помощью файлов моментальных снимков сообщений. Путем проверки содержимого файлов снимков сообщений можно определить, внесли ли агенты транспорта изменения в сообщения конвейерной трассировки передачи должным образом. При обнаружении неисправности необходимо определить, в каком агенте транспорта произошла ошибка. После этого, чтобы устранить неисправность, можно сосредоточиться на поиске ошибок этого агента. Затем можно просмотреть файлы снимков сообщений снова, чтобы убедиться, что устранение неисправности прошло успешно.

⚠ Предупреждение

- Функция конвейерной трассировки копирует все содержимое сообщений электронной почты, которые отправляются с адреса электронной почты отправителя. Чтобы избежать нежелательного раскрытия конфиденциальной информации, необходимо настроить соответствующие разрешения системы безопасности в папке конвейерной трассировки.
- Не следует включать конвейерную трассировку на длительный период времени. Конвейерная трассировка создает файлы, которые могут быстро накапливаться. Если включена конвейерная трассировка, всегда следите за объемом свободного дискового пространства.

Настройка конвейерной трассировки

Перед включением трассировки конвейера необходимо указать адрес электронной почты отправителя, который вы хотите отслеживать. Трассировка конвейера предназначена для регистрации сообщений, отправленных с определенного адреса электронной почты. Адрес электронной почты отправителя может быть внутренним или внешним для вашей организации Exchange. Кроме того, можно включить трассировку конвейера для системных сообщений, созданных транспортной службой на указанном почтовом ящике или пограничном транспортном сервере, таких как автоматические ответы, уведомления о состоянии доставки (DSN), отчеты журнала и другие системные сообщения. Вы также можете изменить расположение папки трассировки конвейера.

Параметры, используемые для настройки трассировки конвейера, приведены в следующей таблице:

Командлет	Параметр	Значение по умолчанию	Описание
Set-TransportService **Set-MailboxTransportService**	*PipelineTracingSenderAddress*	Пустой (`$null`)	Указывает адрес электронной почты отправителя, за которым необходимо вести наблюдение. Укажите значение "`<>`" для мониторинга системных сообщений, отправляемых указанной транспортной службой на сервере.

Командлет	Параметр	Значение по умолчанию	Описание

Set-TransportService
 	
Set-MailboxTransportService
	PipelineTracingPath	**Транспортная служба**:
		`%ExchangeInstallPath%TransportRoles\Logs\Hub\PipelineTracing`
		
		Транспортная служба почтовых ящиков:
		`%ExchangeInstallPath%TransportRoles\Logs\Mailbox\PipelineTracing`
			Путь должен находиться на локальном сервере. UNC-пути не поддерживаются. Указанный путь содержит папку, в которой `MessageSnapshots` хранятся файлы трассировки конвейера.

Set-TransportService **Set-MailboxTransportService**	*PipelineTracingEnabled*	`$false`	Конвейерную трассировку можно включить только для указанной транспортной службы на сервере после настройки адреса отправителя, за которым необходимо вести наблюдение.

Дополнительные сведения о том, как разрешить конвейерную трассировку и настроить для нее адрес отправителя, см. в статье Настройка конвейерной трассировки.

Файлы моментальных снимков сообщений

Моментальные снимки сообщений — это файлы, в которые записываются все изменения, внесенные в сообщение агентами транспорта в транспортной службе или службе доставки с помощью транспорта почтовых ящиков. Эти файлы хранятся в папке `MessageSnapshots` в соответствующем пути трассировки конвейера для транспортной службы.

В папке `MessageSnapshots` Exchange создает по одной папке для каждого сообщения, отправленного отслеживаемым отправителем, которое проходит через указанную службу транспорта. Каждой папке присваивается имя в соответствии с GUID, назначенным сообщению. Если включить трассировку конвейера для транспортной службы и транспортной службы почтовых ящиков на одном сервере почтовых ящиков, каждой транспортной службой одному и тому же сообщению присваивается другой GUID, поэтому имя папки для сообщения в `MessageSnapshots` папке для транспортной службы отличается от имени папки для того же сообщения в `MessageSnapshots` папке для транспортной службы почтовых ящиков. Если включить конвейерную трассировку на нескольких серверах Exchange, по мере продвижения сообщения по указанной транспортной службе на каждом из серверов Exchange этому сообщению назначаются различные GUID.

В каждой папке сообщений служба Exchange создает несколько файлов моментальных снимков сообщений с расширением EML. Эти файлы моментальных снимков сообщений включают в себя содержимое сообщения, которое записывается по мере обнаружения каждого события SMTP и агента транспорта.

Если агент транспорта зарегистрирован в событии SMTP, служба Exchange создает моментальный снимок сообщения еще до того, как сообщение столкнется с агентами транспорта. В результате копия сообщения создается перед тем, как это сообщение обнаружит агентов транспорта, зарегистрированных в этом событии. Затем создается новый снимок сообщения для каждого агента транспорта, которого обнаруживает сообщение независимо от того, изменил ли агент транспорта содержимое сообщения. Однако если для события не зарегистрированы агенты, Exchange не создает моментальные снимки сообщений для этого события.

Например, если в событии **OnEndofData** зарегистрировано три агента транспорта, однако, только два из них изменяют сообщение, создается четвертый снимок сообщения. Первый снимок сообщения делается тогда, когда оно обнаруживает событие **OnEndofData** до внесения в сообщение изменений агентом транспорта, зарегистрированным в этом событии. Затем для каждого агента транспорта создается один снимок сообщения независимо от того, изменил ли его агент транспорта.

Создаваемые файлы моментальных снимков сообщений описаны в следующем списке.

- **Original.eml**: этот файл содержит исходное неизмененном содержимое сообщения электронной почты, прежде чем оно столкнется с событиями SMTP или агентами транспорта.
- **Routingnnnn.eml**: эти файлы содержат содержимое сообщения электронной почты, так как оно обнаруживает события SMTP транспорта и агенты транспорта, зарегистрированные в этих событиях в части классификации службы транспорта. Заполнитель *nnnn* представляет целочисленное значение, начинающееся с `0001`. Это значение увеличивается на единицу для каждого события SMTP и агента транспорта, зарегистрированного в этом событии, в порядке, в котором они выполняют действия в отношении сообщения. Эти файлы моментальных снимков **Routing** не создаются в службе доставки с помощью транспорта почтовых ящиков.
- **SmtpReceivennnn.eml**. Эти файлы содержат содержимое сообщения электронной почты, так как оно обнаруживает события SMTP **OnEndofData** и **OnEndOfHeaders** , зарегистрированные в этих событиях во время получения SMTP-части службы транспорта или службы доставки транспорта почтовых ящиков. Заполнитель *nnnn* представляет целочисленное значение, начинающееся с `0001`. Это значение увеличивается на единицу для каждого события SMTP и агента транспорта, зарегистрированного в этом событии, в порядке, в котором они выполняют действия в отношении сообщения.

Файлы моментальных снимков сообщений можно открыть с помощью Блокнота или любого текстового редактора.

Каждый файл снимка сообщения начинается с заголовков, которые добавляются к содержимому сообщения и перечисляют SMTP-события и агентов транспорта, к которым относится файл снимка сообщений. Эти заголовки начинаются с `X-CreatedBy: MessageSnapshot-Begin injected headers` и заканчиваются на `X-EndOfInjectedXHeaders: MessageSnapshot-End injected headers`. В каждом файле моментального снимка сообщения эти заголовки заменяются каждым последующим агентом транспорта и событием SMTP. Ниже приведен пример заголовков, добавляемых в файл сообщения электронной почты.

Консоль

```
X-CreatedBy: MessageSnapshot-Begin injected headers
X-MessageSnapshot-UTC-Time: 2013-01-23T23:20:18.138Z
X-MessageSnapshot-Record-Id: 21474836486
X-MessageSnapshot-Source: OnSubmittedMessageX-Sender: michelle@nwtraders.com
X-Receiver: chris@contoso.com
X-EndOfInjectedXHeaders: MessageSnapshot-End injected headers
```

После заголовков моментальных снимков сообщений файлы включают содержимое сообщений, в том числе все заголовки исходных сообщений. Если агент транспорта изменяет содержимое сообщения, то изменения отображаются вместе с сообщением. Поскольку сообщение обрабатывается всеми агентами транспорта, вносимые каждым агентом изменения применяются к содержимому сообщения. Если агент транспорта не внес никаких изменений в содержимое сообщения, снимок сообщения, созданного этим агентом, совпадает со снимком сообщения, созданным предыдущим агентом транспорта.

Exchange Server. Настройка трассировки конвейера

Статья • 04.04.2023

Конвейерная трассировка записывает копии почтовых сообщений при их перемещении по транспортному конвейеру в транспортной службе или транспортной службе почтовых ящиков на сервере почтовых ящиков и на пограничных транспортных серверах.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 15 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записях "Транспортная служба" и "Транспортная служба почтовых ящиков" в разделе Разрешения потока обработки почты .
- Для выполнения этой процедуры можно использовать только командную консоль Exchange.
- Функция конвейерной трассировки копирует все содержимое сообщений электронной почты, которые отправляются с адреса электронной почты отправителя. Чтобы избежать раскрытия конфиденциальной информации, необходимо установить для папки конвейерной трассировки соответствующие разрешения системы безопасности.
- Не следует включать конвейерную трассировку на длительный период времени. Во время конвейерной трассировки создается несколько файлов мгновенных снимков, которые быстро накапливаются. Если включена конвейерная трассировка, всегда следите за объемом свободного дискового пространства.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**.

Включение и настройка конвейерной трассировки

Шаг 1. Настройка адреса отправителя трассировки конвейера с помощью командной консоли Exchange

Чтобы настроить адрес отправителя конвейерной трассировки, введите команду в следующем формате.

PowerShell

```
<Set-TransportService | Set-MailboxTransportService> <ServerIdentity> -
PipelineTracingSenderAddress <SMTPAddress | "<>">
```

В этом примере трассировка конвейера настраивается для записи моментальных снимков всех сообщений, отправленных отправителем chris@contoso.com в транспортной службе на сервере почтовых ящиков с именем Mailbox01.

PowerShell

```
Set-TransportService Mailbox01 -PipelineTracingSenderAddress
chris@contoso.com
```

В этом примере конвейерная трассировка настраивается для получения мгновенных снимков всех созданных системой сообщений, полученных службой транспорта на сервере почтовых ящиков Mailbox02.

PowerShell

```
Set-TransportService Mailbox02 -PipelineTracingSenderAddress "<>"
```

> ⚠ **Предупреждение**
>
> Если настроить конвейерную трассировку для записи всех созданных серверами сообщений в службе транспорта, нагрузка на сервер может сильно возрасти, а свободное место на диске может быстро закончиться. Если включена конвейерная трассировка, всегда следите за объемом свободного дискового пространства.

Шаг 2. (Необязательно) Использование командной консоли Exchange для указания настраиваемой папки трассировки конвейера

Папка трассировки конвейера по умолчанию не существует до тех пор, пока не будет включена трассировка конвейера, а сообщения, соответствующие условиям, заданным с помощью параметра *PipelineTracingSenderAddress* , будут проходить через транспортную службу на сервере. Для транспортной службы на сервере почтовых ящиков расположение по умолчанию — `%ExchangeInstallPath%TransportRoles\Logs\Hub\PipelineTracing`. Для службы транспорта почтовых ящиков на сервере почтовых ящиков расположение по умолчанию — `%ExchangeInstallPath%TransportRoles\Logs\Mailbox\PipelineTracing`. Если вы задаете другой путь, он должен указывать на каталог на локальном сервере Exchange.

Чтобы настроить папку конвейерной трассировки, введите команду в следующем формате.

PowerShell

```
<Set-TransportService | Set-MailboxTransportService> <ServerIdentity> -
PipelineTracingPath <LocalFilePath>
```

В этом примере для папки трассировки конвейера для транспортной службы на сервере с именем Mailbox01 `D:\\Hub\\Pipeline Tracing`задается значение .

PowerShell

```
Set-TransportService Mailbox01 -PipelineTracingPath "D:\Hub\Pipeline
Tracing"
```

Шаг 3. Включение трассировки конвейера с помощью командной консоли Exchange

По умолчанию конвейерная трассировка отключена на всех серверах Exchange. Включая конвейерную трассировку, вы активируете ее в указанной транспортной службе только на заданном сервере Exchange. Перед включением конвейерной трассировки укажите адрес отправителя, как описано в шаге 1.

Для включения конвейерной трассировки введите команду в следующем формате.

```
PowerShell

<Set-TransportService | Set-MailboxTransportService> <ServerIdentity> -
PipelineTracingEnabled $true
```

В этом примере активируется конвейерная трассировка в службе транспорта на сервере почтовых ящиков с именем Mailbox01.

```
PowerShell

Set-TransportService Mailbox01 -PipelineTracingEnabled $true
```

Как проверить, что все получилось?

Чтобы убедиться, что вы успешно настроили конвейерную трассировку, выполните следующие действия:

1. Выполните следующую команду:

   ```
   PowerShell

   <Get-TransportService | Get-MailboxTransportService> <ServerIdentity> |
   Format-List PipelineTracing*
   ```

2. Убедитесь, что отображаются значения, которые вы настроили.

3. Проверьте папку конвейерной трассировки для службы транспорта или транспортной службы почтовых ящиков и убедитесь, что файлы снимков сообщений создаются в папке.

Отключение конвейерной трассировки

Из-за вопросов о месте на диске и безопасности, связанных с конвейерной трассировкой, подобная операция — это временное действие для диагностики или устранения неполадок. Включая конвейерную трассировку, не забывайте отключить ее, завершив ее применение.

Для отключения конвейерной трассировки введите команду в следующем формате.

```
PowerShell
```

```
<Set-TransportService | Set-MailboxTransportService> <ServerIdentity> -
PipelineTracingEnabled $false
```

В этом примере отключается конвейерная трассировка в службе транспорта на сервере почтовых ящиков с именем Mailbox01.

PowerShell

```
Set-TransportService Mailbox01 -PipelineTracingEnabled $false
```

Как проверить, что все получилось?

Чтобы убедиться, что вы успешно отключили конвейерную трассировку, выполните следующие действия:

1. Выполните следующую команду:

   PowerShell

   ```
   <Get-TransportService | Get-MailboxTransportService> <ServerIdentity> |
   Format-List PipelineTracingEnabled
   ```

2. Убедитесь, что значение параметра *PipelineTracingEnabled* $false.

3. Проверьте папку конвейерной трассировки и убедитесь, что файлы снимков сообщений больше не создаются в папке.

Очереди и сообщения в очередях в Exchange Server

Статья • 04.04.2023

Очередь — это временное хранилище сообщений, ожидающих дальнейшей обработки или доставки в пункт назначения. Каждая очередь представляет собой логический набор сообщений, которые сервер Exchange Server обрабатывает в определенном порядке. В Exchange 2016 и Exchange 2019 очереди содержат сообщения до, во время и после доставки. Очереди существуют в службе транспорта на серверах почтовых ящиков и на пограничных транспортных серверах. В этой статье эти серверы называются *транспортными серверами*.

Как и во всех предыдущих версиях Exchange, для хранения очередей используется одна база данных расширяемого ядра хранилища (ESE).

Вы можете управлять очередями и сообщениями в очередях с помощью командной консоли Exchange и средства просмотра очередей на панели элементов Exchange. Эти интерфейсы можно использовать для просмотра состояния и содержимого очередей и подробных свойств сообщений. Вы также можете выполнять действия, изменяющие очереди или сообщения в очередях. Дополнительные сведения см. в разделах Процедуры для очередей и Процедуры для сообщений в очередях.

Типы очередей

В Exchange 2016 и Exchange 2019 используются следующие типы очередей, которые совпадают с Exchange 2013:

Очередь	Роль сервера	Описание
Очереди доставки	Серверы почтовых ящиков и пограничные транспортные серверы	Содержит сообщения, доставляемые всем внутренним и внешним адресатам. Очереди доставки создаются динамически, когда они необходимы, и автоматически удаляются, когда очередь пуста и истек срок действия. Время окончания срока действия очереди определяется параметром *QueueMaxIdleTime* командлета **Set-TransportService** . Значение по умолчанию — три минуты. На пограничных транспортных серверах имеется очередь для каждого уникального конечного домена SMTP или промежуточного узла. На серверах почтовых ящиков имеется очередь для каждого уникального пункта назначения, указанного в свойстве **NextHopSolutionKey**. Дополнительные сведения см. в разделе NextHopSolutionKey далее в этой статье. Все сообщения передаются между серверами Exchange 2016 и Exchange 2013 по протоколу SMTP. Если пункт назначения обслуживается соединителем агента доставки, для него также используется очередь доставки. Дополнительные сведения см. в статье Delivery Agents and Delivery Agent Connectors.
Очередь подозрительных сообщений	Серверы почтовых ящиков и пограничные транспортные серверы	Изолирует сообщения, которые содержат ошибки и обозначены как опасные для Exchange после сбоя сервера или службы. Содержимое и формат сообщений могут быть действительно опасными, но иногда сообщения обозначаются так из-за неправильно написанного агента транспорта или ошибки в программном обеспечении, которая привела к сбою на сервере Exchange Server. Как правило, очередь подозрительных сообщений пуста. Если эта очередь не содержит сообщений, она не отображается в средствах управления очередями. Возобновление отправки сообщений в этой очереди и их удаление никогда не происходят автоматически. Сообщения остаются в очереди подозрительных сообщений, пока администратор не возобновит их отправку или не удалит их вручную. На каждом сервере почтовых ящиков или пограничном транспортном сервере есть только одна очередь подозрительных сообщений.
Теневые очереди	Серверы почтовых ящиков	Теневые очереди содержат избыточные копии сообщений во время их передачи. Дополнительные сведения см. в разделе Теневая избыточность в Exchange Server.
Очередь передачи	Серверы почтовых ящиков и пограничные транспортные серверы	Содержит сообщения, принятые службой транспорта, но еще не обработанные. Сообщения в очереди передачи либо находятся в обработке, либо ожидают ее. На серверах почтовых ящиков сообщения принимает соединитель получения, каталог раскладки или преобразования либо служба отправки транспорта почтовых ящиков. На пограничных транспортных серверах сообщения обычно принимает соединитель получения, но также доступны каталоги раскладки и преобразования. Классификатор извлекает сообщения из этой очереди и, помимо всего прочего, определяет расположение получателя и маршрут до него. После классификации сообщение перемещается в очередь доставки или в очередь "Сообщения с недостижимым местом назначения". Дополнительные сведения о классификаторе и транспортном конвейере см. в разделе Поток обработки почты и конвейер транспорта. На каждом сервере почтовых ящиков или пограничном транспортном сервере есть только одна очередь передачи.

Очередь	Роль сервера	Описание
Очередь "Сообщения с недостижимым местом назначения"	Серверы почтовых ящиков и пограничные транспортные серверы	Содержит сообщения, которые не удается доставить в пункт назначения. Обычно это происходит из-за изменений в конфигурации, которые привели к изменению пути маршрутизации для доставки. В этой очереди находятся все сообщения с недоступными адресатами, независимо от пункта назначения. На каждом сервере почтовых ящиков или пограничном транспортном сервере есть только одна очередь "Сообщения с недостижимым местом назначения".

Файлы базы данных очередей

Все очереди хранятся в одной базе данных ESE. По умолчанию эта база данных очереди находится на транспортном сервере по адресу `%ExchangeInstallPath%TransportRoles\data\Queue`.

Как и любая другая база данных ESE, база данных очередей использует файлы журнала для принятия, отслеживания и хранения данных. Для повышения производительности все транзакции с сообщениями записываются сначала в файлы журнала и в память, и только потом — в базу данных. С помощью файла контрольных точек можно отслеживать записи журнала транзакций, зафиксированные в базе данных. В процессе обычного завершения работы службы транспорта Microsoft Exchange несохраненные изменения базы данных, обнаруженные в журналах транзакций, сохраняются в базе данных.

Для базы данных очередей используется циклическое ведение журнала. Это означает, что журналы транзакций старше текущей контрольной точки немедленно удаляются автоматически. Таким образом, журналы транзакций нельзя воспроизвести для восстановления базы данных очередей из резервной копии.

В следующей таблице приведен список файлов, входящих в базу данных очередей.

Файл	Описание
Mail.que	Файл базы данных очередей, в котором хранятся все сообщения, помещенные в очередь.
Tmp.edb	Временный файл базы данных очередей, который используется для проверки схемы базы данных очередей при запуске.
Trn*.log	В журнале транзакций записываются все изменения базы данных очередей. Изменения базы данных сначала записываются в журнал транзакций, и только после этого сохраняются в базе данных. Trn.log — это текущий активный файл журнала транзакций. Trntmp.log — следующий подготовленный к работе файл журнала транзакций, который создается заблаговременно. Если существующий файл журнала транзакций Trn.log достигает максимального размера, Trn.log переименовываются в Trn *nnnn.log*, где *nnnn* — порядковый номер. Затем файл Trntmp.log переименовывается в Trn.log и становится текущим активным файлом журнала транзакций.
Trn.chk	Файл контрольных точек, позволяющий отслеживать записи в журнале транзакций, добавленные в базу данных. Этот файл всегда находится в том же каталоге, что и файл mail.que.
Trnres00001.jrs Trnres00002.jrs	Резервные файлы журналов транзакций, выполняющие роль заполнителей. Они используются лишь для обеспечения правильной остановки работы базы данных очередей в ситуации, когда заканчивается место на жестком диске, на котором хранится журнал транзакций.

Exchange использует *таблицы создания* для хранения и очистки сообщений в базе данных очередей. Вместо обработки и удаления отдельных записей сообщений из одной большой таблицы база данных очередей хранит сообщения в таблицах на основе времени и удаляет всю таблицу только после успешной обработки всех сообщений в таблице. Например, рассмотрим следующий пример:

- Все сообщения, помещенные в очередь с 13:00 до 14:00, независимо от очереди или назначения, хранятся в `1p-2p_msgs` таблице.
- В 14:00 новые сообщения сохраняются в `2p-3p_msgs` таблице.
- В 16:00 создается новая таблица с именем `4p-5p_msgs` . Вся `1p-2p_msgs` таблица удаляется, но только в том случае, если все сообщения в ней успешно обработаны.

Полное удаление таблиц, а не отдельных сообщений позволяет повысить производительность операций ввода-вывода для диска, на котором хранится база данных очередей.

Параметры настройки базы данных очередей

База данных очередей настраивается путем добавления или изменения ключей `%ExchangeInstallPath%Bin\EdgeTransport.exe.config` в XML-файле конфигурации приложения. Этот файл связан с транспортной службой Microsoft Exchange. Изменения, внесенные в файл EdgeTransport.exe.config, вступают в силу после перезапуска службы транспорта Microsoft Exchange.

> ⓘ **Примечание**

При установке накопительного обновления exExchangeNoVersion при установке накопительного обновления exExchangeNoVersion будут перезаписаны все настраиваемые параметры сервера Exchange или Internet Information Server для отдельных серверов (например, файлы web.config или файл EdgeTransport.exe.config). Убедитесь, что вы сохранили эти сведения, чтобы можно было легко повторно настроить сервер после установки. Эти параметры необходимо повторно настроить после установки exExchangeNoVersion CU.

В `<appSettings>` разделе файла EdgeTransport.exe.config можно добавить новые ключи или изменить существующие ключи. Если определенный ключ не существует, вы можете добавить его вручную и изменить его значение.

Ключи для базы данных очередей, имеющиеся в файле EdgeTransport.exe.config, описаны в следующей таблице.

Key	Значение по умолчанию	Описание
QueueDatabaseBatchSize	40	Указывает количество операций ввода-вывода, которое может группироваться перед выполнением. По умолчанию этого ключа нет в файле EdgeTransport.exe.config.
QueueDatabaseBatchTimeout	100	Указывает максимальное время ожидания группировки операций ввода-вывода перед выполнением (в миллисекундах). Операции ввода-вывода базы данных выполняются немедленно, если выполняются следующие условия: • Количество операций ввода-вывода базы данных, указанное ключом *QueueDatabaseBatchSize* , не достигнуто. • Прошло время, указанное ключом *QueueDatabaseBatchTimeout* . По умолчанию этого ключа нет в файле EdgeTransport.exe.config.
QueueDatabaseMaxConnections	4	Указывает максимальное количество открытых подключений к базе данных ESE.
QueueDatabaseLoggingBufferSize	5 МБ	Указывает объем памяти, используемой для кэширования записей транзакций перед занесением в файл журнала транзакций.
QueueDatabaseLoggingFileSize	5 МБ	Указывает максимальный размер файла журнала транзакций. Когда достигается максимальный размер, создается новый файл журнала.
QueueDatabaseLoggingPath	`%ExchangeInstallPath%TransportRoles\data\Queue`	Указывает каталог по умолчанию для файлов журнала базы данных очереди. Инструкции по изменению расположения базы данных очередей см. в разделе Изменение расположения базы данных очередей.
QueueDatabaseMaxBackgroundCleanupTasks	32	Указывает максимальное количество элементов фонового процесса очистки, которые могут в любой момент времени быть помещены в очередь в пул потоков ядра СУБД.
QueueDatabaseOnlineDefragEnabled	True	Включает или отключает запланированную оперативную дефрагментацию базы данных почтовой очереди. По умолчанию этого ключа нет в файле EdgeTransport.exe.config.
QueueDatabaseOnlineDefragSchedule	`1:00:00` или 1:00 A.M.	Указывает время запуска оперативной дефрагментации базы данных почтовой очереди в 24-часовом формате. Указываемое значение должно вводиться как интервал времени: *чч:мм:сс*, где *ч* — часы, *м* — минуты, а *с* — секунды.
QueueDatabaseOnlineDefragTimeToRun	`3:00:00` или 3 часа	Указывает максимальную продолжительность выполнения оперативной дефрагментации. Даже если дефрагментация не завершится за указанное время, база данных останется в согласованном состоянии. Указываемое значение должно вводиться как интервал времени: *чч:мм:сс*, где *ч* — часы, *м* — минуты, а *с* — секунды.

Key	Значение по умолчанию	Описание
QueueDatabasePath	`%ExchangeInstallPath%TransportRoles\data\Queue`	Указывает каталог по умолчанию для файлов базы данных очереди. Инструкции по изменению расположения базы данных очередей см. в разделе Изменение расположения базы данных очередей.

Свойства очереди

Очередь обладает рядом свойств, описывающих ее предназначение и состояние. Некоторые свойства очереди применяются к ней при создании и не изменяются впоследствии. Другие свойства указывают состояние, размер, время или другие показатели, которые часто обновляются.

NextHopSolutionKey

Компонент маршрутизации классификатора в службе транспорта Microsoft Exchange выбирает пункт назначения для сообщения, и этот пункт используется для создания очереди доставки. Пункт назначения для каждого получателя указывается с помощью свойства **NextHopSolutionKey**. Каждое уникальное значение свойства **NextHopSolutionKey** соответствует отдельной очереди доставки.

Свойство **NextHopSolutionKey** содержит следующие поля:

- **DeliveryType**. Представляет результаты классификации сообщения и способ передачи сообщения на следующий прыжок, который может быть конечным местом назначения сообщения или промежуточным прыжком на этом пути. Служба транспорта использует предопределенный список значений для свойства **DeliveryType**.

  В зависимости от значения **DeliveryType** в очередь добавляется свойство **NextHopCategory** :

  - Значение `External` указывает, что следующий прыжок очереди находится за пределами организации Exchange.
  - Значение `Internal` указывает, что следующий прыжок очереди находится в организации Exchange.

    Обратите внимание, что для доставки во внешнюю систему сообщению может потребоваться пройти один или несколько внутренних транзитных участков.

- **NextHopDomain**: использует определенные значения на основе значения поля **DeliveryType** . Значение данного поля фактически является именем очереди доставки.

  Значение свойства **NextHopDomain** не всегда является доменным именем. Например, это может быть имя целевого сайта Active Directory или группы DAG. Это поле следует рассматривать как *имя следующего транзитного участка*.

- **NextHopConnector**: использует определенные значения на основе значения поля **DeliveryType** . Значение этого поля всегда выражается как GUID. Если это поле не используется, его значением будет идентификатор GUID из одних нолей.

  Значение свойства **NextHopConnector** не всегда совпадает с идентификатором GUID соединителя. Например, это может быть GUID целевого сайта Active Directory или группы DAG. Это поле следует рассматривать как *GUID следующего транзитного участка*.

Значения свойств **DeliveryType**, **NextHopCategory**, **NextHopDomain** и **NextHopConnector** описаны в следующей таблице.

Свойство Delivery Type в средстве просмотра очереди	Свойство DeliveryType в командной консоли Exchange	Описание	NextHopCategory	NextHopDomain

Свойство Delivery Type в средстве просмотра очереди	Свойство DeliveryType в командной консоли Exchange	Описание	NextHopCategory	NextHopDomain
Агент доставки	`DeliveryAgent`	Очередь содержит сообщения, адресованные получателям в адресном пространстве без использования протокола SMTP, которое обслуживается агентом доставки и его соединителем. В качестве исходного сервера для соединителя настроен локальный сервер почтовых ящиков. Дополнительные сведения см. в статье Delivery Agents and Delivery Agent Connectors.	Внешний	Это значение представляет целевое адресное пространство, настроенное для соединителя агента доставки. Например, `MOBILE`.
DnsConnectorDelivery	`DnsConnectorDelivery`	Очередь содержит сообщения для доставки получателям в домене SMTP. Для соединителя отправки, обслуживающего домен, в качестве исходного сервера указан локальный транспортный сервер, а также включена маршрутизация DNS.	External	Это значение — целевое адресное пространст настроенное на соединителе отправки. Например, `contoso.com`.
Heartbeat	`Heartbeat`	Это значение зарезервировано для внутреннего использования корпорацией Майкрософт. Дополнительные сведения о пульсе см. в разделе Теневая избыточность в Exchange Server.	н/д	н/д

Свойство Delivery Type в средстве просмотра очереди	Свойство DeliveryType в командной консоли Exchange	Описание	NextHopCategory	NextHopDomain
MapiDelivery	`MapiDelivery`	**Примечание**. Это значение не используется Exchange 2013 или более поздней версии. Оно включено для обеспечения обратной совместимости с Exchange 2010. Очередь содержит сообщения для доставки транспортным сервером-концентратором Exchange 2010 в почтовый ящик на сервере почтовых ящиков Exchange 2010 на локальном сайте Active Directory.	н/д	н/д
NonSmtpGatewayDelivery	`NonSmtpGatewayDelivery`	Очередь содержит сообщения, адресованные получателям в адресном пространстве без использования протокола SMTP, которое обслуживается внешним соединителем. В качестве исходного сервера для соединителя настроен локальный сервер почтовых ящиков. Дополнительные сведения см. в статье Foreign Connectors.	Внешний	Это значение представляет собой целевое адресное пространство, настроенное для внешнего соединителя. Например, `FAX`.

Свойство Delivery Type в средстве просмотра очереди	Свойство DeliveryType в командной консоли Exchange	Описание	NextHopCategory	NextHopDomain
Теневая избыточность	`ShadowRedundancy`	Сообщения хранятся в теневой очереди. В теневой очереди хранятся избыточные копии передаваемых сообщений на случай неуспешной доставки основных сообщений. Дополнительные сведения см. в разделе Теневая избыточность в Exchange Server.	Внутренний	Это значение представляет собой полное доменное имя основного транспортного сервера, для которого в теневой очереди хранятся избыточные копии основных сообщений. Например, `mailbox01.contoso.com`.
SmartHostConnectorDelivery	`SmartHostConnectorDelivery`	Очередь содержит сообщения для доставки получателям в домене SMTP. Для соединителя отправки, обслуживающего домен, в качестве исходного сервера указан локальный транспортный сервер, а также включена маршрутизация через промежуточные узлы.	Внешний	Это значение является списком промежуточны узлов, настроенных на соединителе отправки. Промежуточные узлы можно настроить в качестве полных доменных имен и/или IP-адресов. Значения могут являться одним из следующих элементов. **Полное доменное имя**: синтаксис : `<FQDN1,FQDN2,...>`. Например, `smarthost01.contoso.com` или `smarthost01.contoso.com,smarthost02.fabrikam.` **IP-адрес**: синтаксис : `<[IPAddress1],[IPAddress2],...>`. Например, `[10.10.10.100]` и `[10.10.10.100],[10.10.10.101]`. **Полное доменное имя и IP-адрес**: синтаксис имеет `<[IPAddress1],FQDN1,...>`значение и зависит от того, как интеллектуальные узлы перечислены в соединителе отправки. Например, `[172.17.17.7],relay.tailspintoys.c` или `mail.contoso.com,[192.168.1.50]`.
Доставка в Exchange Online по протоколу SMTP	`SmtpDeliveryToExo`	Это значение не используется в локальной среде Exchange.	н/д	н/д

Свойство Delivery Type в средстве просмотра очереди	Свойство DeliveryType в командной консоли Exchange	Описание	NextHopCategory	NextHopDomain
Доставка в почтовый ящик по протоколу SMTP	`SmtpDeliveryToMailbox`	Очередь содержит сообщения для доставки получателям почтовых ящиков Exchange 2013 или более поздних версий. Целевая база данных почтовых ящиков находится в одном из следующих расположений: • Локальный сервер почтовых ящиков Exchange 2013 или более поздней версии. • Сервер почтовых ящиков Exchange 2019 в том же daG Exchange 2019. • на сервере почтовых ящиков Exchange 2016 в той же группе DAG Exchange 2016; • на сервере почтовых ящиков Exchange 2013 в той же группе DAG Exchange 2013; • Сервер почтовых ящиков Exchange 2013 или более поздней версии на том же сайте Active Directory в средах, отличных от DAG.	Внутренний	Это значение является именем целевой базы данных почтовых ящиков. Например, `Mailbox Database 0471695037`.

Свойство Delivery Type в средстве просмотра очереди	Свойство DeliveryType в командной консоли Exchange	Описание	NextHopCategory	NextHopDomain
Ретрансляция SMTP на исходные серверы соединителя отправки	`SmtpRelayToConnectorSourceServers`	Очередь содержит сообщения для доставки в адресное пространство SMTP или другое, обслуживаемое соединителем отправки, соединителем агента доставки или внешним соединителем. В качестве исходного сервера для соединителя настроен удаленный транспортный сервер. Удаленный транспортный сервер может быть сервером почтовых ящиков Exchange 2013 или более поздней версии или транспортным сервером-концентратором Exchange 2010. Удаленный транспортный сервер может находиться на локальном или удаленном сайте Active Directory.	Внутренний	Это значение является именем целевого соединителя отправки, соединителя агента доставки или внешнего соединителя. Наприме `Contoso.com Send Connector`.
Ретрансляция SMTP на группу обеспечения доступности баз данных	`SmtpRelayToDag`	Очередь содержит сообщения для доставки получателям почтовых ящиков Exchange 2013 или более поздних версий, где целевая база данных почтовых ящиков находится в удаленной daG. Удаленная группа DAG может находиться на локальном или удаленном сайте Active Directory.	Внутренний	Это значение является именем целевой групп обеспечения доступности баз данных. Наприм `DAG1`.

Свойство Delivery Type в средстве просмотра очереди	Свойство DeliveryType в командной консоли Exchange	Описание	NextHopCategory	NextHopDomain
Ретрансляция SMTP на группу доставки в почтовый ящик	`SmtpRelayToMailboxDeliveryGroup`	Очередь содержит сообщения для доставки получателям устаревших почтовых ящиков, где целевой почтовый ящик находится на сервере почтовых ящиков Exchange 2010. Сообщение передается на транспортный сервер-концентратор Exchange 2010. Целевой транспортный сервер-концентратор Exchange 2010 может находиться на локальном или удаленном сайте Active Directory.	Внутренний	Имя очереди использует синтаксис : `Site:<ADSiteName>;Version:<ExchangeVersion>`, где *<ADSiteName>* — это имя целевого сайта Acti Directory, а *<ExchangeVersion>* — версия Exchange 2010 на сервере почтовых ящиков.

Свойство Delivery Type в средстве просмотра очереди	Свойство DeliveryType в командной консоли Exchange	Описание	NextHopCategory	NextHopDomain
Ретрансляция SMTP на удаленный сайт Active Directory	`SmtpRelayToRemoteActiveDirectorySite`	Очередь содержит сообщения для доставки в удаленное место назначения, а топология маршрутизации требует маршрутизации сообщения через определенный сайт Active Directory. Сайт является транзитным участком на пути к конечному пункту назначения. Это происходит в следующих случаях: сообщение необходимо направить через сайт концентратора; сообщение необходимо доставить через соединитель отправки, настроенный на пограничном транспортном сервере, который подписан на удаленный сайт Active Directory.	Внутренний	Это значение является именем целевого сайта Active Directory. Например, `NorthAmericaSite`.
Ретрансляция SMTP в указанный удаленный лес	`SmtpRelayToRemoteForest`	Это значение не используется в локальной среде Exchange.	н/д	н/д

Свойство Delivery Type в средстве просмотра очереди	Свойство DeliveryType в командной консоли Exchange	Описание	NextHopCategory	NextHopDomain
Ретрансляция SMTP на указанные серверы Exchange Server	`SmtpRelayToServers`	Очередь содержит сообщения для доставки в группу рассылки, настроенную для определенного сервера расширения. Сервер расширения может быть сервером почтовых ящиков Exchange 2013 или более поздней версии или транспортным сервером-концентратором Exchange 2010. Сервер расширения может находиться на локальном или удаленном сайте Active Directory.	Внутренний	Это значение является полным доменным именем целевого сервера развертывания. Например, `mailbox01.contoso.com`.
SmtpRelayToTiRg	`SmtpRelayToTiRg`	**Примечание**. Это значение не используется Exchange 2013 или более поздней версии. Оно включено для обеспечения обратной совместимости с Exchange 2010. Очередь содержит сообщения для доставки транспортным сервером-концентратором Exchange 2010 в группу маршрутизации Exchange 2003.	н/д	н/д

Свойство Delivery Type в средстве просмотра очереди	Свойство DeliveryType в командной консоли Exchange	Описание	NextHopCategory	NextHopDomain
Ретрансляция SMTP на сайте Active Directory	`SmtpRelayWithinAdSite`	**Примечание**. Это значение не используется Exchange 2013 или более поздней версии. Оно включено для обеспечения обратной совместимости с Exchange 2010. Очередь содержит сообщения для доставки транспортным сервером-концентратором Exchange 2010 на другой транспортный сервер-концентратор на том же сайте Active Directory.	н/д	н/д
Ретрансляция SMTP из сайта Active Directory на пограничный транспортный сервер	`SmtpRelayWithinAdSiteToEdge`	Очередь содержит сообщения для доставки на внешний SMTP-домен, обслуживаемый соединителем отправки, который настроен на пограничном транспортном сервере. Пограничный транспортный сервер подписан на локальный сайт Active Directory.	Внутренний	Это значение представляет собой имя соединителя отправки, который отправляет исходящую почту с пограничного транспортно сервера в Интернет. Этот соединитель отправ автоматически создается подпиской Edge и называется EdgeSync — <*ADSiteName*> в Интернет.
Undefined	`Undefined`	Это значение используется только для очередей передачи и подозрительных сообщений.	Внутренний	Для очереди отправки это значение равно `Submisssion`. Для очереди подозрительных сообщений это значение равно `Poison Messag`
Недоступен	`Unreachable`	Это значение используется только для очереди недоставленных сообщений.	Внутренний	Это значение равно `Unreachable Domain`.

IncomingRate, OutgoingRate и Velocity

Exchange измеряет скорость сообщений, поступающих в очередь и выходящих из нее, и сохраняет эти значения в свойствах очереди. Эти значения скорости можно использовать в качестве показателей работоспособности очереди и транспортного сервера. Свойства описываются в следующей таблице:

Свойство	Описание
IncomingRate	Скорость поступления сообщений в очередь. Скорость — это количество сообщений в секунду, усредненное за последнюю минуту.
Исходящая скорость	Скорость, с которой сообщения покидают очередь. Скорость — это количество сообщений в секунду, усредненное за последнюю минуту.
Velocity	Скорость очистки очереди, рассчитанная путем вычитания значения **IncomingRate** из значения **OutgoingRate**. Если значение больше 0, сообщения покидают очередь быстрее, чем поступают в нее. Если значение равно 0, сообщения покидают очередь и поступают в нее с одинаковой скоростью. Это значение также отображается, если очередь неактивна. Если значение меньше 0, сообщения поступают в очередь быстрее, чем покидают ее. Значение **Velocity** отображается в результатах вызова метода **Get-Queue**.

На базовом уровне положительное значение свойства **Velocity** является признаком работоспособной очереди, которая быстро опустошается, а отрицательное значение свойства **Velocity** указывает, что очередь опустошается недостаточно эффективно. Однако вам также следует учитывать значения свойств **IncomingRate**, **OutgoingRate** и **MessageCount**, а также абсолютное значение свойства **Velocity**.

Возьмем, к примеру, очередь со следующими значениями свойств:

- **Скорость**: -50
- **MessageCount**: 1000
- **Исходящая скорость**: 10
- **IncomingRate**: 60

Учитывая значения свойств этой очереди, по отрицательному значению свойства **Velocity** становится очевидно, что очередь не очищается должным образом.

Теперь рассмотрим очередь со следующими значениями свойств:

- **Скорость**: -0,85
- **MessageCount**: 2
- **Исходящая скорость**: 0,15
- **IncomingRate**: 1

Хотя значение свойства **Velocity** отрицательное, оно очень близко к нулю, а значения остальных свойств также очень малы. Следовательно, отрицательное значение свойства **Velocity** не указывает на проблему с очередью.

Состояние очереди

Текущее состояние очереди хранится в свойстве **Status**. В приведенной ниже таблице описываются возможные значения состояния очереди.

Состояние очереди	Описание
Активное	Очередь активно передает сообщения.
Connecting	Идет подключение очереди к следующему транзитному участку.
Ready	Очередь недавно передавала сообщения, но сейчас пуста.
Retry	Последняя попытка автоматического или ручного подключения завершилась ошибкой, и очередь ожидает повторного подключения.

Состояние очереди	Описание
Suspended	Администратор вручную приостановил работу очереди, чтобы предотвратить доставку сообщений. Новые сообщения могут поступать в очередь, а сообщения, которые уже передаются на следующий транзитный участок, будут доставлены и покинут очередь. Другие сообщения не покинут очередь, пока администратор не возобновит ее работу вручную. **Примечания.** Вы можете приостанавливать работу следующих очередей: • Очереди доставки с любым состоянием. • Очередь "Сообщения с недостижимым местом назначения". Если приостановить работу этой очереди, сообщения больше не будут автоматически отправляться классификатору при обнаружении изменений конфигурации. Чтобы эти сообщения были автоматически отправлены заново, необходимо вручную возобновить работу очереди. • Очередь передачи. Если приостановить работу этой очереди, классификатор не будет извлекать сообщения, пока работа очереди не будет возобновлена. При этом не меняется состояние сообщений в очереди.

Другие свойства очереди

Есть и другие свойства очереди, не требующие пояснений. Большинство этих свойств очереди можно использовать в качестве параметров фильтра. Указав условия фильтра, вы можете быстро находить очереди и выполнять с ними различные действия. Полное описание фильтруемых свойств очереди см. в разделе Свойства очереди.

Важное свойство очереди, которое следует упомянуть в этом разделе, — **MessageCount**, отвечающее за отображение количества сообщений в очереди. Это свойство является важным индикатором состояния очереди. Например, очередь доставки, содержащая большое количество сообщений, которое продолжает расти и совсем не уменьшается, может указывать на проблему с маршрутизацией или транспортным конвейером, на которую следует обратить внимание.

Свойства сообщений

У сообщения в очереди есть ряд свойств. Многие из них содержат сведения, которые использовались для создания сообщения. На некоторые свойства состояния сообщений и сведений о них в значительной степени влияют соответствующие свойства очереди. Однако значения свойств отдельных сообщений могут не совпадать со значениями соответствующих свойств очереди. Другие свойства содержат сведения о состоянии, времени или других показателях, которые часто обновляются.

Состояние сообщения

Текущее состояние сообщения хранится в его свойстве **Status**. В приведенной ниже таблице описываются возможные значения состояния сообщения.

Состояние сообщения	Описание
Активное	Если сообщение находится в очереди доставки, оно доставляется в пункт назначения. Если же сообщение находится в очереди передачи, его обрабатывает классификатор.
Locked	Майкрософт зарезервировала это значение для внутреннего использования. Оно не применяется в локальных организациях Exchange.
PendingRemove	Сообщение было удалено администратором, но сообщение уже было передано в следующий прыжок. Сообщение будет удалено, если доставка заканчивается ошибкой, которая приводит к повторному входу сообщения в очередь. В противном случае доставка будет продолжена.
PendingSuspend	Сообщение было приостановлено администратором, но сообщение уже было передано в следующий прыжок. Сообщение будет приостановлено, если доставка завершается ошибкой, которая приводит к повторному входу сообщения в очередь. В противном случае доставка будет продолжена.
Ready	Сообщение находится в очереди и готово к обработке.
Retry	Последняя попытка автоматического или ручного подключения для очереди, которая содержит сообщение, завершилась ошибкой. Сообщение ожидает следующей попытки автоматического подключения очереди.
Suspended	Администратор вручную приостановил доставку сообщения. Все сообщения в очереди подозрительных сообщений находятся в состоянии окончательной остановки.

Другие свойства сообщений

Существуют другие свойства сообщений, значения которых очевидны. Большинство этих свойств сообщений можно использовать в качестве параметров фильтрации. Указывая условия отбора, можно быстро находить сообщения и выполнять действия над ними. Полное описание свойств фильтруемых сообщений см. в разделе Свойства сообщений в очередях.

Управление очередями и находящимися в них сообщениями

Средство просмотра очередей и командлеты управления журналами и сообщениями в командной консоли Exchange ограничены одним сервером Exchange. Вы можете просматривать или работать с отдельными очередями или сообщениями, а также с несколькими очередями или сообщениями, но только на определенном сервере.

Командлет **Get-QueueDigest** появился в Exchange 2013 для предоставления общего совокупного представления состояния очередей на всех серверах в определенной области. Областью может быть группа DAG, сайт Active Directory, список серверов или весь лес Active Directory. Обратите внимание, что очереди на подписанном пограничном транспортном сервере в сети периметра не включаются в результаты. Кроме того, командлет **Get-QueueDigest** доступен на пограничных транспортных серверах, но результаты включают только очереди с пограничного транспортного сервера.

> ⓘ **Примечание**
>
> По умолчанию командлет **Get-QueueDigest** отображает очереди доставки, содержащие десять или более сообщений, а результаты находятся в возрасте от одной до двух минут. Инструкции по изменению этих значений по умолчанию см. в разделе **Настройка Get-QueueDigest**.

В следующей таблице описаны задачи управления, которые можно выполнять для очередей или сообщений, находящихся в них.

Задача	Описание	Используемое средство	Инструкции
Просмотр и фильтрация очередей на сервере	Отображается одна или несколько очередей на транспортном сервере. Результаты можно использовать для выполнения действий с очередями.	Средство просмотра очередей или командлет **Get-Queue** .	Действия по работе с очередями
Просмотр и фильтрация очередей на определенных серверах в отдельных группах DAG, на отдельных сайтах Active Directory или во всем лесу Active Directory.	Отображается сводный список очередей.	Командлет **Get-QueueDigest**	Действия по работе с очередями
Приостановка очередей	Приостанавливается доставка сообщений в очереди. Новые сообщения продолжают поступать в очередь, но ни одно сообщение не может ее покинуть.	Средство просмотра очередей или командлет **Suspend-Queue** .	Действия по работе с очередями
Возобновление очередей	Отменяется предыдущее действие и возобновляется доставка сообщений в очереди.	Средство просмотра очередей или командлет **Resume-Queue** .	Действия по работе с очередями
Повтор очередей	Выполняется попытка подключения к следующему транзитному участку. Без ручного вмешательства попытка подключения выполняется указанное количество раз через определенные интервалы времени. Вне зависимости от того, как выполняется подключение (вручную или автоматически), любая попытка подключения приводит к сбросу времени следующей попытки. Дополнительные сведения см. в статье Повторная отправка сообщений и интервалы истечения срока действия.	Средство просмотра очередей или командлет **Retry-Queue** .	Действия по работе с очередями

Задача	Описание	Используемое средство	Инструкции
Повторная отправка сообщений, находящихся в очередях	Сообщения в очереди заново отправляются в очередь передачи для повторной классификации.	**Повторная очередь** с параметром *повторной отправки* Обратите внимание, что средство просмотра очередей можно использовать для повторной отправки сообщений, но только из очереди подозрительных сообщений. Чтобы повторно отправить подозрительное сообщение, сначала необходимо возобновить его в средстве просмотра очередей или с помощью командлета **Resume-Message** .	Действия по работе с очередями
Приостановка сообщений, находящихся в очередях	Приостанавливается доставка сообщения. С помощью этого действия можно предотвратить доставку сообщения всем адресатам в определенной очереди или всем адресатам во всех очередях.	Средство просмотра очередей или командлет **Suspend-Message** .	Инструкции по работе с сообщениями в очередях
Возобновление доставки сообщений, находящихся в очередях	Отменяется предыдущее действие и возобновляется доставка сообщений в очереди. Вы можете возобновить доставку сообщения всем получателям в определенной очереди или всем получателям во всех очередях.	Средство просмотра очередей или командлет **Resume-Message** .	Инструкции по работе с сообщениями в очередях
Удаление сообщений из очередей	Доставка сообщения отменяется окончательно. Вы можете отменить доставку сообщения всем получателям в определенной очереди или всем получателям во всех очередях. Вы также можете отправить отчет о недоставке отправителю при удалении сообщения.	Средство просмотра очередей или командлет **Remove-Message** .	Инструкции по работе с сообщениями в очередях
Экспорт сообщений из очередей	Сообщение копируется в указанное расположение. Сообщение не удаляется из очереди, но его копия сохраняется в виде файла в указанном расположении. Это позволяет администраторам или должностным лицам изучить сообщение позже. Прежде чем экспортировать сообщение, необходимо временно приостановить его доставку.	Только командлет **Export-Message**.	Экспорт сообщений из очередей

Действия по работе с очередями

Статья • 04.04.2023

В Exchange Server для управления очередями можно использовать средство просмотра очередей на панели элементов Exchange или командную консоль Exchange. Дополнительные сведения см. в разделе Queues and messages in queues.

В этой статье рассказывается, как выполнить перечисленные ниже задачи с очередями.

- **Просмотр очередей**
- **Очереди повторных попыток**. Если серверу Exchange Server не удается подключиться к следующему прыжку, очередь помещается в состояние Повтор, и сервер периодически пытается подключиться и доставить сообщения. Повторно запуская очередь вручную, вы переопределяете запланированное время повторной попытки, вызывая незамедлительную попытку подключения.
- **Очереди повторной отправки**. Повторная отправка очереди похожа на повторную попытку очереди, за исключением того, что сообщения отправляются обратно в очередь отправки для обработки классификатором, а не сразу пытаются подключиться к следующему прыжку. Это полезно, если изменения инфраструктуры сети препятствуют доставке сообщений в очереди.
- **Приостановка очередей**. Новые сообщения могут входить в очередь, и сообщения, которые передаются в следующий прыжок, покинут очередь, но в противном случае сообщения не будут покидать очередь, пока очередь не будет возобновлена вручную.
- **Возобновление очередей**. Перезапустите доставку исходящих сообщений для очереди с состоянием Приостановлено. При возобновлении работы очереди состояние сообщений в ней не меняется (например, сообщения с состоянием "Приостановлено" остаются в этом состоянии и не покидают очередь).

Процедуры для сообщений в очередях см. в разделе Процедуры для сообщений в очередях.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут
- Чтобы найти и открыть Элементы управления Exchange, воспользуйтесь одной из указанных ниже процедур.

- **Windows 10**. Щелкните **Запустить**>**все приложения**> Microsoft Exchange Server **<панель элементов Exchange version>**>.
- **Windows Server 2012 R2 или Windows 8.1**. На начальном экране откройте представление Приложения, щелкнув стрелку вниз в левом нижнем углу или проведя пальцем вверх по центру экрана. Ярлык **панели элементов Exchange** находится в группе с именем **Microsoft Exchange Server <version>**.
- **Windows Server 2012**. Используйте любой из следующих методов:
  - На начальном экране щелкните пустую область и введите Панель элементов Exchange.
  - Откройте рабочий стол или начальный экран и нажмите клавиши Windows+Q. На панели чудо-кнопки "Поиск" введите Панель элементов Exchange.
  - Откройте рабочий стол и переместите курсор в его правый верхний угол (или на начальном экране проведите пальцем влево от его правого края), чтобы отобразились чудо-кнопки. Нажмите чудо-кнопку "Поиск" и введите Панель элементов Exchange.

  Когда ярлык появится в результатах, выберите его.

- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Дополнительные сведения об использовании фильтров и значений удостоверений в командной консоли Exchange см. в статье Поиск очередей и сообщений в очередях в командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Очереди" в разделе Разрешения потока обработки почты .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Просмотр очередей

Просмотр очередей с помощью средства просмотра очереди

1. В **Элементы управления Exchange** перейдите к разделу **Средства для потока почты** и дважды щелкните **Средство просмотра очереди**, чтобы открыть инструмент в новом окне.
2. В средстве просмотра очереди перейдите на вкладку **Очереди**. Отобразится список всех очередей на сервере, к которому установлено подключение.
3. Для экспорта списка очередей можно использовать ссылку **Экспортировать список** в области действий. Дополнительные сведения см. в разделе How to Export Lists from the Exchange Management Consoles.

Просмотр очередей с помощью командной консоли Exchange

Для просмотра очередей используйте приведенный ниже синтаксис.

PowerShell

```
Get-Queue [-Filter <Filter> -Server <ServerIdentity> -Include <Internal | External | Empty | DeliveryType> -Exclude <Internal | External | Empty | DeliveryType>]
```

В этом примере показано, как просмотреть основные сведения о непустых очередях на сервере Mailbox01.

PowerShell

```
Get-Queue -Server Mailbox01 -Exclude Empty
```

В этом примере отображаются подробные сведения обо всех очередях на локальном сервере Exchange Server, содержащих более 100 сообщений.

PowerShell

```
Get-Queue -Filter "MessageCount -gt 100" | Format-List
```

Дополнительные сведения см. в статьях Get-Queue и Find queues and messages in queues in the Exchange Management Shell.

Просмотр сводных сведений об очередях на нескольких серверах Exchange Server с помощью командной консоли Exchange

Командлет **Get-QueueDigest** обеспечивает высокоуровневое сводное представление состояния очередей на всех серверах в определенной области (например, в группе обеспечения доступности баз данных, на сайте Active Directory, в списке серверов или во всем лесу Active Directory).

По умолчанию командлет **Get-QueueDigest** отображает очереди доставки, содержащие десять или более сообщений, а результаты находятся в возрасте от одной до двух минут. Инструкции по изменению этих значений по умолчанию см. в разделе Настройка Get-QueueDigest.

Примечания.

- Очереди на подписанном пограничном транспортном сервере не включаются в выходные данные командлета **Get-QueueDigest**.
- Командлет **Get-QueueDigest** доступен на пограничных транспортных серверах, но возвращает только локальные очереди с этих серверов.

Чтобы просмотреть сводные сведения об очередях на нескольких серверах Exchange Server, выполните следующую команду:

PowerShell

```
Get-QueueDigest <-Server <ServerIdentity1,ServerIdentity2...> | -Dag
<DagIdentity1,DagIdentity2...> | -Site <ADSiteIdentity1,ADSiteIdentity2...>
| -Forest> [-Filter <Filter>]
```

В этом примере отображаются сводные сведения об очередях на всех серверах почтовых ящиков Exchange 2013 или более поздних версий на сайте Active Directory с именем FirstSite, где число сообщений больше 100.

PowerShell

```
Get-QueueDigest -Site FirstSite -Filter "MessageCount -gt 100"
```

В этом примере отображаются сводные сведения об очередях на всех серверах почтовых ящиков в группе доступности базы данных (DAG) с именем DAG01, где состояние очереди имеет значение **Retry**.

PowerShell

```
Get-QueueDigest -Dag DAG01 -Filter "Status -eq 'Retry'"
```

Дополнительные сведения см. в статье Get-QueueDigest.

Повторный запуск очередей

При повторном запуске очереди доставки сразу выполняется принудительная попытка подключения и переопределяется время следующей запланированной попытки. Дополнительные сведения о расписании повторных попыток для очередей см. в разделе Повторная отправка сообщений, повторная отправка и интервалы истечения срока действия.

Примечания.

- Чтобы это действие было выполнено, очередь должна находиться в состоянии "Повтор".
- Если попытка подключения не удалась, таймер интервала повторения сбрасывается.

Повторный запуск очереди с помощью средства просмотра очереди

1. В **Элементы управления Exchange** перейдите к разделу **Средства для потока почты** и дважды щелкните **Средство просмотра очереди**, чтобы открыть инструмент в новом окне.

2. В средстве просмотра очереди перейдите на вкладку **Очереди**. Вы увидите список всех очередей на сервере, с которым установлено соединение.

3. Щелкните **Создать фильтр** и введите выражение фильтра следующим образом:
   a. Выберите пункт **Состояние** из раскрывающегося списка свойств очереди.
   b. Выберите пункт **Равно** из раскрывающегося списка операторов сравнения.
   c. Выберите пункт **Повторить** из раскрывающегося списка значений.
   d. Нажмите кнопку **Применить фильтр**. Будут показаны все очереди, которые в данный момент находятся в состоянии **Повтор**.
   e. Выберите в списке одну или несколько очередей. Щелкните выделение правой кнопкой мыши и в контекстном меню выберите пункт **Повторить очередь**. Если попытка подключения будет успешной, состояние очереди изменится на **Активно**. Если установить подключение не удастся, очередь

останется в состоянии **Повтор**, причем время следующего повторения обновится.

Повторный запуск очереди с помощью командной консоли Exchange

Чтобы повторить очереди, введите команду в следующем формате.

```
PowerShell

Retry-Queue <-Identity QueueIdentity | -Filter QueueFilter [-Server
ServerIdentity]>
```

В этом примере показано, как на локальном сервере выполнить повтор всех очередей, находящихся в состоянии "Повтор".

```
PowerShell

Retry-Queue -Filter "Status -eq 'Retry'"
```

В этом примере показано, как повторно запустить очередь с именем contoso.com на сервере Mailbox01.

```
PowerShell

Retry-Queue -Identity Mailbox01\contoso.com
```

Как убедиться, что все получилось?

Чтобы проверить, удалось ли вам повторить обработку очереди, используйте любую из описанных ниже процедур.

- В средстве просмотра очереди проверьте значения свойств **Состояние**, **Время следующей попытки** и **Последняя ошибка**.
- В командной консоли Exchange замените *<QueueIdentity>* удостоверением очереди и используйте следующий синтаксис для проверки значений свойств:

  ```
  PowerShell

  Get-Queue -Identity <QueueIdentity> | Format-Table -Auto
  Identity,Status,LastRetryTime,NextRetryTime
  ```

Повторная отправка очередей

При повторной отправке очереди все сообщения из нее отправляются обратно в очередь передачи для обработки классификатором. Дополнительные сведения о классификаторе см. в статье Mail flow and the transport pipeline.

Примечания.

- С помощью средства просмотра очереди невозможно выполнять повторную отправку. Можно использовать только командную консоль Exchange.
- Вы можете выполнять повторную отправку следующих очередей:
  - очереди доставки в состоянии повтора;
  - очереди "Сообщения с недостижимым местом назначения". Сообщения с состоянием "Приостановлено" не отправляются.
- Для очереди подозрительных сообщений недоступна повторная отправка, но вы можете повторно отправлять отдельные сообщения из очереди. Дополнительные сведения см. в разделе Повторная отправка сообщений, находящихся в очереди подозрительных сообщений далее в этой статье.
- Вместо повторной отправки очереди можно экспортировать сообщения в EML-файлы и повторно отправить их с помощью каталога Воспроизведения на любом сервере Exchange Server. Дополнительные сведения см. в статье Экспорт сообщений из очередей.

Повторная отправка очередей с помощью командной консоли Exchange

Для повторной отправки очереди используйте следующий синтаксис:

PowerShell

```
Retry-Queue <-Identity QueueIdentity | -Filter "Status -eq 'Retry'" -Server
ServerIdentity> -Resubmit $true
```

В этом примере показано, как повторно отправить все сообщения, находящиеся в любых очередях доставки с состоянием "Повтор", на сервере Mailbox01.

PowerShell

```
Retry-Queue -Filter "Status -eq 'Retry'" -Server Mailbox01 -Resubmit $true
```

В этом примере показано, как повторно отправить все сообщения, находящиеся в очереди "Сообщения с недостижимым местом назначения", на сервере Mailbox01.

PowerShell

```
Retry-Queue -Identity Mailbox01\Unreachable -Resubmit $true
```

Дополнительные сведения см. в статье Retry-Queue.

Как проверить, все ли получилось?

Чтобы проверить, удалось ли вам выполнить повторную отправку очереди, используйте любую из описанных ниже процедур.

- В средстве просмотра очереди проверьте ее свойства.
- В командной консоли Exchange замените <*QueueIdentity*> идентификатором очереди и выполните следующую команду, чтобы проверить значения свойств:

  PowerShell

  ```
  Get-Queue -Identity <QueueIdentity>
  ```

Повторная отправка сообщений, находящихся в очереди подозрительных сообщений

Повторная отправка сообщений из очереди подозрительных сообщений — это особый случай. Эти сообщения невозможно отправлять так же, как в других очередях, но вы можете отправлять отдельные сообщения из очереди подозрительных сообщений.

Примечания.

- Сообщения из очереди подозрительных сообщений могут быть либо по-настоящему вредоносными, либо допустимыми сообщениями, которые стали жертвами плохо написанного агента транспорта или программной ошибки. Если вы сомневаетесь в надежности сообщений из очереди подозрительных сообщений, следует экспортировать их в файл для изучения. Дополнительные сведения см. в статье Экспорт сообщений из очередей.
- Процедура повторной отправки сообщений из очереди подозрительных сообщений аналогична возобновлению приостановленных сообщений из других очередей. Вы можете использовать средство просмотра очередей или командную консоль Exchange. Дополнительные сведения о возобновлении сообщений см. в разделе Возобновление сообщений в очередях.

- Очередь подозрительных сообщений видна только в том случае, если очередь содержит сообщения.

Повторная отправка сообщений, находящихся в очереди подозрительных сообщений, с помощью средства просмотра очереди

1. В **Элементы управления Exchange** перейдите к разделу **Средства для потока почты** и дважды щелкните **Средство просмотра очереди**, чтобы открыть инструмент в новом окне.
2. В средстве просмотра очереди перейдите на вкладку **Очереди**. Вы увидите список всех очередей на сервере, с которым установлено соединение.
3. Выберите очередь подозрительных сообщений. В области действий нажмите **Просмотреть сообщения**.
4. Выделите одно или несколько сообщений в списке, щелкните его правой кнопкой мыши и выберите команду **Возобновить**.

Повторная отправка сообщений, находящихся в очереди подозрительных сообщений, с помощью командной консоли Exchange

Чтобы повторно отправить сообщение, находящееся в очереди подозрительных сообщений, выполните указанные ниже действия.

1. Найдите идентификатор сообщения, выполнив приведенную ниже команду на локальном сервере.

   PowerShell

   ```
   Get-Message -Queue Poison | Format-Table Identity
   ```

2. Используйте идентификатор сообщения, найденный на предыдущем шаге, в следующей команде.

   PowerShell

   ```
   Resume-Message <PoisonMessageIdentity>
   ```

   В этом примере возобновляется сообщение из очереди опасных сообщений со значением идентификатора 222.

   PowerShell

```
Resume-Message 222
```

Дополнительные сведения см. в статье Resume-Message.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно повторили отправку сообщения из очереди подозрительных сообщений, проверьте наличие сообщения в очереди с помощью любой из описанных ниже процедур.

- В средстве просмотра очереди откройте очередь подозрительных сообщений, из которой выполнялась повторная отправка сообщения.
- В командной консоли Exchange выполните следующую команду:

```
PowerShell

Get-Message -Queue Poison
```

Если сообщение, которое вы повторно отправили, было единственным элементом очереди подозрительных сообщений, и эта очередь больше не отображается, то это свидетельствует, что повторная отправка сообщения была выполнена успешно.

Приостановка работы очередей

Вы можете приостановить работу очереди, чтобы остановить поток обработки почты, а затем приостановить одно или несколько сообщений в этой очереди. Дополнительные сведения см. в разделе Приостановка отправки сообщений в очередях.

Примечания.

- Вы можете приостанавливать работу следующих очередей:
  - очереди доставки в любом состоянии;
  - очереди "Сообщения с недостижимым местом назначения". Пока вы не возобновите работу этой очереди вручную, при обнаружении обновлений конфигурации не будет выполняться повторная отправка сообщений в классификатор;
  - очереди передачи. Пока вы не возобновите работу очереди вручную, классификатор не будет извлекать сообщения.
- При этом состояние сообщений в очереди не меняется на "Приостановлено".

Приостановка работы очереди с помощью средства просмотра очереди

1. В **Элементы управления Exchange** перейдите к разделу **Средства для потока почты** и дважды щелкните **Средство просмотра очереди**, чтобы открыть инструмент в новом окне.
2. В средстве просмотра очереди перейдите на вкладку **Очереди**. Вы увидите список всех очередей на сервере, с которым установлено соединение. Для просмотра очередей, соответствующих определенному критерию, необходимо создать фильтр.
3. Выберите одну или несколько очередей, щелкните ее правой кнопкой мыши и выберите команду **Приостановить**.

Приостановка очереди с помощью командной консоли Exchange

Чтобы приостановить очередь, используйте следующий синтаксис:

PowerShell

```
Suspend-Queue <-Identity QueueIdentity | -Filter "QueueFilter" [-Server
ServerIdentity]>
```

В этом примере показано, как приостановить все очереди на локальном сервере, которые находятся в состоянии "Повтор" и в которых не менее 1000 сообщений.

PowerShell

```
Suspend-Queue -Filter "MessageCount -ge 1000 -and Status -eq 'Retry'"
```

В этом примере показано, как приостановить очередь с именем contoso.com на сервере с именем Mailbox01.

PowerShell

```
Suspend-Queue -Identity Mailbox01\contoso.com
```

Дополнительные сведения см. в статье Suspend-Queue.

Как проверить, все ли получилось?

Чтобы проверить, удалось ли вам приостановить очередь, используйте любую из описанных ниже процедур.

- В средстве просмотра очереди убедитесь, что в столбце **Состояние** для этой очереди указано значение "Повтор".
- В командной консоли Exchange замените *<QueueIdentity>* идентификатором очереди и выполните следующую команду, чтобы проверить значение свойства **Status** :

```
PowerShell

Get-Queue -Identity <QueueIdentity>
```

Возобновление работы очередей

При возобновлении работы очереди заново запускается доставка исходящих сообщений из очереди с состоянием "Приостановлено".

Примечания.

- Возобновлять работу можно только для приостановленных очередей.
- При возобновлении работы очереди не меняется состояние сообщений в ней. Например, сообщения с состоянием "Приостановлено" остаются в этом состоянии и не покидают очередь, пока ее работа не будет возобновлена.

Возобновление работы очередей с помощью средства просмотра очереди

1. В **Элементы управления Exchange** перейдите к разделу **Средства для потока почты** и дважды щелкните **Средство просмотра очереди**, чтобы открыть инструмент в новом окне.

2. В средстве просмотра очереди перейдите на вкладку **Очереди**. Вы увидите список всех очередей на сервере, с которым установлено соединение.

3. Щелкните **Создать фильтр** и введите выражение фильтра следующим образом:
   a. Выберите пункт **Состояние** из раскрывающегося списка свойств очереди.
   b. Выберите пункт **Равно** из раскрывающегося списка операторов сравнения.
   c. Выберите **Приостановлено** в раскрывающемся списке значений.

4. Нажмите кнопку **Применить фильтр**. Отобразятся все очереди на сервере, которые приостановлены в текущий момент.

5. Выделите одну или несколько очередей в списке, щелкните правой кнопкой мыши и выберите команду **Возобновить**.

Возобновление работы очередей с помощью консоли управления Exchange

Для возобновления очереди используйте следующий синтаксис:

PowerShell

```
Resume-Queue <-Identity QueueIdentity | -Filter "QueueFilter" [-Server
ServerIdentity]>
```

В этом примере показано, как возобновить все очереди на локальном сервере, находящиеся в состоянии "Приостановлено".

PowerShell

```
Resume-Queue -Filter "Status -eq 'Suspended'"
```

В этом примере показано, как возобновить приостановленную очередь доставки с именем contoso.com на сервере с именем Mailbox01.

PowerShell

```
Resume-Queue -Identity Mailbox01\contoso.com
```

Дополнительные сведения см. в статье Resume-Queue.

Как проверить, все ли получилось?

Чтобы проверить, удалось ли вам возобновить работу очереди, используйте любую из описанных ниже процедур.

- В средстве просмотра очереди убедитесь, что в столбце **Состояние** для этой очереди указано значение, отличное от "Приостановлено" (например, "Активно", "Подключение" или "Готово").

- В командной консоли Exchange замените *<QueueIdentity>* идентификатором очереди и выполните следующую команду, чтобы проверить значение

свойства **Status** :

PowerShell

```
Get-Queue -Identity <QueueIdentity>
```

Свойства очереди в Exchange Server

Статья • 04.04.2023

Фильтрация очередей по одному или нескольким свойствам очереди в Exchange Server позволяет быстро находить и выполнять действия с этими очередями. Перечисленные ниже сценарии служат примерами использования фильтрации очередей для управления потоком обработки почты.

- Вы получаете сообщение от System Center Operations Manager о том, что длина очереди превысила установленное пороговое значение. Необходимо разобраться, существует ли проблема с потоком почты на сервере.

  Вы создаете фильтр для просмотра всех очередей, в которых количество сообщений превышает обычно допустимую норму. Если таким образом выявляется проблема с потоком почты, можно выбрать все очереди, полученные в результате фильтрации, и приостановить их, пока вы продолжаете изучать ситуацию.

- Вы приостанавливаете несколько очередей, чтобы выявить причину неполадок в потоке почты. Устанавливается, что неполадка была вызвана неправильной настройкой соединителя, которая уже устранена.

  Можно создать фильтр для просмотра всех очередей, находящихся в состоянии приостановки, а затем выбрать все очереди, полученные в результате фильтрации, и возобновить эти очереди.

Фильтры очередей можно создать в средстве просмотра очередей на панели элементов Exchange или с помощью параметра *Filter* в командлетах управления очередями. Обратите внимание, что командлеты управления очередями поддерживают больше фильтруемых свойств, чем средство просмотра очереди.

Дополнительные сведения о средстве просмотра очереди см. в статье Queue Viewer. Дополнительные сведения о задачах управления очередями см. в статьях Procedures for queues и Find queues and messages in queues in the Exchange Management Shell.

Свойства очередей, используемые в качестве фильтров

В приведенной ниже таблице описываются свойства очередей, которые можно использовать как фильтры в средстве просмотра очереди и командной консоли Exchange.

Средство просмотра очереди	Командная консоль Exchange	Операторы сравнения	Описание
н/д	`DeferredMessageCount`	Равно (`-eq`) Не равно (`-ne`) Больше (`-gt`) Больше или равно (`-ge`) Меньше (`-lt`) Меньше или равно (`-le`)	Число сообщений, возвращаемых в очередь передачи из-за временных ошибок, возникших при сопоставлении получателя. Дополнительные сведения об отложенных сообщениях см. в разделе Разрешение получателей в Exchange Server.
н/д	`DDeferredMessageCountsPerPriority`	Равно (`-eq`) Не равно (`-ne`) Содержит (`-like`)	Массив, который выводит количество отложенных сообщений в очереди по значению приоритета (важности). Свойство **MessageCountsPerPriority** указывает значение каждого числа. Например, значение `{1, 5, 10, 0}` указывает, что очередь содержит 1 отложенное сообщение с высоким приоритетом, 5 отложенных сообщений с обычным приоритетом, 10 отложенных сообщений с низким приоритетом и не содержит отложенных сообщений со значением приоритета None.
Тип доставки	`DeliveryType`	**Равно** (`-eq`) **Не равно** (`-ne`)	Результаты классификации сообщения и способ, которым служба транспорта собирается передать сообщение на следующий прыжок. Список доступных значений **DeliveryType** см. в разделе NextHopSolutionKey.

Средство просмотра очереди	Командная консоль Exchange	Операторы сравнения	Описание
н/д	`FirstRetryTime`	Равно (`-eq`) Не равно (`-ne`) Больше (`-gt`) Больше или равно (`-ge`) Меньше (`-lt`) Меньше или равно (`-le`)	Дата и время первой попытки подключения для очереди с состоянием `Retry`. Дополнительные сведения см. в статье Повторная отправка сообщений и интервалы истечения срока действия.
не применимо	`Identity`	н/д	Удостоверение очереди в виде *<очереди>\><сервера><*. Дополнительные сведения см. в разделе Идентификатор очереди.
н/д	`IncomingRate`	Равно (`-eq`) Не равно (`-ne`) Больше (`-gt`) Больше или равно (`-ge`) Меньше (`-lt`) Меньше или равно (`-le`)	Вычисляемое значение, определяющее, как быстро сообщения попадают в очередь. Дополнительные сведения см. в разделе Скорость входящих сообщений, скорость исходящих сообщений и общая скорость.
Последняя ошибка	`LastError`	**Равно** (`-eq`) **Не равно** (`-ne`) **Содержит** (`-contains`) **Присутствует** **Отсутствует**	Последняя ошибка, записанная для очереди. Дополнительные сведения о кодах ошибок SMTP см. в разделе DSN и NDR в Exchange Server.

Средство просмотра очереди	Командная консоль Exchange	Операторы сравнения	Описание
Время последнего повтора	`LastRetryTime`	**Больше** (`-gt`) **Больше или равно** (`-ge`) **Меньше** (`-lt`) **Меньше или равно** (`-le`) **Присутствует** **Отсутствует**	Дата и время последней попытки подключения для очереди с состоянием `Retry`. Дополнительные сведения см. в статье Повторная отправка сообщений и интервалы истечения срока действия.
не применимо	`LockedMessageCount`	не применимо	Это свойство зарезервировано для внутреннего использования Майкрософт и не применяется в локальных организациях Exchange.
Количество сообщений	`MessageCount`	**Равно** (`-eq`) **Не равно** (`-ne`) **Больше** (`-gt`) **Больше или равно** (`-ge`) **Меньше** (`-lt`) **Меньше или равно** (`-le`)	Количество сообщений в очереди.

Средство просмотра очереди	Командная консоль Exchange	Операторы сравнения	Описание
н/д	`MessageCountsPerPriority`	Равно (`-eq`) Не равно (`-ne`) Содержит (`-like`)	Массив, который выводит количество сообщений в очереди по значению приоритета (важности). Свойство **MessageCountsPerPriority** указывает значение каждого числа. Например, значение `{1, 100, 10, 0}` указывает, что очередь содержит 1 сообщение с высоким приоритетом, 100 сообщений с обычным приоритетом, 10 сообщений с низким приоритетом и нет сообщений с приоритетом None. Дополнительные сведения об организации очередей по приоритетам см. в статье Priority Queuing.
н/д	`NextHopCategory`	Равно (`-eq`) Не равно (`-ne`)	Значение `Internal` или `External` для следующего прыжка на основе значения свойства **DeliveryType** . Дополнительные сведения см. в разделе NextHopSolutionKey.
н/д	`NextHopConnector`	Равно (`-eq`) Не равно (`-ne`) Содержит (`-like`)	GUID следующего прыжка, зависящий от значения свойства **DeliveryType**. Дополнительные сведения см. в разделе NextHopSolutionKey.
Следующий домен для перехода	`NextHopDomain`	**Равно** (`-eq`) **Не равно** (`-ne`) **Содержит** (`-like`)	Имя следующего прыжка, зависящее от значения свойства **DeliveryType**. Дополнительные сведения см. в разделе NextHopSolutionKey.

Средство просмотра очереди	Командная консоль Exchange	Операторы сравнения	Описание
Время следующей попытки	`NextRetryTime`	**Больше** (`-gt`) **Больше или равно** (`-ge`) **Меньше** (`-lt`) **Меньше или равно** (`-le`) **Присутствует** **Отсутствует**	Дата и время следующей попытки подключения для очереди с состоянием `Retry`. Дополнительные сведения см. в статье Повторная отправка сообщений и интервалы истечения срока действия.
не применимо	`OutboundIPPool`	не применимо	Это свойство зарезервировано для внутреннего использования Майкрософт и не применяется в локальных организациях Exchange.
н/д	`OutgoingRate`	Равно (`-eq`) Не равно (`-ne`) Больше (`-gt`) Больше или равно (`-ge`) Меньше (`-lt`) Меньше или равно (`-le`)	Вычисляемое значение, определяющее, как быстро сообщения покидают очередь. Дополнительные сведения см. в разделе Скорость входящих сообщений, скорость исходящих сообщений и общая скорость.
не применимо	`OverrideSource`	не применимо	Это свойство зарезервировано для внутреннего использования Майкрософт и не применяется в локальных организациях Exchange.

Средство просмотра очереди	Командная консоль Exchange	Операторы сравнения	Описание
не применимо	`PriorityDescriptions`	не применимо	Описания значений свойств **DeferredMessageCountsPerPriority** и **MessageCountsPerPriority**. Это свойство имеет `{High, Normal, Low, None}` значение . Так как значение этого свойства никогда не меняется, оно плохо подходит для фильтрации.
н/д	`RetryCount`	Равно (`-eq`) Не равно (`-ne`) Больше (`-gt`) Больше или равно (`-ge`) Меньше (`-lt`) Меньше или равно (`-le`)	Число попыток подключения для очереди с состоянием `Retry`. Дополнительные сведения см. в статье Повторная отправка сообщений и интервалы истечения срока действия.
не применимо	`RiskLevel`	не применимо	Это свойство зарезервировано для внутреннего использования Майкрософт и не применяется в локальных организациях Exchange.
Состояние	`Status`	**Равно** (`eq`) **Не равно** (`-ne`)	Текущее состояние очереди. Это может быть одно из следующих значений: "Активно", "Установка связи", "Приостановлено", "Готово" или "Повторить". Дополнительные сведения см. в разделе Состояние очереди.
н/д	`TlsDomain`	Равно (`-eq`) Не равно (`-ne`) Содержит (`-like`)	Полное доменное имя целевого домена, если для него настроена функция безопасности домена (взаимная проверка подлинности TLS).

Средство просмотра очереди	Командная консоль Exchange	Операторы сравнения	Описание
н/д	`Velocity`	Равно (`-eq`) Не равно (`-ne`) Больше (`-gt`) Больше или равно (`-ge`) Меньше (`-lt`) Меньше или равно (`-le`)	Вычисляемое значение, показывающее эффективность опустошения очереди. Дополнительные сведения см. в разделе Скорость входящих сообщений, скорость исходящих сообщений и общая скорость.

Экспорт сообщений из очередей в Exchange Server

Статья • 04.04.2023

На серверах почтовых ящиков и пограничных транспортных серверах в Exchange Server можно экспортировать сообщения в очереди в файлы. Экспортированные сообщения не удаляются из очереди. Копии сообщений создаются в указанном расположении в виде файлов обычного текста. Файлы сообщений можно просмотреть в Блокноте или Outlook, а также повторно отправить файлы сообщений с помощью каталога Воспроизведения на любом другом сервере почтовых ящиков или пограничном транспортном сервере в организации Exchange или за ее пределами.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Очереди" в разделе Разрешения потока обработки почты .
- Чтобы экспортировать сообщения из очереди доставки, очереди отправки или очереди Недоступно, сообщения должны находиться в состоянии Приостановлено. Для активных и работоспособных очередей сначала нужно приостановить очередь, чтобы затем можно было приостановить сообщения. Сообщения в очереди сообщений о сбое уже находятся в состоянии приостановки. Дополнительные сведения см. в разделах Приостановка очередей и Приостановка сообщений в очередях.
- Экспортировать сообщения с помощью средства просмотра очередей на панели инструментов Exchange невозможно. Однако средство просмотра очередей можно использовать для поиска, идентификации и приостановки сообщений перед их экспортом с помощью командной консоли Exchange. Дополнительные сведения о средстве просмотра очереди см. в статье Queue Viewer. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- При экспорте сообщений из очереди они не удаляются. При повторной отправке экспортированных сообщений с помощью каталога

Воспроизведения следует удалить сообщения из очереди, чтобы избежать дублирования доставки сообщений. Дополнительные сведения см. в разделе Удаление сообщений из очередей.

- Проверьте следующие сведения о целевом расположении экспортированных файлов сообщений:
  - Целевая папка должна существовать перед экспортом сообщений и не будет создана для вас. Если не указать полный путь, файлы записываются в текущий рабочий каталог командной консоли Exchange.
  - Путь может быть локальным для сервера Exchange Server или UNC-путем к общей папке на удаленном сервере (\server\share).
  - Ваша учетная запись должна иметь разрешение **на запись** в целевой папке.

- Мы используем значение свойства **InternetMessageID** сообщения для экспортированных имен файлов сообщений, чтобы обеспечить уникальность. Процедуры включают шаги по удалению угловых скобок (> и <), так как они не разрешены в именах файлов. Кроме того, мы используем расширение EML-файла, чтобы можно было легко открыть файлы в Outlook или повторно отправить их с помощью каталога Воспроизведения.

- Дополнительные сведения об удостоверениях и фильтрах для очередей и сообщений в очередях см. в следующих разделах:
  - Поиск очередей и сообщений в очередях в командной консоли Exchange
  - Свойства очереди
  - Свойства сообщений в очередях

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Экспорт определенного сообщения из очереди с помощью командной консоли Exchange

Чтобы экспортировать определенное сообщение из очереди, используйте следующий синтаксис:

```
PowerShell

Export-Message -Identity <MessageIdentity> | AssembleMessage -Path
<FilePath>\<FileName>.eml
```

В этом примере выполняются следующие действия на сервере с именем Mailbox01:

1. Приостанавливает очередь доставки contoso.com.
2. Приостанавливает сообщение в очереди со значением **InternalMessageID** 1234.
3. Экспортирует копию сообщения в файл D:\contoso Export\export.eml.

```
PowerShell

Suspend-Queue Mailbox01\contoso.com
```

```
PowerShell

Suspend-Message -Identity Mailbox01\contoso.com\1234
```

```
PowerShell

Export-Message -Identity Mailbox01\contoso.com\1234 | AssembleMessage -Path
"D:\Contoso Export\export.eml"
```

Экспорт всех сообщений из очереди с помощью командной консоли Exchange

Чтобы экспортировать все сообщения из очереди и использовать значение **InternetMessageID** каждого сообщения в качестве имени файла, используйте следующий синтаксис:

```
PowerShell

Get-Message -Queue <QueueIdentity> -ResultSize Unlimited | ForEach-Object
{$Temp=<Path>+$_.InternetMessageID+".eml"; $Temp=$Temp.Replace("<","_");
$Temp=$Temp.Replace(">","_"); Export-Message $_.Identity | AssembleMessage -
Path $Temp}
```

В этом примере выполняются следующие действия на сервере с именем Mailbox01:

1. Приостанавливает очередь доставки contoso.com.
2. Приостанавливает все сообщения в очереди.
3. Экспортирует копии сообщений в локальную папку D:\Contoso Export.

PowerShell

```
Suspend-Queue Mailbox01\contoso.com
```

PowerShell

```
Get-Queue Mailbox01\contoso.com | Get-Message -ResultSize Unlimited |
Suspend-Message
```

PowerShell

```
Get-Message -Queue Mailbox01\Contoso.com -ResultSize Unlimited | ForEach-
Object {$Temp="D:\Contoso Export\"+$_.InternetMessageID+".eml";
$Temp=$Temp.Replace("<","_"); $Temp=$Temp.Replace(">","_"); Export-Message
$_.Identity | AssembleMessage -Path $Temp}
```

Экспорт определенных сообщений из всех очередей на сервере с помощью командной консоли Exchange

Чтобы экспортировать определенные сообщения из всех очередей на сервере и использовать значение **InternetMessageID** каждого сообщения в качестве имени файла, используйте следующий синтаксис:

PowerShell

```
Get-Message -Filter "<MessageFilter>" [-Server <ServerIdentity>] -ResultSize
Unlimited | ForEach-Object {$Temp=<Path>+$_.InternetMessageID+".eml";
$Temp=$Temp.Replace("<","_"); $Temp=$Temp.Replace(">","_"); Export-Message
$_.Identity | AssembleMessage -Path $Temp}
```

В этом примере выполняются следующие действия на сервере с именем Mailbox01:

1. Приостанавливает все очереди на сервере.
2. Приостанавливает все сообщения во всех очередях на сервере от отправителей в домене fabrikam.com.

3. Экспортирует копии сообщений в локальную папку С именем D:\Fabrikam Export.

```
PowerShell

Suspend-Queue -Server Mailbox01
```

```
PowerShell

Suspend-Message -Filter "FromAddress -like '*@fabrikam.com'" -Server Mailbox01
```

```
PowerShell

Get-Message -Filter "FromAddress -like '*@fabrikam.com'" -Server Mailbox01 -ResultSize Unlimited | ForEach-Object {$Temp="D:\Fabrikam Export\"+$_.InternetMessageID+".eml"; $Temp=$Temp.Replace("<","_"); $Temp=$Temp.Replace(">","_"); Export-Message $_.Identity | AssembleMessage -Path $Temp}
```

Экспорт всех сообщений из всех очередей на сервере с помощью командной консоли Exchange

Чтобы экспортировать все сообщения из всех очередей на сервере и использовать значение **InternetMessageID** каждого сообщения в качестве имени файла, используйте следующий синтаксис:

```
PowerShell

Get-Message [-Server <ServerIdentity>] -ResultSize Unlimited | ForEach-Object {$Temp=<Path>+$_.InternetMessageID+".eml"; $Temp=$Temp.Replace("<","_"); $Temp=$Temp.Replace(">","_"); Export-Message $_.Identity | AssembleMessage -Path $Temp}
```

В этом примере выполняются следующие действия на сервере с именем Mailbox01:

1. Приостанавливает все очереди на сервере.
2. Приостанавливает все сообщения во всех очередях на сервере.
3. Экспортирует копии сообщений в локальную папку С именем D:\Mailbox01 Export.

PowerShell

```
Suspend-Queue -Server Mailbox01
```

PowerShell

```
Get-Queue -Server Mailbox01 | Get-Message -ResultSize Unlimited | Suspend-
Message
```

PowerShell

```
Get-Message -Server Mailbox01 -ResultSize Unlimited | ForEach-Object
{$Temp="D:\Mailbox01 Export\"+$_.InternetMessageID+".eml";
$Temp=$Temp.Replace("<","_"); $Temp=$Temp.Replace(">","_"); Export-Message
$_.Identity | AssembleMessage -Path $Temp}
```

Инструкции по работе с сообщениями в очередях

Статья • 04.04.2023

В Exchange Server для управления сообщениями в очередях можно использовать средство просмотра очередей на панели элементов Exchange или командную консоль Exchange. Дополнительные сведения о сообщениях в очередях см. в разделе Свойства сообщения.

В этой статье рассказывается, как выполнять перечисленные ниже задачи с сообщениями в очередях.

- **Удаление сообщений**. Вы можете удалить сообщения из очередей с помощью нашего без отчета о недоставке отправителю (также известного как недоставка, уведомление о состоянии доставки, DSN или сообщение о отказе).
- **Приостановка сообщений**. При приостановке сообщения запрещается доставка сообщения. Оно не покинет очередь, пока доставка не будет возобновлена.
- **Возобновление сообщений**. Вы можете возобновить сообщение, которое в настоящее время имеет состояние Приостановлено. При этом включается доставка сообщения.
- **Перенаправление сообщений**. Вы можете сливать сообщения из всех очередей доставки на сервере почтовых ящиков и передавать эти сообщения на другой сервер почтовых ящиков.

Сведения об экспорте сообщений из очередей см. в статье Экспорт сообщений из очередей.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут
- Чтобы найти и открыть Элементы управления Exchange, воспользуйтесь одной из указанных ниже процедур.
  - **Windows 10**. Щелкните **Запустить**>**все приложения**> Microsoft Exchange Server **<панель элементов Exchange version>>**.
  - **Windows Server 2012 R2 или Windows 8.1**. На начальном экране откройте представление Приложения, щелкнув стрелку вниз в левом нижнем углу или проведя пальцем вверх по центру экрана. Ярлык **панели элементов**

Exchange находится в группе с именем **Microsoft Exchange Server <version>**.

- **Windows Server 2012**. Используйте любой из следующих методов:
  - На начальном экране щелкните пустую область и введите Панель элементов Exchange.
  - Откройте рабочий стол или начальный экран и нажмите клавиши Windows+Q. На панели чудо-кнопки "Поиск" введите Панель элементов Exchange.
  - Откройте рабочий стол и переместите курсор в его правый верхний угол (или на начальном экране проведите пальцем влево от его правого края), чтобы отобразились чудо-кнопки. Нажмите чудо-кнопку "Поиск" и введите Панель элементов Exchange.

  Когда ярлык появится в результатах, выберите его.

- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Дополнительные сведения об использовании фильтров и значений удостоверений в командной консоли Exchange см. в статье Поиск очередей и сообщений в очередях в командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Очереди" в разделе Разрешения потока обработки почты .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Удаление сообщений из очередей

Примечание.

Сообщение, отправляемое нескольким получателям, может находиться в нескольких очередях. Чтобы удалить сообщение из нескольких очередей с

помощью одной операции, следует использовать фильтр. Дополнительные сведения см. в разделах Свойства сообщений в очередях и Параметры фильтрации сообщений.

Удаление сообщений из очередей с помощью средства просмотра очереди

1. Откройте **Элементы управления Exchange** и в разделе **Средства для потока почты** дважды щелкните **Средство просмотра очереди**, чтобы открыть его в новом окне.

2. В средстве просмотра очередей перейдите на вкладку **Сообщения** . Отобразится список всех сообщений на сервере, к которому вы подключены. Чтобы выполнить действие с отдельной очередью, откройте вкладку **Очереди**, дважды щелкните имя очереди, а затем откройте вкладку *Server\Queue*.

3. Выделите одно или несколько сообщений в списке, щелкните правой кнопкой мыши и выберите команду **Удалить сообщения (с отправкой отчета о недоставке)** или **Удалить сообщения (без отчета о недоставке)**. Откроется диалоговое окно для подтверждения выбранного действия с запросом **Продолжить?** Нажмите кнопку **Да**.

4. Чтобы удалить все сообщения из определенной очереди, перейдите на вкладку **Очереди**. Выберите очередь, щелкните правой кнопкой мыши и выберите **Удалить сообщения (с NDR)** или **Удалить сообщения (без NDR).** Откроется диалоговое окно для подтверждения выбранного действия с запросом **Продолжить?** Нажмите кнопку **Да**.

   > ⓘ **Примечание**
   >
   > При работе с отфильтрованным списком отображаемая страница может содержать не все элементы в фильтре. В этом случае появится запрос: **Это действие повлияет на все элементы этой страницы. Чтобы расширить область применения этого действия для включения всех элементов в этом фильтре, установите следующий флажок до нажатия кнопки «OK».**

Удаление сообщений с помощью командной консоли Exchange

Чтобы удалить сообщения из очередей, введите команду в следующем формате.

```
PowerShell

Remove-Message <-Identity MessageIdentity | -Filter "MessageFilter"> -
WithNDR <$true | $false>
```

В этом примере из очереди удаляются сообщения с темой "Win Big" без отправки отчета о недоставке.

```
PowerShell

Remove-Message -Filter "Subject -eq 'Win Big'" -WithNDR $false
```

В этом примере из очереди "Сообщения с недостижимым местом назначения" на сервере с именем Mailbox01 удаляются сообщения с идентификатором 3. При этом отправляется отчет о недоставке.

```
PowerShell

Remove-Message -Identity Mailbox01\Unreachable\3 -WithNDR $true
```

Дополнительные сведения см. в статье Remove-Message.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли удалены сообщения из очередей, выполните одно из указанных ниже действий.

- В средстве просмотра очереди выберите очередь или создайте фильтр, чтобы убедиться, что сообщение больше не существует.
- В командной оболочке Exchange *замените MessageFilter* фильтром, который вы использовали, или <*QueueIdentity*> идентификатором очереди и выполните следующую команду, чтобы убедиться, что сообщения больше не существуют:

  ```
  PowerShell

  Get-Message -Filter "MessageFilter"
  ```

  или

  ```
  ```

PowerShell

```
Get-Message -Queue <QueueIdentity>
```

Дополнительные сведения см. в статье Get-Message.

Приостановка доставки сообщений в очередях

Примечания.

- Сообщение, отправляемое нескольким получателям, может находиться в нескольких очередях. Чтобы приостановить доставку сообщения в нескольких очередях с помощью одной операции, необходимо применить фильтр. Дополнительные сведения см. в разделах Свойства сообщений в очередях и Параметры фильтрации сообщений.
- Если приостановить доставку сообщения во время его передачи на следующий узел, то доставка сообщения продолжится, а его состояние станет **PendingSuspend**. Если доставка не удастся, сообщение заново поступит в очередь, а затем его доставка будет приостановлена.

Приостановка доставки сообщений с помощью средства просмотра очереди

1. Откройте **Элементы управления Exchange** и в разделе **Средства для потока почты** дважды щелкните **Средство просмотра очереди**, чтобы открыть его в новом окне.
2. В средстве просмотра очередей перейдите на вкладку **Сообщения** . Отобразится список всех сообщений на сервере, к которому вы подключены. Чтобы отображалась только отдельная очередь, откройте вкладку **Очереди**, дважды щелкните имя очереди, а затем откройте вкладку *Server\Queue*.
3. Выберите одно или несколько сообщений, щелкните правой кнопкой мыши и выберите команду **Приостановить**.

Приостановка доставки сообщений с помощью командной консоли Exchange

Чтобы приостановить доставку сообщений, используйте следующий синтаксис:

PowerShell

```
Suspend-Message <-Identity MessageIdentity | -Filter "MessageFilter">
```

В этом примере приостанавливается доставка сообщения с идентификатором 3 в очереди "Сообщения с недостижимым местом назначения" на сервере с именем Mailbox01.

PowerShell

```
Suspend-Message -Identity Mailbox01\Unreachable\3
```

В этом примере приостанавливается доставка всех сообщений во всех очередях на локальном сервере, отправленных с домена contoso.com.

PowerShell

```
Suspend-Message -Filter "FromAddress -like '*contoso.com'"
```

В этом примере приостанавливается доставка всех сообщений в очереди доставки для домена contoso.com на сервере Mailbox01.

PowerShell

```
Get-Queue Mailbox01\contoso.com | Get-Message | Suspend-Message
```

В этом примере приостанавливается доставка всех сообщений во всех очередях на локальном сервере.

PowerShell

```
Get-Queue | Get-Message | Suspend-Message
```

Дополнительные сведения см. в статье Suspend-Message.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли приостановлена доставка сообщений в очередях, выполните одно из указанных ниже действий.

- В средстве просмотра очереди выберите очередь или создайте фильтр, чтобы убедиться, что сообщения приостановлены.

- В командной консоли Exchange замените *MessageFilter* используемым фильтром или <*QueueIdentity*> идентификатором очереди и выполните следующие команды, чтобы убедиться, что сообщения приостановлены:

  PowerShell

  ```
  Get-Message -Filter "MessageFilter"
  ```

  или

  PowerShell

  ```
  Get-Message -Queue <QueueIdentity>
  ```

  Дополнительные сведения см. в статье Get-Message.

Возобновление доставки сообщений в очередях

Примечания.

- Возобновлять доставку можно только для сообщений с состоянием "Приостановлено".
- Состояние очереди, в которой находятся сообщения, влияет на их доставку. Например, если возобновить приостановленную доставку сообщений в очереди с состоянием "Приостановлено", то сообщения не будут доставлены, пока не будет возобновлена работа очереди. Дополнительные сведения о возобновлении работы очередей см. в разделе Возобновление работы очередей.

Возобновление доставки сообщений с помощью средства просмотра очереди

1. Откройте **Элементы управления Exchange** и в разделе **Средства для потока почты** дважды щелкните **Средство просмотра очереди**, чтобы открыть его в новом окне.

2. В средстве просмотра очередей перейдите на вкладку **Сообщения** . Отобразится список всех сообщений на сервере, к которому вы подключены. Чтобы выполнить действие с отдельной очередью, откройте вкладку

Очереди, дважды щелкните имя очереди, а затем откройте вкладку *Server\Queue*.

3. Щелкните **Создать фильтр** и введите выражение фильтра следующим образом:
   a. Выберите **Состояние** в раскрывающемся списке свойств сообщения.
   b. Выберите пункт **Равно** из раскрывающегося списка операторов сравнения.
   c. Выберите **Приостановлено** в раскрывающемся списке значений.
4. Нажмите кнопку **Применить фильтр**. Отобразятся все сообщения, имеющие состояние «Приостановлено».
5. Выделите одно или несколько сообщений в списке, щелкните правой кнопкой мыши и выберите команду **Возобновить**.

Возобновление доставки сообщений с помощью командной консоли Exchange

Чтобы возобновить доставку сообщений, используйте следующий синтаксис:

```
PowerShell

Resume-Message <-Identity MessageIdentity | -Filter "MessageFilter">
```

В этом примере возобновляется передача всех сообщений от всех отправителей в домене contoso.com.

```
PowerShell

Resume-Message -Filter "FromAddress -like '*contoso.com'"
```

В этом примере возобновляется доставка сообщения с идентификатором 3 в очереди "Сообщения с недостижимым местом назначения" на сервере с именем Mailbox01.

```
PowerShell

Resume-Message -Identity Mailbox01\Unreachable\3
```

Как убедиться в том, что все получилось?

Чтобы проверить, успешно ли возобновлена доставка сообщений в очередях, выполните одно из указанных ниже действий.

- В средстве просмотра очереди выберите очередь или создайте фильтр, чтобы убедиться, что сообщения больше не находятся в приостановленном состоянии.

- В командной консоли Exchange замените *MessageFilter* фильтром, который вы использовали, или *<QueueIdentity>* идентификатором очереди и выполните следующую команду, чтобы убедиться, что сообщения больше не приостановлены:

  PowerShell

  ```
  Get-Message -Filter "MessageFilter"
  ```

  или

  PowerShell

  ```
  Get-Message -Queue <QueueIdentity>
  ```

  Дополнительные сведения см. в статье Get-Message.

Если сообщения нет ни в одной из очередей на сервере, скорее всего, оно было доставлено на следующий узел.

Перенаправление сообщений в очередях

При перенаправлении сообщений все активные сообщения очередей доставки удаляются на исходном сервере почтовых ящиков и направляются на целевой сервер почтовых ящиков. Сообщения добавляются в очередь доставки и направляются на следующий узел.

Примечания.

- Перенаправляются только активные сообщения.
- Теневые очереди и сообщения из очереди подозрительных сообщений не перенаправляются.
- Во время перенаправления исходный сервер почтовых ящиков не принимает новые сообщения.
- Перенаправлять сообщения можно только с помощью командной консоли Exchange.

Перенаправление сообщений с помощью командной консоли Exchange

Чтобы перенаправлять сообщения, используйте следующий синтаксис:

```
PowerShell

Redirect-Message -Server <ServerIdentity> -Target <ServerFQDN>
```

В этом примере сообщения из всех очередей доставки на сервере с именем Mailbox01 перенаправляются на сервер Mailbox02.contoso.com.

```
PowerShell

Redirect-Message -Server Mailbox01 -Target Mailbox02.contoso.com
```

Дополнительные сведения см. в статье Redirect-Message.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли перенаправлены сообщения в очередях, выполните одно из указанных ниже действий.

- В средстве просмотра очереди убедитесь, что значение **Количество сообщений** в очередях доставки на исходном сервере отсутствует или уменьшается.
- В командной консоли Exchange выполните приведенную ниже команду, чтобы убедиться, что значение свойства **MessageCount** для очередей доставки на исходном сервере уменьшается или отсутствует.

  ```
  PowerShell

  Get-Queue
  ```

Свойства сообщений в очередях

Статья • 04.04.2023

Фильтрация сообщений в очередях по одному или нескольким свойствам сообщений в Exchange Server позволяет быстро находить сообщения и выполнять с ними действия. При отправке сообщения электронной почты нескольким получателям сообщение может находиться в нескольких очередях на сервере. При фильтрации сообщений в очередях по свойствам сообщений можно находить сообщения во всех очередях. Следующие сценарии служат примерами использования фильтрации сообщений для управления потоком почты:

- Очередь отправки на сервере почтовых ящиков или пограничном транспортном сервере, которая получает электронную почту из Интернета, содержит большой объем сообщений, которые находятся в очереди на доставку. Многие сообщения имеют одинаковую тему. Поэтому возникает подозрение, что в организацию посылается нежелательная почта. Можно создать фильтр, чтобы просмотреть все сообщения, которые соответствуют условию отбора по теме. Если будет определено, что сообщения являются нежелательной почтой, их все можно выбрать и удалить из очередей без отправки отчета о недоставке.
- Пользователь сообщает о низкой скорости потока почты. Вы просматриваете очереди и видите, что многие сообщения со случайными субъектами, как представляется, поступают из одного домена. Можно создать фильтр, чтобы просмотреть все сообщения в очереди из этого домена. Если будет определено, что сообщения являются нежелательной почтой, их все можно выбрать и удалить из очередей без отправки отчета о недоставке.

Фильтры сообщений можно создать в средстве просмотра очередей на панели элементов Exchange или с помощью параметра *Filter* в командлетах управления сообщениями. Обратите внимание, что командлеты управления сообщениями поддерживают больше фильтруемых свойств, чем средство просмотра очередей.

Дополнительные сведения о средстве просмотра очереди см. в статье Queue Viewer. Дополнительные сведения о командлетах управления сообщениями см. в разделах Процедуры для сообщений в очередях и Поиск очередей и сообщений в очередях в командной консоли Exchange.

Свойства сообщения для использования в качестве фильтров

В следующей таблице описаны свойства сообщения, которые можно использовать в качестве фильтров в средстве просмотра очередей и командной консоли Exchange.

Средство просмотра очереди	Командная консоль Exchange	Операторы сравнения	Описание
н/д	`AccountForest`	н/д	его свойство зарезервировано для внутреннего использования Майкрософт и не используется в локальных организациях Exchange. В локальной среде Exchange это свойство является корневым доменом леса, где находится почтовый ящик (например, contoso.com).

Средство просмотра очереди	Командная консоль Exchange	Операторы сравнения	Описание
н/д	`ComponentLatency`	не применимо	Это свойство зарезервировано для внутреннего использования Майкрософт и не применяется в локальных организациях Exchange.
Дата получения	`DateReceived`	**Больше** (`-gt`) **Больше или равно** (`-ge`) **Меньше** (`-lt`) **Меньше или равно** (`-le`)	Дата и время размещения сообщения в очереди.

н/д	`DeferReason`	Равно (`-eq`)
		
		Не равно (`-ne`)
		
		Содержит (`-like`)
			Указывает, почему сообщение было отложено. Если сообщение не было отложено, это свойство имеет значение `None`. Отложенное сообщение возвращается в очередь отправки из-за временных ошибок, обнаруженных при разрешении получателя. Дополнительные сведения об отложенных сообщениях см. в разделе Разрешение получателей в Exchange Server. Возможные значения:
			
			`AD Transient Failure During Content Conversion`)
			
			`AD Transient Failure During Resolve`
			
			`Agent`
			
			`Ambiguous Recipient`
			
			`Config Update`
			
			`Loop Detected`
			
			`Marked As Retry Delivery If Rejected`
			
			`Recipient does not have a mailbox database`
			
			`Recipient Thread Limit Exceeded`
			
			`Rerouted By Store Driver`
			
			`Storage Transient Failure During Content Conversion`
			
			`Target Site Inbound Mail Disabled`
			
			`Transient Accepted Domains Load Failure`
			
			`Transient Attribution Failure`
			
			`Transient Failure`

н/д	`Directionality`	Равно (`-eq`) Не равно (`-ne`)	Допустимыми являются значения `Incoming`, `Originating` и `Undefined`.

Средство просмотра очереди	Командная консоль Exchange	Операторы сравнения	Описание
Срок действия	`ExpirationTime`	**Больше** (`-gt`) **Больше или равно** (`-ge`) **Меньше** (`-lt`) **Меньше или равно** (`-le`)	Дата и время истечения срока действия сообщения и его удаление из очереди, если сообщение не может быть доставлено.
н/д	`ExternalDirectoryOrganizationId`	не применимо	Это свойство зарезервировано для внутреннего использования Майкрософт и не применяется в локальных организациях Exchange. В локальной среде Exchange значение равно `00000000-0000-0000-0000-000000000000`.
С адреса	`FromAddress`	**Равно** (`-eq`) **Не равно** (`-ne`) **Содержит** (`-contains`)	SMTP-адрес отправителя.
н/д	`Identity`	н/д	Удостоверение сообщения в формате *<Server>**<Queue>**<MessageInteger>*. Дополнительные сведения см. в разделе Идентификатор сообщения.
Идентификатор сообщения Интернета	`InternetMessageId`	**Равно** (`-eq`) **Не равно** (`-ne`) **Содержит** (`-contains`)	Значение поля заголовка **Message-Id:** в заголовке сообщения. Это значение не изменяется на протяжении всего времени жизни сообщения. Для сообщений, созданных в Exchange, значение имеет формат `<GUID@ServerFQDN>`, включая угловые скобки (<>). Например, `<4867a3d78a50438bad95c0f6d072fca5@mailbox01.contoso.com>`.
Последняя ошибка	`LastError`	**Равно** (`-eq`) **Не равно** (`-ne`) **Содержит** (`-contains`) **Присутствует** **Отсутствует**	Последняя ошибка, записанная для сообщения. Например, `A matching connector cannot be found to route the external recipient`.
н/д	`LockReason`	не применимо	Это свойство зарезервировано для внутреннего использования Майкрософт и не применяется в локальных организациях Exchange.

Средство просмотра очереди	Командная консоль Exchange	Операторы сравнения	Описание
н/д	`MessageLatency`	Равно (`-eq`) Не равно (`-ne`) Больше (`-gt`) Больше или равно (`-ge`) Меньше (`-lt`) Меньше или равно (`-le`	Время, затраченное между тем, когда сообщение впервые поступило в очередь отправки на сервере, и когда сообщение было помещено в очередь. Значение использует синтаксис *hh:mm:ss.ff*, где *hh* = час, *mm* = минута, *ss* = секунда, и *ff* = доли секунды.
Имя источника сообщения	`MessageSourceName`	**Равно** (`-eq`) **Не равно** (`-ne`) **Содержит** (`-contains`)	Имя транспортного компонента, отправившего сообщение в очередь. Например, если сообщение поступило через соединитель получения, значение будет: `SMTP:`<*ConnectorName*>. Если сообщение является уведомлением о состоянии доставки (DSN), значение равно `DSN`.
н/д	`OriginalFromAddress`	Равно (`-eq`) Не равно (`-ne`) Содержит (`-like`)	Адрес электронной почты исходного отправителя для любых новых сообщений о побочных эффектах, созданных во время классификации (например, правила журнала, NDR или правила потока обработки почты, также известные как правила транспорта).
н/д	`Priority`	Равно (`-eq`) Не равно (`-ne`)	Приоритет (важность) сообщения, назначенного пользователем в Microsoft Outlook или Outlook в Интернете. Допустимыми являются значения `Low`, `Normal` и `High`. Подробнее см. в разделе Priority Queuing.
Идентификатор очереди	`Queue`	**Равно** (`-eq`) **Не равно** (`-ne`) **Содержит** (`-contains`)	Очередь, в которой находится сообщение. Удостоверение очереди использует синтаксис <*Server*>\<*Queue*>. Дополнительные сведения см. в разделе Удостоверение очереди.
н/д	`Recipients`	Содержит (`-like`)	Массив, содержащий сведения о получателе и соединителе отправки, который будет использоваться, или все возникшие ошибки. Например: `{chris@contoso.com;2;2;A matching connector cannot be found to route the external recipient;16;<No Matching Connector>;0}`

Средство просмотра очереди	Командная консоль Exchange	Операторы сравнения	Описание
н/д	`RetryCount`	Равно (`-eq`) Не равно (`-ne`) Больше (`-gt`) Больше или равно (`-ge`) Меньше (`-lt`) Меньше или равно (`-le`	Количество попыток доставки сообщения в место назначения автоматически или вручную.
Вероятность нежелательной почты	`SCL`	**Равно** (`-eq`) **Не равно** (`-ne`) **Больше** (`-gt`) **Больше или равно** (`-ge`) **Меньше** (`-lt`) **Меньше или равно** (`-le`	Оценка вероятности нежелательной почты сообщения. Допустимые значения представляют собой целые числа от 0 до 9, а также –1 для внутренних (прошедших проверку подлинности) сообщений. Дополнительные сведения см. в статье Пороговые значения уровня достоверности нежелательной почты Exchange (SCL).
Размер (КБ)	`Size`	**Равно** (`-eq`) **Не равно** (`-ne`) **Больше** (`-gt`) **Больше или равно** (`-ge`) **Меньше** (`-lt`) **Меньше или равно** (`-le`	Размер сообщения. В средстве просмотра очередей необходимо указать размер сообщения в килобайтах (КБ), но в командной консоли Exchange можно также указать другие размеры, например байты (B) или мегабайты (МБ).
IP-адрес источника	`SourceIP`	**Равно** (`-eq`) **Не равно** (`-ne`)	IPv4- или IPv6-адрес сервера, отправившего сообщение на сервер Exchange Server, который содержит сообщение в очереди. Это может быть IP-адрес удаленного SMTP-сервера или локального сервера Exchange.

Средство просмотра очереди	Командная консоль Exchange	Операторы сравнения	Описание
Состояние	`Status`	**Равно** (`-eq`) **Не равно** (`-ne`)	Текущее состояние сообщения. Допустимые значения: **Active** **Locked** **Ожидание удаления** (`PendingRemove`) **Ожидание приостановки** (`PendingSuspend`) **Ready** **Повторить** **Suspended** Дополнительные сведения см. в разделе Состояние сообщения.
Тема	`Subject`	**Равно** (`-eq`) **Не равно** (`-ne`) **Содержит** (`-contains`) **Присутствует** **Отсутствует**	Тема сообщения (из поля заголовка **Subject:**).
н/д	`TrafficType`	не применимо	Это свойство зарезервировано для внутреннего использования Майкрософт и не применяется в локальных организациях Exchange. В локальной среде Exchange это свойство пустое или имеет значение `Email`.
н/д	`TrafficSubType`	не применимо	Это свойство зарезервировано для внутреннего использования Майкрософт и не применяется в локальных организациях Exchange.

Exchange Server: средство просмотра очередей

Статья • 04.04.2023

Средство просмотра очередей является частью панели элементов Exchange, установленной на серверах почтовых ящиков и пограничных транспортных серверах в Exchange Server 2016 и Exchange Server 2019. Средство просмотра очередей — это оснастка консоли управления (MMC), которую можно использовать для просмотра сведений о очередях и сообщений в очередях и выполнения действий. Средство просмотра очередей помогает устранить неполадки в потоке обработки почты и определить спам.

Средство просмотра очередей находится в разделе **Средства потока обработки почты** панели элементов Exchange.

Чтобы найти и открыть Элементы управления Exchange, воспользуйтесь одной из указанных ниже процедур.

- **Windows 10**. Щелкните **Запустить**>**все приложения**> Microsoft Exchange Server **<панель элементов Exchange version>>**.
- **Windows Server 2012 R2 или Windows 8.1**. На начальном экране откройте представление Приложения, щелкнув стрелку вниз в левом нижнем углу или проведя пальцем вверх по центру экрана. Ярлык **панели элементов Exchange** находится в группе с именем **Microsoft Exchange Server <version>**.
- **Windows Server 2012**. Используйте любой из следующих методов:
    - На начальном экране щелкните пустую область и введите Панель элементов Exchange.
    - Откройте рабочий стол или начальный экран и нажмите клавиши Windows+Q. На панели чудо-кнопки "Поиск" введите Панель элементов Exchange.
    - Откройте рабочий стол и переместите курсор в его правый верхний угол (или на начальном экране проведите пальцем влево от его правого края), чтобы отобразились чудо-кнопки. Нажмите чудо-кнопку "Поиск" и введите Панель элементов Exchange.

    Когда ярлык появится в результатах, выберите его.

Дополнительные сведения об очередях и сообщениях в очередях см. в разделе Очереди и сообщения в очередях.

Статьи, в которых описаны процедуры, касающиеся средства просмотра очередей

В статьях, указанных в приведенной ниже таблице, описаны процедуры, касающиеся средства просмотра очередей.

Статья	Описание
Подключение к серверу в средстве просмотра очередей	По умолчанию средство просмотра очередей открывает базу данных очереди на том сервере, где запущено само средство. Но подключиться можно и к другому серверу.
Настройка параметров средства просмотра очередей	Вы можете настроить интервалы обновления для очередей и сообщений, а также количество элементов, отображаемых на каждой странице.
Просмотр свойств сообщения в очереди в средстве просмотра очереди	Объясняет, как использовать средство просмотра очередей для просмотра сообщений, а также рассматривает свойства сообщений.
Экспорт списков из средства просмотра очередей	Чтобы устранить неполадки или провести диагностику, можно использовать ссылку **Экспортировать список** на панели операций для экспорта списка очередей или сообщений.
Свойства очереди	Описывает свойства очередей и указывает свойства, доступные в средстве просмотра очередей и командной консоли Exchange.
Свойства сообщений в очередях	Описывает свойства сообщений и указывает свойства, доступные в средстве просмотра очередей и командной консоли Exchange.
Действия по работе с очередями	Объясняет, как выполнять просмотр, повторять попытку подключения или доставки, приостанавливать и возобновлять отправку сообщений для очереди в целом.
Инструкции по работе с сообщениями в очередях	Объясняет, как удалять или перенаправлять сообщения в очередях, а также приостанавливать и возобновлять доставку отдельных таких сообщений.

Exchange Server: просмотр свойств сообщений в очереди в средстве просмотра очередей

Статья • 04.04.2023

Для просмотра самих очередей, а также свойств сообщений в них можно использовать средство просмотра очередей на панели элементов Exchange. В Exchange Server 2016 г. и Exchange Server 2019 г. средство просмотра очередей доступно на серверах почтовых ящиков и пограничных транспортных серверах.

Дополнительные сведения см. в разделе Queues and messages in queues. Дополнительные сведения о средстве просмотра очередей см. в статье Queue Viewer.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Очереди" в разделе Разрешения потока обработки почты .
- Чтобы найти и открыть Элементы управления Exchange, воспользуйтесь одной из указанных ниже процедур.
  - **Windows 10**. Щелкните **Запустить**>**все приложения**> Microsoft Exchange Server **<панель элементов Exchange version>**>.
  - **Windows Server 2012 R2 или Windows 8.1**. На начальном экране откройте представление Приложения, щелкнув стрелку вниз в левом нижнем углу или проведя пальцем вверх по центру экрана. Ярлык **панели элементов Exchange** находится в группе с именем **Microsoft Exchange Server <version>**.
  - **Windows Server 2012**. Используйте любой из следующих методов:
    - На начальном экране щелкните пустую область и введите Панель элементов Exchange.
    - Откройте рабочий стол или начальный экран и нажмите клавиши Windows+Q. На панели чудо-кнопки "Поиск" введите Панель элементов Exchange.

- Откройте рабочий стол и переместите курсор в его правый верхний угол (или на начальном экране проведите пальцем влево от его правого края), чтобы отобразились чудо-кнопки. Нажмите чудо-кнопку "Поиск" и введите Панель элементов Exchange.

  Когда ярлык появится в результатах, выберите его.

- Командлет **Get-Message** также можно использовать в командной консоли Exchange для просмотра дополнительных свойств сообщений, которые не отображаются в средстве просмотра очередей. Дополнительные сведения см. в разделах Свойства сообщений в очередях и Поиск очередей и сообщений в очередях в командной консоли Exchange.

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Просмотр свойств сообщения с помощью средства просмотра очередей

1. In the **Exchange Toolbox**, in the **Mail flow tools** section, double-click **Queue Viewer** to open the tool in a new window.

2. В средстве просмотра очередей откройте вкладку **Сообщения** для просмотра списка сообщений в организации, находящихся в очереди на доставку. В этом списке показаны следующие сведения:

   - **Из адреса**: адрес электронной почты отправителя.

   - **Состояние**. Сообщение может иметь одно из следующих значений состояния:

   - **Активно**. Если сообщение находится в очереди доставки, оно доставляется в место назначения. Если же сообщение находится в очереди передачи, его обрабатывает классификатор.

- **Ожидание удаления**. Сообщение было удалено администратором, но уже доставлено. Сообщение будет удалено, если доставка завершится ошибкой, вызывающей повторное добавление сообщения в очередь. В противном случае доставка будет продолжена.

- **Ожидание приостановки**. Сообщение было приостановлено администратором, но уже доставлено. Обработка сообщения будет приостановлена, если доставка завершится ошибкой, вызывающей повторное добавление сообщения в очередь. В противном случае доставка будет продолжена.

- **Готово**. Сообщение ожидается в очереди и готово к обработке.

- **Повторная попытка**: последняя попытка подключения очереди завершилась сбоем. Сообщение ожидает следующей попытки подключения очереди.

- **Приостановлено**: сообщение было приостановлено администратором. Дополнительные сведения см. в разделе Приостановка отправки сообщений в очередях.

- **Размер (КБ)**: размер сообщения, округленного до ближайшего килобайта (КБ).

- **SCL**: оценка уровня достоверности нежелательной почты (SCL) сообщения. Допустимые значения представляют собой целые числа от 0 до 9, а также –1 для внутренних (прошедших проверку подлинности) сообщений. Дополнительные сведения см. в статье Пороговые значения уровня достоверности нежелательной почты Exchange (SCL).

- **Идентификатор очереди**: очередь, в которой хранится сообщение. Удостоверение очереди использует синтаксис *<Server>*\ *<Queue>*, где *<Queue>* — это одно из следующих значений:

- **Имя постоянной очереди**:

- **Недопустимый**. Изолирует сообщения, содержащие ошибки и определяемые как опасные для Exchange после сбоя сервера или службы. Содержимое и формат сообщений могут быть действительно опасными, но иногда сообщения обозначаются так из-за неправильно написанного агента транспорта или ошибки в программном обеспечении, которая привела к сбою на сервере Exchange Server.

- **Отправка**. Содержит сообщения, принятые службой транспорта, но не обработанные. Сообщения в очереди передачи либо находятся в обработке, либо ожидают ее.

- **Недоступно**: содержит сообщения, которые не могут быть перенаправлены в места назначения. Обычно это происходит из-за изменений в конфигурации, которые привели к изменению пути маршрутизации для доставки. В этой очереди находятся все сообщения с недоступными адресатами, независимо от пункта назначения.

- **Имя очереди доставки**. Значение свойства **NextHopDomain** очереди, которое фактически является именем очереди. Например, доменное имя, имя сайта Active Directory или имя группы доступности базы данных (DAG). Дополнительные сведения см. в разделе NextHopSolutionKey.

- **Имя источника сообщения**: компонент Exchange, отправив сообщение в очередь. Например, `SMTP:Default <ServerName>`.

- **Тема**: тема сообщения.

- **Последняя ошибка**: последняя ошибка, обнаруженная в сообщении.

  Например, если вы не создали соединитель отправки для доставки почты из Интернета, сообщения, адресованные внешним получателям, пойдут в очередь Недоступно, а значение **Последней ошибки** для сообщения будет: `A matching connector cannot be found to route the external recipient`. Дополнительные сведения о создании соединителя отправки см. в статье Create a Send connector to send mail to the Internet.

  Дополнительные сведения о кодах ошибок SMTP см. в разделе DSN и NDR в Exchange Server.

3. Щелкнув сообщение правой кнопкой мыши и выбрав пункт **Свойства**, вы найдете дополнительные сведения на вкладках **Общие** и **Сведения о получателе**.

   - На вкладке **Общие** отображаются те же значения параметров **Тема**, **С адреса**, **Состояние**, **Размер**, **Имя источника сообщений**, **Вероятность нежелательной почты** и **Последняя ошибка**, что и в списке сообщений. На вкладке **Общие** также отображаются дополнительные свойства, приведенные ниже.
   - **Удостоверение**: удостоверение сообщения. Удостоверение сообщения использует синтаксис <*Server*>\ <*Queue*>\ <*MessageInteger*>, где <*Queue*> — это удостоверение очереди, как описано в свойстве **Queue ID** , а

<MessageInteger> — уникальное целое значение сообщения, отображаемое в свойстве **Identity** командлета **Get-Message** .

- **Идентификатор сообщения в Интернете**: значение поля **заголовка Message-Id:** в заголовке сообщения. Это значение не изменяется на протяжении всего времени жизни сообщения. Для сообщений, созданных в Exchange, значение имеет формат `<GUID@ServerFQDN>`, включая угловые скобки (<>). Например, `<4867a3d78a50438bad95c0f6d072fca5@mailbox01.contoso.com>`.
- **Исходный IP-адрес**: IPv4- или IPv6-адрес внутреннего сервера Exchange или внешнего сервера обмена сообщениями, отправившего сообщение.
- **Дата получения**: дата и время, когда сообщение вошло в очередь.
- **Время окончания срока действия**: дата и время истечения срока действия сообщения, которое будет удалено из очереди, если сообщение не может быть доставлено.
- **Получатели**: получатели в сообщении с соответствующими сообщениями об ошибках. Чтобы просмотреть состояние и сообщения об ошибках для каждого получателя, откройте вкладку **Сведения о получателе**.
- На вкладке **Сведения о получателе** отображены значения параметров **Адрес**, **Состояние** и **Последняя ошибка** для каждого из получателей сообщения. Возможные значения параметра **Состояние** для получателя: **Завершено**, **Готово** или **Повторить попытку**.

Поиск очередей и сообщений в очередях в командной консоли Exchange

Статья • 04.04.2023

Как и в предыдущих версиях Exchange, можно использовать командную консоль Exchange в Exchange Server для просмотра сведений об очередях и сообщениях, а также для выполнения действий с очередями и сообщениями. Как правило, активный Exchange содержит большое количество очередей и сообщений для доставки, поэтому важно понимать, как определить очереди или сообщения, которыми вы хотите управлять.

Для управления элементами вы также можете воспользоваться средством просмотра очереди в панели элементов Exchange. Однако командлеты для просмотра очередей и сообщений в командной консоли Exchange поддерживают больше фильтруемых свойств и параметров фильтра, чем средство просмотра очередей. Дополнительные сведения о средстве просмотра очереди см. в разделе Queue Viewer.

Кроме того, помните, что очереди существуют на серверах почтовых ящиков и пограничных транспортных серверах (транспортной службе). Дополнительные сведения об очередях и сообщениях в очередях см. в разделе Очереди и сообщения в очередях.

Параметры фильтрации очередей

В следующей таблице перечислены параметры фильтрации, доступные в командлетах управления очередями.

Командлет	Параметры фильтрации	Comments

Командлет	Параметры фильтрации	Comments
Get-Queue	*Exclude* *Фильтр* *Identity* *Include* *Сервер*	Параметры *Include* и *Exclude* можно использовать вместе с другими параметрами фильтрации в той же команде. Нельзя использовать параметры *Identity* и *Filter* в одной команде. Параметр *Server* указывает сервер, на котором требуется выполнить команду. Параметры *Server* и *Identity* нельзя использовать в одной команде, но параметр *Server* можно использовать с другими параметрами фильтрации в той же команде.
Resume-Queue **Retry-Queue** **Suspend-Queue**	*Identity* *Фильтр* *Сервер*	Параметр *Identity* нельзя использовать с другими параметрами фильтрации в той же команде. Параметр *Server* указывает сервер, на котором требуется выполнить команду. Параметры *Server* и *Filter* можно использовать в одной команде.
Get-QueueDigest	*Dag* *Фильтр* *Forest* *Сервер* *Site*	Необходимо использовать один из параметров *Dag*, *Site*, *Server* или *Forest* , но вы не можете использовать их вместе в одной команде. Параметр *Filter* можно использовать с любым из других параметров фильтрации.

Идентификатор очереди

Параметр *Identity* использует базовый синтаксис <*Серверная*>\ <*очередь*>. Как правило, это значение однозначно идентифицирует очередь, поэтому нельзя использовать другие параметры фильтрации с параметром *Identity* . Исключением является командлет **Get-Queue** , где можно использовать параметры *Include* и *Exclude* с параметром *Identity* .

В следующей таблице описан синтаксис параметра *Identity* в командлетах управления очередями.

Значение параметра Identity	Описание
`<Server>\<PersistentQueueName>` или `<PersistentQueueName>`	Постоянная очередь на указанном или локальном сервере. `<PersistentQueueName>` имеет значение `Submission`, `Unreachable` или `Poison`. Дополнительные сведения о постоянных очередях см. в разделе Типы очередей.

Значение параметра Identity	Описание
`<Server>\<NextHopDomain>` или `<NextHopDomain>`	Очередь доставки на указанном или локальном сервере. `<NextHopDomain>` — это имя очереди из значения свойства **NextHopDomain** очереди. Например, адресное пространство соединителя отправки, имя сайта Active Directory или имя DAG. Дополнительные сведения см. в разделе NextHopSolutionKey.
`<Server>\<QueueInteger>` или `<QueueInteger>`	Очередь доставки на указанном или локальном сервере. `<QueueInteger>` — это уникальное целочисленное значение, присвоенное очереди доставки или теневой очереди в базе данных очередей. Однако необходимо выполнить командлет **Get-Queue** , чтобы найти это значение в свойствах **Identity** или **QueueIdentity** .
`<Server>\Shadow\<QueueInteger>` или `Shadow\<QueueInteger>`	Теневая очередь на указанном или локальном сервере. Дополнительные сведения о теневых очередях и теневой избыточности см. в разделе Теневая избыточность в Exchange Server.

`<Server>\*` или `*`	Все очереди на указанном или локальном сервере. **Примечание.***Identity* — это позиционный параметр, который означает, что можно указать значение, не указывая `-Identity` квалификатор. Например, следующие команды дают тот же результат:
	`Get-Queue -Identity *`
	`Get-Queue *`
	`Get-Queue`

Параметр фильтра в командлетах очередей

Параметр *Filter* можно использовать во всех командлетах управления очередями, чтобы определить одну или несколько очередей на основе свойств очередей. Параметр *Filter* создает фильтр OPath с операторами сравнения, чтобы ограничить команду очередями, которые соответствуют условиям фильтра. Логический оператор `-and` можно использовать для указания нескольких условий для соответствия. Ниже приведен общий пример синтаксиса:

```
Get-Queue -Filter "<Property1> -<ComparisonOperator> '<Value1>' -and <Property2> -<ComparisonOperator> '<Value2>'..."
```

Полный список свойств очереди, которые можно использовать с параметром *Filter* , см. в разделе Свойства очереди.

Список операторов сравнения, которые можно использовать с параметром *Filter* , см. в разделе Операторы сравнения, используемые при фильтрации очередей или

сообщений этого раздела.

Примеры процедур, использующих параметр *Filter* для просмотра очередей и управления ими, см. в разделе Процедуры для очередей.

Включение и исключение параметров в Get-Queue

Параметры *Include* и *Exclude* можно использовать в **командлете Get-Queue** самостоятельно, с каждым параметром othe или с другими параметрами фильтрации для точной настройки результатов. Например, вы можете:

- Исключите пустые очереди.
- Исключите очереди во внешние назначения.
- Включите очереди с определенным значением **DeliveryType**.

Параметры *Include* и *Exclude* используют следующие свойства очередей для фильтрации:

Значение	Описание	Пример
`DeliveryType`	Включает или исключает очереди на основе свойства **DeliveryType** , определяющего способ передачи сообщения в следующий прыжок. Допустимые значения описаны в разделе NextHopSolutionKey. Вы можете указать несколько значений, разделив их запятыми.	Возвращает все очереди доставки на локальном сервере, где следующим прыжком является соединитель отправки, размещенный на локальном сервере и настроенный для маршрутизации интеллектуальных узлов. `Get-Queue -Include SmartHostConnectorDelivery`
`Empty`	Включает или исключает пустые очереди. Пустые очереди имеют значение `0` в свойстве **MessageCount** .	Возвращает все очереди на локальном сервере, содержащие сообщения. `Get-Queue -Exclude Empty`

Значение	Описание	Пример
`External`	Включает или исключает очереди, имеющие значение `External` в свойстве **NextHopCategory** . Свойство **DeliveryType** внешних очередей всегда имеет одно из следующих значений: • `DeliveryAgent` • `DnsConnectorDelivery` • `NonSmtpGatewayDelivery` • `SmartHostConnectorDelivery` Дополнительные сведения см. в разделе NextHopSolutionKey.	Возвращает все внутренние очереди на локальном сервере. `Get-Queue -Exclude External`
`Internal`	Это значение включает или исключает очереди, имеющие значение `Internal` в свойстве **NextHopCategory** . Обратите внимание, что сообщение для внешнего получателя может потребовать нескольких внутренних прыжков, прежде чем оно достигнет сервера шлюза, на котором оно доставлено извне.	Возвращает все внутренние очереди на локальном сервере. `Get-Queue -Include Internal`

Обратите внимание, что можно дублировать функции параметров *Include* и *Exclude* с помощью параметра *Filter* . Например, следующие команды дают тот же результат:

- `Get-Queue -Exclude Empty`
- `Get-Queue -Filter "MessageCount -gt 0"`

Однако, как видите, синтаксис параметров *Include* и *Exclude* проще и проще запоминать.

Get-QueueDigest

Командлет **Get-QueueDigest** позволяет просматривать сведения о некоторых или всех очередях в организации с помощью одной команды. В частности, с помощью командлета **Get-QueueDigest** вы можете просмотреть информацию об очередях в зависимости от их расположения на серверах, в группах обеспечения доступности баз данных, на сайтах Active Directory или во всем лесу Active Directory.

Обратите внимание, что очереди на подписанном пограничном транспортном сервере не включаются в результаты. Кроме того, **Get-QueueDigest** доступен на пограничном транспортном сервере, но результаты ограничены локальными очередями на пограничном транспортном сервере.

> ⓘ **Примечание**
>
> По умолчанию командлет **Get-QueueDigest** отображает очереди доставки, содержащие десять или более сообщений, а результаты находятся в возрасте от одной до двух минут. Инструкции по изменению этих значений по умолчанию см. в разделе **Настройка Get-QueueDigest**.

В следующей таблице описаны параметры фильтрации и сортировки, доступные в командлете **Get-QueueDigest** .

Параметр	Описание
Dag, *Server* или *Site*	Эти параметры являются взаимоисключающими (не могут использоваться в одной команде) и задают область для командлета. Необходимо указать один из этих параметров или параметр *Лес* . Как правило, используется имя сервера, DAG или сайта Active Directory, но можно использовать любое значение, однозначно определяющее сервер, DAG или сайт. Можно указать несколько серверов, групп доступности доступности или сайтов, разделенных запятыми.
Forest	Этот параметр является обязательным, если вы не используете параметры *Dag*, *Server* или *Site* . Значение для этого переключателя указать нельзя. С помощью этого параметра вы получаете очереди со всех серверов почтовых ящиков Exchange в локальном лесу Active Directory. Этот параметр нельзя использовать для просмотра очередей в удаленных лесах Active Directory.

Параметр	Описание
DetailsLevel	`Normal` — значение по умолчанию. В результатах возвращаются следующие свойства: • **QueueIdentity** • **ServerIdentity** • **MessageCount** `Verbose` возвращает следующие дополнительные свойства в результатах: • **DeferredMessageCount** • **LockedMessageCount*** • **IncomingRate** • **Исходящая скорость** • **Velocity** • **NextHopDomain** • **NextHopCategory** • **NextHopConnector** • **DeliveryType*** • **Состояние** • **RiskLevel*** • **OutboundIPPool*** • **LastError** • **TlsDomain** `None` пропускает имя очереди из столбца **Сведения** в результатах. * Эти свойства зарезервированы для внутреннего использования Майкрософт и не используются в локальных организациях Exchange. Дополнительные сведения обо всех свойствах в этом списке см. в разделе Свойства очереди.
Фильтр	Фильтрация очередей на основе свойств очереди, как описано в разделе Фильтровать параметр в командлетах очередей . Можно использовать любое из фильтруемых свойств очереди, как описано в разделе Свойства очереди .
GroupBy	Групповка результатов очереди. Объединить результаты можно по одному из следующих свойств: • **DeliveryType** • **LastError** • **NextHopCategory** • **NextHopDomain** • **NextHopKey** • **Состояние** • **ServerName** По умолчанию результаты группируются по свойству **NextHopDomain**. Дополнительные сведения об этих свойствах очереди см. в разделе Свойства очереди.

Параметр	Описание
ResultSize	Ограничивает результаты очереди указанным значением. Очереди сортируются в порядке убывания в зависимости от количества сообщений в очереди и группируются по значению, заданному параметром *GroupBy* . Значение по умолчанию — 1000. Это значит, что по умолчанию команда отображает первую тысячу очередей, сгруппированных по свойству **NextHopDomain** и упорядоченных по убыванию числа сообщений в очереди.
Timeout	Параметр указывает количество секунд до истечения времени ожидания операции. Значение по умолчанию — `00:00:10` или 10 секунд.

В этом примере возвращаются все непустые внешние очереди на серверах с именами Mailbox01, Mailbox02 и Mailbox03.

PowerShell

```
Get-QueueDigest -Server Mailbox01,Mailbox02,Mailbox03 -Include External -
Exclude Empty
```

Параметры фильтрации сообщений

В следующей таблице перечислены параметры фильтрации, доступные в командлетах управления сообщениями.

Командлет	Параметры фильтрации	Comments
Get-Message	*Фильтр* *Identity* *Очередь* *Сервер*	Нельзя использовать параметры *Filter*, *Identity* или *Queue* в одной команде. Параметр *Server* указывает сервер, на котором требуется выполнить команду. Параметры *Server* и *Filter* можно использовать в одной команде.
Remove-Message **Resume-Message** **Suspend-Message**	*Фильтр* *Identity* *Сервер*	Необходимо использовать параметр *Identity* или *Filter* , но их нельзя использовать в одной и той же команде. Параметр *Server* указывает сервер, на котором требуется выполнить команду. Параметры *Server* и *Filter* можно использовать в одной команде.
Redirect-Message	*Сервер*	Этот командлет истощает активные сообщения из всех очередей доставки на указанном сервере, поэтому *сервер* является единственным доступным параметром фильтрации. Дополнительные сведения см. в статье Перенаправление сообщений в очередях.

Командлет	Параметры фильтрации	Comments
Export-Message	*Identity*	Этот параметр на самом деле не является фильтром, так как он однозначно идентифицирует сообщение. Чтобы определить несколько сообщений для этого командлета, используйте **Командлет Get-Message** и передайте результаты в **Export-Message**. Дополнительные сведения и примеры см. в статье Экспорт сообщений из очередей.

Идентификатор сообщения

Параметр *Identity* в командлетах управления сообщениями однозначно идентифицирует сообщение в одной или нескольких очередях, поэтому вы не можете использовать другие параметры фильтрации сообщений. Параметр *Identity* использует базовый синтаксис `<Server>\<Queue>\<MessageInteger>`.

В следующей таблице описан синтаксис, который можно использовать с параметром *Identity* в командлетах управления сообщениями.

**Значение параметра identity	Описание**
`<Server>\<Queue>\<MessageInteger>` или `<Queue>\<MessageInteger>`	Сообщение в определенной очереди на указанном или локальном сервере. `<Queue>` — это удостоверение очереди, как описано в разделе Удостоверение очереди : • **Имя постоянной очереди**: • **Имя очереди доставки**. • **Номер очереди**. • **Идентификатор теневой очереди**. `<MessageInteger>` — это уникальное целочисленное значение, присваиваемое сообщению при первом входе в базу данных очереди на сервере. Если сообщение отправляется нескольким получателям, которые используют множество очередей, все копии сообщения во всех очередях из базы данных очередей обладают одинаковым целочисленным номером. Однако необходимо выполнить командлет **Get-Message** , чтобы найти это значение в свойствах **Identity** или **MessageIdentity** .
`<Server>\*\<MessageInteger>` или `*\<MessageInteger>` `<MessageInteger>`	Все копии сообщения во всех очередях в базе данных очередей на указанном или локальном сервере.

Параметр filter в командлетах сообщений

Параметр *Filter* можно использовать с командлетами **Get-Message**, **Remove-Message**, **Resume-Message** и **Suspend-Message** , чтобы определить одно или несколько сообщений на основе свойств сообщений. Параметр *Filter* создает фильтр OPath с операторами сравнения, чтобы ограничить команду сообщениями, которые соответствуют условиям фильтра. Логический оператор `-and` можно использовать для указания нескольких условий для соответствия. Ниже приведен общий пример синтаксиса:

```
Get-Message -Filter "<Property1> -<ComparisonOperator> '<Value1>' -and <Property2> -<ComparisonOperator> '<Value2>'..."
```

Полный список свойств сообщения, которые можно использовать с параметром *Filter* , см. в разделе Свойства сообщения.

Список операторов сравнения, которые можно использовать с параметром *Filter* , см. в разделе Операторы сравнения, используемые при фильтрации очередей или сообщений этого раздела.

Примеры процедур, использующих параметр *Filter* для просмотра сообщений и управления ими, см. в разделе Процедуры для сообщений в очередях.

Параметр Queue

Параметр *Queue* доступен только в командлете **Get-Message** . Этот параметр можно использовать для получения всех сообщений в определенной очереди или всех сообщений из нескольких очередей с помощью подстановочного знака (*). При использовании параметра *Queue* используйте формат `<Server>\<Queue>` удостоверения очереди, как описано в разделе Удостоверение очереди в этом разделе.

Операторы сравнения, используемые при фильтрации очередей и сообщений

Когда вы создаете выражение фильтрации очередей или сообщений с помощью параметра *Filter*, следует добавить оператор сравнения для выбора нужного значения свойства. Операторы сравнения, которые можно использовать, а также способы работы каждого оператора описаны в следующей таблице. Для всех операторов регистр задаваемых значений не учитывается.

Оператор	Функция	Пример кода

`-eq`	Точное совпадение указанного значения.	Показать все очереди с состоянием "Повторить".
		`Get-Queue -Filter "Status -eq 'Retry'"`
		Показать все сообщения с состоянием Retry:
		`Get-Message -Filter "Status -eq 'Retry'"`

`-ne`	Не соответствует указанному значению.	Показать все очереди, у которых нет состояния "Активные":
		`Get-Queue -Filter "Status -ne 'Active'"`
		Показать все сообщения, у которых нет состояния "Активный":
		`Get-Message -Filter "Status -ne 'Active'"`

`-gt`	Больше указанного целого числа или значения даты и времени.	Показать очереди, которые в настоящее время содержат более 1000 сообщений:
		`Get-Queue -Filter "MessageCount -gt 1000"`
		Отображение сообщений, для которых в настоящее время число повторных попыток превышает 3:
		`Get-Message -Filter "RetryCount -gt 3"`

`-ge`	Больше указанного целого числа или значения даты и времени или равно ей.	Отображение очередей, которые в настоящее время содержат 1000 или более сообщений:
		`Get-Queue -Filter "MessageCount -ge 1000"`
		Отображение сообщений, для которых в настоящее время количество повторных попыток не превышает 3:
		`Get-Message -Filter "RetryCount -ge 3"`

`-lt`	Меньше указанного целого числа или значения даты и времени.	Показать очереди, которые в настоящее время содержат менее 1000 сообщений:
		`Get-Queue -Filter "MessageCount -lt 1000"`
		Отображение сообщений с SCL меньше 6:
		`Get-Message -Filter "SCL -lt 6"`

`-le`	Меньше указанного целого числа или значения даты и времени или равно ей.	Отображение очередей, которые в настоящее время содержат 1000 или менее сообщений:
		`Get-Queue -Filter "MessageCount -le 1000"`
		Отображение сообщений с числом SCL 6 или меньше:
		`Get-Message -Filter "SCL -le 6"`

Оператор	Функция	Пример кода
`-like`	Содержит указанный текст. В текстовую строку необходимо включить подстановочный знак (*).	Отображение очередей, имеющих назначение, любому домену SMTP, который заканчивается на Contoso.com: `Get-Queue -Filter "Identity -like '*contoso.com'"` Показать сообщения с темой, содержащей текст "кредит на выплату заработной платы": `Get-Message -Filter "Subject -like '*payday loan*'"`

Фильтр, который вычисляет несколько выражений, можно указать с помощью логического оператора `-and`. Очереди или сообщения должны соответствовать всем условиям фильтра, которые должны быть включены в результаты.

Этот пример отображает список очередей, назначениями которых являются любые имена SMTP-доменов, заканчивающихся на Contoso.com, и которые содержат более 500 сообщений.

PowerShell

```
Get-Queue -Filter "Identity -like '*contoso.com*' -and MessageCount -gt 500"
```

В этом примере отображается список сообщений, отправляемых с любого адреса электронной почты в домене contoso.com со значением SCL больше 5.

PowerShell

```
Get-Message -Filter "FromAddress -like '*Contoso.com*' -and SCL -gt 5"
```

Расширенные параметры разбивки по страницам

При использовании командной консоли Exchange для просмотра очередей и сообщений в очередях запрос получает одну страницу информации за раз. Расширенные параметры разбиения на страницы определяют размер результатов и порядок отображения результатов. Все дополнительные параметры подкачки являются необязательными и могут использоваться с другими параметрами фильтрации в командлетах **Get-Queue** и **Get-Message** или без них. Если

расширенные параметры разбивки по страницам не указываются, запрос возвращает результаты в порядке возрастания идентификаторов.

По умолчанию при указании порядка сортировки свойство **Identity** всегда включается и отсортируется по возрастанию, так как другие доступные свойства очереди или сообщения не являются уникальными.

Чтобы пометить позицию в отсортированных результатах, можно использовать параметры *BookmarkIndex* и *BookmarkObject* . Если объект закладки больше не существует при получении следующей страницы результатов, результаты начинаются с ближайшего к закладке элемента, который зависит от указанного порядка сортировки.

Дополнительные параметры подкачки описаны в следующей таблице.

Параметр	**Описание**
BookmarkIndex	Указывает позицию в результатах, с которой начинаются отображаемые результаты. Значение этого параметра представляет собой индекс на основе 1 в общих результатах. Если значение меньше или равно 0, возвращается первая полная страница результатов. Если задано `Int.MaxValue` значение , возвращается последняя полная страница результатов. Этот параметр нельзя использовать с параметром *BookmarkObject* .
BookmarkObject	Указывает объект в результатах, с которого начинаются отображаемые результаты. Если указать объект закладки, этот объект используется в качестве пункта начала поиска. Извлекаются строки до или после этого объекта (в зависимости от значения параметра *SearchForward*). Этот параметр нельзя использовать с параметром *BookmarkIndex* .
IncludeBookmark	Указывает, следует ли включать объект закладки в результаты. Допустимые значения: `$true`: объект закладки включен в результаты. Это значение используется по умолчанию. `$false`: объект закладки не включен в результаты. Используйте это значение при выполнении запроса для ограниченного размера результата, а затем укажите последний элемент в качестве закладки для следующего запроса. Это предотвращает включение объекта закладки в оба результата.
ResultSize	Указывает количество результатов, отображаемых на странице. Если значение не указано, по умолчанию используется размер результатов, равный 1000 объектам. Exchange ограничивает результаты до 250 000.
ReturnPageInfo	Это скрытый параметр. Он возвращает сведения об общем числе результатов и индекс первого объекта текущей страницы. Значение по умолчанию — `$false`.

Параметр	Описание
SearchForward	Задает направление поиска. **Указанная закладка**: поиск вперед или назад в результатах относительно индекса или объекта закладки. **Закладка не указана**: поиск вперед или назад в результатах первого или последнего элемента в результатах. Допустимые значения: `$true`: выполняется поиск вперед из первого элемента в результатах или из указанной закладки. Если за пределами закладки нет результатов, запрос возвращает последнюю полную страницу результатов. Это значение используется по умолчанию. `$false`: выполняется поиск в обратном направлении от последнего элемента в результатах или из указанной закладки. Если за пределами закладки меньше полной страницы результатов, запрос возвращает первую полную страницу результатов.
SortOrder	Задает свойства сообщения, управляющие порядком сортировки результатов. Порядок указания свойств указывает порядок убывания очередности (результаты сортируются по первому свойству, затем эти результаты сортируются по второму свойству, а затем — по свойству son). Этот параметр использует синтаксис : `<+|-><Property1>,<+|-><Property2>...`, где `+` сортирует свойство по возрастанию и `-` сортирует свойство в порядке убывания. Если этот параметр не используется, результаты сортируются по свойству **Identity** в порядке возрастания.

В этом примере показано, как использовать расширенные параметры разбиения на разбиение Команда возвращает первые 500 сообщений на указанном сервере. Результаты сначала сортируются по возрастанию по адресу отправителя, а затем по убыванию по размеру сообщения.

PowerShell

```
Get-Message -Server mailbox01.contoso.com -ResultSize 500 -SortOrder
+FromAddress,-Size
```

Этот пример возвращает первые 500 сообщений на указанном сервере в указанном порядке сортировки, задает объект закладки, исключает объект закладки из результатов и извлекает следующие 500 сообщений в том же порядке сортировки.

1. Выполните следующую команду, чтобы получить первую страницу результатов.

   PowerShell

```
$Results=Get-Message -Server mailbox01.contoso.com -ResultSize 500 -
SortOrder +FromAddress,-Size
```

2. Чтобы задать объект закладки, выполните следующую команду, чтобы сохранить последний элемент первой страницы в переменной.

PowerShell

```
$Temp=$Results[$results.length-1]
```

3. Чтобы получить следующие 500 объектов на указанном сервере и исключить объект закладки, выполните следующую команду.

PowerShell

```
Get-Message -Server mailbox01.contoso.com -BookmarkObject:$Temp -
IncludeBookmark $false -ResultSize 500 -SortOrder +FromAddress,-Size
```

Изменение расположения базы данных очереди в Exchange Server

Статья • 04.04.2023

Exchange Server использует базу данных ESE для хранения сообщений очереди. Все очереди хранятся в одной базе данных ESE. Очереди существуют на серверах почтовых ящиков Exchange и пограничных транспортных серверах. Дополнительные сведения см. в разделе Queues and messages in queues.

Расположение базы данных очереди и журналов транзакций базы данных очереди управляется ключами в `%ExchangeInstallPath%Bin\EdgeTransport.exe.config` XML-файле конфигурации приложения. Этот файл связан со службой Транспорт Exchange. В следующей таблице каждый ключ рассматривается более подробно.

Key	Описание
QueueDatabasePath	Определяет расположение файлов базы данных очереди. Это следующие файлы: • Mail.que • Trn.chk Расположение по умолчанию — `%ExchangeInstallPath%TransportRoles\data\Queue`.
QueueDatabaseLoggingPath	Определяет расположение файлов журналов транзакций базы данных очереди. Это следующие файлы: • Trn.log • Trntmp.log • Trn *nnn.log* • Trnres00001.jrs • Trnres00002.jrs • Temp.edb Обратите внимание, что файл Temp.edb используется для проверки схемы базы данных очереди при запуске службы Транспорт Exchange. Хотя файл Temp.edb не является файлом журнала транзакций, он хранится там же, где и файлы журнала транзакций. Расположение по умолчанию — `%ExchangeInstallPath%TransportRoles\data\Queue`.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 15 минут.
- Разрешения Exchange не применяются к процедурам, описанным в этой статье. Эти процедуры выполняются в операционной системе сервера Exchange.
- При остановке или перезапуске службы Транспорт Exchange поток почты на сервере прерывается.
- Если вы изменяете расположение базы данных очереди или журналов транзакций, существующие файлы базы данных и журналов не перемещаются. Новая база данных и новые журналы транзакций создаются в новом расположении. Старые файлы остаются там же, где и раньше, но больше не используются. Если вы хотите повторно использовать старую базу данных очереди или старые файлы журналов транзакций в новом расположении, переместите файлы в новое расположение после остановки службы Транспорт Exchange.
- Папка для базы данных очереди и журналов транзакций должна иметь следующие разрешения:
  - Сетевая служба: полный доступ
  - Система: полный доступ
  - Администраторы: полный доступ

    Если такой папки нет, но эти разрешения есть у родительской папки, новая папка создается автоматически.
- Все настраиваемые параметры Exchange или IIS, внесенные в файлы конфигурации приложения Exchange XML на сервере Exchange Server (например, web.config файлы или EdgeTransport.exe.config файл), **будут перезаписаны** при установке exchange CU. Обязательно сохраните эти сведения, чтобы можно было легко повторно применить параметры после установки. После установки exchange CU необходимо повторно настроить эти параметры.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.
- Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server, Exchange Online или Exchange Online Protection.

Использование командной строки для создания базы данных очереди и журналов транзакций в новом расположении

1. Создайте папку, в которой вы хотите хранить базу данных очереди и журналы транзакций. Убедитесь, что к папке применяются правильные разрешения.

2. В окне командной строки откройте файл EdgeTransport.exe.config в Блокноте, выполнив следующую команду:

   Консоль

   ```
   Notepad %ExchangeInstallPath%Bin\EdgeTransport.exe.config
   ```

3. Найдите и измените следующие ключи в `<appSettings>` разделе.

   XML

   ```
   <add key="QueueDatabasePath" value="<LocalPath>" />
   <add key="QueueDatabaseLoggingPath" value="<LocalPath>" />
   ```

   Например, чтобы создать новую базу данных очереди и журналы транзакций в папке D:\Queue\QueueDB, используйте следующие значения:

   XML

   ```
   <add key="QueueDatabasePath" value="D:\Queue\QueueDB" />
   <add key="QueueDatabaseLoggingPath" value="D:\Queue\QueueDB" />
   ```

   Закончив, сохраните и закройте файл EdgeTransport.exe.config.

4. Перезапустите службу Транспорт Exchange, выполнив следующую команду:

   Консоль

   ```
   net stop MSExchangeTransport && net start MSExchangeTransport
   ```

Как проверить, все ли получилось?

Чтобы проверить, успешно ли созданы новые журналы транзакций и база данных очереди в новом расположении:

1. Убедитесь, что новые файлы базы данных Mail.que и Trn.chk созданы в новом расположении.
2. Убедитесь в том, что новые файлы журнала транзакций Trn.log, Trntmp.log, Trnres00001.jrs, Trnres00002.jrs и Temp.edb созданы в новом расположении.
3. Если после запуска службы Транспорт Exchange вы можете удалить из старого расположения базу данных очереди и файлы журнала транзакций, старая база данных очереди больше не используется.

Использование командной строки для перемещения существующей базы данных очереди и журналов транзакций в новое расположение

> ⓘ **Примечание**
>
> Существует также скрипт для перемещения базы данных очереди и журналов транзакций. Его можно найти в папке %ExchangeInstallPath%Scripts и называться Move-TransportDatabase.ps1. Необходимо указать следующие параметры: queueDatabasePath, queueDatabaseLoggingPath, iPFilterDatabasePath, iPFilterDatabaseLoggingPath и temporaryStoragePath.

Для сохранения недоставленных сообщений в базе данных очереди вам потребуется ее переместить, однако перемещать соответствующие журналы транзакций обычно не нужно, так как:

- При нормальном завершении работы служба Транспорт Exchange записывает все несохраненные элементы журнала транзакций в базу данных очереди.
- Используется циклическое ведение журнала, поэтому журналы транзакций, которые содержат ранее сохраненные изменения базы данных, не сохраняются.

1. Создайте папку, в которой вы хотите хранить базу данных очереди и журналы транзакций. Убедитесь, что к папке применяются правильные разрешения.
2. В окне командной строки откройте файл EdgeTransport.exe.config в Блокноте, выполнив следующую команду:

```
Консоль
```

```
Notepad %ExchangeInstallPath%Bin\EdgeTransport.exe.config
```

3. Найдите и измените следующие ключи в `<appSettings>` разделе:

```
XML
<add key="QueueDatabasePath" value="<LocalPath>" />
<add key="QueueDatabaseLoggingPath" value="<LocalPath>" />
```

   Например, чтобы заменить расположение базы данных очереди и журналов транзакций на папку D:\Queue\QueueDB, используйте следующие значения:

```
XML
<add key="QueueDatabasePath" value="D:\Queue\QueueDB" />
<add key="QueueDatabaseLoggingPath" value="D:\Queue\QueueDB" />
```

   Закончив, сохраните и закройте файл EdgeTransport.exe.config.

4. Остановите службу Транспорт Exchange, выполнив следующую команду:

```
Консоль
net stop MSExchangeTransport
```

5. Переместите существующие файлы базы данных Mail.que и Trn.chk из старого расположения в новое.

6. Переместите существующие файлы журналов транзакций Trn.log, Trntmp.log, Trn *nnnnn*.log, Trnres00001.jrs, Trnres00002.jrs и Temp.edb из старого расположения в новое.

7. Запустите службу Транспорт Exchange, выполнив следующую команду:

```
Консоль
net start MSExchangeTransport
```

Как проверить, все ли получилось?

Чтобы проверить, были ли существующие журналы транзакций и база данных очереди успешно перемещены в новое расположение:

1. Убедитесь, что файлы базы данных очереди Mail.que и Trn.chk созданы в новом расположении.
2. Убедитесь, что файлы журнала транзакций Trn.log, Trntmp.log, Trnres00001.jrs, Trnres00002.jrs и Temp.edb созданы в новом расположении.
3. Убедитесь, что в старом расположении нет файлов базы данных очереди и журнала транзакций.

Интервалы повтора, повторной отправки и истечения срока действия сообщений в Exchange Server

Статья • 04.04.2023

В Exchange Server сообщения, которые не могут быть успешно доставлены, подвергаются различным срокам повтора, повторной отправки и окончания срока действия в зависимости от источника и назначения сообщения. *Повторная попытка доставки* — это новая попытка подключиться к месту назначения. *Повторная отправка* — это отправка сообщения обратно в очередь передачи для повторной обработки классификатором. После безуспешного выполнения всех попыток доставить сообщение в течение определенного периода срок действия сообщения *заканчивается*. После истечения срока действия сообщения отправитель получит уведомление о неудавшейся доставке, а само сообщение будет удалено из очереди.

При возникновении любого из трех событий — повторной передачи, повторной отправки и истечения срока действия, — прежде чем над сообщениями будут совершены соответствующие автоматические действия, можно выполнить некоторые действия вручную.

Инструкции по настройке этих интервалов см. в разделе Настройка интервалов повторной отправки, повторной передачи и истечения срока действия сообщений.

Параметры конфигурации для повторной передачи сообщений

Когда службе транспорта на сервере почтовых ящиков или на пограничном транспортном сервере не удается подключиться к следующему прыжку, очередь переходит в состояние повторной попытки доставки. Попытки создать подключение продолжаются до тех пор, пока не истечет срок действия очереди либо не будет создано подключение.

Параметры конфигурации для автоматического выполнения повторных попыток доставки сообщений в файле EdgeTransport.exe.config

Параметры интервала повтора автоматического сообщения, доступные в `%ExchangeInstallPath%Bin\EdgeTransport.exe.config` файле конфигурации XML-приложения, описаны в следующей таблице.

> **ⓘ Примечание**
>
> Все настраиваемые параметры Exchange или IIS, внесенные в файлы конфигурации приложения Exchange XML на сервере Exchange Server (например, web.config файлы или EdgeTransport.exe.config файл), **будут перезаписаны** при установке exchange CU. Обязательно сохраните эти сведения, чтобы можно было легко повторно применить параметры после установки. После установки exchange CU необходимо повторно настроить эти параметры.

Название параметра автоматического выполнения повторных попыток доставки сообщений	**Значение по умолчанию**	**Описание**
MailboxDeliveryQueueRetryInterval	`00:05:00` (5 минут)	Этот параметр определяет периодичность, с которой очереди пытаются подключиться к службе доставки транспорта почтовых ящиков для базы данных почтовых ящиков назначения, к которой не удается подключиться. Чтобы указать значение, введите его в качестве интервала времени: `dd.hh:mm:ss` where `dd` = дни, `hh` = часы, `mm` = минуты и `ss` = секунды. Допустимым значением является интервал времени от `00:00:01` (одна секунда) до `1.00:00:00` (один день).

Название параметра автоматического выполнения повторных попыток доставки сообщений	Значение по умолчанию	Описание
QueueGlitchRetryCount	4	Этот параметр указывает количество попыток подключения, которые выполняются сразу после того как транспортному серверу не удается подключиться к серверу назначения. Подобные проблемы при подключении обычно связаны с очень кратковременными перебоями в работе сети. Допустимое значение — целое число от 0 до 15. Обычно нет необходимости изменять этот параметр. Исключение составляют случаи, когда сеть ненадежна, и в ней регулярно происходят случайные разрывы подключений.
QueueGlitchRetryInterval	`00:01:00` (1 минута)	Интервал подключения между каждой попыткой подключения, заданный ключом *QueueGlitchRetryCount* . Обычно нет необходимости изменять этот параметр, если только сеть не оказалась ненадежной и случайные разрывы подключений в ней не случаются регулярно.

Параметры конфигурации для автоматического выполнения повторных попыток доставки сообщений в Центр администрирования Exchange и Командная консоль Exchange

Параметры интервалов между автоматическими повторными попытками доставки сообщений, доступные в Центр администрирования Exchange и Командная консоль Exchange, описаны в таблице ниже.

Название параметра автоматического выполнения повторных попыток доставки сообщений	Значение по умолчанию	Настройка с помощью командной консоли Exchange	Конфигурация Центра администрирования Exchange на серверах почтовых ящиков
Интервал повтора сообщения: интервал повтора для отдельных сообщений, имеющих состояние повтора.	15 минут (`00:15:00`) Рекомендуется не изменять значение по умолчанию, если для этого не будет указана служба поддержки майкрософт или документация по конкретному продукту.	Командлет: **Set-TransportService** Параметр *: MessageRetryInterval*	н/д

Интервал повторных попыток сбоя исходящего подключения: интервал повтора для попыток исходящего подключения, которые ранее завершились сбоем. Для контроля ранее неудавшихся попыток подключения используются значения количества повторных попыток при временных ошибках и интервала между ними.	Транспортная служба на серверах почтовых ящиков: 10 минут (`00:10:00`) Пограничные транспортные серверы: 30 минут (`00:30:00`)	Командлет: **Set-TransportService** Параметр *: OutboundConnectionFailureRetryInterval*	**Серверов**> Выберите сервер >**Изменить** ( ) >**Ограничения**> транспорта Интервал **повтора** в разделе >**"Сбой исходящего подключения" (в секундах)**

Количество повторных попыток временных сбоев: количество попыток подключения, которые были предприняты после сбоя повторных попыток сбоя очереди и значений интервалов. Такие ошибки могут быть вызваны перезапусками сервера или ошибками при подстановке кэшированного DNS. Допустимое значение — целое число от 0 до 15. Значение 0 указывает, что для управления следующей попыткой подключения используется значение интервала между повторными попытками после ошибки исходящего подключения.	6	Командлет: **Set-TransportService** Параметр *: TransientFailureRetryCount*	**Серверов**> Выберите сервер >**Изменить** ( ) >**Ограничения**> транспорта **Повторы**, раздел >**Временный сбой повторных попыток**

Интервал повторных попыток с временным сбоем. Интервал подключения между каждой попыткой подключения, заданный значением счетчика повторных попыток с временным сбоем.	Транспортная служба на серверах почтовых ящиков: 5 минут (`00:05:00`) Пограничные транспортные серверы: 10 минут (`00:10:00`)	Командлет: **Set-TransportService** Параметр *: TransientFailureRetryInterval*	**Серверов**> Выберите сервер >**Изменить** ( ) >**Ограничения**> транспорта Раздел >**Повторы** Интервал **повторных попыток с временным сбоем (в минутах)**

Параметры конфигурации для выполнения повторных попыток доставки сообщений вручную

Если очередь доставки находится в состоянии Retry, можно вручную принудительно выполнить немедленную попытку подключения с помощью средства просмотра очередей на панели элементов Exchange или **командлета Retry-Queue** в командной консоли Exchange. Повторная попытка, выполняемая вручную, переопределяет запланированное время следующей повторной попытки. Если не удалось создать подключение, таймер интервалов между повторными попытками будет сброшен. Чтобы это действие вступило в силу, очередь доставки должна находиться в состоянии Retry (Повторная попытка). Дополнительные сведения см. в разделе Повторный запуск очередей.

Параметры конфигурации для сообщений DSN о задержке

После каждой неудавшейся доставки сообщения служба транспорта на пограничном транспортном сервере или сервере почтовых ящиков создает уведомление о задержанной доставке и помещает его в очередь для доставки отправителю недоставленного сообщения. Уведомление о задержанной доставке отправляется только по истечении интервала уведомления о задержке (по умолчанию он равен 4 часам) и только если сообщение не было доставлено в течение этого времени. Такая задержка позволяет предотвратить отправку ненужных уведомлений о задержанной доставке из-за временных и, в конечном итоге, устраненных ошибок при передаче сообщения. Вы можете выборочно

включать или отключать функцию отправки уведомлений о задержанной доставке для сообщений, отправленных изнутри или извне организации Exchange.

Параметры конфигурации, доступные для уведомлений о задержанной доставке, описаны в таблице ниже.

Параметр уведомления о задержанной доставке	**Значение по умолчанию**	**Настройка с помощью командной консоли Exchange**	**Конфигурация Центра администрирования Exchange на серверах почтовых ящиков**
Время ожидания уведомления о задержке. Время ожидания сервера перед отправкой отправителю сообщения о задержке DSN. Это значение всегда должно быть больше произведения количества повторных попыток при временной ошибке и длительности интервала между повторными попытками при временной ошибке (по умолчанию используется общее значение 30 минут для сервера почтовых ящиков и 1 час для пограничного транспортного сервера).	4 часа (`4:00:00`)	Командлет: **Set-TransportService** Параметр *: DelayNotificationTimeOut*	**Серверов**> Выберите сервер >**Изменить** (✎) >**Ограничения**> транспорта **Раздел**> Уведомления **уведомлять отправителя при задержке сообщения после (часы)**
Включена внешняя задержка DSN. Указывает, можно ли отправлять сообщения DSN задержки внешним отправителям сообщений (отправителям, которые находятся за пределами организации Exchange). *ExternalDelayDSNEnabled*	`$true`	Командлет: **Set-TransportConfig** Параметр: *ExternalDelayDSNEnabled*	Недоступно

Параметр уведомления о задержанной доставке	Значение по умолчанию	Настройка с помощью командной консоли Exchange	Конфигурация Центра администрирования Exchange на серверах почтовых ящиков
Включена внутренняя задержка DSN. Указывает, можно ли отправлять сообщения DSN задержки внутренним отправителям сообщений (отправителям сообщений, которые находятся в организации Exchange).	`$true`	Командлет: **Set-TransportConfig** Параметр: *InternalDelayDSNEnabled*	Недоступно

Параметры конфигурации для повторной отправки сообщений

Функция повторной отправки сообщений помещает недоставленные сообщения обратно в очередь передачи для повторной обработки классификатором. Дополнительные сведения о классификаторе и очереди передачи см. в разделе Общие сведения о службе транспорта на серверах почтовых ящиков.

Автоматическая повторная отправка сообщений

Система автоматически выполняет повторную отправку недоставленных сообщений, находящихся в очереди доставки, если последняя находится в состоянии Retry (Повторная попытка) и не удалось доставить ни одного сообщения в течение заданного времени. Этот период времени управляется ключом *MaxIdleTimeBeforeResubmit* в `%ExchangeInstallPath%Bin\EdgeTransport.exe.config` XML-файле конфигурации приложения. Значение по умолчанию — `12:00:00` или 12 часов.

> ⓘ **Примечание**
>
> Все настраиваемые параметры Exchange или IIS, внесенные в файлы конфигурации приложения Exchange XML на сервере Exchange Server (например, web.config файлы или EdgeTransport.exe.config файл), **будут перезаписаны** при установке exchange CU. Обязательно сохраните эти сведения, чтобы можно было легко повторно применить параметры после

установки. После установки exchange CU необходимо повторно настроить эти параметры.

Повторная отправка сообщений вручную

Вы можете повторно отправлять сообщения вручную, используя указанные ниже методы.

- Повторная отправка сообщений, находящихся в очереди доставки с состоянием Retry (Повторная попытка) или в очереди "Недоступные". Дополнительные сведения см. в разделе Повторная отправка очередей.
- Повторная отправка сообщений, находящихся в очереди подозрительных сообщений. Дополнительные сведения см. в разделе Повторная отправка сообщений, находящихся в очереди подозрительных сообщений.
- Приостановка очереди, приостановка сообщений в очереди, экспорт сообщений в файл и копирование файлов в каталог Replay (Повтор) на любом сервере почтовых ящиков или пограничном транспортном сервере. Дополнительные сведения см. в статье Экспорт сообщений из очередей.

Параметры конфигурации для срока действия сообщения

Параметр *времени ожидания перед завершением срока действия сообщения* указывает максимальное время, в течение которого пограничный транспортный сервер или сервер почтовых ящиков (служба транспорта) пытается доставить недоставленное сообщение. Если не удастся доставить сообщение до истечения времени ожидания, отправитель получит отчет о недоставке (также называемый сообщением о недоставке), содержащий исходное сообщение или его заголовки.

Автоматическое завершение срока действия сообщений

В таблице ниже указаны значения времени ожидания перед завершением срока действия сообщений.

Значение по умолчанию	Настройка с помощью командной консоли Exchange	Конфигурация Центра администрирования Exchange на серверах почтовых ящиков

Значение по умолчанию	Настройка с помощью командной консоли Exchange	Конфигурация Центра администрирования Exchange на серверах почтовых ящиков
2 дня (`2.00:00:00`)	Командлет: **Set-TransportService** Параметр *: MessageExpirationTimeOut*	**Серверов**> Выберите сервер >**Изменить** (✎) >**Ограничения**> транспорта Раздел >**Срок действия сообщения— максимальное время с момента отправки (в днях)**

Завершение срока действия сообщений вручную

Несмотря на то что вам не удастся вручную принудительно завершить срок действия сообщения, вы можете вручную удалить сообщение из любой очереди (за исключением очереди передачи) с созданием отчета о недоставке или без него. Дополнительные сведения см. в разделе Удаление сообщений из очередей.

Настройка интервалов повтора, повторной отправки и истечения срока действия сообщений в Exchange Server

Статья • 04.04.2023

В Exchange Server можно настроить интервалы повторных попыток, повторной отправки и истечения срока действия сообщений в транспортной службе на серверах почтовых ящиков и пограничных транспортных серверах. Подробное описание этих параметров см. в статье Повторная попытка сообщения, повторная отправка и интервалы истечения срока действия.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: менее 5 минут
- Центр администрирования Exchange (EAC) можно использовать только на серверах почтовых ящиков. Дополнительные сведения о EAC см. в разделе Центр администрирования Exchange в Exchange Server. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записях "Транспортная служба" и "Пограничные транспортные серверы" раздела Разрешения потока обработки почты .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование файла EdgeTransport.exe.config для настройки количества повторных попыток при ошибках очереди, интервала между повторными попытками при ошибках очереди, интервала между повторными попытками для очереди доставки почтового ящика и максимального времени простоя перед повторной отправкой.

- **Число повторных** попыток сбоя очереди. Количество попыток подключения, которые были немедленно предприняты, когда у транспортной службы возникли проблемы при подключении к целевому серверу. Обычно нет необходимости изменять этот параметр. Исключение составляют случаи, когда сеть ненадежна, и в ней регулярно происходят случайные разрывы подключений.

- **Интервал повторных попыток сбоя очереди**. Интервал между каждой повторными попытками сбоя очереди. Обычно нет необходимости изменять этот параметр. Исключение составляют случаи, когда сеть ненадежна, и в ней регулярно происходят случайные разрывы подключений.

- **Интервал повторных попыток очереди доставки почтового ящика**: как часто очередь пытается подключиться к службе доставки транспорта почтовых ящиков для целевой базы данных почтовых ящиков, к которому не удается успешно подключиться.

- **Максимальное время простоя перед повторной отправкой**. Как долго незавершенные сообщения в очередях доставки состояние Retry ожидается перед повторной отправкой.

Чтобы настроить эти интервалы, измените соответствующие параметры в XML-файле конфигурации %ExchangeInstallPath%Bin\EdgeTransport.exe.config приложения на серверах почтовых ящиков или на пограничных транспортных серверах. Изменения, вносимые в этот файл, будут применены после перезапуска службы транспорта Exchange. Когда вы перезапустите эту службу, выполнение потока обработки почты на сервере будет временно прервано.

> ⓘ **Примечание**
>
> Все настраиваемые параметры Exchange или IIS, внесенные в файлы конфигурации приложения Exchange XML на сервере Exchange Server (например, web.config файлы или EdgeTransport.exe.config файл), **будут перезаписаны** при установке exchange CU. Обязательно сохраните эти сведения, чтобы можно было легко повторно применить параметры после установки. После установки exchange CU необходимо повторно настроить эти параметры.

1. В окне командной строки на сервере почтовых ящиков или пограничном транспортном сервере откройте файл EdgeTransport.exe.config в Блокноте, выполнив следующую команду:

   Консоль

   ```
   Notepad %ExchangeInstallPath%Bin\EdgeTransport.exe.config
   ```

2. Найдите следующие ключи в `<appSettings>` разделе.

   XML

   ```
   <add key="QueueGlitchRetryCount" value="<Integer>" />
   <add key="QueueGlitchRetryInterval" value="<hh:mm:ss>" />
   <add key="MailboxDeliveryQueueRetryInterval" value="<hh:mm:ss>" />
   <add key="MaxIdleTimeBeforeResubmit" value="<hh:mm:ss>" />
   ```

   В этом примере изменяется значение количества повторных попыток очереди при сбое на 6, интервал повторных попыток очереди при сбое на 30 секунд, интервал между повторными попытками для очереди доставки в почтовые ящики на 3 минуты, а максимальное время простоя перед интервалами повторной передачи — на 6 часов.

   XML

   ```
   <add key="QueueGlitchRetryCount" value="6" />
   <add key="QueueGlitchRetryInterval" value="00:00:30" />
   <add key="MailboxDeliveryQueueRetryInterval" value="00:03:00" />
   <add key="MaxIdleTimeBeforeResubmit" value="6:00:00" />
   ```

3. После внесения изменений сохраните и закройте файл EdgeTransport.exe.config.

4. Перезапустите службу транспорта Exchange, выполнив следующую команду:

```
Консоль

net stop MSExchangeTransport && net start MSExchangeTransport
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы настроили эти интервалы, выполните указанные ниже действия.

1. Откройте файл EdgeTransport.exe.config в Блокноте, выполнив следующую команду:

```
Консоль

Notepad %ExchangeInstallPath%Bin\EdgeTransport.exe.config
```

2. Проверьте значения следующих ключей `<appSettings>` в разделе.

```
XML

<add key="QueueGlitchRetryCount" value="<Integer>" />
<add key="QueueGlitchRetryInterval" value="<hh:mm:ss>" />
<add key="MailboxDeliveryQueueRetryInterval" value="<hh:mm:ss>" />
<add key="MaxIdleTimeBeforeResubmit" value="<hh:mm:ss>" />
```

Настройка количества повторных попыток при временных ошибках, интервала между повторными попытками при временных ошибках и интервала между повторными попытками при ошибке исходящего подключения

- **Повторные попытки с временным сбоем**. Количество попыток подключения, которые были предприняты после неудачных попыток подключения, контролируемых ключами *QueueGlitchRetryCount* и *QueueGlitchRetryInterval* . Допустимое значение от 0 до 15, а значение по умолчанию — 6. Если задать

значение 0, то следующая попытка подключения управляется интервалом повтора сбоя исходящего подключения.

- **Интервал повторных попыток с временным сбоем**. Интервал между каждой временной попыткой повтора сбоя. По умолчанию на серверах почтовых ящиков используется значение 5 минут. По умолчанию на пограничных транспортных серверах используется значение 10 минут.

- **Интервал повторных попыток сбоя исходящего подключения: интервал** повтора для попыток исходящего подключения, которые ранее завершились сбоем (временные попытки неудачных попыток и интервал повторных попыток временного сбоя). По умолчанию на серверах почтовых ящиков используется значение 10 минут. По умолчанию на пограничных транспортных серверах используется значение 30 минут.

Использование Центра администрирования Exchange для настройки количества повторных попыток при временной ошибке, интервала между повторными попытками при временной ошибке или интервала между повторными попытками при ошибке исходящего подключения на серверах почтовых ящиков

1. В EAC перейдите в раздел **Серверы Серверы**>, выберите сервер и нажмите кнопку **Изменить**.

2. На открывшейся странице свойств сервера щелкните **Ограничения транспорта**.

3. В разделе **Повторные попытки** введите значение для любого из указанных ниже параметров.

    - **Интервал повторной попытки при ошибке исходящего подключения (секунд)**

    - **Интервал повтора при временной ошибке (в минутах)**

    - **Количество повторных попыток при временной ошибке**

    По завершении нажмите кнопку **Сохранить**.

Использование командной консоли Exchange для настройки количества повторных попыток при временной ошибке, интервала между повторными попытками при временной ошибке и интервала между повторными попытками при ошибке исходящего подключения на серверах почтовых ящиков или пограничных транспортных серверах

Чтобы настроить интервалы в службе транспорта на серверах почтовых ящиков или пограничных транспортных серверах, выполните следующую команду:

PowerShell

```
Set-TransportService -Identity <ServerIdentity> -TransientFailureRetryCount
<Integer> -TransientFailureRetryInterval <hh:mm:ss> -
OutboundConnectionFailureRetryInterval <dd.hh:mm:ss>
```

Чтобы настроить интервалы в службе транспорта внешнего интерфейса на серверах почтовых ящиков, выполните следующую команду:

PowerShell

```
Set-FrontEndTransportService -Identity <ServerIdentity> -
TransientFailureRetryCount <Integer> -TransientFailureRetryInterval
<hh:mm:ss>
```

В этом примере показано, как изменить указанные ниже значения на сервере почтовых ящиков с именем Mailbox01.

- Количество повторных попыток при временной ошибке равно 8.
- Интервал повторной попытки при временной ошибке равен 1 минуте.
- Интервал повторной попытки при ошибке исходящего подключения равен 45 минутам.

PowerShell

```
Set-TransportService -Identity Mailbox01 -TransientFailureRetryCount 8 -
TransientFailureRetryInterval 00:01:00 -
OutboundConnectionFailureRetryInterval 00:45:00
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы настроили эти интервалы, выполните одно из указанных ниже действий.

- На сервере почтовых ящиков откройте EAC и выберите **Серверы**>**Серверы**, выберите сервер и щелкните **Изменить**. В открывшемся окне свойств сервера щелкните **Ограничения транспорта** и проверьте значения в разделе **Повторные попытки**.

- Чтобы проверить значения свойств, в командной консоли Exchange на сервере почтовых ящиков или на пограничном транспортном сервере, выполните следующую команду:

  PowerShell

  ```
  Get-TransportService | Format-List
  Name,TransientFailureRetry*,OutboundConnectionFailureRetryInterval
  ```

- Чтобы проверить значения свойств, в командной консоли Exchange на сервере почтовых ящиков, выполните следующую команду:

  PowerShell

  ```
  Get-FrontEndTransportService | Format-List Name,TransientFailureRetry*
  ```

Использование командной консоли Exchange для настройки интервала между повторными попытками доставки сообщения

Параметр интервала между повторными попытками доставки сообщения определяет время ожидания между попытками отправки для отдельных сообщений в очередях с состоянием Retry (Повторная попытка). Значение по умолчанию — 15 минут, и мы рекомендуем не изменять значение по умолчанию, если вам не порекомендует служба поддержки майкрософт или документация по конкретному продукту.

Чтобы настроить интервал между повторными попытками доставки сообщения, выполните следующую команду:

PowerShell

```
Set-TransportService -Identity <ServerIdentity> -MessageRetryInterval
<dd.hh:mm:ss>
```

В этом примере показано, как изменить параметр интервала между повторными попытками доставки сообщения и задать для него значение 20 минут на сервере почтовых ящиков с именем Mailbox01.

PowerShell

```
Set-TransportService -Identity Mailbox01 -MessageRetryInterval 00:20:00
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы настроили параметр интервала между повторными попытками доставки сообщения на сервере почтовых ящиков или пограничном транспортном сервере, выполните указанную команду в командной консоли Exchange и проверьте значение свойства **MessageRetryInterval**.

PowerShell

```
Get-TransportService | Format-List Name,MessageRetryInterval
```

Настройка параметров времени ожидания для уведомления о задержке доставки сообщения

- **Интервал ожидания уведомления об уведомлениях о задержке DSN**. Сколько времени следует ждать, прежде чем отправлять сообщения о задержке DSN отправителям. Этот параметр применяется к службе транспорта на сервере почтовых ящиков или на пограничном транспортном сервере.

Примечание. Это значение всегда должно быть больше произведения количества повторных попыток при временной ошибке и длительности интервала между повторными попытками при временной ошибке (по умолчанию используется общее значение 30 минут для сервера почтовых ящиков и 1 час для пограничного транспортного сервера).

- **Внутренние и внешние параметры DSN задержки**. Указывает, могут ли отправляться сообщения DSN задержки внутренним или внешним отправителям сообщений (отправителям, которые находятся в организации Exchange или за ее пределами). Этот параметр применяется к службе транспорта на сервере почтовых ящиков в организации.

Использование Центра администрирования Exchange для настройки времени ожидания перед отправкой уведомления о задержке доставки сообщения на серверах почтовых ящиков

1. В EAC щелкните **Серверы**>**Серверы**, выберите сервер и нажмите кнопку **Изменить**.

2. На открывшейся странице свойств сервера щелкните **Ограничения транспорта**.

3. В разделе **Уведомления** введите значение для параметра **Уведомить отправителя в случае задержки сообщения через (часов)**, а затем нажмите кнопку **Сохранить**.

Использование командной консоли Exchange для настройки времени ожидания перед отправкой уведомления о задержке доставки сообщения на серверах почтовых ящиков или пограничных транспортных серверах

Чтобы настроить время ожидания перед отправкой уведомления о задержке доставки сообщения, выполните следующую команду:

PowerShell

```
Set-TransportService -Identity <ServerIdentity> -DelayNotificationTimeout
<dd.hh:mm:ss>
```

В этом примере показано, как изменить параметр времени ожидания перед отправкой уведомления о задержке доставки сообщения и задать для него значение 6 часов на сервере почтовых ящиков с именем Mailbox01.

PowerShell

```
Set-TransportService -Identity Mailbox01 -DelayNotificationTimeout 06:00:00
```

Использование командной консоли Exchange для включения или отключения функции отправки уведомления о задержке доставки сообщений внешним или внутренним отправителям сообщений

Чтобы настроить параметры уведомлений о задержке доставки сообщений, выполните следующую команду:

PowerShell

```
Set-TransportConfig -ExternalDelayDSNEnabled <$true | $false> -
InternalDelayDSNEnabled <$true |$false>
```

В этом примере запрещается отправка уведомлений о состоянии задержанной доставки внешним отправителям.

PowerShell

```
Set-TransportConfig -ExternalDelayDSNEnabled $false
```

В этом примере запрещается отправка уведомлений о состоянии задержанной доставки внутренним отправителям.

PowerShell

```
Set-TransportConfig -InternalDelayDSNEnabled $false
```

Как проверить, что все получилось?

Чтобы убедиться, что вы настроили параметры уведомлений о задержке доставки сообщений, выполните одно из указанных ниже действий.

- На сервере почтовых ящиков откройте EAC и выберите **Серверы**>**Серверы**, выберите сервер и щелкните **Изменить**. В открывшемся окне свойств сервера щелкните **Ограничения транспорта** и проверьте значение параметра **Уведомить отправителя в случае задержки сообщения через (часов)** в разделе **Уведомления**.

- Чтобы проверить значения свойств, в командной консоли Exchange на сервере почтовых ящиков или на пограничном транспортном сервере выполните следующие команды:

```
PowerShell
```

```
Get-TransportService | Format-List Name,DelayNotificationTimeout
```

```
PowerShell
```

```
Get-TransportConfig | Format-List *DelayDSNEnabled
```

Настройка времени ожидания перед завершением срока действия сообщения

Параметр времени ожидания перед завершением срока действия сообщения указывает, какое время необходимо подождать, прежде чем можно будет завершить срок действия сообщения и возвратить его отправителю в отчете о недоставке (сообщении о недоставке). Этот параметр применяется к службе транспорта на сервере почтовых ящиков или на пограничном транспортном сервере.

Использование Центра администрирования Exchange для настройки времени ожидания перед завершением срока действия сообщения на серверах почтовых ящиков

1. В EAC щелкните **Серверы**>**Серверы**, выберите сервер и нажмите кнопку **Изменить**.

2. На открывшейся странице свойств сервера щелкните **Ограничения транспорта**.

3. В разделе **Срок действия сообщения** введите значение для параметра **Максимальное время с момента отправки (дней)**, а затем нажмите кнопку **Сохранить**.

Использование командной консоли Exchange для настройки времени ожидания перед завершением

срока действия сообщения на серверах почтовых ящиков или пограничных транспортных серверах

Чтобы настроить время ожидания перед завершением срока действия сообщения, выполните указанную ниже команду.

PowerShell

```
Set-TransportService -Identity <ServerIdentity> -MessageExpirationTimeout
<dd.hh:mm:ss>
```

В этом примере показано, как изменить параметр времени ожидания перед завершением срока действия сообщения и задать для него значение 4 дня на сервере Exchange с именем Mailbox01.

PowerShell

```
Set-TransportService -Identity Mailbox01 -MessageExpirationTimeout
4.00:00:00
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы настроили параметр времени ожидания перед завершением срока действия сообщения, выполните одно из указанных ниже действий.

- На сервере почтовых ящиков откройте EAC и выберите **Серверы**>**Серверы**, выберите сервер и щелкните **Изменить**. В открывшемся окне свойств сервера щелкните **Ограничения транспорта** и проверьте значение параметра **Максимальное время с момента отправки (дней)** в разделе **Срок действия сообщения**.
- Чтобы проверить значения свойства **MessageExpirationTimeout**, в командной консоли Exchange на сервере почтовых ящиков или на пограничном транспортном сервере выполните следующую команду:

  PowerShell

  ```
  Get-TransportService | Format-List Name,MessageExpirationTimeout
  ```

DSN и NDR в Exchange Server

Статья • 04.04.2023

Если возникает проблема с доставкой сообщения, Exchange отправляет отправителю сообщение о недоставки, указывающее на наличие проблемы. NDR включают код, указывающий, почему сообщение не было доставлено, и возможные решения для доставки сообщения.

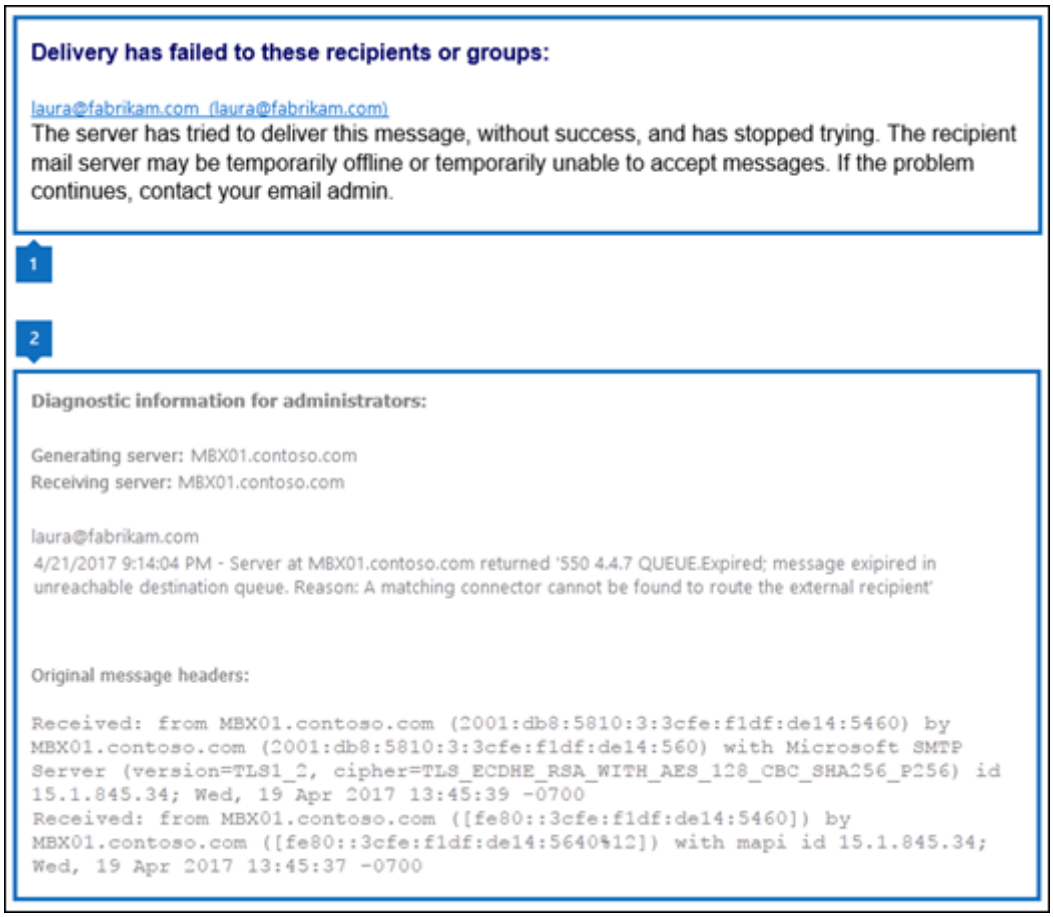
Сведения, включенные в отчеты о недоставке, составлены так, чтобы они были понятны и полезны как для пользователей, так и для администраторов. В некоторых случаях отправители могут самостоятельно определить и устранить проблемы (например, в случае опечатки в электронном адресе получателя). В других случаях может потребоваться, чтобы администратор устранил проблему в среде Exchange либо уведомил администраторов в домене назначения о проблемах в их средах обмена сообщениями.

Процедуры, связанные с NDR в Exchange Server, см. в разделе Процедуры для DSN и NDR в Exchange Server.

Если вам нужна помощь с отчетами о недоставке в Microsoft 365, Office 365 или Exchange Online, см. Email отчеты о недоставке в Exchange Online.

Сведения в отчетах о недоставке

Ниже показан пример отчета о недоставке.



Сведения в отчете о недоставке разделены на два указанных ниже раздела.

1. **Раздел сведений о пользователе**. Этот раздел появляется первым и пытается объяснить (в нетехнических терминах) причину сбоя доставки сообщения и возможные шаги для успешной доставки сообщения.

    - Текст, отображаемый в этом разделе, вставляет сервер Exchange, создавший отчет о недоставке.
    - Если возможно, в раздел сведений для пользователя включается полное доменное имя (FQDN) сервера, отклонившего сообщение (например, mbx01.contoso.com).
    - Если не удалось доставить сообщение нескольким получателям, будут указаны электронный адрес и причина недоставки для каждого получателя.

2. **Раздел Диагностические сведения для администраторов**. В этом разделе содержатся более подробные технические сведения, которые помогут администраторам устранить проблемы, вызвавшие сбой доставки.

    Основная информация в этом разделе — расширенный код состояния (например, 4.4.7).

- Расширенный код состояния возвращается сервером, который создал отчет о недоставке (исходный сервер, которому не удалось доставить сообщение, или сервер назначения, который отклонил сообщение).

- От расширенного кода состояния зависит текст, отображаемый в разделе сведений для пользователя (Exchange не изменяет значение кода).

Командлет **New-SystemMessage** в командной консоли Exchange можно использовать для изменения текста, который отображается в разделе сведений о пользователе для заданного расширенного кода состояния (включая различные тексты на разных языках). Создав настраиваемые пояснения, вы можете предоставить определенный контент для своей среды, например контактные данные службы технической поддержки или ссылки на интрасеть для самостоятельного устранения неполадок. Дополнительные сведения см. в разделе Процедуры для dsn и NDR в Exchange Server.

- В разделе Стандартные расширенные коды состояния этой статьи рассказывается, что означают определенные числа, указаны коды, с которыми вы, вероятно, столкнетесь, а также имеются предложения по устранению причин проблем, из-за которых сообщение не было доставлено.

В этом разделе также содержатся указанные ниже сведения.

- **Создание сервера**. Сервер обмена сообщениями, создавший NDR. Если удаленный сервер не указан под электронным адресом отправителя, создающий сервер также будет сервером, который отклонил исходное письмо. Если доставка сообщений между отправителями и получателями в организации Exchange завершается сбоем, один и тот же сервер обычно отклоняет исходное сообщение и создает отчет о недоставке.

- **Отклоненные получатели**: адрес электронной почты получателя в исходном сообщении, которое не удалось доставить. Если не удается доставить сообщение нескольким получателям, в списке будет отображен электронный адрес каждого получателя. Это поле также содержит указанные ниже вложенные поля для каждого электронного адреса.

- **Удаленный сервер**. Полное доменное имя сервера, который отклонил исходное сообщение во время передачи SMTP (сбой доставки после отправки текста сообщения, но до того, как сервер подтвердил получение сообщения). Это поле не отображается в указанных ниже случаях.

- Сервер, отклонивший сообщение, также создал отчет о недоставке. Такое обычно случается при недоставке сообщений от отправителей получателям в одной и той же организации Exchange.
- Удаленный сервер подтвердил получение исходного сообщения, но сообщение было отклонено по другим причинам (например, из-за ограничений, связанных с контентом).
- **Расширенный код состояния**
- **Ответ SMTP**: текстовая строка US-ASCII, возвращенная сервером обмена сообщениями, который отклонил исходное сообщение. Обычно это краткое описание расширенного кода состояния. Эта строка не переписывается Exchange.
- **Исходные заголовки сообщений**. Эта область содержит заголовок сообщения, отклоненного. В этих полях заголовков могут содержаться полезные диагностические сведения (например, о прыжках сервера в пути маршрутизации сообщения либо о том, совпадает ли значение в поле **Кому:** с электронным адресом отклоненного получателя).

Стандартные расширенные коды состояния

Расширенные коды состояния определяются в RFC 3463 и используют *класс*> *синтаксиса*<. <*subject*>. <*detail*>:

- <*класс*>: **4** указывает на временную ошибку доставки. Код **5** свидетельствует о постоянной ошибке доставки.
- <*subject*>: RFC классифицирует значения следующим образом:
  - **1**. Адресация
  - **2**. Почтовый ящик (получатель)
  - **3**: почтовая система (почтовая система назначения)
  - **4**. Сеть и маршрутизация
  - **5**. Протокол доставки почты
  - **7**. Безопасность или политика
- <*detail*>: число от 1 до 3 цифр, которое дополнительно классифицирует ошибку.

В таблицах ниже перечислены расширенные коды состояний, которые возвращаются в отчетах о недоставке в наиболее распространенных случаях недоставки сообщений.

> ⓘ **Примечание**
>
> Сведения о расширенных кодах состояния в Microsoft 365 или Office 365 и гибридных средах см. **в статье Email отчетов о недоставке в Exchange Online**.

Временные сбои, ставшие причиной недоставки

Расширенный код состояния	Описание	Возможные причины и решения
4.3.1	`Insufficient system resources`	Свободное место на диске невелико (например, на диске, на котором хранится база данных очередей, нет необходимого объема свободного места). Дополнительные сведения см. в разделе Общие сведения о давлении на спину. Сведения о перемещении базы данных очереди на другой диск см. в статье Изменение расположения базы данных очереди. Доступной памяти недостаточно (например, Exchange установлен на виртуальной машине, настроенной для использования динамической памяти). Всегда используйте статическую память на виртуальных машинах Exchange. Дополнительные сведения см. в разделе Требования и рекомендации относительно памяти Exchange.

Расширенный код состояния	Описание	Возможные причины и решения
4.3.2	`Service not available` или `Service not active`	Вы настроили пользовательский соединитель получения в службе транспорта (концентратора) на сервере почтовых ящиков, который прослушивает порт 25. Обычно пользовательские соединители получения, прослушивающие порт 25, принадлежат службе транспорта внешнего интерфейса на сервере почтовых ящиков. Важные серверные компоненты Exchange неактивны. Это можно подтвердить, выполнив следующую команду в командной консоли Exchange: `Get-ServerComponent -Identity <ServerName>`. Чтобы перезапустить все неактивные компоненты, выполните следующую команду: `Set-ServerComponentState -Identity <ServerName> -Component ServerWideOffline -State Active -Requester Maintenance`. Несовместимые агенты транспорта (в частности, после обновления Exchange). После того как вы идентифицируете агент транспорта, отключите или удалите его. Дополнительные сведения см. в разделе Устранение неполадок агентов транспорта.
4.4.1	`Connection timed out`	Временные проблемы с сетью, которые могут исчезнуть без постороннего вмешательства. Сервер Exchange периодически пытается подключиться к серверу назначения, чтобы доставить сообщение. После нескольких неудачных попыток сообщение возвращено отправителю в отчете о недоставке с указанием кода постоянной ошибки. Дополнительные сведения о настройке интервалов повторных попыток и сбоев для очереди см. в разделе Настройка интервалов повторной отправки, повторной передачи и истечения срока действия сообщений. Сведения о том, как вручную повторить попытку для очереди, см. в разделе Повторный запуск очередей. Ограничения, накладываемые брандмауэром или поставщиком услуг Интернета на TCP-порт 25.

Расширенный код состояния	Описание	Возможные причины и решения
4.4.2	`Connection dropped`	Временные проблемы с сетью или проблемы с сервером, которые могут исчезнуть без постороннего вмешательства. Отправляющий сервер будет повторно пытаться доставить сообщение и создавать дальнейшие отчеты о состоянии. Достигнут предельный размер сообщения для подключения либо скорость отправки сообщений для исходного IP-адреса превысила настроенное предельное значение. Дополнительные сведения см. в разделе Ограничения скорости сообщений и регулирование. Не удается доставить почту на сервер Exchange из-за проблем, связанных с конфигурацией защиты от нежелательной почты, прокси SMTP или брандмауэра.

Расширенный код состояния	Описание	Возможные причины и решения
4.4.7	`Message delayed` или `Queue expired; Message expired`	Проблемы, связанные с конфигурацией соединителя отправки. Примеры: • соединитель оправки настроен так, чтобы использовать маршрутизацию DNS, в то время как он должен использовать маршрутизацию промежуточного узла, или наоборот. Используйте программу nslookup, чтобы проверить, доступен ли домен назначения с сервера Exchange. • Полное доменное имя, которое соединитель отправки предоставляет запросам HELO или EHLO, не соответствует имени узла в записи MX (например, mail.contoso.com). Некоторые системы обмена сообщениями настроены для сравнения этих значений, чтобы уменьшить количество нежелательных сообщений. Значение по умолчанию в соединителе отправки пустое, что означает, что используется полное доменное имя сервера Exchange (например, exchange01.contoso.com). На сервере назначения не запущена служба доставки транспорта почтовых ящиков (из-за чего не удается доставить сообщение в почтовый ящик). В конечной системе обмена сообщениями имеются проблемы, связанные с сообщениями в формате TNEF (который также называется RTF в Outlook). Пример: приглашения на собрания или сообщения с изображениями, внедренными в текст сообщения. Если домен назначения использует инфраструктуру политики отправителей для проверки источников сообщений, то в вашем домене могут быть связанные с ней проблемы (например, запись инфраструктуры политики отправителей может не включать все источники почты для вашего домена).

Постоянные сбои, ставшие причиной недоставки

Расширенный код состояния	Описание	Возможные причины и решения

Расширенный код состояния	Описание	Возможные причины и решения
5.1.0	`Sender denied`	Ответы на старые сообщения либо на сообщения, экспортированные в виде файлов (в этом случае могли измениться важные атрибуты получателей). Убедитесь, что адрес получателя указан правильно. Неправильный или отсутствующий атрибут в записях контактов. Отправитель заблокирован системой фильтрации отправителей (непосредственно либо отправитель находится в списке заблокированных отправителей пользователя, и агент фильтра отправителей настроен так, чтобы использовать объединение списков надежных отправителей. Дополнительные сведения см. в статьях Фильтрация отправителей и Агрегирование списков безопасности.

5.1.1	`RESOLVER.ADR.ExRecipNotFound; not found`
	или
	`User unknown`
		Неправильный электронный адрес получателя (получатель не существует в конечной системе обмена сообщениями). Проверьте электронный адрес получателя.
		Вы восстановили удаленный почтовый ящик, и внутренние пользователи обращаются к письмам в Outlook или в Outlook в Интернете, используя старые записи в кэше автозаполнения (теперь значения X.500 или значения **LegacyExchangeDN** для получателя другие). Попросите пользователей удалить запись из кэша автозаполнения и выберите получателя еще раз.

5.1.3	`STOREDRV.Submit; invalid recipient address`	Неправильный электронный адрес получателя (например, электронный адрес содержит неподдерживаемые символы или недопустимое форматирование).

Расширенный код состояния	Описание	Возможные причины и решения
5.1.4	`Recipient address reserved by RFC 2606`	Соединители получения отклоняют SMTP-подключения, содержащие домены верхнего уровня, определенные в RFC 2606 (.test, .example, .invalid или .localhost). Это поведение управляется параметром *RejectReservedTopLevelRecipientDomains* командлетовNew-ReceiveConnector и Set-ReceiveConnector .
5.1.5	`Recipient address reserved by RFC 2606`	Соединители получения отклоняют подключения SMTP, которые содержат домены второго уровня, определенные в стандарте RFC 2606 (example.com, example.net или example.org). Это поведение управляется параметром *RejectReservedSecondLevelRecipientDomains* командлетовNew-ReceiveConnector и Set-ReceiveConnector .
5.1.6	`Recipient addresses in single label domains not accepted`	Соединители получения отклоняют SMTP-подключения, содержащие домены с одной меткой (например, chris@contoso вместо chris@contoso.com) Это поведение управляется *параметром RejectSingleLabelRecipientDomains* командлетовNew-ReceiveConnector и Set-ReceiveConnector .
5.1.7	`Invalid address` или `Unknown sender address`	Имеется проблема, связанная с электронным адресом отправителя. Проверьте электронный адрес отправителя.
5.1.8	`Access denied, bad outbound sender`	Отправитель превысил ограничение скорости сообщений (например, сервер приложений настроен для ретрансляции большого количества сообщений через Exchange). Дополнительные сведения см. в разделах Ограничения скорости сообщений и регулирование и Разрешить анонимный ретранслятор на серверах Exchange.

Расширенный код состояния	Описание	Возможные причины и решения
5.2.1	`Content Filter agent quarantined this message`	Функция фильтрации содержимого поместила сообщение в карантин. Сведения о том, как настроить исключения для функции фильтрации содержимого, см. в разделе Настройка исключений получателей и отправителей для функции фильтрации содержимого с помощью командной консоли Exchange.
5.2.2	`Mailbox full`	Превышена квота хранилища для почтового ящика получателя, и почтовому ящику не удается принимать новые сообщения. Дополнительные сведения о настройке квот почтовых ящиков см. в разделе Настройка квот хранилища для почтового ящика.
5.2.3	`RESOLVER.RST.RecipSizeLimit; message too large for this recipient`	Сообщение слишком велико. Еще раз отправьте сообщение, но без вложений либо увеличьте предельное значение размера сообщений для получателя. Дополнительные сведения см. в разделе Ограничения для получателей.
5.3.0	`Too many related errors`	Обнаружено, что сообщение имеет неправильный формат и было перемещено в очередь подозрительных сообщений. Дополнительные сведения см. в разделе Типы очередей.
5.3.2	`STOREDRV.Deliver: Missing or bad StoreDriver MDB properties`	Вы используете агент маршрутизации политики адресных книг (ABP), а получателя нет в глобальном списке адресов, указанном в этой политике. Дополнительные сведения см. в статье Использование командной консоли Exchange для установки и настройки политик маршрутизации политики адресной книги и политик адресной книги в Exchange Server.

Расширенный код состояния	Описание	Возможные причины и решения
5.3.3	`Unrecognized command`	Соединители получения, используемые для внутреннего потока обработки почты, не имеют необходимого Exchange Server механизма проверки подлинности. Дополнительные сведения о проверке подлинности в соединителях получения см. в разделе Механизмы проверки подлинности соединителя получения.
5.3.4	`Message size exceeds fixed maximum message size`	Сообщение слишком велико. Эта ошибка может возникнуть как в исходной, так и в конечной системе обмена сообщениями. Еще раз отправьте сообщение, но без вложений либо увеличьте предельное значение размера сообщений. Дополнительные сведения см. в статье Размер сообщений и ограничения получателей в Exchange Server.
5.3.5	`System incorrectly configured`	Обнаружен почтовый цикл. Убедитесь, что свойство **FQDN** в соединителе получения не совпадает с FQDN другого сервера, службы или устройства, используемого в потоке обработки почты в организации (по умолчанию соединитель получения использует FQDN сервера Exchange).

Расширенный код состояния	Описание	Возможные причины и решения
5.4.4	`SMTPSEND.DNS.NonExistentDomain; nonexistent domain`	Имеется проблема, связанная с DNS или конфигурацией сетевого адаптера на сервере Exchange. Проверьте внутренние и внешние параметры подстановки DNS для Exchange, выполнив следующую команду в командной консоли Exchange: Get-TransportService | Format-List name,ExternalDNS*,InternalDNS*; Get-FrontEndTransportService | Format-List name,ExternalDNS*,InternalDNS*' Эти параметры можно настроить с помощью параметров *InternalDNS** и *ExternalDNS** в командлетах **Set-TransportService** и **Set-FrontEndTransportService** . По умолчанию эти параметры используются соединителями отправки (значение по умолчанию параметра *UseExternalDNSServersEnabled* — `$false`). Проверьте приоритет (порядок) сетевых адаптеров в операционной системе сервера Exchange.

Расширенный код состояния	Описание	Возможные причины и решения
5.4.6	`Hop count exceeded - possible mail loop`	Ошибка конфигурации привела к созданию почтового цикла. По умолчанию после 20 итераций почтового цикла Exchange прерывает цикл и создает отчет о недоставке. Убедитесь, что это не связано с правилами папки "Входящие" для получателя и отправителя либо с правилами переадресации в почтовом ящике получателя (сообщение создает сообщение, которое, в свою очередь, создает еще одно сообщение, и этот процесс продолжается бесконечно). Убедитесь, что у почтового ящика нет значения свойства **targetAddress** в Active Directory (это свойство соответствует параметру *ExternalEmailAddress для почтовых* пользователей в Exchange). Если вы удаляете серверы Exchange или изменяете параметры, связанные с маршрутизацией почты, обязательно перезапустите службы транспорта Microsoft Exchange и службы транспорта переднего плана Exchange.
5.5.2	`Send hello first`	Нарушена последовательность отправки команд SMTP (например, сервер отправляет команду SMTP AUTH или MAIL FROM, прежде чем идентифицировать себя с помощью команды EHLO). После создания подключения к серверу обмена сообщениями первой командой SMTP обязательно должна быть команда EHLO или HELO.
5.5.3	`Too many recipients`	Общее количество получателей, указанных в строках "Кому", "Копия" и "СК", превышает количество получателей, разрешенное в одном сообщении для организации, соединителя получения или отправителя. Дополнительные сведения см. в статье Размер сообщений и ограничения получателей в Exchange Server.

Расширенный код состояния	Описание	Возможные причины и решения
5.7.1	`Unable to relay` или `Client was not authenticated`	У вас есть сервер приложений или устройство, которое пытается ретранслировать сообщения через Exchange. Дополнительные сведения см. в статье Allow anonymous relay on Exchange servers. Получатель настроен так, чтобы принимать сообщения только от отправителей, прошедших проверку подлинности (обычно это внутренние отправители). Дополнительные сведения см. в статье Настройка ограничений доставки сообщений для почтового ящика.
5.7.3	`Cannot achieve Exchange Server authentication` или `Not Authorized`	Брандмауэр или другое устройство блокирует расширенную команду SMTP, которая необходима для проверки подлинности Exchange Server (X-EXPS). Внутренний почтовый трафик проходит через соединители, которые не настроены для использования метода проверки подлинности Exchange Server. Проверьте диапазоны удаленных IP-адресов на любом настраиваемом соединителе получения.
5.7.900 по 5.7.999	`Delivery not authorized, message refused`	Сообщение было отклонено из-за правила потока обработки почты (также называемого правилом транспорта). Этот диапазон расширенных кодов состояния доступен, если правило настроено так, чтобы отклонять сообщения (в противном случае код, используемый по умолчанию, — 5.7.1). Дополнительные сведения см. в статье Действия правил потока обработки почты в Exchange Server.

Процедуры для dsn и NDR в Exchange Server

Статья • 04.04.2023

Как и в предыдущих версиях Exchange, Exchange Server использует уведомления о состоянии доставки (также известные как dsn, отчеты о недоставке, недоставки или сообщения о недоставке) для предоставления отправителям сообщений о состоянии доставки и уведомления о сбое. Дополнительные сведения о NDR см. в разделе DSN и NDR в Exchange Server.

Вы можете пользоваться стандартными отчетами о недоставке, которые включены в Exchange, или можете использовать Командная консоль Exchange для создания отчетов о недоставке с настраиваемым текстом в соответствии с потребностями вашей организации. Настраиваемый текст заменяет стандартный текст в отчете о недоставке для определенного расширенного кода состояния или события квоты. При удалении настраиваемого отчета о недоставке в отчетах снова используется стандартный текст (стандартный отчет о недоставке полностью удалить невозможно). Вы также можете отключить настраиваемые отчеты о недоставке, чтобы сохранить, но не использовать их (в отчетах снова используется стандартный текст).

Что нужно знать перед началом работы?

- Предполагаемое время для завершения каждой процедуры: менее 10 минут.
- Основное внимание в этом разделе уделяется пользовательскому тексту NDR, который заменяет текст NDR по умолчанию, используемых Exchange. Вы можете создать новые NDR для других расширенных значений кода состояния (например, 5.999.999), но никто не увидит эти NDR, если расширенный код состояния не используется Exchange. Вы можете использовать ряд настраиваемых расширенных кодов состояния в рамках действия для правила потока обработки почты (также известного как правило транспорта). Дополнительные сведения см. в статье Действия правил потока обработки почты в Exchange Server.
- Процедуры, описанные в этой статье, доступны на серверах почтовых ящиков и пограничных транспортных серверах.
- Вы не можете использовать Центр администрирования Exchange (EAC) для большинства процедур, описанных в этом разделе. Необходимо использовать

командную консоль Exchange. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "DSN" в разделе Разрешения потока обработки почты .

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование Командная консоль Exchange для просмотра всех стандартных отчетов о недоставке

Чтобы записать список всех стандартных отчетов о недоставке на всех языках в HTML-файл C:\My Documents\Default NDRs.html, выполните следующую команду:

PowerShell

```
Get-SystemMessage -Original | Select-Object -Property
Identity,DsnCode,Language,Text | ConvertTo-Html | Set-Content -Path "C:\My
Documents\Default NDRs.html"
```

Примечание. Список следует записать в файл, поскольку он очень длинный, и, если у вас не установлены необходимые языковые пакеты, будут возникать ошибки.

Подробные сведения о синтаксисе и параметрах см. в разделе Get-SystemMessage.

Использование Командная консоль Exchange для просмотра настраиваемых отчетов о недоставке

Чтобы просмотреть сводный список всех настраиваемых отчетов о недоставке в организации, выполните следующую команду:

```
PowerShell

Get-SystemMessage
```

Примечание. Настраиваемых отчетов о недоставке по умолчанию не существует, поэтому данная команда не возвращает никаких результатов.

Чтобы просмотреть подробную информацию о настраиваемом отчете о недоставке, используйте следующий синтаксис:

```
PowerShell

Get-SystemMessage -Identity <NDRIdentity>
```

Описание доступных *<значений NDRIdentity>* см. в разделе Значения идентификаторов для NDR этого раздела.

В этом примере показан возврат подробных сведений о настраиваемом отчете о недоставке для расширенного кода состояния 5.1.2, который отправляется внутренним отправителям на английском языке. Если для указанной комбинации языка, аудитории и расширенного кода состояния нет настраиваемых отчетов о недоставке, будет получено сообщение об ошибке.

```
PowerShell

Get-SystemMessage En\Internal\5.1.2 | Format-List
```

В этом примере показан возврат подробных сведений о настраиваемом отчете о недоставке на английском языке для квоты **ProhibitSendReceive** для почтовых ящиков. Если для указанной комбинации языка и квоты нет настраиваемых отчетов о недоставке, будет получено сообщение об ошибке.

```
PowerShell

Get-SystemMessage En\ProhibitSendReceiveMailBox | Format-List
```

Подробные сведения о синтаксисе и параметрах см. в разделе Get-SystemMessage.

Создание настраиваемого отчета о недоставке

Использование Командная консоль Exchange для создания настраиваемых отчетов о недоставке для расширенных кодов состояния

Чтобы создать настраиваемый отчет о недоставке для расширенного кода состояния, используйте следующий синтаксис:

PowerShell

```
New-SystemMessage -Internal <$true | $false> -Language <Locale> -DSNCode
<x.y.z> -Text "<NDR text>"
```

Значения:

- **Внутренний**. Определяет, отправляется ли недоставка внутренним или внешним отправителям. Для внутренних отправителей используйте значение `$true`. Для внешних отправителей используйте значение `$false`. Например, в настраиваемый текст для внутренних отправителей вы можете включить контакты службы технической поддержки, которые вы бы не хотели включать в отчеты о недоставке для внешних пользователей.
- **Язык**. Список доступных языков см. в разделе Поддерживаемые языки для NDR этой статьи.
- **DSNCode**: расширенный код состояния. Допустимые значения: 4. *x*. *y* или 5. *x*. *y* , где *x* и *y* — это числа от одной до трех цифр.
- **Текст**: можно использовать обычный текст или форматирование HTML. Дополнительные сведения см. в этой статье, в разделе HTML-теги и специальные знаки в отчетах о недоставке.

В этом примере показано создание настраиваемого отчета о недоставке с обычным текстом для расширенного кода состояния 5.1.2, который отправляется внешним отправителям на английском языке.

PowerShell

```
New-SystemMessage -Internal $false -Language En -DSNCode 5.1.2 -Text "You
tried to send a message to a disabled mailbox that's no longer accepting
messages. Please contact your System Administrator for more information."
```

В этом примере показано создание настраиваемого отчета о недоставке в формате HTML для расширенного кода состояния 5.1.2, который отправляется внутренним отправителям на английском языке.

```
PowerShell

New-SystemMessage -DSNCode 5.1.2 -Internal $true -Language En -Text 'You
tried to send a message to a <B>disabled</B> mailbox. Please visit <A
HREF="https://it.contoso.com">Internal Support</A> or contact
&quot;InfoSec&quot; for more information.'
```

Подробные сведения о синтаксисе и параметрах см. в разделе New-SystemMessage.

Использование Командная консоль Exchange для создания настраиваемых отчетов о недоставке по квотам

Чтобы создать настраиваемый отчет о недоставке по квотам, используйте следующий синтаксис:

```
PowerShell

New-SystemMessage -Language <Locale> -QuotaMessageType <Quota> -Text "<NDR
text>"
```

Значения:

- **Язык**. Список доступных языков см. в разделе Поддерживаемые языки для NDR.
- **QuotaMessageType**. Список доступных квот см. в разделе Значения идентификаторов для NDR.
- **Текст**: можно использовать обычный текст или форматирование HTML. Дополнительные сведения см. в разделе HTML-теги и специальные знаки в отчетах о недоставке.

В этом примере показано создание настраиваемого отчета о недоставке с обычным текстом на английском языке для квоты **ProhibitSendReceive** для почтовых ящиков.

```
PowerShell

New-SystemMessage -Language En -QuotaMessageType ProhibitSendReceiveMailBox
-Text "Your mailbox is full, and can't send or receive messages. Delete any
```

```
unwanted large messages (messages with attachments) and empty your Deleted
Items folder"
```

Подробные сведения о синтаксисе и параметрах см. в разделе New-SystemMessage.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли создан настраиваемый отчет о недоставке, выполните следующие действия.

- Выполните следующую команду и проверьте значения свойств:

  PowerShell

  ```
  Get-SystemMessage | Format-List Identity,DsnCode,Language,Text
  ```

- Отправьте тестовое сообщение, которое сгенерирует настроенный вами отчет о недоставке.

Использование Командная консоль Exchange для изменения настраиваемых отчетов о недоставке

Чтобы изменить настраиваемые отчеты о недоставке, используйте следующий синтаксис:

PowerShell

```
Set-SystemMessage -Identity <NDRIdentity> [-Text "<NDR text>"] [-Original]
```

Описание доступных *<значений NDRIdentity>* см. в разделе Значения идентификаторов для NDR этого раздела. Описание *текстовых> значений< NDR* см. в разделе HTML-теги и специальные символы в NDR этого раздела.

В этом примере показано изменение текста настраиваемого отчета о недоставке для расширенного кода состояния 5.1.2, который отправляется внутренним отправителям на английском языке.

PowerShell

```
Set-SystemMessage -Identity En\Internal\5.1.2 -Text "The mailbox you tried
to send an email message to is disabled and is no longer accepting messages.
```

```
Please contact the Help Desk at extension 123 for assistance."
```

В этом примере показано изменение текста в настраиваемом отчете о недоставке на английском языке для квоты **ProhibitSendReceive** для почтовых ящиков.

PowerShell

```
Set-SystemMessage -Identity En\ProhibitSendReceiveMailBox -Text "Your
mailbox is full. Delete large messages and empty your Deleted Items folder."
```

В этом примере показано отключение указанного настраиваемого отчета о недоставке. Настраиваемый отчет о недоставке сохраняется и отображается в результатах **Get-SystemMessage**, однако вместо него используется стандартный отчет о недоставке.

PowerShell

```
Set-SystemMessage -Identity En\Internal\5.1.2 -Original
```

Примечание. Если соответствующий NDR по умолчанию отсутствует, при использовании *параметра Original* появляется сообщение об ошибке.

Подробные сведения о синтаксисе и параметрах см. в разделе Set-SystemMessage.

Как проверить, все ли получилось?

Чтобы убедиться, что пользовательский NDR успешно изменен, замените *<NDRIdentity>* соответствующим значением и выполните следующую команду, чтобы проверить значения свойств:

PowerShell

```
Get-SystemMessage -Identity <NDRIdentity> | Format-List
```

Использование Командная консоль Exchange для удаления настраиваемых отчетов о недоставке

Чтобы удалить настраиваемый отчет о недоставке, используйте следующий синтаксис:

PowerShell

```
Remove-SystemMessage -Identity <NDRIdentity>
```

Описание доступных *<значений NDRIdentity>* см. в разделе Значения идентификаторов для NDR этого раздела.

В этом примере показано удаление настраиваемого отчета о недоставке для расширенного кода состояния 5.1.2, который отправляется внутренним отправителям на английском языке.

PowerShell

```
Remove-SystemMessage -Identity En\Internal\5.1.2
```

В этом примере показано удаление настраиваемого отчета о недоставке на английском языке для квоты **ProhibitSendReceive** для почтовых ящиков.

PowerShell

```
Remove-SystemMessage -Identity En\ProhibitSendReceiveMailBox
```

Подробные сведения о синтаксисе и параметрах см. в разделе Remove-SystemMessage.

Как проверить, все ли получилось?

Чтобы убедиться, что настраиваемый отчет о недоставке удален и отсутствует в списке, выполните эту команду:

PowerShell

```
Get-SystemMessage
```

Перешлите копии отчетов о недоставке на почтовый ящик получателя Exchange

Вы можете настроить Exchange так, чтобы отправлять копии отчетов о недоставке получателю Exchange. Однако по умолчанию получателю Exchange не назначено ни одного почтового ящика, поэтому все сообщения, отправленные получателю

Exchange, отклоняются. Чтобы пересылать копии отчетов о недоставке на почтовый ящик получателя Exchange, необходимо:

1. Назначить почтовый ящик получателю Exchange.
2. Указать расширенные коды состояния, которые вы хотите отслеживать (не квоты).

Шаг 1. Используйте Командная консоль Exchange для назначения почтового ящика получателю Exchange

Примечание. Из-за большого объема сообщений рекомендуется использовать выделенный почтовый ящик для получателя Exchange. Дополнительные сведения о создании почтовых ящиков см. в разделах Создание общих почтовых ящиков в Центре администрирования Exchange и Создание почтовых ящиков пользователей в Exchange Server.

Чтобы назначить почтовый ящик получателю Exchange, используйте следующий синтаксис:

PowerShell

```
Set-OrganizationConfig -MicrosoftExchangeRecipientReplyRecipient
<MailboxIdentity>
```

В этом примере показано назначение существующего почтового ящика с названием Contoso System Mailbox получателю Exchange.

PowerShell

```
Set-OrganizationConfig -MicrosoftExchangeRecipientReplyRecipient "Contoso
System Mailbox"
```

Шаг 2. Указание расширенных кодов состояния, которые требуется отслеживать

- Вы можете использовать Центр администрирования Exchange или Командная консоль Exchange.
- По умолчанию, несмотря на то что расширенные коды состояния не указаны, отчеты о недоставке для этих кодов автоматически отправляются получателю Exchange:

- `5.1.4`
- `5.2.0`
- `5.2.4`
- `5.4.4`
- `5.4.6`
- `5.4.8`

- Можно указать только расширенные коды состояния. Нельзя задать квоты.

Используйте Центр администрирования Exchange, чтобы задать расширенные коды состояния для отслеживания

Дополнительные сведения о EAC см. в разделе Центр администрирования Exchange в Exchange Server.

1. В EAC перейдите в раздел**Соединители получения** потока >**обработки почты**.
2. Щелкните **Дополнительные параметры** (••• и выберите **Параметры транспорта организации**.
3. В открывшемся окне **Настройки транспорта в организации** выберите вкладку **Доставка**. В разделе **Коды DSN** выполните одно или несколько следующих действий:

   - Чтобы добавить записи, введите расширенный код состояния, который требуется отслеживать (4. <*y.z*> или 5. <*y.z*>), а затем нажмите кнопку **Добавить** (➕ Повторите этот шаг необходимое количество раз.
   - Чтобы изменить существующую запись, выберите ее, нажмите кнопку **Изменить** (✏ Затем измените ее в виде встроенной записи.
   - Чтобы удалить существующую запись, выберите ее и нажмите кнопку **Удалить** (➖

   По завершении нажмите кнопку **Сохранить**.

Используйте Командная консоль Exchange, чтобы задать расширенные коды состояния для отслеживания

Чтобы добавить расширенные коды состояния для отслеживания, которые заменяют существующие значения, используйте следующий синтаксис:

PowerShell

```
Set-TransportConfig -GenerateCopyOfDSNFor <x.y.z>,<x.y.z>...
```

Этот пример показывает, как в организации Exchange настроить пересылку всех отчетов о недоставке для значений расширенных кодов состояния 5.7.1, 5.7.2 и 5.7.3 получателю Exchange.

PowerShell

```
Set-TransportConfig -GenerateCopyOfDSNFor 5.7.1,5.7.2,5.7.3
```

Чтобы добавить или удалить записи, не изменив существующие значения, используйте следующий синтаксис:

PowerShell

```
Set-TransportConfig -GenerateCopyOfDSNFor @{Add="<x.y.z>","<x.y.z>"...;
Remove="<x.y.z>","<x.y.z>"...}
```

В этом примере показано добавление расширенного кода состояния 5.7.5 и удаление кода 5.7.1 из существующего списка отчетов о недоставке, которые пересылаются получателю Exchange.

PowerShell

```
Set-TransportConfig -GenerateCopyOfDSNFor @{Add="5.7.5"; Remove="5.7.1"}
```

Как проверить, все ли получилось?

Чтобы проверить, настроена ли отправка копий отчетов о недоставке в почтовый ящик получателя Exchange, сделайте следующее.

- Выполните такую команду и проверьте значения свойств:

  PowerShell

  ```
  Get-TransportConfig | Format-List GenerateCopyOfDSNFor
  ```

- Проследите, доставлены ли в почтовый ящик получателя Exchange отчеты о недоставке, содержащие расширенные коды состояния.

Значения идентификатора для отчетов о недоставке

Идентификатор отчетов о недоставке использует один из следующих форматов:

- **NDR для расширенных кодов состояния**: <*Language*>\<Internal | External>\ <*DSNcode*>. Например, `En\Internal\5.1.2` или `Ja\External\5.1.2`.
  - **<DSNcode>**: допустимые значения: 4. *x*. *y* или 5. *x*. *y* , где *x* и *y* — это числа от одной до трех цифр. Чтобы создать список расширенных кодов состояния, используемых Exchange, см. раздел Использование командной консоли Exchange для просмотра всех стандартных NDR ранее в этом разделе.
  - **Внутренний или внешний**. Для внутренних или внешних отправителей можно использовать другой текст в NDR.
  - **<Язык>**. Список поддерживаемых языков см. в разделе Поддерживаемые языки для NDR этого раздела.

- **NDR для квот**: <*Language*>\ <*QuotaMessageType*>. Например, `En\ProhibitSendReceiveMailBox`.

  - **<Язык>**. Список поддерживаемых языков см. в разделе Поддерживаемые языки для NDR этого раздела.

  - **<QuotaMessageType>**: допустимые значения:

    Можно указать несколько критериев с использованием оператора сравнения and. Значения свойств, не выраженные в виде целого числа, должны заключаться в кавычки (").
    - **ProhibitSendReceiveMailBox**: почтовый ящик превышает ограничение `ProhibitSendReceiveQuota` .
    - **ProhibitSendMailbox**: почтовый ящик превышает ограничение `ProhibitSendQuota` .
    - **WarningMailbox**: почтовый ящик превышает ограничение `IssueWarningQuota` , если для `ProhibitSendQuota` него настроено ограничение или `ProhibitSendReceiveQuota` .
    - **WarningMailboxUnlimitedSize**: почтовый ящик превышает ограничение `IssueWarningQuota` , если для `ProhibitSendQuota` него не настроено ограничение или `ProhibitSendReceiveQuota` .

    WarningMailboxUnlimitedSize. Почтовый ящик превышает ограничение IssueWarningQuota, когда для него не настроено ограничение ProhibitSendQuota или ProhibitSendReceiveQuota.

- **ProhibitPostPublicFolder**: общедоступная папка превышает ограничение `ProhibitPostQuota` .
- **WarningPublicFolder**: общедоступная папка превышает ограничение `IssueWarningQuota` , если для нее `ProhibitPostQuota` настроено ограничение.
- **ПредупреждениеPublicFolderUnlimitedSize**: общедоступная папка превышает ограничение `IssueWarningQuota` , если для нее `ProhibitPostQuota` не настроено ограничение.

WarningPublicFolderUnlimitedSize. Общедоступная папка превышает ограничение IssueWarningQuota, когда для нее не настроено ограничение ProhibitPostQuota.

- **ProhibitReceiveMailboxMessagesPerFolderCount**: почтовый ящик превышает ограничение `MailboxMessagesPerFolderCountReceiveQuota` .
- **WarningMailboxMessagesPerFolderCount**: почтовый ящик превышает ограничение `MailboxMessagesPerFolderCountWarningQuota` , если для `ailboxMessagesPerFolderCountReceiveQuota` него настроено ограничение.
- **WarningMailboxMessagesPerFolderUnlimitedCount**: почтовый ящик превышает ограничение `MailboxMessagesPerFolderCountWarningQuota` , если для него не `MailboxMessagesPerFolderCountReceiveQuota` настроено ограничение.

WarningMailboxMessagesPerFolderUnlimitedCount. Почтовый ящик превышает ограничение MailboxMessagesPerFolderCountWarningQuota, когда для него не настроено ограничение MailboxMessagesPerFolderCountReceiveQuota.

- **ProhibitReceiveFolderHierarchyChildrenCountCount:** почтовый ящик превышает ограничение `FolderHierarchyChildrenCountReceiveQuota` .
- **WarningFolderHierarchyChildrenCount**: почтовый ящик превышает ограничение `FolderHierarchyChildrenCountWarningQuota` , если для него `FolderHierarchyChildrenCountReceiveQuota` настроено ограничение.
- **WarningFolderHierarchyChildrenUnlimitedCount**: почтовый ящик превышает ограничение `FolderHierarchyChildrenCountWarningQuota` , если для него не `FolderHierarchyChildrenCountReceiveQuota` настроено ограничение.
- **ProhibitReceiveFoldersCount**: почтовый ящик превышает ограничение `FoldersCountReceiveQuota` .
- **WarningFoldersCount**: почтовый ящик превышает ограничение `FoldersCountWarningQuota` , если для `FoldersCountReceiveQuota` него настроено ограничение.

- **WarningFoldersCountUnlimited** Почтовый ящик превышает ограничение `FoldersCountWarningQuota` , если для `FoldersCountReceiveQuota` него не настроено ограничение.

WarningFoldersCountUnlimited. Почтовый ящик превышает ограничение FoldersCountWarningQuota, когда для него не настроено ограничение FoldersCountReceiveQuota.

- **ProhibitReceiveFolderHierarchyDepth**: почтовый ящик превышает ограничение `FolderHierarchyDepthWarningQuota` .
- **WarningFolderHierarchyDepth**: почтовый ящик превышает ограничение `FolderHierarchyDepthWarningQuota` , если для него `FolderHierarchyDepthReceiveQuota` настроено ограничение.
- **WarningFolderHierarchyDepthUnlimited:**: почтовый ящик превышает ограничение `FolderHierarchyDepthWarningQuota` , если для него не `FolderHierarchyDepthReceiveQuota` настроено ограничение.

Поддерживаемые языки для отчетов о недоставке

В приведенной таблице перечислены коды поддерживаемых языков, которые можно использовать в настраиваемых отчетах о недоставке.

Код языка	Язык
af	Африкаанс
am-ET	Амхарский (Эфиопия)
ar	Арабский
as-IN	Ассамский (Индия)
bg	Болгарский
bn-BD	Бенгальский (Бангладеш)
bn-IN	Бенгальский (Индия)
bs-Cyrl-BA	Боснийский (кириллица, Босния и Герцеговина)
bs-Latn-BA	Боснийский (латиница, Босния и Герцеговина)
ca	Каталонский
cs	Чешский

Код языка	Язык
cy-GB	Уэльский (Великобритания)
da	Датский
de	Немецкий
el	Греческий
ru	Английский
es	Испанский
et	Эстонский
eu	Баскский
fa	Персидский
fi	Финский
fil-PH	Филиппинский (Филиппины)
fr	Французский
ga-IE	Ирландский (Ирландия)
gl	Галисийский
gu	Гуджарати
ha-Latn-NG	Хауса (латиница, Нигерия)
он	Иврит
hi	Хинди
hr	Хорватский
hu	Венгерский
hy	Армянский
id	Индонезийский
ig-NG	Игбо (Нигерия)
есть	Исландский
оно	Итальянский
iu-Latn-CA	Инуктитут (латиница, Канада)

Код языка	Язык
ja	Японский
ka	Грузинский
kk	Казахский
km-KH	Кхмерский (Камбоджа)
kn	Каннада
ko	Корейский
kok	Конкани
ky	Киргизский
lb-LU	Люксембургский (Люксембург)
lo-LA	Лаосский (Лаосская Народно-Демократическая Республика)
lt	Литовский
lv	Латвийский
mi-NZ	Маори (Новая Зеландия)
mk	Македонский
ml-IN	Малаялам (Индия)
mr	Маратхи
ms	Малайский
ms-BN	Малайский (Бруней-Даруссалам)
mt-MT	Мальтийский (Мальта)
ne-NP	Непальский (Непал)
nl	Нидерландский
nn-NO	Норвежский (нюнорск)
нет	Норвежский
nso-ZA	Северный сото (ЮАР)
or-IN	Ория (Индия)
pa	Панджаби

Код языка	Язык
pl	Польский
ps-AF	Пушту (Афганистан)
pt	Португальский язык
pt-PT	Португальский (Португалия)
qut-GT	Кише (Гватемала)
quz-PE	Кечуа (Перу)
ro	Румынский
ru	Русский
rw-RW	Киньяруанда (Руанда)
si-LK	Сингальский (Шри-Ланка)
sk	Словацкий
sl	Словенский
sq	Албанский
sr	Сербский
sr-Cyrl-CS	Сербский (кириллица, Сербия)
sv	Шведский
sw	Суахили
ta	Тамильский
te	Телугу
th	Тайский
tn-ZA	Сетсвана (ЮАР)
tr	Турецкий
tt	Татарский
uk	Украинский
ur	Урду
uz	Узбекский

Код языка	Язык
vi	Вьетнамский
wo-SN	Волоф (Сенегал)
xh-ZA	Коса (ЮАР)
yo-NG	Йоруба (Нигерия)
zh-Hans	Китайский (упрощенный)
zh-Hant	Китайский (традиционный)
zh-HK	Китайский (Гонконг)
zu-ZA	Зулу (ЮАР)

Для управления языками, которые используются в отчетах о недоставке, используйте следующие параметры командлета **Set-TransportConfig**:

- *ExternalDsnDefaultLanguage*: указывает язык по умолчанию для использования во внешних NDR. Значение по умолчанию пустое (`$null`), что означает, что используется язык windows server по умолчанию.
- *InternalDsnDefaultLanguage*: указывает язык по умолчанию для использования во внутренних NDR. Значение по умолчанию пустое (`$null`), что означает, что используется язык windows server по умолчанию.
- *ExternalDsnLanguageDetectionEnabled*:
  - `$true`: Exchange пытается отправить внешний NDR на том же языке, что и исходное сообщение. Это значение используется по умолчанию.
  - `$false`: обнаружение языка отключено для внешних NDR. Язык NDR определяется параметром *ExternalDsnDefaultLanguage* .
- *InternalDsnLanguageDetectionEnabled*:
  - `$true`: Exchange пытается отправить внутренний NDR на том же языке, что и исходное сообщение. Это значение используется по умолчанию.
  - `$false`: обнаружение языка отключено для внутренних NDR. Язык недоставки определяется параметром *InternalDsnDefaultLanguage* .

HTML-теги и специальные знаки в отчетах о недоставке

Настраиваемый текст в отчетах о недоставке может содержать максимум 512 символов, включая текстовые и HTML-теги. Например, можно вставить подробное

описание проблемы, контакты службы технической поддержки и ссылку на веб-сайт отдела поддержки.

Чтобы определить, какой формат использует Exchange в отчетах о недоставке — обычный текст или HTML, — используйте следующие параметры в командлете **Set-TransportConfig**:

- *ExternalDsnSendHtml*:
  - `$true`: используйте теги HTML в NDR для внешних отправителей. Это значение используется по умолчанию.
  - `$false`: используйте обычный текст в NDR для внешних отправителей.
- *InternalDsnSendHtml*:
  - `$true`: используйте html-теги в NDR для внутренних отправителей. Это значение используется по умолчанию.
  - `$false`: используйте обычный текст в NDR для внутренних отправителей.

В приведенной таблице описаны HTML-теги, которые можно использовать в тексте отчета о недоставке.

Описание	**HTML-теги**
Полужирный	`<B>` и `</B>`
Курсив	`<EM>` и `</EM>`
Разрыв строки	` `
Paragraph	`<P>` и `</P>`
Hyperlink	`<A HREF="url">` и `</A>` **Примечание.** Так как этот тег содержит двойные кавычки, необходимо использовать одинарные кавычки (а не двойные кавычки) вокруг полной текстовой строки, если этот тег используется в пользовательском тексте. В противном случае вы получите сообщение об ошибке.

Некоторые символы в отчете о недоставке требуют управляющих кодов, чтобы идентифицировать их буквально, а не по функции в отчете. Эти символы описаны в приведенной ниже таблице.

Знак	**Управляющий код**
<	`<`
>	`>`

Знак	Управляющий код
"	`"`
&	`&`

Например, если вы хотите, чтобы в поле NDR отображалось текст `Please contact the Help Desk at <1234>.`, необходимо указать значение `"Please contact the Help Desk at <1234>."`

Это пример значения настраиваемого текста отчета о недоставке с использованием HTML-тегов и управляющих кодов.

text

```
'You tried to send a message to a <B>disabled</B> mailbox. Please visit <A HREF="https://it.contoso.com">Internal Support</A> or contact &quot;InfoSec&quot; for more information.'
```

Преобразование содержимого в Exchange Server

Статья • 04.04.2023

Преобразование содержимого — это процесс правильного форматирования сообщения для каждого получателя. Решение выполнить преобразование содержимого в сообщении зависит от того, кому отправляется сообщение, и от формата сообщения. Типы преобразования содержимого, происходящие в Exchange 2016 и Exchange 2019, не изменяются по сравнению с Exchange 2013:

- **Преобразование сообщений для внешних получателей**. Этот тип преобразования содержимого включает параметры преобразования TNEF и кодировки сообщений для внешних получателей. Сообщения, отправляемые получателям внутри организации Exchange, не требуют преобразования содержимого такого типа. Он обрабатывается классификатором в службе транспорта на сервере почтовых ящиков. Классификация каждого полученного сообщения выполняется после того как сообщение помещено в очередь передачи. Перед помещением сообщения в очередь доставки для него (помимо разрешения получателей и разрешения маршрутизации) выполняется преобразование содержимого. Если одно сообщение адресовано нескольким получателям, классификатор определяет соответствующее кодирование для каждого получателя сообщения. При трассировке преобразования содержимого не фиксируются ошибки преобразования содержимого, обнаруженные классификатором в ходе преобразования сообщений, отправляемых внешним получателям.

- **Преобразование MAPI для внутренних получателей**. Этот тип преобразования контента обрабатывается службой транспорта почтовых ящиков. Служба передачи почтовых ящиков используется на серверах почтовых ящиков для передачи сообщений между базами данных сообщений на локальном сервере и службой передачи на серверах почтовых ящиков. А именно, служба отправки и передачи почтовых ящиков передает сообщения из папки "Исходящие" отправителя службе передачи на сервере почтовых ящиков. Служба отправки и передачи почтовых ящиков передает сообщения от службы передачи на сервере почтовых ящиков в папку "Входящие" получателя. Служба отправки и передачи почтовых ящиков преобразует все исходящие сообщения с формата MAPI, а служба доставки и передачи почтовых ящиков преобразует все входящие сообщения в формат MAPI. Ошибки преобразования MAPI регистрируются при трассировке

преобразования содержимого. Дополнительные сведения см. в разделе Managing Content Conversion Tracing.

Форматы сообщений Exchange и Outlook

В списке ниже описаны основные форматы сообщений, доступные в Exchange и Outlook.

- **Обычный текст**. В текстовом сообщении используется только текст US-ASCII, как описано в RFC 5322. В сообщении не используются разные шрифты или другие способы форматирования текста. Два возможных формата обычного текстового сообщения:
  - Заголовки и тело сообщения состоят из текстовых знаков US-ASCII. Вложения кодируются с использованием алгоритма *Uuencode* («Unix-to-Unix encoding»). Данный алгоритм представляет собой кодировку Unix-to-Unix и позволяет хранить двоичные вложения в тексте сообщения электронной почты с использованием текстовых символов US-ASCII.
  - Сообщение в кодировке MIME имеет значение `text/plain` **Content-Type** , и значение `7bit` **Content-Transfer-Encoding** для текстовых частей многокомпонентного сообщения. Для любых текстовых вложений используется кодирование Quoted Printable или Base64. По умолчанию при создании и отправке обычного текстового сообщения в Outlook сообщение закодировано MIME со значением `text/plain` **Content-Type** .
- **HTML**: HTML-сообщение поддерживает форматирование текста, фоновые изображения, таблицы, маркеры и другие графические элементы. Для сохранения этих элементов форматирования сообщения в формате HTML должны кодироваться в кодировке MIME.
- **Формат форматированного текста (RTF):** RTF поддерживает форматирование текста и другие графические элементы. RTF — это синоним TNEF (термины TNEF и RTF взаимозаменяемы). Формат сообщений в формате форматов форматов текста полностью отличается от формата документа с форматом форматов, доступных в Word.
- **TNEF**. Формат нейтральной инкапсуляции транспорта — это формат, предназначенный для инкапсулирования свойств сообщения MAPI от Майкрософт. Сообщение в формате TNEF содержит сообщение в виде обычного текста и вложение, в которое упакована исходная

отформатированная версия сообщения. Обычно такое вложение имеет название Winmail.dat. Вложение Winmail.dat включает следующие сведения:

- исходную форматированную версию сообщения (например, шрифты, размеры и цвета текста);
- объекты OLE (например, внедренные изображения или документы Office);
- специальные элементы Outlook (например, настраиваемые формы, кнопки голосования или приглашения на собрания);
- обычные вложения, которые имелись в исходном сообщении

Получающееся обычное текстовое сообщение может быть представлено в следующих форматах:

- сообщение, соответствующее спецификации RFC 5322 и включающее только текстовые знаки US-ASCII, с вложением Winmail.dat в кодировке Uuencode;
- составное сообщение с кодированием MIME и вложением Winmail.dat.

Outlook и другие почтовые клиенты, которые имеют все функции, необходимые для работы с форматом TNEF, обрабатывают вложение Winmail.dat и отображают исходное содержимое сообщения, не отображая само вложение Winmail.dat. Почтовые клиенты, в которых нет функций для работы с форматом TNEF, могут представлять сообщения в формате TNEF любым из следующих способов:

- Отображается версия сообщения в виде обычного текста, а сообщение содержит вложение с именем Winmail.dat, Win.dat или другое универсальное имя, например Att *nnnnn.dat* или Att *nnnnn.eml*, где заполнитель *nnnnnnn* представляет случайное число.
- Отображается обычная текстовая версия сообщения. Вложение TNEF пропускается или удаляется. В результате остается обычное текстовое сообщение.
- Серверы обмена сообщениями, поддерживающие формат TNEF, можно настроить так, чтобы они удаляли вложения TNEF из входящих сообщений. В результате остается обычное текстовое сообщение. Более того, некоторые почтовые клиенты не поддерживают формат TNEF, но могут распознавать и пропускать вложения TNEF. В результате отображается обычное текстовое сообщение.

Существуют программы сторонних разработчиков, с помощью которых можно преобразовывать вложения Winmail.dat.

Формат TNEF поддерживается во всех версиях Exchange, начиная с Exchange Server версии 5.5.

- **Сводный формат нейтрализации транспорта (STNEF):** STNEF эквивалентен TNEF. Формат STNEF эквивалентен формату TNEF, но кодирование сообщений в формате STNEF отличается от кодирования сообщений в формате TNEF. В частности, сообщения STNEF всегда в кодировке MIME и всегда имеют значение `Binary`**Content-Transfer-Encoding** . Таким образом, у этих сообщений нет представления в виде обычного текста, а в тексте сообщения нет отдельного вложения Winmail.dat. Все сообщение представлено с использованием только двоичных данных. Сообщения, у которых параметр **Content-Transfer-Encoding** имеет значение **Binary**, можно передавать только между серверами обмена сообщениями, поддерживающими и объявляющими расширения SMTP **BINARYMIME** и **CHUNKING**, как указано в спецификации RFC 3030. Сообщения всегда передаются между серверами обмена сообщениями с использованием команды **BDAT** вместо стандартной команды **DATA**.

  Формат STNEF поддерживается во всех версиях Exchange, начиная с Exchange 2000. Формат STNEF автоматически используется для всех сообщений, передаваемых между серверами Exchange в организации с момента появления основного режима Exchange Server 2003.

  Exchange никогда не отправляет сообщения в формате STNEF внешним получателям. Получателям за пределами организации Exchange можно отправлять сообщения только в формате TNEF.

Параметры преобразования содержимого для внешних получателей

Параметры преобразования содержимого, которые можно задать в организации Exchange для внешних получателей, делятся на следующие категории:

- **Параметры преобразования TNEF**. Эти параметры преобразования определяют, следует ли сохранять или удалять TNEF из сообщений, покидающих организацию Exchange.
- **Параметры кодирования сообщений**. Эти параметры задают параметры кодирования сообщений, такие как наборы символов MIME и не MIME, кодировка сообщений и форматы вложений.

Эти параметры преобразования и кодирования не зависят друг от друга. Например, то, разрешено ли отправлять сообщения в формате TNEF за пределы организации Exchange, не связано с параметрами кодирования MIME или кодирования в виде обычного текста для этих сообщений.

Вы можете выбрать необходимое преобразование содержимого на различных уровнях организации Exchange, как описано в следующем списке:

- **Параметры удаленного домена**. Удаленные домены определяют параметры для передачи исходящих сообщений между организацией Exchange и внешними доменами. Даже если вы не создаете записи удаленного домена для определенных доменов, существует предопределенный удаленный домен с именем Default (Используемый по умолчанию), который применяется ко всем удаленным адресным пространствам (*). Дополнительные сведения об удаленных доменах см. в статье Remote Domains.

- **Параметры почтового пользователя и почтового контакта**. Почтовые пользователи и почтовые контакты похожи, так как имеют внешние адреса электронной почты и содержат сведения о людях за пределами организации Exchange. Основное отличие заключается в том, что пользователи почты имеют учетные записи, которые они могут использовать для входа в Active Directory и доступа к ресурсам в организации. Дополнительные сведения см. в статье Recipients.

- **Параметры Outlook**. В Outlook можно задать следующие параметры форматирования и кодирования сообщений:
  - **Формат сообщения**. Вы можете задать формат сообщений по умолчанию для всех сообщений. Формат по умолчанию для всех сообщений можно переопределять при создании конкретного сообщения.
  - **Формат сообщений в Интернете**. Вы можете указать, отправляются ли сообщения TNEF удаленным получателям или они сначала преобразуются в более совместимый формат. Можно также задать различные параметры кодирования для сообщений, отправляемых удаленным получателям. Эти параметры не применяются к сообщениям, отправляемых получателям в организации Exchange.
  - **Формат сообщения получателя из Интернета (Outlook 2010 или более ранних версий):** вы можете управлять отправкой сообщений TNEF определенным контактам в папке "Контакты". Эти параметры преобразования недоступны для получателей в организации Exchange.
  - **Параметры кодирования сообщений получателя в Интернете (Outlook 2010 или более ранние версии).** Вы можете управлять параметрами кодирования MIME или обычного текста для определенных контактов в папке "Контакты". Эти параметры преобразования недоступны для получателей в организации Exchange.
  - **Международные параметры**. Вы можете управлять наборами символов, используемыми в сообщениях.

Дополнительные сведения об этих параметрах см. в разделах Параметры преобразования TNEF и Параметры кодирования сообщений в Exchange Server.

Понимание структуры сообщений электронной почты

Чтобы лучше понимать параметры преобразования содержимого для внешних получателей, необходимо понимать структуру сообщений электронной почты. Для написания и отправки сообщений электронной почты в основании сообщения SMTP обычное текстовое сообщение в 7-разрядной кодировке US-ASCII. Стандартное SMTP-сообщение состоит из описанных ниже элементов.

- **Конверт сообщения**: конверт сообщения определен в RFC 5321. Конверт сообщения содержит сведения, необходимые для передачи и доставки сообщения. Конверт сообщения никогда не отображается для получателей, так как он создается в процессе передачи сообщения и фактически не является частью самого сообщения.

- **Содержимое сообщения**. Содержимое сообщения определяется в RFC 5322. Содержимое сообщения состоит из следующих элементов:

  - **Заголовок сообщения**. Заголовок сообщения представляет собой коллекцию полей заголовка. Поля заголовка состоят из имени поля, двоеточия (:), тела поля и сочетания знаков возврата каретки и перевода строки (CR/LF).

    Имя поля может включать все печатные текстовые знаки US-ASCII за исключением двоеточия (:). В частности, знаки ASCII с 33 по 57 и с 59 по 126 включительно.

    Текст поля может включать любые знаки US-ASCII за исключением знаков возврата каретки (CR) и перевода строки (LF). Тем не менее в тексте поля может присутствовать сочетание символов возврата каретки и перевода строки, если оно используется для *развертывания заголовка*. Развертывание заголовка — это разделение текста поля заголовка на несколько строк в соответствии с разделом 2.2.3 спецификации RFC 5322. Другие требования к синтаксису текста поля описаны в разделах 3 и 4 спецификации RFC 5322.

  - **Текст сообщения**. Текст сообщения представляет собой коллекцию строк текстовых символов US-ASCII, которые появляются после заголовка

сообщения. Заголовок и тело сообщения разделяются пустой строкой, которая завершается сочетанием знаков возврата каретки и перевода строки. Тело сообщения может отсутствовать. Ни одна строка текста в теле сообщения не может содержать более 997 знаков. Знаки возврата каретки и перевода строки отмечают конец строки и могут использоваться только вместе.

Если сообщение SMTP содержит элементы, отличные от обычного текста US-ASCII, для сохранения этих элементов необходимо выполнить кодирование сообщения. Способ кодирования нетекстового содержимого сообщений определен в стандарте MIME. Стандарт MIME позволяет использовать текст, представленный знаками из других кодировок, нетекстовые вложения, составные тексты сообщений и поля заголовка, представленные символами из других кодировок. Стандарт MIME описан в документах RFC 2045, RFC 2046, RFC 2047, RFC 4288, RFC 4289 и RFC 2049. В стандарте MIME определена совокупность полей заголовка, которые задают дополнительные атрибуты сообщения. В следующих разделах описываются некоторые важные поля заголовков MIME.

поле заголовка MIME-Version

Значение по умолчанию: `1.0`

Это поле заголовка является первым в сообщении, преобразованном в формат MIME. Оно следует за другими стандартными полями заголовка RFC 5322, но предшествует всем остальным полям заголовка MIME. Почтовые клиенты с поддержкой MIME используют это поле заголовка для идентификации сообщений в кодировке MIME. Если это поле заголовка отсутствует, почтовые клиенты с поддержкой MIME идентифицируют формат сообщения как обычный текст.

Поле заголовка Content-Type

Значение по умолчанию: `text/plain`

Это поле заголовка определяет тип мультимедиа содержимого сообщения в согласно спецификации RFC 2046. Тип носителя состоит из следующих типов:

- **Тип :**
    - Типы, начинающиеся с `x-` , не являются стандартными. Служба Internet Assigned Numbers Authority (IANA) ведет список зарегистрированных типов мультимедиа. Дополнительные сведения см. в разделе Типы носителей MIME.

    - Тип мультимедиа *multipart* (составной) позволяет использовать в одном сообщении несколько разделов, имеющих разные типы мультимедиа. Некоторые значения полей **Content-Type** включают `text/plain`, `text/html`, `multipart/mixed` и `multipart/alternative`.

- **Подтип**: подтипы, которые начинаются с `vnd.` , зависят от поставщика.

- **Один или несколько необязательных параметров**. Например, параметр, определяющий `charset=` кодировку символов MIME.

Поле заголовка Content-Transfer-Encoding

Значение по умолчанию: `7bit`

Это поле заголовка может определять следующие характеристики сообщения:

- алгоритм кодирования, используемый для преобразования текста, отличного от US-ASCII, или двоичных данных в теле сообщения;
- индикатор, описывающий текущее состояние тела сообщения.

В сообщении MIME может использоваться несколько значений поля заголовка **Content-Transfer-Encoding**. Когда поле заголовка **Content-Transfer-Encoding** появляется в заголовке сообщения, оно применяется ко всему тексту сообщения. Когда поле заголовка **Content-Transfer-Encoding** появляется в одной из частей составного сообщения, оно применяется только к этой части сообщения.

Когда алгоритм кодирования применяется к данным текста сообщения, последний преобразуется в обычный текст в кодировке US-ASCII. Это позволяет передавать сообщения через старые серверы обмена сообщениями, которые поддерживают только текстовые сообщения в кодировке US-ASCII. Следующие значения поля заголовка **Content-Transfer-Encoding** указывают алгоритм кодирования, который использовался для преобразования текста сообщения:

- `Quoted-printable`: использует печатные символы US-ASCII для кодирования данных текста сообщения. Если текст исходного сообщения содержит преимущественно знаки US-ASCII, кодирование по алгоритму Quoted Printable позволяет получить компактный текст, относительно пригодный для чтения. Все печатные текстовые знаки US-ASCII за исключением знака равенства (=) можно представить без кодирования.

- `Base64`: в основном на основе стандарта электронной почты с повышенной конфиденциальностью (PEM), определенного в RFC 4648. Для кодирования текста сообщения в этом случае используется 64-знаковый алфавит и знаки

заполнения вывода, определенные в стандарте PEM. Сообщение, закодированное с использованием алгоритма Base64, обычно примерно на треть больше исходного. Этот алгоритм позволяет спрогнозировать итоговый размер сообщения и лучше всего подходит для кодирования двоичных данных и текста в кодировке, отличной от US-ASCII.

Как правило, для кодирования сообщения используется только один алгоритм.

Если для текста сообщения не использовался ни один алгоритм кодирования, поле заголовка **Content-Transfer-Encoding** просто определяет текущее состояние данных в тексте сообщения. Следующие значения поля заголовка **Content-Transfer-Encoding** указывают, что для текста сообщения не был использован ни один алгоритм кодирования:

- `7bit`: указывает, что данные текста сообщения уже находятся в формате RFC 5322. Это означает, что должны быть выполнены следующие условия:
  - каждая строка текста содержит не более 998 знаков;
  - все знаки являются текстовыми знаками из кодировки US-ASCII с номерами от 1 до 127 включительно;
  - знаки возврата каретки и перевода строки используются только вместе для обозначения конца строки текста.

    7-разрядную кодировку можно использовать для всего текста сообщения или для части текста составного сообщения. Если составное сообщение содержит части, включающие двоичные данные или текстовые знаки, отличные от знаков в кодировке US-ASCII, эти части должны быть закодированы с помощью алгоритма Quoted Printable или Base64.

    Сообщения с текстами в 7-разрядной кодировке можно передавать между серверами обмена сообщениями с помощью стандартной команды DATA.
- `8bit`: указывает, что данные текста сообщения содержат символы, отличные от US-ASCII. Это означает, что должны быть выполнены следующие условия:
  - каждая строка текста содержит не более 998 символов;
  - в теле сообщения есть хотя бы один знак, имеющий в кодировке номер больше 127;
  - символы возврата каретки и перевода строки могут использоваться вместе только для обозначения конца строки текста.

8-разрядную кодировку можно использовать для всего текста сообщения или для части текста составного сообщения. Если составное сообщение содержит части, включающие двоичные данные или текстовые знаки, отличные от знаков в кодировке US-ASCII, эти части должны быть закодированы с помощью алгоритма Quoted Printable или Base64.

Сообщения с текстом в 8-разрядной кодировке можно передавать только между серверами обмена сообщениями, поддерживающими SMTP-расширение **8BITMIME** согласно спецификации RFC 6152, например серверами под управлением Exchange 2000 Server или более поздних версий. Это означает, что должны быть выполнены следующие условия:

- в отклике EHLO сервера должно быть объявлено ключевое слово **8BITMIME**;
- Сообщения по-прежнему передаются с помощью стандартной команды **SMTP DATA** . `BODY=8BITMIME` Однако параметр необходимо добавить в конец команды **MAIL FROM**.

- `Binary`: указывает, что текст сообщения содержит текстовые или двоичные данные, отличные от US-ASCII. Это означает, что выполняются следующие условия:
  - разрешены любые последовательности знаков;
  - длина строк не ограничена;
  - двоичные элементы сообщения не нуждаются в кодировании.

  Сообщения с двоичным телом можно передавать только между серверами обмена сообщениями, поддерживающими SMTP-расширение **BINARYMIME** согласно спецификации RFC 3030, например серверами под управлением Exchange 2000 Server или более поздних версий. Это означает, что должны быть выполнены следующие условия:

  - в отклике EHLO сервера должно быть объявлено ключевое слово **BINARYMIME**;
  - SMTP-расширение **BINARYMIME** можно использовать только с SMTP-расширением **CHUNKING**. Функция *фрагментирования* позволяет отправлять сообщения с большими телами в виде нескольких меньших блоков. Понятие функции фрагментирования определено в спецификации RFC 3030. В отклике EHLO сервера должно быть объявлено ключевое слово **CHUNKING**.

- Для передачи сообщений используется команда **BDAT** вместо стандартной команды **DATA**.
- Параметр `BODY=BINARYMIME` должен быть добавлен в конец команды **MAIL FROM** , если сообщение содержит текст сообщения.

Значения `7bit`, `8bit` и `Binary` никогда не существуют вместе в одном многокомпонентном сообщении (значения являются взаимоисключающими). `Quoted-printable` Значения или `Base64` могут отображаться в 7-разрядном или 8-разрядном тексте многокомпонентного сообщения, но никогда не в тексте двоичного сообщения. Если многокомпонентный текст сообщения содержит различные части, состоящие из 7-разрядного и 8-разрядного содержимого, все сообщение классифицируется как 8-разрядное. Если многокомпонентное тело сообщения содержит различные части, состоящие из 7-битового, 8-битового и двоичного содержимого, все сообщение классифицируется как двоичное.

Поле заголовка Content-Disposition

Значение по умолчанию: `Attachment`

Это поле заголовка указывает почтовому клиенту с поддержкой MIME, как он должен отображать вложенный файл, и описано в RFC 2183. Допустимые значения:

- `Inline`: вложение отображается в тексте сообщения.
- `Attachment`: вложенный файл отображается как обычное вложение отдельно от текста сообщения. Другие параметры также имеют эти значения (например, `Filename`, `Creation-date` и `Size`).

Параметры кодирования сообщений в Exchange Server

Статья • 04.04.2023

Параметры кодирования сообщений в Exchange Server позволяют указать характеристики сообщения, такие как mime и наборы символов, отличные от MIME, двоичное кодирование и форматы вложений. Вы можете настраивать параметры кодирования сообщений в следующих разделах:

- Параметры удаленных доменов
- Раздел параметров почтовых пользователей и почтовых контактов.
- Раздел параметров Outlook:
  - формат сообщений;
  - формат сообщений Интернета;
  - формат сообщений Интернета для получателей (Outlook 2010 или более ранней версии);
  - параметры кодировок.
- Параметры формата сообщений Outlook в Интернете (предыдущее название — Outlook Web App)

Как правило, заданные по умолчанию параметры кодирования сообщений подходят для нормальной работы. Однако вам может потребоваться изменить параметры кодирования сообщений для тех получателей, которые пользуются старыми почтовыми клиентами и системами обмена сообщениями. Скорее всего, они сообщат вам, если в сообщениях из вашей среды Exchange имеются проблемы с форматированием.

Дополнительные сведения о преобразовании содержимого в Exchange см. в разделе Преобразование содержимого. Сведения о параметрах TNEF (или форматированного текста) см. в разделе Параметры преобразования TNEF.

Параметры удаленных доменов;

Удаленные домены задают параметры для сообщений, отправляемых в домены, которые являются внешними для вашей организации Exchange. Дополнительные

сведения см. в статье Remote Domains.

Когда вы настраиваете параметры кодирования сообщений для удаленного домена, эти параметры применяются ко всем сообщениям, отправляемым получателям в этом домене. Некоторые параметры можно настраивать в Центре администрирования Exchange (EAC), но большинство параметров доступны только в командной консоли Exchange. В приведенной ниже таблице описываются параметры кодирования сообщений.

Setting	**Настройка в Центре администрирования Exchange**	**Настройка с помощью командной консоли Exchange**
Набор символов MIME. Указанный набор символов используется только для сообщений MIME, которые не содержат набор символов. Этот параметр не заменяет кодировки, уже заданные в исходящих сообщениях. **Набор символов, отличный от MIME**: этот параметр используется, если выполняется одно из следующих условий: • Для входящих сообщений из удаленного домена отсутствует значение параметра *charset*= в поле заголовка MIME **Content-Type:** . • Для исходящих сообщений, отправляемых на удаленный домен, не задано значение кодировки MIME.	Поток >**обработки почтыУдаленные домены**>**Добавьте**+ выберите существующий удаленный домен, а затем нажмите кнопку **Изменить**.✎ >**Поддерживаемый набор символов**.	Командлет: **Set-RemoteDomain** Параметры: *CharacterSet* и *NonMimeCharacterSet*

Setting	Настройка в Центре администрирования Exchange	Настройка с помощью командной консоли Exchange
Тип контента: допустимые значения: `MimeHtmlText`: все сообщения преобразуются в сообщения MIME, использующие форматирование HTML, если исходное сообщение не является текстовым сообщением. Если это так, исходящее сообщение будет сообщением MIME с текстовым форматированием. Это значение используется по умолчанию. `MimeText`: все сообщения преобразуются в сообщения MIME, использующие форматирование текста. `MimeHtml`: все сообщения преобразуются в сообщения MIME, использующие форматирование HTML.	н/д	Командлет: **Set-RemoteDomain** Параметр: *ContentType*
Размер оболочки строки. Можно указать максимальное количество символов, которое может существовать в одной строке текста в тексте сообщения электронной почты. Для устаревших почтовых клиентов предпочтительно задать длину строки 78 символов.	н/д	Командлет: **Set-RemoteDomain** Параметр *: LineWrapSize* Значение по умолчанию — `Unlimited`, что означает, что клиент электронной почты отвечает за настройку размера оболочки строки в новых сообщениях.

Раздел параметров почтовых пользователей и почтовых контактов.

Почтовые контакты и почтовые пользователи представляют пользователей с внешними адресами электронной почты в организации Exchange. Дополнительные сведения см. в статье Recipients.

При настройке параметров кодирования сообщений для почтового контакта или почтового пользователя параметры применяются только к сообщениям, отправленным именно этому получателю. Полный набор параметров доступен только в командной консоли Exchange для следующих командлетов:

- Enable-MailContact, New-MailContact или Set-MailContact.
- Enable-MailUser, New-MailUser или Set-MailUser.

В приведенном ниже списке описываются параметры кодирования сообщений для почтовых контактов и почтовых пользователей.

- *UsePreferMessageFormat parameter**: указывает, переопределяют ли параметры формата сообщений для почтового контакта или почтового пользователя соответствующие параметры удаленного домена. Допустимые значения:
  - `$true`: сообщения, отправляемые почтовому контакту или почтовому пользователю, используют формат сообщений, настроенный для почтового контакта или почтового пользователя.
  - `$false`: сообщения, отправляемые почтовому контакту или почтовому пользователю, используют формат сообщений, настроенный для удаленного домена (удаленный домен по умолчанию или определенный удаленный домен) или настроенный отправителем сообщения. Это значение используется по умолчанию.
- **Параметр MessageFormat**: этот параметр задает формат сообщений, отправляемых почтовому контакту или почтовому пользователю. Допустимые значения: `Text` или `Mime`, а значение по умолчанию — `Mime`.
- **Параметр MessageBodyFormat**: этот параметр задает формат текста сообщения для сообщений, отправляемых почтовому контакту или почтовому пользователю. Допустимые значения: `Text`, `Html` или `TextAndHtml`, а значение по умолчанию — `TextAndHtml`.

  Параметры *MessageFormat* и *MessageBodyFormat* являются взаимозависимыми:
  - Если значение *MessageFormat* равно `Mime`, значение *MessageBodyFormat* может быть `Text`, `Html` или `TextAndHtml`.
  - Если значение *MessageFormat* имеет значение `Text`, значение *MessageBodyFormat* может иметь `Text` только значение .
- **Параметр MacAttachmentFormat**: задает формат вложения сообщений для клиентов операционной системы Apple Macintosh. Допустимые значения: `BinHex`, `UuEncode`, `AppleSingle` или `AppleDouble`, а значение по умолчанию — `BinHex`.

Параметры *MessageFormat* и *MacAttachmentFormat* являются взаимозависимыми:

- Если значение *MessageFormat* имеет значение `Text`, *значением* *MacAttachmentFormat* может быть `BinHex` или `UuEncode`.
- Если значение *MessageFormat* имеет значение `Mime`, значение *MacAttachmentFormat* может иметь значение `BinHex`, `AppleSingle`или `AppleDouble`.

Параметры Outlook

Как отправитель, вы можете настроить кодирование сообщений в Outlook любым из указанных ниже способов.

- Настройка формата сообщений по умолчанию (обычного текста или HTML).
- Настройка формата сообщения (обычного текста или HTML) во время создания сообщений с помощью области **Формат** на вкладке **Формат текста**.
- Настройка параметров кодирования сообщений, отправляемых всем внешним получателям. Эти параметры называются *параметрами формата сообщений в Интернете* и применяются только к удаленным получателям (не к получателям в организации Exchange).
- Настройка параметров кодирования сообщений, отправляемых определенным внешним получателям (Outlook 2010 или более ранней версии). Эти параметры называются *параметрами формата сообщений получателей Через Интернет* и применяются только к удаленным получателям в папке "Контакты" (не к получателям в организации Exchange).

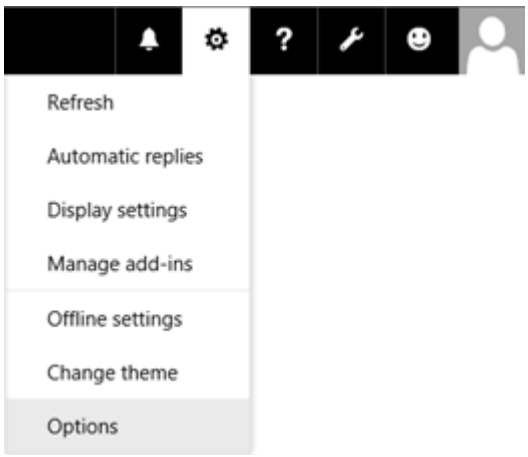
Инструкции по настройке этих параметров в Outlook см. в статье Изменение формата сообщений на HTML, RTF или обычный текст.

По умолчанию в Outlook используется автоматическое кодирование сообщений: весь текст исходящего сообщения сканируется, чтобы определить подходящую кодировку для него. Этот параметр применяется ко внутренним и внешним получателям. Однако можно обойти автоматическое выделение и указать предпочтительную кодировку для исходящих сообщений в разделе**Параметры**>**файла**>**Расширенные**>**международные параметры**.

Параметры Outlook в Интернете

Как отправитель, вы можете настраивать параметры кодирования сообщений в Outlook в Интернете любым из указанных ниже способов.

- Настройте формат сообщения по умолчанию в виде обычного текста или HTML в разделе **Формат сообщения** на странице Параметры**Макетпочты**>>>.



- Настройте формат сообщения в виде обычного текста или HTML при создании сообщения, щелкнув значок **Дополнительные параметры** выбрав **Переключиться на обычный текст** (если текущий формат — HTML) или **Переключиться на HTML** (если текущий формат — обычный текст).

Порядок применения для параметров кодирования сообщений

Некоторые параметры кодирования сообщений доступны в настройках удаленных доменов, почтовых контактов или почтовых пользователей, а также параметрах Outlook или Outlook в Интернете. В приведенном ниже списке представлены параметры кодирования исходящих сообщений, отправляемых внешним получателям, в порядке убывания приоритета.

1. Параметры почтовых контактов и почтовых пользователей (если включен параметр "Использовать рекомендуемый формат сообщений")
2. Параметры Outlook и Outlook в Интернете
3. Параметры удаленных доменов

Параметр более высокого уровня переопределяет соответствующий параметр более низкого уровня. Например, параметры почтовых контактов и почтовых пользователей переопределяют соответствующие параметры для удаленного домена. Уникальные параметры остаются без изменений (для них не возникает конфликт приоритетов).

В приведенных ниже разделах описывается порядок приоритетов для параметров кодирования сообщений.

Порядок применения кодировок сообщений

В приведенной ниже таблице представлены параметры кодировок сообщений в порядке убывания приоритета.

Source	Setting	Значения
Outlook	**Кодировка исходящих сообщений**	**Автовыбор кодировки исходящих сообщений**: включен или отключен (по умолчанию он включен). **Кодировка исходящих сообщений**: задана указанная кодировка. Этот параметр кодировки используется, если параметр **Автовыбор кодировки исходящих сообщений** отключен.
Удаленный домен	"Набор знаков MIME" и "Набор знаков не-MIME"	Заданные кодировки MIME и других типов (они могут быть одинаковыми).

Примечания.

- При настройке набора знаков не-MIME для удаленного домена эта кодировка назначается входящим или исходящим сообщениям в удаленном домене, не содержащим указанную кодировку.
- Значение кодовой страницы ANSI Windows сервера Exchange Server используется для назначения кодировки сообщениям следующих типов:
    - Внутренним сообщениям, которые не содержат определенного набора символов.
    - Внутренним сообщениям, которые содержат определенный набор символов, но не содержат определенной страницы кода сервера.
- Если сообщение содержит определенный, но недопустимый набор символов, сервер Exchange Server пытается заменить его на допустимый.

Порядок применения для параметров кодирования текстовых сообщений

В приведенной ниже таблице представлены параметры кодирования текстовых сообщений в порядке убывания приоритета.

Примечание. Здесь указаны только параметры для текстовых сообщений (а не параметры обычного текста для сообщений в кодировке MIME).

Source	Setting	Значения
Почтовый контакт или почтовый пользователь	Использовать рекомендуемый формат сообщений	Если задано значение `$true`, параметры кодирования обычного текстового сообщения для почтового контакта или пользователя почты переопределяют соответствующие параметры в Outlook. Если значение равно `$false`, параметры кодирования обычных текстовых сообщений для почтового контакта или пользователя почты игнорируются (используются соответствующие параметры в Outlook).
Почтовый контакт или почтовый пользователь	Формат сообщения	Текст
Почтовый контакт или почтовый пользователь	Формат текста сообщения	Текст
Почтовый контакт или почтовый пользователь	Формат вложений для Mac	`BinHex` или UUEncode
Outlook 2010 или более ранней версии	Формат сообщений Интернета для получателей (параметры для определенного контакта)	Отправка только обычным текстом Откройте контакт в папке > Контакты, дважды щелкните адрес > электронной почты, щелкните **Просмотреть дополнительные параметры для взаимодействия с этим пользователем**> выберите **Свойства Outlook**. В открывшемся диалоговом окне **Свойства электронной почты** выберите **Отправить только обычный текст** в поле **Формат Интернета** .
Outlook	Формат сообщений Интернета	Параметры обычного текста для внешних сообщений в**разделе Параметрыфайла**>**Формат**>**сообщения**>: **Кодировать вложения в формате UUENCODE при отправке текстовых сообщений** (не выбрано по умолчанию) **Автоматический перенос текста на nn знаков** (значение по умолчанию составляет 76).
Удаленный домен	Размер переносимой строки	132 символа или меньше, или значение `Unlimited`. Значение по умолчанию — `Unlimited`.

Порядок применения для параметров кодирования сообщений MIME

В приведенной ниже таблице представлены параметры кодирования сообщений MIME в порядке убывания приоритета.

Source	Setting	Значения
Почтовый контакт или почтовый пользователь	Использовать рекомендуемый формат сообщений	Если значение `$true`, параметры кодирования сообщений MIME для почтового контакта или пользователя почты переопределяют соответствующие параметры в Outlook. Если значение равно `$false`, параметры кодирования текстовых сообщений MIME для почтового контакта или пользователя почты игнорируются (используются соответствующие параметры в Outlook, Outlook в Интернете или удаленных доменах).
Почтовый контакт или почтовый пользователь	Формат сообщения	MIME
Почтовый контакт или почтовый пользователь	Формат текста сообщения	Text, HTML или `TextAndHtml` (значение по умолчанию — `TextAndHtml`).
Почтовый контакт или почтовый пользователь	Формат вложений для Mac	`BinHex`, `AppleSingle` или `AppleDouble` (значение по умолчанию — `BinHex`).
Outlook или Outlook в Интернете	формат сообщений;	Обычный текст или HTML
Удаленный домен	Тип содержимого	`MimeHtmlText` (значение по умолчанию), `MimeText` или `MimeHtml`

Exchange Server: параметры преобразования TNEF

Статья • 04.04.2023

TNEF, также известный как транспортный нейтральный формат инкапсуляции, формат форматов форматов текста Outlook или формат форматов текста, предназначенный для инкапсулирования свойств сообщений MAPI от Майкрософт. Все версии Outlook полностью поддерживают TNEF. Outlook в Интернете (ранее известный как Outlook Web App) преобразует TNEF в MAPI и отображает отформатированные сообщения. Другие почтовые клиенты, которые не поддерживают TNEF, обычно отображают сообщения в формате TNEF как обычные текстовые сообщения с вложениями Winmail.dat или Win.dat. Дополнительные сведения о формате TNEF см. в разделе Форматы сообщений в Exchange и Outlook.

Администраторы могут указать, что необходимо сделать с форматом TNEF (удалить или сохранить его) в сообщениях, отправляемых за пределы их организаций Exchange. Вы можете задать параметры преобразования формата TNEF в следующих расположениях:

- Раздел параметров удаленных доменов.
- Раздел параметров почтовых пользователей и почтовых контактов.
- Раздел параметров Outlook:
  - формат сообщений;
  - формат сообщений Интернета;
  - формат сообщений для получателей в Интернете (Outlook 2010 или более ранней версии).

Обычно параметры преобразования формата TNEF, используемые по умолчанию, работают хорошо (по умолчанию для внешних получателей система преобразовывает сообщения в формате TNEF в формат HTML). Тем не менее вам может потребоваться принудительно преобразовывать сообщения в обычный текст для получателей, использующих почтовые клиенты и системы обмена сообщениями более ранних версий. Они, скорее всего, сообщат вам, если в сообщениях в формате TNEF, поступающих из вашей среды Exchange, будут какие-либо проблемы с форматированием.

Дополнительные сведения о других преобразования содержимого в Exchange см. в статье Преобразование содержимого.

Параметры преобразования формата TNEF для удаленных доменов

Удаленные домены задают параметры для сообщений, отправляемых в домены, которые являются внешними для вашей организации Exchange. Дополнительные сведения см. в статье Remote Domains.

Когда вы настраиваете параметры преобразования формата TNEF для удаленного домена, эти параметры применяются ко всем сообщениям, отправляемым получателям в этом домене. Чтобы настроить эти параметры, вы можете использовать Центр администрирования Exchange или командную консоль Exchange.

- В EAC перейдите в раздел **Поток**> обработки**почты Значок Добавить удаленные домены**> или выберите существующий удаленный домен, а затем щелкните **Изменить**✏️>**Изменить Использовать формат форматов в формате форматов.**➕
- В командной консоли Exchange используйте параметр *TnefEnabled* в **командлете Set-RemoteDomain** .

Параметры преобразования формата TNEF для удаленных доменов описаны в таблице ниже.

Setting	**Значение в Центре администрирования Exchange**	**Значение в командной консоли Exchange**
Использовать формат TNEF для всех сообщений, отправляемых в удаленный домен.	**Постоянно**	`$true`
Не использовать формат TNEF для всех сообщений, отправляемых в удаленный домен.	**Никогда**	`$false`

Setting	Значение в Центре администрирования Exchange	Значение в командной консоли Exchange
Сообщения в формате TNEF не разрешены и не запрещены для получателей в удаленном домене. Это значение используется по умолчанию. То, отправляются ли сообщения в формате TNEF получателям в удаленном домене, зависит от определенного параметра почтового контакта или почтового пользователя либо от параметра, указанного отправителем в Outlook.	**Использовать параметры пользователя**	`$null` (пусто)

Параметры преобразования формата TNEF для почтовых пользователей и почтовых контактов

Почтовые контакты и почтовые пользователи представляют пользователей в вашей организации Exchange, у которых имеются внешние электронные адреса. Дополнительные сведения см. в статье Получатели.

Когда вы настраиваете параметры преобразования формата TNEF для почтового контакта или почтового пользователя, эти параметры применяются ко всем сообщениям, отправляемым этому получателю. Параметр *UseMapiRichTextFormat* используется в командлетах **Set-MailUser** и **Set-MailContact** в командной консоли Exchange. Допустимые значения:

- `Always`: TNEF используется для всех сообщений, отправляемых получателю.
- `Never`: TNEF никогда не используется для сообщений, отправляемых получателю.
- `UseDefaultSettings`: это значение по умолчанию. Сообщения в формате TNEF не разрешены и не запрещены для почтового пользователя или почтового контакта. То, следует ли отправлять сообщения в формате TNEF получателю, зависит от параметра преобразования формата TNEF для удаленного домена или параметра преобразования формата TNEF, настроенного отправителем в Outlook.

Параметры преобразования формата TNEF в Outlook

Отправители могут управлять параметрами преобразования, используемыми по умолчанию, для сообщений в формате TNEF, отправляемых внешним получателям. Эти параметры называются параметрами *формата сообщений Интернета*. Эти параметры применяются только ко внешним получателям и не применяются к получателям в организации Exchange.

Примечание. Следующие параметры определяют, как обрабатываются сообщения с форматированным текстом Outlook при их отправке внешним получателям. Если сообщения имеют формат HTML или формат обычного текста, эти параметры не применяются.

В Outlook доступны следующие варианты преобразования формата TNEF:

- **Преобразовать в формат HTML**. Это параметр по умолчанию. Сообщения в формате TNEF, отправляемые внешним получателям, преобразовываются в формат HTML. Любое форматирование в сообщении должно близко походить на форматирование в исходном сообщении. Сообщения в формате HTML с кодированием MIME поддерживаются большинством почтовых клиентов.

- **Преобразование в формат обычного текста**. Все сообщения TNEF, отправляемые удаленным получателям, преобразуются в обычный текст. Форматирование сообщения теряется.

- **Отправка с помощью формата форматированного текста Outlook**. Все сообщения TNEF, отправляемые удаленным получателям, остаются сообщениями TNEF.

В Outlook 2010 или более ранних версий отправители могут управлять параметрами преобразования, используемыми по умолчанию, для сообщений в формате TNEF, отправляемых определенным внешним получателям. Эти параметры называются параметрами *формата сообщений получателей в Интернете*. Эти параметры применяются только ко внешним получателям, хранящимся в вашей папке "Контакты" и не применяются к получателям в организации Exchange. В следующем списке описаны параметры преобразования формата TNEF для внешнего получателя в вашей папке "Контакты":

- **Разрешить Outlook выбрать оптимальный формат отправки**. Это параметр по умолчанию. Этот параметр заставляет Outlook использовать параметр преобразования TNEF, указанный в формате Интернета по умолчанию, как описано в предыдущем списке (**преобразовать в формат HTML**,

преобразовать в формат обычного текста или **Отправить с помощью формата формат rtf).** Таким образом, сообщение в формате TNEF можно оставить в формате TNEF, преобразовать в формат HTML или преобразовать в обычный текст (по умолчанию выполняется преобразование в формат HTML). Если вы хотите, чтобы сообщение в формате TNEF осталось в этом формате для определенного контакта, измените значение этого параметра на **Отправка в формате RTF Outlook**.

- **Отправлять только обычный текст**. Все сообщения TNEF, отправленные получателю, преобразуются в обычный текст. Форматирование сообщения теряется.
- **Отправка с помощью формата форматированного текста Outlook**. Все сообщения TNEF, отправляемые удаленным получателям, остаются сообщениями TNEF.

Сведения о том, как настроить параметры преобразования формата TNEF в Outlook см. в статье Изменение формата сообщения на HTML, RTF или обычный текст.

Приоритеты вариантов преобразования формата TNEF

Варианты преобразования формата TNEF для сообщений, отправляемых внешним получателям, описаны ниже и отсортированы по приоритету (от варианта с высшим приоритетом к варианту с низшим приоритетом).

1. Параметры удаленных доменов;
2. Параметры почтовых пользователей и почтовых контактов
3. Параметры Outlook

Параметр более высокого уровня переопределяет параметр более низкого уровня. Параметр формата TNEF в удаленном домене переопределяет параметр формата TNEF в почтовом контакте или почтовом пользователе либо параметр в Outlook. Например, вы отправляете сообщение в формате RTF в Outlook, но получатель находится в домене, в котором параметр удаленного домена не разрешает сообщения в формате TNEF. В результате получателю будет доставлено сообщение в виде обычного текста или в формате HTML, но не в формате TNEF.

Примечание. Exchange никогда не отправляет сообщения STNEF внешним получателям. Получателям за пределами организации Exchange можно отправлять сообщения только в формате TNEF.

Размер сообщений и ограничения получателей в Exchange Server

Статья • 04.04.2023

К сообщениям, передаваемым в организации, можно применять ограничения. Вы можете задать максимальный размер всего сообщения или отдельных его частей, а также и то, и другое. Например, вы можете ограничить максимальный размер заголовка сообщения или вложений, а также задать максимальное количество получателей, которых можно добавить в сообщение. Вы можете применить эти ограничения ко всей организации Exchange или отдельным соединителям, серверам и почтовым ящикам.

В этой статье описаны только ограничения на размер сообщения и количество получателей. Если вы хотите узнать больше о том, как управлять количеством сообщений, отправляемых с течением времени, сколько подключений разрешено с течением времени и как долго Exchange будет ждать перед закрытием подключения, см. статью Ограничения скорости сообщений и регулирование.

При планировании ограничений на размер сообщений для организации Exchange рассмотрите следующие вопросы:

- Какие ограничения на размер должны применяться ко всем входящим сообщениям?
- Какие ограничения на размер должны применяться ко всем исходящим сообщениям?
- Какова квота почтового ящика для организации и как выбранные ограничения на размер сообщения связаны с размером квоты почтового ящика?
- Есть ли в организации пользователи, которым необходимо отправлять и получать сообщения размера, превышающего максимально допустимый?
- Входят ли в организацию другие системы обмена сообщениями или подразделения, для которых требуются другие ограничения на размер сообщения?

В этой статье приведены рекомендации, которые помогут вам ответить на эти вопросы и применить соответствующее ограничения на размер сообщения в соответствующих местах.

Типы ограничений на размер сообщения

В следующем списке описаны основные типы ограничений на размер сообщений и компоненты сообщений, к которым они применяются.

- **Ограничения на размер всего сообщения**. Указывает максимальный размер сообщения, который включает заголовок сообщения, текст сообщения и все вложения. Exchange использует пользовательский заголовок сообщения **X-MS-Exchange-Organization-OriginalSize:** для записи исходного размера сообщения по мере его поступления в организацию Exchange. При проверке размера используется текущий размер сообщения или заголовок исходного размера сообщения (меньшее из значений). Размер сообщения может меняться из-за преобразования, кодирования или обработки содержимого агентом транспорта.

  Для любого ограничения на размер сообщений необходимо задать значение, которое превышает требуемый фактический размер. Это из-за кодировки Base 64 вложений и других двоичных данных. При кодировании Base64 размер сообщения увеличивается приблизительно на 33 %, поэтому указываемое значение должно быть на 33 % больше требуемого фактического размера сообщения. Например, если вы зададите 64 МБ как максимальный размер сообщения, реальный его размер будет составлять приблизительно 48 МБ или меньше.

- **Ограничения на размер вложений**. Задает максимальный размер одного вложения в сообщении. Сообщение может содержать много небольших вложений, которые значительно увеличивают его общий размер. Однако ограничение на размер вложения применяется только к одному вложению. Вы не можете ограничить количество вложений в сообщении, но можете ограничить максимальный размер сообщения.

- **Ограничения получателей**. Указывает общее число получателей, разрешенных в сообщении. Сюда входит общее число получателей в полях **Кому:**, **Копия:** и **Ск:** . Группа рассылки считается одним получателем.

- **Ограничения на размер заголовков сообщений**. Задает максимальный размер всех полей заголовков сообщений в сообщении. Размер текста сообщения или вложений не учитывается. Поскольку поля заголовка представляют собой обычный текст, размер заголовка определяется числом символов в каждом поле заголовка и общим числом полей заголовка. На каждый символ приходится 1 байт.

Область действия ограничений

В следующих таблицах показаны ограничения сообщений на уровне организации, соединителя, сервера и почтового ящика, включая сведения о настройке ограничений в Центре администрирования Exchange (EAC) или командной консоли Exchange. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

Ограничения для организации

Ограничения организации применяются ко всем серверам Exchange 2019, серверам Exchange 2016, серверам почтовых ящиков Exchange 2013 и транспортным серверам-концентраторам Exchange 2010, существующим в вашей организации. Любые ограничения, настраиваемые для организации на пограничных транспортных серверах, применяются к локальному серверу.

> ⓘ **Примечание**
>
> Ограничения организации также применяются к внешним отправителям и внешним получателям (анонимным или неуверенным отправителям или получателям):
>
> - Для входящих сообщений от внешних отправителей Exchange применяет максимальный размер сообщений для организации (максимальный размер получаемых сообщений, как описано в разделе **Ограничения получателей** , применяется к внутреннему получателю).
> - Для исходящих сообщений внешним получателям Exchange применяет максимальный размер получаемых сообщений организации (максимальный размер сообщения отправки, как описано в разделе **Ограничения получателей** , применяется к внутреннему отправителю).
>
> Таким образом, размер сообщения должен быть в пределах ограничений размера сообщения как для отправителя, так и для получателя. Эта концепция также описана в разделе **Порядок очередности и размещения ограничений на размер сообщений** далее в этом разделе.

Ограничение размера	Значение по умолчанию	Настройка в Центре администрирования Exchange	Настройка с помощью командной консоли Exchange

Ограничение размера	Значение по умолчанию	Настройка в Центре администрирования Exchange	Настройка с помощью командной консоли Exchange
Максимальный размер принимаемых сообщений	10 МБ	Поток >**обработки почтыСоединители**> получения **Другие параметры** ***>**Параметры**> транспорта организации **Вкладка "Ограничения"** >**Максимальный размер сообщения о получении (МБ)**	Командлет: **Set-TransportConfig** Параметр: *MaxReceiveSize*
Максимальный размер отправляемых сообщений	10 МБ	Поток >**обработки почтыСоединители**> получения **Другие параметры** ***>**Параметры**> транспорта организации **Ограничения**>**Максимальный размер сообщения отправки (МБ)**	Командлет: **Set-TransportConfig** Параметр: *MaxSendSize*
Максимальное количество получателей в сообщении	500	Поток >**обработки почтыСоединители**> получения **Другие параметры** ***>**Параметры**> транспорта организации **Ограничиваетмаксимальное число получателей**	Командлет: **Set-TransportConfig** Параметр: *MaxRecipientEnvelopeLimit*
Максимальный размер вложения для сообщения, соответствующего условиям правила потока обработки почты (также известного как правило транспорта)	Не настроено	Поток >**обработки почтыПравила**>**Добавить**+ >**Создайте новое правило** или выберите существующее правило и нажмите кнопку **Изменить**. Нажмите кнопку **Дополнительные параметры**. Используйте условие **Применение этого правила, если**>**размер любого вложения**>**больше или равен**, и введите значение в килобайтах (КБ).	Командлеты: **New-TransportRule**, **Set-TransportRule** Параметр *: AttachmentSizeOver*

Ограничение размера	Значение по умолчанию	Настройка в Центре администрирования Exchange	Настройка с помощью командной консоли Exchange
Максимальный размер сообщения, соответствующего условиям правила потока обработки почты	Не настроено	Поток >**обработки почтыПравила**>**Добавить**➕>**Создайте новое правило** или выберите существующее правило и нажмите кнопку **Изменить**✏️. Нажмите кнопку **Дополнительные параметры**. Используйте условие . **Примените это правило, если**> размер**сообщения**>**больше или равен**, и введите значение в килобайтах (КБ).	Командлеты: **New-TransportRule**, **Set-TransportRule** Параметр *: MessageSizeOver*

Чтобы просмотреть значения этих организационных ограничений, выполните следующие команды в командной консоли Exchange:

PowerShell

```
Get-TransportConfig | Format-List
MaxReceiveSize,MaxSendSize,MaxRecipientEnvelopeLimit
```

PowerShell

```
Get-TransportRule | where {($_.MessageSizeOver -ne $null) -or
($_.AttachmentSizeOver -ne $null)} | Format-Table
Name,MessageSizeOver,AttachmentSizeOver
```

Ограничения для соединителя

Ограничения для соединителя применяются ко всем сообщениям, которые доставляются с помощью указанного соединителя отправки, соединителя получения, соединителя агента доставки или внешнего соединителя.

Вы можете назначить определенные ограничения на размер сообщений для ссылок на сайты Active Directory в организации. Транспортная служба на серверах почтовых ящиков использует сайты Active Directory, а затраты, назначенные для ссылок IP-сайтов Active Directory, являются одним из факторов, определяющих путь маршрутизации с наименьшими затратами между серверами Exchange в организации.

Вы можете назначить ограничения на размер сообщения для соединителей агента доставки и внешних соединителей, которые используются для отправки сообщений не через SMTP-сервер в организации.

Ограничение размера	**Значение по умолчанию**	**Настройка в Центре администрирования Exchange**	**Настройка с помощью командной консоли Exchange**
Максимальный размер сообщения, отправляемого с использованием соединителя получения	36 МБ	Поток >**обработки почтыСоединители**> получения **Изменить**. >**Общие**>**Максимальный размер сообщения о получении (МБ)**	Командлеты: **New-ReceiveConnector**, **Set-ReceiveConnector** Параметр: *MaxMessageSize*
Максимальный размер всех полей заголовка в сообщении, отправляемом через соединитель получения	256 КБ	Недоступно	Командлеты: **New-ReceiveConnector**, **Set-ReceiveConnector** Параметр: *MaxHeaderSize*

Ограничение размера	Значение по умолчанию	Настройка в Центре администрирования Exchange	Настройка с помощью командной консоли Exchange
Максимальное количество получателей в сообщении, отправляемом с использованием соединителя получения	**Транспортная служба на серверах почтовых ящиков** ServerName по умолчанию<*: 5000*> Имя *прокси-сервера*< > клиента: 200 **Внешняя служба транспорта на серверах почтовых ящиков**. Имя внешнего <*сервера*> по умолчанию: 200 Исходящий прокси-сервер Внешнего <*сервера*>: 200 Внешний <*сервер клиента:*> 200 Если в сообщении от анонимного отправителя (например, из Интернета) превышено количество получателей, оно принимается для первых 200 получателей. Большинство серверов обмена сообщениями продолжают отправлять сообщение 200 получателям за раз, пока оно не будет доставлено всем.	Недоступно	Командлеты: **New-ReceiveConnector**, **Set-ReceiveConnector** Параметр: *MaxRecipientsPerMessage*

Ограничение размера	Значение по умолчанию	Настройка в Центре администрирования Exchange	Настройка с помощью командной консоли Exchange
Максимальный размер сообщения, отправляемого через соединитель отправки	10 МБ	Поток >**обработки почтыОтправка соединителей**>**Изменить** >**Вкладка "Общие"** >**Максимальный размер сообщения отправки (МБ)**	Командлеты: **New-SendConnector**, **Set-SendConnector** Параметр: *MaxMessageSize*
Максимальный размер сообщения, отправленного через ссылку на сайт Active Directory	Без ограничений	Недоступно	Командлет **Set-AdSiteLink** Параметр: *MaxMessageSize*
Максимальный размер сообщения, отправляемого с использованием соединителя агента доставки	Без ограничений	Недоступно	Командлеты: **New-DeliveryAgentConnector**, **Set-DeliveryAgentConnector** Параметр: *MaxMessageSize*
Максимальный размер сообщения, отправляемого с использованием внешнего соединителя	Без ограничений	Недоступно	Командлет **Set-ForeignConnector** Параметр: *MaxMessageSize*

Чтобы просмотреть значения этих ограничений соединителя, выполните следующую команду в командной консоли Exchange:

PowerShell

```
Get-ReceiveConnector | Format-Table Name,Max*Size,MaxRecipientsPerMessage; Get-SendConnector | Format-Table Name,MaxMessageSize; Get-AdSiteLink | Format-Table Name,MaxMessageSize; Get-DeliveryAgentConnector | Format-Table Name,MaxMessageSize; Get-ForeignConnector | Format-Table Name,MaxMessageSize
```

Ограничения для сервера

Ограничения для серверов применяются к серверам почтовых ящиков или пограничным транспортным серверам. Эти ограничения на размер сообщения можно задать отдельно для каждого сервера почтовых ящиков или пограничного транспортного сервера.

Ограничение размера	**Значение по умолчанию**	**Настройка в Центре администрирования Exchange**	**Настройка с помощью командной консоли Exchange**
Максимальный размер сообщения, отправленного клиентами Outlook в Интернете	35 МБ	Недоступно	Это значение настраивается в файлах конфигурации XML-приложений (web.config) на сервере почтовых ящиков. Дополнительные сведения см. в разделе Настройка ограничений на размер сообщений, зависящих от клиента.
Максимальный размер сообщения, отправленного клиентами Exchange ActiveSync	10 МБ	Недоступно	Это значение настраивается в файлах конфигурации XML-приложений (web.config) на сервере почтовых ящиков. Дополнительные сведения см. в разделе Настройка ограничений на размер сообщений, зависящих от клиента.
Максимальный размер сообщения, отправляемого клиентами веб-служб Exchange	64 МБ	Недоступно	Это значение настраивается в файлах конфигурации XML-приложений (web.config) на сервере почтовых ящиков. Дополнительные сведения см. в разделе Настройка ограничений на размер сообщений, зависящих от клиента.

Вы также можете настроить ограничения на размер сообщения для каталога раскладки, доступного на пограничных транспортных серверах и серверах почтовых ящиков. Как правило, каталог раскладки не используется в повседневном потоке обработки почты. Он используется администраторами для проверки потока обработки почты или приложениями, которые создают и отправляют собственные файлы сообщений. Дополнительные сведения см. в статье Configure the Pickup Directory and the Replay Directory.

- Максимальный размер всех полей заголовков в файле сообщения, помещаемом в каталог раскладки: 64 КБ.
- Максимальное количество получателей в файле сообщения, помещаемом в каталог раскладки: 100.

Ограничения для получателей

Эти ограничения применяются к определенному объекту-пользователю, например почтовому ящику, почтовому контакту, почтовому пользователю, группе рассылки или общедоступной папке с включенной почтой.

Ограничение размера	**Значение по умолчанию**	**Настройка в Центре администрирования Exchange**	**Настройка с помощью командной консоли Exchange**
Максимальный размер сообщения, которое может быть отправлено конкретному получателю	Политики подготовки почтовых ящиков сайта: 36 МБ Все остальные типы получателей: не ограничено	Для почтовых ящиков: **Получателей**>**Почтовых ящиков**>**Изменить** > Функции >**почтового ящика** Раздел >**Поток обработки почты** Ограничения **размера сообщений** раздел >**Просмотр сведений о**>**полученных сообщениях** раздел >**Максимальный размер сообщения (КБ)** Для почтовых пользователей: **Получателей**>**Контакты**>**Изменить** > редактирования**Параметры потока почты**> Ограничения >**размера сообщенийПросмотр сведений**>**О полученных сообщениях** раздел >**Максимальный размер сообщения (КБ)** Этот параметр доступен в Центре администрирования Exchange для остальных типов получателей.	Командлеты: **Настроить DistributionGroup** **Настроить DynamicDistributionGroup** **Set-Mailbox** **Set-MailContact** **Set-MailUser** **Set-MailPublicFolder** **New-SiteMailboxProvisioningPolicy** **Set-SiteMailboxProvisioningPolicy** Параметр: *MaxReceiveSize*

Ограничение размера	**Значение по умолчанию**	**Настройка в Центре администрирования Exchange**	**Настройка с помощью командной консоли Exchange**
Максимальный размер сообщения, отправляемого определенным отправителем	Без ограничений	Для почтовых ящиков: **Получателей**>**Почтовых ящиков**>**Изменить** > Функции >**почтового ящика** Раздел >**Поток обработки почты** Раздел **Ограничения размера сообщений** раздел >**Просмотр сведений о**>**отправленных сообщениях** раздел >**Максимальный размер сообщения (КБ)** Для почтовых пользователей: **Получателей**>**Контакты**>**Изменить** > редактирования**Параметры потока почты**> Ограничения**размера сообщений** раздел >**Просмотр сведений о**>**отправленных сообщениях** раздел >**Максимальный размер сообщения (КБ)** Этот параметр доступен в Центре администрирования Exchange для остальных типов отправителей.	Командлеты: **Настроить DistributionGroup** **Настроить DynamicDistributionGroup** **Set-Mailbox** **Set-MailContact** **Set-MailUser** **Set-MailPublicFolder** Параметр: *MaxSendSize*
Максимальное количество получателей в сообщении, отправляемом определенным отправителем	Без ограничений	Для почтовых ящиков: **Получателей**>**Почтовых ящиков**>**Изменение** > Функции >**почтового ящика**в разделе "**Поток обработки почты**" **Просмотр**> сведений о >**разделе**> Ограничение **получателей максимальное число получателей** Этот параметр недоступен в Центре администрирования Exchange для почтовых пользователей.	Командлеты: **Set-Mailbox**, **Set-MailUser** Параметр: *RecipientLimits*

Чтобы просмотреть значения этих ограничений, выполните соответствующий командлет **Get-** для типа получателя в командной консоли Exchange.

Например, чтобы просмотреть ограничения, настроенные для определенного почтового ящика, выполните следующую команду:

```
PowerShell
```

```
Get-Mailbox <MailboxIdentity> | Format-List
MaxReceiveSize,MaxSendSize,RecipientLimits
```

Чтобы просмотреть ограничения, настроенные для всех почтовых ящиков пользователей, выполните следующую команду:

PowerShell

```
$mb= Get-Mailbox -ResultSize unlimited; $mb | where {$_.RecipientTypeDetails
-eq 'UserMailbox'} | Format-Table
Name,MaxReceiveSize,MaxSendSize,RecipientLimits
```

Очередность и уровень применения ограничений на размер сообщения

Всегда применяется самое жесткое из доступных ограничение на размер сообщения. Остается только решить, где именно оно применяется. Цель — отклонять слишком большие сообщения в транспортном конвейере как можно раньше. Например, системные ресурсы будут расходоваться бесполезно, если соединитель получения через Интернет будет принимать большие сообщения, которые затем будут отклоняться из-за более низкого ограничения для организации. Убедитесь, что существующие ограничения для организации, серверов и соединителей настроены так, чтобы максимально сократить все ненужные процедуры обработки сообщений. Это можно сделать, сохранив одинаковые ограничения во всех расположениях или настроив более строгие ограничения, в которых сообщения попадают в организацию Exchange.

Исключением из порядка являются ограничения на размер сообщений в почтовых ящиках и ограничения на размер сообщений в правилах потока обработки почты. Exchange проверяет максимальный размер сообщения, допустимый для почтовых ящиков, прежде чем правила потока обработки сообщений. Если ограничение на размер сообщения в организации составляет 50 МБ, настройте, например, ограничение 35 МБ для почтового ящика и правило транспорта для поиска и отклонения сообщений, размер которых превышает 40 МБ. Если внешний отправитель отправит в почтовый ящик сообщение размером 45 МБ, оно будет отклонено, прежде чем правило транспорта сможет его обработать.

Ограничения на размер сообщения для организации не затрагивают ограничения для прошедших аутентификацию отправителей и получателей (как правило, внутренних). Поэтому для отдельных отправителей и получателей можно настроить более мягкие ограничения, чем для остальных. Например, вы можете разрешить

отдельным почтовым ящикам отправлять и получать сообщения, размер которых превышает ограничение для организации, настроив для них особые ограничения.

Однако это исключение применяется только к прошедшим аутентификацию отправителям и получателям (как правило, внутренним). К анонимным отправителям и получателям (как правило, для доставки через Интернет) применяются ограничения для организации. Предположим, что ограничение на размер сообщения в организации — 10 МБ, но вы разрешили пользователям в отделе маркетинга отправлять и получать сообщения размером до 50 МБ. Эти пользователи смогут обмениваться большими сообщениями друг с другом, но не смогут получать или принимать сообщения через Интернет (вовлечение не прошедших аутентификацию получателей и отправителей невозможно).

Совместная работа ограничений получателей

Ограничение получателей для сообщения применяется в двух местах:

- На уровне протокола во время передачи электронной почты, где применяется соединитель получения *MaxRecipientsPerMessage* .
- На уровне транспорта во время классификации, где применяется *MaxRecipientEnvelopeLimit* .

Существует также уровень почтового ящика *RecipientLimits*, который переопределяет уровень транспорта *MaxRecipientEnvelopeLimit* и также применяется во время классификации сообщений. Если для уровня почтового ящика *RecipientLimits* задано значение `unlimited` (значение по умолчанию), максимальное число получателей на сообщение для почтового ящика контролируется уровнем транспорта *MaxRecipientEnvelopeLimit*.

Для входящего сообщения электронной почты сначала проверяется соединитель получения *MaxRecipientsPerMessage* . Однако если число получателей превышает ограничение, сообщение не отклоняется; подключение получает ошибку , `452 4.5.3 Too many recipients`. Большинство почтовых серверов понимают эту ошибку, и они будут продолжать повторно отправлять сообщение в другом соединении, пока сообщение не будет доставлено всем получателям.

Соединитель получения *MaxRecipientsPerMessage* применяется к отправке клиента SMTP с проверкой подлинности и анонимной проверкой подлинности. Однако, когда сервер Exchange server ретранслирует электронную почту через другой сервер Exchange в той же организации, соединитель получения *MaxRecipientsPerMessage* обходится.

При принятии сообщения и отправке сообщения электронной почты в классификатор проверяется уровень почтового ящика *RecipientLimits* (если для него не задано значение `unlimited`) или уровень транспорта *MaxRecipientEnvelopeLimit* . Если число получателей превышает это ограничение, сообщение отклоняется и отправляется сообщение с ошибкой `550 5.5.3 RESOLVER.ADR.RecipLimit; too many recipients`.

Ниже приведен пример сценария:

Соединитель `MaxRecipientsPerMessage` получения имеет значение 100, а уровень `MaxRecipientEnvelopeLimit` транспорта — 500. Теперь, если кто-то отправляет входящие сообщения электронной почты 1000 получателям, это сообщение обычно будет принято, так как ограничение соединителя получения приведет к тому, что сервер отправки будет отправлять сообщения электронной почты в 10 блоках с 100 получателями в каждом сообщении, что ниже, чем параметр `MaxRecipientEnvelopeLimit`классификатора транспорта.

Сообщения, к которым не применяются ограничения размера

Ниже перечислены типы сообщений, создаваемых серверами почтовых ящиков или пограничными транспортными серверами, к которым не применяются ограничения на размер сообщения, кроме ограничения на количество получателей в сообщении для организации.

- Системные сообщения.
- Сообщение, созданное агентом.
- Уведомления о доставке, или отчеты о недоставке. Однако вы можете использовать параметры *ExternalDsnMaxMessageAttachSize* и *InternalDsnMaxMessageAttachSize* в командлете **Set-TransportConfig**, чтобы ограничить размер исходных сообщений, которые включаются в отчеты о недоставке (а значит, и размер самого отчета).
- Отчеты журнала.
- Сообщения на карантине.

Ограничения скорости сообщений и регулирование

Статья • 04.04.2023

Регулирование сообщений — это группа ограничений, устанавливаемых на количество сообщений и подключений, которые могут быть обработаны сервером Exchange Server. В их число входят ограничения на скорость обработки сообщений, скорость SMTP-подключения и время действия сеанса SMTP. Вместе эти ограничения помогают защитить сервер Exchange от перегрузки из-за приема и отправки большого количества сообщений. У вас может накопиться длинная очередь сообщений, ожидающих обработки, но регулирование количества сообщений позволяет серверу Exchange организованно обрабатывать сообщения и подключения.

> ⓘ **Примечание**
>
> *Обратная нагрузка* — это еще одна функция, которая помогает избежать перегрузки системных ресурсов сервера Exchange Server. Отслеживаются ключевые ресурсы, такие как доступное дисковое пространство и использование памяти, а когда уровень использования превышает заданный порог, сервер постепенно прекращает принимать новые подключения и сообщения. Дополнительные сведения см. в разделе **Общие сведения о давлении на спину**. Кроме того, для сообщений доступны статические ограничения, такие как максимальный размер сообщения, размеры отдельных вложений и количество получателей. Дополнительные сведения об ограничениях на размер сообщений см. **в разделе Ограничения размера сообщений и получателей в Exchange Server**.

Вы можете задавать ограничения на количество сообщений и параметры регулирования в следующих расположениях:

- Серверы почтовых ящиков и пограничные транспортные серверы. Их совокупное название — *транспортные серверы*.
- Соединители отправки
- Соединители получения
- Пользователи

Регулирование количества сообщений на транспортных серверах

В представленной ниже таблице приведены параметры регулирования количества сообщений, доступные на серверах почтовых ящиков и пограничных транспортных серверах.

Ограничение частоты	Значение по умолчанию	Настройка с помощью командной консоли Exchange	Настройка в Центре администрирования Exchange

Ограничение частоты	Значение по умолчанию	Настройка с помощью командной консоли Exchange	Настройка в Центре администрирования Exchange
Максимальное количество одновременных доставок почтовых ящиков. Максимальное количество потоков доставки, которые могут одновременно открываться транспортной службой и службой доставки почтовых ящиков для доставки сообщений в почтовые ящики.	20 Рекомендуется не изменять это значение, если только вы не будете направлены на это службой поддержки Майкрософт.	Командлет : **Set-TransportService** и **Set-MailboxTransportService** p> Parameter: *MaxConcurrentMailboxDeliveries*	Недоступно
Максимальное количество одновременных отправки почтовых ящиков. Максимальное количество потоков отправки, которые могут одновременно открываться службой транспорта и службой отправки почтовых ящиков для отправки сообщений из почтовых ящиков.	20 Рекомендуется не изменять это значение, если только вы не будете направлены на это службой поддержки Майкрософт.	Командлеты: **Set-TransportService** и **Set-MailboxTransportService** Параметр: *MaxConcurrentMailboxSubmissions*	Недоступно

Ограничение частоты	Значение по умолчанию	Настройка с помощью командной консоли Exchange	Настройка в Центре администрирования Exchange
Максимальная скорость подключения в минуту: максимальная скорость, которую можно открывать с помощью службы транспорта.	1200	Командлет: **Set-TransportService** Параметр: *MaxConnectionRatePerMinute*	Недоступно
Максимальное количество одновременных подключений. Максимальное количество исходящих подключений, которые может одновременно открывать служба транспорта.	1000 Это значение должно быть больше или равно *значению MaxPerDomainOutboundConnections* .	Командлет: **Set-TransportService** Параметр: *MaxOutboundConnections*	**Серверов**>**Серверов**>**Значок** ✎ > Раздел >**Ограничения транспортаМаксимальное количество одновременных подключений**. **Примечание.** В EAC можно задать только значения 100, 1000, 5000 или неограниченно.
Максимальное количество одновременных подключений на домен. Максимальное число исходящих подключений, которые может одновременно открыть транспортная служба для одного домена.	20 Это значение должно быть меньше или равно *значению MaxOutboundConnections* .	Командлет: **Set-TransportService** Параметр: *MaxPerDomainOutboundConnections*	**Серверов**>**Серверов**>**Значок** ✎ > Раздел >**Ограничения транспортаМаксимальное количество одновременных подключений на домен**. **Примечание.** В EAC можно задать только значения 100, 1000, 5000 или неограниченно.

Чтобы просмотреть значения этих параметров регулирования для сообщений на сервере, выполните следующую команду в командной консоли Exchange:

PowerShell

```
Write-Host "Transport service:" -ForegroundColor yellow; Get-TransportService | Format-List
MaxConcurrent*,MaxConnection*,Max*OutboundConnections; Write-Host "Mailbox Transport service:" -
ForegroundColor yellow; Get-MailboxTransportService | Format-List MaxConcurrent*
```

ⓘ **Примечание**

Каталог Pickup и каталог воспроизведения, доступные на пограничных транспортных серверах и серверах почтовых ящиков, также имеют ограничения скорости сообщений, которые можно настроить. Как правило, каталоги раскладки и преобразования не используются в повседневном потоке обработки почты. Дополнительные сведения см. в статье **Configure the Pickup Directory and the Replay Directory**. Максимальное количество файлов сообщений в минуту, которые могут обрабатываться каталогом Pickup и каталогом воспроизведения, составляет 100. Каждый каталог может независимо обрабатывать файлы сообщений с такой частотой.

Регулирование количества сообщений на соединителях отправки

В приведенной ниже таблице представлены параметры регулирования количества сообщений, доступные на соединителях отправки. Соединители отправки находятся в службе транспорта на серверах почтовых ящиков и на пограничных транспортных серверах. Дополнительные сведения см. в разделе Отправка соединителей.

Ограничение частоты	**Значение по умолчанию**	**Настройка с помощью командной консоли Exchange**	**Настройка в Центре администрирования Exchange**
Время ожидания бездействия подключения. Максимальное время, в течение чего открытое SMTP-подключение с исходным сервером обмена сообщениями может оставаться в состоянии простоя до закрытия подключения.	`00:10:00` (10 минут)	Командлеты: **New-SendConnector** и **Set-SendConnector** Параметр *: ConnectionInactivityTimeOut*	Недоступно
Максимальное число сообщений на подключение: максимальное количество сообщений, которые можно отправить через одно подключение.	20	Командлеты: **New-SendConnector** и **Set-SendConnector** Параметр *: SmtpMaxMessagesPerConnection*	Недоступно

Чтобы просмотреть значения этих параметров регулирования для соединителя отправки, выполните следующую команду в командной консоли Exchange:

PowerShell

```
Get-SendConnector | Format-List Name,ConnectionInactivityTimeout,SmtpMaxMessagesPerConnection
```

Регулирование количества сообщений на соединителях получения

В приведенной ниже таблице представлены параметры регулирования количества сообщений, доступные на соединителях получения. Соединители получения доступны во внешней службе транспорта на серверах почтовых ящиков, в службе транспорта на серверах почтовых ящиков и на пограничных транспортных серверах. Подробнее см. в разделе Соединители получения.

Ограничение частоты	Значение по умолчанию	Настройка с помощью командной консоли Exchange	Настройка в Центре администрирования Exchange
Время ожидания подключения. Максимальное время, в течение чего SMTP-подключение с исходным сервером обмена сообщениями может оставаться открытым, даже если исходный сервер обмена сообщениями передает данные.	`00:10:00` (10 минут) для соединителей получения на серверах почтовых ящиков. `00:05:00` (1 минута) для соединителей получения на пограничных транспортных серверах. Это значение должно быть больше *значения ConnectionInactivityTimeOut* .	Командлеты: **New-ReceiveConnector** и **Set-ReceiveConnector** Параметр: *ConnectionTimeout*	Недоступно
Время ожидания бездействия подключения. Максимальное время, в течение чего открытое SMTP-подключение с исходным сервером обмена сообщениями может оставаться в состоянии простоя до закрытия подключения.	`00:05:00` (5 минут) для соединителей получения на серверах почтовых ящиков. `00:01:00` (1 минута) для соединителей получения на пограничных транспортных серверах. Это значение должно быть меньше значения *ConnectionTimeout* .	Командлеты: **New-ReceiveConnector** и **Set-ReceiveConnector** Параметр *: ConnectionInactivityTimeOut*	Недоступно
Максимальное количество входящих подключений. Максимальное число входящих SMTP-подключений, разрешенных одновременно.	5000	Командлеты: **New-ReceiveConnector** и **Set-ReceiveConnector** Параметр: *MaxInboundConnection*	Недоступно
Максимальное количество входящих подключений на источник. Максимальное количество входящих SMTP-подключений, разрешенных одновременно с исходного сервера обмена сообщениями.	`unlimited` в соединителе получения по умолчанию с именем Default *<ServerName>* в транспортной службе на серверах почтовых ящиков. 20 для других соединителей получения на серверах почтовых ящиков и пограничных транспортных серверах.	Командлеты: **New-ReceiveConnector** и **Set-ReceiveConnector** Параметр: *MaxInboundConnectionPerSource*	Недоступно

Ограничение частоты	Значение по умолчанию	Настройка с помощью командной консоли Exchange	Настройка в Центре администрирования Exchange
Максимальный процент входящих подключений на источник. Максимальный процент входящих SMTP-подключений, которые одновременно разрешены с исходного сервера обмена сообщениями.	100 процентов на соединителе получения по умолчанию с именем Default <*ServerName*> в транспортной службе на серверах почтовых ящиков. 2 процента для других соединителей получения на серверах почтовых ящиков и пограничных транспортных серверах.	Командлеты: **New-ReceiveConnector** и **Set-ReceiveConnector** Параметр: *MaxInboundConnectionPercentagePerSource*	Недоступно

Ограничение частоты	Значение по умолчанию	Настройка с помощью командной консоли Exchange	Настройка в Центре администрирования Exchange
Ограничение скорости сообщений. Максимальное количество сообщений в минуту, которые могут быть отправлены одним источником.	`unlimited` на следующих соединителях получения по умолчанию: • *ServerName> по умолчанию<* в транспортной службе на серверах почтовых ящиков. • Внешний *<сервер по умолчаниюИмя>* в службе транспорта переднего плана на серверах почтовых ящиков. • Исходящий прокси-сервер Frontend *<ServerName>* в транспортной службе переднего плана на серверах почтовых ящиков. 5 на следующих соединителях получения по умолчанию: • *Прокси-сервер< клиентаимя>* в транспортной службе на серверах почтовых ящиков. • Клиентский внешний *<серверимя>* в службе транспорта переднего плана на серверах почтовых ящиков. 600 в соединителе получения по умолчанию с именем По умолчанию внутренний соединитель *<получения ServerName>* на пограничных транспортных серверах.	Командлеты: **New-ReceiveConnector** и **Set-ReceiveConnector** Параметр *: MessageRateLimit*	Недоступно

Ограничение частоты	Значение по умолчанию	Настройка с помощью командной консоли Exchange	Настройка в Центре администрирования Exchange
Источник частоты сообщений. Указывает, как вычисляется скорость отправки сообщений. Допустимые значения: • `User`: скорость отправки пользователя (в зависимости от того, как пользователь проходит проверку подлинности в сеансе SMTP). • `IPAddress`: скорость вычисляется для отправки узлов. • `All`: скорость рассчитывается как для отправки пользователей, так и для отправляя узлы.	`IPAddress` на следующих соединителях получения по умолчанию: • *ServerName> по умолчанию<* в транспортной службе на серверах почтовых ящиков. • Внешний *<сервер по умолчаниюИмя>* в службе транспорта переднего плана на серверах почтовых ящиков. • Исходящий прокси-сервер Frontend *<ServerName>* в транспортной службе переднего плана на серверах почтовых ящиков. • По умолчанию внутренний соединитель *<получения ServerName>* на пограничных транспортных серверах. `User` на следующих соединителях получения по умолчанию: • *Прокси-сервер< клиентаимя>* в транспортной службе на серверах почтовых ящиков. • Внешний *<сервер клиентаимямя>* в службе транспорта переднего плана на серверах почтовых ящиков	Командлеты: **New-ReceiveConnector** и **Set-ReceiveConnector** Параметр: *MessageRateSource*	Недоступно

Ограничение частоты	Значение по умолчанию	Настройка с помощью командной консоли Exchange	Настройка в Центре администрирования Exchange
Интервал тарпита. Время искусственной задержки SMTP-ответов на удаленные серверы без проверки подлинности, которые, как представляется, злоупотребляют подключением. Авторизованные подключения никогда не задерживаются таким образом.	`00:00:05` (5 секунд)	Командлеты: **New-ReceiveConnector** и **Set-ReceiveConnector** Параметр *: TarpitInterval*	Недоступно

Чтобы просмотреть значения этих параметров регулирования для соединителя получения, выполните следующую команду в командной консоли Exchange:

```
PowerShell

Get-ReceiveConnector | Format-List Name,Connection*,MaxInbound*,MessageRate*,TarpitInterval
```

Регулирование количества сообщений для пользователей

Служба регулирования Microsoft Exchange отслеживает параметры ресурсов на предмет определенных применений и кэширует эти сведения в память. Параметры регулирования потока почты также называются *бюджетом*. При перезапуске службы регулирования Microsoft Exchange также выполняется сброс бюджетов регулирования для потоков обработки почты.

Каждый почтовый ящик имеет параметр *ThrottlingPolicy* . Значение по умолчанию для этого параметра пусто (`$null`). Чтобы настроить политику регулирования для почтового ящика, можно использовать параметр *ThrottlingPolicy* в командлете **Set-Mailbox** .

Дополнительную информацию см. в следующих статьях:

- Управление рабочей нагрузкой пользователей в Exchange Server
- Change User Throttling Settings for Specific Users
- Change User Throttling Settings for All Users in Your Organization

Общие сведения о замедленной обратной реакции

Статья • 04.04.2023

Обратная нагрузка — это функция мониторинга системных ресурсов транспортной службы Microsoft Exchange, которая существует на серверах почтовых ящиков и пограничных транспортных серверах. Обратная нагрузка обнаруживает, когда жизненно важные системные ресурсы, такие как место на жестком диске и память, используются чрезмерно, и принимает меры, чтобы предотвратить полную перегрузку и недоступность сервера. Например, если уровень использования системных ресурсов на сервере Exchange Server определен как слишком высокий, сервер задерживает прием новых сообщений. Если использование ресурсов ухудшается, сервер перестает принимать новые сообщения, чтобы работать исключительно над обработкой всех существующих сообщений, и может даже прекратить обработку исходящих сообщений. Когда использование системных ресурсов возвращается к приемлемому уровню, сервер Exchange возобновляет нормальную работу, принимая новые сообщения и обрабатывая исходящие сообщения.

Отслеживаемые ресурсы

Функция замедленной обратной реакции позволяет наблюдать за использованием следующих системных ресурсов:

- **DatabaseUsedSpace[%ExchangeInstallPath%TransportRoles\data\Queue]**: использование жесткого диска для диска, на котором хранится база данных очереди сообщений.
- **PrivateBytes**: память, используемая процессом EdgeTransport.exe.
- **QueueLength[SubmissionQueue]**: количество сообщений в очереди отправки.
- **SystemMemory**: память, используемая всеми другими процессами.
- **UsedDiskSpace[%ExchangeInstallPath%TransportRoles\data\Queue]**: использование жесткого диска для диска, на котором хранятся журналы транзакций базы данных очереди сообщений.
- **UsedDiskSpace[%ExchangeInstallPath%TransportRoles\data]**: использование жесткого диска для диска, используемого для преобразования содержимого.
- **UsedVersionBuckets[%ExchangeInstallPath%TransportRoles\data\Queue\mail.que]**: количество незафиксированных транзакций базы данных очереди сообщений, которые существуют в памяти.

Для каждого отслеживаемого системного ресурса на сервере почтовых ящиков или пограничном транспортном сервере определяются следующие уровни использования ресурсов или *нагрузки* :

- **Низкий или обычный**. Ресурс не используется. Сервер принимает новые подключения и сообщения.
- **Средний**. Ресурс немного переиспользуется. Замедленная обратная реакция применяется к серверу в ограниченном объеме. Поток почты от отправителей на уполномоченных доменах организации не прерывается. Однако в зависимости от перегруженного ресурса сервер использует искусственную задержку ответов, чтобы задержать отклик сервера, или отклоняет входящие команды **MAIL FROM** из других источников.
- **Высокий:** ресурс сильно переиспользуется. Замедленная обратная реакция применяется в полном объеме. Передача всех сообщений прекращается, и сервер отклоняет все новые входящие команды **MAIL FROM**.

Уровни перехода определяют значения низкого, среднего и высокого уровней использования ресурсов в зависимости от того, повышается загруженность или понижается. Как правило, при понижении загруженности ресурса уровень его использования должен быть ниже исходного. Другими словами, не существует постоянных значений для низкой, средней и высокой загруженности ресурсов. Чтобы определить следующее изменение уровня использования ресурса, необходимо знать, повышается загруженность или понижается.

В следующих разделах поясняется, какие операции выполняет Exchange при перегрузке определенного ресурса.

Использование жесткого диска, на котором хранится база данных очереди сообщений

Ресурс: **DatabaseUsedSpace[%ExchangeInstallPath%TransportRoles\data\Queue]**

Описание. Отслеживает процент общего дискового пространства, потребляемого всеми файлами на диске, на котором хранится база данных очереди сообщений. Обратите внимание, что файл базы данных очереди содержит неиспользуемое пространство, поэтому точным описанием общего дискового пространства, занятого всеми файлами, является следующее значение: размер диска минус свободное дисковое пространство минус свободное место в базе данных.

Сведения об изменении стандартного расположения базы данных очереди см. в статье Изменение расположения базы данных очереди.

Переходы загруженности (%):

- **LowToMedium**: 96
- **MediumToHigh**: 99
- **HighToMedium**: 97
- **MediumToLow**: 94 **Комментарии:**

По умолчанию высокий уровень использования жесткого диска рассчитывается по следующей формуле:

100 * (<*размер жесткого диска в МБ*> — 500 МБ) / <*размер жесткого диска в МБ*>

В этой формуле учитывается, что в базе данных очереди есть неиспользуемое пространство

1 ГБ = 1024 МБ. Результат округляется до ближайшего целого числа.

Например, если база данных очереди сообщений находится на диске объемом 1 терабайт (ТБ, 1 048 576 МБ), то высокий уровень использования составляет 100 * (1 048 576 – 500) / 1 048 576), или 99 %.

Как видите, согласно формуле и принципу округления, на жестком диске должно быть очень мало места, чтобы значение высокого уровня использования было меньше 99 %. Например, чтобы значение высокой загруженности составляло 98 %, необходим жесткий диск размером 25 ГБ или меньше.

Объем памяти, используемый процессом EdgeTransport.exe

Ресурс: **PrivateBytes**

Описание. Отслеживает процент памяти, используемый EdgeTransport.exe процессом, входящим в службу транспорта Microsoft Exchange. Это не включает виртуальную память в файле подкачки и память, используемую другими процессами.

Переходы загруженности (%):

- **LowToMedium**: 72
- **MediumToHigh**: 75
- **HighToMedium**: 73
- **MediumToLow**: 71

Примечания

По умолчанию высокий уровень использования памяти процессом EdgeTransport.exe составляет 75 процентов от общей физической памяти или 1 терабайт (смотря что меньше). Результат всегда округляется до ближайшего целого числа.

Exchange ведет журнал использования памяти процессом EdgeTransport.exe. Если использование не опускается до низкого уровня для определенного количества интервалов опроса, известного как *глубина журнала*, Exchange отклоняет входящие сообщения до тех пор, пока использование ресурсов не вернется к низкому уровню.

По умолчанию глубина журнала для EdgeTransport.exe использования памяти с интервалами опроса 30.

Количество сообщений в очереди передачи

Ресурс: **QueueLength[SubmissionQueue]**

Описание: отслеживает количество сообщений в очереди отправки. Как правило, сообщения поступают в очередь передачи из соединителей получения. Дополнительные сведения см. в разделе Поток обработки почты и конвейер транспорта. Большое количество сообщений в очереди передачи говорит о том, что в классификаторе возникли проблемы при обработке сообщений.

Переходы загруженности:

- **LowToMedium**: 9999
- **MediumToHigh**: 15000
- **HighToMedium**: 10000
- **MediumToLow**: 2000

Примечания

Если очередь передачи перегружена, Exchange регулирует входящие подключения, задерживая подтверждение входящих сообщений. Exchange снижает скорость потока входящих сообщений путем *тарпирирования*, что задерживает подтверждение команды SMTP **MAIL FROM** на отправляющем сервере. Если состояние перегрузки сохраняется, Exchange постепенно увеличивает длительность искусственной задержки ответов. Когда использование очереди передачи возвращается на низкий уровень, Exchange сокращает задержку подтверждения и возвращается к обычной работе. По умолчанию при перегрузке очереди передачи Exchange задерживает подтверждение сообщений на 10 секунд. Если ресурс остается перегруженным, задержка повышается до 55 секунд с шагом в 5 секунд.

Exchange ведет журнал использования очереди передачи. Если использование очереди отправки не опускается до низкого уровня для определенного количества интервалов опроса, известного как *глубина журнала*, Exchange останавливает задержку тарпитирования и отклоняет входящие сообщения до тех пор, пока использование отправки не вернется к низкому уровню. По умолчанию интервал журнала для очереди передачи составляет 300 интервалов опроса.

Объем памяти, используемый всеми процессами

Ресурс: **SystemMemory**

Описание: отслеживает процент памяти, используемый всеми процессами на сервере Exchange Server. Это не включает виртуальную память в файле подкачки.

Переходы загруженности (%):

- **LowToMedium**: 88
- **MediumToHigh**: 94
- **HighToMedium**: 89
- **MediumToLow**: 84

Примечания

Когда использование памяти на сервере достигает высокого уровня, происходит *консервация сообщений*. При этом удаляются ненужные элементы сообщений в очереди, кэшируемых в памяти. Как правило, сообщения кэшируются в памяти полностью для повышения производительности. При удалении содержимого MIME из сообщений в кэше используемый объем памяти сокращается за счет повышения задержки, так как сообщения теперь считываются непосредственно из базы данных очереди сообщений. Консервация сообщений включена по умолчанию.

Использование жесткого диска, на котором хранятся журналы транзакций для базы данных очереди

Ресурс: **UsedDiskSpace[%ExchangeInstallPath%TransportRoles\data\Queue]**

Описание. Отслеживает процент общего дискового пространства, используемого всеми файлами на диске, на котором хранятся журналы транзакций базы данных очереди сообщений. Сведения об изменении расположения по умолчанию см. в статье Изменение расположения базы данных очереди.

Переходы загруженности (%):

- **LowToMedium**: 89
- **MediumToHigh**: 99
- **HighToMedium**: 90
- **MediumToLow**: 80

Примечания

По умолчанию высокий уровень использования жесткого диска рассчитывается по следующей формуле:

100 * (<*размер жесткого диска в МБ*> — 1152 МБ) / <*размер жесткого диска в МБ*>

1 ГБ = 1024 МБ. Результат округляется до ближайшего целого числа.

Например, если база данных очереди находится на диске объемом 1 терабайт (ТБ, 1 048 576 МБ), то высокий уровень использования составляет 100 * (1 048 576 – 1152) / 1 048 576), или 99 %.

Как видите, согласно формуле и принципу округления, на жестком диске должно быть довольно мало места, чтобы значение высокого уровня использования было меньше 99 %. Например, чтобы значение высокой загруженности составляло 98 %, необходим жесткий диск размером 56 ГБ или меньше.

Файл `%ExchangeInstallPath%Bin\EdgeTransport.exe.config` конфигурации приложения содержит ключ *DatabaseCheckPointDepthMax* со значением `384MB` по умолчанию . Этот ключ управляет общим допустимым размером всех журналов незафиксированных транзакций на жестком диске. Значение этого ключа используется в формуле для вычисления высокого уровня использования. Если изменить это значение, формула примет следующий вид:

100 * (<*размер жесткого диска в МБ*> — min(5120 MB, 3* *DatabaseCheckPointDepthMax*)) / <*размер жесткого диска в МБ*>

> ⓘ **Примечание**
>
> Значение ключа *DatabaseCheckPointDepthMax* применяется ко всем связанным с транспортировкой базам данных ESE, существующим на сервере Exchange Server. На серверах почтовых ящиков это база данных очереди сообщений и база данных репутации отправителей. На пограничных транспортных серверах это база данных очереди сообщений, база данных репутации отправителей и база данных IP-фильтра, используемая агентом фильтра подключений.

Использование жесткого диска, применяемого для преобразования содержимого

Ресурс: **UsedDiskSpace[%ExchangeInstallPath%TransportRoles\data]**

Описание. Отслеживает процент общего пространства на диске, который потребляется всеми файлами на диске, используемым для преобразования содержимого. Расположение папки по умолчанию — `%ExchangeInstallPath%TransportRoles\data\Temp` и управляется ключом *TemporaryStoragePath* в `%ExchangeInstallPath%Bin\EdgeTransport.exe.config` файле конфигурации приложения.

Переходы загруженности (%):

- **LowToMedium**: 89
- **MediumToHigh**: 99

- **HighToMedium**: 90
- **MediumToLow**: 80

Примечания

По умолчанию высокий уровень использования жесткого диска рассчитывается по следующей формуле:

100 * (<*размер жесткого диска в МБ*> — 500 МБ) / <*размер жесткого диска в МБ*>

1 ГБ = 1024 МБ. Результат округляется до ближайшего целого числа.

Например, если база данных очереди сообщений находится на диске объемом 1 терабайт (ТБ, 1 048 576 МБ), то высокий уровень использования составляет 100 * (1 048 576 – 500) / 1 048 576), или 99 %.

Как видите, согласно формуле и принципу округления, на жестком диске должно быть очень мало места, чтобы значение высокого уровня использования было меньше 99 %. Например, чтобы значение высокой загруженности составляло 98 %, необходим жесткий диск размером 25 ГБ или меньше.

Количество незавершенных транзакций базы данных очереди сообщений

Ресурс:
UsedVersionBuckets[%ExchangeInstallPath%TransportRoles\data\Queue\mail.queue]

Описание. Отслеживает количество незафиксированных транзакций для базы данных очереди сообщений, которая существует в памяти.

Переходы загруженности:

- **LowToMedium**: 999
- **MediumToHigh**: 1500
- **HighToMedium**: 1000
- **MediumToLow**: 800

Примечания

Список изменений, вносимых в базу данных очереди сообщений, хранится в памяти до тех пор, пока эти изменения не будут зафиксированы в журнале транзакций. После этого список сохраняется непосредственно в базу данных очереди сообщений. Невыполненные транзакции базы данных очереди сообщений, хранящиеся в памяти, называются *сегментами версий*. Количество сегментов версий может достигать недопустимо высокого уровня вследствие неожиданно большого количества входящих

сообщений, атак с использованием нежелательной почты, нарушения целостности базы данных очереди сообщений или снижения производительности жесткого диска.

Если сегменты версий перегружены, сервер Exchange регулирует входящие подключения, задерживая подтверждение входящих сообщений. Exchange снижает скорость потока входящих сообщений путем *тарпирирования*, что задерживает подтверждение команды SMTP **MAIL FROM** на отправляющем сервере. Если состояние перегрузки ресурса сохраняется, Exchange постепенно увеличивает длительность искусственной задержки ответов. Когда использование ресурса возвращается к обычному уровню, Exchange постепенно сокращает задержку подтверждения и возвращается к обычной работе. По умолчанию при перегрузке ресурса Exchange задерживает подтверждение сообщений на 10 секунд. Если перегрузка сохраняется, задержка повышается до 55 секунд с шагом в 5 секунд.

При перегрузке сегментов версий сервер Exchange также останавливает обработку исходящих сообщений.

Exchange ведет журнал использования сегментов версий. Если использование ресурсов не опускается до низкого уровня для определенного количества интервалов опроса, известного как *глубина журнала*, Exchange останавливает задержку тарпитирования и отклоняет входящие сообщения до тех пор, пока использование ресурсов не вернется к низкому уровню. По умолчанию интервал журнала для сегментов версий составляет 10 интервалов опроса.

Действия, выполняемые функцией замедленной обратной реакции при перегрузке ресурсов

В приведенной ниже таблице представлены сводные данные о действиях, выполняемых функцией замедленной обратной реакции при перегрузке отслеживаемого ресурса.

Перегруженный ресурс	Уровень использования	Выполняемые действия

Перегруженный ресурс	Уровень использования	Выполняемые действия
DatabaseUsedSpace	Средний	Отклонение входящих сообщений от серверов, отличных от Exchange Server. Отклонение сообщений, отправленных из каталогов раскладки и преобразования. Повторная отправка сообщений приостанавливается. Функция теневой избыточности отклоняет сообщения. Дополнительные сведения о теневой избыточности см. в разделе Теневая избыточность в Exchange Server.
DatabaseUsedSpace	Высокий	Все действия, выполняемые на среднем уровне использования. Отклонение входящих сообщений от других серверов Exchange. Отклонение сообщений, отправляемых из баз данных почтовых ящиков службой отправки транспорта почтовых ящиков Microsoft Exchange на серверах почтовых ящиков.
PrivateBytes	Средний	Отклонение входящих сообщений от серверов, отличных от Exchange Server. Отклонение сообщений, отправленных из каталогов раскладки и преобразования. Повторная отправка сообщений приостанавливается. Функция теневой избыточности отклоняет сообщения. Обработка сообщений после перезагрузки сервера или службы транспорта (т. н. *сканирование при запуске*) приостанавливается. Запуск консервации сообщений.

Перегруженный ресурс	Уровень использования	Выполняемые действия
PrivateBytes	Высокий	Все действия, выполняемые на среднем уровне использования. Отклонение входящих сообщений от других серверов Exchange. Отклонение сообщений, отправляемых из баз данных почтовых ящиков службой отправки транспорта почтовых ящиков Microsoft Exchange на серверах почтовых ящиков.
QueueLength[SubmissionQueue]	Средний	Введение или увеличение искусственной задержки ответов для входящих сообщений. Если интервала журнала очереди передачи недостаточно для достижения нормального уровня использования, выполните следующие действия. • Отклонение входящих сообщений от серверов, отличных от Exchange Server. • Отклонение сообщений, отправленных из каталогов раскладки и преобразования. • Повторная отправка сообщений приостанавливается. • Функция теневой избыточности отклоняет сообщения. • Сканирование при загрузке приостановлено.
QueueLength[SubmissionQueue]	Высокий	Все действия, выполняемые на среднем уровне использования. Отклонение входящих сообщений от других серверов Exchange. Отклонение сообщений, отправляемых из баз данных почтовых ящиков службой отправки транспорта почтовых ящиков Microsoft Exchange на серверах почтовых ящиков. Очистка расширенного кэша DNS из памяти. Запуск консервации сообщений.
SystemMemory	Средняя	Запуск консервации сообщений. Очистка кэша.

Перегруженный ресурс	Уровень использования	Выполняемые действия
SystemMemory	Высокий	Все действия, выполняемые на среднем уровне использования.
UsedDiskSpace (журналы транзакций для базы данных очереди сообщений)	Средний	Отклонение входящих сообщений от серверов, отличных от Exchange Server. Отклонение сообщений, отправленных из каталогов раскладки и преобразования. Повторная отправка сообщений приостанавливается. Функция теневой избыточности отклоняет сообщения.
UsedDiskSpace (журналы транзакций для базы данных очереди сообщений)	Высокий	Все действия, выполняемые на среднем уровне использования. Отклонение входящих сообщений от других серверов Exchange. Отклонение сообщений, отправляемых из баз данных почтовых ящиков службой отправки транспорта почтовых ящиков Microsoft Exchange на серверах почтовых ящиков.
UsedDiskSpace (преобразование содержимого)	Средний	Отклонение входящих сообщений от серверов, отличных от Exchange Server. Отклонение сообщений, отправленных из каталогов раскладки и преобразования.
UsedDiskSpace (преобразование содержимого)	Высокий	Все действия, выполняемые на среднем уровне использования. Отклонение входящих сообщений от других серверов Exchange. Отклонение сообщений, отправляемых из баз данных почтовых ящиков службой отправки транспорта почтовых ящиков Microsoft Exchange на серверах почтовых ящиков.

Перегруженный ресурс	Уровень использования	Выполняемые действия
UsedVersionBuckets	Средний	Введение или увеличение искусственной задержки ответов для входящих сообщений. Если степени детализации журнала сегмента версий недостаточно для достижения нормального уровня использования, выполните следующие действия: • Отклонение входящих сообщений от серверов, отличных от Exchange Server. • Отклонение сообщений, отправленных из каталогов раскладки и преобразования.
UsedVersionBuckets	Высокий	Все действия, выполняемые на среднем уровне использования. Отклонение входящих сообщений от других серверов Exchange. Отклонение сообщений, отправляемых из баз данных почтовых ящиков службой отправки транспорта почтовых ящиков Microsoft Exchange на серверах почтовых ящиков. Остановка обработки исходящих сообщений. Удаленная доставка приостанавливается.

Просмотр пороговых значений и уровней использования ресурсов для замедленной обратной реакции

Командлет **Get-ExchangeDiagnosticInfo** в командной консоли Exchange можно использовать для просмотра отслеживаемых ресурсов и текущих уровней использования. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

Чтобы просмотреть параметры замедленной обратной реакции на сервере Exchange, выполните следующую команду:

```
PowerShell
```

```
[xml]$bp=Get-ExchangeDiagnosticInfo [-Server <ServerIdentity> ] -Process
EdgeTransport -Component ResourceThrottling;
$bp.Diagnostics.Components.ResourceThrottling.ResourceTracker.ResourceMeter
```

Чтобы просмотреть значения на локальном сервере, можно опустить параметр *Server* .

Параметры конфигурации замедленной обратной реакции в файле EdgeTransport.exe.config

Все параметры конфигурации для обратного `%ExchangeInstallPath%Bin\EdgeTransport.exe.config` давления выполняются в xml-файле конфигурации приложения. Однако по умолчанию в файле мало параметров.

> ⊗ **Внимание!**
>
> Эти параметры перечислены исключительно в справочных целях как значения по умолчанию. Настоятельно не рекомендуем вносить изменения в параметры замедленной обратной реакции в файле EdgeTransport.exe.config. Изменение этих параметров может привести к снижению производительности или потере данных. Рекомендуем исследовать и устранить главную причину проблем с замедленной обратной реакцией.

Общие параметры замедленной обратной реакции

Имя ключа	**Значение по умолчанию**
ResourceMeteringInterval	`00:00:02` (2 секунд)
DehydrateMessagesUnderMemoryPressure	true

Параметры DatabaseUsedSpace

Имя ключа	**Значение по умолчанию (%)**
DatabaseUsedSpace.LowToMedium	96
DatabaseUsedSpace.MediumToHigh	99
DatabaseUsedSpace.HighToMedium	97
DatabaseUsedSpace.MediumToLow	94

Параметры PrivateBytes

Имя ключа	Значение по умолчанию (%)
PrivateBytes.LowToMedium	72
PrivateBytes.MediumToHigh	75
PrivateBytes.HighToMedium	73
PrivateBytes.MediumToLow	71
PrivateBytesHistoryDepth	30

Параметры QueueLength[SubmissionQueue]

Имя ключа	Значение по умолчанию
QueueLength[SubmissionQueue]. LowToMedium	9999
QueueLength[SubmissionQueue]. MediumToHigh	15000
QueueLength[SubmissionQueue]. HighToMedium	10000
QueueLength[SubmissionQueue]. MediumToLow	2000
SubmissionQueueHistoryDepth	300 (через 10 минут)

Параметры SystemMemory

Имя ключа	Значение по умолчанию (%)
SystemMemory.LowToMedium	88
SystemMemory.MediumToHigh	94
SystemMemory.HighToMedium	89
SystemMemory.MediumToLow	84

Параметры UsedDiskSpace (журналы транзакций для базы данных очереди сообщений)

Имя ключа	Значение по умолчанию (%)
UsedDiskSpace[%ExchangeInstallPath%TransportRoles\data\Queue]. LowToMedium	89

Имя ключа	Значение по умолчанию (%)
UsedDiskSpace[%ExchangeInstallPath%TransportRoles\data\Queue].MediumToHigh	99
UsedDiskSpace[%ExchangeInstallPath%TransportRoles\data\Queue].HighToMedium	90
UsedDiskSpace[%ExchangeInstallPath%TransportRoles\data\Queue].MediumToLow	80

> ⓘ **Примечание**
>
> Значения, содержащие только `UsedDiskSpace` (например, `UsedDiskSpace.MediumToHigh`) применяются к журналам транзакций базы данных очереди сообщений и к преобразованию содержимого.

Параметры UsedDiskSpace (преобразование содержимого)

Имя ключа	Значение по умолчанию (%)
UsedDiskSpace[%ExchangeInstallPath%TransportRoles\data].LowToMedium	89
UsedDiskSpace[%ExchangeInstallPath%TransportRoles\data].MediumToHigh	99
UsedDiskSpace[%ExchangeInstallPath%TransportRoles\data].HighToMedium	90
UsedDiskSpace[%ExchangeInstallPath%TransportRoles\data].MediumToLow	80
TemporaryStoragePath	`%ExchangeInstallPath%TransportRoles\data\Temp`

Параметры UsedVersionBuckets

Имя ключа	Значение по умолчанию
UsedVersionBuckets.LowToMedium	999
UsedVersionBuckets.MediumToHigh	1500
UsedVersionBuckets.HighToMedium	1000

Имя ключа	Значение по умолчанию
UsedVersionBuckets.MediumToLow	800
VersionBucketsHistoryDepth	10

Сведения в журнале замедленной обратной реакции

В следующем списке описаны записи журнала событий, создаваемые при регистрации определенных событий замедленной обратной реакции.

- **Запись журнала событий при увеличении уровня использования ресурса**

  Тип события: Ошибка

  Источник события: MSExchangeTransport

  Категория события: Диспетчер ресурсов

  Код события: 15004

  Описание: давление на ресурсы возросло с *<предыдущего уровня> использования* до *<текущего уровня> использования*.

- **Запись журнала событий при снижении уровня использования ресурса**

  Тип события: Сведения

  Источник события: MSExchangeTransport

  Категория события: Диспетчер ресурсов

  Код события: 15005

  Описание: давление на ресурсы снизилось с *<уровня> предыдущего использования* до *<текущего уровня> использования*.

- **Запись в журнале событий при критически малом объеме свободного места на диске**

  Тип события: Ошибка

  Источник события: MSExchangeTransport

  Категория события: Диспетчер ресурсов

  Код события: 15006

Описание: служба транспорта Microsoft Exchange отклоняет сообщения, так как количество доступного места на диске ниже указанного порогового значения. Возможно, для продолжения работы службы администратору требуется освободить место на диске.

- **Запись в журнале событий при критически малом объеме доступной памяти**

  Тип события: Ошибка

  Источник события: MSExchangeTransport

  Категория события: Диспетчер ресурсов

  Код события: 15007

  Описание: служба транспорта Microsoft Exchange отклоняет отправленные сообщения, так как объем памяти, используемой службой, больше настроенного порога. Возможно, для продолжения нормальной работы службы ее следует перезапустить.

Проверка связи по протоколу SMTP на серверах Exchange с помощью Telnet

Статья • 18.10.2023

Вы можете использовать Telnet для проверки связи по протоколу SMTP между серверами обмена сообщениями. SMTP — это протокол, используемый для отправки сообщений электронной почты с одного сервера обмена сообщениями на другой. Использование Telnet может быть полезно, если у вас возникли проблемы с отправкой или получением сообщений, так как вы можете вручную отправлять smtp-команды на сервер обмена сообщениями. В ответ сервер будет отвечать ответами, которые будут возвращены в обычном соединении. Иногда эти результаты помогут вам понять, почему вы не можете отправлять или получать сообщения.

Telnet можно использовать для проверки smtp-связи для:

- Протестируйте поток почты из Интернета в организации Exchange.
- Протестируйте поток почты из Exchange на другой сервер обмена сообщениями в Интернете.

> **Совет**
>
> Знаете ли вы, что вместо того, чтобы использовать Telnet для проверки smtp-подключения, вы можете использовать Microsoft Remote Connectivity Analyzer по адресу **https://testconnectivity.microsoft.com/**? С помощью анализатора удаленного подключения можно выбрать тест подключения, который нужно выполнить, в данном случае **входящий SMTP-Email**, и следовать приведенным инструкциям. Он предоставит вам сведения, необходимые для ввода, запустит тест, а затем предоставит результаты. Попробуйте!

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 15 минут.
- Разрешения Exchange не применяются к процедурам, описанным в этом разделе. Эти процедуры выполняются в операционной системе сервера Exchange Server или клиентского компьютера.

- В этом разделе показано, как использовать клиент Telnet, который входит в состав Windows. Сторонним клиентам Telnet может потребоваться синтаксис, отличный от синтаксиса, показанного в этом разделе.
- В этом разделе показано, как подключиться к серверу с выходом в Интернет, который разрешает анонимные подключения с помощью TCP-порта 25. Если вы пытаетесь подключиться к этому серверу из Интернета, необходимо убедиться, что сервер Exchange доступен из Интернета через TCP-порт 25. Аналогичным образом, если вы пытаетесь подключиться к серверу в Интернете с сервера Exchange Server, необходимо убедиться, что сервер Exchange server может открыть подключение к Интернету через TCP-порт 25.
- Вы можете заметить некоторые соединители получения, использующие TCP-порт 2525. Это внутренние соединители получения и не используются для приема анонимных SMTP-подключений.
- Если вы тестируете подключение на удаленном сервере обмена сообщениями, выполните действия, описанные в этом разделе, на сервере Exchange Server. Удаленные серверы обмена сообщениями часто настраиваются так, чтобы IP-адрес, из которого поступает SMTP-подключение, соответствовал домену в адресе электронной почты отправителя.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Шаг 1. Установка клиента Telnet на компьютере

В большинстве версий Windows необходимо установить клиент Telnet, прежде чем использовать его. Сведения об установке см. в статье Установка клиента Telnet.

Шаг 2. Поиск полного доменного имени или IP-адреса smtp-сервера назначения

Чтобы подключиться к SMTP-серверу с помощью Telnet через порт 25, необходимо использовать полное доменное имя (FQDN) (например, mail.contoso.com) или IP-адрес SMTP-сервера. Если вы не знаете полное доменное имя или IP-адрес, вы можете использовать программу командной строки Nslookup, чтобы найти запись MX для целевого домена.

> ⓘ **Примечание**
>
> Политики сети могут препятствовать использованию средства Nslookup для запроса общедоступных DNS-серверов в Интернете. В качестве альтернативы можно использовать один из доступных веб-сайтов подстановки DNS или mx record lookup в Интернете.

1. В командной строке введите `nslookup` и нажмите клавишу ВВОД. Эта команда открывает сеанс Nslookup.
2. Введите `set type=mx`, а затем нажмите Ввод.
3. Введите имя домена, для которого требуется найти запись MX. Например, чтобы найти запись MX для fabrikam.com домена, введите `fabrikam.com.` и нажмите клавишу ВВОД.

   > ⓘ **Примечание**
   >
   > При использовании конечного периода (.) вы предотвращаете случайное добавление DNS-суффиксов по умолчанию в доменное имя.

   Выходные данные команды выглядят так:

   ```dos
   fabrikam.com mx preference=10, mail exchanger = mail1.fabrikam.com
   fabrikam.com mx preference=20, mail exchanger = mail2.fabrikam.com
   mail1.fabrikam.com internet address = 192.168.1.10
   mail2 fabrikam.com internet address = 192.168.1.20
   ```

   В качестве SMTP-сервера назначения можно использовать любые имена узлов или IP-адреса, связанные с MX-записями. Более низкое значение для предпочтения (предпочтение = 10 против 20) указывает на предпочтительный SMTP-сервер. Для балансировки нагрузки и отказоустойчивости используется несколько записей MX и различные значения параметров.

4. Когда вы будете готовы завершить сеанс Nslookup, введите `exit` и нажмите клавишу ВВОД.

Действие 3. Использование протокола Telnet на порте 25 для проверки связи по протоколу SMTP.

В этом примере мы будем использовать следующие значения. При выполнении команд на сервере замените эти значения значениями для SMTP-сервера организации, домена и т. д.

- **Smtp-сервер назначения**: mail1.fabrikam.com
- **Исходный домен**: contoso.com
- **Адрес электронной почты отправителя**: chris@contoso.com
- **Адрес электронной почты получателя**: kate@fabrikam.com
- **Тема сообщения**: Тестирование из Contoso
- **Текст сообщения**: это тестовое сообщение

> **Совет**
>
> В командах в клиенте Telnet регистр не учитывается. Команды SMTP в этом примере используются с прописной буквы для ясности. Ключ backspace нельзя использовать в сеансе Telnet после подключения к целевому SMTP-серверу. Если вы допустили ошибку при вводе команды SMTP, необходимо нажать клавишу ВВОД, а затем ввести команду еще раз. Нераспознанные команды SMTP или синтаксические ошибки приводят к появляется сообщение об ошибке, которое выглядит следующим образом: `500 5.3.3 Unrecognized command`.

1. Откройте окно командной строки, введите `telnet` и нажмите клавишу ВВОД.

   Эта команда открывает сеанс Telnet.

2. Введите `set localecho`, а затем нажмите Ввод.

   Эта **необязательная** команда позволяет просматривать символы по мере их ввода, и это может потребоваться для некоторых SMTP-серверов.

3. Введите `set logfile <filename>`, а затем нажмите Ввод.

Эта **необязательная** команда включает ведение журнала и задает файл журнала для сеанса Telnet. Если указать только имя файла, файл журнала находится в текущей папке. Если указать путь и имя файла, путь должен находиться на локальном компьютере, и может потребоваться ввести путь и имя файла в формате Windows DOS 8.3 (короткое имя без пробелов). Путь должен существовать, но файл журнала создается автоматически.

4. Введите `OPEN mail1.fabrikam.com 25`, а затем нажмите Ввод.
5. Введите `EHLO contoso.com`, а затем нажмите Ввод.
6. Введите `MAIL FROM:<chris@contoso.com>`, а затем нажмите Ввод.
7. Введите `RCPT TO:<kate@fabrikam.com> NOTIFY=success,failure`, а затем нажмите Ввод.

   Необязательная команда NOTIFY указывает конкретные сообщения уведомления о состоянии доставки (DSN) (также известные как сообщения о отказе, отчеты о недоставке или недоставка), которые необходимо предоставить SMTP. В этом примере вы запрашиваете сообщение DSN для успешной или неудачной доставки сообщений.

8. Введите `DATA`, а затем нажмите Ввод.
9. Введите `Subject: Test from Contoso`, а затем нажмите Ввод.
10. Еще раз нажмите клавишу ВВОД.

    Между полем **Subject:** и текстом сообщения требуется пустая строка.

11. Введите `This is a test message`, а затем нажмите Ввод.
12. Введите точку (`.`), а затем нажмите клавишу ВВОД.
13. Чтобы отключиться от SMTP-сервера, введите `QUIT` и нажмите клавишу ВВОД.
14. Чтобы закрыть сеанс Telnet, введите `quit` и нажмите клавишу ВВОД.

Вот как выглядит успешный сеанс с помощью описанных выше действий.

dos

```
C:\Windows\System32> telnet
Microsoft Telnet> set localecho
Microsoft Telnet> set logfile c:\TelnetTest.txt
Microsoft Telnet> OPEN mail1.fabrikam.com 25
220 mail1.fabrikam.com Microsoft ESMTP MAIL Service ready at Fri, 5 Aug 2016
```

```
16:24:41 -0700
EHLO contoso.com
250-mail1.fabrikam.com Hello [172.16.0.5]
250-SIZE 37748736
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-X-ANONYMOUSTLS
250-AUTH NTLM
250-X-EXPS GSSAPI NTLM
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 XRDST
MAIL FROM: <chris@contoso.com>
250 2.1.0 Sender OK
RCPT TO: <kate@fabrikam.com> NOTIFY=success,failure
250 2.1.5 Recipient OK
DATA
354 Start mail input; end with <CRLF>.<CRLF>
Subject: test

This is a test message.
.
250 2.6.0 <c89b4fcc-3ad1-4758-a1ab-1e820065d622@mail1.fabrikam.com>
[InternalId=5111011082268, Hostname=mail1.fabrikam.com] Queued mail for
delivery
QUIT
221 2.0.0 Service closing transmission channel
```

Шаг 4. Сообщения об успешном выполнении и ошибках в сеансе Telnet

В этом разделе содержатся сведения об успешных и неудачных ответах на команды, которые использовались в предыдущем примере.

> ⓘ **Примечание**
>
> Трехзначные коды ответа SMTP, определенные в RFC 5321, одинаковы для всех SMTP-серверов обмена сообщениями, но текстовые описания в ответах могут немного отличаться.

Коды ответа SMTP

SMTP-серверы отвечают на команды различными числовыми кодами ответа в формате x.y.z, где:

- X указывает, была ли команда хорошей, плохой или неполной.
- Y указывает тип отправленного ответа.
- Z предоставляет дополнительные сведения о команде

Когда сервер, открывший подключение, получает ответ, он может определить, принял ли удаленный сервер команду и готов ли к следующей, или произошла ошибка.

Первая цифра (X) особенно важна для понимания, так как она указывает на успешное или неудачное выполнение отправленной команды. Ниже приведены возможные значения и их значения.

Код ответа	**Смысл**
2.y.z	Отправленная команда успешно выполнена на удаленном сервере. Удаленный сервер готов к выполнению следующей команды.
3.y.z	Команда была принята, но удаленный сервер нуждается в дополнительных сведениях, прежде чем операция будет завершена. Отправляющий сервер должен отправить новую команду с необходимыми сведениями.
4.y.z	Команда не была принята удаленным сервером по временной причине. Отправляя сервер должен попытаться подключиться еще раз позже, чтобы узнать, может ли удаленный сервер успешно принять команду. Отправляющий сервер будет продолжать повторять подключение, пока не завершится успешное подключение (указано в коде 2.y.z) или не завершится окончательной ошибкой (указано в коде 5.y.z). Примером временной ошибки является недостаточно места на удаленном сервере. Как только будет доступно больше места, удаленный сервер сможет успешно принять команду.
5.y.z	Команда не была принята удаленным сервером по причине, которую невозможно восстановить. Отправляющий сервер не будет повторять подключение и отправит отчет о недоставке пользователю, отправившему сообщение. Примером неустранимой ошибки является сообщение, которое отправляется на несуществующий адрес электронной почты.

Таблица выше основана на информации, предоставленной RFC 5321 (simple Mail Transfer Protocol), раздел 4.2.1. Дополнительные сведения, включая описания второй (Y) и третьей (Z) цифры кодов ответа SMTP, включены в этот раздел, а также в разделах 4.2.2 и 4.2.3.

Команда OPEN

Успешный ответ: `220 mail1.fabrikam.com Microsoft ESMTP MAIL Service ready at <day-date-time>`

Ответ на сбой: `Connecting to mail1.fabrikam.com...Could not open connection to the host, on port 25: Connect failed`

Возможные причины сбоя:

- SMTP-служба назначения недоступна.
- Ограничения на целевой брандмауэр.
- Ограничения на брандмауэр источника.
- Неверное полное доменное имя или IP-адрес smtp-сервера назначения.
- Неправильный номер порта.

Команда EHLO

Успешный ответ: `250 mail1.fabrikam.com Hello [<sourceIPaddress>]`

Ответ на сбой: `501 5.5.4 Invalid domain name`

Возможные причины сбоя:

- Недопустимые символы в доменном имени.
- Ограничения подключения на целевом SMTP-сервере.

> ⓘ **Примечание**
>
> EHLO — это глагол ESMTP, определенный в RFC 5321. ESMTP-серверы могут объявлять о своих возможностях в процессе начального подключения. Эти возможности включают максимальный допустимый размер сообщения и поддерживаемые методы проверки подлинности. HELO — это более старая команда SMTP, определенная в RFC 821. Большинство SMTP-серверов обмена сообщениями поддерживают ESMTP и EHLO. Если сервер, отличный от Exchange, к которому вы пытаетесь подключиться, не поддерживает EHLO, вместо него можно использовать HELO.

Команда MAIL FROM

Успешный ответ: `250 2.1.0 Sender OK`

Ответ на сбой: `550 5.1.7 Invalid address`

Возможные причины сбоя: синтаксическая ошибка в адресе электронной почты отправителя.

Ответ на сбой: `530 5.7.1 Client was not authenticated`

Возможные причины сбоя: конечный сервер не принимает отправки анонимных сообщений. Эта ошибка возникает при попытке использовать Telnet для отправки сообщения непосредственно на сервер почтовых ящиков, на который нет соединителя получения, настроенного для приема анонимных подключений.

Команда RCPT TO

Успешный ответ: `250 2.1.5 Recipient OK`

Ответ на сбой: `550 5.1.1 User unknown`

Возможные причины сбоя: указанный получатель не существует.

Функции совместной работы в Exchange Server

Статья • 04.04.2023

Exchange Server предоставляет следующие функциональные возможности, которые могут помочь конечным пользователям совместно работать с электронной почтой:

- Почтовые ящики сайта (устаревшие в SharePoint 2019)
- Общедоступные папки
- Общие почтовые ящики
- Группы рассылки

Каждая из этих функций отличается взаимодействием с пользователем и набором компонентов, и выбирается с учетом потребностей пользователя и возможностей организации. Например, сайт для совместной работы обеспечивает отличную документацию в почтовых ящиках. Однако почтовые ящики сайтов используют SharePoint Server, поэтому если вы не планируете развертывать SharePoint, следует использовать общедоступные папки для предоставления общего доступа к документам.

В этом разделе сравниваются эти функции совместной работы, что помогает определить, какие функции предлагать пользователям.

Почтовые ящики сайта

Почтовый ящик сайта функционально состоит из членства в сайте SharePoint 2013 или более поздней версии (владельцы и участники), общего хранилища через почтовый ящик Exchange 2016 или более поздней версии для сообщений электронной почты и сайта SharePoint для хранения и совместного использования информации. Почтовый ящик сайта объединяет электронную почту Exchange и документы SharePoint. Для пользователей почтовый ящик сайта служит центральной картотекой проекта, предоставляя место электронной почте и документам проекта файла, которые могут открывать и редактировать только участники сайта. Кроме того, у почтовых ящиков сайта определенный жизненный цикл, и они оптимизированы для использования проектами с конкретной датой начала и окончания. Чтобы полностью реализовать почтовые ящики сайта, конечные пользователи должны использовать Outlook 2013 или более поздней версии.

Дополнительные сведения см. в разделе Почтовые ящики сайта.

Общедоступные папки

Общие папки предназначены для осуществления общего доступа к файлам. Это простой и эффективный способ сбора, организации и использования информации внутри рабочей группы или в масштабах всей организации.

Общие папки упорядочивают это содержимое в глубокую иерархию, которую легко просматривать. Пользователи находят интересное и соответствующее содержимое, переходя по необходимым ветвям этой иерархии. Полная иерархия всегда отображается в представлении папок Outlook пользователей. Общие папки — это отличная технология для архивации групп рассылки. Общая папка может поддерживать электронную почту, и ее можно добавить в качестве члена группы рассылки. Электронная почта, отправленная группе рассылки, будет автоматически добавляться в общую папку для последующего просмотра. Общедоступные папки также обеспечивают простой общий доступ к документам и не требуют установки SharePoint Server в вашей организации. Пользователи могут использовать общедоступные папки с Outlook 2007 или более поздних версий.

Дополнительные сведения см. в разделе Общедоступные папки.

Общие почтовые ящики

Общий почтовый ящик — это почтовый ящик, в который пользователи могут обращаться для чтения и отправки сообщений электронной почты и общего календаря. Общие почтовые ящики могут предоставлять универсальный адрес электронной почты (например info@contoso.com , или sales@contoso.com), который клиенты могут использовать для получения справки о вашей компании. Если общему почтовому ящику назначено разрешение Отправить как, когда делегированный пользователь отвечает на сообщение электронной почты, он может выглядеть так, как будто отвечает почтовый ящик (например, sales@contoso.com) , а не фактический пользователь.

Дополнительные сведения см. в разделе Общие почтовые ящики.

Группы

Группы, также называемые группами рассылки, представляют собой совокупность двух и более получателей, которая содержится в общей адресной книге. При отправке в группу сообщения электронной почты оно будет передано всем ее участникам. Группы рассылки могут быть организованы по определенному обсуждению темы (например, "Собаководы") или пользователям, которые имеют общую рабочую структуру, которая требует частого общения.

Дополнительные сведения см. в разделе Получатели.

Какую функцию использовать?

В таблице ниже приведено краткое описание всех функций совместной работы, чтобы вы смогли решить, какую из них использовать.

Развернуть таблицу

Сценарий	Почтовые ящики сайта	Общие папки	Общие почтовые ящики	Группы
Тип группы	Совместная работа команды над конкретным проектом с определенными датами начала и окончания.	С соответствующими разрешениями все пользователи в организации смогут получить доступ к общим папкам и вести поиск. Общие папки являются идеальным решением для поддержания истории беседы или группы рассылки.	Делегаты, работающие от имени виртуального удостоверения, могут отвечать на сообщения электронной почты в качестве удостоверения общего почтового ящика. Пример: support@tailspintoys.com	Потребность отправлять электронную почту группе получателей с общими интересами или характеристиками.
Идеальный размер группы	Малый	Большая	Малый	Большая
Access	Владельцы и участники почтового ящика сайта.	Доступен каждому в вашей организации.	Пользователям могут быть предоставлены разрешения "Полный доступ" и/или "Отправить как". Чтобы получить доступ к общему почтовому ящику, пользователи, имеющие разрешения на полный доступ, должны добавить общий почтовый ящик в свой профиль Outlook.	Для групп рассылки члены должны быть добавлены вручную. Для динамических групп рассылки члены добавляются на основе условий фильтрации.
Общий календарь?	Нет	Да	Да	Нет
Доставка в личную папку входящих сообщений пользователя?	Нет. Сообщения электронной почты доставляются в почтовый ящик сайта.	Нет. Сообщения электронной почты доставляются в общую папку.	Нет. Сообщения электронной почты доставляются в папку "Входящие" общего почтового ящика.	Да. Да, электронная почта доставляется в папку входящих сообщений члена группы рассылки.

Сценарий	Почтовые ящики сайта	Общие папки	Общие почтовые ящики	Группы
Поддерживаемые клиенты	Outlook 2013 или более поздней версии SharePoint 2013	Outlook 2007 или более поздней версии	Outlook 2007 или более поздней версии Outlook Web App	Outlook 2007 или более поздней версии Outlook Web App

Почтовые ящики сайта в Exchange Server

Статья • 04.04.2023

Сообщения электронной почты и документы традиционно хранятся в двух уникальных и отдельных репозиториях данных. В большинстве организаций совместная работа ведется с использованием обоих методов. Трудность состоит в том, что доступ к сообщениям электронной почты и документам осуществляется через разные клиенты. Обычно это приводит к уменьшению производительности и ухудшению работы пользователей.

Почтовый *ящик сайта*, впервые представленный в Exchange 2013, является решением этой проблемы. Почтовые ящики сайта повышают совместную работу и производительность пользователей, предоставляя доступ как к документам Microsoft SharePoint, так и к электронной почте Exchange с помощью одного клиентского интерфейса. Почтовый ящик сайта функционально состоит из членства сайта SharePoint (владельцев и участников), общего хранилища через почтовый ящик Exchange 2016 или Exchange 2019 для сообщений электронной почты и сайта SharePoint для документов, а также интерфейса управления, который отвечает требованиям к подготовке и жизненному циклу.

Для почтовых ящиков сайта требуется интеграция и настройка Exchange 2016 или более поздней версии, а также SharePoint Server 2013 или более поздней версии. Дополнительные сведения о настройке организации Exchange Server для работы с организацией SharePoint см. в следующих разделах:

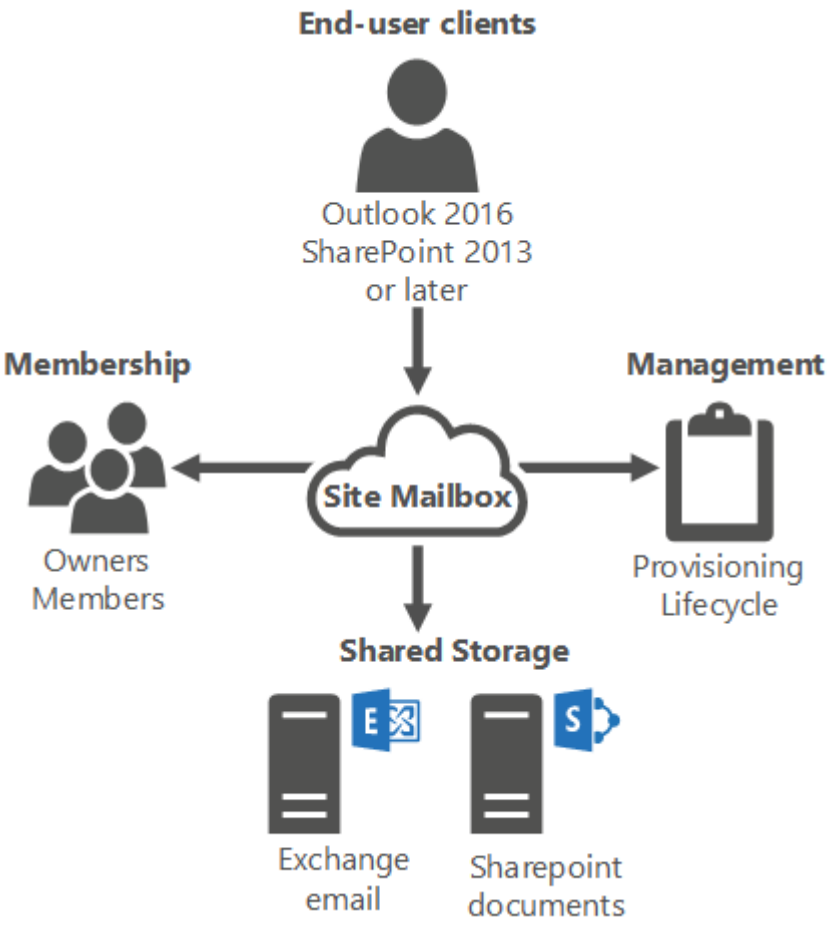
- Настройка почтовых ящиков сайта в SharePoint Server.
- Планирование интеграции Exchange Server с SharePoint и Skype для бизнеса

Дополнительные сведения о функциях совместной работы в Exchange Server см. в разделе Совместная работа.

Сведения о работе почтовых ящиков сайта

Когда один участник проекта отправляет почту или документы в почтовый ящик сайта, любой другой участник проекта может получить к ним доступ. Почтовые ящики сайта представлены в Outlook 2013 или более поздней версии. С их помощью пользователи могут получить доступ к сообщениям электронной почты и документам для важных проектов. Кроме того, к тому же содержимому можно

получить доступ с сайта SharePoint. Электронная почта хранится в Exchange, поэтому отображается так же, как в почтовых ящиках пользователей. Документы хранятся в SharePoint, что позволяет совместно редактировать документы и управлять их версиями. Exchange синхронизирует достаточно метаданных из SharePoint для создания представления документа в Outlook (например, название документа, дата последнего изменения, автор последнего изменения, размер).



Политики подготовки почтовых ящиков сайта

Квоты почтовых ящиков сайта можно задать с помощью командлетов **SiteMailboxProvisioningPolicy** в командной консоли Exchange. Политики подготовки почтовых ящиков сайта применяются только к сообщениям электронной почты, отправленным с почтовых ящиков сайта или отправленных на них, и определяют размер почтового ящика на сервере Exchange. Параметры репозитория документов настраиваются в SharePoint. Хотя с помощью командлета **New-SiteMailboxProvisioningPolicy** можно создать несколько политик подготовки почтовых ящиков сайта, только политика подготовки по умолчанию будет применена ко всем почтовым ящикам сайта. В вашей организации невозможно

применить несколько политик. Политики подготовки позволяют задать следующие квоты:

Quota	**Описание**	**Значение по умолчанию**
IssueWarningQuota	Параметр *IssueWarningQuota* указывает размер почтового ящика сайта, который активирует предупреждающее сообщение в почтовый ящик сайта.	4,5 ГБ
MaxReceiveSize	Параметр *MaxReceiveSize* указывает максимальный размер сообщений электронной почты, которые могут быть получены почтовым ящиком сайта.	36 МБ
ProhibitSendReceiveQuota	Параметр *ProhibitSendReceiveQuota* указывает размер, при котором почтовый ящик сайта больше не может отправлять или получать сообщения.	5 ГБ

Дополнительные сведения о настройке политик подготовки почтовых ящиков сайта см. в разделе Управление политиками создания почтовых ящиков сайта.

Политика жизненного цикла и хранения

Жизненным циклом почтового ящика сайта управляет SharePoint. Именно через SharePoint вы должны выполнять все задачи почтового ящика сайта, такие как создание и удаление почтовых ящиков сайта. Кроме того, можно создать политику жизненного цикла SharePoint для управления жизненным циклом почтового ящика сайта. Например, можно создать политику жизненного цикла в SharePoint, которая автоматически закрывает все почтовые ящики сайта через 6 месяцев. Если пользователю по-прежнему требуется использовать почтовый ящик сайта, он может повторно активировать почтовый ящик сайта через SharePoint. Рекомендуется использовать приложение жизненного цикла в ферме. Удаление активных почтовых ящиков сайта из Exchange вручную приведет к потере почтовых ящиков сайта.

Если приложение жизненного цикла в SharePoint закрывает почтовый ящик сайта, он хранится в течение периода, указанного в политике жизненного цикла в закрытом состоянии. Затем почтовый ящик может быть повторно активирован конечным пользователем или администратором из SharePoint. После окончания периода хранения к имени почтового ящика сайта Exchange, размещенного в базе

данных почтовых ящиков, будет добавлена приставка **MDEL:**, чтобы указать, что он был помечен для удаления. Вам потребуется вручную удалить эти ящики из базы данных, чтобы освободить место на диске и псевдоним. Если политики жизненного цикла SharePoint не включены, вы не сможете определить, какие почтовые ящики сайта отмечены для удаления. Пока такой ящик не будет удален администратором, его содержимое можно восстановить.

Для поиска и удаления почтовых ящиков сайта, отмеченных для удаления, можно использовать следующую команду.

PowerShell

```
Get-Mailbox MDEL:* | ?{$_.RecipientTypeDetails -eq "TeamMailbox"} | Remove-Mailbox -Confirm:$false
```

Почтовые ящики сайта не поддерживают функцию хранения на уровне элементов. Функция хранения для почтовых ящиков сайта работает на уровне проекта, поэтому при удалении всего ящика сайта удаляются все хранимые элементы.

Соответствие требованиям

При использовании консоли eDiscovery в SharePoint почтовые ящики сайта могут быть частью области для обнаружения данных на месте и поиска почтовых ящиков сайта и других ящиков по ключевым словам. Кроме того, вы можете поместить почтовый ящик сайта на судебное удержание. Дополнительные сведения см. в разделе Обнаружение электронных данных на месте в Exchange Server.

Резервное копирование и восстановление

Архивация и восстановление для почтовых ящиков сайта Exchange, размещенных на сервере почтовых ящиков, используют тот же метод архивации и восстановления, который применялся для всех почтовых ящиков Exchange. Дополнительные сведения см. в разделе Группы доступности баз данных.

Для документов SharePoint следует создать резервную копию и восстановить их в том же месте. Если вы восстановите содержимое SharePoint по тем же URL-адресам, почтовый ящик сайта продолжит работать, и дальнейшая настройка не требуется. При восстановлении по другому URL-адресу необходимо выполнить командлет **Set-SiteMailbox** , чтобы обновить свойство *SharePointURL* . Не рекомендуется восстанавливать SharePoint в новом лесу.

Общедоступные папки в Exchange Server

Статья • 04.04.2023

Общие папки предназначены для осуществления общего доступа к файлам. Это простой и эффективный способ сбора, организации и использования информации внутри рабочей группы или в масштабах всей организации. Общедоступные папки упрощают просмотр содержимого в глубокой иерархии. Пользователи увидят полную иерархию в Outlook, что позволяет им легко найти интересующее их содержимое.

Общедоступные папки доступны в следующих клиентах Outlook:

- Outlook в Интернете (прежнее название — Outlook Web App) для Exchange 2016 или более поздней версии
- Поддерживаемые версии Outlook для Exchange Server.
- Outlook для Mac 2016 и Outlook для Mac для Office 365.

Общедоступные папки также можно использовать в качестве метода архивирования для групп рассылки. Когда вы включаете поддержку почты для общедоступной папки и добавляете ее в качестве члена группы рассылки, электронная почта, отправляемая в группу, автоматически добавляется в общедоступную папку для последующего просмотра.

Общедоступные папки не предназначены для выполнения следующих действий:

- **Архивация данных**. Пользователи с ограничениями на почтовые ящики иногда используют общедоступные папки вместо почтовых ящиков для архивации данных. Этого делать не рекомендуется, поскольку это приводит к увеличению занимаемого пространства в общедоступных папках и лишает смысла использование ограничений для почтовых ящиков. Вместо этого рекомендуется использовать архивирование на месте в Exchange 2016 в качестве решения для архивации.
- **Общий доступ к документам и совместная работа**. Общедоступные папки не предоставляют управление версиями или другие функции управления документами, такие как контролируемые функции возврата и возврата, а также автоматические уведомления об изменениях содержимого. Вместо этого рекомендуется использовать SharePoint в качестве решения для совместного использования документации.

Дополнительные сведения об общедоступных папках и других методах совместной работы в Exchange см. в разделе Совместная работа.

Чтобы просмотреть некоторые часто задаваемые вопросы об общедоступных папках в Exchange, см. раздел Вопросы и ответы: общедоступные папки.

Дополнительные сведения об ограничениях и квотах для общедоступных папок см. в разделе Ограничения для общедоступных папок.

Архитектура общедоступных папок

Общедоступные папки используют инфраструктуру почтовых ящиков, чтобы воспользоваться преимуществами существующих технологий высокого уровня доступности и хранения базы данных почтовых ящиков. Архитектура общедоступных папок использует специальные почтовые ящики для хранения иерархий и содержимого общедоступных папок. Это также означает, что база данных общедоступных папок больше не существует, как в более ранней версии Exchange. Высокая доступность почтовых ящиков общедоступных папок обеспечивается группой DAG. Дополнительные сведения о группах доступности баз данных см. в разделе Группы доступности баз данных.

Основные архитектурные компоненты общедоступных папок — это почтовые ящики общедоступных папок, которые могут храниться в одной или нескольких базах данных почтовых ящиков.

Почтовые ящики общедоступных папок

Существует два типа почтовых ящиков общедоступных папок: *основной почтовый ящик иерархии* и *дополнительные почтовые ящики иерархии*. Оба типа почтовых ящиков могут иметь следующее содержимое.

- **Почтовый ящик первичной иерархии**. Почтовый ящик первичной иерархии — это одна записываемая копия иерархии общедоступных папок. Иерархия общедоступных папок копируется во все другие почтовые ящики общедоступных папок, но эти копии будут доступны только для чтения.
- **Почтовые ящики вторичной иерархии**. Почтовые ящики вторичной иерархии также содержат содержимое общедоступных папок и копию иерархии общедоступных папок только для чтения.

> **Примечание**

Политики хранения не поддерживаются для почтовых ящиков общедоступных папок.

Управлять почтовыми ящиками общедоступных папок можно двумя способами.

- В Центре администрирования Exchange перейдите в раздел **Общедоступные папки**>**Почтовые ящики общедоступных папок**.
- В командной консоли Exchange используйте набор командлетов ***-Mailbox** . В командлет New-Mailbox добавлены следующие параметры для поддержки почтовых ящиков общедоступных папок:
  - *PublicFolder*: этот параметр используется с командлетом **New-Mailbox** для создания почтового ящика общедоступных папок. При создании почтового ящика общедоступной папки создается новый почтовый ящик с типом почтового ящика `PublicFolder`. Дополнительные сведения см. в статье Создание почтового ящика общедоступных папок.
  - *HoldForMigration*. Этот параметр используется только при переносе общедоступных папок из Exchange 2010 в Exchange 2016. Дополнительные сведения см. в разделе Миграция общедоступных папок далее в этом разделе.
  - *IsHierarchyReady*: этот параметр указывает, готов ли почтовый ящик общедоступных папок для обслуживания иерархии общедоступных папок для пользователей. Для параметра задано значение `$True` только после синхронизации всей иерархии с почтовым ящиком общедоступных папок. Если для параметра установлено значение $False, пользователи не будут использовать его для доступа к иерархии. Однако если для свойства *DefaultPublicFolderMailbox* в почтовом ящике пользователя задан определенный почтовый ящик общедоступных папок, пользователь по-прежнему будет обращаться к указанному почтовому ящику общедоступных папок, даже если параметр *IsHierarchyReady* имеет значение `$False`.
  - *IsExcludedFromServingHierarchy*: этот параметр запрещает пользователям доступ к иерархии общедоступных папок в указанном почтовом ящике общедоступных папок. Для оптимального распределения нагрузки пользователи равномерно распределяются между почтовыми ящиками общедоступных папок по умолчанию. Когда значение этого параметра установлено для почтового ящика общедоступной папки, он не включается в автоматическое выравнивание нагрузки, и пользователи не будут иметь к

нему доступ для получения иерархии общедоступных папок. Но если у почтового ящика пользователя задать свойство *DefaultPublicFolderMailbox* равным определенному почтовому ящику общедоступных папок, пользователь сможет получить доступ к указанному ящику, даже если для него установлен параметр *IsExcludedFromServingHierarchy*.

Дополнительный почтовый ящик иерархии обеспечит передачу пользователям сведений об иерархии общедоступных папок, только если он явно указан в списке почтовых ящиков пользователей с помощью свойства *DefaultPublicFolderMailbox*, либо если соблюдены следующие условия:

- Свойство *IsHierarchyReady* в почтовом ящике общедоступной папки имеет значение `$True`.
- Свойство *IsExcludedFromServingHierarchy* в почтовом ящике общедоступной папки имеет значение `$False`.

Иерархия общедоступных папок

Иерархия общедоступных папок содержит свойства папок и информацию организации, включая структуру дерева. Каждый почтовый ящик общедоступных папок содержит копию иерархии общедоступных папок. Существует только одна записываемая копия иерархии, которая находится в основном почтовом ящике общедоступных папок. Данные об иерархии используются для определения следующей информации о папке:

- разрешения на папку;
- положение папки в дереве общедоступных папок (в том числе сведения о родительских и дочерних папках).

> **Примечание**
>
> В иерархии не хранится информация об адресах электронной почты для общедоступных папок с поддержкой почты. Адреса электронной почты хранятся в объекте каталога в Active Directory.

Синхронизация иерархии

В процессе синхронизации иерархии общедоступных папок используется инкрементная синхронизация изменений (ICS), которая предоставляет механизм для мониторинга и синхронизации изменений в иерархии или содержимом

хранилища Exchange. Изменения включают создание, изменение и удаление папок и сообщений. Когда пользователи подключены к почтовым ящикам содержимого и используют их, синхронизация выполняется каждые 15 минут. Если пользователи не подключены к почтовому ящику содержимого, синхронизация будет запускаться реже (каждые 24 часа). Если операция записи, например создание папки, выполняется в первичной иерархии, синхронизация запускается немедленно (синхронно) с почтовым ящиком содержимого.

> **Важно!**
>
> Поскольку существует только одна записываемая копия иерархии, создание папки передается в почтовый ящик иерархии почтовым ящиком содержимого, к которому подключены пользователи.

В большой организации при создании нового почтового ящика общедоступной папки иерархия должна быть синхронизирована с этой папкой до того, как к ней смогут подключаться пользователи. В противном случае пользователи, подключающиеся с помощью Outlook, будут видеть неполную структуру общедоступной папки. Чтобы не привязывать время синхронизации к попыткам пользователей подключиться к новому почтовому ящику общедоступных папок, при создании почтового ящика общедоступных папок задайте параметр *IsExcludedFromServingHierarchy* в командлете **New-Mailbox**. Благодаря этому параметру становится невозможным подключение пользователей к созданному почтовому ящику общедоступных папок. После завершения синхронизации выполните командлет Set-Mailbox с параметром `false` *IsExcludedFromServingHierarchy*, указывающим, что почтовый ящик общедоступных папок готов к подключению. К тому же, можно использовать командлет Get-PublicFolderMailboxDiagnostics, чтобы просматривать состояние синхронизации с помощью свойств *SyncInfo* и *AssistantInfo*.

Дополнительные сведения см. в статье Создание общедоступной папки.

Содержимое общедоступной папки

Содержимое общедоступной папки может включать адреса электронной почты, публикации, документы и электронные бланки. Содержимое хранится в почтовом ящике общедоступных папок, но не реплицируется в различные почтовые ящики общедоступных папок. Все пользователи получают доступ к одному и тому же почтовому ящику общедоступных папок и одному и тому же набору содержимого. Несмотря на то что доступен полнотекстовый поиск в содержимом общедоступных

папок, нельзя выполнять поиск среди содержимого различных общедоступных папок, и содержимое не индексируется системой поиска Exchange.

> 7 **Примечание**
>
> Outlook в Интернете поддерживается, но с ограничениями. Вы можете добавлять общедоступные папки в избранное и удалять их оттуда, а также создавать, редактировать, удалять записи и отвечать на них. Однако в Outlook в Интернете нельзя создавать и удалять общедоступные папки. Кроме того, в список избранного в Outlook в Интернете можно добавлять только общедоступные папки "Почта", "Публикации", "Календарь" и "Контакты".

Перенос общедоступных папок

- Общедоступные папки можно перенести в следующих сценариях:
- От Exchange 2010 до Exchange 2016 или Exchange Online.
- С Exchange 2016 или более поздней версии до Exchange Online.

Общедоступные папки 2010 SP3 необходимо перенести в Exchange 2016. Для этого используйте командлеты **PublicFolderMigrationRequst**. Дополнительные сведения см. в статье Использование пакетной миграции для переноса общедоступных папок Exchange 2010 в Exchange 2016. Если ваша организации переходит на Exchange Online, вы можете перенести общедоступные папки в облако и обновить их одновременно. Дополнительные сведения см. в разделах Использование пакетной миграции для переноса устаревших общедоступных папок в Microsoft 365, Office 365 и Exchange Online и Использование пакетной миграции для переноса Exchange Server общедоступных папок в Exchange Online.

Из-за изменений в способе хранения общедоступных папок почтовые ящики Exchange 2010 не могут получить доступ к иерархии общедоступных папок в Exchange 2016 или на Exchange Online. Однако почтовые ящики пользователей в Exchange 2016 могут подключаться к общедоступным папкам Exchange 2010. Общедоступные папки Exchange 2016 и устаревшие общедоступные папки не могут существовать одновременно в организации Exchange. Это фактически означает, что между версиями не существует сосуществования. Перенос общедоступных папок в Exchange Server 2016 или Exchange Online в настоящее время является одноразовым процессом перехода.

По этой причине рекомендуется перед переносом общедоступных папок Exchange 2010 сначала перенести почтовые ящики Exchange 2010 в Exchange 2016 или Exchange Online. Дополнительные сведения о переносе почтовых ящиков см. в разделах Перемещение почтовых ящиков в Exchange Server, Миграция электронной почты с помощью метода прямой передачи Exchange и Выполнение поэтапной миграции электронной почты в Microsoft 365 или Office 365.

Перемещение общедоступных папок

Вы можете переместить общедоступные папки в другой почтовый ящик общедоступных папок, а почтовые ящики общедоступных папок — в другую базу данных почтовых ящиков. Чтобы переместить общедоступные папки в другие почтовые ящики общедоступных папок, используйте набор командлетов **PublicFolderMoveRequest**. Вложенные папки в перемещаемой общедоступной папке не будут перемещаться по умолчанию. Если вы хотите переместить ветвь общедоступных папок, можно использовать `Move-PublicFolderBranch.ps1` скрипт, установленный по умолчанию в Exchange. Дополнительные сведения см. в разделе Перемещение общедоступной папки в другой почтовый ящик общедоступных папок.

Помимо перемещения общедоступных папок можно перемещать почтовые ящики общедоступных папок в другие базы данных почтовых ящиков с помощью набора командлетов **MoveRequest**. Это тот же набор командлетов, который использовался для перемещения обычных почтовых ящиков. Подробнее см. в статье Move a public folder mailbox to a different mailbox database.

Для асинхронного перемещения общедоступных папок командлеты **PublicFolderMoveRequest** и **MoveRequest** используют службу репликации почтовых ящиков. Это означает, что командлет не выполняет реальную работу, и в течение большей части перемещения общедоступные папки и почтовые ящики общедоступных папок по-прежнему будут доступны пользователям. Так как служба репликации почтовых ящиков выполняет перемещения почтовых ящиков, импорт и экспорт запросов, а также запросы на перемещение общедоступных папок, важно рассмотреть возможность регулирования и управления рабочей нагрузкой.

Квоты общедоступных папок

По умолчанию новые почтовые ящики общедоступных папок автоматически наследуют ограничения размера базы данных почтовых ящиков. В результате, чтобы точно оценить текущее состояние квоты хранилища для почтового ящика

общедоступных папок с помощью командлета Get-Mailbox , сначала необходимо проверить значение свойства *UseDatabaseQuotaDefaults* :

- Если значение равно `True`, параметры для каждого почтового ящика игнорируются и используются ограничения базы данных почтовых ящиков.
- Если значение равно `False`, используются параметры для каждого почтового ящика.

Если свойство *UseDatabaseQuotaDefaults* имеет значение `True` , а свойства *ProhibitSendQuota*, *ProhibitSendReceiveQuota* и *IssueWarningQuota* имеют значение `unlimited`, размер почтового ящика на самом деле не является неограниченным. Вместо этого необходимо использовать командлет Get-MailboxDatabase и просмотреть соответствующие ограничения хранилища базы данных почтовых ящиков, чтобы узнать, какие ограничения для почтового ящика. Квота базы данных почтовых ящиков по умолчанию:

- *IssueWarningQuota*: 1,9 ГБ
- *ProhibitSendQuota*: 2 ГБ
- *ProhibitSendReceiveQuota*: 2,3 ГБ

Чтобы получить сведения о квотах базы данных почтовых ящиков, используйте командлет Get-MailboxDatabase.

Чтобы задать квоты для почтового ящика общедоступных папок, используйте командлет Set-OrganizationConfig с параметрами *DefaultPublicFolderIssueWarningQuota* и *DefaultPublicFolderProhibitPostQuota* .

Аварийное восстановление

Общедоступные папки основаны на инфраструктуре почтовых ящиков и используют те же механизмы доступности и избыточности. Как и обычные почтовые ящики, каждый почтовый ящик общедоступных папок может иметь несколько резервных копий с автоматической отработкой отказа. Дополнительные сведения см. в статье Планирование высокого уровня доступности и устойчивости сайта.

Помимо сценария комплексного аварийного восстановления можно также восстанавливать общедоступные папки в следующих ситуациях.

- **Обратимо удаленное восстановление общедоступных папок**.
  Общедоступная папка была удалена, но по-прежнему находится в пределах

срока хранения.

- **Обратимо удаленное восстановление почтового ящика общедоступных папок**. Почтовый ящик общедоступной папки был удален и по-прежнему находится в пределах срока хранения почтового ящика.

- **Восстановление почтового ящика общедоступных папок из базы данных восстановления**. Вы можете восстановить отдельный почтовый ящик общедоступных папок из резервной копии по истечении срока хранения удаленного почтового ящика. Затем вы можете извлечь данные из восстановленного почтового ящика и скопировать их в папку или добавить в другой почтовый ящик.

Во всех этих ситуациях восстановление общедоступных папок или почтовых ящиков общедоступных папок можно выполнить с помощью командлетов **MailboxRestoreRequest**.

Дополнительные сведения см. в статье Восстановление общедоступных папок и почтовых ящиков общедоступных папок после неудачных перемещений.

Часто задаваемые вопросы о переносе общедоступных папок

Статья • 04.04.2023

В этой статье содержатся часто задаваемые вопросы о миграции общедоступных папок.

Часто задаваемые вопросы и дополнительные сведения

Дополнительные сведения об общедоступных папках см. в статье Общедоступные папки.

Дополнительные сведения о переносе общедоступных папок см. в разделе:

- Использование пакетной миграции для переноса общедоступных папок Exchange 2010 в Exchange 2016
- Перенос общедоступных папок из Exchange 2013 в Exchange 2016 или Exchange 2019
- Использование пакетной миграции для переноса устаревших общедоступных папок в Microsoft 365, Office 365 или Exchange Online
- Использование пакетного переноса для переноса общедоступных папок Exchange Server в Exchange Online
- Использование пакетной миграции для миграции Exchange Server общедоступных папок в Группы Microsoft 365

Какие сценарии переноса общедоступных папок поддерживаются?

В следующем списке описаны доступные варианты переноса общедоступных папок в Exchange или Exchange Online.

- Общедоступные папки Exchange 2010 (SP3 RU8 или более поздней версии) можно перенести в группы Exchange 2016, Exchange Online или Microsoft 365.

- Общедоступные папки Exchange 2013 (CU15 или более поздней версии) можно перенести в группы Exchange 2016, Exchange 2019, Exchange Online или Microsoft 365.

- Общедоступные папки Exchange 2016 (CU4 или более поздней версии) можно перенести в группы Exchange Online или Microsoft 365.
- Общедоступные папки Exchange 2019 можно перенести в группы Exchange Online или Microsoft 365.

В настоящее время поддерживается только миграция в Exchange 2016 или Exchange 2019 в том же лесу Active Directory. Миграция общедоступных папок между лесами из Exchange 2013, Exchange 2016 или Exchange 2019 в другую локальную организацию Exchange не поддерживается.

Что происходит с иерархией на исходных серверах Exchange 2010 после миграции на Exchange 2016?

На этапе завершения миграции на исходном сервере устанавливается блокировка, чтобы сделать его недоступным для пользователей. Эта блокировка предотвращает доступ пользователей к исходным общедоступным папкам и после миграции. Снимать блокировку не рекомендуется, потому что изменения невозможно синхронизировать с Exchange 2016.

Что происходит с существующими правилами общедоступных папок при их переносе?

Правила общедоступных папок переносятся вместе с данными и сохраняются в качестве правил общедоступных папок. Они не преобразуются в правила почтовых ящиков.

Что происходит, если изменения иерархии выполняются в источнике после создания исходного CSV-файла? Каким образом это отразится на точке назначения?

CSV-файл используется для определения сопоставления исходной иерархии и почтового ящика назначения. Он содержит только папки верхнего уровня. Миграция папок, являющихся дочерними для папок верхнего уровня, выполняется автоматически. Поэтому добавляемая новая дочерняя папка переносится непосредственно в ходе процесса. Создание папки верхнего уровня осуществляется в почтовом ящике, который содержит доступную для записи копию иерархию.

Как при миграции географически распределенной иерархии можно убедиться, что общие папки создаются в ближайшем расположении к конечным пользователям?

В процессе миграции создается файл .csv (с помощью скрипта `publicfoldertomailboxmapgenerator.ps1`). Этот файл содержит сопоставление папки и почтового ящика для новой иерархии. Этот .csv файл можно использовать для создания почтовых ящиков общедоступных папок в соответствующем географическом расположении и изменения файла, чтобы поместить необходимые папки в соответствующий почтовый ящик, чтобы они были рядом с целевыми пользователями.

Входной .csv файл можно создать, запустив скрипт `AggregatePFData.ps1`, расположенный в каталоге < Каталог >*установки Exchange*\V15\Scripts. Выполните сценарий следующим образом.

PowerShell

```
.\AggregatePFData.ps1 | Select-Object -property @{Name="FolderName";
Expression = {$_.Identity}}, @{Name="FolderSize"; Expression =
{$_.TotalItemSize.Value.ToBytes()}} | Export-CSV -Path <Path followed by the
name of the CSV>
```

Выполняется ли перенос существующих разрешений общих папок?

Да, разрешения будут автоматически перенесены на уровне папки вместе с данными. Выполнять это действие отдельно не требуется.

Использование общих папок прекращается?

Нет. Общедоступные папки отлично подходят для интеграции с Outlook, простых сценариев общего доступа и предоставления доступа к одним и тем же данным большому количеству пользователей.

Какие клиенты поддерживают общие папки?

Поддерживаемые в настоящее время клиенты Outlook для Exchange Server могут получать доступ к общедоступным папкам. Однако пользователи с почтовыми

ящиками на серверах Exchange 2016 не могут подключаться к общедоступным папкам Exchange 2010 с помощью клиентов веб-служб Exchange (EWS) (например, Outlook 2016 для Mac). Рекомендуется перенести общедоступные папки Exchange 2010 в Exchange 2016, чтобы обеспечить доступ для этих пользователей.

Можно ли получить доступ к общедоступным папкам с помощью смартфонов или мобильных телефонов?

Доступ к общедоступным папкам работает из Классического приложения Outlook для Windows и Outlook для Mac. Однако клиентские приложения для смартфонов, включая Outlook для Android или Outlook для iOS, не поддерживают подключение к общедоступным папкам.

Если вы хотите использовать функции, аналогичные общедоступным папкам с содержимым, доступным на мобильных устройствах, ознакомьтесь с дополнительными сведениями о Группы Microsoft 365.

Существуют ли ограничения для клиентов?

Outlook в Интернете (предыдущее название — Outlook Web App) поддерживается, но с некоторыми ограничениями. Вы можете добавлять общедоступные папки в избранное и удалять их оттуда (если это общедоступные папки почты, публикаций, календаря и контактов), а также создавать, редактировать, удалять записи и отвечать на них. Однако в Outlook в Интернете недоступны следующие функции:

- создание и удаление общедоступных папок;
- перетаскивание содержимого;
- доступ к общедоступным папкам, расположенным на серверах под управлением предыдущих версий Exchange.

> ⓘ **Примечание**
>
> Правила общих папок, которые содержат элемент **ответить, используя указанный шаблон**, можно создать только в общих папках с включенной поддержкой почты. Возможно, что существующие правила, содержащие элемент **ответить, используя указанный шаблон**, продолжат работать с общими папками с отключенной поддержкой почты, но для таких папок

невозможно создать новые правила с этим элементом шаблона или изменить существующие правила с этим элементом.

В гибридном сценарии Outlook в Интернете не поддерживается для кросс-локальных общедоступных папок. Пользователи должны находиться в том же расположении, что и общедоступные папки, чтобы получить к ним доступ с помощью Outlook в Интернете. Outlook 2016 для Mac пользователи могут получить доступ к общедоступным папкам в гибридном сценарии, если выполняются следующие условия:

- Вы выполнили процедуры, описанные в статье Процедуры гибридного развертывания.
- Обновление за апрель 2016 г. для Outlook 2016 для Mac установлено на всех клиентах.

Каким образом можно сохранить очень большую иерархию в почтовом ящике общих папок?

Дополнительные сведения о размерах общедоступных папок см. в статье Ограничения общедоступных папок.

Как можно просмотреть иерархию общих папок в почтовом ящике?

Выполните следующую команду:

```
PowerShell

Get-OrganizationConfig | Format-List RootPublicFolderMailbox
```

Подробные сведения о синтаксисе и параметрах см. в разделе Get-OrganizationConfig.

Как создать почтовые ящики содержимого для общих папок с помощью командлетов командной консоли Exchange?

Чтобы создать первый почтовый ящик иерархии общих папок и дополнительные почтовые ящики иерархии, выполните следующую команду.

PowerShell

```
New-Mailbox -PublicFolder -Name <name of public folder>
```

Дополнительные сведения см. в разделе Создание общедоступной папки.

В Exchange 2010 для каждой базы данных почтовых ящиков можно было указать свою базу данных общедоступных папок. Как это работает сейчас?

Больше нет параметра уровня базы данных. Вместо этого Exchange имеет возможность указывать почтовый ящик общедоступной папки на уровне почтового ящика, но по умолчанию Exchange автоматически вычисляет почтовый ящик иерархии для каждого пользователя.

Как используются средства метрик общедоступных папок в Exchange?

Для получения данных метрик общедоступных папок можно использовать командлеты Get-PublicFolderStatistics и Get-PublicFolderItemStatistics . Это же решение было доступно с Exchange 2010, поэтому здесь ничего не изменилось. Для создания отчетов об общедоступных папках не требуются дополнительные надстройки.

Могут ли общедоступные папки отличать доступ к общедоступным папкам от доступа третьей стороны?

Начиная с Exchange 2013, разрешениями для общедоступных папок можно управлять с помощью управления доступом на основе ролей (RBAC); списки управления доступом (ACL) больше не используются. Командлеты Get-PublicFolderStatistics и Get-PublicFolderItemStatistics можно использовать для отслеживания учетных записей, выполняющих административные задачи, и

последующего аудита доступа соответствующим образом. Дополнительные сведения о RBAC см. в статье Общие сведения о контроль доступа на основе ролей.

Работает ли функция ведения журнала аудита для общих папок?

Нет. В настоящее время нет.

Если вы хотите, чтобы функции, аналогичные общедоступным папкам с ведением журнала аудита, см. в статье Дополнительные сведения о Группы Microsoft 365 .

Какие существуют ограничения для общих папок? Что делать?

Дополнительные сведения об ограничениях общедоступных папок см. в статье Ограничения общедоступных папок.

Какие существуют рекомендации по разделению почтовых ящиков общих папок? Должны ли они оставаться в той же базе данных?

В предыдущих версиях Exchange можно было разделять общедоступные папки между базами данных общедоступных папок. Можно расположить разделенный почтовый ящик общедоступных папок в одной или нескольких базах данных почтовых ящиков. Обычно рекомендуется размещать разделенный почтовый ящик в различных базах данных, чтобы сбалансировать хранилище с вводом-выводом.

Можно ли установить политики хранения для общедоступных папок?

Как и в предыдущих версиях Exchange, можно установить ограничения на хранение элементов. Дополнительные сведения см. в разделе Ограничения для общедоступных папок.

Можно ли указать пользователей, которые используют определенный почтовый ящик общедоступных папок?

В Exchange 2010 можно было указать, какие пользователи имеют доступ к определенным общедоступным папкам. В Exchange 2013 или более поздней версии можно задать почтовый ящик общедоступных папок по умолчанию для каждого пользователя. Для этого выполните командлет Set-Mailbox с параметром *DefaultPublicFolderMailbox* . Например:

PowerShell

```
Set-Mailbox -Identity kweku@contoso.com -DefaultPublicFolderMailbox
"PF_Administration"
```

Как влияет на пользователя нарушение основной иерархии?

Если почтовый ящик общедоступной папки главной иерархии выходит из строя, пользователи могут просматривать общедоступные папки, но не записывать их. Чтобы предотвратить снижение иерархии, рекомендуется включить общедоступные папки в группу доступности базы данных (DAG). Дополнительные сведения о группах доступности баз данных см. в разделе Группы доступности баз данных.

Можно ли изменить почтовый ящик общедоступных папок, который является основной иерархией?

Нет. При изменении будет выведено сообщение об ошибке.

Доступен ли для общедоступных папок полнотекстовый поиск?

Да, полнотекстовый поиск доступен для общедоступных папок с Exchange 2013. Однако нельзя выполнять поиск в нескольких общедоступных папках.

Ограничения для общедоступных папок в Exchange Server

Статья • 04.04.2023

В Exchange Server общедоступные папки основаны на архитектуре почтового ящика, которая обладает устойчивостью группы доступности базы данных (DAG) и другими улучшениями почтовых ящиков. Тем не менее, существуют ограничения и рекомендации по производительности, которые следует учитывать.

Ограничения

В следующей таблице перечислены ограничения для общедоступных папок в локальной Exchange Server. Если ограничения не указаны, как рекомендуется, значения, перечисленные в этой таблице, являются поддерживаемыми ограничениями для общедоступных папок.

> **ⓘ Важно!**
>
> Ищете ограничения Exchange Online для Microsoft 365 или Office 365? в статье **Ограничения Exchange Online**.

Элемент	Ограничения	Примечания
Общее число почтовых ящиков общедоступных папок	1,000	1000 — это ограничение для Exchange Server 2016 cu2 или более поздней версии. Хотя вы можете создать более 1000 почтовых ящиков общедоступных папок, он официально не поддерживается. См . статью Создание почтового ящика общедоступных папок.
Общее число общедоступных папок в иерархии	1,000,000	Хотя вы можете создать более 1 000 000 общедоступных папок, она официально не поддерживается. При развертывании 100 000 или более общих папок мы рекомендуем изучить раздел Рекомендации по развертыванию общедоступных папок.
Вложенные папки в родительской папке	10,000	Хотя в родительской папке можно создать более 1000 вложенных папок, это не рекомендуется. Ограничение можно применить с помощью параметра *FolderHierarchyChildrenCountReceiveQuota* в командлете Set-Mailbox .

Элемент	Ограничения	Примечания
Глубина вложенности папок	300	Глубина папок — это число уровней вложенных папок, допустимое в одной ветви дерева общедоступной папки. Ограничение можно применить с помощью параметра *FolderHierarchyDepthReceiveQuota* в командлете Set-Mailbox .
Максимальное число сообщений на общую папку	1 миллион	Ограничение можно применить с помощью параметра *MailboxMessagesPerFolderCountRecieveQuota* в командлете Set-Mailbox .
Максимальный размер отдельной общедоступной папки	10 ГБ	В это ограничение не входят вложенные папки в одной папке. См . раздел Настройка квот хранилища для почтового ящика.
Размер почтового ящика общедоступной папки	100 ГБ	Хотя размер почтового ящика общедоступных папок может превышать 100 ГБ, он официально не поддерживается. См . раздел Настройка квот хранилища для почтового ящика.
Количество входов пользователей на почтовый ящик общедоступных папок	2000 параллельных входов пользователей	Рекомендуется настроить иерархию так, чтобы на почтовый ящик общедоступных папок было не более 2000 пользователей. Например, если у вас 20 000 пользователей, у вас должно быть 10 почтовых ящиков общедоступных папок.
Хранение перемещенных элементов	Рекомендуемый срок составляет 14 дней	Используйте параметр *DefaultPublicFolderMovedItemRetention* в командлете Set-OrganizationConfig .
Ограничения времени хранения	Рекомендуем установить для этого параметра то же значение, что по умолчанию используется для обычных почтовых ящиков.	Эти параметры можно установить на следующих уровнях. **Уровень организации**. Используйте параметр *DefaultPublicFolderAgeLimit* в командлете Set-OrganizationConfig . **Уровень папки**. Используйте параметр *AgeLimit* в командлете Set-PublicFolder .

Элемент	Ограничения	Примечания
Хранение удаленного элемента	Рекомендуем установить для этого параметра то же значение, что по умолчанию используется для обычных почтовых ящиков.	Эти параметры можно установить на следующих уровнях. **Уровень организации**. Используйте параметр *DefaultPublicFolderMovedItemRetention* в командлете Set-OrganizationConfig . **Уровень почтового ящика**. Используйте *RetainDeletedItemsFor* в командлете Set-Mailbox . **Уровень папки**. Используйте параметр *RetainDeleteItemsFor* в командлете Set-PublicFolder .
Максимальное количество общедоступных папок, которые можно перенести из Exchange 2010 в Exchange 2016	500 000	Это максимальное количество общедоступных папок, которые можно переместить в Exchange из Exchange 2010 за одну миграцию. Хотя вы можете попытаться перенести более 500 000 папок, она официально не поддерживается. Дополнительные сведения о переносе общедоступных папок см. в статье Использование пакетной миграции для переноса общедоступных папок из Exchange 2010 в Exchange 2016.

Рекомендации по развертыванию общедоступных папок Exchange

Статья • 04.04.2023

Хотя использование общедоступных папок Exchange имеет много преимуществ, перед их реализацией в организации следует учитывать некоторые моменты.

Аспекты развертывания общедоступных папок

В этой статье описаны аспекты, которые необходимо учитывать при развертывании общедоступных папок в организации, особенно если вы собираетесь создать большое количество общедоступных папок. Exchange Server поддерживает до миллиона общедоступных папок.

- От действий в общедоступной папке напрямую зависит нагрузка на почтовый ящик общедоступных папок, в котором она находится. Во избежание проблем с подключением к клиенту, например высоких задержек или недоступности общедоступной папки, рекомендуется следующее.

  - Следите за тем, чтобы почтовые ящики общедоступных папок не превышали 50 % от максимального размера почтового ящика. В этом случае рассмотрите возможность использования скрипта `Split-PublicFolderMailbox.ps1`, расположенного в папке C:\Program Files\Microsoft\Exchange Server\V15\Scripts на сервере Exchange Server, для перемещения некоторых общедоступных папок в новый почтовый ящик общедоступных папок.

  - Рассмотрите возможность перемещения широко используемых общедоступных папок в выделенный почтовый ящик общедоступных папок.

  - Исключите широко используемые общедоступные папки из иерархии общедоступных папок. Это можно сделать, задав свойство *IsExcludedFromServingHierarchy* в почтовом ящике общедоступной папки с помощью командлета **Set-Mailbox** .

  - В больших организациях, где используется много общедоступных папок, рекомендуется добавить дополнительные почтовые ящики общедоступных

папок для распределения нагрузки запросов к иерархии обслуживания общедоступных папок.

- Чтобы улучшить доступность основного почтового ящика общедоступных папок, поместите его в группу обеспечения доступности баз данных. Основной почтовый ящик общедоступных папок является достоверной копией иерархии общедоступных папок.

- Поместите дополнительные почтовые ящики общедоступных папок в группу обеспечения доступности баз данных, или часто создавайте резервные копии почтовых ящиков.

- Разместите почтовые ящики общедоступных папок в географическом местонахождении как можно ближе к пользователям, которые будут обращаться к контенту таких папок.

- Чтобы ускорить доступ к иерархии общедоступных папок, в свойстве DefaultPublicFolderMailbox почтовых ящиков пользователей укажите почтовый ящик общедоступных папок, расположенный рядом с ними. Таким образом, эти пользователи не смогут получать иерархию общедоступных папок из почтового ящика общедоступных папок в других географических местонахождениях.

- Если в развертывании более 50 дополнительных почтовых ящиков общедоступных папок, мы рекомендуем не хранить контент общедоступных папок в основном почтовом ящике общедоступных папок. Так у вас будет основной почтовый ящик общедоступных папок, выделенный для синхронизации с дополнительными почтовыми ящиками общедоступных папок.

- Exchange 2016 не поддерживает базы данных общедоступных папок. В результате пользователи Outlook в Интернете не смогут получить доступ к общедоступным папкам Exchange 2010. Пользователи Exchange 2016 могут получить доступ к общедоступным папкам Exchange 2010 в Outlook или Outlook для Mac.

- Outlook в Интернете поддерживается, но с ограничениями. Вы можете добавлять общедоступные папки в избранное и удалять их оттуда, а также создавать, редактировать, удалять записи и отвечать на них. Однако в Outlook в Интернете нельзя создавать и удалять общедоступные папки. Кроме того, в список избранного в Outlook в Интернете можно добавлять только общедоступные папки "Почта", "Публикации", "Календарь" и "Контакты".

- Хотя полнотекстовый поиск содержимого общедоступных папок доступен, содержимое общедоступных папок невозможно найти в общедоступных папках, и содержимое не индексируется поиском Exchange.
- Для доступа к общедоступным папкам на серверах Exchange server необходимо использовать Outlook 2010 или более поздней версии.
- Политики хранения не поддерживаются для почтовых ящиков общедоступных папок.

Перенос общедоступных папок в компонент "Группы" Microsoft 365

Статья • 04.04.2023

В этой статье приводится сравнение общедоступных папок и Группы Microsoft 365, а также то, как одно или другое может быть лучшим решением для вашей организации. Общедоступные папки существовали с первого выпуска Exchange, а служба "Группы Office 365" появилась только недавно. Если вы хотите перенести все общедоступные папки (или некоторые из них) в группы Office 365, то в этой статье вы найдете описание процесса и ссылки на статьи с пошаговыми инструкциями.

Что такое общедоступные папки?

Public folders содержат различные данные, упорядоченные в виде иерархической структуры.

Общедоступные папки не рекомендуется использовать в следующих ситуациях:

- **Архивация данных**. Пользователи с ограничениями почтовых ящиков иногда используют общедоступные папки вместо почтовых ящиков для архивации данных. Этого делать не рекомендуется, поскольку это приводит к увеличению занимаемого пространства в общедоступных папках и лишает смысла использование ограничений для почтовых ящиков.
- **Общий доступ к документам и совместная работа**. Общедоступные папки не предоставляют функции управления документами, такие как управление версиями, управляемые функции возврата и возврата, а также автоматическое уведомление об изменениях содержимого.

Что такое Группы Microsoft 365?

Группы Microsoft 365 позволяют выбрать набор людей, с которыми вы хотите сотрудничать, а затем легко настроить коллекцию ресурсов, которыми эти пользователи могут поделиться. Вам не придется вручную назначать разрешения для этих ресурсов, так как при добавлении членов группы они автоматически получают разрешения, необходимые для доступа к инструментам и ресурсам группы. Такие группы также упрощают выполнение задач, для которых раньше использовались списки рассылки и общие почтовые ящики.

Полный рассказ о группах см. в статье Сведения об Группы Microsoft 365.

Следует ли перенести общедоступные папки в Группы Microsoft 365?

Группы Microsoft 365 — это последнее предложение корпорации Майкрософт для совместной работы. Это означает, что существует множество причин, по которым они предпочтительнее, чем общедоступные папки, гораздо более старая технология. Например, в Outlook группы могут полностью заменить общедоступные папки с поддержкой почты. Составление списка всех сценариев, в которых Группы Microsoft 365 работает лучше, чем общедоступные папки, невозможно, но вот основные моменты:

- **Совместная работа по электронной почте**. Группы в Outlook имеют выделенное пространство **бесед,** в котором хранятся все сообщения электронной почты и пользователи могут совместно работать над ними. Группу можно даже настроить для получения сообщений от людей за пределами группы или организации. Например, если в настоящее время вы используете общедоступные папки, поддерживающие почту, для хранения обсуждений проектов или заказов на покупку, которые должны быть доступны нескольким людям, то использовать группы будет предпочтительнее. Кроме того, группы лучше подходят для тех случаев, когда вам просто нужно публиковать сведения для нескольких пользователей.

- **Совместная работа над документами**. В Outlook в группе есть выделенная вкладка **Файлы** , на которую отображаются все файлы с сайта группы SharePoint и из почтовых вложений. Все файлы отображаются в одном представлении, и их не приходится искать повсюду, как в общедоступных папках. Совместное редактирование также становится проще. Если вы используете общедоступные папки для хранения файлов, предназначенных для использования несколькими людьми, рассмотрите возможность миграции в службу "Группы Office 365".

- **Общий календарь**. При создании каждая группа получает общий календарь (см. раздел Общий доступ к календарю в Microsoft 365. Любой участник группы может создавать события в этом календаре. Если вы предпочитаете группу, календарь этой группы может отображаться вместе с вашим личным календарем. Вы также можете подписаться на события группы. В этом случае события, созданные в соответствующей группе, отображаются в вашем личном календаре. Если вы размещаете в общедоступных папках календари для своей команды, например, чтобы у нее был доступ к расписанию или

графику, то служба «Группы Microsoft 365» также расширит ваши возможности.

- **Упрощенные разрешения**. При назначении пользователей группе они сразу же получают необходимые разрешения, в то время как с общедоступными папками необходимо вручную назначить соответствующие разрешения. Участники могут быть добавлены как "владельцы" или "члены". Владельцы обладают полными правами в группе, включая возможность выполнения задач по управлению группами. Участники также могут создавать содержимое и редактировать файлы, например владельцы, но не могут удалять содержимое, которое они не создали. Если модель разрешений общедоступных папок слишком ошеломляющая, и вы хотите что-то простое и быстрое, Группы Microsoft 365 — это путь.

- **Мобильное и веб-присутствие**. Общедоступные папки не могут быть доступны через мобильные устройства и имеют ограниченный набор функциональных возможностей в Интернете. Группы Microsoft 365, с другой стороны, доступен через мобильные приложения Outlook и имеет более широкий набор функций в Интернете. Если участники вашей команды постоянно путешествуют и им нужен мобильный доступ, то следует использовать службу «Группы Microsoft 365».

- **Доступ к широкому спектру приложений Microsoft 365 или Office 365**. При создании группы вы открываете доступ к широкому кругу приложений из Microsoft 365 или Office 365 набора. Вы получаете сайт группы SharePoint для хранения файлов и расписание в Планировщике для отслеживания задач. Группы Microsoft 365 — это служба членства, объединяющая элементы всего набора Microsoft 365 или Office 365.

Хотя Группы Microsoft 365 предлагает множество преимуществ, следует учитывать значительное различие, которое вы заметите после выхода из интерфейса общедоступных папок. Это различие в первую очередь:

- **Детализированные роли разрешений**. Хотя общедоступные папки имеют различные роли разрешений, Группы Microsoft 365 предоставляет только две роли: владельца и участника.

Прежде чем переходить на "Группы Office 365", также рекомендуем учесть различные ограничения, связанные с созданием и обслуживанием групп. Дополнительные сведения см. в разделе *Разделы справки управлять группами?* статьи Сведения о Группы Microsoft 365 .

Перенос общедоступных папок в Группы Microsoft 365

Если вы решили переключиться на Группы Microsoft 365, можно использовать процесс, известный как *пакетная миграция*, для перемещения электронной почты и содержимого календаря из существующих общедоступных папок в группы. Конкретный способ запуска пакетной миграции зависит от того, в какой версии Exchange на данный момент размещается иерархия общедоступных папок. В конце этой статьи вы найдете ссылки на инструкции по пакетной миграции.

В качестве необходимого условия для переноса общедоступных папок из Exchange в группы Microsoft 365 необходимо убедиться, что параметр **"Общедоступная папка почты Exchange**" в средстве Azure AD Connect *не* установлен. Если этот параметр установлен, снимите флажок перед началом миграции общедоступных папок. По умолчанию этот параметр не установлен.

> ⓘ **Примечание**
>
> После завершения миграции общедоступной папки с поддержкой почты в определенную группу в Microsoft 365 или Office 365 все сообщения электронной почты, адресованные общедоступной папке, будут получены группой.

Ниже перечислены ключевые преимущества пакетной миграции.

- **Миграция на основе службы репликации почтовых ящиков (MRS).** В процессе миграции используются командлеты пакетной миграции. В одном пакете миграции можно запустить миграцию в несколько групп. Существуют также скрипты, которые помогут в процессе миграции.

- **Поддерживает общедоступные папки почты и календаря**. Скопированные сообщения электронной почты и записи будут отображаться в разделе Группы как групповые беседы, а скопированные элементы календаря будут отображаться в календарях групп. Для других типов общедоступных папок, например с задачами и контактами, в настоящее время не поддерживается такая миграция.

- **Локальные общедоступные папки можно перенести непосредственно в Группы Microsoft 365**. Для этой миграции не требуется сначала переместить общедоступные папки в Microsoft 365 или Office 365, а затем перейти в группы. Командлеты копирования данных MRS считывают данные

общедоступных папок непосредственно из локальной среды, а затем копируют данные в Группы Microsoft 365. Для общедоступных папок Exchange потребуется конечная точка на основе прокси-сервера MRS.

- **Миграция "все или ничего" не** выполняется. Вы можете выбрать определенные общедоступные папки для миграции в группы, и только выбранные общедоступные папки будут перенесены.

- **Одноразовое копирование данных**. Пакетная миграция предназначена для одноразового копирования данных из исходных общедоступных папок в целевые группы без сложностей добавочной синхронизации и завершения.

- **Объединяет данные общедоступных папок с существующими данными в группе**. Копия данных объединяет содержимое общедоступной папки с содержимым существующей группы, если таковое имеется. Если требуется добавочное копирование данных, можно выполнить копирование данных столько раз, сколько потребуется для копирования добавочных данных в группу.

Обзор пакетной миграции

Ниже описан общий процесс переноса содержимого общедоступных папок в Группы Microsoft 365 при пакетной миграции.

1. **Выбор исходного объекта:** выберите общедоступные папки, которые требуется перенести. Вы можете выбрать любую папку, содержащую почту или календарь.

2. **Создание целевого объекта:** создайте для папок соответствующие группы с нужными настройками (например, с заданными членами групп, параметрами конфиденциальности и классификации данных).

3. **Копирование данных:** скопируйте данные из общедоступных папок в "Группы Office 365" с помощью командлетов пакетной миграции.

4. **Блокировка источника**. Блокировка общедоступных папок после проверки данных в группах.

5. **Прямая передача**: скопируйте все новые данные, созданные между шагами 3 и 4.

Ваши общедоступные папки и соответствующие им группы останутся в сети для пользователей во время действий **Выбор источника** и **Копирование данных** . После шага **Копирования данных** вы можете оценить, следует ли продолжить

оставшуюся часть миграции, на основе интерфейса групп и подходит ли она вашим пользователям и вашей организации. На этом этапе вы можете откатить миграцию и вернуться к использованию общедоступных папок. Если вы продолжите миграцию, после завершения этапа **перехода** вы можете удалить исходные общедоступные папки. Даже после миграции можно выполнить откат к общедоступным папкам, если вы сохранили файлы резервных копий в процессе миграции и не удалили исходные общедоступные папки.

Необходимые условия и пошаговые инструкции по пакетной миграции

Ниже перечислены необходимые условия для пакетной миграции в среде Exchange. Конкретные требования зависят от используемой в данный момент версии Exchange.

1. Если общедоступные папки находятся в локальной среде, то серверы должны работать под управлением одной из следующих версий:

    - Exchange 2010 с пакетом обновления 3 (SP3) и накопительным пакетом обновления 8 (RU8) или более поздней версии;
    - Exchange 2013 CU15 или более поздней версии
    - Exchange 2016 с накопительным пакетом обновления 4 (CU4) или более поздней версии.
    - Exchange 2019

2. Если общедоступные папки находятся в локальной среде, должна быть настроена гибридная среда Exchange. Дополнительные сведения см. в разделе Exchange Server гибридных развертываний.

Инструкции по миграции

Щелкните одну из следующих ссылок, чтобы пошаговые инструкции по выполнению пакетной миграции.

- Использование пакетной миграции для переноса общедоступных папок Exchange Online в Группы Microsoft 365
- Использование пакетной миграции для переноса общедоступных папок Exchange 2013 в Группы Microsoft 365

- Использование пакетной миграции для переноса общедоступных папок Exchange 2010 в Группы Microsoft 365

Процедуры общедоступных папок в Microsoft Exchange

Статья • 04.04.2023

Воспользуйтесь приведенными ниже процедурами, чтобы подготовить инфраструктуру общедоступных папок, а также выполнить другие необходимые действия по управлению ими.

Настройка общедоступных папок в новой организации

Настройка локальных общедоступных папок прежних версий для гибридного развертывания

Настройка современных локальных общедоступных папок для гибридного развертывания

Использование пакетной миграции для переноса общедоступных папок Exchange 2010 в Exchange 2016

Использование пакетной миграции для переноса устаревших общедоступных папок в Microsoft 365 или Office 365 и Exchange Online

Использование пакетного переноса для переноса общедоступных папок Exchange Server в Exchange Online

Перенос общедоступных папок из Exchange 2013 в Exchange 2016 или Exchange 2019

Configure legacy public folders where user mailboxes are on Exchange 2016 servers

Создание почтового ящика общедоступных папок

Создание общедоступной папки

Using favorite public folders in Outlook on the web

Включение и отключение поддержки почты для общедоступной папки

Update the public folder hierarchy

Remove a public folder

Move a public folder mailbox to a different mailbox database

Move a public folder to a different public folder mailbox

Restore public folders and public folder mailboxes from failed moves

Просмотр статистики для общих папок и элементов общедоступной папки

Настройка устаревших локальных общедоступных папок для гибридного развертывания Exchange Server

Статья • 04.04.2023

В гибридном развертывании пользователи могут находиться в Exchange Online, локальной среде Exchange или в обеих средах, а общедоступные папки находятся в Exchange Online или локальной среде Exchange. Общедоступные папки могут находиться только в одном расположении, поэтому нужно решить, где именно: в Exchange Online или на локальном сервере. Они не могут находиться в обоих расположениях. Почтовые ящики общедоступных папок синхронизируются с Exchange Online при помощи службы синхронизации каталогов. Однако общедоступные папки с поддержкой почты не синхронизируются между локальными и облачными организациями.

В этой статье описывается синхронизация общедоступных папок с поддержкой почты, если пользователи находятся в Microsoft 365 или Office 365, а общедоступные папки Exchange 2010 с пакетом обновления 3 (SP3) или более поздней версии являются локальными. Однако пользователь Microsoft 365 или Office 365, который не представлен локальным объектом MailUser (локальным для целевой иерархии общедоступных папок), не сможет получить доступ к устаревшим или локальным общедоступным папкам Exchange.

> ⓘ **Примечание**
>
> В этом разделе серверы Exchange 2010 с пакетом обновления 3 (SP3) или более поздних версий называются *устаревшими серверами Exchange Server*.

Для синхронизации общедоступных папок с поддержкой почты будут использоваться следующие скрипты. Скрипты инициируются задачей Windows, которая выполняется в локальной среде:

- `Sync-MailPublicFolders.ps1`: этот скрипт синхронизирует объекты общедоступных папок с поддержкой почты из локального развертывания Exchange с Microsoft 365 или Office 365. Он использует локальное развертывание Exchange в качестве главного, чтобы определить, какие изменения необходимо применить к Microsoft 365 или Office 365. Скрипт

создает, обновляет или удаляет объекты общедоступных папок с поддержкой почты в Microsoft 365 или Office 365 Active Directory в зависимости от того, что существует в локальном развертывании Exchange.

- `SyncMailPublicFolders.strings.psd1`: это файл поддержки, используемый предыдущим скриптом синхронизации и должен быть скопирован в то же расположение, что и предыдущий скрипт.

После выполнения этой процедуры локальные пользователи и пользователи Microsoft 365 или Office 365 смогут получить доступ к одной и той же локальной инфраструктуре общедоступных папок.

Какие гибридные версии Exchange будут работать с общедоступными папками?

В следующей таблице описаны поддерживаемые сочетания версий и расположения почтовых ящиков пользователей и общедоступных папок. "Гибридное неприменимое" по-прежнему поддерживается, но не считается гибридным сценарием, так как общедоступные папки и пользователи находятся в одном расположении.

Сценарий	**Локальный почтовый ящик пользователя Exchange 2010**	**Локальный почтовый ящик пользователя Exchange 2016/2019**	**Почтовый ящик пользователей Exchange Online**
Локальные общедоступные папки Exchange 2010	Гибридная конфигурация не применяется	Гибридная конфигурация не применяется	Поддерживается
Локальные общедоступные папки Exchange 2013, Exchange 2016 или Exchange 2019	Гибридная конфигурация не применяется	Гибридная конфигурация не применяется	Поддерживается
Общедоступные папки Exchange Online	Не поддерживается	Поддерживается	Гибридная конфигурация не применяется

Гибридная конфигурация с общедоступными папками Exchange 2003 не поддерживается. Если вы используете Exchange 2003 в своей организации, необходимо переместить все базы данных и реплики общедоступных папок в

Exchange 2010 с пакетом обновления 3 (SP3) или более поздней версии. В Exchange 2003 не должно остаться ни одной реплики общедоступных папок.

Этап 1. Что нужно знать перед началом работы

- В этих инструкциях предполагается, что вы использовали мастер гибридной конфигурации для настройки и синхронизации локальных и Exchange Online сред, а записи DNS, используемые для автообнаружения большинства пользователей, ссылаются на локальную конечную точку. Подробнее см. в разделе Hybrid Configuration Wizard.

- В этих инструкциях предполагается, что на локальных серверах Exchange server прежних версий включен и работает мобильный Outlook. Сведения о включении мобильного Outlook см. в разделе Outlook Anywhere.

- Реализация устаревшего сосуществования общедоступных папок для гибридного развертывания Exchange с Microsoft 365 или Office 365 может потребовать устранения конфликтов во время процедуры импорта. Конфликты могут возникать из-за не-маршрутизируемых адресов электронной почты, назначенных общедоступным папкам с поддержкой почты, конфликтов с другими пользователями и группами в Microsoft 365 или Office 365, а также из-за других атрибутов.

- Эти инструкции предполагают, что ваша организация Exchange Online была обновлена до версии, поддерживающей общедоступные папки.

- В Exchange Online вам необходимо быть членом группы ролей "Управление организацией". Эта группа ролей отличается от разрешений, которые назначаются при подписке на Exchange Online. Дополнительные сведения о том, как включить группу ролей Управление организацией, см. в разделе Управление группами ролей.

- В Exchange 2010 необходимо быть членом групп ролей контроль доступа (RBAC) управления организацией или сервером. Дополнительные сведения см. в разделе Добавление участников в группу ролей.

- Чтобы получить доступ к общедоступным папкам в локальной среде, пользователи должны обновить свои клиенты Outlook до общедоступного обновления Outlook за ноябрь 2012 г. или более поздней версии.

    - Чтобы скачать обновление за ноябрь 2012 г. для Outlook 2010, см. статью с обновлением для 32-разрядного выпуска Microsoft Outlook 2010 (KB2687623) .
    - Чтобы скачать обновление Outlook за ноябрь 2012 г. для Outlook 2007, см. статью Обновление для Microsoft Office Outlook 2007 (KB2687404) и скачать на предпочитаемом языке.
- Outlook 2016 для Mac и Outlook для Mac для Microsoft 365 или Office 365 поддерживаются для общедоступных папок, если выполняются следующие условия:
    - Установлено обновление за апрель 2016 г. для Outlook 2016 для Mac.
    - Exchange 2016 с накопительным пакетом обновления 2 (CU2) или более поздней версии.
    - Exchange 2013 с накопительным пакетом обновления 14 (CU14) или более поздней версии.
- После настройки локальных общедоступных папок для гибридного развертывания согласно инструкциям в этой статье внешние пользователи не смогут отправлять сообщения в ваши локальные общедоступные папки, если вы не выполните дополнительные действия. Вы можете задать для обслуживаемого домена общедоступных папок значение Internal Relay (дополнительные сведения см. в разделе Управление принятыми доменами в Exchange Online) или отключить блокировку пограничных адресов на основе каталогов (DBEB), как описано в статье Об отказе от сообщений, отправляемых недопустимым получателям, на основе каталога.
- В гибридном режиме пользователи Exchange Online не могут получить доступ к общедоступным папкам с помощью Outlook в Интернете (прежнее название — Outlook Web App).

Этап 2. Сделайте удаленные общедоступные папки обнаруживаемыми

1. Если общедоступные папки находятся на серверах Exchange 2010, необходимо установить службы клиентского доступа на всех серверах почтовых ящиков с базой данных общедоступных папок. Это позволяет запускать службу Exchange RpcClientAccess, которая позволяет всем клиентам получать доступ к

общедоступным папкам. Дополнительные сведения см. в статье Установка Exchange Server 2010.

> ⓘ **Примечание**
>
> Этот сервер не обязательно должен быть частью балансировки нагрузки клиентского доступа. Дополнительные сведения см. **в статье Общие сведения о балансировке нагрузки в Exchange 2010**.

2. Создайте пустую базу данных почтовых ящиков на каждом сервере общедоступных папок.

   Для Exchange 2010 выполните следующую команду в командной консоли Exchange. Эта команда исключает базу данных почтовых ящиков из подсистемы балансировки нагрузки подготовки почтовых ящиков. Это предотвратит автоматическое добавление новых почтовых ящиков в эту базу данных.

   PowerShell

   ```
   New-MailboxDatabase -Server <PFServerName_with_CASRole> -Name
   <NewMDBforPFs> -IsExcludedFromProvisioning $true
   ```

   Для Exchange 2007 выполните следующую команду в командной консоли Exchange:

   PowerShell

   ```
   New-MailboxDatabase -StorageGroup "<PFServerName>\StorageGroup>" -Name
   <NewMDBforPFs>
   ```

   > ⓘ **Примечание**
   >
   > Рекомендуется добавить в эту базу данных только прокси-почтовый ящик, который вы создадите на следующем шаге. В этой базе данных почтовых ящиков не нужно добавлять никакие другие почтовые ящики.

3. Создайте прокси-почтовый ящик в новой базе данных почтовых ящиков и скройте его из адресной книги. Smtp этого почтового ящика будет возвращен автообнаружителем в качестве *SMTP-сервера DefaultPublicFolderMailbox* ,

чтобы, разрешая этот SMTP, клиент может получить доступ к устаревшим серверам Exchange для доступа к общедоступным папкам.

```
PowerShell

New-Mailbox -Name <PFMailbox1> -Database <NewMDBforPFs>
```

```
PowerShell

Set-Mailbox -Identity <PFMailbox1> -HiddenFromAddressListsEnabled $true
```

4. В Exchange 2010 включите функцию автообнаружения, чтобы вернуть почтовые ящики общедоступных папок прокси-сервера.

```
PowerShell

Set-MailboxDatabase <NewMDBforPFs> -RPCClientAccessServer
<PFServerName_with_CASRole>
```

5. Повторите предыдущие действия для каждого сервера общедоступных папок в своей организации.

Шаг 3. Скачайте сценарии

1. На странице Общедоступные папки с поддержкой почты: скрипт для синхронизации каталога скачайте следующие файлы:

   - `Sync-MailPublicFolders.ps1`
   - `SyncMailPublicFolders.strings.psd1`

2. Сохраните файлы на локальном компьютере, с которого вы планируете запустить PowerShell. Например, в папку C:\PFScripts.

Этап 4. Настройте синхронизацию службы каталогов

Служба синхронизации каталогов не синхронизирует общедоступные папки с поддержкой почты. Запустив следующий сценарий, можно синхронизировать общедоступные папки, поддерживающие почту, на различных площадках. Для общедоступных папок, поддерживающих почту, необходимо повторно создать

специальные разрешения в облаке, так как в сценариях гибридного развертывания не поддерживаются разрешения для нескольких площадок.

> ⓘ **Примечание**
>
> Синхронизированные общедоступные папки с поддержкой почты будут отображаться в качестве объектов контактов почты в целях потока обработки почты и не будут доступны для просмотра в Центре администрирования Exchange. См. команду Get-MailPublicFolder. Чтобы повторно создать разрешения SendAs в облаке, используйте команду Add-RecipientPermission.

1. На сервере Exchange Server устаревшей версии выполните следующую команду, чтобы синхронизировать общедоступные папки с поддержкой почты из локальной локальная служба Active Directory в Microsoft 365 или Office 365.

   PowerShell

   ```
   Sync-MailPublicFolders.ps1 -Credential (Get-Credential) -
   CsvSummaryFile:sync_summary.csv
   ```

   Где `Credential` — это ваше имя и пароль Microsoft 365 или Office 365, а `CsvSummaryFile` также путь к тому, куда нужно регистрировать операции и ошибки синхронизации в .csv формате.

> ⓘ **Примечание**
>
> Перед выполнением скрипта рекомендуется сначала имитировать действия, которые скрипт будет выполнять в вашей среде, выполнив его, как описано выше, с параметром `-WhatIf` . Рекомендуем также запускать этот сценарий ежедневно, чтобы синхронизировать общедоступные папки, поддерживающие почту.

Этап 5. Настройте для пользователей Exchange Online доступ к локальным общедоступным папкам

Конечный этап этой процедуры — настройка организации Exchange Online и разрешение доступа к локальным общедоступным папкам прежних версий.

Вы укажете все почтовые ящики общедоступных папок прокси-сервера, созданные на шаге 2. Сделайте удаленные общедоступные папки доступными для обнаружения , чтобы организацияExchange Online могла получить доступ к локальным общедоступным папкам.

Выполните следующую команду в Exchange Online PowerShell. Сведения о том, как с помощью Windows PowerShell подключаться к Exchange Online, см. в статье Подключение к Exchange Online PowerShell.

PowerShell

```
Set-OrganizationConfig -PublicFoldersEnabled Remote -
RemotePublicFolderMailboxes PFMailbox1,PFMailbox2,PFMailbox3
```

Чтобы увидеть изменения, необходимо подождать, пока не завершится синхронизация Active Directory. Это может занять до трех часов. Если вы не хотите ждать повторяющихся синхронизаций, которые происходят каждые три часа, вы можете в любое время принудительно выполнить синхронизацию каталогов. Подробные инструкции по принудительной синхронизации каталогов см. в разделе Синхронизация Azure AD Connect: Планировщик. Microsoft 365 или Office 365 случайным образом выбирает один из почтовых ящиков общедоступных папок, указанных в этой команде.

> ⓘ **Важно!**
>
> Пользователь Microsoft 365 или Office 365, который не представлен локальным объектом MailUser (локальным для целевой иерархии общедоступных папок), не сможет получить доступ к общедоступным папкам прежних версий, Exchange 2016 или Exchange 2019. См. статью базы знаний **Exchange Online пользователи не могут получить доступ к устаревшим локальным общедоступным папкам** для решения.

Как проверить, что это работает

Войдите в Outlook для пользователя, который находится в Exchange Online, и выполните следующие проверки общедоступных папок.

- Просмотр иерархии.
- Проверка разрешений.
- Создание и удаление общедоступных папок.

- Опубликуйте содержимое в общедоступной папке и удалите его.

Использование пакетного переноса для переноса общедоступных папок Exchange Server в Exchange Online

Статья • 04.04.2023

Область применения: Exchange Server 2013 г., **Exchange Server 2016** г. и **Exchange Server 2019** г.

> ⓘ **Примечание**
>
> Собственный метод миграции поддерживает не более 100 целевых почтовых ящиков общедоступных папок в Exchange Online (хотя после миграции можно создать до 1000 почтовых ящиков), при этом каждый почтовый ящик общедоступных папок максимальной емкостью 100 ГБ. 5 ТБ — это максимальный рекомендуемый размер, который можно перенести в Exchange Online. Согласно нашим рекомендациям по заполнению каждого целевого почтового ящика общедоступных папок до 50 % емкости.

> ⓘ **Примечание**
>
> В этой статье перечислены шаги по переносу общедоступных папок из локальной среды в Exchange Online. Обратите внимание, что нет собственных средств для миграции и перемещения общедоступных папок из Exchange Online в локальную среду Exchange.

Для миграции общедоступных папок Exchange Server в Exchange Online требуется Exchange Server 2013 CU15 или более поздней версии или Exchange Server 2016 с накопительным пакетом обновления 4 (CU4) или более поздней версии в локальной среде. Все версии Exchange Server 2019 поддерживаются для пакетной миграции общедоступных папок.

Если в вашей организации используется смешанная среда с общедоступными папками Exchange 2013 и Exchange 2016/2019 и вы хотите переместить их все в Exchange Online, инструкции в этой статье будут работать для вас при условии, что на серверах Exchange 2013 установлены накопительные обновления 15 или более поздней версии.

Инструкции по переносу общедоступных папок Exchange Server 2010 в Exchange Online см. в статье Использование пакетной миграции для переноса устаревших общедоступных папок в Exchange Online.

Что нужно знать перед началом работы

- Мы настоятельно рекомендуем ознакомиться с часто задаваемыми вопросами: Общедоступные папки , прежде чем пытаться выполнить миграцию.

- При обновлении до Exchange Server 2013 CU15 или более поздней версии либо до Exchange Server 2016 с накопительным пакетом обновления 4 (CU4) или более поздней версии необходимо также подготовить Active Directory, в противном случае миграция общедоступных папок завершится сбоем. Такая подготовка Active Directory гарантирует, что все соответствующие командлеты и параметры PowerShell будут доступны для подготовки к миграции и ее запуска. Дополнительные сведения см. в разделе Подготовка Active Directory и доменов .

- В Exchange Online вам необходимо быть членом группы ролей Organization Management. Эта группа ролей отличается от разрешений, назначенных вам при подписке на Microsoft 365, Office 365 или Exchange Online. Дополнительные сведения о включении группы ролей "Управление организацией" см. в разделе Управление группами ролей.

- В Exchange Server необходимо быть членом групп ролей RBAC "Управление организацией" или "Управление сервером". Дополнительные сведения см. в разделе Добавление участников в группу ролей.

- Если в организации есть общедоступные папки, размер которых превышает 25 ГБ, перед началом миграции рекомендуем удалить из них содержимое, чтобы сделать их меньше, или разделить их на несколько меньших общедоступных папок. Ограничение в 25 ГБ, приведенное здесь, применяется только к общедоступной папке, а не к дочерним или вложенным папкам, которые могут иметься в соответствующей папке. Если ни один их этих вариантов невозможен, рекомендуем не перемещать общедоступные папки в Exchange Online. Дополнительные сведения см. в разделе Ограничения Exchange Online.

  > ⓘ **Примечание**

> Если текущие квоты общедоступных папок в Exchange Online меньше 25 ГБ, можно использовать командлет Set-OrganizationConfig, чтобы увеличить их с помощью параметров DefaultPublicFolderIssueWarningQuota и DefaultPublicFolderProhibitPostQuota.

- В Microsoft 365, Office 365 и Exchange Online можно создать не более 1000 почтовых ящиков общедоступных папок. Однако для миграции из Exchange Server поддерживается не более 100 почтовых ящиков общедоступных папок.

- Если вы планируете перенести пользователей в Microsoft 365 или Office 365, необходимо завершить миграцию пользователей перед переносом общедоступных папок. Дополнительные сведения см. в статье Способы переноса нескольких учетных записей электронной почты в Microsoft 365 или Office 365.

- Прокси-сервер MRS должен быть включен по крайней мере на одном сервере Exchange, на котором также размещаются почтовые ящики общедоступных папок. Дополнительные сведения см . в разделе Включение конечной точки прокси-сервера MRS для удаленных перемещений .

- Для выполнения процедур миграции, описанных в этой статье, нельзя использовать Центр администрирования Exchange (EAC). Вместо этого необходимо использовать командную консоль Exchange на серверах Exchange. В Exchange Online необходимо использовать Exchange Online PowerShell. Дополнительные сведения см. в статье Connect to Exchange Online PowerShell.

- Чтобы запустить скрипты миграции, приведенные в этой статье, необходимо использовать учетную запись с включенной обычной проверкой подлинности. Учетные записи, использующие многофакторную проверку подлинности (MFA), в настоящее время не поддерживаются.

- Поддерживается пропуск переноса удаленных элементов и удаленных папок из Exchange Server в Exchange Online. Дополнительные сведения см. в записи блога команды Exchange о переносе современных общедоступных папок без данных мусора.

- Для переноса всех данных общедоступных папок необходимо использовать один пакет миграции. Exchange позволяет создать только один пакет миграции для миграции общедоступных папок. При попытке создать несколько пакетов миграции общедоступных папок одновременно,

результатом будет ошибка. Кроме того, обратите внимание, что после того как пакет миграции будет иметь состояние "Завершено", данные больше не могут быть скопированы из исходной среды.

- Не рекомендуется использовать функцию экспорта PST в Outlook для переноса общедоступных папок в Microsoft 365, Office 365 или Exchange Online. Увеличение размера почтового ящика общедоступных папок в Exchange Online управляется с помощью функции автоматического разделения, которая разделяет почтовый ящик общедоступных папок при превышении квот на размер. Автоматическое разделение не может справиться с внезапным ростом почтовых ящиков общедоступных папок при использовании экспорта PST для переноса общедоступных папок. Возможно, вам придется ждать до двух недель автоматического разделения, чтобы переместить данные из основного почтового ящика. Вместо этого рекомендуется использовать инструкции на основе командлетов, описанные в этой статье, для переноса общедоступных папок. Если вы по-прежнему решили перенести общедоступные папки с помощью экспорта PST, см. раздел Перенос общедоступных папок в Office 365 с помощью экспорта PST в Outlook далее в этой статье.

- Убедитесь, что defaultPublicFolderAgeLimit настроен на уровне организации (`Get-OrganizationConfig | Format-List DefaultPublicFolderAgeLimit`) или для отдельных общедоступных папок настроен параметр AgeLimit (`Get-PublicFolder <FolderPath> | Format-List AgeLimit`), чтобы предотвратить автоматическое удаление содержимого.

- Прежде чем начать, ознакомьтесь с этой статьей полностью. Для некоторых действий требуется простой. Во время этого простоя общедоступные папки не будут доступны никому. Также просмотрите список известных проблем. Кроме того, ознакомьтесь с рекомендациями по переносу общедоступных папок, чтобы спланировать миграцию.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server** или **Exchange Online**.

Шаг 1. Скачивание сценариев миграции

1. Скачайте все скрипты и вспомогательные файлы из общедоступных папок Exchange 2013/2016/2019 и Exchange 2010/2013/2016/EXO общедоступных папок в Microsoft 365 или Office 365 скрипты перед миграцией.

2. Сохраните эти сценарии на локальном компьютере, с которого вы собираетесь запускать оболочку PowerShell. (Например, в папку C:\PFScripts). Убедитесь, что все сценарии сохранены в одном и том же месте.

   Описание сценариев и файлов:

   - `SourceSideValidations.ps1`: скрипт проверки на стороне источника сканирует общедоступные папки в источнике и сообщает об обнаруженных проблемах вместе с действиями, необходимыми для устранения проблем. Этот скрипт будет выполняться на локальном сервере Exchange Server.

   - `Sync-ModernMailPublicFolders.ps1`Этот скрипт синхронизирует объекты общедоступных папок с поддержкой почты между локальной средой Exchange и Microsoft 365 или Office 365. Этот скрипт будет выполняться на локальном сервере Exchange Server.

   - `SyncModernMailPublicFolders.strings.psd1`. Этот вспомогательный файл используется сценарием Sync-ModernMailPublicFolders.ps1, их необходимо скачать в одну папку.

   - `Export-ModernPublicFolderStatistics.ps1` Этот скрипт создает файл сопоставления имени папки с размером папки и размером удаленного элемента. Этот скрипт будет выполняться на локальном сервере Exchange Server.

   - `Export-ModernPublicFolderStatistics.strings.psd1`. Этот вспомогательный файл используется сценарием Export-ModernPublicFolderStatistics.ps1, поэтому их необходимо скачать в одну папку.

   - `ModernPublicFolderToMailboxMapGenerator.ps1` Этот скрипт создает файл сопоставления общедоступных папок с почтовым ящиком, используя выходные данные скрипта Export-ModernPublicFolderStatistics.ps1. Этот скрипт будет выполняться на локальном сервере Exchange Server.

   - `ModernPublicFolderToMailboxMapGenerator.strings.psd1`. Этот вспомогательный файл используется сценарием ModernPublicFolderToMailboxMapGenerator.ps1, поэтому их необходимо скачать в одну папку.

- `SetMailPublicFolderExternalAddress.ps1`Этот скрипт обновляет `ExternalEmailAddress` общедоступные папки с поддержкой почты в локальной среде до Exchange Online коллег, чтобы сообщения электронной почты, адресованные общедоступным папкам с поддержкой почты после миграции, правильно перенаправляются в Exchange Online. Этот скрипт необходимо запустить на локальном сервере Exchange Server.

- `SetMailPublicFolderExternalAddress.strings.psd1`. Этот файл поддержки используется сценарием Create-PublicFolderMailboxesForMigration.ps1 и должен быть скачан в то же расположение.

Шаг 2. Подготовьте организацию к миграции

> **Примечание**
>
> Настоятельно рекомендуется запустить скрипт **проверки на стороне источника** с локального сервера почтовых ящиков Exchange. Скрипт будет проверять и сообщать о проблемах, которые, как известно, приводят к медленной миграции, а также рекомендации по устранению этих проблем. Скрипт выполнит все указанные ниже предварительные требования.

Перед переносом общедоступных папок выполните все необходимые действия, описанные в разделах ниже.

Общие предварительные условия

Для успешной миграции сделайте следующее:

- Убедитесь, что в Active Directory отсутствуют потерянные объекты почты общедоступных папок. Это объекты в Active Directory без соответствующего объекта Exchange.

- Убедитесь, что адреса электронной почты SMTP, настроенные для общедоступных папок в Active Directory, совпадают с адресами электронной почты SMTP в объектах Exchange.

- Убедитесь, что в Active Directory нет повторяющихся объектов общедоступных папок. Это необходимо, чтобы избежать наличия двух или более объектов Active Directory, указывающих на одну и ту же общедоступную папку с поддержкой почты.

Необходимые действия в локальной среде сервера Exchange 2013, Exchange 2016 или Exchange 2019

В командной консоли Exchange (локальная среда) сделайте следующее:

1. После завершения миграции кэши DNS через Интернет могут направлять сообщения в общедоступные папки с поддержкой почты в новом расположении в Exchange Online. Чтобы перенесенные общедоступные папки, поддерживающие почту, получали сообщения в течение этого переходного периода, создайте обслуживаемый домен с известным именем. Для этого выполните приведенную ниже команду в локальной среде Exchange. В этом примере `target domain` — это домен Microsoft 365, Office 365 или Exchange Online, для которого мастер гибридной конфигурации уже настроил соединитель отправки.

   PowerShell

   ```
   New-AcceptedDomain -Name
   PublicFolderDestination_78c0b207_5ad2_4fee_8cb9_f373175b3f99 -
   DomainName <target domain> -DomainType InternalRelay
   ```

   Пример.

   PowerShell

   ```
   New-AcceptedDomain -Name
   PublicFolderDestination_78c0b207_5ad2_4fee_8cb9_f373175b3f99 -
   DomainName "contoso.mail.onmicrosoft.com" -DomainType InternalRelay
   ```

   Если принятый домен уже существует в локальной среде, переименуйте его `PublicFolderDestination_78c0b207_5ad2_4fee_8cb9_f373175b3f99` в и оставьте остальные атрибуты без изменений.

   Чтобы проверка, если принятый домен уже присутствует в локальной среде, выполните следующую команду:

   PowerShell

   ```
   Get-AcceptedDomain | Where {$_.DomainName -eq "<target domain>"}
   ```

   Чтобы переименовать принятый домен `PublicFolderDestination_78c0b207_5ad2_4fee_8cb9_f373175b3f99` в , выполните следующую команду:

PowerShell

```
Get-AcceptedDomain | Where {$_.DomainName -eq "<target domain>"} | Set-AcceptedDomain -Name
PublicFolderDestination_78c0b207_5ad2_4fee_8cb9_f373175b3f99
```

> **Примечание**
>
> Если поддерживающие почту общедоступные папки в Exchange Online должны получать внешние письма из Интернета, необходимо отключить DBEB в Exchange Online и Exchange Online Protection (EOP). Дополнительные сведения см. в статье Use Directory Based Edge Blocking to Reject Messages Sent to Invalid Recipients.

2. Если имя общедоступной папки содержит обратную косую черту **** или косую черту **/**, она может не быть перенесена в назначенный почтовый ящик во время процесса миграции. Перед миграцией переименуйте все такие папки, чтобы удалить эти символы.

   А. Чтобы найти общедоступные папки с обратной косой чертой в имени, выполните следующую команду:

   PowerShell

   ```
   Get-PublicFolder -Recurse -ResultSize Unlimited | Where {$_.Name -like "*\*" -or $_.Name -like "*/*"} | Format-List Name, Identity, EntryId
   ```

   Б. Если эта команда возвращает сведения об общедоступных папках, переименуйте их с помощью такой команды:

   PowerShell

   ```
   Set-PublicFolder -Identity "<public folder EntryId>" -Name "<new public folder name>"
   ```

3. (Этот шаг требуется только в том случае, если по какой-либо причине вы выполняете предыдущую попытку миграции. Если это не так, перейдите к следующему шагу.) Выполните следующие командлеты, чтобы убедиться, что в вашей организации нет записи об успешной миграции. Если это так, необходимо задать для этого значения значение `$false`.

Прежде чем изменять значения, убедитесь, что предыдущую миграцию можно не учитывать, чтобы случайно не выполнить вторую миграцию.

А. Выполните следующую команду, чтобы проверить наличие предыдущих миграций и их состояния:

```
PowerShell

Get-OrganizationConfig | Format-List
PublicFolderMailboxesLockedForNewConnections,
PublicFolderMailboxesMigrationComplete
```

Б. Если какое-либо из указанных выше значений возвращается со значением `$true`, сделайте их `$false` , выполнив следующую команду:

```
PowerShell

Set-OrganizationConfig -
PublicFolderMailboxesLockedForNewConnections:$false -
PublicFolderMailboxesMigrationComplete:$false
```

4. Чтобы проверить успешность миграции после ее завершения, рекомендуется выполнить следующие команды на всех соответствующих серверах Exchange 2016 или Exchange 2019. Они сделают моментальные снимки текущего развертывания общедоступных папок, которые позднее можно будет сравнить с перенесенными общедоступными папками.

> ⓘ **Примечание**
>
> В зависимости от размера организации Exchange это может занять некоторое время.

   - Выполните следующую команду, чтобы сделать моментальный снимок начальной структуры исходных папок.

     ```
     PowerShell

     Get-PublicFolder -Recurse -ResultSize Unlimited | Export-CliXML
     OnPrem_PFStructure.xml
     ```

   - Выполните следующую команду, чтобы сделать моментальный снимок статистики общедоступных папок, такой как число элементов, размер и владелец.

```
PowerShell

Get-PublicFolderStatistics -ResultSize Unlimited | Export-CliXML
OnPrem_PFStatistics.xml
```

- Выполните команду ниже, чтобы сделать моментальный снимок разрешений общедоступных папок.

```
PowerShell

Get-PublicFolder -Recurse -ResultSize Unlimited | Get-
PublicFolderClientPermission | Select-Object
Identity,User,AccessRights -ExpandProperty AccessRights | Export-
CliXML OnPrem_PFPerms.xml
```

- Выполните следующую команду, чтобы сделать моментальный снимок общедоступных папок, поддерживающих почту:

```
PowerShell

Get-MailPublicFolder -ResultSize Unlimited | Export-CliXML
OnPrem_MEPF.xml
```

- Сохраните файлы, созданные предыдущими командами, в надежном месте, чтобы выполнить сравнение в конце миграции.

5. Если вы используете Microsoft Entra Connect (Microsoft Entra Connect) для синхронизации локальных каталогов с Microsoft Entra ID, необходимо выполнить следующие действия (если вы не используете Microsoft Entra Connect, этот шаг можно пропустить):

   a. На локальном компьютере откройте Microsoft Entra Подключить, а затем выберите **Настроить**.

   b. На экране **Дополнительные задачи** выберите **Настроить параметры синхронизации** и нажмите кнопку **Далее**.

   c. На экране **Подключение к Microsoft Entra ID** введите соответствующие учетные данные и нажмите кнопку **Далее**. После подключения нажимайте кнопку **Далее** , пока не перейдете на экран **Дополнительные компоненты** .

   d. Убедитесь, что **общедоступные папки почты Exchange** не выбраны. Если он не выбран, можно перейти к следующему разделу *Предварительные*

действия в Exchange Online. Если он выбран, щелкните, чтобы очистить поле проверка, а затем нажмите кнопку **Далее**.

> ⓘ **Примечание**
>
> Если вы не видите **общедоступные папки Почты Exchange** в качестве параметра на экране **Необязательные компоненты**, вы можете выйти из Microsoft Entra Connect и перейти к следующему разделу Предварительные *требования в Exchange Online*.

e. После того как вы снимите флажок **Общедоступные папки почты Exchange** , нажимайте кнопку **Далее** , пока не перейдете на экран **Готово к настройке** , а затем нажмите кнопку **Настроить**.

Необходимые действия в Exchange Online

В Exchange Online PowerShell выполните следующие действия.

1. Убедитесь, что отсутствуют запросы на перенос общедоступных папок. Если они есть, очистите их, иначе выполнить ваш запрос не удастся. Это необходимо, только если вы считаете, что в конвейере уже есть запрос на миграцию (который не удалось выполнить или который вы хотите прервать).

   В следующем примере показано, как найти существующие запросы на пакетную миграцию:

   ```
   PowerShell
   Get-MigrationBatch | ?{$_.MigrationType.ToString() -eq "PublicFolder"}
   ```

   В следующем примере показано, как удалить существующие запросы на пакетную миграцию общедоступных папок:

   ```
   PowerShell
   Remove-MigrationBatch <name of migration batch> -Confirm:$false
   ```

2. Убедитесь, что в Exchange Online нет общедоступных папок или почтовых ящиков общедоступных папок. Если вы обнаружите общедоступные папки в Exchange Online после выполнения приведенных ниже действий, важно определить, почему они там и кто в вашей организации запустил иерархию

общедоступных папок, прежде чем приступать к удалению всех общедоступных папок и почтовых ящиков общедоступных папок.

A. В Exchange Online PowerShell выполните следующую команду, чтобы узнать, существуют ли почтовые ящики общедоступных папок:

```
PowerShell

Get-Mailbox -PublicFolder
```

Б. Если команда не возвращает почтовые ящики общедоступных папок, перейдите к шагу 3 Шаг 3. Создание CSV-файлов. В противном случае выполните следующую команду, чтобы проверить наличие общедоступных папок:

```
PowerShell

Get-PublicFolder -Recurse
```

3. Если у вас есть какие-либо общедоступные папки в Microsoft 365, Office 365 или Exchange Online, выполните следующую команду PowerShell, чтобы удалить их (убедившись, что они не нужны). Убедитесь, что вы сохранили всю нужную информацию, потому что при удалении общедоступных папок она будет навсегда потеряна.

```
PowerShell

Get-MailPublicFolder -ResultSize Unlimited | where {$_.EntryId -ne
$null}| Disable-MailPublicFolder -Confirm:$false
Get-PublicFolder -GetChildren \ -ResultSize Unlimited | Remove-
PublicFolder -Recurse -Confirm:$false
```

4. После удаления общедоступных папок выполните следующие команды, чтобы удалить все почтовые ящики общедоступных папок:

```
PowerShell

$hierarchyMailboxGuid = $(Get-
OrganizationConfig).RootPublicFolderMailbox.HierarchyMailboxGuid
Get-Mailbox -PublicFolder | Where-Object {$_.ExchangeGuid -ne
$hierarchyMailboxGuid} | Remove-Mailbox -PublicFolder -Confirm:$false -
Force
Get-Mailbox -PublicFolder | Where-Object {$_.ExchangeGuid -eq
$hierarchyMailboxGuid} | Remove-Mailbox -PublicFolder -Confirm:$false -
Force
Get-Mailbox -PublicFolder -SoftDeletedMailbox | % {Remove-Mailbox -
```

```
PublicFolder $_.PrimarySmtpAddress -PermanentlyDelete:$true -force -
Confirm:$false}
$soft=Get-Mailbox -PublicFolder -SoftDeletedMailbox; foreach ($mbx in
$soft){if ($mbx.Name -like "*CNF:*" -or $mbx.identity -like "*CNF:*")
{Remove-Mailbox -PublicFolder        $mbx.ExchangeGUID.GUID -
RemoveCNFPublicFolderMailboxPermanently -Force -Confirm:$false}}
```

Повторите приведенный выше блок команд в течение нескольких раз с интервалом 5–10 минут, чтобы очистить softDeletedMailboxes и не остаться объектов CNF.

> ⓘ **Примечание**
>
> Приведенный выше блок команд может возвращать ошибку, например "Не удалось выполнить операцию, так как не удалось найти объект <MailboxName> ", которую можно спокойно игнорировать из-за задержки репликации AD.

5. Выполните следующую команду еще раз, чтобы убедиться, что не осталось почтовых ящиков SoftDeleted или CNF.

```
PowerShell
```

```
Get-Mailbox -PublicFolder -SoftDeletedMailbox
```

Если отображается список обратимо удаленных почтовых ящиков, повторите блок команд из шага 4, в противном случае перейдите к следующему шагу.

Шаг 3. Создание CSV-файлов

Используйте скачанные сценарии, чтобы создать файлы CSV, которые будут использоваться в процессе миграции.

1. В командной консоли Exchange (локально) запустите `Export-ModernPublicFolderStatistics.ps1` скрипт, чтобы создать файл сопоставления имени папки с размером папки. Для запуска этого сценария необходимы права администратора. Результирующий файл содержит три столбца: **FolderName**, **FolderSize** и **DeletedItemSize**. Значения **столбцов FolderSize** и **DeletedItemSize** отображаются в байтах. Например, **\PublicFolder01,10240, 100 означает,** что общая папка в корневой папке иерархии с именем PublicFolder01 имеет размер 10240 байт (10 КБ), а в ней есть 100 байтов восстанавливаемых элементов.

PowerShell

```
.\Export-ModernPublicFolderStatistics.ps1 <Folder-to-size map path>
```

Пример.

PowerShell

```
.\Export-ModernPublicFolderStatistics.ps1 stats.csv
```

2. `ModernPublicFolderToMailboxMapGenerator.ps1` Запустите скрипт, чтобы создать файл .csv, который сопоставляет исходные общедоступные папки с почтовыми ящиками общедоступных папок в Exchange Online назначении. Этот файл используется для вычисления правильного количества почтовых ящиков общедоступных папок в Exchange Online.

Созданный файл `ModernPublicFolderToMailboxMapGenerator.ps1` не будет содержать имена всех общедоступных папок в вашей организации. Он содержит ссылки на родительские папки больших деревьев папок или имена папок, которые сами по себе значительно велики. Этот файл можно рассматривать как файл "исключений", который гарантирует, что определенные деревья папок и большие папки будут помещены в специальные почтовые ящики общедоступных папок. Обычно в этом файле не отображаются все общедоступные папки. Дочерние папки папок, перечисленных в этом файле сопоставления, также будут перенесены в тот же почтовый ящик, что и их родительская папка (если в файле сопоставления явно не указан другой почтовый ящик общедоступных папок).

PowerShell

```
.\ModernPublicFolderToMailboxMapGenerator.ps1 <Maximum mailbox size in
bytes><Maximum mailbox recoverable item size in bytes><Folder-to-size map
path><Folder-to-mailbox map path>
```

- `Maximum mailbox size in bytes` — это максимальный объем данных, который вы хотите перенести в один почтовый ящик общедоступных папок в Exchange Online. Максимальный размер этого поля в настоящее время составляет 100 ГБ, но мы рекомендуем использовать меньший размер, например 50 % от максимального размера, чтобы обеспечить будущий рост.

- `Maximum mailbox recoverable items size in bytes` — это квота элементов для восстановления в почтовых ящиках Exchange Online. Максимальный размер почтовых ящиков общедоступных папок в Exchange Online сейчас составляет

100 ГБ. Рекомендуется установить для *параметра RecoverableItemsQuota* значение 15 ГБ или меньше.

- `Folder-to-size map path` — это путь к файлу .csv, созданному при выполнении скрипта `Export-ModernPublicFolderStatistics.ps1` .

- `Folder-to-mailbox map path` — это путь к файлу из папки в почтовый ящик .csv файла, создаваемого на этом шаге. Если указать только имя файла, файл создается в текущем каталоге PowerShell на локальном компьютере.

Пример.

PowerShell

```
.\ModernPublicFolderToMailboxMapGenerator.ps1 -MailboxSize 50GB -
MailboxRecoverableItemSize 1GB -ImportFile .\stats.csv -ExportFile map.csv
```

> ⓘ **Примечание**
>
> В map.csv, созданном скриптом, используются универсальные имена для целевых почтовых ящиков общедоступных папок, которые будут созданы в EXO на следующем шаге (например, Mailbox1 и Mailbox2). Мы рекомендуем изменить имена почтовых ящиков общедоступных папок в map.csv в соответствии с политиками именования вашей организации. Кроме того, если в вашей локальной организации уже есть почтовые ящики, соответствующие универсальным именам, следует изменить map.csv и указать уникальные имена для целевых почтовых ящиков общедоступных папок в Exchange Online. Используйте Блокнот или аналогичный редактор, чтобы изменить имена TargetMailbox в map.csv

> ⓘ **Примечание**
>
> Перенос общедоступных папок в Exchange Online не поддерживается, если в Exchange Online более 100 уникальных почтовых ящиков общедоступных папок. Во время миграции можно включить до 100 почтовых ящиков общедоступных папок.

Шаг 4. Создание почтовых ящиков общедоступных папок в Exchange Online

Затем в Exchange Online PowerShell создайте целевые почтовые ящики общедоступных папок, содержащие перенесенные общедоступные папки.

Выполните приведенный ниже сценарий, чтобы создать целевые почтовые ящики общедоступных папок. Скрипт создает целевой почтовый ящик для каждого почтового ящика в файле .csv, созданном ранее на *шаге 3. Создание файлов .csv* при выполнении скрипта `ModernPublicFoldertoMailboxMapGenerator.ps1` .

PowerShell

```
$mappings = Import-Csv <Folder-to-mailbox map path>
$primaryMailboxName = ($mappings | Where-Object FolderPath -eq "\"
).TargetMailbox;
New-Mailbox -HoldForMigration:$true -PublicFolder -
IsExcludedFromServingHierarchy:$false $primaryMailboxName
($mappings | Where-Object TargetMailbox -ne
$primaryMailboxName).TargetMailbox | Sort-Object -unique | ForEach-Object {
New-Mailbox -PublicFolder -IsExcludedFromServingHierarchy:$false $_ }
```

`Folder-to-mailbox map path` — это путь к файлу folder-to-mailbox.csv, созданному `ModernPublicFoldertoMailboxMapGenerator.ps1` скриптом на *шаге 3. Создание файлов .csv*.

Шаг 5. Запуск запроса на миграцию

Теперь необходимо выполнить ряд команд как в локальной среде Exchange Server, так и в Exchange Online.

1. На любом сервере Exchange 2016 или Exchange 2019, на котором размещены почтовые ящики общедоступных папок, выполните следующий скрипт. Этот скрипт синхронизирует общедоступные папки с поддержкой почты из локальной службы Active Directory с Exchange Online. Убедитесь, что вы загрузили последнюю версию этого скрипта и выполнили его из командной консоли Exchange.

   PowerShell

   ```
   .\Sync-ModernMailPublicFolders.ps1 -CsvSummaryFile:sync_summary.csv
   ```

   - `CsvSummaryFile` — это путь к файлу журнала операций и ошибок синхронизации. Журнал будет в формате CSV.

   ⓘ Примечание

Если во время выполнения скрипта вы видите ошибки, воспользуйтесь функцией **синхронизации скрипта** `Sync-ModernMailPublicFolders.ps1` MEPF.

2. В Exchange Online PowerShell передайте учетные данные пользователя, имеющего разрешения администратора в локальной среде Exchange 2013, Exchange 2016 или Exchange 2019, в переменную `$Source_Credential`. Запрос на миграцию, выполняемый в Exchange Online, будет использовать эти учетные данные для получения доступа к локальным серверам Exchange Server и копирования содержимого общедоступных папок в Exchange Online.

```
PowerShell

$Source_Credential = Get-Credential <source_domain>\
<PublicFolder_Administrator_Account>
```

3. В Exchange Online PowerShell передайте полное доменное имя службы репликации почтовых ящиков Exchange (MRS) в переменную `$Source_RemoteServer`. Запрос на миграцию, выполняемый в Exchange Online, будет использовать этот удаленный сервер для копирования содержимого общедоступной папки в Exchange Online.

```
PowerShell

$Source_RemoteServer = "<MRS proxy endpoint server>"
```

4. На локальном сервере Exchange Server откройте командную консоль Exchange и найдите GUID основного почтового ящика иерархии с помощью следующей команды:

```
PowerShell

(Get-
OrganizationConfig).RootPublicFolderMailbox.HierarchyMailboxGuid.GUID
```

Обратите внимание на выходные данные этой команды. Оно вам понадобится на следующем шаге. Например:

> 91edc6dd-478a-497c-8731-b0b793f5a986

ⓘ Примечание

Идентификатор GUID почтового ящика общедоступных папок, упомянутый в предыдущей команде, должен быть получен с локального сервера; Если он получен из Exchange Online, пакет миграции завершится ошибкой с временной ошибкой.

5. В Exchange Online PowerShell выполните следующие команды, чтобы создать конечную точку миграции и запрос на миграцию общедоступных папок:

```
PowerShell

$bytes = [System.IO.File]::ReadAllBytes('folder_mapping.csv')
$PfEndpoint = New-MigrationEndpoint -PublicFolder -Name
PublicFolderEndpoint -RemoteServer $Source_RemoteServer -Credentials
$Source_Credential
New-MigrationBatch -Name PublicFolderMigration -CSVData $bytes -
SourceEndpoint $PfEndpoint.Identity -SourcePfPrimaryMailboxGuid <guid
you noted from previous step> -NotificationEmails <email addresses for
migration notifications>
```

Где `folder_mapping.csv` — файл карты, созданный на шаге 3. Создание .csv файлов , и `HierarchyMailboxGUID` является выходными данными, которые вы записали на предыдущем шаге. Обязательно укажите полный путь к файлу `folder_mapping.csv`. If the map file was moved for any reason, be sure to use the new location.

Несколько адресов электронной почты необходимо разделить запятыми.

> ⓘ **Примечание**
>
> Вы можете заметить, что приведенная выше команда завершается ошибкой "Не удается найти получателя с идентификатором GUID почтового ящика" с указанным идентификатором GUID почтового ящика общедоступных папок в EXO. Это может произойти из-за задержки репликации AD. В этом случае подождите час и повторите команду еще раз.

6. Начните миграцию, используя следующую команду в Exchange Online PowerShell:

```
PowerShell

Start-MigrationBatch PublicFolderMigration
```

Хотя пакетную миграцию необходимо создать с помощью командлета `New-MigrationBatch` в Exchange Online PowerShell, ход выполнения и завершение миграции можно просматривать и управлять ими в EAC или с помощью командлета Get-MigrationBatch. Командлет `New-MigrationBatch` инициирует запрос на миграцию почтового ящика для каждого почтового ящика общедоступных папок, и состояние этих запросов можно просмотреть на странице миграции почтовых ящиков.

Чтобы перейти на страницу миграции почтовых ящиков:

1. Войдите в Exchange Online и откройте Центр администрирования Exchange.
2. Navigate to **Recipients**, and then select **Migration**.
3. Выберите новый запрос на миграцию и щелкните **Просмотр сведений** в области **Сведения**.

Прежде чем перейти к *шагу 6. Блокировка общедоступных папок на локальном сервере Exchange*, убедитесь, что все данные скопированы и что при миграции нет ошибок. Убедившись, что пакет перешел в состояние **Синхронизировано**, выполните команды, описанные в разделе *Шаг 2. Подготовка к миграции*, на последнем шаге в разделе **Предварительные требования в локальной среде Exchange Server**, чтобы snapshot общедоступных папок в локальной среде.

Once these commands have run, you can proceed to the next step. Note that these commands could take a while to complete depending on the number of folders you have. Процесс миграции синхронизирует данные из исходной (локальной) среды каждые 24 часа.

Для мониторинга миграции можно использовать следующие командлеты:

- Get-PublicFolderMailboxMigrationRequest
- Get-PublicFolderMailboxMigrationRequestStatistics
- Get-MigrationBatch

Шаг 6. Блокировка общедоступных папок на локальном сервере Exchange (требуется время простоя общедоступных папок)

До этого момента локальные общедоступные папки Exchange 2013 были доступны для пользователей. Следующие шаги теперь выведут пользователей из Exchange

Server общедоступных папок, а затем заблокируют папки по мере завершения окончательной синхронизации процесса миграции. В течение этого времени общедоступные папки будут заблокированы для пользователей, и все сообщения, отправляемые в поддерживающие почту общедоступные папки, будут доставлены только после завершения миграции.

> ⓘ **Примечание**
>
> Окончательная синхронизация может занять значительное количество времени в зависимости от изменений, внесенных в исходную среду, размера развертывания общедоступных папок, емкости сервера и т. д. Если в иерархии папок было много поврежденных списков ACL, которые не были очищены до миграции, может возникнуть значительная задержка в завершении. Рекомендуется запланировать не менее 48 часов простоя для завершения окончательной синхронизации.

Убедитесь, что пакет миграции и отдельные запросы на миграцию успешно синхронизированы.

Выполните следующую команду в EXO PowerShell для получения дополнительных сведений:

```
Get-MigrationBatch |?{$_.MigrationType -like "*PublicFolder*"} | ft *last*sync*
```

```
Get-PublicFolderMailboxMigrationRequest | Get-
PublicFolderMailboxMigrationRequestStatistics |ft targetmailbox,*last*sync*
```

LastSyncedDate (в пакете миграции) и LastSuccessfulSyncTimestamp (для отдельных заданий) должны находиться в течение последних 7 дней. Если дата слишком далека в прошлом, например более месяца назад, вам может потребоваться просмотреть запросы на миграцию общедоступных папок и убедиться, что все запросы были синхронизированы недавно.

На этом этапе рекомендуется повторно запустить следующий скрипт, чтобы все новые общедоступные папки с поддержкой почты были синхронизированы с Exchange Online:

PowerShell

```
.\Sync-ModernMailPublicFolders.ps1 -CsvSummaryFile:sync_summary.csv
```

Убедившись, что пакет и все запросы на миграцию успешно синхронизированы, в локальной среде выполните следующую команду, чтобы заблокировать Exchange Server общедоступных папок для завершения.

```
PowerShell

Set-OrganizationConfig -PublicFolderMailboxesLockedForNewConnections $true
```

> ⓘ **Примечание**
>
> Если вы не можете получить доступ к параметру `-PublicFolderMailboxesLockedForNewConnections`, это может быть связано с тем, что ваша Служба Active Directory не была подготовлена во время обновления CU, как мы рекомендовали выше в разделе *Что необходимо знать, прежде чем приступить к работе?* Дополнительные сведения см. в разделе Подготовка Active Directory и доменов. Обратите внимание, что **сначала** нужно перенести всех пользователей, которым необходим доступ к общедоступным папкам.

Если в вашей организации есть почтовые ящики общедоступных папок на нескольких серверах Exchange, необходимо подождать, пока репликация Active Directory завершится. После завершения вы можете убедиться, что все почтовые ящики общедоступных папок выбрали `PublicFolderMailboxesLockedForNewConnections` флаг и что все ожидающие изменения, недавно внесенные пользователями в их общедоступные папки, сошлись по всей организации. Все это может занять несколько часов.

Выполните следующую команду в локальной среде, чтобы убедиться, что общедоступные папки заблокированы:

```
PowerShell

Get-PublicFolder \
```

Ожидаемый результат, если общедоступные папки заблокированы:

`Couldn't find the public folder mailbox. + CategoryInfo : NotSpecified: (:) [Get-PublicFolder], ObjectNotFoundException`

Шаг 7. Завершение миграции общедоступных папок (требуется отключение общедоступных папок)

Прежде чем завершить миграцию общедоступных папок, необходимо проверка следующие элементы:

1. Убедитесь, что в локальной среде Exchange не происходит других перемещений почтовых ящиков общедоступных папок или общедоступных папок. Для этого используйте командлеты **Get-MoveRequest** и **Get-PublicFolderMoveRequest** , чтобы получить список всех существующих перемещений общедоступных папок. Если какие-либо перемещения выполняются или **находятся в состоянии Завершено** , удалите их.

2. Если в вашей среде несколько доменов Active Directory, убедитесь, что перед инициализацией выполните действия, описанные в разделе Ошибка "Активные почтовые ящики общедоступных папок", а пакет миграции завершается сбоем при Complete-MigrationBatch команде .

3. Чтобы завершить миграцию общедоступных папок, выполните следующую команду в Exchange Online PowerShell:

   PowerShell

   ```
   Complete-MigrationBatch PublicFolderMigration
   ```

> ⓘ **Важно!**
>
> После завершения пакета миграции дополнительные данные не могут быть синхронизированы с локальных серверов Exchange и Exchange Online.

При запуске `Complete-MigrationBatch PublicFolderMigration` Exchange выполнит окончательную синхронизацию между локальной организацией Exchange и Exchange Online. В этот период состояние пакета миграции изменится с **Синхронизировано** на **Завершение**, а затем на **Завершено**. После окончательной синхронизации общедоступные папки в Exchange Online будут разблокированы. Однако настоятельно рекомендуется выполнить шаги 8 и 9 этой статьи, прежде чем открывать общедоступные папки для пользователей.

Состояние пакета миграции обычно остается **синхронизированным** в течение нескольких часов, прежде чем переключение на **Завершение**. При миграциях с

большим количеством целевых почтовых ящиков обычно состояние остается в **синхронизированном** состоянии более 24 часов при условии, что ни один из базовых запросов на миграцию общедоступных папок не завершился сбоем или был помещен в карантин.

Шаг 8. Проверка и разблокировка общедоступных папок в Exchange Online

После миграции выполните указанные ниже действия, чтобы проверить и официально подтвердить, что она завершена. Эти действия позволят проверить иерархию перенесенных общедоступных папок, прежде чем окончательно переходить на общедоступные папки Exchange Online.

1. В Exchange Online PowerShell настройте некоторые почтовые ящики тестовых пользователей, чтобы использовать один из недавно перенесенных почтовых ящиков общедоступных папок в качестве почтового ящика общедоступных папок по умолчанию:

   PowerShell

   ```
   Set-Mailbox -Identity <test user> -DefaultPublicFolderMailbox <public
   folder mailbox identity>
   ```

   Убедитесь, что у тестовых пользователей есть необходимые разрешения для создания общедоступных папок.

2. Откройте Outlook, войдите в учетную запись тестового пользователя, указанного на предыдущем шаге, и выполните следующие проверки общедоступных папок. Обратите внимание, что изменения вступят в силу в течение 15-30 минут. После этого вам может потребоваться несколько раз перезапустить Outlook.

   А. просмотр иерархии;

   Б. проверка разрешений;

   с. Создайте несколько общедоступных папок, а затем удалите их.

   d. Поместите содержимое в общедоступную папку и удалите его.

   Если у вас возникли проблемы и вы не готовы полностью переключать общедоступные папки организации на Exchange Online, см. раздел Откат переноса общедоступных папок с Exchange Server на Exchange Online.

3. Выполните приведенную ниже команду в Exchange Online PowerShell, чтобы разблокировать общедоступные папки в Exchange Online. Изменения вступят в силу в течение 15-30 минут после выполнения команды. После этого пользователям может потребоваться несколько раз перезапустить Outlook.

```PowerShell
Set-OrganizationConfig -RemotePublicFolderMailboxes $Null -
PublicFoldersEnabled Local
```

Шаг 9. Завершение локальной миграции

Чтобы включить электронную почту в локальных общедоступных папках с поддержкой почты, выполните следующие действия.

1. Выполните следующую команду в локальной среде, чтобы создать резервную копию сообщений электронной почты в очереди, которые были отправлены в общедоступные папки с поддержкой почты. Эту резервную копию можно использовать в сценариях, когда доставка электронной почты в общедоступные папки с поддержкой почты завершилась сбоем по любой причине:

```PowerShell
$Server=Get-TransportService;ForEach ($t in $server) {Get-Message -
Server $t -ResultSize Unlimited| ?{$_.Recipients -like
"*PF.InTransit*"} | ForEach-Object {Suspend-Message $_.Identity -
Confirm:$False; $Temp="C:\ExportFolder\"+$_.InternetMessageID+".eml";
$Temp=$Temp.Replace("<","_"); $Temp=$Temp.Replace(">","_"); Export-
Message $_.Identity | AssembleMessage -Path $Temp;Resume-message
$_.Identity -Confirm:$false}}
```

2. В локальной среде выполните следующий сценарий, чтобы убедиться, что все сообщения, отправляемые в поддерживающие почту общедоступные папки, перенаправляются в Exchange Online. Скрипт помеет общедоступные папки с поддержкой `ExternalEmailAddress` почты с помощью , который указывает на их Exchange Online коллег:

```PowerShell
.\SetMailPublicFolderExternalAddress.ps1 -
ExecutionSummaryFile:mepf_summary.csv
```

3. Если проверка прошла успешно, в локальной среде выполните следующую команду, чтобы указать, что миграция общедоступных папок завершена:

```
PowerShell

Set-OrganizationConfig -PublicFolderMailboxesMigrationComplete:$true -
PublicFoldersEnabled Remote
```

Как проверить, что это работает

На шаге 2 Подготовка к миграции вы сделали моментальные снимки структуры, статистики и разрешений локальных общедоступных папок. Ниже описано, как сделать такие же моментальные снимки в Exchange Online после миграции. Сравните данные в обоих файлах, чтобы проверить успешность.

1. В Exchange Online PowerShell выполните следующую команду, чтобы сделать моментальный снимок новой структуры папок:

```
PowerShell

Get-PublicFolder -Recurse -ResultSize Unlimited | Export-CliXML
Cloud_PFStructure.xml
```

2. В Exchange Online PowerShell выполните следующую команду, чтобы сделать моментальный снимок статистики общедоступных папок, в том числе количества, размеров и владельцев элементов:

```
PowerShell

Get-PublicFolder -Recurse -ResultSize Unlimited | Get-
PublicFolderStatistics | Export-CliXML Cloud_PFStatistics.xml
```

3. В Exchange Online PowerShell выполните следующую команду, чтобы сделать моментальный снимок разрешений:

```
PowerShell

Get-PublicFolder -Recurse -ResultSize Unlimited | Get-
PublicFolderClientPermission | Select-Object Identity,User,AccessRights
| Export-CliXML Cloud_PFPerms.xml
```

4. Exchange Online PowerShell выполните следующую команду, чтобы snapshot общедоступных папок с поддержкой почты:

PowerShell

```
Get-MailPublicFolder -ResultSize Unlimited | Export-CliXML
Cloud_MEPF.xml
```

Примечание

После миграции, если внешние сообщения электронной почты не поддерживают общедоступные папки с поддержкой почты в Exchange Online с ошибкой 5.7.13 или 5.4.1, убедитесь, что общедоступная папка имеет разрешение *CreateItems* для анонимных пользователей, а **блокировка пограничных серверов на основе домена (DBEB)** отключена для домена электронной почты, настроенного в общедоступной папке.

Известные проблемы

Ниже перечислены распространенные проблемы, которые могут возникнуть при переносе общедоступных папок в вашей организации.

- Перенос общедоступных папок в Exchange Online не поддерживается, если в Exchange Online более 100 уникальных почтовых ящиков общедоступных папок.

- Разрешения для корневой общедоступной папки и папки EFORMS REGISTRY не будут перенесены в Exchange Online, и вам придется вручную применить их в Exchange Online. Для этого выполните команду ниже в Exchange Online PowerShell. Выполните команду по одному разу для каждого разрешения в локальной среде, которого нет в Exchange Online:

  PowerShell

  ```
  Add-PublicFolderClientPermission "\" -User <user> -AccessRights <access
  rights>
  Add-PublicFolderClientPermission "\NON_IPM_SUBTREE\EFORMS REGISTRY" -
  User <user> -AccessRights <access rights>
  ```

- Сбой миграции может произойти, если некоторые почтовые ящики общедоступных папок не обслуживают иерархические запросы. Это означает, что параметру `IsExcludedFromServingHierarchy` одного или нескольких почтовых ящиков присвоено значение `$true`. Чтобы этого избежать, сделайте

так, чтобы все почтовые ящики в Exchange Online обслуживают иерархические запросы.

- Разрешения **Отправить как** и **Отправить от имени** не переносятся в Exchange Online. Используйте приведенные ниже команды в локальной среде, чтобы узнать, у кого есть эти разрешения.

  Чтобы узнать, у каких локальных общедоступных папок есть разрешения "Отправить как":

  ```
  PowerShell

  Get-MailPublicFolder | Get-ADPermission | ?{$_.ExtendedRights -like "*Send-As*"}
  ```

  Чтобы узнать, у каких локальных общедоступных папок есть разрешения "Отправить от имени":

  ```
  PowerShell

  Get-MailPublicFolder | ?{$_.GrantSendOnBehalfTo -ne "$null"} | Format-Table name,GrantSendOnBehalfTo
  ```

  Чтобы добавить разрешение "Отправить от имени" для поддерживающей почту общедоступной папки в Exchange Online, выполните следующую команду в Exchange Online PowerShell:

  ```
  PowerShell

  Add-RecipientPermission -Identity <mail-enabled public folder primary SMTP address> -Trustee <name of user to be assigned permission> -AccessRights SendAs
  ```

  Пример:

  ```
  PowerShell

  Add-RecipientPermission -Identity send1 -Trustee Exo1 -AccessRights SendAs
  ```

  Чтобы добавить разрешение "Отправить как" для поддерживающей почту общедоступной папки в Exchange Online, выполните следующую команду в Exchange Online PowerShell:

  ```
  ```

```
PowerShell

Set-MailPublicFolder -Identity <name of public folder> -
GrantSendOnBehalfTo <user or comma-separated list of users>
```

Пример:

```
PowerShell

Set-MailPublicFolder send2 -GrantSendOnBehalfTo exo1,exo2
```

- Если в папке "\NON_IPM_SUBTREE\DUMPSTER_ROOT" более 10 000 папок, может возникнуть ошибка миграции. Проверяйте количество папок, вложенных в "\NON_IPM_SUBTREE\DUMPSTER_ROOT" (непосредственных дочерних элементов). Чтобы посмотреть, сколько общедоступных папок находится в этом расположении, используйте следующую команду:

  ```
  PowerShell

  (Get-PublicFolder -GetChildren "\NON_IPM_SUBTREE\DUMPSTER_ROOT").Count
  ```

  Exchange Online не поддерживает более 10 000 вложенных папок, поэтому миграция из более чем 10 000 папок завершится ошибкой. В настоящее время мы разрабатываем сценарий для поддержки таких конфигураций. Советуем подождать.

- Задания миграции не выполняются или застопорились. Это может произойти, если слишком много заданий выполняется параллельно, в результате чего возникают временные ошибки. Число одновременных заданий можно уменьшить, изменив `MaxConcurrentMigrations` и `MaxConcurrentIncrementalSyncs` до меньшего числа. Используйте следующий пример, чтобы установить эти значения:

  ```
  PowerShell

  Set-MigrationEndpoint <PublicFolderEndpoint> -MaxConcurrentMigrations
  30 -MaxConcurrentIncrementalSyncs 20 -SkipVerification
  ```

- Выполнение заданий миграции заканчивается, при этом отображается такое сообщение об ошибке: "Ошибка. Корзина папки корзины". Чтобы устранить эту ошибку, остановите обработку пакета и запустите ее снова.

- Сбой заданий миграции с ошибкой "Запрос помещен в карантин из-за следующей ошибки: Указанный ключ отсутствует в словаре". Это происходит, когда поврежденный элемент присутствует в папке, которую задания миграции не могут скопировать. Обходное решение:

    1. Остановите обработку пакета миграции.
    2. Определите папку, содержащую поврежденный элемент. В отчете о миграции должны быть ссылки на папку, которая копировалась при возникновении ошибки.
    3. В локальной среде переместите эту папку в основной почтовый ящик общедоступных папок. Командлет можно использовать `New-PublicFolderMoveRequest` для перемещения папок.
    4. Дождитесь перемещения папки. После этого удалите запрос на перемещение. Перезапустите обработку пакета миграции.

Удаление почтовых ящиков общедоступных папок из локальной среды Exchange

После того как миграция закончится и вы убедитесь, что общедоступные папки в Exchange Online работают должным образом и содержат все нужные данные, можно удалять локальные почтовые ящики общедоступных папок.

Обратите внимание, что после удаления их невозможно будет восстановить. Поэтому настоятельно рекомендуем не только проверить, выполнена ли миграция, но и понаблюдать за общедоступными папками Exchange Online в течение нескольких недель, прежде чем удалять локальные почтовые ящики общедоступных папок.

Перенос общедоступных папок в Microsoft 365 или Office 365 с помощью экспорта PST-файлов Outlook

Не рекомендуется использовать функцию экспорта PST в Outlook для переноса общедоступных папок в Microsoft 365 или Office 365 или Exchange Online, если локальная иерархия общедоступных папок превышает 30 ГБ. Microsoft 365 и Office 365 рост почтового ящика общедоступных папок в Интернете управляется с помощью функции автоматического разделения, которая разделяет почтовый

ящик общедоступных папок при превышении квот на размер. Автоматическое разделение не может справиться с внезапным ростом почтовых ящиков общедоступных папок при использовании экспорта PST для переноса общедоступных папок. Возможно, вам придется ждать до двух недель автоматического разделения, чтобы переместить данные из основного почтового ящика. Кроме того, прежде чем использовать PST-приложение Outlook для экспорта общедоступных папок в Microsoft 365 или Office 365 или Exchange Online, учитывайте следующее:

- Разрешения общих папок будут потеряны в ходе этого процесса. Запишите текущие разрешения перед переносом и вручную добавьте их после его завершения.
- Если вы используете сложные разрешения или переносите большое число папок, мы рекомендуем использовать командлеты.
- Любые изменения элементов или папок в исходных общих папок во время экспорта в PST-файл будут потеряны. Поэтому мы рекомендуем использовать инструкции на основе командлетов, если для процесса экспорта и импорта потребуется много времени.

Если вы все равно хотите переместить общедоступные папки с помощью PST-файлов, выполните следующие действия, чтобы успешно завершить операцию.

1. Следуйте инструкциям в разделе Шаг 1. Загрузка сценариев переноса, чтобы загрузить сценарии переноса. Вам нужно только скачать `PublicFolderToMailboxMapGenerator.ps1` файл.
2. Выполните шаг No 2 из шага 3. Создайте файлы .csv , чтобы создать файл сопоставления общедоступных папок с почтовым ящиком. Этот файл используется для вычисления правильного количества почтовых ящиков общедоступных папок в Exchange Online.
3. Создайте необходимые почтовые ящики общедоступных папок на основе файла сопоставления. Дополнительные сведения см . в статье Создание почтового ящика общедоступных папок с помощью EAC.
4. Используйте командлет **New-PublicFolder**, чтобы создать общую папку верхнего уровня в каждом почтовом ящике общих папок, с параметром *Mailbox*.
5. Экспорт и импорт PST-файлов с помощью Outlook.

6. Установите разрешения для общих папок с помощью EAC. Дополнительные сведения см. в разделе Шаг 3. Назначение разрешений для общедоступной папки в статье Настройка общедоступных папок в новой организации .

⊗ **Внимание!**

Если вы уже начали миграцию PST и сталкивались с проблемой, из-за которой основной почтовый ящик был заполнен, у вас есть два варианта восстановления миграции PST:

Первый вариант — дождаться, пока автоматическое разделение переместит данные из основного почтового ящика. Это может занять до двух недель. Однако все общедоступные папки в заполненном почтовом ящике общедоступных папок не смогут получать новое содержимое, пока авторазбиение не завершится.

Второй вариант — **создать почтовый ящик общедоступных папок в Exchange Server**, а затем использовать командлет **New-PublicFolder** с параметром *Mailbox* для создания оставшихся общедоступных папок в дополнительном почтовом ящике общедоступных папок.

Устранение неполадок миграции общедоступных папок

Нажмите следующую кнопку для распространенных проблем во время миграции общедоступных папок:

Выполнение тестов: устранение неполадок с переносом общедоступных папок

Откроется всплывающее окно в Центр администрирования Microsoft 365, войдите с помощью учетной записи администратора клиента и выберите соответствующий параметр.

Удаление развертывания общедоступных папок с Exchange Server 2013 или более поздней версии

Статья • 25.09.2024

После переноса всех локальных пользователей и общедоступных папок в Exchange Online необходимо удалить локальное развертывание общедоступных папок. Выполнение чистого удаления локального развертывания общедоступных папок имеет решающее значение, так как неправильное удаление может привести к проблемам, таким как потерянные **общедоступные папки с поддержкой почты (MEPF)** и заблокированные SMTP-адреса в Microsoft Entra ID или Exchange Online.

В этой статье перечислены шаги по безопасному удалению общедоступных папок и связанных данных из локального развертывания Exchange Server 2013 или более поздних версий.

Предварительные условия

Перед началом работы убедитесь, что:

- Вы перенесли локальные общедоступные папки в Exchange Online.
- Нет пользователей в локальной среде или в Exchange Online, которые подключаются к общедоступным папкам, развернутыми локально, или используют их.
- Локальные почтовые ящики общедоступных папок создаются перед удалением.
- Все следующие действия необходимо выполнить из командной консоли Exchange с учетной записью администратора, для которого назначены необходимые роли.

Отключение доступа к общедоступным папкам для пользователей

1. Выполните следующую команду, чтобы отключить назначение системного почтового ящика общедоступных папок для пользователей:

```
PowerShell

Set-OrganizationConfig -PublicFoldersEnabled None
```

2. Затем выполните следующую команду, чтобы удалить все назначенные администратором почтовые ящики общедоступных папок пользователей:

```
PowerShell

Set-ADServerSettings -ViewEntireForest:$true
Get-Mailbox -ResultSize unlimited | where
{$_.DefaultPublicFolderMailbox -ne $Null} | Set-Mailbox -
DefaultPublicFolderMailbox $Null
```

3. Разрешите до часа для репликации AD и изменений, которые вступают в силу. Затем выполните следующую команду, чтобы убедиться в отсутствии назначения почтового ящика общедоступных папок для пользователей:

```
PowerShell

Set-ADServerSettings -ViewEntireForest:$true
Get-Mailbox -ResultSize unlimited |?{$_.DefaultPublicFolderMailbox -ne
$Null -OR $_.EffectivePublicFolderMailbox -ne $Null}
```

Очистка общедоступных папок с поддержкой почты

Используйте командную консоль Exchange для выполнения команд PowerShell, перечисленных в этих шагах.

1. Создайте резервную копию сведений о MEPF. Общедоступные папки с поддержкой почты не содержат никаких данных, но являются объектами в Active Directory, связанными с общедоступной папкой, в которую размещаются фактические данные. Бежать:

```
PowerShell

Set-ADServerSettings -ViewEntireForest:$true
Get-MailPublicFolder -ResultSize Unlimited| Export-Clixml MEPF.XML
```

2. Отключите MEPFs.

Выполните следующую команду:

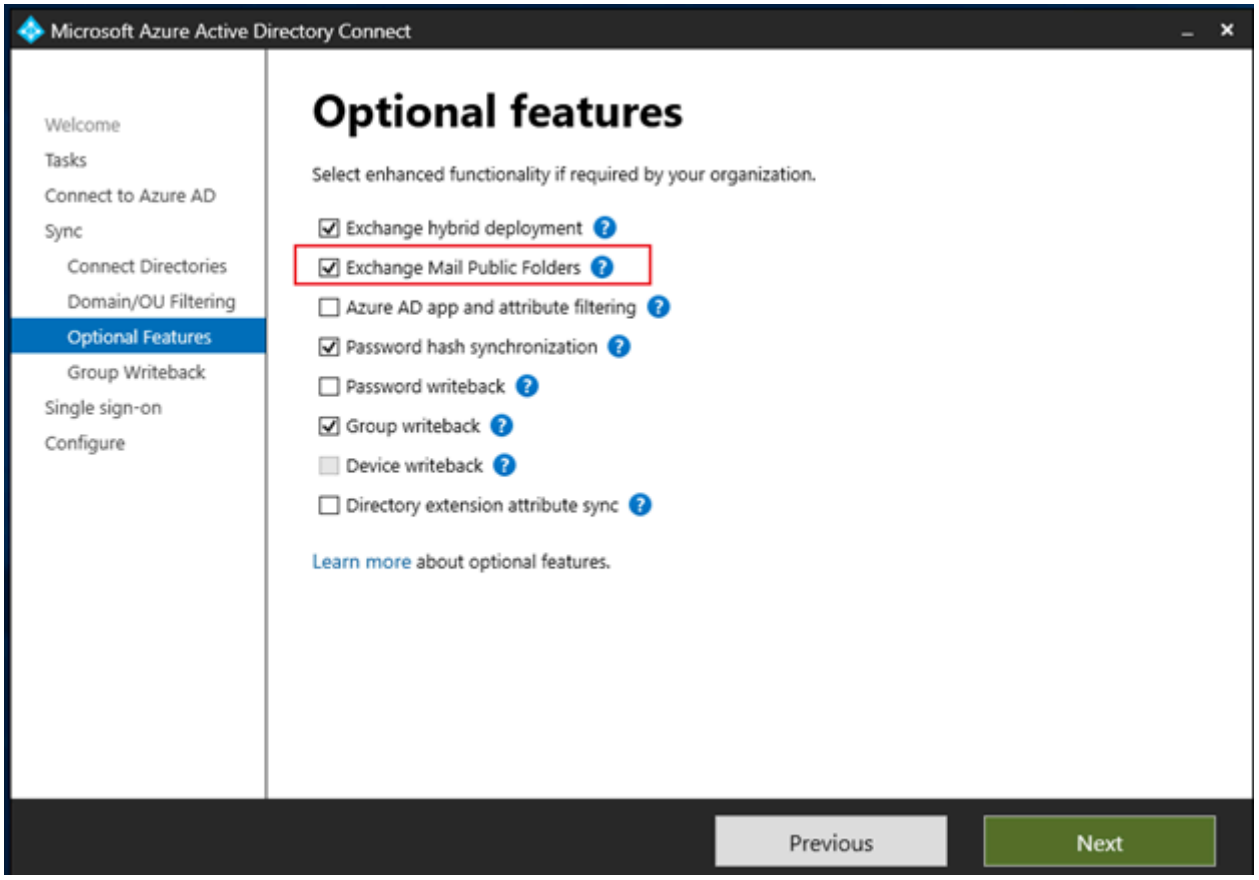
```
PowerShell

Set-ADServerSettings -ViewEntireForest:$true
Get-MailPublicFolder -ResultSize Unlimited | Disable-MailPublicFolder
```

3. Убедитесь, что в списке отсутствуют MEPF. Вы также можете убедиться, что больше нет объекта типа PublicFolder ни в одном из подразделений системных объектов Microsoft Exchange в локальной службе AD.

Бежать:

```
PowerShell

Get-MailPublicFolder
```

4. Убедитесь, что флажок **Общедоступные папки почты Exchange** снят в средстве Microsoft Entra Подключиться.



5. Выполните синхронизацию Microsoft Entra Connect.

Удаление почтовых ящиков общедоступных папок

Следующая команда блокирует общедоступные папки для подключений пользователей и указывает, что миграция общедоступных папок завершена в среде:

PowerShell

```
Set-OrganizationConfig -PublicFolderMailboxesLockedForNewConnections $true -
PublicFolderMailboxesMigrationComplete $true
```

2. Удалите почтовые ящики PF вторичной иерархии.

PowerShell

```
Set-ADServerSettings -ViewEntireForest:$true

Get-Mailbox -PublicFolder -ResultSize Unlimited |?
{$_.IsRootPublicFolderMailbox -ne "True"} | Remove-Mailbox -PublicFolder
```

2. Удалите основной почтовый ящик PF иерархии:

PowerShell

```
Get-Mailbox -PublicFolder |?{$_.IsRootPublicFolderMailbox -eq "True"} |
Remove-Mailbox -PublicFolder
```

Откат миграции общедоступных папок с Exchange Server на Exchange Online

Статья • 25.07.2023

Если у вас возникли проблемы с переносом общедоступных папок в Exchange Online или по какой-либо другой причине необходимо повторно активировать Exchange Server общедоступные папки, выполните следующие действия.

Откат миграции

При откате миграции вы потеряете все содержимое, добавленное в общедоступные папки в Exchange Online после миграции, через клиенты или по электронной почте для общедоступных папок с поддержкой почты. Чтобы его сохранить, можно экспортировать содержимое общедоступной папки после миграции в PST-файл, который импортируется в локальные общедоступные папки после завершения отката.

1. В локальной среде Exchange выполните следующую команду, чтобы разблокировать Exchange Server общедоступных папок:

   PowerShell

   ```
   Set-OrganizationConfig -
   PublicFolderMailboxesLockedForNewConnections:$false -
   PublicFolderMailboxesMigrationComplete:$false -PublicFoldersEnabled
   Local
   ```

   > **Примечание**
   >
   > Разблокировка может занять несколько часов.

2. В локальной среде Exchange отменить изменения `ExternalEmailAddress` всех общедоступных папок с поддержкой почты, которые были обновлены SetMailPublicFolderExternalAddress.ps1 (скрипт, используемый в *шаге 8. Проверка и разблокировка общедоступных папок в Exchange Online*использования пакетной миграции для миграции Exchange Server общедоступных папок в Exchange Online). . Вы можете обратиться к файлу сводки, созданному скриптом, чтобы определить те, которые были изменены,

или использовать файл OnPrem_MEPF.xml, созданный ранее в том же процессе пакетной миграции, чтобы получить исходные свойства для всех общедоступных папок с поддержкой почты.

3. В Exchange Online PowerShell выполните указанные ниже команды, чтобы удалить все общедоступные папки и почтовые ящики Exchange Online.

```
PowerShell

Get-MailPublicFolder -ResultSize Unlimited | where {$_.EntryId -ne
$null}| Disable-MailPublicFolder -Confirm:$false
Get-PublicFolder -GetChildren \ -ResultSize Unlimited | Remove-
PublicFolder -Recurse -Confirm:$false
$hierarchyMailboxGuid = $(Get-
OrganizationConfig).RootPublicFolderMailbox.HierarchyMailboxGuid
Get-Mailbox -PublicFolder | Where-Object {$_.ExchangeGuid -ne
$hierarchyMailboxGuid} | Remove-Mailbox -PublicFolder -Confirm:$false -
Force
Get-Mailbox -PublicFolder | Where-Object {$_.ExchangeGuid -eq
$hierarchyMailboxGuid} | Remove-Mailbox -PublicFolder -Confirm:$false -
Force
Get-Mailbox -PublicFolder -SoftDeletedMailbox | Remove-Mailbox -
PublicFolder -PermanentlyDelete:$true -Force
```

4. Выполните следующую команду в среде Exchange Online, чтобы перенаправить трафик общедоступных папок обратно в локальную среду (Exchange Server):

```
PowerShell

Set-OrganizationConfig -PublicFoldersEnabled Remote
```

5. Инструкции по перенастройки доступа к локальным общедоступным папкам, чтобы пользователи Exchange Online могли получить к ним доступ, см. в статье Настройка общедоступных папок Exchange 2013 для гибридного развертывания.

Использование пакетной миграции для переноса устаревших общедоступных папок в Microsoft 365 или Office 365

Статья • 04.04.2023

Сводка. Используйте эти процедуры для перемещения общедоступных папок Exchange 2010 в Microsoft 365 или Office 365.

В этом разделе описывается, как перенести общедоступные папки в прямой или поэтапной миграции из накопительного пакета обновления 8 для Exchange Server 2010 с пакетом обновления 3 (SP3) в Microsoft 365 или Office 365 и Exchange Online.

В этом разделе сервер Exchange 2010 SP3 RU8 называется устаревшим сервером Exchange Server. Кроме того, действия, описанные в этом разделе, относятся к Exchange Online и Microsoft 365 или Office 365. Данные продукты в контексте этого раздела являются взаимозаменяемыми.

Не рекомендуется использовать функцию экспорта PST Outlook для переноса общедоступных папок в Microsoft 365, Office 365 или Exchange Online. Microsoft 365, Office 365 и Exchange Online увеличением почтовых ящиков общедоступных папок управляется с помощью функции автоматического разделения, которая разделяет почтовый ящик общедоступных папок при превышении квот на размер. Автоматическое разделение не может справиться с внезапным ростом почтовых ящиков общедоступных папок при использовании экспорта PST для переноса общедоступных папок. Возможно, вам придется ждать до двух недель автоматического разделения, чтобы переместить данные из основного почтового ящика. Рекомендуется использовать инструкции на основе командлетов в этом документе для переноса общедоступных папок в Microsoft 365, Office 365 или Exchange Online. Однако если вы решили перенести общедоступные папки с помощью экспорта PST, см. раздел Миграция общедоступных папок в Microsoft 365 или Office 365 с помощью экспорта PST Outlook далее в этом разделе.

Миграция выполняется с помощью командлетов ***-MigrationBatch** в дополнение к следующим сценариям PowerShell:

- `SourceSideValidations.ps1`: исходный скрипт проверки на стороне источника сканирует общедоступные папки в источнике и сообщает об обнаруженных

проблемах вместе с действием по устранению проблем. Этот скрипт будет выполняться на локальном сервере Exchange Server прежних версий.

- `Export-PublicFolderStatistics.ps1`: этот скрипт создает файл сопоставления имени папки с размером папки. Этот сценарий запускается на сервере Exchange прежних версий.

- `Export-PublicFolderStatistics.psd1`: этот файл поддержки используется скриптом `Export-PublicFolderStatistics.ps1` и должен быть скачан в то же расположение.

- `PublicFolderToMailboxMapGenerator.ps1`: этот скрипт создает файл сопоставления общедоступных папок с почтовым ящиком с помощью выходных данных скрипта `Export-PublicFolderStatistics.ps1` . Этот сценарий запускается на сервере Exchange прежних версий.

- `PublicFolderToMailboxMapGenerator.strings.psd1`: этот файл поддержки используется скриптом `PublicFolderToMailboxMapGenerator.ps1` и должен быть скачан в то же расположение.

- `Create-PublicFolderMailboxesForMigration.ps1`: этот скрипт создает целевые почтовые ящики общедоступных папок для миграции. Кроме того, этот сценарий подсчитывает необходимое количество почтовых ящиков для обработки прогнозируемой пользовательской нагрузки, основываясь на указаниях по количеству входов пользователей на почтовый ящик общедоступных папок с учетом рекомендаций в Limits for Public Folders.

- `Create-PublicFolderMailboxesForMigration.strings.psd1`: этот файл поддержки используется скриптом Create-PublicFolderMailboxesForMigration.ps1 и должен быть скачан в то же расположение.

- `Sync-MailPublicFolders.ps1`: этот скрипт синхронизирует объекты общедоступных папок с поддержкой почты между локальным развертыванием Exchange и Microsoft 365 или Office 365. Этот сценарий запускается на сервере Exchange прежних версий.

- `SyncMailPublicFolders.strings.psd1`: это файл поддержки, используемый `Sync-MailPublicFolders.ps1` скриптом и должен быть скопирован в то же расположение, что и предыдущие скрипты.

Шаг 1. Загрузка сценариев переноса содержит сведения о том, куда их скачивать. Убедитесь, что все сценарии скачиваются в одно и то же расположение.

Какие версии Exchange поддерживаются для переноса общедоступных папок в Microsoft 365 или Office 365 и Exchange Online?

Exchange поддерживает перемещение общедоступных папок в Microsoft 365 или Office 365 и Exchange Online из следующих устаревших версий Exchange Server:

- Exchange 2010 с пакетом обновления 3 (SP3) и накопительным пакетом обновления 8 (RU8) или более поздней версии;

Если вам нужно переместить общедоступные папки в Exchange Online но локальные серверы не работают с минимальной поддержкой версий Exchange 2010, настоятельно рекомендуется обновить локальные серверы и использовать пакетную миграцию, которая является единственным поддерживаемым методом миграции общедоступных папок.

Невозможно перенести общедоступные папки непосредственно из Exchange 2003 или Exchange 2007. Если вы используете Exchange 2007 или более раннюю версию в организации, необходимо переместить все базы данных и реплики общедоступных папок в Exchange 2010 с пакетом обновления 3 (SP3) RU8 или более поздней версии. В Exchange 2007 или более ранних версиях не могут оставаться реплики общедоступных папок. Кроме того, почта, предназначенная для общедоступной папки Exchange 2013 или более поздней версии, не может быть перенаправлена через сервер Exchange 2003 или Exchange 2007.

Что нужно знать перед началом работы

- Сервер Exchange 2010 должен работать под управлением Exchange 2010 с пакетом обновления 3 (SP3) и накопительным пакетом обновления 8 (RU8) или более поздних версий.

- В Microsoft 365 или Office 365 и Exchange Online необходимо быть членом группы ролей "Управление организацией". Эта группа ролей отличается от разрешений, назначенных вам при подписке на Microsoft 365, Office 365 или Exchange Online. Дополнительные сведения о том, как включить группу ролей Управление организацией, см. в разделе Управление группами ролей в Exchange Online.

- В Exchange 2010 вы должны быть участником группы ролей RBAC "Управление организацией" или "Управление сервером". Дополнительные сведения см. в разделе Добавление участников в группу ролей.

- Если размер одной общедоступной папки в организации превышает 25 ГБ, перед началом миграции общедоступных папок рекомендуется удалить содержимое из этой папки, чтобы уменьшить ее размер. Кроме того, рекомендуется разделить содержимое общедоступной папки на несколько небольших общедоступных папок. Обратите внимание, что указанное здесь ограничение в 25 ГБ применяется только к общедоступной папке, а не ее дочерним папкам или подпапкам. Если ни один их этих вариантов невозможен, рекомендуем не перемещать общедоступные папки в Exchange Online. Дополнительные сведения см. в разделе Ограничения Exchange Online. **Примечание.** Если текущие квоты общедоступных папок в Exchange Online менее 25 ГБ, можно использовать командлет Set-OrganizationConfig, чтобы увеличить их с `DefaultPublicFolderIssueWarningQuota` помощью параметров и `DefaultPublicFolderProhibitPostQuota` .

Если вы используете брандмауэр и списки управления доступом (ACL), убедитесь, что диапазоны IP-адресов, используемые Microsoft 365 или Office 365 в вашем регионе, разрешены через брандмауэр.

- В Microsoft 365, Office 365 и Exchange Online можно создать не более 1000 почтовых ящиков общедоступных папок.

- Перед переносом общедоступных папок рекомендуется сначала переместить все почтовые ящики пользователей в Microsoft 365 или Office 365 и Exchange Online. Дополнительные сведения см. в статье Способы переноса нескольких учетных записей электронной почты в Microsoft 365 или Office 365. Однако вам по-прежнему потребуется сохранить в локальной среде почтовый ящик для администратора PF, выполняющего миграцию, или создать учетную запись администратора PF и назначить почтовый ящик, размещенный на сервере Exchange Server прежних версий.

- На сервере Exchange Server прежних версий должен быть включен мобильный Outlook. Дополнительные сведения о включении Outlook Anywhere на серверах Exchange 2010 см. в разделе Включение Outlook Anywhere.

- Для выполнения этой процедуры нельзя использовать Центр администрирования Exchange (EAC) или консоль управления Exchange (EMC). На серверах Exchange прежних версий необходимо использовать командную консоль Exchange. В Exchange Online необходимо использовать Exchange Online PowerShell. Дополнительные сведения см. в статье Connect to Exchange Online PowerShell.

- Для переноса всех данных общедоступных папок необходимо использовать один пакет миграции. Exchange позволяет одновременно создавать только один пакет миграции. При попытке создать несколько пакетов миграции одновременно, результатом будет ошибка.
- Перед началом мы советуем вам полностью прочитать этот раздел, поскольку при выполнении некоторых действий требуется простой.
- Сведения о сочетаниях клавиш, которые могут применяться к процедурам, описанным в этом разделе, см. в разделе Сочетания клавиш для Центра администрирования Exchange.
- Убедитесь, что DefaultPublicFolderAgeLimit настроен на уровне организации (`Get-OrganizationConfig | Format-List DefaultPublicFolderAgeLimit`) или для отдельных общедоступных папок настроен параметр AgeLimit (`Get-PublicFolder <FolderPath> | Format-List AgeLimit`), чтобы предотвратить автоматическое удаление содержимого.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по **адресу Exchange Online** или **Exchange Online Protection**.

Шаг 1. Скачивание сценариев миграции

1. Скачайте все сценарии и сопутствующие файлы со страницы Public Folders Migration Scripts.
2. Сохраните эти сценарии на локальном компьютере, с которого вы собираетесь запускать оболочку PowerShell. (Например, в папку C:\PFScripts). Убедитесь, что все сценарии сохранены в одном и том же месте.
3. Скачайте указанные ниже файлы на странице Общедоступные папки с включенной поддержкой почты: скрипт для синхронизации каталогов.
   - `Sync-MailPublicFolders.ps1`
   - `SyncMailPublicFolders.strings.psd1`
4. Скачайте скрипт проверки на стороне источника по ссылке https://www.microsoft.com/download/confirmation.aspx?id=100414

5. Сохраните скрипты в том же расположении, что и на шаге 2. Например, в папку C:\PFScripts.

Действие 2. Подготовка к миграции

Перед началом миграции выполните указанные ниже предварительные действия.

> ⓘ **Примечание**
>
> Настоятельно рекомендуется запустить скрипт проверки на стороне источника из локального сервера Exchange Server2010 с ролью почтового ящика. Скрипт будет проверять и сообщать о проблемах, которые, как известно, приводят к медленной миграции, а также рекомендации по устранению этих проблем. Используйте примеры, как **описано здесь**.

Общие предварительные условия

- Убедитесь, что в Active Directory нет потерянных почтовых объектов общедоступной папки, то есть объектов без соответствующих им объектов Exchange.
- Убедитесь, что электронный адрес SMTP, настроенный для общедоступных папок в Active Directory, совпадает с электронными адресами SMTP в объектах Exchange.
- Убедитесь, что в Active Directory нет повторяющихся объектов общедоступной папки, чтобы два (или больше) объекта Active Directory не указывали на одну общедоступную папку, поддерживающую почту.

Предварительные действия на сервере Exchange прежней версии

> ⓘ **Примечание**
>
> Настоятельно рекомендуется запустить скрипт проверки на стороне источника из локального сервера Exchange Server2010 с ролью почтового ящика. Скрипт будет проверять и сообщать о проблемах, которые, как известно, приводят к медленной миграции, а также рекомендации по устранению этих проблем. Используйте примеры, как **описано здесь**. Скрипт выполнит все указанные ниже предварительные требования.

1. На сервере Exchange Server прежних версий убедитесь, что маршрутизация к общедоступным папкам с поддержкой почты, которые будут существовать в Microsoft 365, Office 365 или Exchange Online, будет работать до тех пор, пока все кэши DNS через Интернет не будут обновлены, чтобы они указывали на Microsoft 365, Office 365 или Exchange Online DNS, где сейчас находится ваша организация. Для этого выполните следующую команду, чтобы настроить обслуживаемый домен с известным именем, которое будет правильно направлять сообщения электронной почты в домен Microsoft 365, Office 365 или Exchange Online.

```
PowerShell

New-AcceptedDomain -Name
"PublicFolderDestination_78c0b207_5ad2_4fee_8cb9_f373175b3f99" -
DomainName <target domain> -DomainType InternalRelay
```

Пример.

```
PowerShell

New-AcceptedDomain -Name
PublicFolderDestination_78c0b207_5ad2_4fee_8cb9_f373175b3f99 -
DomainName 'contoso.mail.onmicrosoft.com' -DomainType InternalRelay
```

Если в локальной среде уже есть обслуживаемый домен, измените его имя на PublicFolderDestination_78c0b207_5ad2_4fee_8cb9_f373175b3f99 и оставьте остальные атрибуты без изменений.

Чтобы проверить, присутствует ли принятый домен в локальной среде, выполните следующую команду:

```
PowerShell

Get-AcceptedDomain | Where {$_.DomainName -eq "<target domain>"}
```

Чтобы переименовать обслуживаемый домен на PublicFolderDestination_78c0b207_5ad2_4fee_8cb9_f373175b3f99, выполните следующую команду:

```
PowerShell

Get-AcceptedDomain | Where {$_.DomainName -eq "<target domain>"} | Set-
AcceptedDomain -Name
PublicFolderDestination_78c0b207_5ad2_4fee_8cb9_f373175b3f99
```

Если поддерживающие почту общедоступные папки в Exchange Online должны получать внешние письма из Интернета, необходимо отключить DBEB в Exchange Online и Exchange Online Protection (EOP). Дополнительные сведения см. в статье Использование блокировки пограничных адресов на основе каталога для отклонения сообщений, отправленных недопустимым получателям.

Если имя общедоступной папки содержит обратную косую черту (****) или косую черту (**/**), то общедоступные папки могут быть созданы в родительской общедоступной папке при миграции. Перед миграцией рекомендуется переименовать все общедоступные папки с обратной косой чертой или косой чертой в имени.

Чтобы найти общедоступные папки с обратной косой чертой в имени, на сервере Exchange 2010 выполните следующую команду:

```
PowerShell

Get-PublicFolderStatistics -ResultSize Unlimited | Where {($_.Name -
like "*\*") -or ($_.Name -like "*/*") } | Format-List Name,Identity
```

2. Если эта команда возвращает сведения об общедоступных папках, переименуйте их с помощью следующей команды:

```
PowerShell

Set-PublicFolder -Identity <public folder identity> -Name <new public
folder name>
```

3. Убедитесь в отсутствии записи о предыдущей успешной миграции. Если это так, необходимо задать для этого значения значение `$false`. Если задано `$true` значение , запрос на миграцию завершится ошибкой.

   В следующем примере проверяется состояние миграции общедоступных папок.

```
PowerShell

Get-OrganizationConfig | Format-List
PublicFoldersLockedforMigration,PublicFolderMigrationComplete
```

4. (Обратите внимание, что этот шаг необходим только в том случае, если вы повторно пытаетесь выполнить миграцию, которая ранее завершилась

сбоем.) Если состояние свойств *PublicFoldersLockedforMigration* или *PublicFolderMigrationComplete* равно `$true`, выполните следующую команду, чтобы задать значение `$false`.

PowerShell

```
Set-OrganizationConfig -PublicFoldersLockedforMigration:$false -
PublicFolderMigrationComplete:$false
```

> ⊗ **Внимание!**
>
> После сброса этих свойств необходимо дождаться обнаружения новых параметров системой Exchange. На это может потребоваться до двух часов.

5. Для проверки в конце миграции рекомендуем сначала выполнить указанные ниже команды командной консоли Exchange на сервере Exchange прежних версий, чтобы сделать моментальные снимки текущего развертывания общедоступных папок.

   Выполните следующую команду, чтобы сделать моментальный снимок начальной структуры исходных папок.

   PowerShell

   ```
   Get-PublicFolder -Recurse -ResultSize Unlimited | Export-CliXML
   C:\PFMigration\Legacy_PFStructure.xml
   ```

   Выполните следующую команду, чтобы сделать моментальный снимок статистики общедоступных папок, такой как число элементов, размер и владелец.

   PowerShell

   ```
   Get-PublicFolderStatistics -ResultSize Unlimited | Export-CliXML
   C:\PFMigration\Legacy_PFStatistics.xml
   ```

   Выполните следующую команду, чтобы сделать моментальный снимок разрешений.

   PowerShell

```
Get-PublicFolder -Recurse -ResultSize Unlimited | Get-
PublicFolderClientPermission | Select-Object Identity,User -
ExpandProperty AccessRights | Export-CliXML
C:\PFMigration\Legacy_PFPerms.xml
```

Сохраните информацию, полученную в результате выполнения этих команд, для сравнения в конце процесса миграции.

6. Если вы используете Microsoft Azure Active Directory Connect (Azure AD Connect) для синхронизации локальных каталогов с Azure Active Directory, необходимо выполнить следующие действия (если вы не используете Azure AD Connect, этот шаг можно пропустить):

   a. На локальном компьютере откройте Microsoft Azure Active Directory Подключить, а затем выберите **Настроить**.

   b. На экране **Дополнительные задачи** выберите **Настроить параметры синхронизации** и нажмите кнопку **Далее**.

   c. На экране **Подключение к Azure AD** введите соответствующие учетные данные и нажмите кнопку **Далее**. После подключения нажимайте кнопку **Далее** , пока не перейдете на экран **Дополнительные компоненты** .

   d. Убедитесь, что **общедоступные папки почты Exchange** не выбраны. Если он не выбран, можно перейти к следующему разделу Предварительные *требования в Microsoft 365, Office 365 или Exchange Online*. Если он выбран, щелкните, чтобы снять флажок, а затем нажмите кнопку **Далее**.

   > ⓘ **Примечание**
   >
   > Если вы не видите **общедоступные папки Почты Exchange** в качестве параметра на экране **Необязательные компоненты**, вы можете выйти из Microsoft Azure Active Directory Connect и перейти к следующему разделу *Предварительные требования в Microsoft 365, Office 365 или Exchange Online*.

7. После того как вы снимите флажок **Общедоступные папки почты Exchange** , нажимайте кнопку **Далее** , пока не перейдете на экран **Готово к настройке** , а затем нажмите кнопку **Настроить**.

Подробные сведения о синтаксисе и параметрах см. в таких разделах:

- New-AcceptedDomain

- Get-PublicFolder
- Get-PublicFolderDatabase
- Set-PublicFolder
- Get-PublicFolderStatistics
- Get-PublicFolderClientPermission
- Get-OrganizationConfig
- Set-OrganizationConfig

Необходимые действия в Microsoft 365, Office 365 или Exchange Online

1. Убедитесь, что отсутствуют запросы на перенос общедоступных папок. Если они есть, очистите их, иначе выполнить ваш запрос не удастся. Этот шаг не является обязательным во всех случаях. Это необходимо только в том случае, если вы считаете, что в конвейере может существовать запрос на миграцию.

   > ⓘ **Важно!**
   >
   > Перед удалением запроса на миграцию важно понять, почему он существовал. Выполните следующие команды, чтобы определить, когда сделан предыдущий запрос, и обнаружить любые возможные проблемы. Чтобы определить, почему сделано это изменение, может потребоваться консультация с другими администраторами в организации.

   В следующем примере показано, как найти существующие запросы на пакетную миграцию:

   PowerShell

   ```
   $batch = Get-MigrationBatch | ?{$_.MigrationType.ToString() -eq "PublicFolder"}
   ```

   В примере ниже показано удаление существующих запросов на пакетную миграцию общедоступных папок.

   PowerShell

   ```
   $batch | Remove-MigrationBatch -Confirm:$false
   ```

2. Убедитесь, что в Microsoft 365 или Office 365 отсутствуют общедоступные папки или почтовые ящики общедоступных папок.

> ⓘ **Важно!**
>
> Если вы видите общедоступные папки в Microsoft 365, Office 365 или Exchange Online, перед удалением общедоступных папок и почтовых ящиков общедоступных папок важно определить, почему они существуют и кто в вашей организации запустил иерархию общедоступных папок.

a. В Exchange Online PowerShell выполните следующую команду, чтобы узнать, существуют ли почтовые ящики общедоступных папок:

```
PowerShell

Get-Mailbox -PublicFolder
```

b. Если команда не вернула никаких почтовых ящиков общедоступных папок, перейдите на Действие 3. Создание CSV-файлов. Если команда вернула какие-либо почтовые ящики общедоступных папок, запустите следующую команду, чтобы проверить, имеются ли какие-либо общедоступные папки.

```
PowerShell

Get-PublicFolder
```

c. Если у вас есть какие-либо общедоступные папки в Microsoft 365, Office 365 или Exchange Online, выполните следующую команду PowerShell, чтобы удалить их. Убедитесь, что вы сохранили все сведения, которые находились в общедоступных папках в Microsoft 365 или Office 365.

> ⊗ **Внимание!**
>
> При удалении общедоступных папок все данные в них удаляются без возможности восстановления.

```
PowerShell

Get-MailPublicFolder | where {$_.EntryId -ne $null}| Disable-
MailPublicFolder -Confirm:$false
Get-PublicFolder -GetChildren \ | Remove-PublicFolder -Recurse -
Confirm:$false
```

d. После удаления общедоступных папок выполните следующие команды, чтобы удалить все почтовые ящики общедоступных папок.

PowerShell

```
$hierarchyMailboxGuid = $(Get-
OrganizationConfig).RootPublicFolderMailbox.HierarchyMailboxGuid
Get-Mailbox -PublicFolder:$true | Where-Object {$_.ExchangeGuid -ne
$hierarchyMailboxGuid} | Remove-Mailbox -PublicFolder -Confirm:$false
Get-Mailbox -PublicFolder:$true | Where-Object {$_.ExchangeGuid -eq
$hierarchyMailboxGuid} | Remove-Mailbox -PublicFolder -Confirm:$false
```

Подробные сведения о синтаксисе и параметрах см. в следующих статьях.

- Get-MigrationBatch
- Get-PublicFolderMailboxMigrationRequest
- Remove-PublicFolderMailboxMigrationRequest
- Get-Mailbox
- Get-PublicFolder
- get-MailPublicFolder
- Disable-MailPublicFolder
- remove-PublicFolder
- Remove-Mailbox

Шаг 3. Создание CSV-файлов

1. На сервере Exchange Server прежних версий `Export-PublicFolderStatistics.ps1` запустите скрипт, чтобы создать файл сопоставления размера папки с именем папки. Этот скрипт всегда должен выполняться локальным администратором. Этот файл будет иметь два столбца: **FolderName** и **FolderSize**. Значения для столбца **FolderSize** будут отображены в байтах. Например, **\PublicFolder01,10000**.

   PowerShell

   ```
   .\Export-PublicFolderStatistics.ps1  <Folder to size map path> <FQDN of
   source server>
   ```

   - *FQDN of source server* указывает полное доменное имя сервера почтовых ящиков, на котором размещена иерархия общедоступных папок.
   - *Folder to size map path* указывает имя файла и путь к этому файлу в сетевой общедоступной папке, в которой необходимо сохранить CSV-

файл. Далее в этом разделе вам понадобится использовать Exchange Online PowerShell для доступа к этому файлу. Если указать только имя файла, он будет создан в текущем каталоге оболочки PowerShell на локальном компьютере.

- При необходимости, прежде чем продолжить, удалите системные папки, поддерживающие почту, из выходных данных сценария.

2. `PublicFolderToMailboxMapGenerator.ps1` Запустите скрипт, чтобы создать файл сопоставления общедоступных папок с почтовым ящиком. Этот файл используется для вычисления правильного количества почтовых ящиков общедоступных папок в Exchange Online.

```
PowerShell

.\PublicFolderToMailboxMapGenerator.ps1 <Maximum mailbox size in bytes>
<Folder to size map path> <Folder to mailbox map path>
```

   - Перед выполнением скрипта используйте следующую команду, чтобы проверить текущие ограничения общедоступных папок в клиенте Exchange Online. Затем обратите внимание на текущие значения квот для общедоступных папок.

```
PowerShell

Get-OrganizationConfig | Format-List *quota*
```

     В Exchange Online значение по умолчанию — 1,7 ГБ для **DefaultPublicFolderIssueWarningQuota** и 2 ГБ для **DefaultPublicFolderProhibitPostQuota**.

   - *Максимальный размер почтового ящика в байтах* равен максимальному размеру, который необходимо задать для новых почтовых ящиков общедоступных папок. В Exchange Online максимальный размер почтовых ящиков общедоступных папок составляет 100 ГБ. Рекомендуется использовать параметр 75 ГБ, чтобы каждому почтовому ящику общедоступных папок было место для увеличения. Меньшее число почтовых ящиков общедоступных папок будет означать меньше подключений для клиентов Outlook, что может помочь избежать проблем с производительностью; Для пользователей это прозрачно, где размещена информация, так как они будут видеть ту же иерархию на стороне клиента. Exchange Online имеет квоту на 2 ГБ общедоступной папки "Запретить запись" по умолчанию. Если у вас есть отдельные

общедоступные папки размером более 2 ГБ, можно использовать любой из следующих вариантов, чтобы устранить эту проблему:

- Перед запуском пакета миграции увеличьте квоту общедоступной папки по умолчанию "запретить пост", выполнив следующую команду:

```
PowerShell

Set-OrganizationConfig -DefaultPublicFolderProhibitPostQuota <size value> -DefaultPublicFolderIssueWarningQuota <size value>
```

- Перед запуском пакета миграции удалите содержимое общедоступных папок, чтобы уменьшить размер содержимого до 2 ГБ или меньше.
- Перед запуском пакета миграции разделите общедоступную папку на несколько общедоступных папок размером не более 2 ГБ.

> ⓘ **Примечание**
>
> Если размер общедоступной папки превышает 30 ГБ и удалить содержимое или разделить ее на несколько общедоступных папок, рекомендуется не перемещать общедоступные папки в Exchange Online.

- *Путь к карте папки с размером* равен пути к файлу .csv файла, созданного при выполнении скрипта `Export-PublicFolderStatistics.ps1` .
- *Путь к карте папки в почтовый ящик* равен имени файла и пути .csv файла, создаваемого на этом шаге. Если указать только имя файла, файл создается в текущем каталоге PowerShell на локальном компьютере.

> ⓘ **Примечание**
>
> После выполнения скриптов и создания файлов .csv все новые общедоступные папки или обновления существующих общедоступных папок не будут собираться.

Шаг 4. Создание почтовых ящиков общедоступных папок в Exchange Online

Выполните следующую команду, чтобы создать целевые почтовые ящики общедоступной папки. Скрипт создаст целевой почтовый ящик для каждого почтового ящика в файле .csv, созданном ранее на шаге `PublicFoldertoMailboxMapGenerator.ps1` 3, запустив скрипт.

PowerShell

```
.\Create-PublicFolderMailboxesForMigration.ps1 -FolderMappingCsv Mapping.csv
-EstimatedNumberOfConcurrentUsers:<estimate>
```

Mapping.csv — это файл, созданный скриптом на шаге `PublicFoldertoMailboxMapGenerator.ps1` 3. Предполагаемое количество одновременных подключений пользователей, просматривающих иерархию общедоступной папки, обычно меньше, чем общее количество пользователей в организации.

> ⓘ **Примечание**
>
> Используйте Exchange Online PowerShell для запуска этого скрипта. Дополнительные сведения см. в статье **Connect to Exchange Online PowerShell**.

Шаг 5. Запуск запроса на миграцию

1. Выполните следующие действия на сервере Exchange Server, чтобы выполнить необходимые условия для выполнения скрипта *Sync-MailPublicFolders.ps1* .

   a. Войдите с учетной записью, которая имеет разрешения администратора предприятия.

   b. Установите EXO PowerShell. Сведения об установке EXO PowerShell см. здесь.

   c. Запустите PowerShell в режиме администратора.

   d. Выполните следующие команды, чтобы запустить синхронизацию:

   PowerShell

   ```
   Add-PSSnapin *exchange* | .\Sync-MailPublicFolders.ps1 -
   CsvSummaryFile:sync_summary.csv
   ```

   e. После запроса введите учетные данные для учетной записи администратора клиента Microsoft 365.

2. На сервере Exchange прежних версий получите следующие сведения, необходимые для запуска запроса на миграцию.

   a. `LegacyExchangeDN` Найдите учетную запись пользователя, который является членом роли администратора общедоступных папок. Это будет тот же пользователь, чьи учетные данные потребовались на шаге 3 этой процедуры.

   > ⓘ **Примечание**
   >
   > Используемая учетная запись должна быть включена в локальной Exchange Server. Создайте локальный почтовый ящик для учетной записи администратора общедоступных папок, если он там не существует.

   ```
   PowerShell

   Get-Mailbox <PublicFolder_Administrator_Account> | Select-Object LegacyExchangeDN
   ```

   b. `LegacyExchangeDN` Найдите любой сервер почтовых ящиков с базой данных общедоступных папок.

   ```
   PowerShell

   Get-ExchangeServer <public folder server> | Select-Object -Expand ExchangeLegacyDN
   ```

   c. Найдите полное доменное имя для имени узла мобильного Outlook. Если имеется несколько экземпляров мобильного Outlook, рекомендуется выбрать либо экземпляр, находящийся ближе всего к конечной точке миграции, либо экземпляр, находящийся ближе всего к репликам общедоступных папок в устаревшей организации Exchange. С помощью следующей команды можно найти все экземпляры мобильного Outlook.

   ```
   PowerShell

   Get-OutlookAnywhere | Format-Table Identity,ExternalHostName
   ```

3. В Exchange Online PowerShell выполните следующие команды, чтобы передать сведения, возвращенные на предыдущем шаге, в переменные, которые затем будут использоваться в запросе на миграцию.

a. Передайте учетные данные пользователя, имеющего разрешения администратора на сервере Exchange Прежних версий, в переменную `$Source_Credential`. Запрос на миграцию, запущенный в Exchange Online, будет использовать эти учетные данные для получения доступа к серверам Exchange прежних версий для копирования содержимого.

```
PowerShell

$Source_Credential = Get-Credential
<source_domain\PublicFolder_Administrator_Account>
```

b. `ExchangeLegacyDN` Используйте имя пользователя миграции на сервере Exchange, который вы нашли на шаге 2a, и передайте его в переменную `$Source_RemoteMailboxLegacyDN`.

```
PowerShell

$Source_RemoteMailboxLegacyDN = "<paste the value here>"
```

c. `ExchangeLegacyDN` Используйте сервер общедоступных папок, который вы нашли на шаге 2b выше, и передайте его в переменную `$Source_RemotePublicFolderServerLegacyDN`.

```
PowerShell

$Source_RemotePublicFolderServerLegacyDN = "<paste the value here>"
```

d. Используйте имя внешнего узла Outlook Anywhere, которое вы нашли на шаге 2c выше, и передайте его в переменную `$Source_OutlookAnywhereExternalHostName`.

```
PowerShell

$Source_OutlookAnywhereExternalHostName = "<paste the value here>"
```

4. Наконец, в оболочке Exchange Online PowerShell выполните следующие команды, чтобы создать запрос на миграцию.

> ⓘ **Примечание**
>
> Метод проверки подлинности в следующем примере должен соответствовать параметрам Outlook Anywhere. В противном случае

команда завершится с ошибкой.

```
PowerShell

$PfEndpoint = New-MigrationEndpoint -PublicFolder -Name
PublicFolderEndpoint -RPCProxyServer
$Source_OutlookAnywhereExternalHostName -Credentials $Source_Credential
-SourceMailboxLegacyDN $Source_RemoteMailboxLegacyDN -
PublicFolderDatabaseServerLegacyDN
$Source_RemotePublicFolderServerLegacyDN -Authentication Basic
$bytes = [System.IO.File]::ReadAllBytes('folder_mapping.csv')
New-MigrationBatch -Name PublicFolderMigration -CSVData $bytes -
SourceEndpoint $PfEndpoint.Identity -NotificationEmails <email
addresses for migration notifications>
```

Где `folder_mapping.csv` — файл карты, созданный на шаге 3. Создание файлов .csv.

> ⓘ **Примечание**
>
> Вы можете заметить сбой приведенной выше команды с ошибкой "Не удается найти получателя с идентификатором GUID почтового ящика" с указанным идентификатором GUID почтового ящика общедоступных папок в EXO. Это может произойти из-за задержки репликации AD. В этом случае подождите час и повторите команду еще раз.

5. Запустите миграцию, выполнив следующую команду.

```
PowerShell

Start-MigrationBatch PublicFolderMigration
```

Пакетную миграцию необходимо запускать с помощью командлета **New-MigrationBatch** в Командная консоль Exchange, но просматривать ход миграции и управлять им можно в Центре администрирования Exchange. Так как командлет **New-MigrationBatch** инициирует запрос на миграцию почтовых ящиков для каждого почтового ящика общедоступных папок, вы можете просмотреть состояние этих запросов на странице миграции почтовых ящиков. Чтобы перейти на страницу переноса почтовых ящиков и создать отчеты о переносе, доставляемые по электронной почте, выполните следующие действия.

1. Войдите в Exchange Online и откройте Центр администрирования Exchange.

2. Перейдите в раздел**Миграцияпочтовых ящиков**>.

3. Выберите только что созданный запрос на перенос и щелкните **Просмотр сведений** в области **Сведения**.

Подробные сведения о синтаксисе и параметрах см. в следующих разделах:

- Get-Mailbox
- Get-ExchangeServer
- Get-OutlookAnywhere
- New-MigrationBatch
- Get-PublicFolderDatabase
- Get-PublicFolderMailboxMigrationRequest
- Get-PublicFolderMailboxMigrationRequestStatistics

Действие 6. Блокировка общедоступных папок на сервере Exchange предыдущей версии для окончательной миграции (требуется простой в работе)

До этого этапа в процессе миграции у пользователей был доступ к общедоступным папкам. На следующих этапах общедоступные папки прежних версий блокируются для последней синхронизации. В это время пользователи не смогут обратиться к общедоступным папкам. Кроме того, все сообщения, отправленные в общедоступные папки с поддержкой почты, будут занесены в очередь и не будут доставлены до окончания миграции общедоступных папок.

> ⓘ **Примечание**
>
> Окончательная синхронизация может занять значительное время в зависимости от изменений, внесенных в исходную среду, размера развертывания общедоступных папок, емкости сервера и т. д. Если в иерархии папок было много поврежденных списков управления доступом и они не были очищены перед началом миграции, это может привести к значительной задержке при завершении. Рекомендуется запланировать не менее 48 часов простоя для завершения окончательной синхронизации.

Убедитесь, что пакет миграции и отдельные запросы на миграцию успешно синхронизированы.

Выполните следующие команды в Exchange Online PowerShell, чтобы получить подробные сведения:

PowerShell

```
Get-MigrationBatch |?{$_.MigrationType -like "*PublicFolder*"} | Format-Table *last*sync*
```

PowerShell

```
Get-PublicFolderMailboxMigrationRequest | Get-PublicFolderMailboxMigrationRequestStatistics | Format-Table targetmailbox,*last*sync*
```

LastSyncedDate (в пакете миграции) и LastSuccessfulSyncTimestamp (для отдельных заданий) должны находиться в течение последних 7 дней. Если это слишком далеко, например, более месяца или около того, вы можете взглянуть на запросы на миграцию общедоступных папок и убедиться, что все запросы были синхронизированы недавно.

Убедившись, что пакет и все запросы на миграцию успешно синхронизированы, на сервере Exchange Server устаревшей версии выполните следующую команду, чтобы заблокировать устаревшие общедоступные папки для завершения.

PowerShell

```
Set-OrganizationConfig -PublicFoldersLockedForMigration:$true
```

Дополнительные сведения о синтаксисе и параметрах см. в статье set-OrganizationConfig.

Если в вашей организации есть несколько баз данных общедоступных папок, необходимо подождать, пока репликация общедоступных папок не завершится, чтобы убедиться, что все базы данных общедоступных папок подхватили `PublicFoldersLockedForMigration` флаг и все ожидающие изменения, недавно внесенные пользователями в папки, сошлись по всей организации. Это может занять несколько часов.

Шаг 7. Завершение переноса общедоступных папок (требуется простой в работе)

Чтобы завершить миграцию общедоступных папок, выполните следующую команду.

PowerShell

```
Complete-MigrationBatch PublicFolderMigration
```

> ⓘ **Важно!**
>
> После завершения пакета миграции дополнительные данные не могут быть синхронизированы с локальных серверов Exchange и Exchange Online.

После завершения миграции Exchange выполнит окончательную синхронизацию между устаревшим сервером Exchange Server и Exchange Online. Если окончательная синхронизация прошла успешно, общедоступные папки в Exchange Online будут разблокированы, а состояние пакета миграции изменится на **Завершено**. Состояние пакета миграции обычно остается синхронизированным в течение нескольких часов, прежде чем он переключится на Завершение. При миграции с большим количеством целевых почтовых ящиков обычно состояние "Синхронизировано" в течение более 24 часов при условии, что ни один из базовых запросов на миграцию общедоступных папок не завершился сбоем или помещен в карантин.

Если вы настроили гибридное развертывание между локальными серверами Exchange Server и Microsoft 365 или Office 365, выполните следующую команду в Exchange Online PowerShell после завершения миграции:

PowerShell

```
Set-OrganizationConfig -RemotePublicFolderMailboxes $Null -
PublicFoldersEnabled Local
```

Действие 8. Проверка результатов миграции и разблокировка общедоступных папок

После завершения миграции общедоступных папок необходимо выполнить указанную ниже проверку и убедиться, что миграция прошла успешно. Это позволяет протестировать перенесенную иерархию общедоступных папок перед переходом на использование Microsoft 365, Office 365 или Exchange Online общедоступных папок.

1. В Exchange Online PowerShell назначьте некоторые тестовые почтовые ящики, чтобы использовать все недавно перенесенные почтовые ящики общедоступных папок в качестве почтового ящика общедоступных папок по умолчанию.

   PowerShell

   ```
   Set-Mailbox -Identity <Test User> -DefaultPublicFolderMailbox <Public Folder Mailbox Identity>
   ```

2. Войдите в Outlook 2010 или более поздней версии с помощью тестового пользователя, определенного на предыдущем шаге, а затем выполните следующие тесты общедоступных папок:

   - просмотр иерархии;
   - проверка разрешений;
   - создание и удаление общедоступных папок;
   - помещение содержимого в общедоступную папку и его удаление.

3. Если у вас возникнут какие-либо проблемы, см. раздел Откат миграции далее в этой статье. Если содержимое и иерархия общедоступных папок приемлемы и работает должным образом, перейдите к следующему шагу.

4. На сервере Exchange прежних версий выполните приведенную ниже команду, чтобы указать завершение миграции общедоступных папок:

   PowerShell

   ```
   Set-OrganizationConfig -PublicFolderMigrationComplete:$true
   ```

5. Убедившись, что миграция завершена, выполните следующую команду в Exchange Online PowerShell, чтобы убедиться, что параметр *PublicFoldersEnabled* в **Set-OrganizationConfig** имеет значение `Local`:

   PowerShell

   ```
   Set-OrganizationConfig -PublicFoldersEnabled Local
   ```

Подробные сведения о синтаксисе и параметрах см. в таких разделах:

Set-Mailbox

Get-Mailbox

Set-OrganizationConfig

Как проверить, что это работает

В Step 2: Prepare for the migration указывалось, что перед началом миграции необходимо сделать моментальные снимки структуры, статистики и разрешений общедоступных папок. С помощью приведенных ниже действий можно проверить успешность миграции общедоступных папок, сделав такие же моментальные снимки после завершения миграции. Затем можно сравнить данные в обоих файлах, чтобы проверить успешность.

1. В Exchange Online PowerShell выполните следующую команду, чтобы сделать моментальный снимок новой структуры папок.

   ```
   PowerShell

   Get-PublicFolder -Recurse -ResultSize Unlimited | Export-CliXML
   C:\PFMigration\Cloud_PFStructure.xml
   ```

2. В Exchange Online PowerShell выполните следующую команду, чтобы сделать моментальный снимок статистики общедоступных папок, таких как число элементов, размер и владелец.

   ```
   PowerShell

   Get-PublicFolderStatistics | Export-CliXML
   C:\PFMigration\Cloud_PFStatistics.xml
   ```

3. В Exchange Online PowerShell выполните следующую команду, чтобы сделать моментальный снимок разрешений.

   ```
   PowerShell

   Get-PublicFolder -Recurse -ResultSize Unlimited | Get-
   PublicFolderClientPermission | Select-Object Identity,User -
   ExpandProperty AccessRights | Export-CliXML
   C:\PFMigration\Cloud_PFPerms.xml
   ```

Удаление баз данных общедоступных папок с серверов Exchange прежних версий

После окончания миграции и проверки надлежащей работы общедоступных папок Exchange Online, необходимо удалить базы данных общедоступных папок с устаревших серверов Exchange.

> ⓘ **Важно!**
>
> Так как все почтовые ящики были перенесены в Microsoft 365 или Office 365 до переноса общедоступных папок, настоятельно рекомендуется направлять трафик через Microsoft 365 или Office 365 (децентрализованный поток почты), а не через централизованный поток почты через локальную среду. Если вы выберете централизованный поток обработки почты, могут возникнуть ошибки доставки в общедоступные папки, так как в локальной организации удалены базы данных почтовых ящиков для общедоступных папок.

- Дополнительные сведения об удалении баз данных общедоступных папок с серверов Exchange 2010 см. в разделе Удаление баз данных общих папок.

Откат миграции

Если из-за ошибок при переносе необходимо повторно активировать общедоступные папки Exchange прежних версий, выполните следующие действия.

> ⊗ **Внимание!**
>
> Если выполнять откат миграции на серверы Exchange прежних версий, то будут потеряны все сообщения электронной почты, которые отправлены на общедоступные папки, поддерживающие почту, и содержимое, опубликованное в общедоступных папках после миграции. Чтобы сохранить это содержимое, необходимо экспортировать содержимое общедоступных папок в PST-файл, а затем импортировать его в общедоступные папки прежних версий после отката.

1. На сервере Exchange прежних версий выполните следующую команду, чтобы разблокировать общедоступные папки на сервере Exchange прежних версий. Этот процесс может занять несколько часов.

   ```
   
   ```

```
PowerShell

Set-OrganizationConfig -PublicFoldersLockedForMigration:$False
```

2. Чтобы удалить все общедоступные папки Exchange Online, в Exchange Online PowerShell выполните следующие команды.

```
PowerShell

$hierarchyMailboxGuid = $(Get-
OrganizationConfig).RootPublicFolderMailbox.HierarchyMailboxGuid
Get-Mailbox -PublicFolder:$true | Where-Object {$_.ExchangeGuid -ne
$hierarchyMailboxGuid} | Remove-Mailbox -PublicFolder -Confirm:$false -
Force
Get-Mailbox -PublicFolder:$true | Where-Object {$_.ExchangeGuid -eq
$hierarchyMailboxGuid} | Remove-Mailbox -PublicFolder -Confirm:$false -
Force
```

3. На сервере Exchange Server устаревшей версии выполните следующую команду, чтобы установить для флага `PublicFolderMigrationComplete` значение `$false`.

```
PowerShell

Set-OrganizationConfig -PublicFolderMigrationComplete:$False
```

Перенос общедоступных папок в Microsoft 365 или Office 365 с помощью экспорта PST-файлов Outlook

Не рекомендуется использовать функцию экспорта PST в Outlook для переноса общедоступных папок в Microsoft 365, Office 365 или Exchange Online, если локальная иерархия общедоступных папок превышает 30 ГБ. Microsoft 365 и Office 365 рост почтовых ящиков общедоступных папок в Интернете управляется с помощью функции автоматического разделения, которая разделяет почтовый ящик общедоступных папок при превышении квот на размер. Автоматическое разделение не может справиться с внезапным ростом почтовых ящиков общедоступных папок при использовании экспорта PST для переноса общедоступных папок. Возможно, вам придется ждать до двух недель автоматического разделения, чтобы переместить данные из основного почтового ящика. Кроме того, прежде чем использовать PST-приложение Outlook для

экспорта общедоступных папок в Microsoft 365, Office 365 или Exchange Online, рассмотрите следующее.

- Разрешения общих папок будут потеряны в ходе этого процесса. Запишите текущие разрешения перед переносом и вручную добавьте их после его завершения.
- Если вы используете сложные разрешения или переносите большое число папок, мы рекомендуем использовать командлеты.
- Любые изменения элементов или папок в исходных общих папок во время экспорта в PST-файл будут потеряны. Поэтому мы рекомендуем использовать инструкции на основе командлетов, если для процесса экспорта и импорта потребуется много времени.

Если вы все равно хотите переместить общедоступные папки с помощью PST-файлов, выполните следующие действия, чтобы успешно завершить операцию.

1. Следуйте инструкциям в разделе Шаг 1. Загрузка сценариев переноса, чтобы загрузить сценарии переноса. Вам нужно только скачать `PublicFolderToMailboxMapGenerator.ps1` файл.
2. Выполните шаг 2 Действие 3. Создание CSV-файлов, чтобы создать файл сопоставления общедоступных папок и почтовых ящиков. Этот файл используется для вычисления правильного количества почтовых ящиков общедоступных папок в Exchange Online.
3. Создайте необходимые почтовые ящики общедоступных папок на основе файла сопоставления. Дополнительные сведения см. в статье Создание почтового ящика общедоступных папок.
4. Используйте командлет **New-PublicFolder**, чтобы создать общую папку верхнего уровня в каждом почтовом ящике общих папок, с параметром *Mailbox*.
5. Экспорт и импорт PST-файлов с помощью Outlook.
6. Установите разрешения для общих папок с помощью EAC. Дополнительные сведения см. в разделе Шаг 3. Назначение разрешений для общедоступной папки.

⊗ **Внимание!**

Если вы уже начали миграцию PST и сталкивались с проблемой, из-за которой основной почтовый ящик заполнен, у вас есть два варианта восстановления миграции PST. Первый вариант — дождаться, пока автоматическое разделение переместит данные из основного почтового ящика. Это может занять до двух недель. Однако все общедоступные папки в заполненном почтовом ящике общедоступных папок не смогут получать новое содержимое, пока авторазбиение не завершится. Другой вариант — **создать почтовый ящик общедоступных папок** , а затем использовать командлет **New-PublicFolder** с параметром *Mailbox* , чтобы создать остальные общедоступные папки в дополнительном почтовом ящике общедоступных папок.

Устранение неполадок миграции общедоступных папок

Нажмите следующую кнопку для распространенных проблем во время миграции общедоступных папок:

Выполнение тестов: устранение неполадок с переносом общедоступных папок

Откроется всплывающее окно в Центр администрирования Microsoft 365, войдите с помощью учетной записи администратора клиента и выберите соответствующий параметр.

Перенос общедоступных папок из Exchange 2013 в Exchange 2016 или Exchange 2019

Статья • 04.04.2023

Чтобы перенести общедоступные папки Exchange 2013 в Exchange 2016 или Exchange 2019, необходимо переместить все почтовые ящики общедоступных папок Exchange 2013 на сервер Exchange 2016 или Exchange 2019.

Перед перемещением почтовых ящиков общедоступных папок следует учесть ряд моментов:

- **Емкость**. Размер почтовых ящиков общедоступных папок может значительно отличаться в зависимости от количества общедоступных папок и почтовых ящиков общедоступных папок. Убедитесь, что целевые серверы Exchange, на которые будут перемещаться почтовые ящики общедоступных папок, имеют достаточный объем хранилища.

- **Время**. Перемещение почтовых ящиков общедоступных папок может занять некоторое время. Следующие элементы могут повлиять на то, сколько времени это займет:

- Размер почтового ящика общедоступной папки

- Количество почтовых ящиков общедоступных папок

- Сетевой диапазонсов

Хорошая новость заключается в том, что общедоступные папки останутся доступными во время перемещения их почтовых ящиков. Существует только краткое временное окно, в котором общедоступные папки могут быть недоступны (по мере завершения перемещения).

Что нужно знать перед началом работы

- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование командной консоли Exchange для перемещения почтовых ящиков общедоступных папок из Exchange 2013 в Exchange 2016 или Exchange 2019

1. Выполните следующую команду, чтобы получить список всех почтовых ящиков общедоступных папок Exchange 2013:

   PowerShell

   ```
   Get-ExchangeServer | Where {($_.AdminDisplayVersion -Like 'Version 15.0*') -And ($_.ServerRole -Like '*Mailbox*')} | Get-Mailbox -PublicFolder | Get-MailboxStatistics | Format-Table -Auto ServerName,DisplayName,TotalItemSize
   ```

2. Используйте следующий синтаксис для вывода списка всех баз данных почтовых ящиков на всех серверах почтовых ящиков Exchange 2016 или Exchange 2019:

   PowerShell

   ```
   Get-ExchangeServer | Where {($_.AdminDisplayVersion -like '<Version>') -and ($_.ServerRole -Like "*Mailbox*")} | Get-MailboxDatabase | Format-List Server,Name,EdbFilePath
   ```

   Сведения о расположении, возвращаемые этой командой, можно использовать для проверки свободного места на диске для каждой базы данных почтовых ящиков.

   В этом примере возвращаются расположения всех баз данных почтовых ящиков на всех серверах почтовых ящиков Exchange 2016.

   PowerShell

   ```
   Get-ExchangeServer | where {($_.AdminDisplayVersion -like 'Version 15.1*') -and ($_.ServerRole -Like '*Mailbox*')} | Get-MailboxDatabase |
   ```

```
Format-List Server,Name,EdbFilePath
```

В этом примере возвращаются расположения всех баз данных почтовых ящиков на всех серверах почтовых ящиков Exchange 2019.

PowerShell

```
Get-ExchangeServer | where {($_.AdminDisplayVersion -like 'Version 15.2*') -and ($_.ServerRole -Like '*Mailbox*')} | Get-MailboxDatabase | Format-List Server,Name,EdbFilePath
```

В этом примере возвращаются расположения всех баз данных почтовых ящиков на всех серверах почтовых ящиков Exchange 2016 и Exchange 2019.

PowerShell

```
Get-ExchangeServer | where {(($_.AdminDisplayVersion -like 'Version 15.1*') -or ($_.AdminDisplayVersion -like 'Version 15.2*')) -and ($_.ServerRole -Like '*Mailbox*')} | Get-MailboxDatabase | Format-List Server,Name,EdbFilePath
```

3. Используйте сведения из предыдущих шагов, чтобы выбрать целевую базу данных почтовых ящиков и (или) сервер почтовых ящиков (если у вас несколько) для перемещения некоторых или всех почтовых ящиков общедоступных папок. Например, не стоит перемещать три больших почтовых ящика общедоступных папок на сервер, на котором осталось мало места на диске.

   Кроме того, можно решить, следует ли перемещать все почтовые ящики общедоступных папок сразу, все почтовые ящики общедоступных папок на один конкретный сервер или один конкретный почтовый ящик общедоступных папок.

   Выберите команду, которая подходит для требуемого типа перемещения. Обязательно замените имена серверов Exchange, имена баз данных и почтовых ящиков общедоступных папок собственными.

   - Переместите сразу все почтовые ящики общедоступных папок Exchange 2013.

     PowerShell

     ```
     Get-ExchangeServer | Where {($_.AdminDisplayVersion -Like "Version 15.0*") -And ($_.ServerRole -Like "*Mailbox*")} | Get-Mailbox -PublicFolder | New-MoveRequest -TargetDatabase Ex2016MbxDatabase
     ```

- Переместите сразу все почтовые ящики общедоступных папок на конкретном сервере Exchange 2013.

```
PowerShell

Get-Mailbox -PublicFolder -Server Ex2013Mbx | New-MoveRequest -
TargetDatabase Ex2016MbxDatabase
```

- Переместите конкретный почтовый ящик общедоступных папок Exchange 2013.

```
PowerShell

New-MoveRequest "Sales Public Folder Mailbox" -TargetDatabase
Ex2016MbxDatabase
```

4. Чтобы просмотреть состояние созданных запросов на перемещение, выполните следующую команду:

```
PowerShell

Get-MoveRequest
```

В зависимости от размера перемещаемых почтовых ящиков общедоступных папок и доступной пропускной способности сети перемещение может занять несколько часов или даже дней.

Список возможных значений состояния, которые можно вернуть, см. в следующем разделе.

Как проверить, все ли получилось?

Чтобы убедиться, что все общедоступные папки Exchange 2013 успешно перенесены в Exchange 2016 или Exchange 2019, выполните следующие действия.

- Проверьте состояние созданных запросов на перемещение, выполнив следующую команду в командной консоли Exchange на сервере почтовых ящиков Exchange 2016 или Exchange 2019:

```
PowerShell

Get-MoveRequest
```

Команда возвращает каждый созданный запрос на перемещение вместе с одним из следующих значений состояния:

- **Завершено**. Почтовый ящик общедоступной папки успешно перемещен в целевую базу данных почтовых ящиков.
- **CompletedWithWarning**: почтовый ящик общедоступной папки был перемещен в целевую базу данных почтовых ящиков, но во время перемещения возникла одна или несколько проблем. Дополнительные сведения можно просмотреть в отчете о перемещении, доставленном в почтовый ящик администратора.
- **CompletionInProgress**: перемещение почтового ящика общедоступной папки в целевую базу данных почтового ящика находится на завершающем этапе. Общедоступные папки, размещенные в этом почтовом ящике, могут быть недоступны на короткий промежуток времени до завершения перемещения.
- **InProgress**: выполняется перемещение почтового ящика общедоступной папки в целевую базу данных почтовых ящиков. Общедоступные папки, размещенные в этом почтовом ящике, доступны во время этого этапа перемещения.
- **Сбой**: перемещение почтового ящика общедоступных папок завершилось сбоем по одной или нескольким причинам. Дополнительные сведения можно просмотреть в отчете о перемещении, доставленном в почтовый ящик администратора.
- **В очереди**: перемещение почтового ящика общедоступных папок отправлено, но перемещение еще не началось.
- **Повторная попытка**. В настоящее время у службы миграции возникают проблемы с выполнением задания, но она не сдалась и будет продолжать попытки.
- **AutoSuspended**. Перемещение почтового ящика общедоступных папок готово к переходу на заключительные этапы, но не будет продолжаться дальше, пока вы не возобновите перемещение вручную.

  Этот параметр может быть полезен, если вы хотите выбрать время завершения перемещения. Вы можете автоматически приостановить перемещение при его создании с помощью параметра *SuspendWhenReadyToComplete* в **командлете New-MoveRequest** . Чтобы

возобновить перемещение, воспользуйтесь командлетом **Resume-MoveRequest**, когда будете готовы.

- **Приостановлено**. Перемещение почтового ящика общедоступных папок было приостановлено вручную с помощью командлета **Suspend-MoveRequest** и не будет продолжаться, пока вы не возобновите перемещение вручную. Чтобы возобновить перемещение, воспользуйтесь командлетом **Resume-MoveRequest**, когда будете готовы.

- Просмотрите расположение почтовых ящиков общедоступных папок после выполнения запроса на перемещение, выполнив следующую команду на сервере Exchange 2016 или Exchange 2019:

  PowerShell

  ```
  Get-Mailbox -PublicFolder | Get-MailboxStatistics | Format-Table ServerName,DisplayName,TotalItemSize
  ```

  В списке возвращаемых значений для почтовых ящиков общедоступных папок проверьте, все ли они перемещены на сервер почтовых ящиков Exchange 2016.

Настройка общедоступных папок в новой организации

Статья • 04.04.2023

Общедоступные папки в Exchange основаны на архитектуре почтовых ящиков, которая позволяет общедоступным папкам воспользоваться такими преимуществами, как устойчивость группы доступности баз данных (DAG) и другие функции почтовых ящиков.

Ограничения в локальных Exchange Server см. в разделе Ограничения для общедоступных папок.

Дополнительные задачи управления, связанные с общедоступными папками в Exchange Server, см. в разделе Процедуры общедоступных папок.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 30 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Общедоступные папки" в разделе Разрешения для общего доступа и совместной работы .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Действие 1. Создайте почтовый ящик основного общих папок

Почтовый ящик основной общедоступной папки содержит доступную для записи копию иерархии общедоступных папок, а также содержимое и является первым почтовым ящиком общедоступных папок, который вы создаете для своей

организации. Последующие почтовые ящики общедоступных папок будут дополнительными почтовыми ящиками общедоступных папок, которые будут содержать только для чтения копию иерархии и содержимого.

Подробные инструкции см. в статье Создание почтового ящика общедоступных папок.

Действие 2. Создание ваш первый общей папки

Подробные инструкции см. в статье Создание общедоступной папки.

Действие 3. Назначить разрешения для общей папки

После создания общедоступной папки необходимо назначить уровень разрешений **владельца** , чтобы хотя бы один пользователь смог получить доступ к общедоступной папке из клиента и создать вложенные папки. Все общие папки, созданные после этого один наследуют разрешения родительской общей папке.

1. В Центре администрирования Exchange перейдите в раздел **Общедоступные папки**>**Общедоступные папки**.
2. В представлении списка выберите общую папку.
3. В области сведений в разделе **Разрешения папки** щелкните **Управление**.
4. В **разделе Разрешения общедоступных папок** нажмите кнопку **Добавить**➕
5. Нажмите кнопку **Обзор**, чтобы выбрать местоположение.
6. В **уровень разрешений** список, выберите уровень. По крайней мере один пользователь должен быть **владелец**.
7. Щелкните **Сохранить**.
8. Вы можете добавить несколько пользователей, щелкнув ➕ и назначив соответствующие разрешения, выполнив описанные выше действия. Кроме того, можно настроить уровень доступа, установив или сняв ее флажок. При изменении предварительно определенный уровень разрешений например **владелец** , уровень разрешений будет **обычай** .

Сведения об использовании командной консоли Exchange для назначения разрешений общедоступной папке см. в разделе Add-PublicFolderClientPermission.

Действие 4 (дополнительно). Включение поддержки электронной почты для общедоступной папки

Если требуется разрешить пользователям отправлять сообщения в общедоступную папку, можете включить для нее поддержку электронной почты. Это действие необязательно. Если вы не включите общедоступную папку для почты, пользователи могут публиковать сообщения в общедоступной папке, перетаскивая в нее элементы из Outlook.

1. В EAC перейдите в раздел **Общедоступные папки**>**Общедоступные папки**.
2. В представлении списка, выберите общую папку, для которой необходимо включить поддержку почты.
3. В области сведений в разделе **Параметры почты — отключено** нажмите кнопку **Включить**.

   Появится предупреждение с запросом на включение почты для общедоступной папки. Нажмите кнопку **Да**.

Общая папка с включенной поддержкой почты будет и имя общей папки станут псевдоним общей папки. Если у вас есть несколько получателей с этим именем, псевдоним общедоступной папки будет добавлен с числом. Например, если имеется группа рассылки с именем SalesTeam и создании общих папок и затем названный SalesTeam включить для нее поддержку почты всего, псевдоним будет SalesTeam1 этой общей папки.

Сведения об использовании командной консоли Exchange для включения почты в общедоступной папке см. в разделе Enable-MailPublicFolder.

Создание почтового ящика общедоступных папок в Exchange Server

Статья • 04.04.2023

Прежде чем создать общедоступную папку в Exchange Server, необходимо сначала создать почтовый ящик общедоступной папки. Почтовые ящики общедоступных папок содержат сведения об иерархии, а также содержимое общедоступных папок.

Первый почтовый ящик общедоступных папок, создаваемый в организации, — это основной почтовый ящик иерархии, который содержит единственную доступную для записи копию иерархии общедоступных папок. Все дополнительные почтовые ящики общедоступных папок, которые вы создаете, являются почтовыми ящиками вторичной иерархии, которые содержат только для чтения копию иерархии общедоступных папок. Для балансировки нагрузки можно создать несколько почтовых ящиков общедоступных папок.

> ⓘ **Примечание**
>
> Дополнительные сведения о квотах и ограничениях хранилища для общедоступных папок в локальной среде Exchange см. в разделе **Ограничения для общедоступных папок**.

Дополнительные задачи управления, связанные с общедоступными папками в Exchange Server, см. в разделе Процедуры общедоступных папок.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: менее 5 минут.
- Общедоступные папки на серверах Exchange 2010 не могут существовать в одной организации с общедоступными папками Exchange 2016 или более поздних версий. При попытке создать почтовый ящик общедоступной папки, если имеются устаревшие общедоступные папки, появится ошибка **Обнаружено существующее развертывание общедоступных папок. Чтобы перенести данные из существующих общедоступных папок, создайте новый почтовый ящик общедоступных папок с помощью параметра -HoldForMigration.**

Перед созданием общедоступных папок в Exchange Server 2016 или более поздней версии необходимо перенести общедоступные папки Exchange 2010, выполнив действия, описанные в разделе Использование пакетной миграции для переноса общедоступных папок из Exchange 2010 в Exchange 2016.

- Сведения о перемещении почтовых ящиков общедоступных папок из Exchange 2013 в Exchange 2016 или Exchange 2019 см. в статье Перенос общедоступных папок из Exchange 2013 в Exchange 2016 или Exchange 2019.
- Дополнительные сведения о Центре администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Общедоступные папки" в разделе Разрешения для общего доступа и совместной работы .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование Центра администрирования Exchange для создания почтового ящика общедоступных папок

1. В EAC перейдите в раздел **Общедоступные папки** > **Почтовые ящики общедоступных папок** и нажмите кнопку **Добавить** ➕
2. На открывающейся странице **Новый почтовый ящик общедоступной папки** введите следующие сведения:
   - **Имя**. Введите имя почтового ящика общедоступной папки.

- **Подразделение**. Нажмите кнопку **Обзор** , чтобы выбрать расположение в Active Directory, где создается объект почтового ящика.
- **База данных почтовых ящиков**. Нажмите кнопку **Обзор** , чтобы выбрать базу данных почтовых ящиков, в которой создается почтовый ящик.

По завершении нажмите кнопку **Сохранить**.

Создание почтового ящика общедоступных папок с помощью командной консоли Exchange

Чтобы создать почтовый ящик общедоступных папок, используйте следующий синтаксис:

PowerShell

```
New-Mailbox -PublicFolder -Name <Name>
```

В этом примере создается почтовый ящик общедоступной папки основной иерархии с именем Master Hierarchy, так как это первый почтовый ящик общедоступных папок в организации (значение параметра *Name* не определяет, является ли почтовый ящик основным почтовым ящиком общедоступных папок иерархии).

PowerShell

```
New-Mailbox -PublicFolder -Name "Master Hierarchy"
```

В этом примере создается почтовый ящик общедоступной папки вторичной иерархии с именем Istanbul, так как это не первый почтовый ящик общедоступных папок в организации (значение параметра *Name* не определяет, является ли почтовый ящик дополнительным почтовым ящиком общедоступных папок иерархии).

PowerShell

```
New-Mailbox -PublicFolder -Name Istanbul
```

Дополнительные сведения о синтаксисе и параметрах см. в статье New-Mailbox.

Как проверить, все ли получилось?

Чтобы убедиться, что почтовый ящик общедоступной папки успешно создан, выполните одно из следующих действий:

- В EAC перейдите в раздел **Общедоступные папки**>**Почтовые ящики общедоступных папок** и убедитесь, что почтовый ящик общедоступных папок указан в списке. Почтовый ящик общедоступной папки первичной иерархии имеет значение **Primary Hierarchy** для свойства **Contains** . Все остальные почтовые ящики общедоступных папок имеют значение **Secondary Hierarchy** для свойства **Contains** .

- В командной консоли Exchange выполните следующую команду, чтобы убедиться, что почтовый ящик указан в списке, и проверьте значение свойства **IsRootPublicFolderMailbox** , чтобы узнать, является ли почтовый ящик основным почтовым ящиком общедоступных папок иерархии (`True`) или дополнительным почтовым ящиком общедоступных папок иерархии (`False`):

  PowerShell

  ```
  Get-Mailbox -PublicFolder | Format-Table -Auto
  Name,ServerName,Database,IsRootPublicFolderMailbox
  ```

- В командной консоли Exchange выполните следующие команды, чтобы проверить основной почтовый ящик общедоступных папок иерархии:

  1. Выполните следующую команду:

     PowerShell

     ```
     Get-OrganizationConfig | Format-List RootPublicFolderMailbox
     ```

  2. Используйте значение GUID, возвращаемое первой командой **get-Mailbox** , чтобы подтвердить имя почтового ящика. Чтобы скопировать значение GUID, щелкните правой кнопкой мыши в окне командной консоли Exchange, выберите **Пометить**, выделите значение GUID и нажмите клавишу ВВОД.

     PowerShell

     ```
     Get-Mailbox -PublicFolder -Identity <GUID>
     ```

Создание общедоступной папки

Статья • 04.04.2023

Общие папки предназначены для осуществления общего доступа к файлам. Это простой и эффективный способ сбора, организации и использования информации внутри рабочей группы или в масштабах всей организации.

По умолчанию общая папка наследует параметры родительской папки, включая параметры разрешений.

Дополнительные сведения о задачах управления, связанных с общедоступными папками, см. в разделе Процедуры с общедоступными папками.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Общедоступные папки" в разделе Разрешения для общего доступа и совместной работы.
- Вы не можете создать общедоступную папку, если только вы не создали почтовый ящик общедоступной папки. Дополнительные сведения о создании почтового ящика общедоступных папок см. в разделе Создание почтового ящика общедоступной папки.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Использование Центра администрирования Exchange (EAC) для создания общедоступной папки

При создании общей папки в EAC можно указать только имя и путь к общей папке. Чтобы настроить дополнительные параметры, нужно отредактировать общедоступную папку после ее создания.

1. Перейдите в раздел **Общедоступные папки**>**Общедоступные папки**.

2. Если необходимо создать общедоступную папку в качестве дочерней к существующей общедоступной папке, выберите последнюю в списке. Чтобы создать общую папку верхнего уровня, пропустите этот шаг.
3. Щелкните **Добавить**➕
4. В разделе **Общедоступная папка** введите имя общедоступной папки.

   > ⓘ **Важно!**
   >
   > Не используйте обратную косую черту () в имени при создании общедоступной папки.

5. В поле **Путь** проверьте путь к общедоступной папке. Если нет требуемого пути, нажмите кнопку **Отмена** и выполните действие 2 данной процедуры.
6. Щелкните **Сохранить**.

Использование командной консоли Exchange для создания общедоступной папки

В этом примере создается общедоступная папка Reports по пути Marketing\2016.

PowerShell

```
New-PublicFolder -Name Reports -Path \Marketing\2016
```

> ⓘ **Важно!**
>
> Не используйте обратную косую черту () в имени при создании общедоступной папки.

Подробные сведения о синтаксисе и параметрах см. в разделе New-PublicFolder.

Как проверить, все ли получилось?

Чтобы убедиться в том, что общая папка успешно создана, выполните следующие действия:

- В EAC щелкните **Обновить** для обновления списка общих папок. В списке отобразится новая общедоступная папка.
- Выполните любую из следующих команд в командной консоли Exchange:

```
PowerShell
Get-PublicFolder -Identity \Marketing\2016\Reports | Format-List
```

```
PowerShell
Get-PublicFolder -Identity \Marketing\2016 -GetChildren
```

```
PowerShell
Get-PublicFolder -Recurse
```

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Включение и отключение поддержки почты для общедоступной папки

Статья • 04.04.2023

Общие папки предназначены для осуществления общего доступа к файлам. Это простой и эффективный способ сбора, организации и использования информации внутри рабочей группы или в масштабах всей организации. Включите поддержку почты для общедоступной папки, чтобы пользователи могли публиковать в ней файлы, отправляя их по электронной почты. Если для общедоступной папки включена поддержка почты, в Центре администрирования Exchange для нее становятся доступны дополнительные параметры, например адреса электронной почты и почтовые квоты. Если поддержка почты не включена, для управления параметрами общедоступной папки в командной консоли используется командлет **Set-PublicFolder**. Если же она включена, для этого используются командлеты **Set-PublicFolder** и **Set-MailPublicFolder**.

Чтобы пользователи могли по Интернету отправлять сообщения в общедоступную папку с включенной поддержкой почты, необходимо задать дополнительные разрешения с помощью командлета **Add-PublicFolderClientPermission**.

Дополнительные сведения о задачах, связанных с управлением общедоступными папками, см. в статье Процедуры с общедоступными папками.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Чтобы пользователи могли отправлять сообщения в общедоступную папку с поддержкой почты через Интернет, анонимной учетной записи должно быть предоставлено по крайней мере право доступа *CreateItems*. Дополнительные сведения см. в разделе Как разрешить анонимным пользователям отправлять почту в общедоступную папку с поддержкой почты далее в этой статье.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Общедоступные папки" в разделе Разрешения для общего доступа и совместной работы .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Включение или отключение поддержки почты для общедоступной папки с помощью Центра администрирования Exchange

1. Перейдите в раздел **Общедоступные папки**>**Общедоступные папки**.
2. В представлении списка выберите общедоступную папку, для которой нужно включить или отключить поддержку почты.
3. В области сведений в разделе **Настройки почты** щелкните **Включить** или **Отключить**.
4. Появится окно с предупреждением о том, хотите ли вы включить или отключить электронную почту для общедоступной папки. Чтобы продолжить, нажмите кнопку **Да**.

Чтобы внешние пользователи могли отправлять сообщения в эту общедоступную папку, обязательно выполните действия, приведенные в разделе Предоставление анонимным пользователям разрешения на отправку сообщений в общедоступную папку с включенной поддержкой почты.

Включение поддержки почты для общедоступной папки с помощью командной консоли Exchange

В этом примере включается поддержка почты для общедоступной папки Help Desk.

PowerShell

```
Enable-MailPublicFolder -Identity "\Help Desk"
```

В этом примере включается поддержка почты для общедоступной папки Reports в родительской папке Marketing, но папка скрывается в списках адресов.

PowerShell

```
Enable-MailPublicFolder -Identity "\Marketing\Reports" -
HiddenFromAddressListsEnabled $True
```

Чтобы внешние пользователи могли отправлять сообщения в эту общедоступную папку, обязательно выполните действия, приведенные в разделе Предоставление анонимным пользователям разрешения на отправку сообщений в общедоступную папку с включенной поддержкой почты.

Подробные сведения о синтаксисе и параметрах см. в разделе Enable-MailPublicFolder.

Отключение поддержки почты для общедоступной папки с помощью командной консоли Exchange

В этом примере отключается поддержка почты для общедоступной папки Marketing\Reports.

PowerShell

```
Disable-MailPublicFolder -Identity "\Marketing\Reports"
```

Подробные сведения о синтаксисе и параметрах см. в разделе Disable-MailPublicFolder.

Предоставление анонимным пользователям разрешения на отправку сообщений в общедоступную папку с включенной поддержкой почты

Установить разрешения для анонимной учетной записи общедоступной папки можно с помощью Outlook или командной консоли Exchange. Установить разрешения для анонимной учетной записи с помощью Центра администрирования Exchange нельзя.

Задание разрешений для анонимной учетной записи с помощью Outlook

1. Откройте Outlook с учетной записи, которой предоставлены разрешения владельца для общедоступной папки с включенной поддержкой электронной почты, в которую будут отправлять сообщения анонимные пользователи.
2. Перейдите к разделу **Общедоступные папки — <имя_пользователя>**.
3. Перейдите в общедоступную папку, которую требуется изменить.
4. Щелкните общедоступную папку правой кнопкой мыши, нажмите кнопку **Свойства**, а затем выберите вкладку **Разрешения**.
5. Выберите **анонимную** учетную запись, щелкните **Создание элементов** в разделе **Запись**, а затем нажмите кнопку **OK**.

Задание разрешений для анонимной учетной записи с помощью командной консоли Exchange

В этом примере задается `CreateItems` разрешение для анонимной учетной записи в общедоступной папке "Отзывы клиентов" с поддержкой почты.

PowerShell

```
Add-PublicFolderClientPermission "\Customer Feedback" -AccessRights
CreateItems -User Anonymous
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе Add-PublicFolderClientPermission.

Просмотр статистики для общедоступных папок и их элементов

Статья • 02.06.2023

С помощью командной консоли Exchange можно получить статистику по общедоступной папке, например отображаемое имя, время создания, время последнего изменения пользователя и размер элемента. Эти сведения можно использовать для принятия решений об удалении или сохранении общедоступных папок.

> **Примечание**
>
> Хотя некоторые сведения о квотах и использовании можно просмотреть в Центре администрирования Exchange (EAC), эти сведения являются неполными, и рекомендуется использовать командную консоль Exchange для просмотра статистики общедоступных папок. Чтобы просмотреть сведения о квоте и использовании общедоступных папок, перейдите к **общедоступных папок**>.>**Использование почтового ящика**.

Дополнительные сведения о задачах управления, связанных с общедоступными папками, см. в разделе Public Folder Procedures in Exchange Online.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 1 минута.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Общедоступные папки" в разделе Разрешения для общего доступа и совместной работы .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Получение статистики общедоступных папок с помощью командной консоли Exchange

В этом примере показано, как вернуть статистику для общей папки "Маркетинг" с помощью переданной по конвейеру команды для форматирования списка.

PowerShell

```
Get-PublicFolderStatistics -Identity \Marketing | Format-List
```

> **Примечание**
>
> Значение параметра *Identity* должно содержать путь к общедоступной папке. Например, если общедоступная папка Marketing существовала в родительской папке Business, необходимо указать следующее значение: `\Business\Marketing`

Подробные сведения о синтаксисе и параметрах см. в разделе Get-PublicFolderStatistics.

Обратите внимание, что некоторые параметры и параметры могут быть доступны только в Exchange Online или только в Exchange Server.

Использование командной консоли Exchange для просмотра статистики по элементам общедоступных папок

Можно просматривать следующие сведения об элементах в общедоступной папке.

- Тип элемента
- Тема
- Время последнего изменения
- Время создания
- Вложения
- Размер сообщения

В этом примере выполняется возвращение статистики по умолчанию для всех элементов в общедоступной папке Pamphlets по пути \Marketing\2013. К сведениям по умолчанию относятся идентификатор элемента, время создания и тема.

PowerShell

```
Get-PublicFolderItemStatistics -Identity "\Marketing\2013\Pamphlets"
```

В этом примере выполняется возвращение дополнительных сведений об элементах в общедоступной папке Pamphlets, таких как тема, время последнего изменения и создания, вложения, размер сообщения и тип элемента. Этот пример также включает переданную команду для форматирования списка.

PowerShell

```
Get-PublicFolderItemStatistics -Identity "\Marketing\2010\Pamphlets" |
Format-List
```

Подробные сведения о синтаксисе и параметрах см. в разделе Get-PublicFolderItemStatistics.

Обратите внимание, что некоторые параметры и параметры могут быть доступны только в Exchange Online или только в Exchange Server.

Экспорт выходных данных командлета Get-PublicFolderItemStatistics в файл .csv с помощью командной консоли Exchange

В этом примере полученные с помощью командлета данные экспортируются в файл PFItemStats.csv, который содержит следующие сведения о всех элементах общедоступной папки \Marketing\Reports.

- Тема сообщения (`Subject`)
- Дата и время последнего изменения элемента (`LastModificationTime`)
- Содержит ли элемент вложения (`HasAttachments`)
- Тип элемента (`ItemType`)
- Размер элемента (`MessageSize`)

```
```

PowerShell

```
Get-PublicFolderItemStatistics -Identity "\Marketing\Reports" | Select
Subject,LastModificationTime,HasAttachments,ItemType,MessageSize | Export-
CSV C:\PFItemStats.csv
```

Подробные сведения о синтаксисе и параметрах см. в разделе Get-PublicFolderItemStatistics.

Общие почтовые ящики в Exchange Server

Статья • 04.04.2023

Общий почтовый ящик — это почтовый ящик, который могут использовать несколько пользователей. Общие почтовые ящики также предоставляют общий календарь, что позволяет нескольким пользователям планировать и просматривать даты отпуска и рабочих смен.

Общий почтовый ящик — это почтовый ящик, который могут использовать несколько пользователей. Общие почтовые ящики также предоставляют общий календарь, что позволяет нескольким пользователям планировать и просматривать даты отпуска и рабочих смен.

- Предоставляет универсальный адрес электронной почты (например, info@contoso.com или sales@contoso.com), который клиенты могут использовать для получения сведений о вашей компании.
- Они обеспечивают общий адрес электронной почты (например, info@contoso.com или sales@contoso.com), с помощью которого клиенты будут узнавать вашу компанию.
- Они позволяют отделам, предоставляющим сотрудникам организации централизованные услуги (например, службе поддержки, отделу кадров или отделу печати), отвечать на запросы.

Сведения об общих почтовых ящиках

Общий почтовый ящик — это тип почтового ящика пользователя, который не имеет собственного имени пользователя и пароля. В результате пользователи не могут войти в них напрямую. Чтобы пользователи могли получить доступ к общему почтовому ящику, им сначала необходимо предоставить разрешение "Отправить как" или "Полный доступ" для ящика. После этого пользователи входят в собственные почтовые ящики, а затем получают доступ к общему почтовому ящику путем его добавления в свой профиль Outlook. В Exchange 2003 и более ранних версиях общие почтовые ящики представляли собой обычные почтовые ящики, к которым администратор мог предоставить делегированный доступ. Начиная с Exchange 2007, у общих почтовых ящиков появился собственный тип получателя:

- **RecipientType**: UserMailbox
- **RecipientTypeDetails**: SharedMailbox

В предыдущей версии Exchange создание общего почтового ящика проходило в несколько этапов и предполагало использование командной консоли Exchange для выполнения некоторых задач. В Exchange 2013 и более поздних версиях можно использовать Центр администрирования Exchange (EAC) для создания общего почтового ящика за один шаг. Дополнительные сведения см. в статье Создание общих почтовых ящиков в Центре администрирования Exchange. В Центре администрирования Exchange есть функциональная область, специально предназначенная для общих почтовых ящиков. Просто перейдите в раздел **Получатели**>**Общие почтовые ящики** , чтобы просмотреть все задачи управления для общих почтовых ящиков.

Перед внесением изменений в записи DNS настоятельно рекомендуем максимально снизить значение срока жизни для каждой записи DNS. Значение срока жизни определяет, как долго запись DNS остается в кэше на серверах DNS. Меньший интервал, например 5–10 минут, позволит быстрее отменить любые изменения события, для которого необходимо вернуть исходную конфигурацию. Если вам действительно необходимо изменить значение срока жизни для ваших записей DNS, не вносите другие изменения, пока не истечет исходный интервал.

- **Полный доступ**. Разрешение полный доступ позволяет пользователю войти в общий почтовый ящик и действовать в качестве владельца этого почтового ящика. После входа в систему пользователь может создавать элементы календаря; читать, просматривать, удалять и изменять сообщения электронной почты; создавать задачи и вести календарь контактов. Тем не менее, пользователь с разрешением на полный доступ не может отправлять электронную почту из общего почтового ящика, если у него нет также разрешения "Отправить как" или "Отправить от имени".

- **Отправить как**. Разрешение "Отправить как" позволяет пользователю олицетворять общий почтовый ящик при отправке почты. Например, если Сергей войдет в общий почтовый ящик отдела маркетинга и отправит электронное сообщение, оно будет выглядеть так, будто отправителем был отдел маркетинга.

- **Отправить от имени.** Разрешение "Отправить от имени" позволяет пользователю отправлять электронную почту от имени общего почтового ящика. Например, если Джон входит в общий почтовый ящик Reception Building 32 и отправляет сообщение электронной почты, это будет выглядеть так, как будто сообщение было отправлено "Джон от имени здания ресепшн

32". Вы не можете использовать EAC для предоставления разрешений Отправить от имени. Необходимо использовать командлет **Set-Mailbox** с параметром *GrantSendonBehalf* .

> ⓘ **Примечание**
>
> Общий почтовый ящик не предназначен для прямого входа. Учетная запись пользователя для общего почтового ящика должна оставаться отключенной (или выключенной).

Преобразование общих почтовых ящиков

В предыдущих версиях Exchange обычный почтовый ящик можно было использовать в качестве делегированного. Если у вас есть делегированные почтовые ящики, можно использовать командную консоль Exchange для преобразования этих почтовых ящиков делегатов в общие почтовые ящики. Дополнительные сведения см. в разделе Преобразование почтового ящика в Exchange Server.

Создание общих почтовых ящиков в Центре администрирования Exchange

Статья • 04.04.2023

Если ваша организация использует гибридную среду Exchange, вам следует использовать локальный Центр администрирования Exchange (EAC) для создания общих почтовых ящиков и управления ими. Центр администрирования Exchange (EAC) — это единая унифицированная консоль управления, которая позволяет управлять как локальными, так и Exchange Online организациями, а также подключать и настраивать функции для обеих организаций. Дополнительные сведения см. в разделе Гибридное управление в гибридных развертываниях Exchange.

Использование Центра администрирования Exchange для создания общего почтового ящика

Сведения об ограничениях, автоматическом сопоставлениях и настройке пользователей см. в статье Создание общего почтового ящика.

Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Почтовые ящики пользователей" в разделе Разрешения получателей .

1. Перейдите к разделу **Получатели, которым предоставлен общий>>доступ Добавить**➕

2. Заполнение обязательные поля:

   - **Краткое имя**
   - **Адрес электронной почты**

3. Чтобы предоставить разрешения на полный доступ или Отправить как, щелкните ➕ а затем выберите пользователей, которым вы хотите предоставить разрешения. Для выбора нескольких пользователей можно использовать клавишу CTRL. Путаются с тем, какое разрешение следует использовать? См . раздел Какие разрешения следует использовать? далее в этом разделе.

> ⓘ **Примечание**
>
> Разрешение "Полный доступ" позволяет пользователю открывать почтовый ящик, а также создавать из изменять в нем элементы. Разрешение "Отправлять как" позволяет всем пользователям, кроме владельца почтового ящика, отправлять электронную почту из этого общего почтового ящика. Для эффективной работы с общим почтовым ящиком необходимы оба разрешения.

4. Нажмите кнопку **Сохранить**, чтобы сохранить изменения и создать общий почтовый ящик.

Изменение делегирования общего почтового ящика с помощью Центра администрирования Exchange

1. Перейдите к **разделу Получатели, которым предоставлен общий>>доступ изменить**.✎

2. Нажмите кнопку **Делегирование почтовых ящиков**.

3. Чтобы предоставить или удалить разрешения на полный доступ и отправить как, щелкните **+Удалить−**, а затем выберите пользователей, которым вы хотите предоставить разрешения.

> ⓘ **Примечание**
>
> Разрешение "Полный доступ" позволяет пользователю открывать почтовый ящик, а также создавать из изменять в нем элементы. Разрешение "Отправлять как" позволяет всем пользователям, кроме владельца почтового ящика, отправлять электронную почту из этого общего почтового ящика. Для эффективной работы с общим почтовым ящиком необходимы оба разрешения.

4. Нажмите кнопку **Сохранить**, чтобы сохранить изменения.

Создание общего почтового ящика с помощью командной консоли Exchange

В этом примере показано создание общего почтового ящика "Отдел продаж" и предоставление группе безопасности MarketingSG разрешений "Полный доступ" и

"Отправить от имени". Пользователям, являющимся членами группы безопасности, будут предоставлены разрешения на доступ к данному почтовому ящику.

> ⓘ **Примечание**
>
> В этом примере предполагается, что вы уже создали группу безопасности MarketingSG и что в этой группе безопасности включена почта. См. **статью Управление группами безопасности с поддержкой почты в Exchange Server**.

PowerShell

```
New-Mailbox -Shared -Name "Sales Department" -DisplayName "Sales Department"
-Alias Sales | Set-Mailbox -GrantSendOnBehalfTo MarketingSG | Add-
MailboxPermission -User MarketingSG -AccessRights FullAccess -
InheritanceType All
```

Дополнительные сведения о синтаксисе и параметрах см. в статье New-Mailbox.

Какие разрешения следует использовать?

Перед внесением изменений в записи DNS настоятельно рекомендуем максимально снизить значение срока жизни для каждой записи DNS. Значение срока жизни определяет, как долго запись DNS остается в кэше на серверах DNS. Меньший интервал, например 5–10 минут, позволит быстрее отменить любые изменения события, для которого необходимо вернуть исходную конфигурацию. Если вам действительно необходимо изменить значение срока жизни для ваших записей DNS, не вносите другие изменения, пока не истечет исходный интервал.

- **Полный доступ**. Разрешение полный доступ позволяет пользователю войти в общий почтовый ящик и действовать в качестве владельца этого почтового ящика. После входа в систему пользователь может создавать элементы календаря; читать, просматривать, удалять и изменять сообщения электронной почты; создавать задачи и вести календарь контактов. Тем не менее, пользователь с разрешением на полный доступ не может отправлять электронную почту из общего почтового ящика, если у него нет также разрешения "Отправить как" или "Отправить от имени".

- **Отправить как**. Разрешение "Отправить как" позволяет пользователю олицетворять общий почтовый ящик при отправке почты. Например, если Сергей войдет в общий почтовый ящик отдела маркетинга и отправит

электронное сообщение, оно будет выглядеть так, будто отправителем был отдел маркетинга.

- **Отправить от имени.** Разрешение "Отправить от имени" позволяет пользователю отправлять электронную почту от имени общего почтового ящика. Например, если Джон входит в общий почтовый ящик Reception Building 32 и отправляет сообщение электронной почты, это будет выглядеть так, как будто сообщение было отправлено "Джон от имени здания ресепшн 32". Вы не можете использовать EAC для предоставления разрешений Отправить от имени. Необходимо использовать командлет **Set-Mailbox** с параметром *GrantSendonBehalf* .

Дополнительные сведения

Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Email адреса и адресные книги в Exchange Server

Статья • 04.04.2023

Чтобы упорядочивать и хранить сведения об электронных адресах получателей в организации, в Exchange используются адресные книги. Разделы, которые помогут вам узнать и настроить адреса электронной почты и адресные книги в Exchange Server, описаны в следующей таблице.

Основные термины	Описание	Статья
Политики адресных книг	Глобальный список адресов (GAL) — это главный список всех получателей в организации Exchange. Политики адресных книг обеспечивают простой механизм сегментации глобальных списков адресов в организациях, которым необходимо несколько таких списков. Политика адресных книг определяет глобальный список адресов, автономную адресную книгу и один или несколько списков адресов. Затем вы можете назначать политику адресных книг пользователям.	Политики адресных книг в Exchange Server
Списки адресов	Список адресов представляет собой подмножество глобального списка адресов. Каждый адрес представляет собой динамическую коллекцию получателей одного или нескольких типов. Списки адресов помогают пользователям находить нужных им получателей и ресурсы.	Списки адресов в Exchange Server
Шаблоны сведений	Шаблоны сведений управляют внешним видом свойств получателей, отображаемых в списках адресов Outlook.	Шаблоны сведений
Политики адресов электронной почты	Политики адресов электронной почты — это правила создания электронных адресов для получателей в Exchange.	Email адреса политик в Exchange Server
Иерархические адресные книги	Иерархическая адресная книга представляет получателей из глобального списка адресов, используя уникальную коммерческую структуру вашей организации (например, иерархию старшинства и руководства), обеспечивая эффективное обнаружение внутренних получателей.	Иерархические адресные книги

Основные термины	Описание	Статья
Автономные адресные книги	Автономная адресная книга — это коллекция списков адресов, которую могут скачивать и использовать в Outlook пользователи, не подключенные к организации Exchange.	Автономные адресные книги в Exchange Server

Email адреса политик в Exchange Server

Статья • 04.04.2023

В политиках адресов электронной почты определяются правила создания электронных адресов для получателей в организации Exchange. Политики адресов электронной почты в Exchange Server 2016 и Exchange Server 2019 практически не изменились по сравнению с Exchange Server 2010.

Домены SMTP, доступные для использования в политиках адресов электронной почты, определяются *обслуживаемыми доменами*, настроенными в организации Exchange (в частности, уполномоченными доменами и доменами внутренней ретрансляции). Дополнительные сведения о принятых доменах см. в разделе Принятые домены в Exchange Server.

Ниже перечислены основные компоненты политики адресов электронной почты.

- **Email шаблоны адресов**. Определите формат адреса электронной почты для получателей (например, `<firstname>@contoso.com` или `<lastname>.<firstname>@contoso.com`).
- **Фильтр получателей**. Указывает получателей, адреса электронной почты которых настроены политикой.
- **Приоритет**. Указывает порядок применения политик адресов электронной почты (важно, если получатель идентифицируется несколькими политиками).

Сведения о настройке политик адресов электронной почты см. в статье Процедуры для политик адресов электронной почты в Exchange Server.

Шаблоны электронных адресов

Шаблон электронного адреса содержит **тип** и **формат адреса**. Политика адресов электронной почты может содержать несколько шаблонов. Один шаблон должен определять основной SMTP-адрес электронной почты (для ответов), а в политике может быть определен только один основной SMTP-адрес электронной почты (это электронный адрес **Reply-To:** для получателей). Другие шаблоны электронных адресов в политике определяют дополнительные адреса получателей, или *прокси*-адреса.

Типы адресов

В политиках адресов электронной почты чаще всего используются SMTP-адреса, но доступны и другие типы электронных адресов. Допускаются следующие значения типа адреса:

- **SMTP**
- **GWISE**: Novell GroupWise. По умолчанию ищет отсутствующий `%ExchangeInstallPath%Mailbox\address\gwise\amd64\gwxpxgen.dll` файл для проверки формата адреса электронной почты.
- **ЗАМЕТКИ**: Lotus Notes. По умолчанию использует включенный `%ExchangeInstallPath%Mailbox\address\notes\amd64\ntspxgen.dll` файл для проверки формата адреса электронной почты.
- **X400**: по умолчанию использует включенный `%ExchangeInstallPath%Mailbox\address\notes\amd64\x400prox.dll` файл для проверки формата адреса электронной почты.

Примечания.

- В командной консоли Exchange значение `SMTP` указывает основной адрес электронной почты, а значение `smtp` — дополнительные (прокси-адреса).

  В Центре администрирования Exchange только флажок **Назначить форматом адреса для ответа по умолчанию** указывает, является ли электронный адрес основным или прокси-адресом. Значения SMTP и smtp в поле **Введите пользовательский тип адреса** равноценны. Однако в списке шаблонов электронных адресов для политики в Центре администрирования Exchange для основного адреса отображается значение **SMTP** (полужирное и в верхнем регистре), а для прокси-адресов — значение smtp (обычное начертание в нижнем регистре).

- Для политики адресов электронной почты можно настроить меньше типов электронных адресов, чем для отдельных получателей.
- Все электронные адреса, не являющиеся SMTP-адресами, относятся к пользовательским типам. Exchange не предоставляет уникальные диалоговые окна или страницы свойств для типов адресов электронной почты X.400, Novell GroupWise или Lotus Notes. Для электронных адресов, не являющихся SMTP-адресами, необходимы подходящие DLL-файлы.

Форматы адресов

В SMTP-адресе электронной почты используется синтаксис `chris@contoso.com`, где значение `chris` является *локальной частью* адреса электронной почты, а значение `contoso.com` — доменОМ SMTP (также называемым *адресным пространством* или *пространством имен*). Доступные значения домена SMTP определяются обслуживаемыми доменами, настроенными для организации.

С помощью политик адресов электронной почты можно назначить получателям несколько SMTP-адресов электронной почты, используя различные сочетания локальной части и домена. Однако только один SMTP-адрес электронной почты можно настроить в качестве основного.

Для всех форматов SMTP-адресов электронной почты в Командная консоль Exchange, а также для пользовательских форматов SMTP-адресов в Центре администрирования Exchange необходимо использовать переменные, чтобы определять локальную часть электронного адреса. Эти переменные описаны в приведенной ниже таблице.

Переменная	**Значение**
%d	Краткое имя
%g	Имя
%i	Буква отчества
%m	Псевдоним Exchange
%r*xy*	Замените все вхождения *x* на *y*
%r*xx*	Удаление всех вхождений *x*
%s	Фамилия
%*n*g	Первые *n* букв имени. Например, `%2g` использует первые две буквы имени.
%*n*s	Первые *n* букв фамилии. Например, `%2s` использует первые две буквы фамилии.

В дополнение к переменным можно также использовать текстовые символы US ASCII, которые разрешены в адресах электронной почты Exchange (например, точки (`.`) или символы подчеркивания (`_`). Обратите внимание, что каждая точка должна быть окружена другими допустимыми символами (например `%g.%s`,).

В Центре администрирования Exchange вы можете выбрать вариант из краткого списка заранее подготовленных форматов SMTP-адресов. Эти форматы адресов описаны в следующей таблице, где пример пользователя называется Elizabeth Brunner, а домен — contoso.com:

Пример	Эквивалент в Командная консоль Exchange
`<alias>@contoso.com`	`%m@contoso.com`
`elizabeth.brunner@contoso.com`	`%g.%s@contoso.com`
`ebrunner@contoso.com`	`%1g%s@contoso.com`
`elizabethb@contoso.com`	`%g%1s@contoso.com`
`brunner.elizabeth@contoso.com`	`%s.%g@contoso.com`
`belizabeth@contoso.com`	`%1s%g@contoso.com`
`brunnere@contoso.com`	`%s%1g@contoso.com`

Фильтры получателей для политик адресов электронной почты

Фильтры получателей указывают, к каким получателям применяется политика адресов электронной почты. Существует два основных варианта фильтров получателей: **заранее подготовленные** и **пользовательские**. По сути, доступны те же параметры фильтрации получателей, что и в динамических группах рассылки и адресных книгах. В приведенной ниже таблице представлена сводка различий между двумя способами фильтрации.

Способ фильтрации получателей	Пользовательский интерфейс	Фильтруемые свойства получателей	Операторы фильтра

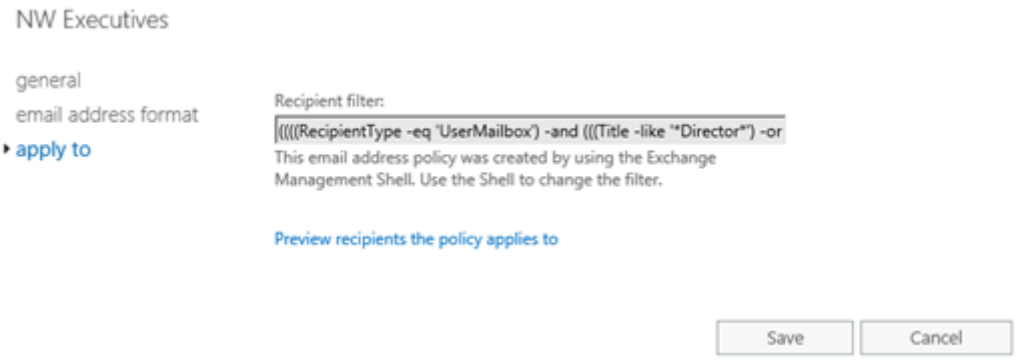
Способ фильтрации получателей	Пользовательский интерфейс	Фильтруемые свойства получателей	Операторы фильтра
Заранее подготовленные фильтры получателей	Центр администрирования Exchange (EAC) и Командная консоль Exchange	Поддерживаются только: • тип получателя (все типы получателей или любое сочетание почтовых ящиков пользователей, почтовых ящиков ресурсов, почтовых контактов, почтовых пользователей и групп); • компания; • настраиваемый атрибут от 1 до 15; • регион или область; • Отдел	Значения свойств должны полностью совпадать. Подстановочные знаки и частичные совпадения не поддерживаются. Например, значение "Продажи" не совпадает со значением "Продажи и маркетинг". Чтобы задать несколько значений для одного и того же свойства, всегда используйте оператор **or**. Пример: "Отдел равно Продажи или Отдел равно Маркетинг". Чтобы задать несколько свойств, всегда используется оператор **and**. Пример: "Отдел равно Продажи и Компания равно Contoso".
Пользовательские фильтры получателей	Только в Командная консоль Exchange	Можно использовать практически любые доступные атрибуты получателей.	Используйте синтаксис фильтра OPATH, чтобы задавать доступные операторы фильтра в Оболочка Windows PowerShell. Подстановочные знаки и частичные совпадения поддерживаются.

Примечания.

- Одновременно использовать заранее подготовленные и пользовательские фильтры невозможно.
- Расположение получателя в Active Directory (в подразделении или контейнере) доступно как в заранее подготовленных, так и в

пользовательских фильтрах получателей.

- Если вы создали в командной консоли Exchange политику, использующую пользовательский фильтр получателей, этот фильтр невозможно изменить в Центре администрирования Exchange.



- Вы можете задать отдельных получателей, на которых не влияют политики адресов электронной почты. Например:
  - В свойствах получателя на вкладке **Адрес электронной почты** Центра администрирования Exchange снимите флажок **Автоматически обновлять адреса электронной почты на основе политики адресов электронной почты, применимой к этому получателю**.
  - В командной консоли Exchange задайте для параметра *EmailAddressPolicyEnabled* значение `$false` в командлете управления получателями (например, **Set-Mailbox** или **Set-DistributionGroup**).

Приоритет политик адресов электронной почты

Если получатель определяется несколькими политиками адресов электронной почты, адреса электронной почты получателя настраиваются только первой оцениваемой политикой адресов электронной почты. Вы настраиваете порядок оценки политик с помощью приоритета политики. Более низкий приоритет указывает на более высокий приоритет, политики с более высоким приоритетом оцениваются в первую очередь, а политика адресов электронной почты по умолчанию всегда вычисляется последним. Вы назначаете более высокий приоритет (меньшее число) политикам, которые используют наиболее конкретные или ограничивающие фильтры получателей.

Ниже представлены некоторые факторы, которые следует учитывать.

- На получателя может влиять только одна политика адресов электронной почты. После того как пользователь сопоставляется по свойствам фильтрации для политики, все остальные политики игнорируются.
- **Все** политики адресов электронной почты, включая те, которые никогда не применялись, оцениваются по приоритету. Например, если имеются две политики с приоритетами 1 и 2 и в обеих определен один и тот же получатель, то после совпадения с первой политикой вторая не будет обновлять электронные адреса получателя, *даже если первая политика не применялась к получателю*.

Стандартная политика адресов электронной почты

При установке Exchange создается стандартная политика адресов электронной почты, применяющая электронные адреса ко всем получателям в организации. В приведенном ниже списке представлены свойства стандартной политики адресов электронной почты.

- **Имя**: политика по умолчанию
- **Приоритет**: самый низкий (все остальные политики адресов электронной почты оцениваются до политики по умолчанию).
- **Формат адреса электронной почты**.
  - **Тип**: `SMTP` (основной адрес электронной почты)
  - **Домен**: `<alias>@<ADForestRootFQDN>`. Это значение домена используется, поскольку это первый обслуживаемый домен в организации Exchange.
- **Применить к**: все типы получателей.

Стандартную политику адресов электронной почты невозможно удалить, а другую политику невозможно сделать стандартной. Вы можете менять некоторые свойства стандартной политики, но возможности изменения ограничены.

- Невозможно фильтровать получателей по типу или свойствам (относится ко всем типам получателей).
- Невозможно изменить имя и приоритет политики.
- Вы можете полностью настраивать шаблоны адресов электронной почты в политике (менять, добавлять и удалять шаблоны). Дополнительные сведения

см. в разделе Изменение политик адресов электронной почты.

Применение политик адресов электронной почты

Создав или изменив политику адресов электронной почты в Центре администрирования Exchange или командной консоли Exchange, необходимо применить ее к соответствующим получателям.

Если обновления затрагивают большое число получателей (наша рекомендация превышает 3000), следует использовать командную консоль Exchange, чтобы применить обновления к затронутым получателям. Дополнительные сведения см. в разделе Применение политик адресов электронной почты к получателям.

Процедуры для политик адресов электронной почты в Exchange Server

Статья • 04.04.2023

Политики адресов электронной почты назначают адреса электронной почты получателям в организации Exchange. Вы используете Центр администрирования Exchange (EAC) или командную консоль Exchange для настройки политик адресов электронной почты в Exchange Server.

Дополнительные сведения о политиках адресов электронной почты см. в разделе политики адресов Email в Exchange Server.

Что нужно для начала?

- Предполагаемое время для завершения каждой процедуры: 5 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "политики адресов Email" в разделе Email адреса и адресные книги Exchange Server.
- Процедуры в этом разделе в основном касаются SMTP-адресов электронной почты в политиках адресов электронной почты, но доступны и другие типы адресов. Дополнительные сведения см. в разделе Типы адресов.
- Прежде чем использовать SMTP-домен в политике адресов электронной почты, необходимо настроить его как обслуживаемый домен (в частности, домен внутренней ретрансляции или уполномоченный домен). Дополнительные сведения см. в разделе Обслуживаемые домены в Exchange Server.
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форум по адресу: **Exchange Server**.

Создание политик адресов электронной почты

Создав политику адресов электронной почты, необходимо применить ее к получателям. Дополнительные сведения см. в разделе Применение политик адресов электронной почты к получателям далее в этой статье.

Создание политик адресов электронной почты с помощью Центра администрирования Exchange

1. В EAC перейдите в **раздел Поток**> обработки **почты Email политики адресов**, а затем щелкните **Добавить**➕

2. В открывшемся окне **Новая политика адресов электронной почты** настройте указанные ниже параметры.

   - **Имя политики**: Укажите уникальное, понятное имя политики.

   - **Email формате адреса**: нажмите кнопку **Добавить** (➕ Чтобы настроить шаблон адреса электронной почты. После добавления первого шаблона для определения основного SMTP-адреса электронной почты можно добавить дополнительные шаблоны для прокси-адресов электронной почты (SMTP или иным образом) или нажать кнопку **Изменить** (✏️ Чтобы изменить существующий шаблон. Дополнительные сведения о доступных параметрах см. в разделе Окно "Формат адреса электронной почты" в Центре администрирования Exchange далее в этой статье.

     Вы также можете нажать кнопку **Удалить** (🗑 Чтобы удалить существующие шаблоны.

   Примечания.

   - Первый созданный здесь шаблон SMTP-адреса определяет основной SMTP-адрес (**Ответить:**). This template has the **Type** value **SMTP** (bold and uppercase), while other SMTP templates for proxy addresses have the **Type** value smtp (not bold and lowercase).

   - Невозможно удалить шаблон адреса электронной почты, который определяет основной SMTP-адрес в политике. Но вы можете добавить или изменить другой шаблон, применить его к основному адресу электронной почты, а затем удалить исходный шаблон.

- **Выполнять эту политику вместе с другими политиками в следующей последовательности**. Выбранное здесь значение зависит от того, сколько еще политик адресов электронной почты вы создали вручную. Например, для первой созданной политики адресов электронной почты доступно только значение 1. Создав еще одну политику, вы сможете выбрать значение 1 или 2. Помните, что первая политика адресов электронной почты, идентифицирующая получателя, задает его адреса электронной почты. Все остальные политики игнорируются, даже если первая политика не применяется и не может настраивать адреса электронной почты получателя.

- Дополнительные сведения о доступных фильтрах получателей см. в разделе Фильтры получателей в Центре администрирования Exchange далее в этой статье.

3. Когда закончите, нажмите **Сохранить**. Появится предупреждение о том, что нужно нажать кнопку **Применить** в области сведений, чтобы применить политику к получателям. Дополнительные сведения см. в разделе Применение политик адресов электронной почты к получателям далее в этой статье.

Создание политик адресов электронной почты с помощью командной консоли Exchange

Для политики адресов электронной почты в командной консоли Exchange требуется **фильтр получателей** и один или несколько **шаблонов адресов электронной почты**. Дополнительные сведения о фильтрах получателей см. в разделе Фильтры получателей в командной консоли Exchange этой статьи.

Email шаблонах адресов используется синтаксис `<Type>:<AddressFormat>`:

- `<Type>`: допустимый тип адреса электронной почты, как описано в разделе Типы адресов. Например, `SMTP` для основного адреса электронной почты и `smtp` для прокси-адресов.

- `<AddressFormat>`: для SMTP-адресов электронной почты — домен или поддомен, настроенный как обслуживаемый домен (полномочный или внутренний ретранслятор), а также допустимые переменные и текстовые символы ASCII, как описано в разделе Форматы адресов. Например, `<alias>@contoso.com` требуется значение `%m@contoso.com`, а `<firstname>.<lastname>@contoso.com` — значение `%g.%s@contoso.com`.

Чтобы создать политику адресов электронной почты, используйте следующий синтаксис:

PowerShell

```
New-EmailAddressPolicy -Name "<Policy Name>" <Precanned recipient filter | Custom recipient filter> [-RecipientContainer <OrganizationalUnit>] [-Priority <AllowedInteger>] -EnabledEmailAddressTemplates "SMTP:<PrimaryEmailAddressFormat>","smtp:<ProxyEmailAddress1>","smtp:<ProxyEmailAddress2>"...
```

В этом примере создается политика адресов электронной почты с заранее подготовленным фильтром получателей:

- **Название**: Юго-Восточные офисы
- **Предуклонированный фильтр получателей**: все пользователи с почтовыми ящиками, где значение **штата или провинции** — GA, AL или LA (Джорджия, Алабама или Луизиана).
- **Основной SMTP-адрес электронной почты**: `<last name>.<first two letters of the first name>@contoso.com`
- **Дополнительные адреса электронной почты прокси-сервера**: `<last name>.<first two letters of the first name>@contoso.net`
- **Приоритет**: *n*+1, где *n* — количество уже созданных вручную политик адресов электронной почты (мы не использовали параметр *Priority* , а значение по умолчанию — *n*+1). Помните, что первая политика адресов электронной почты, идентифицирующая получателя, задает его адреса электронной почты. Все остальные политики игнорируются, даже если первая политика не применяется и не может настраивать адреса электронной почты получателя.

PowerShell

```
New-EmailAddressPolicy -Name "Southeast Offices" -IncludedRecipients MailboxUsers -ConditionalStateorProvince "GA","AL","LA" -EnabledEmailAddressTemplates "SMTP:%s%2g@southeast.contoso.com","smtp:%s%2g@southeast.contoso.net"
```

В этом примере создается политика адресов электронной почты с пользовательским фильтром получателей:

- **Имя**: Северо-Западные руководители

- **Настраиваемый фильтр получателей**: все пользователи с почтовыми ящиками, в которых значение **Title** содержит Director или Manager, а значение **штата или провинции** — WA, OR или ID (Вашингтон, Орегон или Айдахо).
- **Основной SMTP-адрес электронной почты**: `<first two letters of the first name><last name>@contoso.com`
- **Дополнительные адреса электронной почты прокси-сервера**: нет
- **Приоритет**: 2

PowerShell

```
New-EmailAddressPolicy -Name "Northwest Executives" -RecipientFilter "
(RecipientType -eq 'UserMailbox') -and (Title -like '*Director*' -or Title -
like '*Manager*') -and (StateOrProvince -eq 'WA' -or StateOrProvince -eq
'OR' -or StateOrProvince -eq 'ID')" -EnabledEmailAddressTemplates
"SMTP:%2g%s@contoso.com" -Priority 2
```

Примечания.

- Как правило, параметр *EnabledEmailAddressTemplates* используется для определения основного SMTP-адреса электронной почты и одного или нескольких прокси-адресов (SMTP или иным образом). Однако если вы собираетесь определить только основной SMTP-адрес электронной почты и не будет дополнительных прокси-адресов, можно использовать параметр *EnabledPrimarySMTPAddressTemplate* . Для этого параметра не требуется `SMTP:` префикс, и его нельзя использовать с параметром *EnabledEmailAddressTemplates* .
- Для параметра *EnabledEmailAddressTemplates* требуется по крайней мере один шаблон со значением `<Type>SMTP` (для определения основного SMTP-адреса электронной почты). После этого, если не включить `<Type>` префикс для шаблона, предполагается значение `smtp` (адрес прокси-сервера SMTP).

Дополнительные сведения о синтаксисе и параметрах см. в статье New-EmailAddressPolicy.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли создана политика адресов электронной почты, выполните одно из указанных ниже действий.

- В EAC перейдите в раздел Поток >**обработки почтыEmail политики адресов**, убедитесь, что указана политика и указаны правильные сведения. Выберите политику и нажмите кнопку **Изменить** (✎ Чтобы просмотреть сведения, которые не отображаются в представлении списка.

- В командной консоли Exchange выполните следующую команду, чтобы проверить значения свойств:

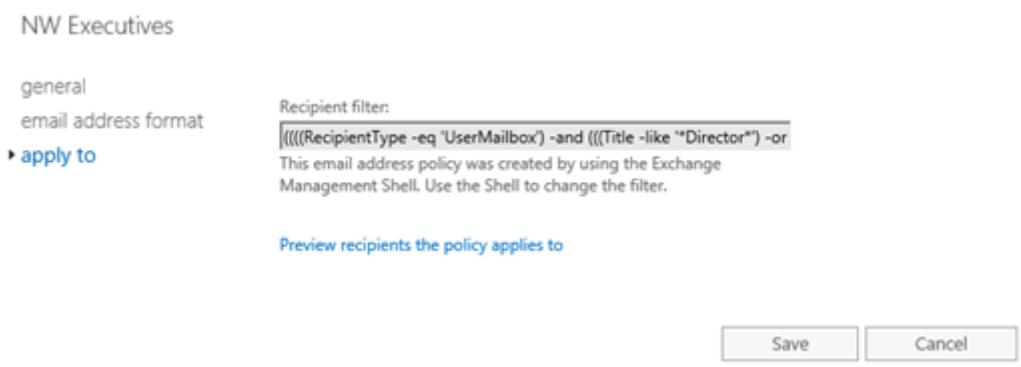
```
PowerShell

Get-EmailAddressPolicy | Format-List
Name,Priority,Enabled*,RecipientFilterType,RecipientContainer,Recipient
Filter,IncludedRecipients,Conditional*
```

Изменение политик адресов электронной почты

- Для политики адресов электронной почты по умолчанию нельзя изменить имя, приоритет и параметры фильтра получателей. Вы можете менять только шаблоны адресов электронной почты.

- Изменив политику адресов электронной почты, необходимо применить ее к получателям. Дополнительные сведения см. в разделе Применение политик адресов электронной почты к получателям далее в этой статье.

- Если вы создали политику, использующую пользовательский фильтр получателей, в командной консоли Exchange, этот фильтр нельзя изменить в Центре администрирования Exchange. Необходимо использовать командную консоль Exchange.



- Ни Центр администрирования Exchange, ни Командная консоль Exchange не позволяют заменить пользовательский фильтр получателей в существующей

политике адресов электронной почты заранее заготовленным фильтром получателей (или наоборот).

Изменение политик адресов электронной почты в Центре администрирования Exchange

Доступны те же параметры, что и при создании политики, но теперь они расположены на отдельных вкладках.

1. В EAC перейдите в раздел **Поток**> обработки почты **Email политики адресов**, выберите политику в списке и нажмите кнопку **Изменить** (✏️

2. Настройте параметры на следующих вкладках:

   - **Общие**

   - **Имя политики**: Уникальное, понятное имя политики.

   - **Выполнять эту политику вместе с другими политиками в следующей последовательности**: Помните, что первая политика адресов электронной почты, идентифицирующая получателя, задает его адреса электронной почты. Все остальные политики игнорируются, даже если первая политика не применена и не может настраивать адреса электронной почты получателя.

   - **Email формат адреса**. Дополнительные сведения о параметрах, доступных при нажатии кнопки **Добавить** (➕) или **Изменить** (✏️), см. в окне формата адреса Email в разделе EAC этой статьи.

     Вы также можете нажать кнопку **Удалить** (🗑️), чтобы удалить существующие шаблоны адресов электронной почты.

   Примечания.

   - **SMTP** (полужирным шрифтом и прописными буквами) в качестве значения **Тип** указывает на основной SMTP-адрес, а smtp (обычным шрифтом и в нижнем регистре) — на прокси-адрес.

   - Невозможно удалить шаблон адреса электронной почты, который определяет основной SMTP-адрес в политике. Но вы можете добавить или изменить другой шаблон, определить в нем основной адрес электронной почты, а затем удалить исходный шаблон.

- **Применить к**. Дополнительные сведения о фильтрах получателей, доступных здесь, см. в разделе Фильтры получателей в EAC этой статьи.

  Примечание. Даже если вы настроили пользовательский фильтр получателей в командной консоли Exchange, вы можете выбрать **Просмотреть получателей, к которым применяется политика** здесь.

3. Когда закончите, нажмите **Сохранить**. Появится предупреждение о том, что нужно нажать кнопку **Применить** в области сведений, чтобы применить политику к получателям. Дополнительные сведения см. в разделе Применение политик адресов электронной почты к получателям далее в этой статье.

Изменение политик адресов электронной почты в командной консоли Exchange

Доступны те же основные параметры, что и при создании политики. Дополнительные сведения см. в разделе Создание политик адресов электронной почты с помощью командной консоли Exchange этой статьи.

Чтобы изменить существующий шаблон электронного адреса, используйте следующий синтаксис:

PowerShell

```
Set-EmailAddressPolicy -Identity <EmailAdressPolicyIdentity> [-Name <Name>]
[<Precanned recipient filter | Custom recipient filter>] [-
RecipientContainer <OrganizationalUnit>] [-Priority <AllowedInteger>] [-
EnabledEmailAddressTemplates
<"Type1:AddressFormat1","Type2:AddressFormat2"...] [-
DisabledEmailAddressTemplates
<"Type1:AddressFormat1","Type2:AddressFormat2"... | $null>]
```

При изменении значений *условного* параметра можно использовать следующий синтаксис для добавления или удаления значений, не затрагивая другие существующие значения: `@{Add="<Value1>","<Value2>"...; Remove="<Value1>","<Value2>"...}`.

В этом примере показано, как изменить политику адресов электронной почты Southeast Executives, добавив TX (Texas) в качестве значения **Область, край** к заранее подготовленному фильтру получателей.

PowerShell

```
Set-EmailAddressPolicy -Identity "Southeast Executives" -
ConditionalStateOrProvince @{Add="TX"}
```

Параметр *DisabledEmailAddressTemplates* указывает неактивные шаблоны адресов электронной почты, которые больше не используются в политике, и использует тот же синтаксис, что и параметр *EnabledEmailAddressTemplates* (за исключением того, что *DisabledEmailAddressTemplates* не может содержать основной SMTP-адрес электронной почты). Как правило, это свойство заполняется только в том случае, если вы выполнили миграцию из предыдущей версии Exchange. Однако если домен указан в этом свойстве, вы не сможете удалить соответствующий обслуживаемый домен.

В этом примере показано, как удалить отключенные шаблоны электронных адресов из политики адресов электронной почты Contoso Executives.

PowerShell

```
Set-EmailAddressPolicy -Identity "Contoso Executives" -
DisabledEmailAddressTemplates $null
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе Set-EmailAddressPolicy.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли изменена политика адресов электронной почты, выполните одно из указанных ниже действий.

- В EAC перейдите в раздел Поток >**обработки почтыEmail политики адресов** и убедитесь, что свойства верны. Выберите политику и щелкните **Изменить** (✎), чтобы просмотреть свойства, которые не отображаются в представлении списка.

- В командной консоли Exchange выполните следующую команду, чтобы проверить значения свойств:

  PowerShell

  ```
  Get-EmailAddressPolicy | Format-List
  Name,Priority,*Template*,RecipientFilterType,RecipientContainer,Recipie
  ntFilter,IncludedRecipientsConditional*
  ```

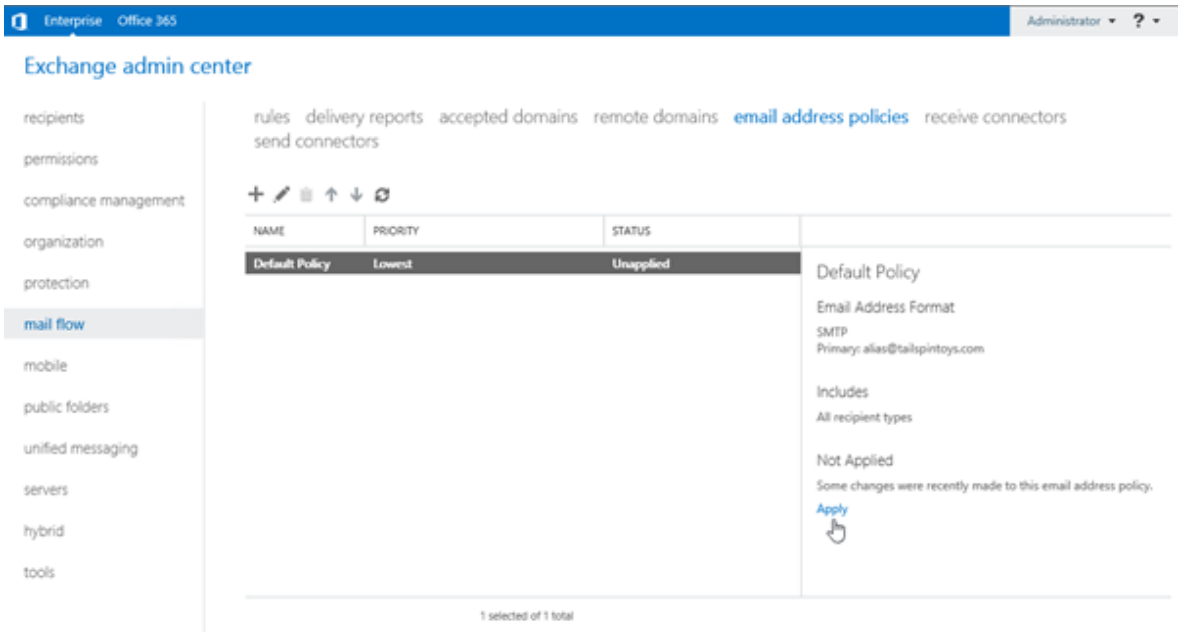
Применение политик адресов электронной почты к получателям

Создав или изменив политику адресов электронной почты в Центре администрирования Exchange или командной консоли Exchange, ее необходимо применить к получателям.

- Если политика влияет более чем на 3000 получателей, рекомендуем использовать командную консоль Exchange. Обновление получателей займет много времени, а сеанс Центра администрирования Exchange будет недоступен для использования, пока обновление не будет завершено.
- Если же политика влияет менее чем на 3000 получателей, можно использовать Центр администрирования Exchange.

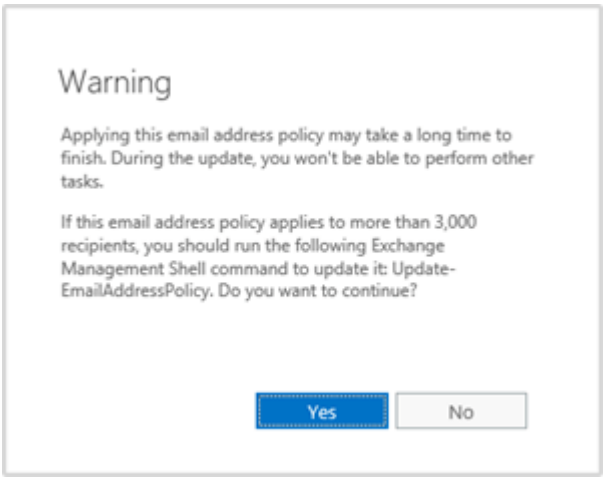
Применение политик адресов электронной почты к получателям с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел Поток >**обработки почтыEmail политики адресов**.
2. Выберите нужную политику адресов электронной почты (для которой в столбце **Состояние** указано **Не применена**).
3. В области сведений нажмите **Применить**.



4. После нажатия кнопки **Применить** появится предупреждающее сообщение. Нажмите **Да**, чтобы применить политику с помощью Центра

администрирования Exchange. Индикатор выполнения позволяет отслеживать процесс. После обновления нажмите **Закрыть**.



Применение политик адресов электронной почты к получателям с помощью командной консоли Exchange

Чтобы применить политику адресов электронной почты к получателям, используйте следующий синтаксис:

PowerShell

```
Update-EmailAddressPolicy -Identity <EmailAddressPolicyIdentity> [-FixMissingAlias] -[UpdateSecondaryAddressesOnly]
```

В этом примере применяется политика адресов электронной почты Northwest Executives.

PowerShell

```
Update-EmailAddressPolicy -Identity "Northwest Executives"
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Update-EmailAddressPolicy.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли применена политика адресов электронной почты, выполните одно из указанных ниже действий.

- В EAC перейдите в **раздел Поток**> обработки почты **Email политики адресов** и убедитесь, что для параметра **Состояние** политики **задано значение Применено**.
- В командной консоли Exchange выполните следующую команду, чтобы убедиться, что свойство **RecipientFilterApplied** имеет значение `True`:

```
PowerShell

Get-EmailAddressPolicy | Format-Table -Auto Name,RecipientFilterApplied
```

Удаление политик адресов электронной почты

- Политику адресов электронной почты по умолчанию нельзя удалить.
- Если политика влияет более чем на 3000 получателей, рекомендуем использовать командную консоль Exchange. Обновление получателей займет много времени, а сеанс Центра администрирования Exchange будет недоступен для использования, пока обновление не будет завершено. Если же удаление политики влияет менее чем на 3000 получателей, можно использовать Центр администрирования Exchange.

Удаление политики адресов электронной почты с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел Поток >**обработки почтыEmail политики адресов**.
2. Выберите политику адресов электронной почты, которую нужно удалить, и нажмите кнопку **Удалить**🗑
3. Нажмите **Да** в появившемся предупреждающем сообщении. Индикатор выполнения позволяет отслеживать процесс. После обновления нажмите **Закрыть**.

Удаление политик адресов электронной почты с помощью командной консоли Exchange

Чтобы удалить политику адресов электронной почты, используйте следующий синтаксис:

PowerShell

```
Remove-EmailAddressPolicy -Identity <EmailAddressPolicyIdentity>
```

В этом примере удаляется политика адресов электронной почты Southeast Offices.

PowerShell

```
Remove-EmailAddressPolicy -Identity "Southeast Offices"
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Remove-EmailAddressPolicy.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли удалена политика адресов электронной почты, выполните одно из указанных ниже действий.

- В EAC перейдите в раздел Поток >**обработки почтыEmail политики адресов** и убедитесь, что политика больше не указана в списке.
- В командной консоли Exchange выполните следующую команду, чтобы убедиться, что политики адресов электронной почты нет в списке:

  PowerShell

  ```
  Get-EmailAddressPolicy
  ```

Ссылка

Окно "Формат адреса электронной почты" в Центре администрирования Exchange

При создании или изменении политики адресов электронной почты в EAC в разделе **формат адреса Email** при нажатии кнопки **Добавить** (➕) или **Изменить** (✏) появляется окно **Email формата адреса**. В этом окне доступны следующие параметры:

- Заранее подготовленные SMTP-адреса:

- **Выберите обслуживаемый домен**. Выберите обслуживаемый домен (доверенный домен или домен внутренней ретрансляции) в раскрывающемся списке. Обратите внимание, что если вы настроили обслуживаемый домен для домена и всех поддоменов (например, `*.contoso.com`), в раскрывающемся списке доступен только корневой домен (`contoso.com`).

  или

- **Укажите имя личного домена для адреса электронной почты**. Выберите этот параметр, если необходимо ввести поддомен принятого `*.<domain>` домена. Например, если `*.contoso.com` настроен как полномочный домен, можно ввести eu.contoso.com в этом поле.

  Затем настройте следующий параметр:

- **Email формат адреса**. Выберите один из доступных шаблонов адресов электронной почты в списке.

- Пользовательские SMTP-адреса или другие адреса электронной почты:

  - Нажмите **Дополнительные параметры** и выберите **Введите пользовательский тип адреса**.

  - **Введите пользовательский тип адреса**. Если это первый шаблон адреса электронной почты, который вы настраиваете в политике, введите SMTP, а затем перейдите к Email поле **параметров адреса**, чтобы определить основной формат АДРЕСА SMTP.

    После того как вы определите основной SMTP-адрес, можете ввести SMTP или другое значение типа адреса, чтобы настроить шаблоны адресов электронной почты для дополнительных прокси-адресов. Дополнительные сведения о значениях типов, которые можно использовать, см. в разделе Типы адресов.

  - **Email параметры адреса**: для SMTP-адресов электронной почты это значение содержит следующее:

  - Допустимые переменные и текстовые символы ASCII, описываемые в разделе Форматы адресов.

  - Домен или поддомен, настроенный в качестве обслуживаемого домена (домена внутренней ретрансляции или уполномоченного домена).

В качестве примера используется `%3g.%s@contoso.com` значение @ `<first three letters of the first name>.<last name>`contoso.com.

- **Сделайте этот формат адресом электронной почты для ответа**. Первый шаблон адреса электронной почты в политике автоматически настраивается в качестве основного (ответного) адреса электронной почты (флажок снять нельзя). При добавлении дополнительных шаблонов в политику можно установить этот флажок, чтобы определить основной адрес электронной почты.

Фильтры получателей в Центре администрирования Exchange

При создании и изменении политик адресов электронной почты в Центре администрирования Exchange доступны следующие параметры фильтров получателей:

- **Укажите типы получателей, к которые будет применяться эта политика адресов электронной почты**:
  - **Все типы получателей**

    или

  - **Только следующие типы получателей**: Выберите одно или несколько из следующих значений:
    - **Пользователи с почтовыми ящиками Exchange**
    - **Пользователи почты с внешними адресами электронной почты**
    - **Почтовые ящики ресурсов**
    - **Почтовые контакты с внешними адресами электронной почты**
    - **Группы с включенной поддержкой почты**
- **Создайте правила для дальнейшего определения получателей, к которым применяется эта политика адресов электронной почты**:
  1. Нажмите **Добавить правило** и выберите одно из свойств получателей в раскрывающемся списке:
     - **Контейнер получателя** (контейнер или подразделение);

- **Область, край;**
- **Компания;**
- **Отдел;**
- Настраиваемый атрибут от 1 до 15.

2. Введите значение для выбранного свойства:
   - Если выбрать свойство **Контейнер получателя**, откроется диалоговое окно **Выбор подразделения**, в котором можно выбрать контейнер или подразделение в Active Directory.
   - Для других свойств получателей открывается диалоговое окно **Определение слов или фраз**, в котором можно добавлять, изменять и удалять текстовые значения.
   - Значения свойств должны полностью совпадать. Подстановочные знаки и частичные совпадения не поддерживаются. Например, значение "Продажи" не совпадает со значением "Продажи и маркетинг".
   - Чтобы задать несколько значений для одного и того же свойства, используйте оператор **or**. Пример: "Отдел равно Продажи или Отдел равно Маркетинг".
3. Выбрав свойство и значение, нажмите **Добавить правило**.
4. Повторите предыдущие шаги, чтобы настроить дополнительные фильтры. Обратите внимание, что в нескольких свойствах используется оператор **and**. Пример: "Отдел равно Продажи и Компания равно Contoso".

   Получатели предварительного просмотра, к которым применяется политика. При выборе этого параметра появляется диалоговое окно **Предварительный просмотр** , в которое показано, какие получатели определены настроенными фильтрами.

Примечания.

- Параметры фильтров получателей нельзя настраивать в политике адресов электронной почты по умолчанию (выбрано значение **Все типы получателей**).

- Если вы настроите слишком много правил фильтра получателей, в политике может не остаться ни одного получателя.

Фильтры получателей в командной консоли Exchange

В командной консоли Exchange можно указать **заранее подготовленные** или **пользовательские фильтры получателей**, но не оба типа сразу.

- **Предварительно настроенные фильтры получателей**:
  - Использует обязательный параметр *IncludedRecipient* со значением `AllRecipients` *или* одним или несколькими из следующих значений: `MailboxUsers`, `MailContacts`, `MailGroups`, `MailUsers` или `Resources`. Вы можете указать несколько значений, разделив их запятыми.
  - Можно также использовать любой из необязательных параметров *условного* фильтра: *ConditionalCompany*, *ConditionalCustomAttribute[1to15]*, *ConditionalDepartment* и *ConditionalStateOrProvince*.

    Вы указываете несколько значений для *условного* параметра с помощью синтаксиса `"<Value1>","<Value2>"...`. При указании нескольких значений для одного свойства неявно используется оператор **or**. Пример: "Отдел равно Продажи или Маркетинг или Финансы".
- **Настраиваемые фильтры получателей**. Использует обязательный параметр *RecipientFilter* с фильтром OPATH.
  - Основной синтаксис фильтра OPATH — .`"<Property1> -<Operator> '<Value1>' <Property2> -<Operator> '<Value2>'..."`
  - Для всего фильтра OPATH требуются двойные кавычки `" "` . Хотя фильтр является строкой (не системным блоком), можно также использовать фигурные скобки `{ }`, но только в том случае, если фильтр не содержит переменные, требующие расширения.
  - Дефисы (`-`) требуются перед всеми операторами. Вот некоторые из наиболее часто используемых операторов:
  - `and`, `or` и `not`.
  - `eq` и `ne` (равно и не равно; без учета регистра).
  - `lt` и `gt` (меньше и больше).

- `like` и `notlike` (строка содержит и не содержит; требуется по крайней мере один подстановочный знак в строке. Например, `"Department -like 'Sales*'"`.

- Используйте круглые скобки для группировки `<Property> -<Operator> '<Value>'` операторов в сложных фильтрах. Например, `"(Department -like 'Sales*' -or Department -like 'Marketing*') -and (Company -eq 'Contoso' -or Company -eq 'Fabrikam')"`. Exchange сохраняет фильтр в свойстве **RecipientFilter**, заключая каждый оператор в круглые скобки, но их необязательно вводить в таком формате.

- Дополнительные сведения см. в разделе Дополнительные сведения о синтаксисе OPATH.

- Если для создания политики вы использовали командлет **New-EmailAddressPolicy**, пользовательские фильтры получателей нельзя редактировать в Центре администрирования Exchange. Необходимо использовать командлет **Set-EmailAddressPolicy** с параметром *RecipientFilter* в командной консоли Exchange.

Примечание. Параметр фильтра *получателей RecipientContainer* (подразделение) доступен как для предварительно настроенных фильтров получателей, так и для настраиваемых фильтров получателей.

Автономные адресные книги в Exchange Server

Статья • 04.04.2023

Автономная адресная книга (OAB) — это локальная копия коллекции списков адресов. OAB используются для запросов адресной книги клиентами Outlook, настроенными в режиме кэширования Exchange. OAB являются единственным вариантом для клиентов Outlook, которые отключены от Exchange Server, но они также запрашиваются первыми подключенными клиентами Outlook, чтобы уменьшить рабочую нагрузку на серверах Exchange. Вы можете настроить списки адресов, включенные в автономную адресную книгу, доступ к определенным OAB, частоту создания OAB и место их распространения.

По умолчанию новая установка Exchange создает автономную адресную книгу по умолчанию на сервере. Эта автономная адресная книга используется почтовыми ящиками и базами данных почтовых ящиков, которым не назначена собственная автономная адресная книга.

OAB в Exchange 2013 и более поздних версиях улучшены по сравнению с OAB в Exchange 2010. Эти изменения были введены в Exchange 2013:

- Поддерживается только распространение через Интернет (распространение через общедоступные папки больше не поддерживается). Распространение через Интернет позволяет:
    - Увеличить количество одновременных загрузок с клиентских компьютеров.
    - Уменьшить объем трафика.
    - Контролировать точки распространения автономной адресной книги.
- Поддерживается только автономная адресная книга версии 4. Эта юникодовая версия автономной адресной книги, она позволяет клиентам скачивать только файл изменений, а не полную версию. Все версии Outlook, поддерживаемые Exchange, полностью поддерживают автономную адресную книгу версии 4.
- Помощник по почтовым ящикам (не служба системного помощника Microsoft Exchange) — это процесс, отвечающий за создание OAB. Это позволяет запускать или приостанавливать формирование автономной адресной книги в зависимости от загруженности сервера (управлять рабочей нагрузкой).

- Формирование автономной адресной книги происходит в специальном почтовом ящике разрешения конфликтов (не на специальном сервере). Эти почтовые ящики могут использовать группы DAG, чтобы предотвратить отказ, вызванный неисправностью одного элемента, во время формирования или скачивания автономной адресной книги.

Процедуры автономной адресной книги см. в разделе Процедуры для автономных адресных книг в Exchange Server.

Дополнительные сведения о списках адресов см. в статье Списки адресов в Exchange Server.

Формирование автономной адресной книги

Создание автономной адресной области управляется помощником по почтовому ящику **С именем OABGeneratorAssistant** , который выполняется в службе помощников по почтовым ящикам Microsoft Exchange. Создание OAB происходит в указанном почтовом ящике арбитража `OrganizationCapabilityOABGen` со значением свойства **PersistedCapability** . Почтовый ящик разрешения конфликтов с такой функцией известен также как *почтовый ящик организации*.

По умолчанию автономные адресные книги формируются каждые 8 часов. Сведения об изменении расписания создания автономной адресной книги см. в статье Изменение расписания создания автономной адресной книги в Exchange Server. Чтобы вручную обновить автономную адресную книгу, см. раздел Обновление автономных адресных книг с помощью командной консоли Exchange.

Почтовый ящик `SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}` арбитража — это первый почтовый ящик организации в вашей организации. По умолчанию этот почтовый ящик отвечает за формирование всех автономных адресных книг.

Вы можете создавать дополнительные почтовые ящики организации, чтобы формировать автономные адресные книги. Exchange Server содержит улучшения в создании автономной адресной области, которые были добавлены в накопительный пакет обновления 7 (CU7) для Exchange 2013:

- Вы можете настроить формирование нескольких автономных адресных книг одним почтовым ящиком организации, но нельзя настроить формирование одной автономной адресной книги несколькими почтовыми ящиками. В первом случае у каждой копии автономной адресной книги будет свой уникальный идентификатор. Поэтому при использовании прокси-сервера будет требоваться полная загрузка.

- Вы можете настроить распространение нередактируемой копии автономной адресной книги (*теневой копии*) по всем почтовым ящикам организации (*теневое распространение*). Все копии автономной адресной книги имеют один уникальный идентификатор, поэтому при использовании прокси-сервера не требуется полная загрузка.

  Как правило, теневые копии требуются только в организациях Exchange с несколькими сайтами. Почтовый ящик организации на каждом сайте и теневое распространение автономной адресной книги настраиваются, чтобы клиенты не отправляли запросы на скачивание между сайтами (вероятно, через медленные каналы связи WAN). Чтобы создать дополнительные почтовые ящики организации, см. раздел Создание почтовых ящиков организации с помощью командной консоли Exchange.

  Теневое распространение подробно описано в следующем разделе.

Чтобы найти все почтовые ящики организации, а также почтовый ящик организации, назначенный для автономной адресной книги, см. раздел Поиск почтовых ящиков организации с помощью командной консоли Exchange.

Файлы автономной адресной книги формируются и хранятся в специальном почтовом ящике организации, поэтому запросы на скачивание автономной адресной книги отсылаются на сервер почтовых ящиков, который содержит активную копию почтового ящика организации. Файлы автономной адресной книги копируются из почтового ящика `%ExchangeInstallPath%ClientAccess\OAB\<OAB GUID>` организации в для получения клиентами. Клиенты никогда напрямую не подключаются к этому внутреннему серверу. Запросы клиентов на получение автономной адресной книги перенаправляются на этот сервер при помощи служб клиентского доступа на сервере почтовых ящиков.

Распространение автономной адресной книги

По умолчанию клиенты Outlook настроены на скачивание автономной адресной адресной области каждые 24 часа, или пользователи могут инициировать скачивание вручную из Outlook в любое время.

Распределение автономной адресной адресной области между клиентами зависит от виртуальных каталогов служб IIS и службы автообнаружения. Виртуальный каталог IIS, используемый для клиентского доступа к OAB, находится на веб-сайте по умолчанию в службах клиентского доступа (внешний интерфейс) на сервере

почтовых ящиков и называется OAB (веб-сайт по умолчанию). Этот виртуальный каталог автоматически создается при установке Exchange и настраивается для обслуживания внутренних клиентов по URL-адресу `https://<ServerName>/oab` (например, `https://mailbox01.contoso.com/oab`). Вам потребуется вручную настроить внешний URL-адрес, используемый для распространения OAB между внешними клиентами. Дополнительные сведения см. в разделе Шаг 4. Настройка внешних URL-адресовв статье Настройка потока обработки почты и клиентского доступа на серверах Exchange Server.

В свойствах автономной адресной книги можно настроить виртуальные каталоги, которые могут распространять ее по клиентам. По умолчанию это могут делать только виртуальные каталоги на сервере, который содержит почтовый ящик организации автономной адресной книги. Однако службы клиентского доступа на *любом* сервере почтовых ящиков могут перенаправлять входящие запросы на скачивание автономных адресных книг на нужный сервер. Поэтому рекомендуется сделать так, чтобы все виртуальные каталоги принимали запросы на скачивание автономной адресной книги. Инструкции

Служба автообнаружения оповещает о тех URL-адресах автономной адресной книги, которые были настроены. Автообнаружение поддерживается всеми версиями Outlook и практически всеми мобильными устройствами, которые в настоящее время предоставляются Exchange. Вот краткое описание процесса распространения автономной адресной книги:

1. Outlook получает URL-адрес автономной адресной области от автообнаружения и подключается к службам клиентского доступа (внешний интерфейс) на сервере почтовых ящиков.

2. Службы клиентского доступа на сервере почтовых ящиков, которые приняли запрос на подключение, выполняют следующие действия:

    a. Запрашивает Active Directory, чтобы найти почтовый ящик организации, который отвечает за создание автономной адресной адресной записи пользователя (автономная адресная запись по умолчанию, автономная адресная адресная запись, указанная для базы данных почтовых ящиков, или автономная адресная запись, указанная для почтового ящика).

    b. Снова запросит Active Directory, чтобы найти базу данных почтовых ящиков, в которой размещается почтовый ящик организации для автономной адресной записи, и сервер почтовых ящиков, на котором в настоящее время хранится активная копия базы данных.

c. Перенаправляют запрос на скачивание автономной адресной книги на идентифицированный сервер почтовых ящиков.

d. Извлекает файлы OAB из расположения `%ExchangeInstallPath%ClientAccess\OAB\<GUID>` серверной части и отправляет их обратно клиенту.

Если теневая копия автономной адресной записи существует в почтовом ящике организации на локальном сайте Active Directory (сайте, с которого подключается пользователь), то для скачивания автономной адресной адресной записи используется локальный сервер почтовых ящиков. Однако синхронизация теневой копии между почтовыми ящиками организации выполняется по запросу. Вот как это делается:

1. Предположим, что в почтовом ящике организации нет подходящей теневой копии автономной адресной книги. Возможные причины:

   - Клиент не запрашивал скачивание теневой копии.
   - Теневая копия устарела. Теневые копии знают, когда была создана и опубликована обновленная копия родительской автономной адресной книги (вручную или по расписанию создания 8-часовой автономной адресной книги по умолчанию). Затронутые серверы почтовых ящиков перестанут распространять устаревшую теневые копии среди клиентов.

2. Первый клиент пытается скачать теневой копии, в Outlook появится сообщение об ошибке `0x80190194 (BG_E_HTTP_ERROR_404)` . После этого запустится полное копирование родительской автономной адресной книги в теневую копию. Отобразятся следующие события:

   - `Event ID: 102`

     `Source: MSExchange OABRequestHandler`

     `Description: The OABRequestHandler has begun downloading the OAB <GUID> from the server <Server>.`

   - `Event ID: 103`

     `Source: MSExchange OABRequestHandler`

     `Description: The OABRequestHandler has finished downloading the OAB <GUID>.`

3. Выполняет `OABRequestHandler` до трех немедленных попыток копирования файлов OAB с сервера почтовых ящиков, на котором хранится родительский почтовый ящик создания OAB. Если все три попытки завершаются сбоем `OABRequestHandler` , объект повторит копирование через час. Отобразятся следующие события:

    - `Event ID: 104`

      `Source: MSExchange OABRequestHandler`

      `Description: Download of the OAB <GUID> failed. The job will be re-submitted. The error was: BG_ERROR_CONTEXT=BE_ERROR_CONTEXT_REMOTE_FILE; error code=0x80190194`

    - `Event ID: 105`

      `Source: MSExchange OABRequestHandler`

      `Description: Download of the OAB <GUID> has failed too many times. The job will not be resubmitted for the next hour.`

4. Если автономная адресная адресная папка настроена для теневых распределений, но на локальном сайте Active Directory нет почтового ящика организации (сайт, с которого подключается пользователь), службы клиентского доступа будут прокси-серверу почтовых ящиков, на котором хранится почтовый ящик организации для родительской OAB.

Условия, которые приводят к скачиванию полной версии автономной адресной книги

Обычно клиенты скачивают обновления автономной адресной книги, а не ее полную версию. Однако иногда необходимо скачивать полную версию автономной адресной книги. Например:

- Размер `Changes.oab` файлов больше или равен половине полного размера OAB-файлов. Outlook сравнивает общий размер сжатых `Changes.oab` файлов, необходимых для обновления автономной адресной области, с общим размером сжатых полных файлов OAB на сервере.
- На компьютере нет автономной адресной области (например, во время начальной настройки Outlook).
- На сервере отсутствует файл изменений. Возможные причины:

    - Вы не использовали Outlook для подключения к почтовому ящику Exchange более 30 дней (по умолчанию разностные файлы хранятся на сервере в течение 30 дней).
    - Серверу не удалось создать файл изменений за день, необходимый для обновления локальной копии автономной адресной книги.
- На сервере доступна более поздняя версия автономной адресной записи (например, почтовый ящик был обновлен с Exchange 2010, а локальная копия автономной адресной адресной записи — версия 3).
- Не удалось применить изменения к автономной адресной книге. Например, файлы изменений на сервере повреждены (произошел сбой сервера во время их создания).
- На вашем компьютере нет автономной адресной книги (например, вы вручную удалили один или несколько локальных файлов автономной адресной книги).
- Предыдущая полная загрузка завершилась сбоем, поэтому Outlook нужно начать заново.
- Вы начали скачивание полной версии автономной адресной книги вручную.

Планирование и развертывание автономных адресных книг

Учитывайте следующие факторы при планировании и развертывании автономных адресных книг:

- Размер каждой автономной адресной книги в организации. Размеры автономных адресных книг могут варьироваться от нескольких до сотен мегабайт. На размер могут влиять следующие факторы:
    - Использование сертификатов в организации. Чем больше сертификатов PKI, тем больше автономная адресная книга. Сертификаты PKI имеют размер 1–3 КБ. Они оказывают наибольшее влияние на размер автономной адресной книги.
    - Количество получателей электронной почты в организации.
    - Количество групп в организации.

    - Сведения о пользователях, которые организация добавляет в объекты получателя. Например, некоторые организации указывают полный адрес и контактные данные для каждого пользователя.

- Количество скачиваний автономной адресной книги.
- Количество и частота изменений родительского различающегося имени для объектов-получателей в Active Directory.
- Несовпадения SMTP-адреса.
- Общее количество изменений, внесенных в Active Directory.
- Получатели, скрытые в Active Directory с помощью методов за пределами Exchange, будут видны в OAB (например, с помощью дескриптора безопасности Windows). Чтобы эффективно скрыть получателей в OAB, настройте свойство **Скрыть из списков адресов** для получателя в Центре администрирования Exchange (EAC) или *HiddenFromAddressListsEnabled* в соответствующем командлете управления получателями в командной консоли Exchange. Дополнительные сведения см. в разделе Скрытие получателей из списков адресов. Кроме того, можно создать список адресов, не включающий скрытых получателей, назначить список адресов автономной адресной книге и назначить автономную адресную книгу пользователям (напрямую или сделав автономную адресную книгу по умолчанию). Дополнительные сведения о создании списков адресов см. в разделе Создание списков адресов.

Перенос процесса формирования автономной адресной книги на другой сервер

В Exchange 2010 при перемещении создания автономной адресной записи на другой сервер необходимо указать другой сервер поколения в свойствах автономной адресной адресной записи. Но в Exchange 2013, Exchange 2016 и Exchange 2019 создание автономной адресной папки происходит в созданном почтовом ящике организации, а не на указанном сервере. Чтобы перенести процесс формирования автономной адресной книги на другой сервер, нужно переместить почтовый ящик организации. Например:

- Переместите существующий почтовый ящик организации на другой сервер Exchange 2013, Exchange 2016 или Exchange 2019 (вы не можете переместить

почтовый ящик организации на сервер Exchange 2010).

- Настройте автономную адресную книгу на его использование. Дополнительные сведения см. в разделе Изменение почтового ящика организации, который отвечает за формирование автономной адресной книги, с помощью командной консоли Exchange.

- Создайте почтовый ящик организации на другом сервере и настройте автономную адресную книгу на его использование. Дополнительные сведения см. в разделе Создание почтовых ящиков организации с помощью командной консоли Exchange.

Помните, что вы можете настроить формирование нескольких автономных адресных книг одним почтовым ящиком организации, но нельзя настроить формирование одной автономной адресной книги несколькими почтовыми ящиками. Если требуется несколько копий автономной адресной книги в разных расположениях (обычно на разных сайтах Active Directory), убедитесь, что на сайте существует почтовый ящик организации, и включите теневое распределение для автономной адресной книги. Дополнительные сведения см. в разделе Включение теневого распространения автономных адресных книг с помощью командной консоли Exchange.

Процедуры для автономных адресных книг в Exchange Server

Статья • 04.04.2023

Автономная адресная книга (OAB) в Exchange Server позволяет пользователям Outlook в кэшированном режиме Exchange получать доступ к сведениям списка адресов и глобального списка адресов при отключении от сервера. Дополнительные сведения см. в статье Автономные адресные книги в Exchange Server.

Ниже приведен список процедур автономной адресной адресной области, которые рассматриваются в этом разделе:

- Использование командной консоли Exchange для просмотра автономных адресных книг
- Создание автономных адресных книг с помощью командной консоли Exchange
- Используйте командную консоль Exchange для изменения автономных адресных книг:
  - Настройка автономной адресной книги по умолчанию с помощью командной консоли Exchange
  - Добавление и удаление списков адресов из автономных адресных книг с помощью командной консоли Exchange
  - Использование командной консоли Exchange для изменения почтового ящика организации, который отвечает за создание автономной адресной книги
  - Используйте командную консоль Exchange, чтобы настроить любой виртуальный каталог в организации для приема запросов на скачивание для автономной адресной папки.
  - Использование командной консоли Exchange для включения распределения теней для автономных адресных книг
- Обновление автономных адресных книг с помощью командной консоли Exchange

- Удаление автономных адресных книг с помощью командной консоли Exchange
- Поиск почтовых ящиков организации с помощью командной консоли Exchange
- Создание почтовых ящиков организации с помощью командной консоли Exchange
- Назначение автономных адресных книг базам данных почтовых ящиков
- Использование командной консоли Exchange для назначения автономных адресных книг почтовым ящикам

Сведения об изменении расписания создания автономной адресной книги см. в статье Изменение расписания создания автономной адресной книги в Exchange Server.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Автономные адресные книги" в разделе разрешения Email адреса и адресной книги.
- Вы не можете выполнить большинство из этих процедур в Центре администрирования Exchange (EAC). Необходимо использовать командную консоль Exchange. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell. Дополнительные сведения о EAC см. в разделе Центр администрирования Exchange в Exchange Server.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование командной консоли Exchange для просмотра автономных адресных книг

Чтобы просмотреть OAB, используйте следующий синтаксис:

PowerShell

```
Get-OfflineAddressBook [-Identity <OABIdentity>]
```

В этом примере возвращается сводный список всех OAB в вашей организации.

PowerShell

```
Get-OfflineAddressBook
```

Этот пример возвращает подробные сведения об автономной адресной книге с именем "Автономная адресная книга по умолчанию".

PowerShell

```
Get-OfflineAddressBook -Identity "Default Offline Address Book" | Format-
List
```

В этом примере возвращаются значения для указанных свойств для всех OAB в организации.

PowerShell

```
Get-OfflineAddressBook | Format-List
Name,GUID,AddressLists,GeneratingMailbox,IsDefault,VirtualDirectories,Global
WebDistributionEnabled,ShadowMailboxDistributionEnabled
```

Подробные сведения о синтаксисе и параметрах см. в разделе Get-OfflineAddressBook.

Создание автономных адресных книг с помощью командной консоли Exchange

Если вы создали несколько списков адресов, вы можете использовать OAB, чтобы сделать списки адресов доступными для пользователей, когда они находятся в

автономном режиме.

Чтобы создать новые автономные адресные книги, используйте следующий синтаксис:

PowerShell

```
New-OfflineAddressBook -Name "<Name>" -AddressLists "
<GlobalAddressListOrAddressList1>","<GlobalAddressListOrAddressList2>,..."
[-GlobalWebDistributionEnabled $true] [-GeneratingMailbox
<OrganizationMailboxIdentity>] [-IsDefault $true] [-
ShadowMailboxDistributionEnabled $true]
```

В этом примере создается новая автономная адресная запись Contoso Executives со следующими свойствами:

- Глобальный список адресов по умолчанию и список адресов руководителей Contoso включены в автономную адресную книгу.
- Все виртуальные каталоги OAB в организации могут принимать запросы на скачивание автономной адресной папки.
- Почтовый ящик организации, отвечающий за создание автономной адресной записи, — `SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}` (мы не использовали параметр *GeneratingMailbox* для указания другого почтового ящика организации).
- Автономная адресная адресная папка не используется почтовыми ящиками и базами данных почтовых ящиков, в которых не указана автономная адресная адресная запись не используется в почтовых ящиках и базах данных почтовых ящиков, `$true` в которых
- Теневое распределение для автономной адресной книги отключено (копии автономной адресной книги, доступные только для чтения, не копируются во все почтовые ящики организации, так как мы не использовали параметр *ShadowMailboxDistributionEnabled* со значением `$true`).

PowerShell

```
New-OfflineAddressBook -Name "Contoso Executives OAB" -AddressLists "Default
Global Address List","Contoso Executives Address List" -
GlobalWebDistributionEnabled $true
```

Подробные сведения о синтаксисе и параметрах см. в разделе New-OfflineAddressBook.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно создали автономную адресную книгу, выполните следующую команду, чтобы проверить значения свойств:

PowerShell

```
Get-OfflineAddressBook | Format-List
Name,AddressLists,GeneratingMailbox,IsDefault,VirtualDirectories,GlobalWebDi
stributionEnabled
```

Изменение автономных адресных книг с помощью командной консоли Exchange

Чтобы изменить OAB, используйте следующий синтаксис:

PowerShell

```
Set-OfflineAddressBook -Identity "<OABIdentity>" [-Name <Name>] [-
AddressLists "<GlobalAddressListOrAddressList1>","
<GlobalAddressListOrAddressList2>,..."] [-VirtualDirectories $null] [-
GlobalWebDistributionEnabled $true] [-GeneratingMailbox
<OrganizationMailboxIdentity>] [-IsDefault $true] [-
ShadowMailboxDistributionEnabled <$true | $false>]
```

Подробные сведения о синтаксисе и параметрах см. в разделе Set-OfflineAddressBook.

Настройка автономной адресной книги по умолчанию с помощью командной консоли Exchange

По умолчанию автоматически созданная автономная адресная книга по умолчанию является автономной адресной книгой по умолчанию. Автономная адресная область по умолчанию используется:

- Почтовые ящики в базах данных почтовых ящиков, где база данных не назначена автономной адресной адресной адресом (по умолчанию все базы данных);
- Почтовые ящики без назначенной политики адресной книги (ABP) или в тех случаях, когда назначенная политика ABP не определена автономная адресная книга (по умолчанию ASP не существует).

- Почтовые ящики без назначенного автономного адресного адреса (по умолчанию все почтовые ящики)

В этом примере настраивается автономная адресная

PowerShell

```
Set-OfflineAddressBook -Identity "Contoso Executives OAB" -IsDefault $true
```

Добавление и удаление списков адресов из автономных адресных книг с помощью командной консоли Exchange

При изменении списков адресов, настроенных в автономной адресной книге, указанные значения *заменят* все списки адресов в автономной адресной книге. Чтобы добавить списки адресов в автономную адресную книгу, укажите текущие списки адресов, а также те, которые нужно добавить. Чтобы удалить списки адресов из автономной адресной книги, укажите текущие списки адресов, кроме тех, которые нужно удалить.

В этом примере для автономной адресной книги с названием Marketing OAB уже настроены списки адресов Address List 1 и Address List 2. Чтобы сохранить эти списки адресов и добавить список адресов 3, выполните следующую команду:

PowerShell

```
Set-OfflineAddressBook -Identity "Marketing OAB" -Address Lists "Address
List1","Address List 2","Address List 3"
```

Аналогичным образом, чтобы настроить автономную адресную книгу со списком адресов 1 и адресом 2, но удалить список адресов 3, выполните следующую команду:

PowerShell

```
Set-OfflineAddressBook -Identity "Marketing OAB" -AddressLists "Address List
1","Address List 2"
```

Использование командной консоли Exchange для изменения почтового ящика организации, который отвечает за создание автономной адресной книги

Как правило, необходимо настроить несколько почтовых ящиков организации, только если у вас есть серверы Exchange на разных сайтах Active Directory. Вы можете настроить несколько OAB для использования одного и того же почтового ящика организации, но нельзя настроить автономную адресную книгу для использования нескольких почтовых ящиков организации. Если требуется несколько копий автономной адресной книги в разных расположениях, включите теневое распределение для автономной адресной книги. Дополнительные сведения см. в разделе Использование командной консоли Exchange для включения распределения теней для автономных адресных книг этого раздела.

В этом примере изменяется почтовый ящик организации, отвечающий за создание автономной адресной книги по умолчанию.

PowerShell

```
Set-OfflineAddressBook -Identity "Default Offline Address Book" -
GeneratingMailbox OABGen2
```

Примечание. Сведения о настройке почтового ящика арбитража, который можно использовать в качестве почтового ящика организации, см. в разделе Создание почтовых ящиков организации с помощью командной консоли Exchange .

Используйте командную консоль Exchange, чтобы настроить любой виртуальный каталог в организации для приема запросов на скачивание для автономной адресной папки.

Службы клиентского доступа (внешний интерфейс) на любом сервере почтовых ящиков могут выполнять прокси-запрос на скачивание автономной адресной папки в правильном расположении. Файлы автономной адресной области загружаются из серверной части `%ExchangeInstallPath%ClientAccess\OAB\<OAB GUID>` на сервере почтовых ящиков, на котором хранится активная копия почтового ящика организации автономной адресной области (или с сервера, на котором хранится теневая копия автономной адресной области).

В этом примере изменяется автономная адресная книга по умолчанию, чтобы любой виртуальный каталог в организации принимал запросы на скачивание автономной адресной книги.

1. Выполните следующую команду:

PowerShell

```
Set-OfflineAddressBook -Identity "Default Offline Address Book" -
VirtualDirectories $null
```

2. Выполните следующую команду:

PowerShell

```
Set-OfflineAddressBook -Identity "Default Offline Address Book" -
GlobalWebDistributionEnabled $true
```

Использование командной консоли Exchange для включения распределения теней для автономных адресных книг

Прежде чем включить теневое распределение для распространения копии автономной адресной папки только для чтения в почтовые ящики организации на разных сайтах Active Directory, убедитесь, что почтовый ящик организации существует на каждом сайте. Сведения о создании почтовых ящиков организации см. в разделе Создание почтовых ящиков организации с помощью командной консоли Exchange .

В этом примере включается распределение тени для автономной адресной адресной области с именем Contoso Executives OAB.

PowerShell

```
Set-OfflineAddressBook -Identity "Contoso Executives OAB" -
ShadowMailboxDistributionEnabled $true
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно изменили автономную адресную книгу, выполните следующую команду, чтобы проверить значения свойств:

PowerShell

```
Get-OfflineAddressBook | Format-List
Name,AddressLists,GeneratingMailbox,IsDefault,VirtualDirectories,GlobalWebDi
stributionEnabled,
```

Обновление автономных адресных книг с помощью командной консоли Exchange

Изменения в автономной адресной записи недоступны пользователям до запланированного создания автономной адресной записи (по умолчанию каждые 8 часов). Если вы не хотите ждать, можно использовать процедуры, описанные в этом разделе, чтобы немедленно обновить автономную адресную книгу.

Сведения об изменении расписания создания автономной адресной книги см. в статье Изменение расписания создания автономной адресной книги в Exchange Server.

Чтобы обновить автономную адресную книгу, используйте следующий синтаксис:

```
PowerShell

Update-OfflineAddressBook -Identity <OABIdentity>
```

В этом примере обновляется автономная адресная книга по умолчанию.

```
PowerShell

Update-OfflineAddressBook -Identity "Default Offline Address Book"
```

В этом примере обновляются все OAB.

```
PowerShell

Get-OfflineAddressBook | Update-OfflineAddressBook
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе Update-OfflineAddressBook.

Удаление автономных адресных книг с помощью командной консоли Exchange

Чтобы удалить OAB, используйте следующий синтаксис:

```
PowerShell

Remove-OfflineAddressBook -Identity <OABIdentity>
```

В этом примере удаляется автономная адресная

```
PowerShell

Remove-OfflineAddressBook -Identity "Contoso Executives OAB"
```

Примечание. Если удаленная автономная адресная адресная область является автономной адресной адресом по умолчанию, необходимо создать или настроить другую автономную адресную книгу в качестве значения по умолчанию (значение параметра *IsDefault* равно `$true`).

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно удалили автономную адресную книгу, выполните следующую команду, чтобы убедиться, что автономная адресная адресная запись исчезла.

```
PowerShell

Get-OfflineAddressBook
```

Поиск почтовых ящиков организации с помощью командной консоли Exchange

Только почтовые ящики организации могут создавать OAB. Почтовый ящик организации — это почтовый ящик арбитража `OrganizationCapabilityOABGen` , имеющий значение свойства **PersistedCapability** . Чтобы найти почтовые ящики организации в организации, выполните следующую команду:

```
PowerShell

Get-Mailbox -Arbitration | where {$_.PersistedCapabilities -like "*OAB*"} |
Format-List Name,ServerName,PersistedCapabilities
```

Чтобы найти почтовый ящик организации, который используется для создания автономной адресной папки, выполните следующую команду:

```
PowerShell

Get-OfflineAddressBook | Format-List
Name,AddressLists,GeneratingMailbox,IsDefault
```

Создание почтовых ящиков организации с помощью командной консоли Exchange

Как правило, необходимо только создать несколько почтовых ящиков арбитража в организациях Exchange с несколькими сайтами. Вы можете иметь почтовый ящик организации на каждом сайте и настроить теневое распределение для автономной адресной записи (так, чтобы копия автономной адресной записи хранимая только для чтения хранится во всех почтовых ящиках организации). Дополнительные сведения см. в разделе Включение теневого распространения автономных адресных книг с помощью командной консоли Exchange.

Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения подготовки получателей" раздела Разрешения получателей .

1. Создайте почтовый ящик арбитража, используя следующий синтаксис:

   PowerShell

   ```
   New-Mailbox -Arbitration -Name <UniqueName> -UserPrincipalName <UPN> [-
   Database <DBIdentity>] [-Alias <Alias>] [-DisplayName "<DisplayName>"]
   ```

   В этом примере создается новый почтовый ящик арбитража С именем OAB 2-го поколения с именем участника-пользователя (именем учетной записи) oabgen2@contoso.comв базе данных по умолчанию.

   PowerShell

   ```
   New-Mailbox -Arbitration -Name "OAB Gen 2" -UserPrincipalName
   oabgen2@contoso.com
   ```

2. Превратите почтовый ящик арбитража в почтовый ящик организации, используя следующий синтаксис:

   PowerShell

   ```
   Set-Mailbox -Identity <MailboxIdentity> -Arbitration -OABGen $true -
   MaxSendSize 1GB
   ```

   В этом примере почтовый ящик арбитража OAB 2-го поколения преобразуется в почтовый ящик организации.

   PowerShell

```
Set-Mailbox -Identity "OAB Gen 2" -Arbitration -OABGen $true -
MaxSendSize 1GB
```

3. Чтобы активировать возможности создания автономной адресной книги для нового почтового ящика организации, выполните **команду Update-OfflineAddressBook** для *любой* автономной адресной книги в организации. Например:

PowerShell

```
Update-OfflineAddressBook -Identity "Default Offline Address Book"
```

Как проверить, все ли получилось?

Чтобы убедиться, что почтовый ящик организации успешно создан, выполните следующую команду и убедитесь, что почтовый ящик возвращен:

PowerShell

```
Get-Mailbox -Arbitration | where {$_.PersistedCapabilities -like "*OAB*"} |
Format-List Name,ServerName,PersistedCapabilities
```

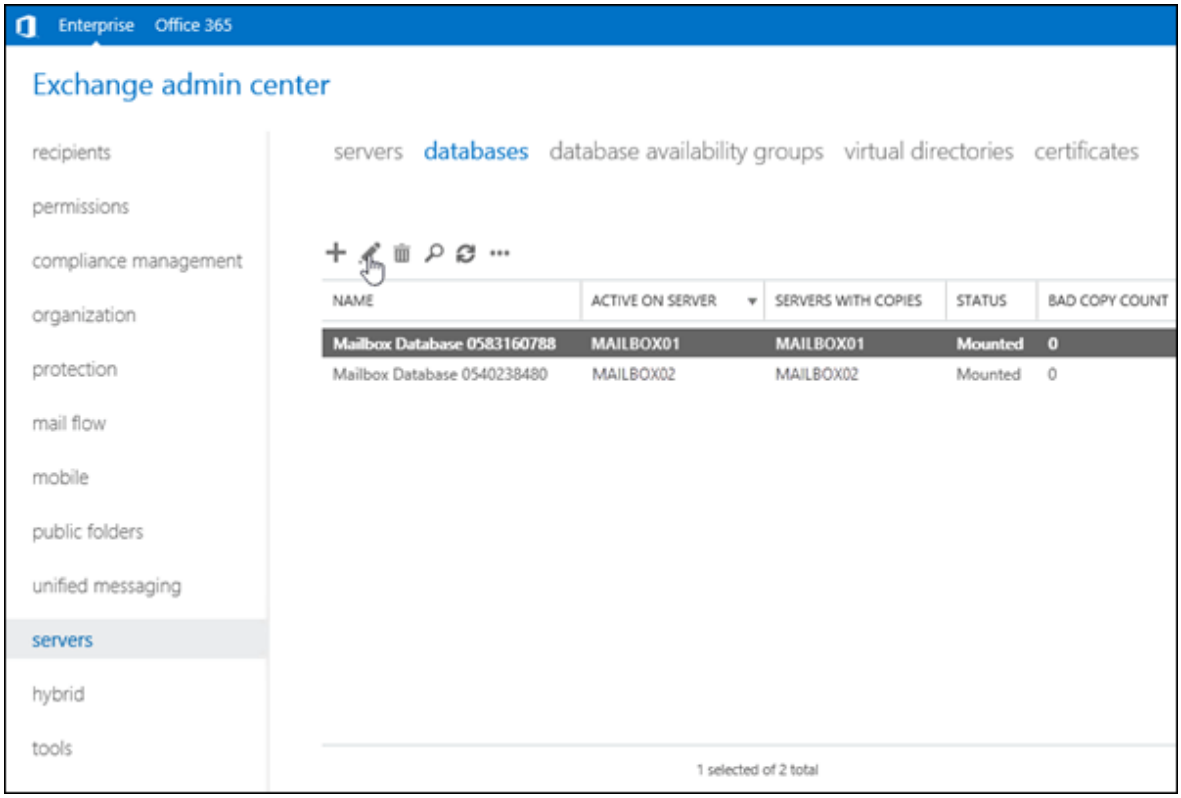
Назначение автономных адресных книг базам данных почтовых ящиков

При назначении автономной адресной адресной области базе данных почтовых ящиков все почтовые ящики в базах данных будут использовать эту автономную адресную адресную книгу вместо автономной адресной записи по умолчанию, если почтовому ящику не назначена автономная адресная запись. По умолчанию базам данных почтовых ящиков не назначается автономная адресная адресная область.

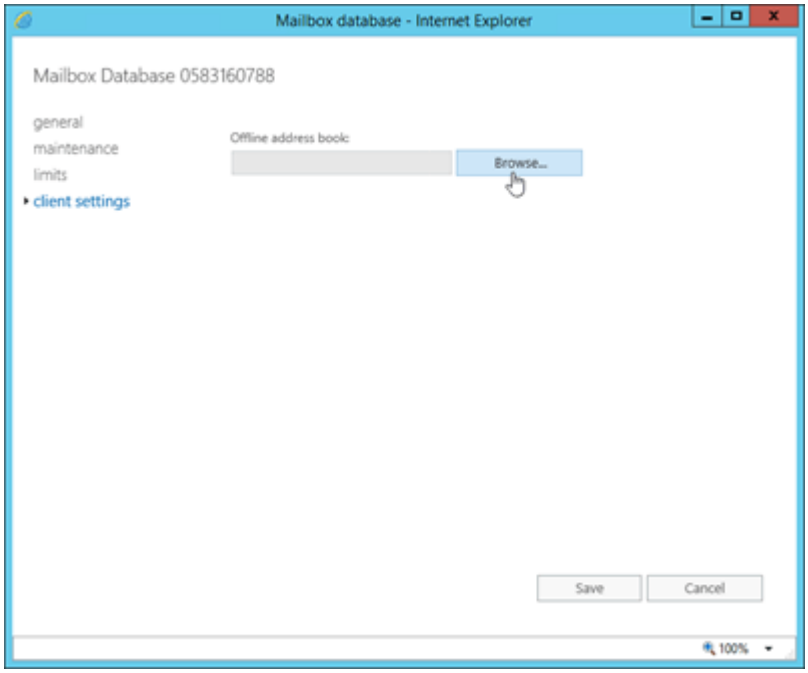
Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Базы данных почтовых ящиков" в разделе Разрешения получателей .

Использование EAC для назначения автономной адресной книги базе данных почтового ящика

1. Откройте EAC и выберите **Серверы**>**Базы данных**. Выберите базу данных из списка и нажмите кнопку **Изменить** (



2. Откроется окно **База данных почтовых ящиков** . Перейдите на вкладку **Параметры клиента** и нажмите кнопку **Обзор** рядом с **параметром Автономная адресная книга**.



3. В открывающемся окне **Выбор автономной адресной книги** выберите автономную адресную книгу из списка и нажмите кнопку **OK**.

4. В окне **База данных почтовых ящиков** нажмите кнопку **Сохранить**.

Использование командной консоли Exchange для назначения автономной адресной книги базе данных почтовых ящиков

Используйте следующий синтаксис.

```
PowerShell

Set-MailboxDatabase -Identity <DatabaseIdentity> -OfflineAddressBook
<OABIdentity>
```

В этом примере автономная адресная папка Contoso Executives назначается базе данных почтовых ящиков MBX DB02.

```
PowerShell

Set-MailboxDatabase -Identity "MBX DB02" -OfflineAddressBook "Contoso
Executives OAB"
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно назначили автономную адресную книгу базе данных почтовых ящиков, выполните одно из следующих действий:

- В EAC выберите **Серверы**>**Базы данных**. Выберите базу данных из списка и нажмите кнопку **Изменить** (✎ В открывшейся окне **База данных почтовых ящиков** перейдите на вкладку **Параметры клиента** и убедитесь, что автономная адресная книга указана в **автономной адресной книге**.
- В командной консоли Exchange выполните следующую команду:

  ```
  PowerShell

  Get-MailboxDatabase | Format-Table -Auto Name,OfflineAddressBook
  ```

Использование командной консоли Exchange для назначения автономных адресных книг почтовым ящикам

При назначении автономной адресной адресной записи почтовому ящику почтовый ящик не используются автономной адресной адресом по умолчанию и

автономная адресная запись, назначенная базе данных почтового ящика (если она имеется). По умолчанию почтовому ящику не назначается автономная адресная адресная адрес.

Примечание. Если почтовому ящику назначена политика адресной книги (ABP), а в ABP определена автономная адресная книга, то эта автономная адресная книга будет иметь приоритет над ABP. Дополнительные сведения см. в статье Политики адресных книг в Exchange Server.

Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения подготовки получателей" раздела Разрешения получателей .

Чтобы назначить автономную адресную книгу почтовому ящику, используйте следующий синтаксис:

PowerShell

```
Set-Mailbox -Identity <MailboxIdentity> -OfflineAddressBook <OABIdentity>
```

В этом примере почтовому ящику laura@contoso.comназначается автономная адресная адресная адресная папка Contoso Executives .

PowerShell

```
Set-Mailbox -Identity laura@contoso.com -OfflineAddressBook "Contoso
Executives OAB"
```

В этом примере OAB с именем Contoso US назначается отфильтрованный список почтовых ящиков.

PowerShell

```
$USContoso = Get-User -ResultSize Unlimited -Filter "RecipientType -eq
'UserMailbox' -and Company -eq 'Contoso' -and CountryOrRegion -eq 'US'";
$USContoso | foreach {Set-Mailbox $_.Identity -OfflineAddressBook "Contoso
United States"}
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно назначили автономную адресную книгу почтовому ящику, замените *<MailboxIdentity>* идентификатором почтового ящика и выполните следующую команду:

PowerShell

```
Get-Mailbox -Identity "<MailboxIdentity>" | Format-Table -Auto
Name,OfflineAddressBook
```

Списки адресов в Exchange Server

Статья • 04.04.2023

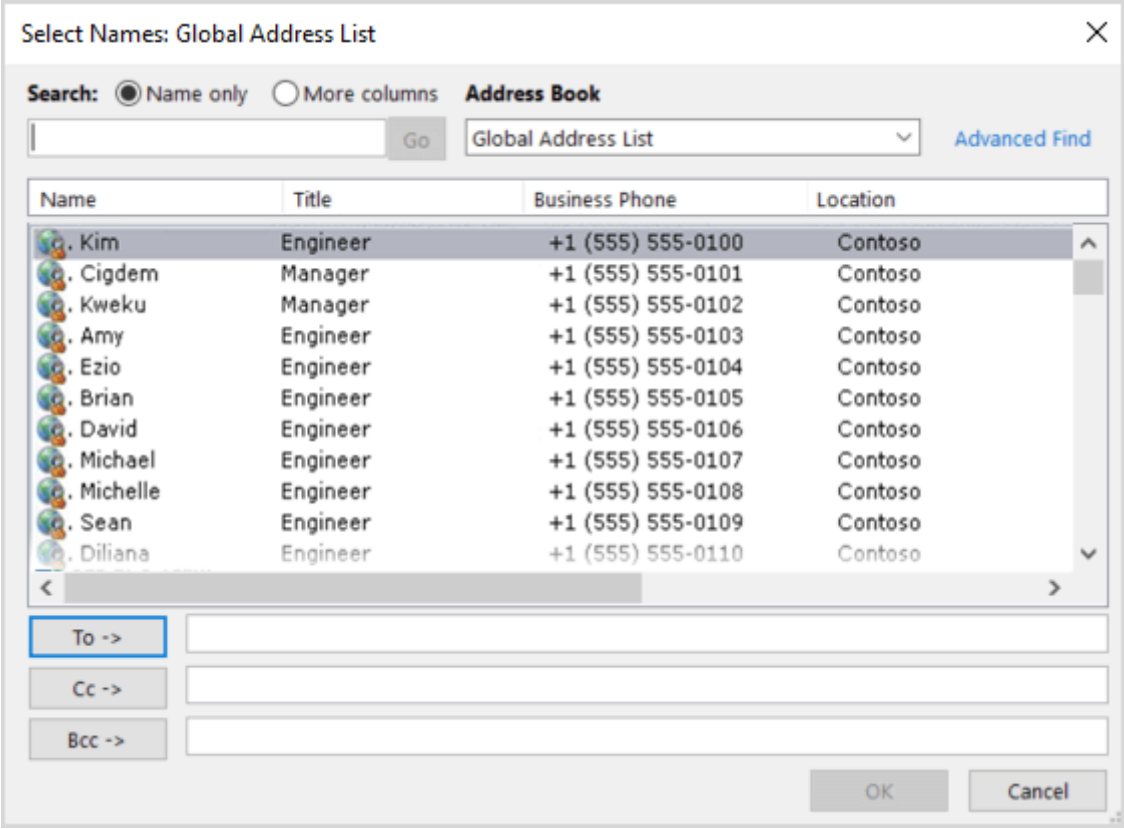
Список адресов — это коллекция объектов получателей с поддержкой почты из Active Directory. Списки адресов основаны на фильтрах получателей и в основном не изменяются по сравнению с Exchange 2010. Вы можете выполнять фильтрацию по типу получателя (например, почтовым ящикам и почтовым контактам), свойствам получателя (например, компании, штата или провинции) или по обоим. Списки адресов не являются статическими; они обновляются динамически. При создании или изменении получателей в организации они автоматически добавляются в соответствующие списки адресов. Доступны следующие типы списков адресов:

- **Глобальные списки адресов (GALs).** Встроенный глобальный список адресов, автоматически создаваемый Exchange, включает каждый объект с поддержкой почты в лесу Active Directory. Вы можете создать дополнительные общедоступные лицензии, чтобы разделить пользователей по организации или расположению, но пользователь может видеть и использовать только один глобальный глобальный список.

- **Списки адресов**. Списки адресов — это подмножества получателей, которые сгруппированы в один список, что упрощает их поиск пользователями. Exchange поставляется с несколькими встроенными списками адресов, и вы можете создавать дополнительные списки на основе потребностей организации.

- **Автономные адресные книги (OAB): OAB** содержат списки адресов и общедоступные лицензии. OAB используются клиентами Outlook в кэшированном режиме Exchange для предоставления локального доступа к спискам адресов и общедоступным спискам для поиска получателей. Дополнительные сведения см. в статье Автономные адресные книги в Exchange Server.

Пользователи в вашей организации используют списки адресов и глобальный список адресов для поиска получателей сообщений электронной почты. Ниже приведен пример того, как выглядят списки адресов в Outlook 2016:



Процедуры, связанные со списками адресов, см. в разделе Процедуры для списков адресов в Exchange Server.

Фильтры получателей для списков адресов

Фильтры получателей идентифицируют получателей, включенных в списки адресов и общедоступные лицензии. Существует два основных варианта фильтров получателей: **заранее подготовленные** и **пользовательские**. В основном это те же параметры фильтрации получателей, которые используются динамическими группами рассылки и политиками адресов электронной почты. В приведенной ниже таблице представлена сводка различий между двумя способами фильтрации.

Способ фильтрации получателей	Пользовательский интерфейс	Фильтруемые свойства получателей	Операторы фильтра

Способ фильтрации получателей	Пользовательский интерфейс	Фильтруемые свойства получателей	Операторы фильтра
Заранее подготовленные фильтры получателей	**Списки адресов**: Центр администрирования Exchange (EAC) и командная консоль Exchange **Общедоступные лицензии**: только командная консоль Exchange	Поддерживаются только: • тип получателя (все типы получателей или любое сочетание почтовых ящиков пользователей, почтовых ящиков ресурсов, почтовых контактов, почтовых пользователей и групп); • компания; • настраиваемый атрибут от 1 до 15; • отдел; • область или район.	Значения свойств должны полностью совпадать. Подстановочные знаки и частичные совпадения не поддерживаются. Например, значение "Продажи" не совпадает со значением "Продажи и маркетинг". Чтобы задать несколько значений для одного и того же свойства, всегда используйте оператор **or**. Пример: "Отдел равно Продажи или Отдел равно Маркетинг". Чтобы задать несколько свойств, всегда используется оператор **and**. Пример: "Отдел равно Продажи и Компания равно Contoso".
Пользовательские фильтры получателей	Только в Командная консоль Exchange	Можно использовать практически любые доступные атрибуты получателей. Дополнительные сведения см. в разделе Фильтруемые свойства для параметра - RecipientFilter.	Используйте синтаксис фильтра OPATH, чтобы задавать доступные операторы фильтра в Оболочка Windows PowerShell. Подстановочные знаки и частичные совпадения поддерживаются.

Примечания.

- Одновременно использовать заранее подготовленные и пользовательские фильтры невозможно.
- Расположение получателя в Active Directory (в подразделении или контейнере) доступно как в заранее подготовленных, так и в

пользовательских фильтрах получателей.

- Если в списке адресов используются пользовательские фильтры получателей, а не предварительно настроенные фильтры, список адресов можно просмотреть в EAC, но его нельзя изменить или удалить с помощью EAC.

- Вы можете скрыть получателей из всех списков адресов и общедоступных лицензий. Дополнительные сведения см. в разделе Скрытие получателей из списков адресов.

Глобальные списки адресов

По умолчанию новая установка Exchange Server создает глобальный список адресов по умолчанию, который является основным репозиторием всех получателей в организации Exchange. Как правило, в большинстве организаций есть только один глобальный список адресов, так как пользователи могут видеть и использовать только один глобальный список в Outlook и Outlook в Интернете (ранее — Outlook Web App). Если вы хотите запретить группам получателей видеть друг друга, может потребоваться создать несколько общедоступных лицензий (например, одна организация Exchange содержит две отдельные компании). Если вы планируете создать дополнительные общедоступные лицензии, рассмотрите следующие проблемы:

- Командная консоль Exchange может использоваться только для создания, изменения, удаления и обновления общедоступных лицензий.

- Глобальный список адресов, отображаемый пользователями в Outlook и Outlook в Интернете, называется "Глобальный список адресов", несмотря на то, что глобальный список адресов по умолчанию называется "Глобальный список адресов по умолчанию", а для всех созданных вами глобальных лицензий потребуется уникальное имя (пользователи не могут определить, какой глобальный список адресов используется по имени).

- Пользователи могут видеть только глобальный список адресов, к которому они принадлежат (фильтр получателей глобального списка адресов включает их). Если пользователь принадлежит к нескольким общедоступным спискам, он по-прежнему будет видеть только один глобальный список на основе следующих условий:

    - Пользователю требуются разрешения для просмотра глобального списка адресов. Разрешения пользователей назначаются общедоступным спискам

с помощью политик адресной книги (ASP). Дополнительные сведения см. в разделе Политики адресных книг в Exchange Server.

- Если пользователь по-прежнему имеет право на просмотр нескольких общедоступных лицензий, используется только самый большой глобальный список (глобальный список, содержащий большинство получателей).
- Каждой глобальной адресной книге требуется соответствующая автономная адресная книга (OAB), включающая глобальный список адресов. Сведения о создании автономных адресных книг см. в статье Создание автономных адресных книг с помощью командной консоли Exchange.

Списки адресов по умолчанию

По умолчанию Exchange поставляется с пятью встроенными списками адресов и одним глобальным списком адресов. Эти списки адресов описаны в следующей таблице. Обратите внимание, что по умолчанию связанные с системой почтовые ящики, такие как почтовые ящики арбитража и почтовые ящики общедоступных папок, скрыты из списков адресов.

Имя	Тип	Описание	Используемый фильтр получателей
Все контакты.	Список адресов	Включает все почтовые контакты в организации. Дополнительные сведения о почтовых контактах см. в разделе Получатели.	`"Alias -ne $null -and (ObjectCategory -like 'person' -and ObjectClass -eq 'contact')"`
Все списки рассылки.	Список адресов	Включает все группы рассылки и группы безопасности с поддержкой почты в организации. Дополнительные сведения о группах с поддержкой почты см. в разделе Получатели.	`"Alias -ne $null -and ObjectCategory -like 'group'"`

Имя	Тип	Описание	Используемый фильтр получателей
Все помещения	Список адресов	Включает все почтовые ящики комнат. Почтовые ящики оборудования не включены. Дополнительные сведения о почтовых ящиках помещений и оборудования (ресурсов) см. в разделе Получатели.	`"Alias -ne $null -and (RecipientDisplayType -eq 'ConferenceRoomMailbox' -or RecipientDisplayType -eq 'SyncedConferenceRoomMailbox')"`
Все пользователи	Список адресов	Включает все почтовые ящики пользователей, связанные почтовые ящики, удаленные почтовые ящики (Microsoft 365 или Office 365 почтовые ящики), общие почтовые ящики, почтовые ящики комнат, почтовые ящики оборудования и почтовые ящики пользователей в организации. Дополнительные сведения об этих типах получателей см. в статье Получатели.	`"((Alias -ne $null) -and (((((((ObjectCategory -like 'person') -and (ObjectClass -eq 'user') -and (-not(Database -ne $null)) -and (-not(ServerLegacyDN -ne $null)))) -or (((ObjectCategory -like 'person') -and (ObjectClass -eq 'user') -and (((Database -ne $null) -or (ServerLegacyDN -ne $null))))))) -and (-not(RecipientTypeDetailsValue -eq 'GroupMailbox'))))))"`
Глобальный список адресов по умолчанию.	Гал	Включает все объекты получателей с поддержкой почты в организации (пользователи, контакты, группы, динамические группы рассылки и общедоступные папки).	`"((Alias -ne $null) -and (((ObjectClass -eq 'user') -or (ObjectClass -eq 'contact') -or (ObjectClass -eq 'msExchSystemMailbox') -or (ObjectClass -eq 'msExchDynamicDistributionList') -or (ObjectClass -eq 'group') -or (ObjectClass -eq 'publicFolder'))))"`

Имя	Тип	Описание	Используемый фильтр получателей
Общедоступные папки	Список адресов	Включает все общедоступные папки с поддержкой почты в вашей организации. Разрешения доступа определяют, кто может просматривать и использовать общедоступные папки. Дополнительные сведения об общедоступных папках см. в разделе Общедоступные папки.	`"Alias -ne $null -and ObjectCategory -like 'publicFolder'"`

Custom address lists

Организация Exchange может содержать тысячи получателей, поэтому встроенные списки адресов могут стать довольно большими. Чтобы избежать этого, можно создать настраиваемые списки адресов, которые помогут пользователям найти то, что они ищут.

Например, рассмотрим компанию, которая имеет два крупных подразделения в одной организации Exchange:

- Четвертый кофе, который импортирует и продает кофейные бобы.
- Contoso, Ltd, которая выполняет страховые полисы.

Для большинства повседневных мероприятий сотрудники Компании Fourth Coffee не общаются с сотрудниками Contoso, Ltd. Таким образом, чтобы сотрудникам было проще находить получателей, которые существуют только в их подразделении, можно создать два новых списка адресов: один для Fourth Coffee и один для Contoso, Ltd. Однако если сотрудник не знаете, где существует получатель, он может выполнить поиск в глобальном списке, который содержит всех получателей из обоих подразделений.

Вы также можете создавать списки адресов в других списках адресов. Например, можно создать список адресов, содержащий всех получателей в Манчестере, и другой список адресов в манчестере с именем Продажи, содержащий только продавцов в офисе Манчестера. Вы также можете переместить списки адресов обратно в корневой каталог или в другие списки адресов после их создания.

Дополнительные сведения см. в статье Перемещение списков адресов с помощью командной консоли Exchange.

Рекомендации по созданию дополнительных списков адресов

Несмотря на всю полезность списков адресов, при плохом планировании они могут вызывать затруднения. Чтобы списки адресов можно было эффективно использовать, соблюдайте указанные ниже рекомендации.

- Списки адресов должны облегчить пользователям поиск получателей.
- Избегайте создания столько списков адресов, что пользователи не могут определить, какой список следует использовать.
- Используйте соглашение об именовании и иерархию расположений для списков адресов, чтобы пользователи могли сразу же определить, для чего предназначен список (какие получатели включены в список). Если выбрать имена для списков адресов трудно, уменьшите число списков и напомните пользователям, что в глобальном списке адресов можно найти сведения обо всех сотрудниках организации.

Подробные инструкции по созданию списков адресов в Exchange Server см. в разделе Создание списков адресов.

Обновление списков адресов

После создания или изменения списка адресов необходимо обновить членство.

Если список адресов содержит большое количество получателей (наша рекомендация превышает 3000), следует использовать командную консоль Exchange, чтобы обновить список адресов (а не EAC). Дополнительные сведения см. в разделе Обновление списков адресов.

Чтобы обновить глобальный список адресов, всегда необходимо использовать командную консоль Exchange. Дополнительные сведения см. в статье Обновление глобальных списков адресов с помощью командной консоли Exchange.

Процедуры для списков адресов в Exchange Server

Статья • 04.04.2023

Списки адресов и глобальные списки адресов (GALs) — это коллекции объектов получателей с поддержкой почты из Active Directory. Вы можете создавать или изменять общедоступные лицензии, а также обновлять их с помощью средств, доступных в Центре администрирования Exchange (EAC) и командной консоли Exchange. Дополнительные сведения см. в разделе Списки адресов в Exchange Server.

Ниже приведен список адресов и процедуры gal, которые вы найдете в этом разделе:

- **Процедуры глобального списка адресов**
  - Обновление глобальных списков адресов с помощью командной консоли Exchange
  - Использование командной консоли Exchange для просмотра членов глобальных списков адресов
  - Создание глобальных списков адресов с помощью командной консоли Exchange
  - Изменение глобальных списков адресов с помощью командной консоли Exchange
  - Удаление глобальных списков адресов с помощью командной консоли Exchange
- **Процедуры списка адресов**
  - Обновление списков адресов
  - Просмотр членов списков адресов
  - Создание списков адресов
  - Изменение списков адресов
  - Перемещение списков адресов с помощью командной консоли Exchange
  - Удаление списков адресов

- Скрытие получателей в списках адресов

Фильтры получателей в Центре администрирования Exchange

Фильтры получателей в командной консоли Exchange

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Списки адресов" в разделе разрешения Email адресной книги.
- Некоторые процедуры, описанные в этом разделе, можно выполнить с помощью EAC. Дополнительные сведения о EAC см. в разделе Центр администрирования Exchange в Exchange Server. Для некоторых процедур требуется командная консоль Exchange. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Процедуры глобального списка адресов

Для всех процедур изменения или обновления глобального списка адресов требуется командная консоль Exchange.

Обновление глобальных списков адресов с помощью командной консоли Exchange

После создания или изменения глобального списка адресов необходимо обновить его членство. Обновление глобального списка адресов запускает только процесс

обновления. Для завершения обновления глобального списка адресов может потребоваться несколько часов.

Чтобы обновить глобальный список адресов, используйте следующий синтаксис:

```
PowerShell

Update-GlobalAddressList -Identity <GALIdentity>
```

В этом примере обновляется глобальный список адресов с именем Contoso GAL.

```
PowerShell

Update-AddressList -Identity "Contoso GAL"
```

В этом примере обновляются все общедоступные лицензии в организации, для которых требуются обновления.

```
PowerShell

Get-GlobalAddressList | where {$_.RecipientFilterApplied -eq $false} |
Update-GlobalAddressList
```

Подробные сведения о синтаксисе и параметрах см. в разделе Update-GlobalAddressList.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно обновили глобальный список адресов, замените *<GALIdentity>* именем списка адресов и выполните следующую команду, чтобы убедиться в наличии значения свойства **RecipientFilterApplied** :

```
PowerShell

Get-AddressList -Identity <GALIdentity> | Format-Table -Auto
Name,RecipientFilterApplied
```

Использование командной консоли Exchange для просмотра членов глобальных списков адресов

- Технически эта процедура возвращает *всех* получателей (включая скрытых получателей), которые соответствуют фильтрам получателей для глобального

списка адресов. Получатели, фактически видимые в глобальном списке, имеют значение `False` свойства **HiddenFromAddressListsEnabled** .

- Если глобальный список адресов не обновлен (свойство **RecipientFilterApplied** имеет значение `False`), необходимо обновить глобальный список адресов перед просмотром участников. Дополнительные сведения см. в предыдущем разделе.

Чтобы просмотреть члены глобального списка адресов, используйте следующий синтаксис:

PowerShell

```
$GAL = Get-GlobalAddressList -Identity <GALIdentity>; Get-Recipient -
ResultSize unlimited -RecipientPreviewFilter $GAL.RecipientFilter | select
Name,PrimarySmtpAddress,HiddenFromAddressListsEnabled
```

В этом примере возвращаются члены gal с именем Humongous Insurance.

PowerShell

```
$GAL = Get-GlobalAddressList -Identity "Humongous Insurance"; Get-Recipient
-ResultSize unlimited -RecipientPreviewFilter $GAL.RecipientFilter | select
Name,PrimarySmtpAddress,HiddenFromAddressListsEnabled
```

В этом примере результаты экспортируются в файл C:\My Documents\Humongous Insurance Export.csv.

PowerShell

```
$GAL = Get-GlobalAddressList -Identity "Humongous Insurance"; Get-Recipient
-ResultSize unlimited -RecipientPreviewFilter $GAL.RecipientFilter | select
Name,PrimarySmtpAddress,HiddenFromAddressListsEnabled | Export-Csv -
NoTypeInformation -Path "C:\My Documents\Humongous Insurance Export.csv"
```

Создание глобальных списков адресов с помощью командной консоли Exchange

Дополнительные сведения о требованиях и последствиях использования нескольких общедоступных лицензий в организации см. в статье Глобальные списки адресов.

Дополнительные сведения о фильтрах получателей в командной консоли Exchange см. в разделе Фильтры получателей в командной консоли Exchange этой статьи.

Чтобы создать глобальный список адресов, используйте следующий синтаксис:

PowerShell

```
New-GlobalAddressList -Name "<GAL Name>" [<Precanned recipient filter | Custom recipient filter>]
```

В этом примере создается глобальный список адресов с предварительно заданным фильтром получателей:

- **Имя**: Contoso GAL
- **Фильтр предварительно настроенных получателей**: все типы получателей, где значение **Company** — Contoso.

PowerShell

```
New-GlobalAddressList -Name "Contoso GAL" -IncludedRecipients AllRecipients -ConditionalCompany Contoso
```

В этом примере создается глобальный список адресов с настраиваемым фильтром получателей:

- **Имя**: Агентство A GAL
- **Настраиваемый фильтр получателей**: все типы получателей, в которых свойство CustomAttribute15 содержит значение AgencyA.

PowerShell

```
New-GlobalAddressList -Name "Agency A GAL" -RecipientFilter "CustomAttribute15 -like '*AgencyA*'"
```

Подробные сведения о синтаксисе и параметрах см. в разделе New-GlobalAddressList.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно создали глобальный список адресов, используйте один из следующих процедур:

- В EAC перейдите в**раздел Списки адресоворганизации**>, выберите список адресов и нажмите кнопку **Изменить** (✎

- В командной консоли Exchange замените *<GAL Name>* именем глобального списка и выполните следующую команду, чтобы проверить значения свойств:

```
PowerShell

Get-GlobalAddressList -Identity "<GAL Name>" | Format-List
Name,RecipientFilterType,RecipientContainer,RecipientFilter,IncludedRec
ipients,Conditional*
```

Изменение глобальных списков адресов с помощью командной консоли Exchange

- Доступны те же параметры, что и при создании глобального списка адресов. Дополнительные сведения см. в предыдущем разделе.
- После изменения глобального списка адресов необходимо обновить его членство. Дополнительные сведения см. в разделе Использование командной консоли Exchange для обновления глобальных списков адресов этой статьи.
- Вы не можете заменить настраиваемый фильтр получателей предварительно настроенным фильтром получателей или наоборот в существующем глобальном списке адресов.

Чтобы изменить глобальный список адресов, используйте следующий синтаксис:

```
PowerShell

Set-GlobalAddressList -Identity <GALIdentity>] [-Name <Name>] [<Precanned
recipient filter | Custom recipient filter>] [-RecipientContainer
<OrganizationalUnit>]
```

При изменении значений *условного* параметра можно использовать следующий синтаксис для добавления или удаления значений, не затрагивая другие существующие значения: `@{Add="<Value1>","<Value2>"...; Remove="<Value1>","<Value2>"...}`.

В этом примере изменяется существующий gal с именем Contoso GAL, добавляя значение **Company** Fabrikam в предварительно настроенный фильтр получателей.

```
PowerShell

Set-GlobalAddressList -Identity "Contoso GAL" -ConditionalCompany
@{Add="Fabrikam"}
```

Подробные сведения о синтаксисе и параметрах см. в разделе Set-GlobalAddressList.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно изменили глобальный список адресов, используйте один из следующих процедур:

- В EAC перейдите в**раздел Списки адресоворганизации**>, выберите список адресов и нажмите кнопку **Изменить** (✎

- В командной консоли Exchange замените <*GAL Name*> именем глобального списка и выполните следующую команду, чтобы проверить значения свойств:

  PowerShell

  ```
  Get-GlobalAddressList -Identity "<GAL Name>" | Format-List Name,RecipientFilterType,RecipientContainer,RecipientFilter,IncludedRecipients,Conditional*
  ```

Удаление глобальных списков адресов с помощью командной консоли Exchange

- Невозможно удалить глобальный список адресов с именем Автономная адресная книга по умолчанию, который представляет собой глобальный список адресов, автоматически создаваемый Exchange, и единственный глобальный список, имеющий значение `True`свойства **IsDefaultGlobalAddressList**.

- Невозможно удалить глобальный список адресов, определенный в автономной адресной книге (OAB). Сведения об изменении списков адресов, определенных в автономной адресной книге, см. в статье Использование командной консоли Exchange для добавления и удаления списков адресов из автономных адресных книг.

Чтобы удалить глобальный список адресов, используйте следующий синтаксис:

PowerShell

```
Remove-GlobalAddressList -Identity <GALIdentity>
```

В этом примере удаляется список адресов с именем Agency A GAL.

PowerShell

```
Remove-GlobalAddressList -Identity "Agency A GAL"
```

Подробные сведения о синтаксисе и параметрах см. в разделе Remove-GlobalAddressList.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно удалили глобальный список адресов, выполните одно из следующих действий:

- В EAC перейдите в раздел**Списки адресоворганизации**> и убедитесь, что глобальный список больше не указан.
- В командной консоли Exchange выполните следующую команду, чтобы убедиться, что глобальный список адресов отсутствует в списке:

  PowerShell

  ```
  Get-GlobalAddressList
  ```

Процедуры списка адресов

Обновление списков адресов

После создания или изменения списка адресов в Центре администрирования Exchange или командной консоли Exchange необходимо обновить членство в списке адресов.

- Если список адресов содержит более 3000 получателей, рекомендуется использовать командную консоль Exchange для обновления списка адресов. Обновление членства в списке адресов займет много времени и не позволит использовать сеанс EAC, пока список адресов не будет полностью обновлен.
- Если список адресов содержит менее 3000 получателей, можно использовать EAC.

Обновление списков адресов с помощью EAC

1. В центре администрирования EAC перейдите в**раздел Списки адресоворганизации**> и выберите список адресов, который требуется обновить.

    - Если список адресов необходимо обновить, в области сведений **появится раздел Не обновлен** со ссылкой **Обновить** . Нажмите кнопку **Обновить**.

    - Если список адресов уже обновлен, вы увидите, **что этот список адресов обновлен** в области сведений.

2. После нажатия кнопки **Обновить** появится предупреждающее сообщение. Нажмите кнопку **Да** , чтобы обновить список адресов с помощью Центра администрирования EAC. Индикатор выполнения позволяет отслеживать процесс обновления. После завершения обновления нажмите кнопку **Закрыть**.

Обновление списков адресов с помощью командной консоли Exchange

Чтобы обновить список адресов, используйте следующий синтаксис:

```
PowerShell

Update-AddressList -Identity [<AddressListIdentity>]
```

В этом примере обновляется список адресов с именем Northwest Executives.

```
PowerShell

Update-AddressList -Identity "Northwest Executives"
```

В этом примере обновляется список адресов с именем Продажи, расположенный в списке адресов с именем Северная Америка.

```
PowerShell

Update-AddressList "North America\Sales"
```

В этом примере обновляются все списки адресов в организации, для которых требуются обновления.

```
PowerShell
```

```
Get-AddressList | where {$_.RecipientFilterApplied -eq $false} | Update-AddressList
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе Update-AddressList.

Как проверить, все ли получилось?

Чтобы убедиться, что список адресов успешно обновлен, выполните одно из следующих действий:

- В Центре администрирования Майкрософт перейдите в**раздел Списки адресоворганизации**>, выберите список адресов и убедитесь, что в области **сведенийотображается актуальный список адресов** (а не не обновлен по ссылке **Обновить**).
- В командной консоли Exchange замените <*AddressListIdentity*> именем списка адресов и выполните следующую команду, чтобы проверить значение свойства **RecipientFilterApplied** :

  PowerShell

  ```
  Get-AddressList -Identity <AddressListIdentity> | Format-Table -Auto Name,RecipientFilterApplied
  ```

Просмотр членов списков адресов

Если список адресов не обновлен, необходимо обновить список адресов перед просмотром участников. Дополнительные сведения см. в предыдущем разделе.

Использование EAC для просмотра членов списков адресов

1. В EAC перейдите в раздел**Списки адресоворганизации**>, выберите список адресов и нажмите кнопку **Изменить** (✎
2. Щелкните **Предварительный просмотр получателей, которые содержатся в списке адресов**.

Использование командной консоли Exchange для просмотра членов списков адресов

- Технически эта процедура возвращает *всех* получателей (включая скрытых получателей), которые соответствуют фильтрам получателей для списка адресов. Получатели, фактически видимые в списке адресов, имеют значение `False` свойства **HiddenFromAddressListsEnabled** .

Чтобы просмотреть члены списка адресов, используйте следующий синтаксис:

PowerShell

```
$AL = Get-AddressList -Identity <AddressListIdentity>; Get-Recipient -
ResultSize unlimited -RecipientPreviewFilter $AL.RecipientFilter | select
Name,PrimarySmtpAddress,HiddenFromAddressListsEnabled
```

В этом примере возвращаются члены списка адресов с именем Юго-Восточные офисы.

PowerShell

```
$AL = Get-AddressList -Identity "Southeast Offices"; Get-Recipient -
ResultSize unlimited -RecipientPreviewFilter $AL.RecipientFilter | select
Name,PrimarySmtpAddress,HiddenFromAddressListsEnabled
```

В этом примере результаты экспортируются в файл C:\My Documents\South Office Export.csv.

PowerShell

```
$AL = Get-AddressList -Identity "Southeast Offices"; Get-Recipient -
ResultSize unlimited -RecipientPreviewFilter $AL.RecipientFilter | select
Name,PrimarySmtpAddress,HiddenFromAddressListsEnabled | Export-Csv -
NoTypeInformation -Path "C:\My Documents\Southeast Offices Export.csv"
```

Создание списков адресов

Списки адресов можно создавать с помощью EAC или командной консоли Exchange. В EAC при создании списка адресов необходимо включить фильтр получателей, основанный на типе получателя (определенные типы или все получатели). В командной консоли Exchange не требуется включать фильтр получателей, основанный на типе получателя.

Создание списков адресов с помощью EAC

1. В EAC перейдите в**раздел Списки адресоворганизации**> и нажмите кнопку **Создать** (➕

2. В открывавшемся окне **списка адресов** настройте следующие параметры:

   - **Имя**. Введите уникальное описательное имя для списка адресов.

   - **Путь к списку адресов**. Список адресов можно создать в корневом каталоге ("***", также известном как Все списки адресов) или создать список адресов в существующем списке адресов. Чтобы создать список адресов в существующем списке адресов, нажмите кнопку **Обзор**, выберите список адресов в окне выбора и нажмите кнопку **ОК**.

   - Дополнительные сведения о фильтрах получателей и параметрах предварительного просмотра, доступных здесь, см. в разделе Фильтры получателей в EAC этой статьи.

3. По завершении нажмите кнопку **Сохранить**. Вы получите предупреждающее сообщение с сообщением о необходимости нажать кнопку **Обновить** в области сведений, чтобы обновить членство в списке адресов. Дополнительные сведения см. в разделе Обновление списков адресов этого раздела.

Создание списков адресов с помощью командной консоли Exchange

Вы можете создавать списки адресов как с фильтрами получателей, так и без них. Дополнительные сведения о фильтрах получателей в командной консоли Exchange см. в разделе Фильтры получателей в командной консоли Exchange этой статьи.

Чтобы создать список адресов, используйте следующий синтаксис:

PowerShell

```
New-AddressList -Name "<Address List Name>" [-Container
<ExistingAddressListPath>] [<Precanned recipient filter | Custom recipient
filter>] [-RecipientContainer <OrganizationalUnit>]
```

В этом примере создается список адресов с предварительно заданным фильтром получателей:

- **Название**: Юго-Восточные офисы

- **Расположение**: в корневом каталоге (" `\`, также известном как Все списки адресов), так как мы не использовали параметр *Container* , а значение по умолчанию — " `\`".

- **Предуклонированный фильтр получателей**: все пользователи с почтовыми ящиками, где значение **штата или провинции** — GA, AL или LA (Джорджия, Алабама или Луизиана).

```
PowerShell

New-AddressList -Name "Southeast Offices" -IncludedRecipients MailboxUsers -
ConditionalStateorProvince "GA","AL","LA"
```

В этом примере создается список адресов с настраиваемым фильтром получателей:

- **Имя**: Северо-Западные руководители

- **Расположение**: в существующем списке адресов с именем Северная Америка.

- **Настраиваемый фильтр получателей**: все пользователи с почтовыми ящиками, в которых значение **Title** содержит Director или Manager, а значение **штата или провинции** — WA, OR или ID (Вашингтон, Орегон или Айдахо).

```
PowerShell

New-AddressList -Name "Northwest Executives" -Container "\North America"-
RecipientFilter "(RecipientType -eq 'UserMailbox') -and (Title -like
'*Director*' -or Title -like '*Manager*') -and (StateOrProvince -eq 'WA' -or
StateOrProvince -eq 'OR' -or StateOrProvince -eq 'ID')"
```

Подробные сведения о синтаксисе и параметрах см. в разделе New-AddressList.

Как проверить, все ли получилось?

Чтобы убедиться, что список адресов успешно создан, выполните одно из следующих действий:

- В EAC перейдите в**раздел Списки адресоворганизации**>, выберите список адресов и нажмите кнопку **Изменить** (

- В командной консоли Exchange замените *[<AddressListPath>]* *<AddressListName>* именем и (при необходимости) расположением списка

адресов и выполните следующую команду, чтобы проверить значения свойств:

```
PowerShell

Get-AddressList -Identity "[<AddressListPath>\]<AddressListName>" | Format-List Name,RecipientFilterType,RecipientContainer,RecipientFilter,IncludedRecipients,Conditional*
```

Изменение списков адресов

- Если вы создали список адресов без фильтров получателей или настраиваемый фильтр получателей в командной консоли Exchange, вы не сможете изменить список адресов в EAC. Необходимо использовать командную консоль Exchange.
- После изменения списка адресов необходимо обновить его членство. Дополнительные сведения см. в разделе Обновление списков адресов этого раздела.
- Вы не можете заменить настраиваемый фильтр получателей предварительно настроенным фильтром получателей или наоборот в существующем списке адресов.
- Расположение списка адресов можно изменить с помощью командлета **Move-AddressList** в командной консоли Exchange. Дополнительные сведения см. в разделе Перемещение списков адресов с помощью командной консоли Exchange .

Изменение списков адресов в EAC

1. В EAC перейдите в раздел**Списки адресоворганизации**>, выберите список адресов и нажмите кнопку **Изменить** (✎
2. В открывающихся окнах **списка адресов** настройте следующие параметры:
   - **Отображаемое имя**. Введите уникальное описательное имя для списка адресов.
   - Дополнительные сведения о фильтрах получателей и параметрах предварительного просмотра, доступных здесь, см. в разделе Фильтры получателей в EAC этой статьи.

3. По завершении нажмите кнопку **Сохранить**. Вы получите предупреждающее сообщение с сообщением о необходимости нажать кнопку **Обновить** в области сведений, чтобы обновить членство в списке адресов. Дополнительные сведения см. в разделе Обновление списков адресов этого раздела.

Изменение списков адресов в командной консоли Exchange

- Доступны те же основные параметры, что и при создании списка адресов. Дополнительные сведения см. в разделе Создание списков адресов с помощью командной консоли Exchange .
- Эту процедуру нельзя использовать для перемещения списка адресов. Дополнительные сведения см. в разделе Перемещение списков адресов с помощью командной консоли Exchange .

Чтобы изменить существующий список адресов, используйте следующую синтаксическую конструкцию:

PowerShell

```
Set-AddressList -Identity <AddressListIdentity> [-Name <Name>] [<Precanned recipient filter | Custom recipient filter>] [-RecipientContainer <OrganizationalUnit>]
```

При изменении значений *условного* параметра можно использовать следующий синтаксис для добавления или удаления значений, не затрагивая другие существующие значения: `@{Add="<Value1>","<Value2>"...; Remove="<Value1>","<Value2>"...}`.

В этом примере изменяется существующий список адресов с именем "Юго-Восточные офисы", добавляя значение **штата или провинции** TX (Техас) в предканированный фильтр получателей.

PowerShell

```
Set-AddressList -Identity "Southeast Offices" -ConditionalStateOrProvince @{Add="TX"}
```

Подробные сведения о синтаксисе и параметрах см. в разделе Set-AddressList.

Как проверить, все ли получилось?

Чтобы убедиться, что список адресов успешно изменен, выполните одно из следующих действий:

- В EAC перейдите в**раздел Списки адресоворганизации**>, выберите список адресов и нажмите кнопку **Изменить** (✎
- В командной консоли Exchange замените <*AddressListIdentity*> путем\name списка адресов и выполните следующую команду, чтобы проверить значения свойств:

  PowerShell

  ```
  Get-AddressList -Identity "<AddressListIdentity>" | Format-List
  Name,RecipientFilterType,RecipientContainer,RecipientFilter,IncludedRec
  ipients,Conditional*
  ```

Перемещение списков адресов с помощью командной консоли Exchange

Расположение списка адресов можно выбрать при создании списка адресов в EAC или командной консоли Exchange. Но переместить существующий список адресов можно только с помощью командлета **Move-AddressList** в командной консоли Exchange. Если исходный список адресов содержит дочерние списки адресов, иерархия списков адресов перемещается в указанное целевое расположение.

Чтобы переместить список адресов, используйте следующий синтаксис:

PowerShell

```
Move-AddressList -Identity "<AddressListIdentity>" -Target "
<AddressListIdentity or \>"
```

В этом примере список адресов с именем "Юго-Восточные офисы" перемещается из корневого каталога ("`\`, также известного как Все списки адресов) в список адресов с именем Северная Америка.

PowerShell

```
Move-AddressList -Identity "Southeast Offices" -Target "North America"
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе Move-AddressList.

Как проверить, все ли получилось?

Чтобы убедиться, что список адресов успешно изменен, выполните одно из следующих действий:

- В EAC перейдите в**раздел Списки адресоворганизации**>, выберите список адресов и нажмите кнопку **Изменить** (✎

- В командной консоли Exchange замените <*AddressListIdentity*> путем\name списка адресов и выполните следующую команду, чтобы проверить значения свойств:

  PowerShell

  ```
  Get-AddressList -Identity "<AddressListIdentity>" | Format-List
  Name,RecipientFilterType,RecipientContainer,RecipientFilter,IncludedRec
  ipients,Conditional*
  ```

Удаление списков адресов

Если список адресов содержит более 3000 получателей, рекомендуется использовать командную консоль Exchange для удаления списка адресов. Удаление списка адресов займет много времени и не позволит использовать сеанс EAC, пока список адресов не будет полностью удален. Если список адресов содержит менее 3000 получателей, можно использовать EAC для удаления списка адресов.

- Невозможно удалить список адресов, определенный в автономной адресной книге (OAB). Сведения об изменении списков адресов, определенных в автономной адресной книге, см. в статье Использование командной консоли Exchange для добавления и удаления списков адресов из автономных адресных книг.

- Невозможно удалить список адресов, содержащий дочерние списки адресов (вы получите сообщение об ошибке). Сначала необходимо выполнить одно из следующих действий.

  - Используйте EAC для одновременного удаления родительского и всех дочерних списков адресов.

  - Используйте командную консоль Exchange для перемещения всех дочерних списков адресов в другое расположение с помощью командлета **Move-AddressList** .

Удаление списков адресов с помощью EAC

1. В EAC перейдите к**списку адресоворганизации**>.
2. Выберите список адресов или списки, которые нужно удалить, а затем нажмите кнопку **Удалить** (🗑 Вы можете выбрать несколько списков адресов, нажав клавишу CTRL при выборе каждого списка.
3. Нажмите **Да** в появившемся предупреждающем сообщении. Индикатор выполнения позволяет отслеживать процесс удаления. После завершения удаления нажмите **Закрыть**.

Удаление списков адресов с помощью командной консоли Exchange

Чтобы удалить список адресов, используйте следующую синтаксическую конструкцию:

```
PowerShell

Remove-AddressList -Identity "[<AddressListPath>\]<AddressListName>" [-
Recursive]
```

В этом примере список адресов с именем "Юго-Восточные офисы" и все его дочерние элементы удаляются из списка адресов Северная Америка.

```
PowerShell

Remove-AddressList -Identity "North America\Southeast Offices" -Recursive
```

Подробные сведения о синтаксисе и параметрах см. в разделе Remove-AddressList.

Как проверить, все ли получилось?

Чтобы убедиться, что список адресов успешно удален, выполните одно из следующих действий:

- В EAC перейдите в раздел**Списки адресоворганизации**> и убедитесь, что список адресов больше не указан.
- В командной консоли Exchange выполните следующую команду, чтобы убедиться, что список адресов отсутствует в списке:

  ```
  
  ```

PowerShell

```
Get-AddressList
```

Скрытие получателей в списках адресов

Скрытие получателя из списков адресов не препятствует получателю получать сообщения электронной почты; она не позволяет пользователям найти получателя в списках адресов. Получатель скрыт во **всех** списках адресов и в общих адресных книгах (фактически он является исключением в фильтрах получателей во всех списках адресов). Если вы хотите выборочно включить получателя в определенные списки адресов и не включать в другие, вам необходимо настроить фильтры получателей в списках адресов таким образом, чтобы включить или исключить получателя.

Скрытие почтового ящика из списков адресов также предотвращает поиск почтового ящика в глобальном списке при создании нового профиля или добавлении дополнительного почтового ящика в существующий профиль. Чтобы добавить скрытый почтовый ящик в Outlook, можно временно сделать почтовый ящик видимым в списках адресов, настроить Outlook, а затем снова скрыть его из списков адресов.

Использование EAC для скрытия получателей из списков адресов

1. В EAC перейдите в одно из следующих расположений в зависимости от типа получателя:

   - **Получателей**>**Почтовые ящики**: почтовые ящики пользователей, связанные почтовые ящики и удаленные почтовые ящики.
   - **Получателей**>**Группы**: группы рассылки, группы безопасности с поддержкой почты и динамические группы рассылки.
   - **Получателей**>**Ресурсы**: почтовые ящики помещений и оборудования.
   - **Получателей**>**Контакты**: почтовые пользователи и почтовые контакты.
   - **Получателей**>**Общий**: общие почтовые ящики.
   - **Общедоступные папки**>**Общедоступные папки**: общедоступные папки с поддержкой почты.

2. Выберите получателя, которого нужно скрыть из списков адресов, и нажмите кнопку **Изменить** (✎).

3. Откроется окно свойств получателя. Дальнейшие действия зависят от типа получателя:

   - **Почтовые ящики, контакты и общие**. На вкладке **Общие** выберите **Скрыть из списков адресов**.
   - **Группы**: на вкладке **Общие** нажмите **Скрыть эту группу в списке адресов**.
   - **Ресурсы**: на вкладке **Общие** нажмите **Дополнительные параметры**, а затем выберите параметр **Не отображать в списках адресов**.
   - **Общедоступные папки**: на вкладке **Общие свойства почты** нажмите **Не отображать в списке адресов Exchange**.

   По завершении нажмите **Сохранить**.

Использование командной консоли Exchange для скрытия получателей из списков адресов

Чтобы скрыть получателя из списков адресов, используйте следующий синтаксис:

PowerShell

```
Set-<RecipientType> -Identity <RecipientIdentity> -
HiddenFromAddressListsEnabled $true
```

<*RecipientType*> является одним из следующих значений:

- `DistributionGroup`
- `DynamicDistributionGroup`
- `Mailbox`
- `MailContact`
- `MailPublicFolder`
- `MailUser`
- `RemoteMailbox`

В этом примере группа рассылки с именем Internal Affairs скрывается из списков адресов.

PowerShell

```
Set-DistributionGroup -Identity "Internal Affairs" -
HiddenFromAddressListsEnabled $true
```

В этом примере почтовый ящик michelle@contoso.com скрывается из списков адресов.

PowerShell

```
Set-Mailbox -Identity michelle@contoso.com -HiddenFromAddressListsEnabled
$true
```

Примечания.

- Чтобы получатель снова отображался в списках адресов, используйте значение `$false` параметра *HiddenFromAddressListsEnabled* .
- По умолчанию почтовые ящики арбитража и почтовые ящики общедоступных папок скрыты из списков адресов. Если вы используете командлет **Set-Mailbox** для изменения этого или любого другого параметра для почтовых ящиков арбитража или общедоступных папок, необходимо включить параметры *Арбитраж* или *PublicFolder* .

Как проверить, все ли получилось?

Вы можете убедиться, что получатель успешно скрыт из списков адресов, выполнив любую из следующих процедур:

- В EAC выберите получателя, нажмите кнопку **Изменить** (✎) и убедитесь, что выбран параметр Скрыть из списков адресов.
- В командной консоли Exchange выполните следующую команду и убедитесь, что указан получатель:

  PowerShell

  ```
  Get-Recipient -ResultSize unlimited -Filter
  "HiddenFromAddressListsEnabled -eq `$true"
  ```

- Откройте глобальный список адресов в Outlook или Outlook в Интернете (прежнее название — Outlook Web App) и убедитесь, что получатель не отображается.

Фильтры получателей в Центре администрирования Exchange

При создании или изменении списков адресов в EAC доступны следующие параметры фильтра получателей:

- **Типы получателей для включения**
  - **Все получатели**

    или

  - **Только следующие типы получателей**: Выберите одно или несколько из следующих значений:
  - **Пользователи с почтовыми ящиками Exchange**
  - **Пользователи почты с внешними адресами электронной почты**
  - **Почтовые ящики ресурсов**
  - **Почтовые контакты с внешними адресами электронной почты**
  - **Группы с включенной поддержкой почты**
- **Создание правил для дальнейшего определения получателей**

1. Нажмите **Добавить правило** и выберите одно из свойств получателей в раскрывающемся списке:
   - **Контейнер получателя** (контейнер или подразделение);
   - **Область, край;**
   - **Компания;**
   - **Отдел;**
   - Настраиваемый атрибут от 1 до 15.
2. Введите значение для выбранного свойства:

- Если выбрать свойство **Контейнер получателя**, откроется диалоговое окно **Выбор подразделения**, в котором можно выбрать контейнер или подразделение в Active Directory.

- Для других свойств получателей открывается диалоговое окно **Определение слов или фраз**, в котором можно добавлять, изменять и удалять текстовые значения.

- Значения свойств должны полностью совпадать. Подстановочные знаки и частичные совпадения не поддерживаются. Например, значение "Продажи" не совпадает со значением "Продажи и маркетинг".

- Чтобы задать несколько значений для одного и того же свойства, используйте оператор **or**. Пример: "Отдел равно Продажи или Отдел равно Маркетинг".

3. Выбрав свойство и значение, нажмите **Добавить правило**.

4. Повторите предыдущие шаги, чтобы настроить дополнительные фильтры. Обратите внимание, что в нескольких свойствах используется оператор **and**. Пример: "Отдел равно Продажи и Компания равно Contoso".

   Предварительный просмотр получателей в списке адресов. При выборе этого параметра появляется диалоговое окно **предварительного просмотра** , в которое показано, какие получатели определены настроенными фильтрами.

Фильтры получателей в командной консоли Exchange

В командной консоли Exchange можно указать **заранее подготовленные** или **пользовательские фильтры получателей**, но не оба типа сразу.

- **Заранее подготовленные фильтры получателей**

  - Использует обязательный параметр *IncludedRecipient* со значением `AllRecipients` *или* одним или несколькими из следующих значений: `MailboxUsers`, `MailContacts`, `MailGroups`, `MailUsers` или `Resources`. Вы можете указать несколько значений, разделив их запятыми.

  - Можно также использовать любой из необязательных параметров *условного* фильтра: *ConditionalCompany*, *ConditionalCustomAttribute[1to15]*, *ConditionalDepartment* и *ConditionalStateOrProvince*.

Вы указываете несколько значений для *условного* параметра с помощью синтаксиса `"<Value1>","<Value2>"...`. При указании нескольких значений для одного свойства неявно используется оператор **or**. Пример: "Отдел равно Продажи или Маркетинг или Финансы".

- **Настраиваемые фильтры получателей**. Использует обязательный параметр *RecipientFilter* с фильтром OPATH.
  - Основной синтаксис фильтра OPATH — .`"<Property1> -<Operator> '<Value1>' <Property2> -<Operator> '<Value2>'..."`
  - Для всего фильтра OPATH требуются двойные кавычки `" "` . Хотя фильтр является строкой (не системным блоком), можно также использовать фигурные скобки `{ }`, но только в том случае, если фильтр не содержит переменные, требующие расширения.
  - Дефисы (`-`) требуются перед всеми операторами. Вот некоторые из наиболее часто используемых операторов:
  - `and`, `or` и `not`.
  - `eq` и `ne` (равно и не равно; без учета регистра).
  - `lt` и `gt` (меньше и больше).
  - `like` и `notlike` (строка содержит и не содержит; требуется по крайней мере один подстановочный знак в строке. Например, `"Department -like 'Sales*'"`.
  - Используйте круглые скобки для группировки `<Property> -<Operator> '<Value>'` операторов в сложных фильтрах. Например, `"(Department -like 'Sales*' -or Department -like 'Marketing*') -and (Company -eq 'Contoso' -or Company -eq 'Fabrikam')"`. Exchange сохраняет фильтр в свойстве **RecipientFilter**, заключая каждый оператор в круглые скобки, но их необязательно вводить в таком формате.
  - Дополнительные сведения см. в разделе Дополнительные сведения о синтаксисе OPATH.
  - После использования командлета **New-AddressList** для создания списка адресов, использующего настраиваемые фильтры получателей, вы не сможете изменить список адресов в EAC. Необходимо использовать

командлет **Set-AddressList** с параметром *RecipientFilter* в командной консоли Exchange.

Примечание. Параметр фильтра *получателей RecipientContainer* (подразделение) доступен как для предварительно настроенных фильтров получателей, так и для настраиваемых фильтров получателей.

Политики адресных книг в Exchange Server

Статья • 04.04.2023

Политики адресных книг позволяют администраторам разделять пользователей на группы и настраивать для них персонализированные представления глобального списка адресов (GAL) организации. Они призваны упростить механизм сегментации глобального списка адресов (т. н. *разделения GAL*) в локальных организациях, где требуется несколько таких списков.

Политика адресных книг содержит следующие элементы:

- Один глобальный список адресов. Дополнительные сведения о глобальных списках адресов см. в разделе Глобальные списки адресов.
- Одна автономная адресная книга. Дополнительные сведения о OAB см. в статье Автономные адресные книги в Exchange Server.
- Один список помещений. Обратите внимание, что этот список помещений является настраиваемым списком адресов, указывающим комнаты (содержит фильтр `RecipientDisplayType -eq 'ConferenceRoomMailbox'`). Это не средство поиска комнат, создаваемое с помощью параметра *RoomList* командлета **New-DistributionGroup** или **Set-DistributionGroup**. Дополнительные сведения см. в статье Создание почтовых ящиков комнат и управление ими.
- Один или несколько списков адресов. Дополнительные сведения о списках адресов см. в разделе Пользовательские списки адресов.

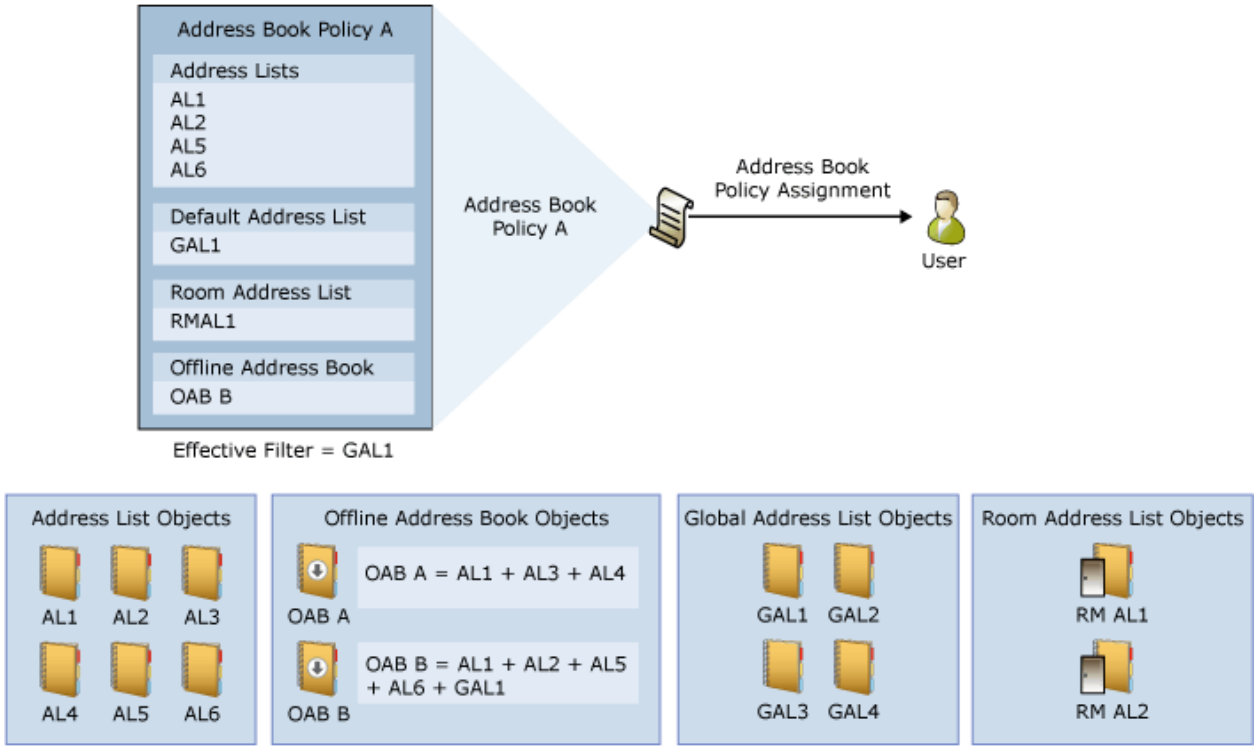
Процедуры, включающие ASP, см. в разделе Процедуры для политик адресной книги в Exchange Server.

Примечания.

- Политики адресных книг создают только виртуальное, а не фактическое разделение пользователей с точки зрения каталога.
- Реализация политики адресных книг — это многоэтапный процесс, требующий планирования. Дополнительные сведения см. в разделе Сценарий. Развертывание политик адресной книги в Exchange Server.

Принципы работы политик адресных книг

На приведенной ниже схеме показано, как работают политики адресных книг. Пользователю назначается политика адресных книг A, которая содержит подмножество списков адресов, доступных в организации. Когда вы создадите политику адресных книг и назначите ее пользователю, она станет областью списков адресов, которые может просматривать пользователь.



Политики адресных книг вступают в силу, когда пользователь подключается к службам клиентского доступа (интерфейсным) на сервере почтовых ящиков. Если изменить политику адресных книг, обновленная политика вступит в силу, когда пользователь перезапустит или заново подключит свое клиентское приложение либо вы перезагрузите сервер почтовых ящиков (в частности, службу клиентского доступа к Microsoft Exchange RPC в фоновых службах).

Агент маршрутизации политик адресных книг

В организации Exchange, где не используются политики адресных книг, когда пользователь создает электронное сообщение в Outlook или Outlook в Интернете и отправляет его другому получателю в организации, происходит следующее:

1. Электронный адрес разрешается до отображаемого имени пользователя. Например, если ввести sardor@contoso.com поле **Кому** , smtp-адрес электронной почты будет разрешен в **Сара Дорси**.

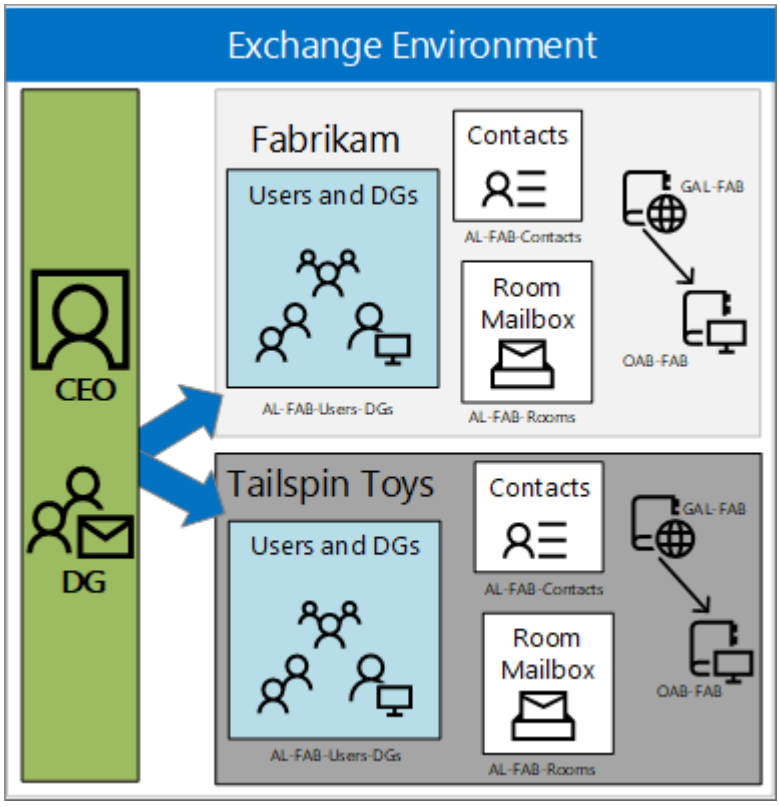
2. После разрешения имени вы можете просмотреть карточку контакта получателя, дважды щелкнув имя пользователя. Карточка контакта содержит контактные данные получателя, например место работы и номер телефона.

Если используются политики адресных книг и необходимо, чтобы пользователи в политиках адресных книг не могли просматривать потенциально конфиденциальные сведения друг друга, то можно включить агент маршрутизации политик адресных книг. Агент маршрутизации политик адресных книг — это агент транспорта, управляющий разрешением получателей в организации. После установки и настройки агента маршрутизации политик адресных книг пользователи, назначенные разным глобальным спискам адресов с помощью разных политик адресных книг, не могут просматривать карточки контактов других пользователей (они отображаются для них как внешние получатели).

Сведения о том, как включить агент маршрутизации политик адресных книг, см. в разделе Установка и настройка агента маршрутизации политик адресных книг с помощью командной консоли Exchange.

Пример политики адресных книг

На приведенной ниже схеме у компаний Fabrikam и Tailspin Toys есть общая организация Exchange и общий исполнительный директор. Исполнительный директор — это единственный сотрудник, относящийся к обеим компаниям.



Рекомендуемая конфигурация включает три политики адресных книг:

- Один ABP назначается сотрудникам Fabrikam. Список адресов и адресов в ABP включает сотрудников Fabrikam и генерального директора.

- Один ABP назначен сотрудникам Tailspin Toys. Список адресов и списки адресов в ABP включают сотрудников Tailspin Toys и генерального директора.
- Еще одна политика назначается только исполнительному директору. Список адресов (по умолчанию) и списки адресов в ABP включают всех сотрудников (Fabrikam, Tailspin Toys и генерального директора).

В этой конфигурации политики адресных книг обеспечивают соблюдение следующих требований:

- при просмотре глобального списка адресов пользователи в Tailspin Toys могут видеть только сотрудников и исполнительного директора Tailspin Toys;
- при просмотре глобального списка адресов пользователи в Fabrikam могут видеть только сотрудников и исполнительного директора Fabrikam;
- при просмотре глобального списка адресов исполнительному директору видны все сотрудники компаний Fabrikam и Tailspin Toys;
- пользователи, просматривающие сведения о группах, в которых состоит исполнительный директор, видят только группы из своей компании. Им не видны группы, относящиеся к другой компании.

Сценарий. Развертывание политик адресной книги в Exchange Server

Статья • 04.04.2023

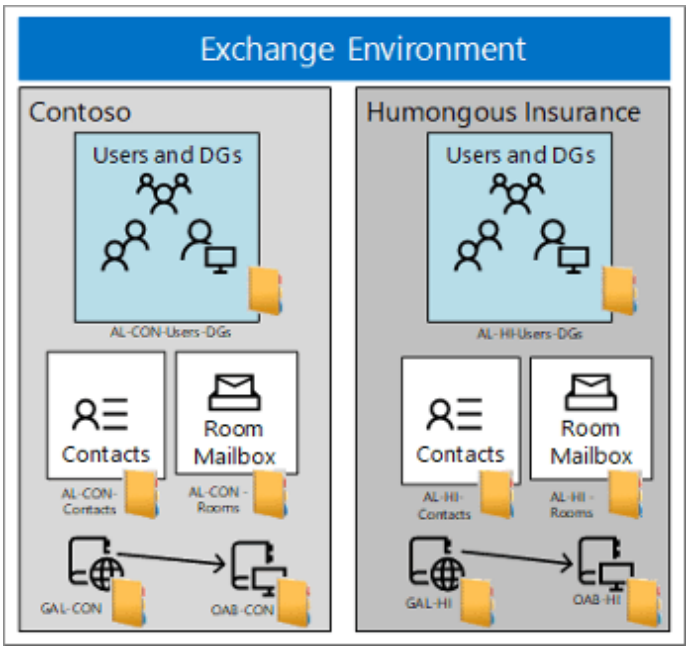
Сценарии в этом разделе описывают решения для развертывания политик адресных книг (ASP) в трех наиболее распространенных типах организаций, в которых несколько организаций (компании, государственные учреждения, учебные классы и т. д.) совместно используют общую среду Exchange. Во всех сценариях фильтр получателей делит получателей на отдельные виртуальные организации, которые затем определяют ASP, применяемые к пользователям в этих виртуальных организациях. Дополнительные сведения о фильтрах получателей и виртуальных организациях см. в разделе Рекомендации и рекомендации по политикам адресной книги далее в этом разделе.

Дополнительные сведения о ASP см. в разделе Политики адресной книги в Exchange Server. Процедуры ABP см. в разделе Процедуры для политик адресной книги в Exchange Server.

Сценарий 1. Две отдельные компании в одной организации Exchange

Этот сценарий применяется к компаниям или подразделениям, которые используют одну и ту же среду Exchange, но не имеют общих сотрудников или руководителей. Кроме того, в подразделениях нет особых требований к безопасности или конфиденциальности.

В этом сценарии Contoso и Humongous Insurance являются двумя отдельными компаниями, которые используют одну и ту же среду Exchange. AbP для каждой компании позволяет сотрудникам одной компании видеть только членов одной компании в глобальном списке адресов (GAL) в Outlook и Outlook в Интернете (ранее известный как Outlook Web App). Все группы рассылки принадлежат одной или другой компании, и ни одна группа рассылки не содержит участников из обеих компаний.



В таблице ниже приведены данные о глобальном списке адресов, автономной адресной книге, списке помещений и списках адресов, которые требуются для политик адресных книг в этом сценарии:

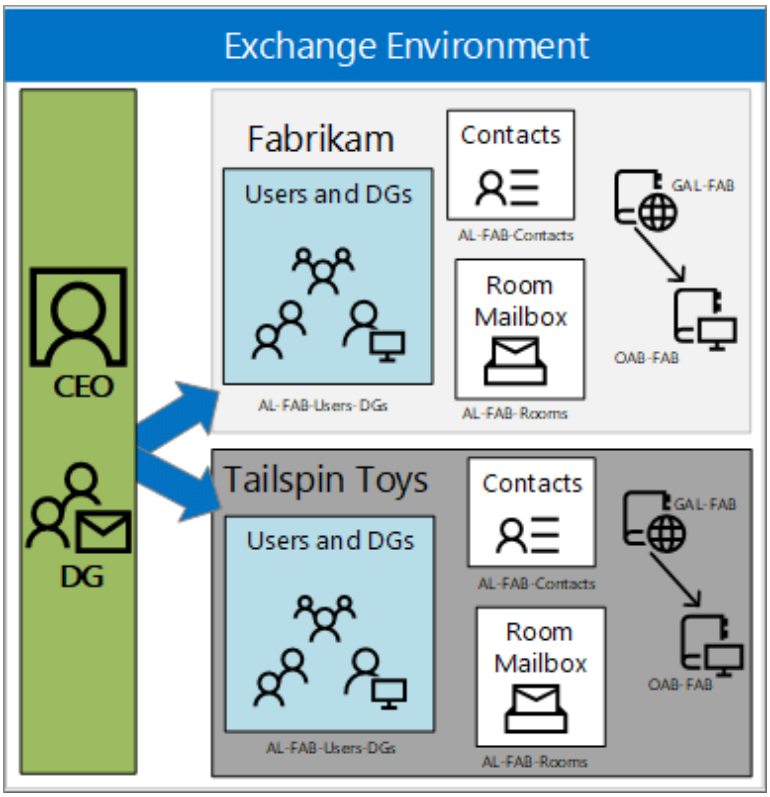
Элемент политики адресных книг	**Contoso**	**Humongous Insurance**
Глобальный список адресов	GAL_CON	GAL_HI
Автономная адресная книга	OAB_CON	OAB_HI
Список помещений	AL_CON_Rooms	AL_HI_Rooms
Списки адресов	AL_CON_Groups AL_CON_Users AL_CON_Contacts	AL_HI_Groups AL_HI_Users AL_HI_Contacts

Сценарий 2. Две компании совместно используют генерального директора в одной организации Exchange

Этот сценарий применяется к компаниям или подразделениям, которые совместно используют среду Exchange, и единственные сотрудники, как правило, находятся в высшем руководстве.

В этом сценарии Fabrikam и Tailspin Toys являются отдельными компаниями в одной среде Exchange, которые совместно используют одного и того же генерального директора, который является единственным общим человеком между двумя компаниями. В этом сценарии используются три ASP, которые имеют следующие требования:

- При просмотре глобального списка адресов сотрудники одной компании могут видеть получателей только из своей компании. При этом сотрудники обеих компаний могут видеть исполнительного директора в глобальном списке адресов и группах рассылки.
- Генеральный директор может видеть всех получателей в обеих компаниях, может создавать группы распространения, охватывающие обе компании, и группы отображаются в списке глобальных адресов каждой компании. Однако участники группы видят только других участников из соответствующей компании (участники группы из другой компании скрыты).
- Пользователи, просматривающие участие исполнительного директора в группах, будут видеть только группы в своей компании. Группы в другой компании им не видны.
- В каждой компании есть группа рассылки Senior Leadership, в которую входят руководители компании и исполнительный директор.
- Имена трех используемых политик адресных книг: ABP_FAB, ABP_TAIL и ABP_CEO.



В таблице ниже приведены данные о глобальном списке адресов, автономной адресной книге, списке помещений и списках адресов, которые требуются для политик адресных книг в этом сценарии.

Элемент политики адресных книг	Fabrikam	Tailspin Toys	Директор

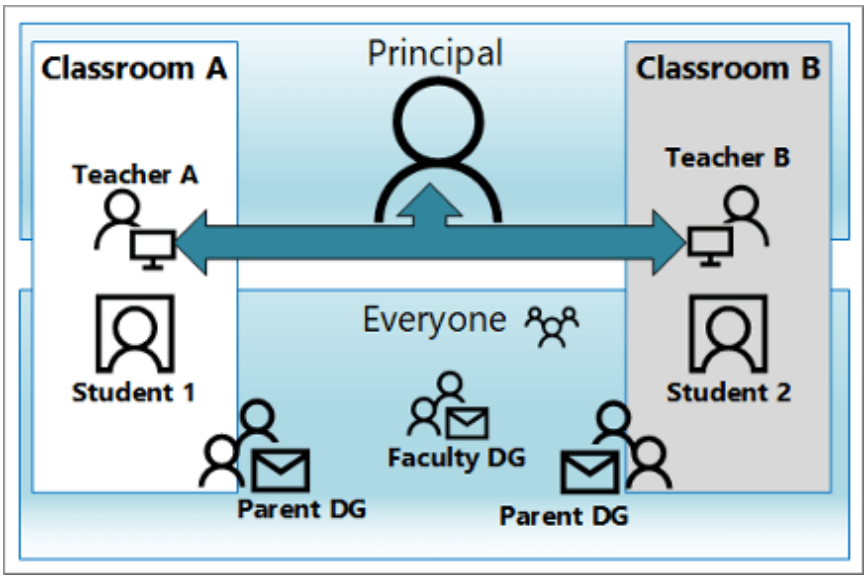
Элемент политики адресных книг	Fabrikam	Tailspin Toys	Директор
Имя	ABP_FAB	AB_TAIL	ABP_CEO
Глобальный список адресов	GAL_FAB	GAL_TAIL	Глобальная адресная книга по умолчанию
Автономная адресная книга	OAB_FAB	OAB_TAIL	Автономная адресная книга по умолчанию
Список адресов помещений	AL_FAB_Rooms	AL_TAIL_Rooms	Все помещения
Списки адресов	AL_FAB_Users_DGs AL_FAB_Contacts	AL_TAIL_Users_DGs AL_TAIL_Contacts	AL_FAB_Users_DGs AL_FAB_Contacts AL_TAIL_Users_DGs AL_TAIL_Contacts

Полное пошаговое руководство по созданию необходимых элементов для этого сценария см. в разделе Пошаговая инструкция по развертыванию сценария 2. Две компании, у которых общий исполнительный директор в одной организации Exchange в конце этой статьи.

Сценарий 3. Учебные заведения

Этот сценарий применяется в учебных заведениях, в которых требуется разделить классы, чтобы обеспечить конфиденциальность учащихся. Сценарий содержит следующие требования:

- Учащиеся в каждом классе могут видеть только других учащихся своего класса, своего преподавателя и директора.
- Преподаватели могут видеть только учащихся в своих классах.
- Преподаватели могут видеть всех остальных преподавателей и директора.
- Для родителей и преподавателей каждого класса создаются группы рассылки.



В таблице ниже приведены данные о глобальном списке адресов, автономной адресной книге, списке помещений и списках адресов, которые требуются для политик адресных книг в этом сценарии.

Элемент политики адресных книг	**Students_ClassA**	**Teachers_ClassA**	**Principal**
Глобальный список адресов	GAL_StudentsClassA	GAL_TeachersClassA	GAL_Everyone
Автономная адресная книга	OAB_StudentsClassA	OAB_TeachersClassA	Автономная адресная книга по умолчанию
Список адресов помещений	AL_BlankRoom	AL_BlankRoom	Все помещения
Списки адресов	AL_ClassAAL_Principal	AL_ClassAAL_AllTeachersAL_AllGroupsAL_Principal	AL_ClassA AL_ClassB AL_AllTeachers AL_AllStudents AL_AllGroups

Рекомендации для политик адресных книг

Ниже приведены важные факторы, которые следует учитывать при использовании политик адресных книг в своей организации:

- Нельзя одновременно использовать иерархические адресные книги и политики адресных книг. Дополнительные сведения см. в статье Understanding Hierarchical Address Books.

- Пользователь, которому назначена политика адресных книг, должен присутствовать в глобальном списке адресов, заданном для этой политики адресных книг.

- Если вы создаете ASP в организации и не назначаете abp некоторым пользователям, эти получатели смогут просматривать *все* списки адресов.

- Чтобы разделить получателей на виртуальные организации, мы рекомендуем использовать для них атрибуты с **CustomAttribute1** по **CustomAttribute15**. Эти атрибуты эффективнее, чем другие предустановленные условные атрибуты, например **Company**, **Department** или **StateOrProvince**, так как:

  - Не все типы получателей поддерживают атрибуты **Company**, **Department** или **StateOrProvince** (например, группы рассылки, динамические группы рассылки и общедоступные папки с поддержкой почты).

  - Пользователи не могут настраивать атрибуты с **CustomAttribute1** по **CustomAttribute15** в своих почтовых ящиках, поэтому эти атрибуты полностью контролируются администраторами.

  - Даже тем типам получателей, которые поддерживают атрибуты **Company**, **Department** или **StateOrProvince**, требуются другие командлеты для их настройки.

    Например, чтобы настроить значения для атрибутов **Company**, **Department** или **StateOrProvince** для почтовых ящиков, пользователей почты или почтовых контактов, нельзя использовать командлеты **Set-Mailbox**, **Set-MailUser** или **Set-MailContact**. Вместо этого следует использовать командлеты **Set-User** и **Set-Contact**. В то же время для всех типов получателей доступны параметры с *CustomAttribute1* по *CustomAttribute15* для соответствующих командлетов **Set-***.

    Дополнительные сведения о фильтрации получателей см. в разделе Фильтрация получателей на пограничных транспортных серверах.

- Клиентские приложения, которые обращаются к Active Directory напрямую через LDAP, будут обходить логику, встроенную в ASP.

- Глобальный список адресов, указанный в политике адресных книг, должен по меньшей мере содержать все списки адресов (включая список адресов помещений), указанные в политике адресных книг (считается нормой, если

политика адресных книг содержит дополнительные списки адресов). Не создавайте глобальный список адресов, который содержит меньше получателей, чем списков адресов в одной политике адресных книг.

- Мы не рекомендуем создавать группы рассылки, которые выходят за пределы виртуальной организации. Создание групп рассылки из участников различных виртуальных организаций приведет к возникновению следующих проблем:

  - Если участник группы запрашивает уведомление о доставке или прочтении при отправке сообщения в группу рассылки, он увидит адреса электронной почты всех участников группы.

  - Зашифрованные сообщения, отправляемые в группу рассылки, могут вызвать проблемы, если у некоторых участников группы нет допустимых цифровых идентификаторов. Например, предположим, что группа рассылки содержит трех членов из агентства A и двух членов из агентства B. Кроме того, один из членов агентства A и два члена агентства B имеют недопустимые цифровые идентификаторы. Если участник из агентства A отправляет зашифрованные сообщения в группу рассылки, он получит предупреждение о том, что есть три получателя без допустимых цифровых идентификаторов. Однако в предупреждающем сообщении будет отображаться только адрес электронной почты участника агентства A.

  - Политики адресных книг не применяются ко всем пользователям или процессам, использующим командлет **Get-Group**, поэтому пользователь увидит всех участников любой группы, к которой у него есть доступ.

    Так как в этом случае рекомендуется запретить пользователям управлять собственными группами в Outlook или Outlook в Интернете. Для этого удалите назначение роли RBAC MyDistributionGroupMembership для пользователей. Дополнительные сведения см. в статье Управление политиками назначения ролей.

    Если вы разрешаете пользователям использовать Outlook или Outlook в Интернете для управления группами, видимость полного списка членства в группах должна быть нормальной для владельцев групп.

- Все политики адресных книг должны содержать список адресов помещений. Однако, если в организации не используются списки адресов помещений, можно создать пустой список адресов помещений.

  Примечание. Список помещений, необходимый для ABP, — это список адресов, указывающий комнаты (содержит фильтр `RecipientDisplayType -eq 'ConferenceRoomMailbox'`). Это не группа рассылки для поиска помещений,

созданная с помощью параметра *RoomList* в командлетах **New-DistributionGroup** или **Set-DistributionGroup** . Дополнительные сведения см. в статье Создание почтовых ящиков комнат и управление ими.

- Развертывание политик адресных книг не помешает пользователям одной виртуальной организации отправлять электронную почту пользователям другой виртуальной организации. Если вы хотите запретить пользователям отправлять электронную почту между виртуальными организациями, рекомендуем создать правило потока обработки почты (также называемого правилом транспорта), которое отслеживает сообщения, отправленные между получателями. Например, чтобы запретить пользователям Contoso получать сообщения от пользователей Fabrikam и наоборот, но по-прежнему разрешить группе старших руководителей Fabrikam отправлять сообщения пользователям Contoso, можно создать следующее правило потока обработки почты в командной консоли Exchange:

  PowerShell

  ```
  New-TransportRule -Name "Ethical Wall: Contoso-Fabrikam" -
  BetweenMemberOf1 "AllFabrikamEmployees" -BetweenMemberOf2
  "AllContosoEmployees" -DeleteMessage -ExceptIfFrom
  seniorleadership@fabrikam.com
  ```

  Дополнительные сведения о правилах потока обработки почты см. в разделе Правила потока обработки почты в Exchange Server.

- Чтобы настроить функцию, аналогичную политикам адресной книги в Skype для бизнеса или клиенте Lync, можно задать атрибут **msRTCSIP-GroupingID** для определенных пользователей. Дополнительные сведения см. в разделе PartitionByOU Replaced with msRTCSIP-GroupingID.

Подробные шаги по развертыванию для сценария 2. Две компании совместно используют генерального директора в одной организации Exchange

В этом разделе описаны шаги по развертыванию сценария 2. Две компании, совместно использующие генерального директора в одной организации Exchange. Если вы помните, Fabrikam и Tailspin Toys являются отдельными компаниями, которые разделяют одного генерального директора.

Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

Этап 1. Установка и настройка агента маршрутизации политики адресных книг

При включенном агенте маршрутизации политики адресных книг пользователи, которым назначены различные глобальные списки адресов, будут отображаться друг другу как внешние получатели. Подробные инструкции см. в разделе Установка и настройка агента маршрутизации политик адресных книг с помощью командной консоли Exchange.

Этап 2. Определение виртуальных организаций

В этом сценарии атрибут **CustomAttribute15 определяет виртуальные** организации: значение `FAB` для получателей Fabrikam, значение `TAIL` для получателей Tailspin Toys и значение `CEO` для генерального директора, которое необходимо, чтобы пользователи Fabrikam и Tailspin могли видеть генерального директора. Если вы не включаете генерального директора в виртуальные организации Fabrikam и Tailspin Toys, генеральный директор может видеть всех, но никто не может видеть генерального директора. Дополнительные сведения о фильтрации получателей см. в разделе Фильтрация получателей на пограничных транспортных серверах.

Чтобы задать значение атрибута **CustomAttribute15** для почтовых ящиков Fabrikam и Tailspin Toys, групп рассылки, динамических групп рассылки, почтовых контактов и почтовых пользователей, используйте следующий синтаксис:

PowerShell

```
$<VariableName> = Get-<RecipientType> -ResultSize Unlimited | where
PrimarySMTPAddress -match <fabrikam.com | tailspintoys.com>
$<VariableName> | foreach {Set-<RecipientType> -Identity ($_.GUID).ToString()
-CustomAttribute15 <FAB | TAIL>
```

Примечания.

- Использование значения GUID получателя для параметра *Identity* поможет избежать конфликтов при наличии одинаковых имен пользователей в обеих организациях (например, julia@fabrikam.com и julia@contoso.com).
- Допустимые <значения RecipientType> для имен командлетов: Mailbox, DistributionGroup, DynamicDistributionGroup, MailContact и MailUser.

Необходимо настроить значение атрибута **CustomAttribute15** для каждого типа получателя отдельно.

В этом примере задается значение `FAB` атрибута **CustomAttribute15** во всех почтовых ящиках Fabrikam.

PowerShell

```
$FAB_MBX = Get-Mailbox -ResultSize Unlimited | where PrimarySMTPAddress -
match fabrikam.com
$FAB_MBX | foreach {Set-Mailbox -Identity ($_.GUID).ToString() -
CustomAttribute15 FAB}
```

Этап 3. Создание необходимых элементов для политик адресных книг

Создание списков адресов

Этой организации требуются четыре настраиваемых списка адресов:

- AL_FAB_Users_DGs
- AL_FAB_Contacts
- AL_TAIL_Users_DGs
- AL_TAIL_Contacts

В этом примере создается список адресов с именем AL_FAB_Users_DGs, содержащий всех пользователей Fabrikam, групп рассылки, динамических групп рассылки *и* генерального директора.

PowerShell

```
New-AddressList -Name "AL_FAB_Users_DGs" -RecipientFilter "((RecipientType -
eq 'UserMailbox') -or (RecipientType -eq 'MailUniversalDistributionGroup') -
or (RecipientType -eq 'DynamicDistributionGroup')) -and (CustomAttribute15 -
eq 'FAB') -or (CustomAttribute15 -eq 'CEO')"
```

В этом примере создается список адресов AL_FAB_Contacts, содержащий все почтовые контакты Fabrikam.

PowerShell

```
New-AddressList -Name "AL_FAB_Contacts" -RecipientFilter "(RecipientType -eq
'MailContact') -and (CustomAttribute15 -eq 'FAB')"
```

В этом примере создается список адресов с именем AL_TAIL_Users_DGs, содержащий всех пользователей Tailspin Toys, групп рассылки, динамических групп рассылки *и* генерального директора.

PowerShell

```
New-AddressList -Name "AL_TAIL_Users_DGs" -RecipientFilter "((RecipientType -
eq 'UserMailbox') -or (RecipientType -eq 'MailUniversalDistributionGroup') -
or (RecipientType -eq 'DynamicDistributionGroup')) -and (CustomAttribute15 -
eq 'TAIL') -or (CustomAttribute15 -eq 'CEO')"
```

В этом примере создается список адресов AL_TAIL_Contacts, содержащий все почтовые контакты Tailspin Toys.

PowerShell

```
New-AddressList -Name "AL_TAIL_Contacts" -RecipientFilter "(RecipientType -eq
'MailContact') -and (CustomAttribute15 -eq 'TAIL')"
```

Подробнее см. в разделе Создание списков адресов.

Создание списков помещений

Этой организации требуется два настраиваемых списка помещений:

- AL_FAB_Rooms
- AL_TAIL_Rooms

В этом примере создается список помещений AL_FAB_Rooms для почтовых ящиков помещений Fabrikam.

PowerShell

```
New-AddressList -Name AL_FAB_Rooms -RecipientFilter "(Alias -ne $null) -and
(CustomAttribute15 -eq 'FAB') -and (RecipientDisplayType -eq
'ConferenceRoomMailbox') -or (RecipientDisplayType -eq
'SyncedConferenceRoomMailbox')"
```

В этом примере создается список помещений AL_TAIL_Rooms для почтовых ящиков помещений Tailspin Toys.

PowerShell

```
New-AddressList -Name AL_TAIL_Rooms -RecipientFilter "(Alias -ne $null) -and
(CustomAttribute15 -eq 'TAIL') -and (RecipientDisplayType -eq
'ConferenceRoomMailbox') -or (RecipientDisplayType -eq
'SyncedConferenceRoomMailbox')"
```

Примечание. В этом примере создается пустой список помещений AL_BlankRoom, если в организации отсутствуют почтовые ящики помещений (для создания политики адресных книг необходимо предоставить список помещений, даже если он будет пустым):

`New-AddressList -Name AL_BlankRoom -RecipientFilter "(Alias -ne $null) -and ((RecipientDisplayType -eq 'ConferenceRoomMailbox') -or (RecipientDisplayType -eq 'SyncedConferenceRoomMailbox'))"`

Дополнительные сведения о создании списков адресов см. в разделе Создание списков адресов.

Создание глобальных списков адресов

Этой организации требуется два настраиваемых глобальных списка адресов:

- GAL_FAB
- GAL_TAIL

В этом примере создается gal с именем GAL_FAB для Fabrikam, который включает всех получателей Fabrikam *и* позволяет пользователям Fabrikam видеть генерального директора.

PowerShell

```
New-GlobalAddressList -Name "GAL_FAB" -RecipientFilter "(CustomAttribute15 -
eq 'FAB') -or (CustomAttribute15 -eq 'CEO')"
```

В этом примере создается gal с именем GAL_TAIL для Tailspin Toys, который включает всех получателей Tailspin Toys *и* позволяет пользователям Tailspin Toys видеть генерального директора.

PowerShell

```
New-GlobalAddressList -Name "GAL_TAIL" -RecipientFilter "(CustomAttribute15 -
eq 'TAIL') -or (CustomAttribute15 -eq 'CEO')"
```

Примечание. Не используйте глобальный список адресов в ABP, который содержит получателей, отсутствующих в списках адресов в ABP. Сочетание всех списков адресов должно соответствовать получателям в глобальном списке адресов.

Дополнительные сведения см. в разделе Создание глобальных списков адресов с помощью командной консоли Exchange.

Создание автономных адресных книг

Этой организации требуется два настраиваемых глобальных списка адресов:

- OAB_FAB
- OAB_TAIL

В этом примере создается автономная адресная книга OAB_FAB для Fabrikam, включающая глобальный список адресов Fabrikam.

PowerShell

```
New-OfflineAddressBook -Name "OAB_FAB" -AddressLists "GAL_FAB"
```

В этом примере создается автономная адресная книга OAB_TAIL для Tailspin Toys, включающая глобальный список адресов Tailspin Toys.

PowerShell

```
New-OfflineAddressBook -Name "OAB_TAIL" -AddressLists "GAL_TAIL"
```

Примечание: Если вы хотите, чтобы пользователи видели всех получателей в виртуальной организации, убедитесь, что вы включили глобальный список адресов в автономную адресную книгу. В противном случае размер скачивания автономной адресной книги можно уменьшить, указав сокращенный перечень списков адресов, включенных в автономную адресную книгу.

Дополнительные сведения см. в разделе Создание автономных адресных книг с помощью командной консоли Exchange.

Этап 4. Создание политик адресных книг

Этой организации требуются три политики адресных книг:

Элемент политики адресных книг	Fabrikam	Tailspin Toys	Директор

Элемент политики адресных книг	Fabrikam	Tailspin Toys	Директор
Имя	ABP_FAB	ABP_TAIL	ABP_CEO
Глобальный список адресов	GAL_FAB	GAL_TAIL	Глобальная адресная книга по умолчанию
Автономная адресная книга	OAB_FAB	OAB_TAIL	Автономная адресная книга по умолчанию
Список адресов помещений	AL_FAB_Rooms	AL_TAIL_Rooms	Все помещения
Списки адресов	AL_FAB_Users_DGs AL_FAB_Contacts	AL_TAIL_Users_DGs AL_TAIL_Contacts	AL_FAB_Users_DGs AL_FAB_Contacts AL_TAIL_Users_DGs AL_TAIL_Contacts

В этом примере создается политика адресных книг ABP_FAB, содержащая глобальный список адресов, автономную адресную книгу, список помещений и списки адресов компании Fabrikam.

PowerShell

```
New-AddressBookPolicy -Name "ABP_FAB" -AddressLists
"AL_FAB_Users_DGs","AL_FAB_Contacts" -OfflineAddressBook "\OAB_FAB" -
GlobalAddressList "\GAL_FAB" -RoomList "\AL_FAB_Rooms"
```

В этом примере создается политика адресных книг ABP_TAIL, содержащая глобальный список адресов, автономную адресную книгу, список помещений и списки адресов компании Tailspin Toys.

PowerShell

```
New-AddressBookPolicy -Name "ABP_TAIL" -AddressLists
"AL_TAIL_Users_DGs","AL_TAIL_Contacts" -OfflineAddressBook "\OAB_TAIL" -
GlobalAddressList "\GAL_TAIL" -RoomList "\AL_TAIL_Rooms"
```

В этом примере создается политика адресных книг ABP_CEO, содержащая глобальный список адресов, автономную адресную книгу, список помещений и списки адресов исполнительного директора.

PowerShell

```
New-AddressBookPolicy -Name "ABP_CEO" -AddressLists
"AL_FAB_Users_DGs","AL_FAB_Contacts","AL_TAIL_Users_DGs","AL_TAIL_Contacts" -
```

```
OfflineAddressBook "\Default Offline Address Book" -GlobalAddressList
"\Default Global Address List" -RoomList "\All Rooms"
```

Дополнительные сведения см. в разделе Процедуры для политик адресной книги в Exchange Server.

Этап 5. Назначение политик адресных книг почтовым ящикам

В этом примере всем почтовым ящикам Fabrikam назначается политика адресных книг ABP_FAB.

PowerShell

```
$Fab = Get-Mailbox -ResultSize unlimited -Filter "CustomAttribute15 -eq
'FAB'"; $Fab | foreach {Set-Mailbox -Identity $_.Identity -AddressBookPolicy
'ABP_FAB'}
```

В этом примере всем почтовым ящикам Tailspin Toys назначается политика адресных книг ABP_TAIL.

PowerShell

```
$Tail = Get-Mailbox -ResultSize unlimited -Filter "CustomAttribute15 -eq
'TAIL'"; $Tail | foreach {Set-Mailbox -Identity $_.Identity -
AddressBookPolicy 'ABP_TAIL'}
```

В этом примере исполнительному директору по имени Gabriela Laureano назначается политика адресных книг ABP_CEO.

PowerShell

```
Set-Mailbox -Identity "Gabriela Laureano" -AddressBookPolicy "ABP_CEO"
```

Примечание. Если пользователь уже подключен к Outlook или Outlook в Интернете, когда ABP применяется к его почтовому ящику, ей необходимо закрыть и перезапустить клиентское приложение, чтобы увидеть новые списки адресов и глобальный список адресов.

Подробнее см. в разделе Назначение политик адресных книг почтовым ящикам.

Другие особенности

После создания или изменения списка адресов или глобального списка адресов необходимо обновить членство.

Если список адресов содержит большое количество получателей (наша рекомендация — более 3000), следует использовать командную консоль Exchange, чтобы обновить список адресов (а не Центр администрирования Exchange). Дополнительные сведения см. в разделе Обновление списков адресов.

Чтобы обновить глобальный список адресов, всегда необходимо использовать командную консоль Exchange. Дополнительные сведения см. в статье Обновление глобальных списков адресов с помощью командной консоли Exchange.

Процедуры для политик адресной книги в Exchange Server

Статья • 04.04.2023

Политики адресных книг (ASP) позволяют сегментировать пользователей на определенные группы, чтобы предоставить им настраиваемые глобальные списки адресов (GAL) в Outlook и Outlook в Интернете (ранее известные как Outlook Web App). Дополнительные сведения о ASP см. в разделе Политики адресной книги в Exchange Server.

Примечание. Реализация ABP — это многоэтапный процесс, требующий планирования. Дополнительные сведения см. в разделе Сценарий. Развертывание политик адресной книги в Exchange Server.

Что нужно знать перед началом работы

- Предполагаемое время выполнения каждой процедуры: менее 5 минут.
- Вы можете назначить ASP почтовым ящикам в Центре администрирования Exchange (EAC), но для всех остальных процедур ABP требуется командная консоль Exchange. Дополнительные сведения о доступе и использовании Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Политики адресной книги" в разделе разрешения Email адресной книги.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.
- Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server, Exchange Online или Exchange Online Protection.

Просмотр политик адресных книг при помощи Командная консоль Exchange

Чтобы просмотреть политики адресных книг, используйте следующий синтаксис:

```
PowerShell

Get-AddressBookPolicy [-Identity <ABPIdentity>]
```

Этот пример возвращает сводный список всех политик адресных книг в организации:

```
PowerShell

Get-AddressBookPolicy
```

Этот пример возвращает подробные сведения о политике адресных книг All Fabrikam.

```
PowerShell

Get-AddressBookPolicy -Identity "All Fabrikam ABP" | Format-List
```

Подробные сведения о синтаксисе и параметрах см. в разделе Get-AddressBookPolicy.

Создание политик адресных книг при помощи Командная консоль Exchange

Для политики адресных книг требуется один глобальный список адресов (GAL), одна автономная адресная книга (OAB), один список помещений и один или несколько списков адресов. Чтобы просмотреть доступные объекты, используйте командлеты **Get-GlobalAddressList**, **Get-OfflineAddressBook** и **Get-AddressList**.

Примечание. Список помещений, необходимый для ABP, — это список адресов, указывающий комнаты (содержит фильтр `RecipientDisplayType -eq 'ConferenceRoomMailbox'`). Это не группа рассылки для поиска помещений, созданная с помощью параметра *RoomList* в командлетах **New-DistributionGroup** или **Set-DistributionGroup** .

Чтобы создать политику адресных книг, используйте следующий синтаксис:

```
PowerShell
```

```
New-AddressBookPolicy -Name "<Unique Name>" -GlobalAddressList "<GAL>" -
OfflineAddressBook "<OAB>" -RoomList "<RoomList>" -AddressLists "
<AddressList1>","<AddressList2>"...
```

В этом примере создана политика адресных книг All Fabrikam с такими параметрами:

- **Глобальный список адресов**: All Fabrikam
- **Автономная адресная книга**: Fabrikam-All-OAB
- **Список помещений**: All Fabrikam-Rooms
- **Списки адресов**: All Fabrikam, All Fabrikam Mailboxes, All Fabrikam DLs и All Fabrikam Contacts

PowerShell

```
New-AddressBookPolicy -Name "All Fabrikam ABP" -GlobalAddressList "\All
Fabrikam" -OfflineAddressBook \Fabrikam-All-OAB -RoomList "\All Fabrikam
Rooms" -AddressLists "\All Fabrikam Mailboxes","\All Fabrikam DLs","\All
Fabrikam Contacts"
```

Подробные сведения о синтаксисе и параметрах см. в разделе New-AddressBookPolicy.

Как проверить, все ли получилось?

Чтобы убедиться, что политика адресных книг успешно создана, сделайте одно из двух.

- Запустите эту команду в Командная консоль Exchange, чтобы проверить, присутствует ли политика адресных книг в списке:

  PowerShell

  ```
  Get-AddressBookPolicy
  ```

- Замените <*ABPIdentity*> именем ABP и выполните следующую команду в командной консоли Exchange, чтобы проверить значения свойств:

  PowerShell

  ```
  Get-AddressBookPolicy -Identity "<ABPIdentity>" | Format-List
  ```

Изменение политик адресных книг при помощи Командная консоль Exchange

Используйте командлет **Set-AddressBookPolicy**, чтобы изменить существующую политику адресных книг. Параметры идентичны тем параметрам, которые доступны при создании политики адресных книг.

- Параметры *Name*, *GlobalAddressList*, *OfflineAddressBook* и *RoomList* принимают одиночные значения, поэтому указанное значение заменяет существующее значение.

  В этом примере изменяется политика адресных книг "All Fabrikam ABP" путем замены автономной адресной книги на указанную автономную адресную книгу.

  PowerShell

  ```
  Set-AddressBookPolicy -Identity "All Fabrikam ABP" -OfflineAddressBook
  \Fabrikam-OAB-2
  ```

- Параметр *AddressLists* принимает несколько значений, поэтому необходимо решить, следует ли *заменить* существующие списки адресов в ABP или *добавить и удалить* списки адресов, не затрагивая другие списки адресов в ABP.

  В этом примере существующие списки адресов в политике адресных книг Government Agency A заменяются на указанные списки адресов.

  PowerShell

  ```
  Set-AddressBookPolicy -Identity "Government Agency A" -AddressLists
  "GovernmentAgencyA-Atlanta","GovernmentAgencyA-Moscow"
  ```

  Чтобы добавить списки адресов к политике адресных книг, укажите новые списки адресов *и* все списки адресов, которые нужно сохранить.

  В этом примере список адресов Contoso-Chicago добавляется к политике ABP Contoso, которая уже настроена на использование списка адресов Contoso-Seattle.

  PowerShell

  ```
  Set-AddressBookPolicy -Identity "ABP Contoso" -AddressLists "Contoso-
  Chicago","Contoso-Seattle"
  ```

Чтобы удалить списки адресов из политики адресных книг, укажите существующие списки адресов, которые нужно сохранить, пропуская те списки, которые нужно удалить.

К примеру, политика адресных книг ABP Fabrikam использует списки адресов Fabrikam-HR и Fabrikam-Finance. Чтобы удалить список адресов Fabrikam-HR, укажите только список Fabrikam-Finance.

PowerShell

```
Set-AddressBookPolicy -Identity "ABP Fabrikam" -AddressLists Fabrikam-Finance
```

Подробные сведения о синтаксисе и параметрах см. в разделе Set-AddressBookPolicy.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно изменяете ABP, замените *<ABPIdentity>* именем ABP и выполните следующую команду в командной консоли Exchange, чтобы проверить значения свойств:

PowerShell

```
Get-AddressBookPolicy -Identity "<ABPIdentity>" | Format-List
```

Удаление политик адресных книг при помощи Командная консоль Exchange

- Политику адресных книг невозможно удалить, если она назначена почтовому ящику. Чтобы узнать, назначен ли ABP почтовому ящику, замените *<ABPIdentity>* именем ABP и выполните следующую команду в командной консоли Exchange, чтобы получить значение **Различающееся имя** :

  `Get-AddressBookPolicy -Identity <ABPIdentity> | Format-List DistinguishedName`

  Затем для отображения всех почтовых ящиков, которым назначена политика адресных книг, используйте значение **DistinguishedName** этой политики в указанной ниже команде:

`Get-Mailbox -ResultSize unlimited -Filter "AddressBookPolicy -eq '<DistinguishedName>'"`

- Информацию об удалении назначений политики адресных книг из почтовых ящиков см. в разделе этой темы Назначение политик адресных книг почтовым ящикам.

Чтобы удалить политику адресных книг, используйте следующий синтаксис:

```
PowerShell

Remove-AddressBookPolicy -Identity <ABPIdentity>
```

В этом примере удаляется политика адресных книг ABP_TailspinToys.

```
PowerShell

Remove-AddressBookPolicy -Identity "ABP_TailspinToys"
```

Подробные сведения о синтаксисе и параметрах см. в разделе Remove-AddressBookPolicy.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно удалили политику адресных книг, сделайте одно из двух.

- Запустите указанную ниже команду в Командная консоль Exchange и проверьте, есть ли политика адресных книг в списке:

  ```
  PowerShell

  Get-AddressBookPolicy
  ```

- Замените <*ABPIdentity*> именем ABP и выполните следующую команду, чтобы убедиться, что возвращается ошибка:

  ```
  PowerShell

  Get-AddressBookPolicy -Identity "<ABPIdentity>"
  ```

Назначение политик адресных книг почтовым ящикам

- Политика адресных книг не назначается пользователям автоматически при создании почтовых ящиков. Если не назначить политику адресных книг почтовому ящику, пользователь будет видеть глобальный список адресов для всей организации в Outlook и Outlook в Интернете.

- При определении виртуальных организаций для политик адресных книг рекомендуем использовать атрибуты CustomAttribute1–15 для почтовых ящиков, контактов и групп, поскольку эти атрибуты являются наиболее доступными и управляемыми для всех типов получателей. Дополнительные сведения см. в разделе Сценарий. Развертывание политик адресной книги в Exchange Server.

- Процедуры назначения политик адресных книг почтовым ящикам и процедуры удаления назначений этих политик из почтовых ящиков одинаковы:

  - Чтобы назначить политику адресных книг почтовым ящикам, выберите ее в Центре администрирования Exchange или укажите в Командная консоль Exchange.

  - Чтобы удалить назначения АВР из почтовых ящиков, выберите значение **[Нет политики]** в ЕАС или используйте значение `$null` в командной консоли Exchange.

Назначение политики адресных книг одному почтовому ящику при помощи Центр администрирования Exchange (ЕАС)

1. В ЕАС перейдите в раздел **Почтовые ящики получателей**>.

2. В списке почтовых ящиков найдите нужный почтовый ящик. Для этого выполните одно из следующих действий:

   - Прокрутите список почтовых ящиков.

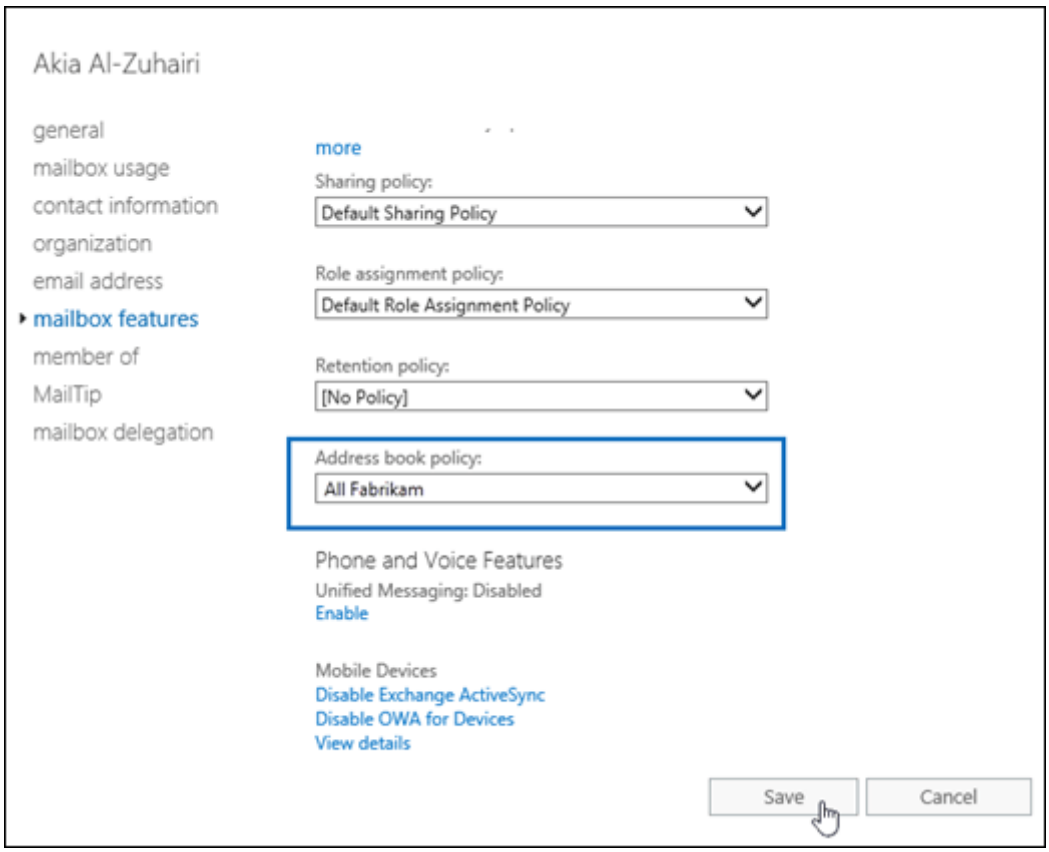
   - Щелкните 🔎 введите часть имени пользователя, адреса электронной почты или псевдонима.

- Щелкните **Значок Дополнительные параметры** > **Расширенный поиск** для поиска почтового ящика.

Найдя почтовый ящик, который требуется изменить, выберите его и нажмите кнопку **Изменить**.

3. На открывшейся странице свойств выберите **Функции почтового ящика**.

4. Щелкните стрелку раскрывающегося списка в **политике адресной книги** и выберите adp, который нужно применить.



По завершении нажмите кнопку **Сохранить**.

Примечание. Вы также можете назначить ABP при создании почтового ящика пользователя в EAC, щелкнув **Дополнительные параметры** и щелкнув стрелку раскрывающегося списка в **политике адресной книги**.

Назначение политики адресных книг одному почтовому ящику при помощи Командная консоль Exchange

При назначении политики адресных книг почтовому ящику используйте следующий синтаксис:

```
PowerShell
```

```
Set-Mailbox -Identity <MailboxIdentity> -AddressBookPolicy <ABPIdentity> or
$null
```

В этом примере abp с именем All Fabrikam назначается почтовому ящику joe@fabrikam.com.

PowerShell

```
Set-Mailbox -Identity joe@fabrikam.com -AddressBookPolicy "All Fabrikam"
```

Примечание. Вы также можете назначить ABP при создании почтового ящика пользователя с помощью командлета **New-Mailbox** с помощью параметра *AddressBookPolicy* . Если не указать ABP при создании почтового ящика, ABP не назначается (значение по умолчанию пустое или `$null`).

Подробные сведения о синтаксисе и параметрах см. в разделе Set-Mailbox.

Назначение политики адресных книг нескольким почтовым ящикам при помощи Центра администрирования Exchange

1. В EAC перейдите в раздел **Почтовые ящики получателей**>.
2. В списке почтовых ящиков найдите почтовые ящики, которые нужно изменить. Например:
   a. Щелкните **Значок Дополнительные параметры**•••>**Расширенный поиск**.
   b. В открывшемся окне **Расширенный поиск** выберите элемент **Типы получателя** и проверьте заданное по умолчанию значение элемента **Почтовый ящик пользователя**.
   c. Выберите **Дополнительно**, а затем нажмите **Добавить условие**.
   d. В появившемся раскрывающемся списке **Выберите один** выберите соответствующие значения **Настраиваемый атрибут 1** — **Настраиваемый атрибут 15** , определяющий виртуальные организации.
   e. В появившемся диалоговом окне **Укажите слова или фразы** введите значение, которое нужно найти, и нажмите кнопку **OK**.
   f. Когда снова откроется окно **Расширенный поиск**, нажмите кнопку **OK**. В центре администрирования Exchange на странице **Почтовые ящики**

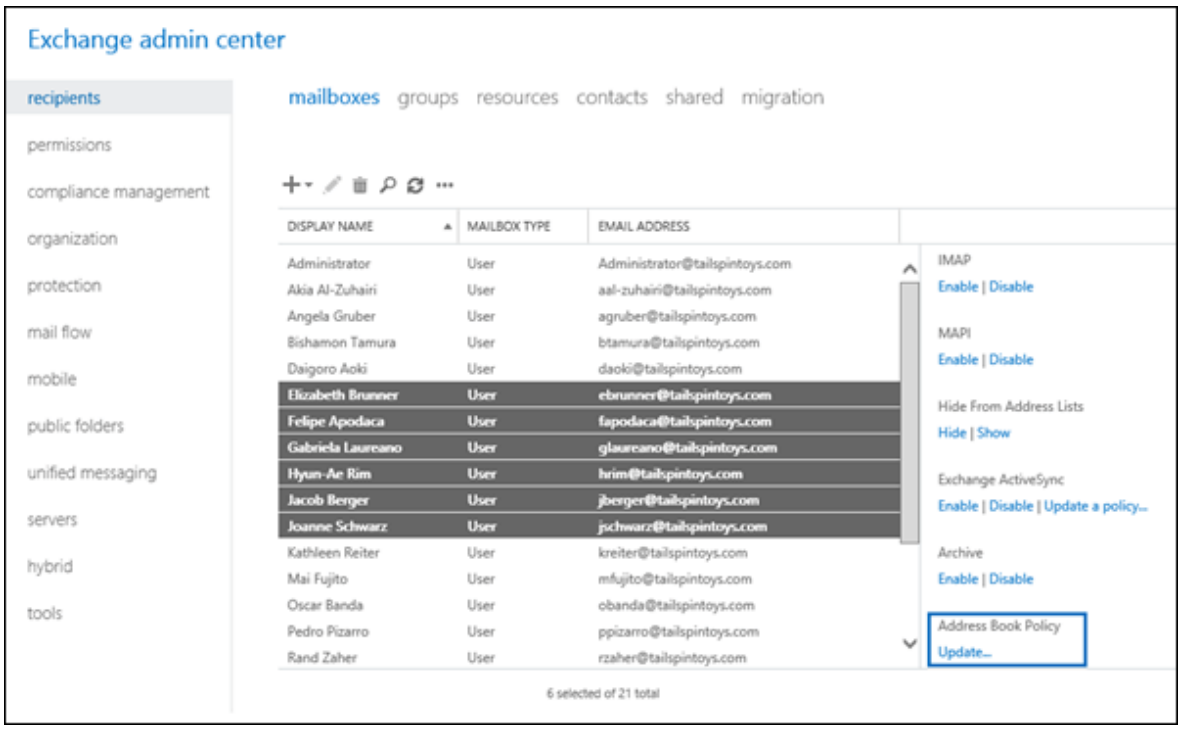
получателей> щелкните ••• > **Расширенный поиск** для поиска почтовых ящиков пользователей.

3. В списке почтовых ящиков выберите несколько почтовых ящиков одного типа (например, **Пользователь**). Например:

   - Выберите почтовый ящик. Удерживая клавишу SHIFT, выберите другой ящик, расположенный ниже в списке.
   - Выберите нужные почтовые ящики, удерживая клавишу CTRL.

   После выбора нескольких почтовых ящиков одного типа заголовок области сведений изменится на **Массовое изменение**.

4. В области сведений прокрутите список вниз и нажмите кнопку **Дополнительные параметры**, перейдите к разделу **Политика адресных книг** и нажмите кнопку **Обновление**.



5. В открывающемся окне **Политика массового назначения адресной книги** выберите АВР, щелкнув стрелку раскрывающегося списка **в разделе Выбор политики адресной книги**, а затем нажмите кнопку **Сохранить**.

Назначение политики адресных книг нескольким почтовым ящикам при помощи Командная консоль Exchange

Указать почтовые ящики, которым нужно назначить политику адресных книг, можно при помощи командлетов **Get-Mailbox** или **Get-Content**. Например:

- Используйте параметр *Filter* для создания фильтров OPATH, определяющих почтовые ящики. Дополнительные сведения см. в статье Filterable Properties for the -Filter Parameter.

- Используйте текстовый файл для указания почтовых ящиков. В каждой строке текстового файла указан один почтовый ящик (адрес электронной почты, имя или другой уникальный идентификатор), например:

  > ebrunner@tailspintoys.com
  > fapodaca@tailspintoys.com
  > glaureano@tailspintoys.com
  > hrim@tailspintoys.com

В этом примере abp с именем ABP_EngineeringDepartment назначается всем почтовым ящикам пользователей `CustomAttribute11` , где атрибут содержит значение Engineering Department.

PowerShell

```
Get-Mailbox -Filter "RecipientType -eq 'UserMailbox' -and CustomAttribute11
-like '*Engineering Department'" | Set-Mailbox -AddressBookPolicy
"ABP_EngineeringDepartment"
```

В этом примере для назначения одной и той же политики адресных книг указанным почтовым ящикам используется текстовый файл C:\My Documents\Accounts.txt.

PowerShell

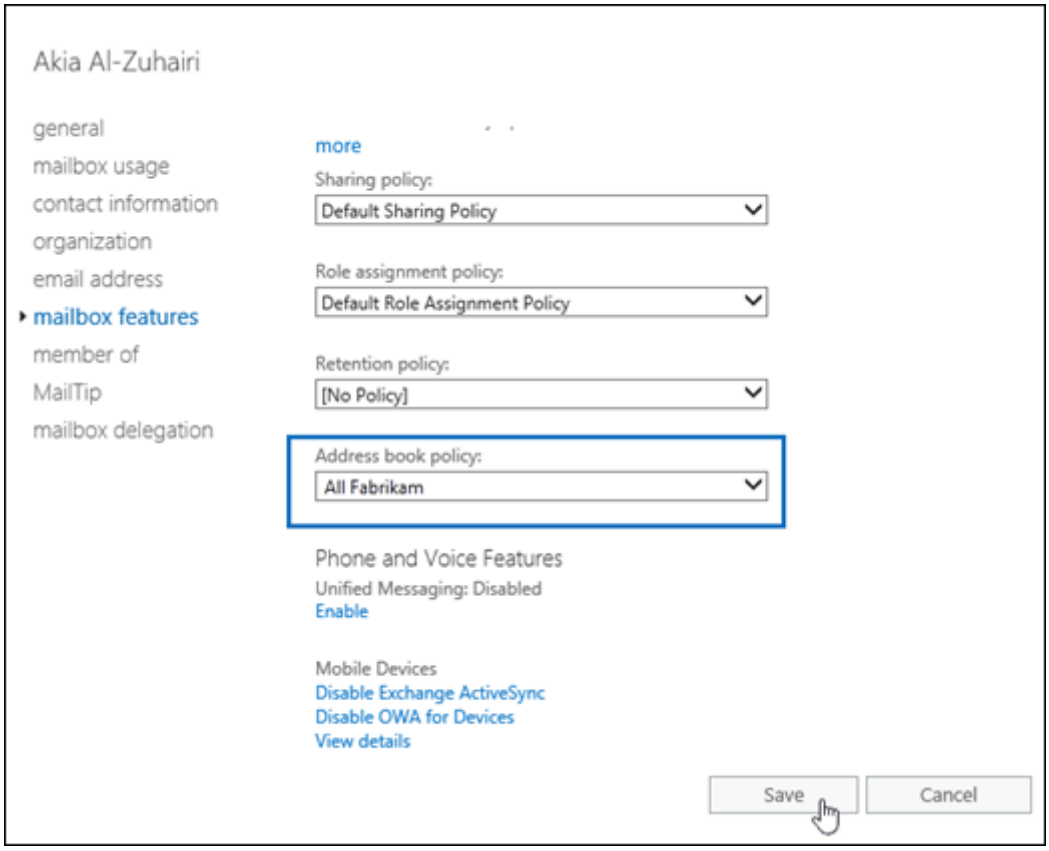
```
Get-Content "C:\My Documents\Accounts.txt" | foreach {Set-Mailbox $_ -
AddressBookPolicy "ABP_EngineeringDepartment"}
```

Подробные сведения о синтаксисе и параметрах см. в разделе Get-Mailbox.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли вы назначили политику адресных книг почтовому ящику, выполните одно из следующих действий:

- В EAC перейдите в раздел Почтовые**ящики**>**получателей**>, выберите почтовый ящик > щелкните >**Функции почтового ящика** и проверьте значение **политики адресной книги**.



- В командной консоли Exchange *замените*< *MailboxIdentity*> удостоверением почтового ящика (например, именем, псевдонимом или адресом электронной почты) и выполните следующую команду:

```
PowerShell

Get-Mailbox -Identity "<MailboxIdentity>" | Format-List
AddressBookPolicy
```

- В Командная консоль Exchange используйте тот же фильтр, что и для определения почтовых ящиков. Например:

```
PowerShell

Get-Mailbox -Filter "RecipientType -eq 'UserMailbox' -and
CustomAttribute11 -like '*Engineering Department'" | Format-Table -Auto
Name,EmailAddress,AddressBookPolicy
```

- В командной консоли Exchange замените <*ABPIdentity*> именем ABP и выполните следующую команду, чтобы получить значение **Различающееся имя** :

PowerShell

```
Get-AddressBookPolicy -Identity <ABPIdentity> | Format-List
DistinguishedName
```

Затем для отображения всех почтовых ящиков, которым назначена политика адресных книг, используйте значение **DistinguishedName** этой политики в указанной ниже команде:

PowerShell

```
Get-Mailbox -ResultSize unlimited -Filter "AddressBookPolicy -eq
'<DistinguishedName>'"
```

Установка и настройка агента маршрутизации политики адресных книг при помощи Командная консоль Exchange

Маршрутизация политики адресных книг управляет разрешением получателей в организациях, которые используют политики адресных книг. При включенной маршрутизации политики адресных книг пользователи, которым назначены разные глобальные списки адресов, будут отображаться друг для друга как внешние получатели.

Для маршрутизации политики адресных книг требуется установить и включить агент маршрутизации политики адресных книг на всех серверах почтовых ящиков в вашей организации и включить глобальную маршрутизацию в вашей организации. После этого обработка сообщений агентом маршрутизации политики адресных книг может занять до 30 минут.

Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Агенты транспорта" в разделе Разрешения потока обработки почты .

Шаг 1. Установите агент маршрутизации политики адресных книг

Чтобы установить агент маршрутизации политики адресных книг на локальном сервере почтовых ящиков, выполните следующую команду на каждом сервере почтовых ящиков в организации.

PowerShell

```
Install-TransportAgent -Name "ABP Routing Agent" -TransportAgentFactory
"Microsoft.Exchange.Transport.Agent.AddressBookPolicyRoutingAgent.AddressBoo
kPolicyRoutingAgentFactory" -AssemblyPath
$env:ExchangeInstallPath\TransportRoles\agents\AddressBookPolicyRoutingAgent
\Microsoft.Exchange.Transport.Agent.AddressBookPolicyRoutingAgent.dll
```

Примечание. Вы получите предупреждение о том, что служба транспорта должна быть перезапущена, чтобы изменения вступили в силу. Но не перезапускайте транспортную службу до завершения шага 2 (поэтому перезапустить транспортную службу придется только один раз).

Подробные сведения о синтаксисе и параметрах см. в разделе Install-TransportAgent.

Шаг 2. Включите агент маршрутизации политики адресных книг

Чтобы включить агент маршрутизации политики адресных книг на локальном сервере почтовых ящиков, выполните следующую команду на каждом сервере почтовых ящиков в организации.

PowerShell

```
Enable-TransportAgent "ABP Routing Agent"
```

Подробные сведения о синтаксисе и параметрах см. в разделе Enable-TransportAgent.

Шаг 3. Перезапустите службу транспорта

Чтобы перезапустить службу транспорта, выполните эту команду на каждом сервере почтовых ящиков в организации.

PowerShell

```
Restart-Service MSExchangeTransport
```

Подробные сведения о синтаксисе и параметрах см. в разделе Get-TransportAgent.

Шаг 4. Включите глобальную маршрутизацию политики адресных книг в организации Exchange

Чтобы включить глобальную маршрутизацию политики адресных книг в организации Exchange, выполните следующую команду однократно на любом сервере почтовых ящиков:

```
PowerShell

Set-TransportConfig -AddressBookPolicyRoutingEnabled $true
```

Подробные сведения о синтаксисе и параметрах см. в разделе Set-TransportConfig.

Примечание. Чтобы отключить маршрутизацию политики адресных книг после ее включения, выполните следующие действия:

1. Выполните следующую команду однократно на любом сервере почтовых ящиков, чтобы глобально отключить маршрутизацию политики адресных книг:

   ```
   PowerShell

   Set-TransportConfig -AddressBookPolicyRoutingEnabled $false
   ```

2. Отключите агент маршрутизации политики адресных книг, выполнив следующую команду на каждом сервере почтовых ящиков, на котором установлен агент:

   ```
   PowerShell

   Disable-TransportAgent "ABP Routing Agent"
   ```

3. Выполните следующую команду на каждом сервере почтовых ящиков, на котором установлен агент:

   ```
   PowerShell

   Restart-Service MSExchangeTransport
   ```

Как убедиться, что все получилось?

Чтобы убедиться, что вы успешно установили и настроили агент маршрутизации политики адресных книг, выполните одно из следующих действий.

- Выполните следующую команду на сервере почтовых ящиков, чтобы проверить, включена ли маршрутизация политики адресных книг для организации:

  PowerShell

  ```
  Get-TransportConfig | Format-List AddressBookPolicyRoutingEnabled
  ```

- Выполните следующую команду на каждом сервере почтовых ящиков, чтобы проверить, включен ли агент маршрутизации политики адресных книг:

  PowerShell

  ```
  Get-TransportAgent "ABP Routing Agent"
  ```

- Организуйте отправку сообщения от пользователя, которому назначена политика адресных книг, пользователю, которому назначена другая политика адресных книг, и проверьте, разрешен ли адрес электронной почты отправителя в его отображаемом имени.

Политика обмена сообщениями и соответствие требованиям в Exchange Server

Статья • 04.04.2023

Электронная почта стала надежной и повсеместной средой связи для информационных работников в организациях всех размеров. Хранилища сообщений и почтовые ящики становятся репозиториями ценной информации. Для организаций, которые собираются применить политики обмена сообщениями, которые определяют добросовестное использование их систем обмена сообщениями, важно предоставить пользователям указания по политикам, а там, где это требуется, предоставить подробную информацию о типах связи, которые могут быть запрещены.

Организации должны также создать правила для управления жизненным циклом электронной почты, хранить сообщения в зависимости от требований бизнеса, юридических и нормативных требований, сохранять электронную почту для судебных и следственных целей, и быть готовыми к поиску и предоставлению необходимой электронной почты при запросах обнаружения электронных данных.

Политика обмена сообщениями и соответствие требованиям в Exchange Server

В следующей таблице представлен обзор политики обмена сообщениями и функций соответствия требованиям в Exchange 2016 и Exchange 2019, а также ссылки на разделы, которые помогут вам узнать об этих функциях и использовать их.

Возможность	Описание	Ресурсы
Архивация на месте	*Архивация на месте* помогает взять под контроль данные обмена сообщениями в организации, избавляя вас от необходимости в файлах личного хранилища сертификатов (PST) и позволяя пользователям хранить сообщения в *архивном почтовом ящике*, доступном в Outlook 2010 и более поздних версий, а также Outlook в Интернете.	Архивация на месте в Exchange Server

Возможность	Описание	Ресурсы
Удержание на месте и хранение для судебного разбирательства	В тех случаях, когда существует обоснованное ожидание судебного разбирательства, организации обязаны сохранять сведения, хранящиеся в электронном виде, включая сообщения электронной почты, имеющие отношение к делу. In-Place удержание позволяет выполнять поиск и сохранение сообщений, соответствующих параметрам запроса. Хранение для судебного разбирательства позволяет только поместить все элементы в почтовый ящик на удержание. Для обоих типов удержаний сообщения защищены от постоянного удаления, изменения и изменения и изменения и могут храниться неограниченное время или в течение указанного периода.	Удержание на месте и удержание для судебного разбирательства в Exchange Server
Обнаружение электронных данных на месте	Обнаружение электронных данных на месте позволяет искать данные почтовых ящиков в организации Exchange, просматривать результаты поиска, копировать эти результаты в почтовый ящик найденных сообщений и экспортировать эти результаты в PST-файл.	Обнаружение электронных данных на месте в Exchange Server
Ведение журнала аудита действий администратора	Журналы аудита действий администратора позволяют вести журнал изменений, внесенных администраторами относительно сервера Exchange, конфигурации организации и получателей Exchange. Журнал аудита действий администратора можно вести в ходе управления изменениями или для их отслеживания, а также получения доступа к конфигурации и получателям, чтобы обеспечить соответствие требованиям.	Ведение журнала аудита администратора в Exchange Server
Ведение журнала аудита почтового ящика	Так как почтовые ящики могут потенциально содержать конфиденциальные, важные сведения для бизнеса и личные данные, важно отслеживать, кто входит в почтовые ящики в вашей организации и какие действия выполняются. Особенно важно отслеживать доступ к почтовым ящикам пользователей, отличных от владельца почтового ящика (называемых пользователями-делегатами). С помощью ведения журнала аудита почтовых ящиков можно регистрировать доступ к почтовым ящикам администраторов, делегатов (включая администраторов с разрешениями на полный доступ) и владельцев почтовых ящиков.	Ведение журнала аудита почтового ящика в Exchange Server

Возможность	Описание	Ресурсы
Защита от потери данных	Защита от потери данных (DLP) в Exchange Server включает 80 типов конфиденциальной информации, которые можно использовать в политиках защиты от потери данных.	Типы конфиденциальной информации в Exchange Server
Правила потока обработки почты (также известные как правила транспорта)	Используйте правила потока почты для поиска определенных условий в сообщениях, проходящих через организацию, и принятия мер по их использованию. Можно использовать условия и исключения, чтобы определить, когда применяется правило потока обработки почты, а затем применить действие к сообщениям при выполнении условий.	Условия и исключения (предикаты) правил потока обработки почты в Exchange Server Действия правил потока обработки почты в Exchange Server

Архивация In-Place в Exchange Server

Статья • 19.03.2023

Архивация на месте в Exchange Server помогает восстановить контроль над данными для обмена сообщениями организации, устраняя необходимость в файлах личного хранилища (PST) и позволяя пользователям хранить сообщения в *архивном почтовом ящике*. Архивный почтовый ящик — это дополнительный почтовый ящик пользователя. Архивный почтовый ящик доступен в Outlook и Outlook в Интернете (прежнее название — Outlook Web App). Пользователи могут просматривать архивный почтовый ящик и перемещать или копировать сообщения между основным почтовым ящиком и архивом.

Архивный почтовый ящик пользователя можно создать в той же базе данных почтовых ящиков, что и основной почтовый ящик, в другой базе данных почтовых ящиков на том же сервере почтовых ящиков или в базе данных почтовых ящиков на другом сервере почтовых ящиков на том же сайте Active Directory. В гибридных развертываниях Exchange также можно создать облачный архивный почтовый ящик для основных почтовых ящиков, размещенных в локальной организации.

Клиентский доступ к архивным почтовым ящикам

В следующей таблице приведены клиентские приложения, которые могут использоваться для доступа к архивным почтовым ящикам.

Клиентская	**Доступ к архивным почтовым ящикам?**
Outlook для Mac для Office 365 Outlook 2016 для Mac или более поздней версии Microsoft 365 корпоративные приложения Outlook 2013 или более поздней версии Outlook в Интернете	Да. Пользователи могут копировать и перемещать элементы из основного почтового ящика в архивный почтовый ящик, а также могут использовать политики хранения для перемещения элементов в архив. Outlook не создает локальную копию архивного почтового ящика на компьютере пользователя, даже если включен режим кэширования Exchange. Архивный почтовый ящик доступен только в сети.
Exchange ActiveSync	Нет

Примечание

- In-Place архивация — это функция уровня "Премиум" и требует наличия клиентской лицензии (CAL) Exchange Enterprise. Дополнительные сведения о лицензировании Exchange см. в разделе **Часто задаваемые вопросы о лицензировании Exchange**.
- Дополнительные сведения о версиях Outlook, необходимых для доступа к архивным почтовым ящикам, см. в статье **Требования к лицензиям Outlook для функций Exchange**.

Перемещение сообщений в архивный почтовый ящик

Перемещать сообщения из основного почтового ящика пользователя в архивный почтовый ящик можно несколькими способами:

- **Перемещение или копирование сообщений вручную**. Пользователи могут вручную перемещать или копировать сообщения из основного почтового ящика или PST-файла в архивный почтовый ящик. Архивный почтовый ящик отображается как другой почтовый ящик Outlook и Outlook в Интернете или как подключенный PST-файл в Outlook.
- **Перемещение или копирование сообщений с помощью правил папки "Входящие"**. Пользователи могут создавать правила папки "Входящие" в Outlook для автоматического перемещения сообщений в папку в архивном почтовом ящике.
- **Перемещение сообщений с помощью политик хранения**. Политики хранения можно использовать для автоматического перемещения сообщений в архивный почтовый ящик. Пользователи также могут применять личные теги для перемещения сообщений в архивный почтовый ящик. Дополнительные сведения о политиках архивации и хранения см. в следующем разделе этой статьи.
- **Импорт сообщений из PST-файлов**. В Exchange Server можно использовать запрос на импорт почтовых ящиков для импорта сообщений из PST-файла в архив пользователя или основной почтовый ящик. Дополнительные сведения см. в статье Импорт и экспорт почтовых ящиков в Exchange Server.

Политики архивации и хранения

В Exchange Server можно применить политики архивирования к почтовому ящику, чтобы автоматически перемещать сообщения из основного почтового ящика пользователя в архивный почтовый ящик по истечении указанного периода. Политики архивации реализованы путем создания тегов хранения, которые задают действие **Переместить в архив**.

Сообщения перемещаются в папку в архивном почтовом ящике, имеющую имя исходной папки в основном почтовом ящике пользователя. Если в архивном почтовом ящике папка с тем же именем не существует, она создается, когда помощник по обслуживанию

управляемых папок перемещает сообщение. Благодаря воссозданию той же иерархии папок в архивном почтовом ящике пользователи легко могут находить сообщения.

Дополнительные сведения о политиках хранения, тегах хранения и **действии "Переместить в архив"** см. в статье Теги хранения и политики хранения в Exchange Server.

Политика управления записями сообщений по умолчанию

Exchange Server программа установки создает политику архива и хранения по умолчанию с именем **Политика MRM по умолчанию**. Эта политика содержит теги хранения с действием **Переместить в архив** , как показано в следующей таблице.

Имя тега хранения	Тип тега	Описание
Перемещать в архив по умолчанию через 2 года	По умолчанию (DPT)	Сообщения автоматически перемещаются в архивный почтовый ящик через 2 года. Применяется к тем элементам во всем почтовом ящике, к которым не был применен тег хранения, явный или унаследованный от папки.
Перемещать в архив личные элементы через 1 год	Персональный	Сообщения автоматически перемещаются в архивный почтовый ящик через один год.
Перемещать в архив личные элементы через 5 лет	Персональный	Сообщения автоматически перемещаются в архивный почтовый ящик через пять лет.
Никогда не перемещать личные элементы в архив	Персональный	Сообщения никогда не перемещаются в архивный почтовый ящик.
Перемещать в архив элементы для восстановления через 14 дней	Папка "Элементы с возможностью восстановления"	Сообщения перемещаются из папки "Элементы с возможностью восстановления" основного почтового ящика пользователя в папку "Элементы с возможностью восстановления" архивного почтового ящика. Пользователи, которые пытаются восстановить удаленные элементы в своем архивном почтовом ящике, должны воспользоваться средством восстановления удаленных элементов в архивном почтовом ящике.

Если вы включите архив In-Place для пользователя почтового ящика и ему еще не назначена политика хранения, автоматически назначается политика архивации и хранения по умолчанию. После того как помощник для управляемых папок обработает почтовый ящик, эти теги становятся доступными для пользователя, который затем может разметить с их помощью папки или сообщения для перемещения в архивный почтовый ящик. По

умолчанию сообщения электронной почты из всего почтового ящика перемещаются в архив через два года.

Перед предоставлением архивных почтовых ящиков пользователям рекомендуется информировать их о политиках архивации, применяемых к их почтовым ящикам, и предоставить последующее обучение или документацию для удовлетворения их потребностей. В эту документацию должны входить следующие сведения:

- Функциональные возможности, доступные в архиве, и политики хранения архивов по умолчанию.
- Сведения о том, когда сообщения автоматически перемещаются в архив.
- Информация об иерархии папок, созданных в архивном почтовом ящике.
- Применение личных тегов (отображается в меню Архивация политики в Outlook и Outlook в Интернете).

> ⓘ **Примечание**
>
> Если вы применяете политику хранения к пользователям с архивным почтовым ящиком, политика хранения заменяет политику MRM по умолчанию. Можно создать один или несколько тегов хранения с помощью действия **Переместить в архив**, а затем связать эти теги с политикой хранения. Вы также можете добавить теги по умолчанию **Переместить в архив** (которые создаются программой установки и связаны с политикой MRM по умолчанию) к любым политикам хранения, которые вы создаете.

Архивные квоты

Архивные почтовые ящики были разработаны для хранения журнальных данных пользователей системы обмена сообщениями за пределами их основных почтовых ящиков. Часто пользователи используют PST-файлы в связи с низкими квотами на хранение в почтовых ящиках и ограничениями, налагаемыми при превышении этих квот. Например, пользователи могут запретить отправку сообщений, если размер их почтового ящика превышает *квоту Запретить отправку*. Аналогичным образом пользователям можно запретить отправку и получение сообщений, если размер их почтового ящика превышает *квоту Запретить отправку и получение*.

Чтобы устранить необходимость в использовании PST-файлов, можно установить для архивного почтового ящика предельные размеры хранилища, которые удовлетворяют требованиям пользователя. Тем не менее, может по-прежнему требоваться сохранять некоторый контроль над квотами хранилища и ростом архивных почтовых ящиков для отслеживания затрат и расширения.

Для улучшения контроля можно настроить архивные почтовые ящики с помощью *квоты предупреждения архива* и *квоты архива*. Если архивный почтовый ящик превышает указанную квоту выдачи предупреждений для архива, событие предупреждения

регистрируется в журнале событий приложения. Когда архивный почтовый ящик превышает указанную квоту архива, то сообщения больше не перемещаются в архив, событие предупреждения регистрируется в журнале событий приложения, а в почтовый ящик пользователя отправляется сообщение квоты. По умолчанию в Exchange Server квота предупреждений архива устанавливается в 90 ГБ, а квота архива — 100 ГБ.

В следующей таблице приведены зарегистрированные события и сообщения с предупреждениями, отправляемые в случае достижения квоты выдачи предупреждений для архива и квоты архива.

Quota	**Код события**	**Тип**	**Source**	**Категория**	**Сообщение**
Квота выдачи предупреждений для архива	10022	Предупреждение	MSExchangeMailboxAssistants	Помощник по работе с управляемыми папками	`The archive mailbox '<Display Name>: <GUID>: <Mailbox Database>: <Server FQDN>' exceeded the archive warning quota '<Archive warning quota>'. Archive mailbox size is '<Size>' bytes.`

Quota	Код события	Тип	Source	Категория	Сообщение
Квота архива	8537	Предупреждение	Msexchangeis	Общие	`The archive mailbox for <Legacy DN> has exceeded the maximum archive mailbox size. You can't copy or move items into the archive mailbox. All message retention actions that move items to the archive mailbox will fail, and the primary mailbox may contain items with expired retention tags until the archive mailbox is within the maximum size limit. The mailbox owner should be notified about the condition of the archive mailbox.`

Архивация на месте и другие функции Exchange

В этом разделе описаны функциональные возможности In-Place архивации и различных функций Exchange:

- **Поиск Exchange**. Возможность быстрого поиска сообщений становится еще более важной в архивных почтовых ящиках. Для поиска Exchange разница между основным и

архивным почтовым ящиком отсутствует. Содержимое обоих почтовых ящиков индексируется. Так как архивный почтовый ящик не кэширован на компьютере пользователя (даже при использовании Outlook в режиме кэширования Exchange), результаты поиска для архива всегда предоставляются поиском Exchange. При поиске по всему почтовому ящику в Outlook результаты поиска включают основной и архивный почтовый ящик пользователей.

- **Обнаружение электронных данных на месте**. Когда диспетчер обнаружения выполняет In-Place поиска eDiscovery, также выполняется поиск в архивных почтовых ящиках пользователей. При создании поиска обнаружения из Центра администрирования Exchange (EAC) невозможно исключить архивные почтовые ящики. При использовании командной консоли Exchange для создания поиска можно исключить архив с помощью параметра *DoNotIncludeArchive* . Дополнительные сведения см. в разделе New-MailboxSearch. Дополнительные сведения см. в статье Обнаружение электронных данных на месте в Exchange Server.

- **Удержание на месте и удержание для судебного разбирательства**. Когда вы помещаете почтовый ящик в In-Place удержание или удержание для судебного разбирательства, удержание помещается как в основной, так и в архивный почтовый ящик. Дополнительные сведения см. в статье Удержание на месте и удержание для судебного разбирательства в Exchange Server.

- **Папка "Элементы с возможностью восстановления**". Архивный почтовый ящик содержит собственную папку "Элементы с возможностью восстановления" и к ней применяются те же квоты папок с возможностью восстановления, что и для основного почтового ящика. Дополнительные сведения о восстанавливаемых элементах см. в статье Папка "Элементы с возможностью восстановления" в Exchange Server.

- **Архивация Skype для бизнеса содержимого в Exchange**. Вы можете архивировать беседы с мгновенными сообщениями и документы общих собраний по сети в основном почтовом ящике пользователя. Почтовый ящик должен находиться на сервере почтовых ящиков Exchange, а в организации должен быть развернут Skype для бизнеса Server 2015.

Управление архивными почтовыми ящиками

В Exchange Server создание архивных почтовых ящиков и управление ими интегрируется с общими задачами управления почтовыми ящиками. Пошаговые процедуры см. в статье Управление архивами In-Place в Exchange Server.

- **Создание архивного почтового ящика**. Вы можете включить архивный почтовый ящик для существующего почтового ящика или создать архивный почтовый ящик при создании нового почтового ящика.

- **Перемещение архивного почтового ящика**. Архивный почтовый ящик пользователя можно переместить в другую базу данных почтовых ящиков на том же сервере почтовых ящиков или на другой сервер независимо от основного почтового ящика. Для

перемещения архивного почтового ящика пользователя необходимо создать запрос на перемещение почтового ящика. Подробнее см. в разделе Управление перемещениями локальных почтовых ящиков в Exchange Server.

- **Отключение архивного почтового ящика**. Вы можете отключить архивный почтовый ящик пользователя для устранения неполадок или переместить основной почтовый ящик в версию Exchange, которая не поддерживает архивацию In-Place. Отключение архива аналогично отключению основного почтового ящика. В локальных развертываниях отключенный архивный почтовый ящик сохраняется в базе данных почтовых ящиков до тех пор, пока не будет достигнут срок хранения удаленного почтового ящика для этой базы данных. В течение этого периода вы можете повторно подключить тот же отключенный архивный почтовый ящик к основному почтовому ящику пользователя. Когда будет достигнут период хранения удаленных почтовых ящиков, отключенный архивный почтовый ящик удаляется из базы данных почтовых ящиков.

- **Получение статистики почтовых ящиков и статистики папок**. Статистику почтовых ящиков и статистику папок почтовых ящиков для архивного почтового ящика пользователя можно получить с помощью параметра *Архив* с командлетами Get-MailboxStatistics и Get-MailboxFolderStatistics .

- **Проверка подключения к архиву**. В Exchange Server можно использовать командлет Test-ArchiveConnectivity для проверки подключения к локальному или облачному архиву почтового ящика указанного пользователя.

Управление архивами In-Place в Exchange Server

Статья • 04.04.2023

Архивация на месте помогает обеспечить контроль над данными системы обмена сообщениями в организации путем исключения необходимости в личных хранилищах сертификатов (PST) и позволяет удовлетворить требования организации к хранению сообщений и обнаружению электронных данных. Если архивация включена, пользователи могут хранить сообщения в архивном почтовом ящике, который доступен с помощью Microsoft Outlook и Outlook в Интернете.

Что нужно знать перед началом работы

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Архив на месте" в разделе Политика обмена сообщениями и разрешения на соответствие требованиям в Exchange Server.
- Процедуры, описанные в этой статье, относятся к локальным архивным почтовым ящикам. Сведения об архивных почтовых ящиках в Exchange Online см. в статье Включение архивных почтовых ящиков на портале соответствия требованиям.
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Основной почтовый ящик пользователя не может располагаться в Exchange более ранней версии, чем архив пользователя. Если основной почтовый ящик пользователя по-прежнему находится в Exchange 2010 или Exchange 2013, необходимо переместить его в Exchange 2016 или Exchange 2019, а архивный почтовый ящик — в Exchange 2016 или Exchange 2019.

Включение архивного почтового ящика

Вы можете использовать Центр администрирования Exchange или командную консоль Exchange, чтобы включить архивные почтовые ящики для тех пользователей, у которых уже есть основной почтовый ящик.

Включение архивного почтового ящика с помощью Центра администрирования Exchange

1. Перейдите в раздел **Почтовые ящики**>**получателей**.
2. Выберите почтовый ящик.
3. В области сведений в разделе **Встроенный архив** нажмите кнопку **Включить**.

   Примечание. Вы также можете массово включить архивы, выбрав несколько почтовых ящиков (используйте клавиши SHIFT или CTRL). Выбрав несколько почтовых ящиков, в области сведений выберите пункт **Дополнительные опции**. Потом в разделе **Архив** нажмите кнопку **Включить**.
4. На странице **Создание архива на месте** нажмите кнопку **ОК**, чтобы Exchange автоматически выбрал базу данных почтовых ящиков для архива, или кнопку **Обзор**, чтобы указать ее самостоятельно.

Включение архивного почтового ящика с помощью командной консоли Exchange

В этом примере включается архивный почтовый ящик пользователя Tony Smith.

PowerShell

```
Enable-Mailbox "Tony Smith" -Archive
```

В этом примере показано, как извлечь из базы данных DB01 почтовые ящики, для которых не включен локальный или облачный архив и имя которых не начинается со строки DiscoverySearchMailbox. Результаты передаются в командлет **Enable-Mailbox**, который включает архив для всех почтовых ящиков в базе данных почтовых ящиков DB01.

PowerShell

```
Get-Mailbox -Database DB01 -Filter "ArchiveGuid -Eq `$null -AND
ArchiveDomain -eq `$null -AND Name -NotLike 'DiscoverySearchMailbox*'" |
Enable-Mailbox -Archive
```

Как проверить, все ли получилось?

Чтобы проверить, успешно ли включен локальный архив для существующего почтового ящика, выполните одно из следующих действий.

- В EAC перейдите в раздел **Почтовые ящики получателей**>, а затем выберите почтовый ящик из списка. Убедитесь, что в разделе **Архив на месте** области сведений установлено значение **Включено**. Нажмите **Просмотреть сведения**, чтобы просмотреть свойства архива, в том числе его состояние и базу данных почтовых ящиков, в которой он создан.
- Чтобы вывести сведения о новом архиве, выполните в командной консоли Exchange приведенную ниже команду.

  PowerShell

  ```
  Get-Mailbox <MailboxIdentity> | Format-List Name,*Archive*
  ```

- В командной консоли Exchange проверьте подключение к архиву с помощью командлета **Test-ArchiveConnectivity**. Пример проверки подключения к архиву приведен в разделе "Примеры" статьи Test-ArchiveConnectivity.

Включение архивного почтового ящика при создании нового почтового ящика

Вы также можете включить архивный почтовый ящик при создании первого почтового ящика для пользователя.

Включение архивного почтового ящика при создании нового почтового ящика с помощью Центра администрирования Exchange

1. Перейдите в раздел **Почтовые ящики**>**получателей**.
2. Щелкните **Создать**>**почтовый ящик пользователя**.
3. На странице **Создание почтового ящика пользователя** в поле **Псевдоним** введите псевдоним пользователя.

   Примечание. Если оставить это поле пустым, для псевдонима будет использоваться значение, введенное в поле **Имя входа пользователя** .
4. Выберите один из приведенных ниже вариантов.

- **Существующий пользователь, который не поддерживает почту**. Нажмите эту кнопку и нажмите кнопку **Обзор** , чтобы открыть диалоговое окно **Выбор пользователя — весь лес** . В этом диалоговом окне отображается список учетных записей пользователей Active Directory в лесу, которые не поддерживают почту или не имеют почтовых ящиков Exchange. Выберите учетную запись пользователя, для которой необходимо включить поддержку почты, а затем нажмите кнопку **OK**. При выборе этого параметра не требуется указывать данные учетной записи пользователя, потому что они уже присутствуют в службе Active Directory.

- **Новый пользователь**. Нажмите эту кнопку, чтобы создать учетную запись пользователя в Active Directory и создать почтовый ящик для пользователя. При выборе этого варианта вам придется указать обязательные сведения об учетной записи пользователя.

5. Чтобы настроить следующие параметры, нажмите кнопку **Дополнительные параметры**.

   - **База данных почтовых ящиков**. Нажмите кнопку **Обзор** , чтобы выбрать базу данных почтовых ящиков, в которой будет храниться почтовый ящик. Если не выбрать базу данных, Exchange автоматически назначит ее.

   - **Архивировать**. Установите этот флажок, чтобы создать архивный почтовый ящик для почтового ящика. При создании архивного почтового ящика элементы автоматически перемещаются из основного почтового ящика в архивный на основе параметров политики хранения по умолчанию или на основе параметров, указанных пользователем.

   Нажмите кнопку **Обзор**, чтобы выбрать базу данных для хранения архивного почтового ящика.

6. По завершении нажмите кнопку **Сохранить**, чтобы создать почтовый ящик и его архив.

Включение архивного почтового ящика при создании нового почтового ящика с помощью командной консоли Exchange

В этом примере показано, как создать в Active Directory пользователя с именем Chris Ashton, создать почтовый ящик в базе данных почтовых ящиков DB01, а также создать и включить в этой базе данных архивный почтовый ящик. Чтобы задать

исходное значение пароля, в этом примере создается переменная ($password), появляется запрос на ввод пароля, а затем этот пароль назначается переменной как объект SecureString.

PowerShell

```
$password = Read-Host "Enter password" -AsSecureString
```

PowerShell

```
New-Mailbox -UserPrincipalName cashton@contoso.com -Alias cashton -Database "DB01" -Archive -Name "Chris Ashton" -OrganizationalUnit Users -Password $password -FirstName Chris -LastName Ashton
```

Как проверить, все ли получилось?

Чтобы проверить, успешно ли создан почтовый ящик пользователя с локальным архивом, выполните одно из следующих действий.

- В EAC перейдите в раздел **Почтовые ящики получателей**>, а затем выберите новый почтовый ящик пользователя из списка. Убедитесь, что в разделе **Архив на месте** области сведений установлено значение **Включено**. Нажмите **Просмотреть сведения**, чтобы просмотреть свойства архива, в том числе его состояние и базу данных почтовых ящиков, в которой он создан.

- Чтобы просмотреть сведения о новом почтовом ящике пользователя и архиве, выполните в командной консоли Exchange приведенную ниже команду.

  PowerShell

  ```
  Get-Mailbox <Name> | Format-List Name,RecipientTypeDetails,PrimarySmtpAddress,*Archive*
  ```

- В командной консоли Exchange проверьте подключение к архиву с помощью командлета **Test-ArchiveConnectivity**. Пример проверки подключения к архиву приведен в разделе "Примеры" статьи Test-ArchiveConnectivity.

Отключение архивного почтового ящика

Может потребоваться отключить архив пользователя в целях устранения неполадок или соответствия требованиям. При отключении архивного почтового

ящика все сведения в нем хранятся, пока не истечет срок хранения почтового ящика, после чего они безвозвратно удаляются. По умолчанию удаленные почтовые ящики, в том числе архивные, хранятся в Exchange в течение 30 дней.

Отключение архивного почтового ящика с помощью Центра администрирования Exchange

1. Перейдите в раздел **Почтовые ящики**>**получателей**.
2. Выберите почтовый ящик.
3. В области сведений в разделе **Встроенный архив** нажмите кнопку **Отключить**.

   Примечание. Вы также можете массово отключить архивы, выбрав несколько почтовых ящиков (используйте клавиши SHIFT или CTRL). Выбрав несколько почтовых ящиков, в области сведений выберите пункт **Дополнительные опции**. Затем в разделе **Архив** нажмите кнопку **Отключить**.

Отключение архивного почтового ящика с помощью командной консоли Exchange

В этом примере отключается архивный почтовый ящик для почтового ящика пользователя Chris Ashton. Основной почтовый ящик пользователя не отключается.

PowerShell

```
Disable-Mailbox "Chris Ashton" -Archive
```

Как проверить, что все получилось?

Чтобы проверить, успешно ли отключен архивный почтовый ящик, выполните указанные ниже действия.

- Выберите почтовый ящик в Центре администрирования. В области сведений проверьте состояние его архива в поле **Архив на месте**.
- Чтобы в командной консоли Exchange проверить свойства архива для пользователя почтового ящика, введите указанную ниже команду.

  PowerShell

  ```
  Get-Mailbox "Chris Ashton" | Format-List *Archive*
  ```

Если архив отключен, для его свойств возвращаются следующие значения.

Свойство	Значение
ArchiveDatabase (для локальных архивов)	<blank>
ArchiveState	`None`
DisabledArchiveDatabase (для локальных архивов)	*<name of mailbox database>*
DisabledArchiveGuid	*<GUID of disabled archive>*

Повторное включение архивного почтового ящика

При отключении архивного почтового ящика теряется соединение с ним. Отключенный архивный почтовый ящик остается в базе данных почтовых ящиков в течение определенного времени. По умолчанию отключенные архивные почтовые ящики хранятся в Exchange в течение 30 дней. В течение 30 дней после отключения архивного почтового ящика вы можете снова подключить его к основному почтовому ящику пользователя. В этом случае восстанавливается исходное содержимое архивного почтового ящика. Однако спустя 30 дней после отключения почтового ящика исходное содержимое архивного почтового ящика безвозвратно удаляется из базы данных почтовых ящиков и не может быть восстановлено. Поэтому при повторном включении архива по прошествии более 30 дней с момента его отключения создается новый архивный почтовый ящик.

Повторное включение архивного почтового ящика с помощью Центра администрирования Exchange

1. Перейдите в раздел **Почтовые ящики**>**получателей**.
2. Выберите почтовый ящик.
3. В области сведений в разделе **Личный архив** нажмите кнопку **Включить**.
4. На странице **Создание архива на месте** нажмите кнопку **OK**.

   Exchange может автоматически выбрать базу данных почтовых ящиков для повторно включенного архивного почтового ящика. Вы также можете нажать кнопку **Обзор**, чтобы выбрать базу данных самостоятельно.

Повторное включение архивного почтового ящика с помощью командной консоли Exchange

Чтобы снова включить архивный почтовый ящик, используйте команду **Enable-Mailbox -Archive**. Например:

PowerShell

```
Enable-Mailbox "Chris Ashton" -Archive
```

Как проверить, все ли получилось?

Чтобы убедиться, что отключенный архивный почтовый ящик успешно подключен к основному почтовому ящику пользователя, выполните следующую команду, чтобы получить свойства архива пользователя почтового ящика и проверить значения, возвращенные для свойств *ArchiveGuid* и *ArchiveDatabase* .

PowerShell

```
Get-Mailbox "Chris Ashton" | Format-List *Archive*
```

Как упоминалось ранее, при повторном включении архивного почтового ящика в течение 30 дней после его отключения пользователю будет доступно его исходное содержимое. Если снова включить архив по прошествии более 30 дней после его отключения, будет создан пустой архивный почтовый ящик.

удержание In-Place и удержание для судебного разбирательства в Exchange Server

Статья • 04.04.2023

При наличии обоснованных предпосылок для судебных исков организациям требуется сохранять электронные данные (включая почту), связанные с делом. Такие предпосылки нередко возникают до уточнения подробностей дела, и сохранение часто имеет широкие масштабы. Организациям может понадобиться сохранять всю почту, относящуюся к конкретному вопросу, или всю электронную почту отдельных лиц. В зависимости от политики организации в отношении обнаружения электронных данных, можно принять следующие меры по сохранению электронной почты.

- Пользователям можно порекомендовать хранить почту, не удаляя сообщения. Однако пользователи все же могут удалять электронную почту намеренно или случайно.

- Могут быть приостановлены механизмы автоматического удаления, например управление записями обмена сообщениями. Это может привести к тому, что в почтовых ящиках пользователей будет скапливаться большой объем электронной почты, из-за чего производительность их работы может снижаться. Приостановка автоматического удаления также не мешает пользователям вручную удалять электронную почту.

- В некоторых организациях электронная почта копируется или перемещается в архив, что позволяет предотвратить ее удаление, изменение или подмену. Это ведет к повышению расходов, обусловленных необходимостью ручного копирования или перемещения сообщений в архив или внедрения сторонних продуктов для сбора и хранения электронной почты вне Exchange.

Отсутствие возможности хранения электронной переписки может подвергнуть организацию юридическим и финансовым рискам, например к критическому анализу процессов обнаружения и хранения записей в организации, неблагоприятным судебным решениям, санкциям или штрафам.

Хранение для судебного разбирательства и хранение на месте.

В Exchange Server доступно два типа удержаний: удержание для судебного разбирательства и удержание In-Place. Хранение для судебного разбирательства использует свойство **LitigationHoldEnabled** почтового ящика. Если включено удержание для судебного разбирательства, все элементы почтового ящика помещаются на удержание. В отличие от этого, вы можете использовать In-Place Удержание, чтобы сохранить только те элементы, которые соответствуют условиям поискового запроса, определяемого с помощью средства обнаружения электронных данных In-Place. Вы можете разместить несколько In-Place удержаний в почтовом ящике, но удержание для судебного разбирательства включено или отключено для почтового ящика. Для обоих типов удержаний можно также указать период длительности хранения элементов. Этот срок рассчитывается с даты получения или создания элемента почтового ящика. Если длительность не задана, элементы хранятся на неопределенный срок или до тех пор, пока удержание не будет удалено. Если удалить удержание для судебного разбирательства из почтового ящика, но один или несколько In-Place удержаний по-прежнему размещаются в почтовом ящике, элементы, соответствующие условиям хранения In-Place, будут храниться в течение периода, указанного в параметрах удержания.

При удержании на месте можно указать для пользователя несколько сценариев удержания. В этом случае поисковые запросы от сценариев удержания по запросу объединяются (с помощью операторов **OR**). При этом максимальное количество ключевых слов во всех сценариях удержания по запросу, назначенных для почтового ящика, не должно превышать 500. Если ключевых слов больше, на хранение помещается все содержимое почтового ящика, а не только то, которое соответствует критериям поиска. Все содержимое удерживается, пока общее количество ключевых слов не станет равно или меньше 500.

При перемещении почтового ящика с удержанием для судебного разбирательства в Exchange 2010 или Exchange 2013 на сервер почтовых ящиков в Exchange 2016 параметр Удержание для судебного разбирательства продолжает применяться, гарантируя соблюдение требований соответствия во время и после перемещения.

> ⓘ **Важно!**
>
> При переводе почтового ящика в режим хранения для судебного удержания или хранения на месте это действие применяется как к основному, так и архивному почтовому ящику.

Дополнительные сведения об использовании каждого типа удержания см. в разделе Размещение всех почтовых ящиков на удержание.

Цели и особенности удержания

Вы можете использовать удержание для судебного разбирательства и In-Place удержание для достижения следующих целей:

- Помещать почтовые ящики пользователей на хранение и хранить их элементы без изменений.
- Хранить элементы бесконечно или в течение заданного периода времени.
- Сохранять элементы почтовых ящиков, удаленные пользователями или автоматическими процессами, например службой управления записями сообщений.
- Сохранять сообщения, пересылаемые в другой почтовый ящик.
- Использование In-Place удержания на основе запросов для поиска и хранения элементов, соответствующих указанным условиям (вы также можете разместить все элементы, включив все содержимое почтового ящика при создании удержания).
- Устанавливать несколько запретов на удаление для разных дел или расследований.
- Скрывать запреты на удаление от пользователя, так как работа службы управления записями сообщений не прерывается.
- Используйте In-Place eDiscovery для поиска элементов, которые сохраняются при удержании

При обновлении с Exchange Server 2010 г. понятие юридического удержания заключается в том, чтобы хранить все данные почтового ящика пользователя на неопределенный срок или до тех пор, пока удержание не будет удалено. В Exchange 2016 In-Place Hold представила другую модель, которая позволяет указать следующие параметры:

- **Удержание на основе запросов**. При удержании для судебного разбирательства все элементы в почтовом ящике сохраняются. Однако удержание In-Place позволяет указать, какие элементы следует хранить, с помощью параметров поискового запроса, таких как ключевые слова, отправители и получатели, даты начала и окончания, а также указать типы сообщений, такие как сообщения электронной почты, элементы календаря и Skype для бизнеса беседы, которые необходимо поместить на удержание. После создания удержания на месте на основе запроса сохраняются все

соответствующие параметрам запроса элементы почтового ящика (как существующие, так и создаваемые в будущем, включая сообщения, которые будут получены позже). Удержание для судебного разбирательства не поддерживает удержание на основе запросов.

- **Продолжительность удержания**. В случае удержания для судебного разбирательства и In-Place удержания можно указать срок хранения элементов. Можно указать бесконечную длительность удержания или длительность удержания на основе времени. Этот срок рассчитывается с даты получения или создания элемента почтового ящика. Например, если ваша организация требует, чтобы все элементы почтового ящика сохранялись в течение 7 лет, можно создать удержание на основе времени. Таким образом, если почтовый ящик помещается на удержание, а срок хранения равен 7 годам, а элемент в почтовом ящике окончательно удаляется через 2 года с даты его получения, он хранится в течение 5 лет до очистки из базы данных почтового ящика.

  > **Совет**
  >
  > Вы можете использовать удержание на основе времени вместе с политикой хранения, чтобы убедиться, что элементы сохраняются в течение указанного времени, а затем окончательно удаляются из Exchange по истечении срока хранения и срока хранения.

Помещение почтового ящика на удержание

Роль управления юридическим удержанием необходима для размещения почтового ящика в хранилище для судебного разбирательства или In-Place удержания. Но для создания In-Place удержания на основе запросов вам также должна быть назначена роль поиска в почтовых ящиках. Пользователи, добавленные в группу ролей управления доступом на основе ролей (RBAC) (или назначенные роли "Поиск по юридическим причинам" и "Поиск в почтовых ящиках"), могут размещать пользователей и создавать In-Place удержания на основе запросов. Сведения о добавлении участников в группу ролей "Управление обнаружением" см. в статье Назначение разрешений на обнаружение электронных данных в Exchange Server.

Вы можете разместить удержание для судебного разбирательства почтового ящика на странице **Получатели** в Центре администрирования Exchange или с помощью `Set-Mailbox -LitigationHoldEnabled $true` команды командной консоли Exchange.

Функция удержания In-Place интегрирована с In-Place поисками по обнаружению электронных данных. Вы можете поместить почтовый ящик в In-Place **удержание & с помощью мастера удержания электронных данных на месте** в EAC или командлета **New-MailboxSearch** в командной консоли Exchange. Чтобы узнать, как это сделать, см. следующие статьи:

- Применение к почтовому ящику функции судебного удержания
- Создание или удаление инцидента хранения на месте

> ⓘ **Примечание**
>
> Если вы используете Exchange Online Archiving для подготовки облачного архива для локальных почтовых ящиков, необходимо управлять удержаниями In-Place из локальной Exchange Server организации. Параметры хранения автоматически передаются в облачный архив с помощью DirSync.

Во многих организациях уведомление пользователей о включении режима хранения является обязательным. Кроме того, когда почтовый ящик находится на хранении, не требуется приостанавливать действие политик хранения, применяемых к пользователю почтового ящика. Так как сообщения продолжают удаляться как обычно, пользователи могут не замечать, что включен режим хранения. Если ваша организация требует, чтобы пользователи, удерживаемые на удержании, были уведомлены, вы можете добавить сообщение уведомления для пользователя почтового ящика, заполив свойство **Комментарий к хранению** и используя свойство **RetentionUrl** для ссылки на веб-страницу для получения дополнительных сведений. В Outlook 2010 и более поздних версиях комментарий к хранению и URL-адрес отображаются в области Backstage, расположенной на ленте **Файлы** . Для добавления этих свойств можно использовать командлет **Set-Mailbox** .

Функции хранения и папка "Элементы с возможностью восстановления"

Хранение для судебного разбирательства и хранение In-Place используют папку "Элементы с возможностью восстановления" для сохранения элементов. Папка "Элементы с возможностью восстановления" скрыта в представлении по умолчанию в Outlook, Outlook в Интернете и других почтовых клиентах. Дополнительные сведения о папке "Элементы с возможностью восстановления" см. в статье Папка "Элементы с возможностью восстановления" в Exchange Server.

По умолчанию при удалении сообщения из папки, отличной от папки "Удаленные", сообщение перемещается в папку "Удаленные". Когда пользователь *обратимо удаляет* элемент (нажав клавиши SHIFT+DELETE) или удаляет элемент из папки "Удаленные", сообщение перемещается в папку "Элементы с возможностью восстановления", тем самым исчезая из представления пользователя.

Элементы хранятся в папке элементов для восстановления в течение срока хранения удаленных элементов, настроенного для базы данных почтовых ящиков пользователя. По умолчанию период хранения удаленного элемента в базах данных почтовых ящиков равен 14 дням.

Папка "Элементы с возможностью восстановления" содержит следующие вложенные папки, используемые для хранения удаленных элементов на различных сайтах и упрощения удержания для судебного разбирательства и In-Place удержания:

- **Удаления**. Элементы, удаленные из папки "Удаленные" или обратимо удаленные из других папок, перемещаются во вложенную папку Удаления и отображаются пользователю при использовании функции "Восстановить удаленные элементы" в Outlook и Outlook в Интернете. По умолчанию элементы находятся в этой папке до тех пор, пока не истечет срок хранения удаленных элементов, настроенный для базы данных почтовых ящиков, или до истечения срока хранения почтового ящика.

- **Очистка**. Когда пользователь удаляет элемент из папки "Элементы с возможностью восстановления" (с помощью средства "Восстановить удаленные" в Outlook и Outlook в Интернете, элемент перемещается в папку Очистка. Элементы, для которых истек период хранения, заданный для базы данных почтовых ящиков, также перемещаются в эту папку. Элементы в этой папке не будут видимы пользователям, использующим средство восстановления удаленных элементов. Когда помощник по обслуживанию почтовых ящиков обрабатывает почтовый ящик, элементы в папке "Очистка" удаляются из базы данных почтовых ящиков. Когда вы помещете пользователя почтового ящика в удержание для судебного разбирательства, помощник по почтовым ящикам не очищает элементы в этой папке.

- **DiscoveryHolds**. Если пользователь помещается в In-Place удержание, удаленные элементы перемещаются в эту папку. Когда помощник по обслуживанию почтовых ящиков обрабатывается почтовый ящик, он оценивает сообщений в этой папке. Элементы, соответствующие запросу In-Place удержания, хранятся до указанного в запросе периода удержания. Если период удержания не указан, неопределенное время или до тех пор, пока

пользователь не удаляется из удержания. Однако если вы помещаете пользователя, который уже был в In-Place удержание для судебного разбирательства, предпочтение отдается удержанию для судебного разбирательства. Поэтому удаленные элементы перемещаются в папку Очистка.

- **Версии**. Когда пользователь помещается в In-Place удержание или удержание для судебного разбирательства, элементы почтового ящика должны быть защищены от незаконного изменения или изменения пользователем или процессом. Для этого используется процесс *копирования при записи* . Когда пользователь или процесс изменяет определенные свойства элемента почтового ящика, копия исходного объекта сохраняется в папке версий, прежде чем изменение будет совершено. Этот процесс повторяется для последующих изменений. Сообщения, попавшие в папку версий, также индексируются и возвращаются во время обнаружения электронных данных на месте. После удаления сценария хранения помощник по обслуживанию управляемых папок удаляет копии из папки "Версии".

Свойства, активирующие копирование при записи

Тип элемента	Свойства, активирующие копирование при записи
Сообщения (IPM.Note*) Сообщения (IPM.Post*)	Subject Текст сообщения Вложения Отправители и получатели Даты отправки и получения
Элементы, отличные от сообщений	Любые изменения видимых свойств за исключением следующих: • Расположение элемента (когда элемент перемещается между папками) • Изменение состояния элемента (прочитан или не прочитан) • Изменения тега хранения, примененного к элементу
Элементы в папке "Черновики" по умолчанию	Нет (элементы в папке "Черновики", для которых отменено копирование при записи)

> **ⓘ Важно!**
>
> Помощник по восстановлению календаря определяет, что некоторые участники ответили на приглашение на собрание в форме "Принять" или "Под вопросом" и этот элемент отсутствует в календаре участника. Для элементов

календаря и элементов с заданным напоминанием функция копирования при записи отключена для свойств ReminderTime и ReminderSignalTime. Изменения этих свойств не фиксируются функцией копирования при записи. Изменения в RSS-каналах не фиксируются функцией копирования при записи.

Хотя папки DiscoveryHolds, "Очистка" и "Версии" не видны пользователю, все элементы в папке "Элементы с возможностью восстановления" можно обнаружить с помощью обнаружения электронных данных на месте. После удаления пользователя почтового ящика из In-Place удержания или удержания для судебного разбирательства элементы в папках DiscoveryHolds, Purges и Versions очищаются помощником по управляемым папкам.

Если почтовый ящик не помещается в удержание для судебного разбирательства или In-Place удержание, элементы в папке Очистки окончательно удаляются из папки "Элементы с возможностью восстановления", когда элемент находится в папке дольше, чем период хранения удаленного элемента.

Запреты на удаление и квоты почтового ящика

Элементы в папке корзины не учитываются в квоте почтового ящика пользователя. В Exchange папка корзины имеет свою собственную квоту. Для Exchange значения по умолчанию для свойств почтовых ящиков *RecoverableItemsWarningQuota* и *RecoverableItemsQuota* имеют значение 20 ГБ и 30 ГБ соответственно. Чтобы изменить эти значения для базы данных почтовых ящиков для Exchange Server, используйте командлет Set-MailboxDatabase. Чтобы изменить их для отдельных почтовых ящиков, используйте командлет Set-Mailbox.

Если папка "Элементы с возможностью восстановления" пользователя превышает квоту предупреждений для восстанавливаемых элементов (как указано в параметре *RecoverableItemsWarningQuota*), событие регистрируется в журнале событий приложений сервера почтовых ящиков. Когда папка превышает квоту для восстанавливаемых элементов (как указано в параметре *RecoverableItemsQuota*), пользователи не смогут очистить папку "Удаленные" или окончательно удалить элементы почтового ящика. Функция копирования при записи также не сможет создавать копии изменяемых элементов. Поэтому критически важно отслеживать квоты папки элементов с возможностью восстановления для пользователей почтовых ящиков, помещенных в режим удержания на месте.

Запреты на удаление и пересылка электронной почты

Пользователи с почтовыми ящиками на сервере Exchange Server могут использовать Outlook и Outlook в Интернете для настройки переадресации электронной почты для своего почтового ящика. Email переадресация позволяет пользователям настраивать свои почтовые ящики для пересылки сообщений электронной почты, отправленных в почтовый ящик, в другой почтовый ящик, расположенный внутри или за ее пределами. Администраторы также могут настроить правила потока обработки почты (также известные как правила транспорта) для пересылки сообщений в другой почтовый ящик. В обоих случаях переадресацию электронной почты можно настроить таким образом, чтобы любое сообщение, отправленное в исходный почтовый ящик, не копировалось в этот почтовый ящик, а отправлялось только на адрес пересылки.

Если почтовый ящик находится на удержании, выполняются дополнительные действия. В процессе доставки проверяются параметры удержания для почтового ящика. Если сообщение соответствует условиям удержания для почтового ящика, копия сообщения сохраняется в папке "Входящие". Это значит, что пересланные сообщения можно найти в исходном почтовом ящике с помощью функции обнаружения электронных данных на месте.

Сохранение архивного содержимого Skype для бизнеса

Exchange 2016 и Exchange 2019, Skype для бизнеса и SharePoint 2016 предоставляют интегрированный интерфейс сохранения и обнаружения электронных данных, позволяющий сохранять и искать элементы в разных хранилищах данных. Exchange 2016 и 2019 позволяют архивировать Skype для бизнеса содержимое в Exchange, устраняя требование наличия отдельной базы данных SQL Server для хранения архивного содержимого Lync. Встроенная возможность удержания и обнаружения электронных данных в SharePoint 2016 позволяет сохранять и искать данные во всех хранилищах с одной консоли.

Когда вы помещаете почтовый ящик Exchange Server в In-Place удержание или удержание для судебного разбирательства, Skype для бизнеса содержимое (например, беседы с мгновенными сообщениями и файлы, к которым предоставлен доступ на собрании по сети) архивируются в почтовом ящике. При поиске в почтовом ящике с помощью In-Place обнаружения электронных данных все архивные Skype для бизнеса содержимое, соответствующее поисковому

запросу, также возвращается в результатах поиска. Вы также можете ограничить поиск Skype для бизнеса содержимого, заархивированного в почтовом ящике.

Чтобы включить архивацию содержимого Skype для бизнеса в почтовых ящиках Exchange Server, необходимо настроить интеграцию Skype для бизнеса Server 2015 с Exchange Server. Дополнительные сведения см. в следующих разделах:

- Планирование архивации
- Развертывание архивации

Удаление почтового ящика на хранении

Если удалить учетную запись пользователя с почтовым ящиком, хранилище сведений Exchange в конечном итоге обнаружит, что почтовый ящик больше не подключен к учетной записи пользователя, и помечает этот почтовый ящик для удаления, даже если почтовый ящик находится на удержании. Если вы хотите сохранить почтовый ящик, выполните следующие действия.

1. Не удаляйте учетную запись пользователя, а отключите ее.
2. Измените свойства почтового ящика, чтобы ограничить использование и доступ к почтовому ящику. Например, установите для квот на отправку и получение значение 1, заблокируйте потенциальных отправителей сообщений на этот почтовый ящик и ограничьте возможность доступа к нему.
3. Храните почтовый ящик до тех пор, пока не будут удалены все данные или пока сохранение данных не потребуется.

Перенос почтовых ящиков на удержание из Exchange Server в Microsoft 365 или Office 365

Если у вас есть гибридное развертывание Exchange, при перемещении (подключении) локального почтового ящика Exchange Server в Exchange Online в Microsoft 365 или Office 365 выполняются следующие условия:

- Если локальный почтовый ящик помещен на хранение для судебного разбирательства или хранение на месте, параметры хранения сохраняются после переноса почтового ящика в Exchange Online.

- Если локальный почтовый ящик помещен на хранение для судебного разбирательства или хранение на месте, все содержимое папки корзины перемещается в почтовый ящик Exchange Online.

Параметры удержания и содержимое в папке элементов с возможностью восстановления также сохраняются при перемещении (за пределами системы) почтового ящика Exchange Online в локальную организацию Exchange Server.

> **Совет**
>
> Для Exchange Server гибридное развертывание Exchange — это рекомендуемый способ переноса локальных почтовых ящиков в Microsoft 365 или Office 365.

Создание или удаление инцидента удержания на месте

Статья • 10.01.2024

Запрет на удаление позволяет сохранить все содержимое почтового ящика и общедоступной папки, в том числе удаленные элементы и исходные версии измененных элементов. Все такие элементы возвращаются при поиске методом обнаружения электронных данных на месте. Запрет на удаление почтового ящика пользователя также распространяется на содержимое соответствующего архивного почтового ящика (если он включен).

При создании In-Place удержания можно поместить все элементы в исходный почтовый ящик или в общедоступную папку на удержание или удерживать только те элементы, которые соответствуют условиям поиска, указанным для удержания. Аналогичным образом можно хранить элементы неограниченное время или в течение определенного периода времени. Дополнительные сведения о удержании In-Place см. в разделе Удержание на месте и удержание по делу в Exchange Server.

Вы можете создавать запреты на удаление в Центр администрирования Exchange (EAC) или Командная консоль Exchange.

Перед началом работы

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Удержание на месте" в разделе Политика обмена сообщениями и разрешения на соответствие требованиям Exchange Server.
- В зависимости от топологии Active Directory и времени задержки репликации включение удержания на месте может занять до часа.
- Как указывалось ранее, запрет на удаление почтового ящика пользователя также распространяется на содержимое его архивного почтового ящика.
- Искать содержимое и помещать его на удержание можно только во всех общедоступных папках организации. Нельзя указать отдельные общедоступные папки.
- Описание рабочего процесса хранения на месте см. в разделе Дополнительные сведения.

- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

Создание удержания на месте

Использование EAC для создания удержания на месте

1. Перейдите в **раздел Управление соответствием**> на**месте eDiscovery & Удержание**, а затем щелкните ➕

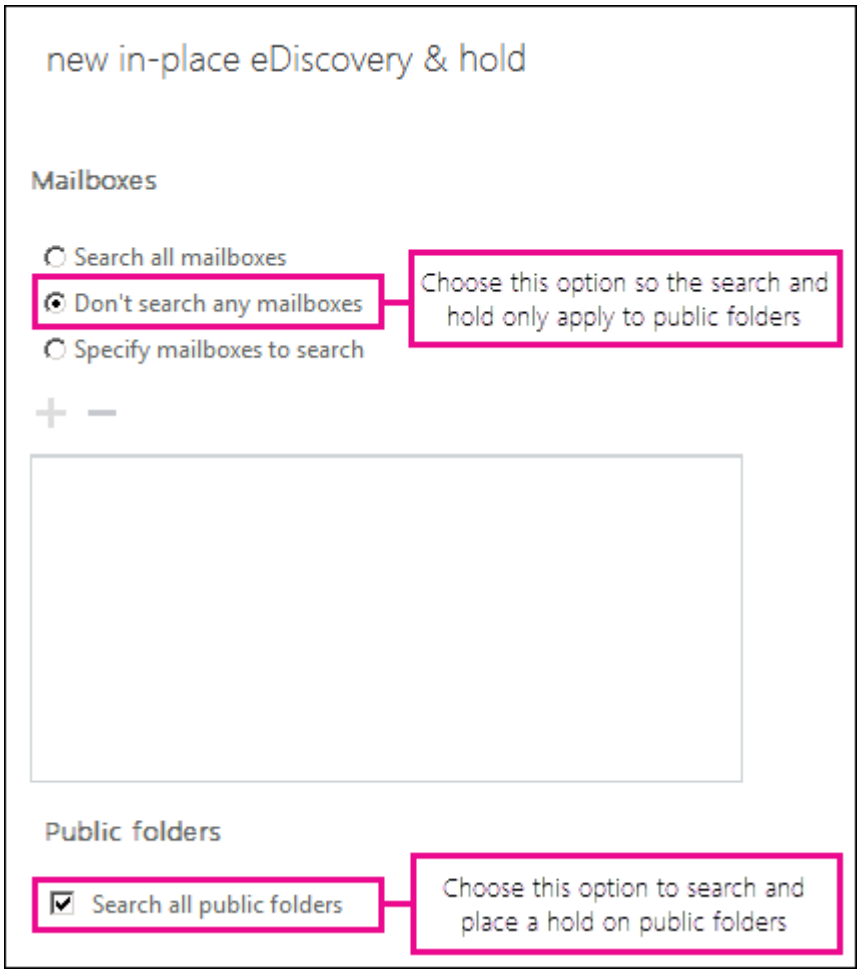
2. В окне **New In-Place eDiscovery & Удержание** на странице **Имя и описание** введите имя удержания и необязательное описание, а затем нажмите кнопку **Далее**.

3. На странице **Почтовые ящики и общедоступные папки** выберите источники контента для поиска:

    - Чтобы исключить почтовые ящики (и поместить на хранение только общедоступные папки), нажмите кнопку **Не выполнять поиск в почтовых ящиках**.

    - Чтобы выполнить поиск в определенных почтовых ящиках, выберите пункт **Указать почтовые ящики для поиска**, а затем добавьте нужные почтовые ящики.

    - Чтобы поместить общедоступные папки на хранение, нажмите кнопку **Поиск во всех общедоступных папках**.



> ⓘ **Важно!**
>
> При создании In-Place удержания нельзя выбрать параметр **Поиск по всем почтовым ящикам** . Чтобы создать In-Place удержание, необходимо выбрать определенные почтовые ящики, которые нужно поместить на удержание.

4. На странице **Поисковый запрос** заполните указанные ниже поля, а затем нажмите кнопку **Далее**.

   - **Включить все содержимое**. Выберите этот параметр, чтобы поместить все содержимое в выбранные источники на удержание.
   - **Фильтр на основе условий**. Выберите этот параметр, чтобы указать критерии поиска, включая ключевые слова, даты начала и окончания, адреса отправителей и получателей, а также типы сообщений.

   > ⓘ **Важно!**
   >
   > Если при хранении на месте для пользователя указано несколько сценариев хранения, поисковые запросы от сценариев хранения на

основе запроса объединяются (с помощью операторов **OR**). В этом случае максимальное количество ключевых слов во всех сценариях хранения на основе запроса, назначенных для почтового ящика, не должно превышать 500. Если ключевых слов больше, на хранение помещается все содержимое почтового ящика, а не только то, которое соответствует критериям поиска. Все содержимое удерживается, пока общее количество ключевых слов не станет равно или меньше 500.

5. На странице **Параметры хранения на месте** установите флажок **Поместить содержимое, соответствующее поисковому запросу в выбранных источниках, на удержание**, а затем выберите один из следующих параметров:

   - **Удержание на неопределенный срок**. Поместите элементы, возвращенные поиском, на неопределенное удержание. Найденные элементы будут храниться, пока вы не измените срок хранения, не удалите почтовый ящик (или общедоступные папки) из поискового запроса или сам поисковый запрос.

   - **Укажите количество дней для хранения элементов относительно даты их получения**: хранение элементов на определенный период. Например, эту функцию можно использовать, если для вашей организации необходимо, чтобы все сообщения сохранялись на протяжении не менее семи лет. Вы можете использовать In-Place удержания *на основе времени* вместе с политикой хранения, чтобы убедиться, что элементы будут окончательно удалены в течение семи лет.

6. Нажмите кнопку **Готово**, чтобы создать запрет на удаление.

Создания запрета на удаление с помощью Командная консоль Exchange

В этом примере создается In-Place удержание с именем Hold-CaseId012 и добавляется почтовый ящик joe@contoso.com в удержание.

> ⓘ **Важно!**
>
> Если не указать дополнительные параметры поиска для удержания на месте, все элементы в указанных исходных почтовых ящиках ставятся на удержание. Если не указать параметр *ItemHoldPeriod* , элементы помещаются на удержание

на неопределенный срок или до тех пор, пока почтовый ящик не будет удален из удержания или удержание не будет удалено.

PowerShell

```
New-MailboxSearch "Hold-CaseId012" -SourceMailboxes "joe@contoso.com" -
InPlaceHoldEnabled $true
```

В этом примере все общедоступные папки в организации помещаются на хранение на месте на 7 лет. Запрет не распространяется на почтовые ящики.

PowerShell

```
New-MailboxSearch -Name "Hold for Public Folders" -AllPublicFolderSources
$true -AllSourceMailboxes $false -ItemHoldPeriod 2555 -InPlaceHoldEnabled
$true
```

Подробные сведения о синтаксисе и параметрах см. в разделе New-MailboxSearch.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли создано удержание на месте, выполните одно из следующих действий:

- Используйте EAC, чтобы убедиться, что удержание In-Place отображается в представлении списка на странице **& удержания электронных данных на месте** .
- Используйте командлет **Get-MailboxSearch** для получения операции поиска в почтовых ящиках и проверьте свойства хранения. Например, следующая команда отображает свойства хранения для операции поиска Hold-CaseId012:

  PowerShell

  ```
  Get-MailboxSearch "Hold-CaseId012" | Format-List
  InPlaceHoldEnabled,ItemHoldPeriod,InPlaceHoldIdentity
  ```

- Используйте командлет **Get-Mailbox** для отображения сведений о хранении на месте для определенных почтовых ящиков пользователей или общедоступных папок. Например, следующая команда отображает идентификатор GUID хранения на месте:

  PowerShell

```
Get-Mailbox "joe@contoso.com" | Format-List InPlaceHolds
```

В этом примере отображается идентификатор GUID хранения на месте для всех почтовых ящиков общедоступных папок в организации.

PowerShell

```
Get-Mailbox -PublicFolder | Format-List Name,InPlaceHolds
```

Удаление удержания на месте

В Exchange Server для хранения и поиска содержимого в источниках контента используются поисковые запросы eDiscovery. Невозможно удалить поиск методом обнаружения электронных данных на месте, с помощью которого источники контента помещены на хранение. Сначала необходимо удалить In-Place Удержание, очистив поле **Разместить содержимое, соответствующее поисковому запросу в выбранных источниках на** удержание проверка на странице **Удержание на месте**, или установив для параметра *InPlaceHoldEnabled* значение `$false` в командной консоли Exchange. Кроме того, можно удалить почтовые ящики и общедоступные папки из In-Place Hold, изменив значение параметров *SourceMailboxes* или *AllPublicFolderSources, указанных* в поиске.

Использование EAC для удаления удержания на месте

1. Перейдите в раздел **Управление соответствием**> требованиям**на месте & удержание электронных** данных.

2. В представлении списка выберите In-Place Удержание, которое нужно удалить, и нажмите кнопку **Изменить**.

3. В разделе Свойства **& удержания электронных данных на месте на странице Удержание** на **месте** снимите флажок **Разместить содержимое, соответствующее поисковому запросу в выбранных источниках при удержании** проверка, и нажмите кнопку **Сохранить**.

4. Выберите In-Place Удержание еще раз в представлении списка и нажмите кнопку **Удалить**

5. В окне предупреждения нажмите кнопку **Да**, чтобы удалить поиск.

Снятие запрета на удаление с помощью Командная консоль Exchange

В этом примере сначала отключается удержание Hold-CaseId012, а затем удаляется поиск в почтовых ящиках.

PowerShell

```
Set-MailboxSearch "Hold-CaseId012" -InPlaceHoldEnabled $false; Remove-
MailboxSearch "Hold-CaseId012"
```

Подробные сведения о синтаксисе и параметрах см. в разделе Set-Mailboxsearch.

Как проверить, все ли получилось?

Чтобы убедиться в том, что вы успешно удалили удержание на месте, выполните одно из следующих действий:

- Используйте EAC, чтобы убедиться, что In-Place Удержание не отображается в представлении списка на вкладке **& удержание электронных данных на месте** .
- Используйте командлет **Get-MailboxSearch** для получения всех операций поиска в почтовых ящиках и убедитесь, что среди них удаленного поиска.

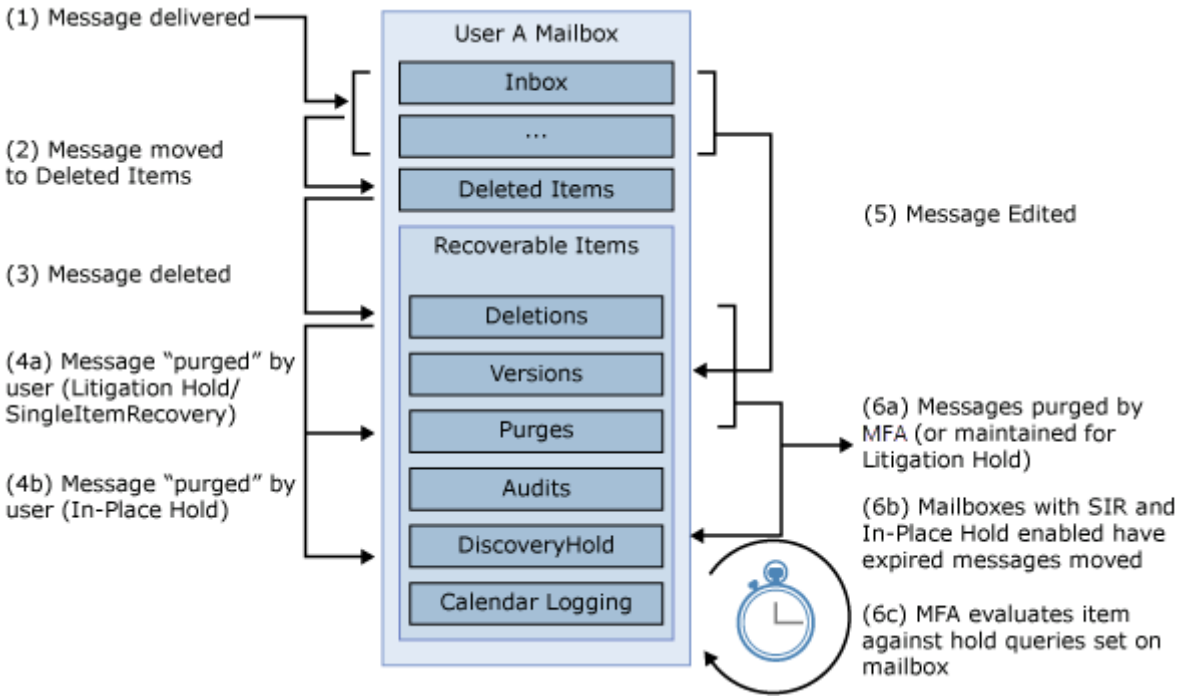
Дополнительная информация

Как работает In-Place удержание? Если почтовый ящик или общедоступная папка не находится на удержании, элемент перемещается во вложенную папку "Удаления" в папке "Элементы с возможностью восстановления", когда он окончательно удаляется (SHIFT+Delete) или удаляется из папки "Удаленные". Политика удаления (срок хранения элементов) также перемещает элементы во вложенную папку Удаления по истечении срока хранения. Когда пользователь удаляет элемент из папки "Элементы с возможностью восстановления" или истекает срок хранения удаленного элемента, он перемещается во вложенную папку очистки и помечается для окончательного удаления. Он будет удален из Exchange при следующей обработке почтового ящика помощником по управляемым папкам.

Если почтовый ящик или общедоступная папка находится на хранение на месте, удаленные элементы не перемещаются в подпапку очистки, а вместо этого перемещаются в подпапку удержаний для обнаружения и хранятся в течение

указанного периода времени. Срок хранения рассчитывается от даты получения или создания элемента и определяет срок хранения элементов в подпапке удержаний для обнаружения. По истечении срока хранения в подпапке удержаний для обнаружения элемент помечается для окончательного удаления и удаляется из Exchange при следующей обработке почтового ящика или общедоступной папки помощником для управляемых папок. Если почтовый ящик или общедоступная папка помещена на бессрочное хранение, элементы никогда не удаляются из подпапки удержаний для обнаружения.

На следующем рисунке показаны подпапки в папке "Элементы с возможностью восстановления" и рабочий процесс хранения.



> ⓘ **Примечание**
>
> Если почтовый ящик помещен на хранение для судебного разбирательства, удаленные элементы перемещаются в подпапку очистки и хранятся в течение настроенного срока хранения.

Перевод почтового ящика в режим хранения для судебного разбирательства

Статья • 04.04.2023

Поместите почтовый ящик на хранение для судебного разбирательства, чтобы сохранить все его содержимое, в том числе удаленные элементы и исходные версии измененных элементов. На хранение также помещается архивный почтовый ящик пользователя (если он включен). Удаленные и измененные элементы хранятся в течение указанного периода или пока вы не отключите режим хранения для судебного разбирательства. Все такие элементы почтового ящика возвращаются при обнаружении электронных данных на месте в Exchange Server поиска.

Перед началом работы

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Удержание на месте" в разделе Политика обмена сообщениями и разрешения на соответствие требованиям Exchange Server.

- Вступление в силу режима хранения для судебного разбирательства может занять до 60 минут.

- В режиме хранения для судебного разбирательства элементы сохраняются в папке "Элементы с возможностью восстановления" почтового ящика пользователя. Размер этой папки по умолчанию — 30 ГБ. В зависимости от количества и размера удаленных или измененных элементов размер папки может быстро увеличиться. Для папки "Элементы с возможностью восстановления" по умолчанию задается высокая квота. Рекомендуем еженедельно проверять размер почтовых ящиков, помещенных на хранение для судебного разбирательства, чтобы не допустить исчерпания квоты.

- Как указывалось ранее, запрет на удаление почтового ящика пользователя также распространяется на его архивный почтовый ящик.

- В режиме хранения для судебного разбирательства сохраняются удаленные элементы и исходные версии измененных элементов. При желании вы можете указать продолжительность хранения элемента почтового ящика.

Длительность периода хранения рассчитывается с даты получения сообщения или создания элемента почтового ящика.

- Описание рабочего процесса хранения для судебного разбирательства см. в разделе Дополнительные сведения.

Как поместить почтовый ящик на хранение для судебного разбирательства, используя Центр администрирования Exchange

1. Перейдите в раздел **Почтовые ящики**>**получателей**.
2. В списке почтовых ящиков пользователей щелкните почтовый ящик, который нужно поместить в удержание для судебного разбирательства, а затем щелкните **Изменить**.
3. На странице свойств почтового ящика щелкните **Функции почтового ящика**.
4. В разделе **Хранение для судебного разбирательства: отключено** нажмите кнопку **Включить**, чтобы применить к почтовому ящику хранение для судебного разбирательства.
5. На странице **Хранение для судебного разбирательства** введите значения для приведенных ниже дополнительных параметров.

    - **Продолжительность удержания для судебного разбирательства (в днях)**. Используйте это поле, чтобы указать, как долго хранятся элементы почтового ящика, когда почтовый ящик помещается в удержание для судебного разбирательства. Длительность будет вычислена с даты получения или создания элемента почтового ящика. Если оставить это поле пустым, элементы будут храниться в течение неопределенного времени или до отмены хранения. Длительность указывается в днях.

    - **Примечание***. Используйте это поле, чтобы сообщить пользователю, что его почтовый ящик находится на удержании для судебного разбирательства. Заметка появится на вкладке **Файл** в Outlook 2010 или более поздней версии.

    - **URL-адрес***. Используйте это поле, чтобы направить пользователя на веб-сайт для получения дополнительных сведений о удержании для судебного разбирательства. Этот URL-адрес отображается на вкладке **Файл** Outlook 2010 или более поздней версии.

*Если оставить значения **Примечание** и **URL-адрес** пустыми, пользователь не будет уведомлен о том, что вы наложили удержание в его почтовом ящике.

6. Нажмите кнопку **Сохранить** на странице **Хранение для судебного разбирательства**, а затем щелкните **Сохранить** на странице свойств почтового ящика.

Как поместить почтовый ящик на бессрочное хранение для судебного разбирательства, используя командную консоль Exchange

В этом примере почтовый ящик bsuneja@contoso.com помещается в хранилище для судебного разбирательства. Элементы в почтовом ящике хранятся в течение неопределенного времени или до отмены хранения.

PowerShell

```
Set-Mailbox bsuneja@contoso.com -LitigationHoldEnabled $true
```

> **Примечание**
>
> Если вы размещаете почтовый ящик в удержании для судебного разбирательства на неопределенный срок (не указывая период длительности), для почтового ящика свойства *LitigationHoldDuration* устанавливается `Unlimited`значение .

Как поместить почтовый ящик на хранение для судебного разбирательства в течение указанного срока, используя командную консоль Exchange

В этом примере почтовый ящик bsuneja@contoso.com помещается в хранилище для судебного разбирательства и сохраняет элементы в течение 2555 дней (приблизительно 7 лет).

PowerShell

```
Set-Mailbox bsuneja@contoso.com -LitigationHoldEnabled $true -
LitigationHoldDuration 2555
```

Как поместить все почтовые ящики на хранение для судебного разбирательства, используя командную консоль Exchange

Организация может требовать сохранения всех данных почтовых ящиков.

В этом примере все почтовые ящики пользователей в организации помещаются на хранение для судебного разбирательства на один год (365 дней).

PowerShell

```
Get-Mailbox -ResultSize Unlimited -Filter "RecipientTypeDetails -eq
'UserMailbox'" | Set-Mailbox -LitigationHoldEnabled $true -
LitigationHoldDuration 365
```

В этом примере с помощью командлета Get-Mailbox извлекаются все почтовые ящики в организации, с помощью фильтра получателей включаются все почтовые ящики пользователей, а затем список почтовых ящиков передается командлету Set-Mailbox, чтобы включить хранение для судебного разбирательства и задать срок хранения.

Чтобы поместить все почтовые ящики пользователей на неопределенное удержание, выполните предыдущую команду, но не включайте параметр *LitigationHoldDuration* .

Примеры включения или исключения одного либо нескольких почтовых ящиков с помощью других свойств получателей в фильтре приведены в разделе Дополнительные сведения.

Как отключить хранение для судебного разбирательства для почтового ящика, используя командную консоль Exchange

В этом примере почтовый ящик bsuneja@contoso.com удаляется из удержания для судебного разбирательства.

PowerShell

```
Set-Mailbox bsuneja@contoso.com -LitigationHoldEnabled $false
```

Как проверить, все ли получилось?

Чтобы убедиться, что почтовый ящик успешно переведен в режим хранения для судебного разбирательства, выполните одно из следующих действий.

- В Центре администрирования Exchange:

    1. Перейдите в раздел **Почтовые ящики**>**получателей**.
    2. В списке почтовых ящиков пользователей щелкните почтовый ящик, для которого нужно проверить параметры удержания для судебного разбирательства, а затем щелкните **Изменить**.
    3. На странице свойств почтового ящика щелкните **Функции почтового ящика**.
    4. В разделе **Хранение для судебного разбирательства** убедитесь, что включен режим хранения.
    5. Щелкните **Просмотр сведений**, чтобы проверить, кто и когда перевел почтовый ящик в режим хранения для судебного разбирательства. Вы также можете проверить или изменить значения дополнительных параметров в полях **Длительность хранения для судебного разбирательства (дней)**, **Примечание** и **URL-адрес**.

- Выполните одну из следующих команд в командной консоли Exchange:

    PowerShell

    ```
    Get-Mailbox <name of mailbox> | Format-List LitigationHold*
    ```

    или

    PowerShell

    ```
    Get-Mailbox -ResultSize Unlimited -Filter "RecipientTypeDetails -eq
    'UserMailbox'" | Format-List Name,LitigationHold*
    ```

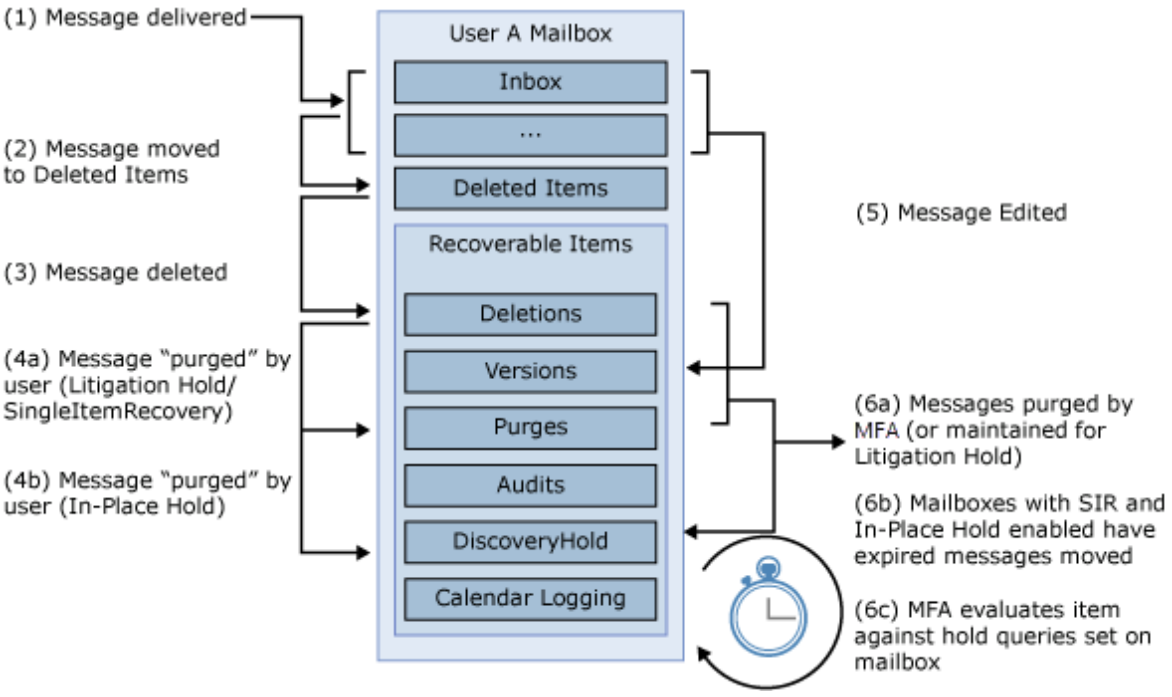
    Если почтовый ящик помещается в удержание для судебного разбирательства на неопределенный срок, для почтового ящика свойства *LitigationHoldDuration* устанавливается `Unlimited`значение .

Дополнительные сведения

- **Как работает хранение для судебного разбирательства?** Если почтовый ящик не на хранении, после удаления с помощью клавиш Shift+Delete или удаления из папки "Удаленные" элемент перемещается в подпапку удаления в папке "Элементы с возможностью восстановления". По истечении срока хранения, заданного политикой удаления (тег хранения, для которого настроено действие хранения), элементы также перемещаются в подпапку удаления. Когда пользователь удаляет элемент в папке "Элементы с возможностью восстановления" или истекает срок хранения удаленного элемента, он перемещается в подпапку очистки и помечается для окончательного удаления. Он будет удален из Exchange при следующей обработке почтового ящика помощником для управляемых папок.

  Если почтовый ящик находится на хранении для судебного разбирательства, элементы в подпапке очистки хранятся в течение указанного срока. Срок хранения рассчитывается от даты получения или создания элемента. По истечении срока хранения элемент в подпапке очистки помечается для окончательного удаления и удаляется из Exchange при следующей обработке почтового ящика помощником для управляемых папок. Если почтовый ящик помещен на бессрочное хранение, элементы никогда не удаляются из подпапки очистки.

  На следующем рисунке показаны подпапки в папке "Элементы с возможностью восстановления" и рабочий процесс хранения.



> ⓘ **Примечание**

> Если почтовый ящик помещен на хранение на месте, удаленные элементы перемещаются из подпапки Deletions в подпапку DiscoveryHolds и хранятся в течение указанного срока.

- Если в организации требуется сохранять данные всех почтовых ящиков в течение определенного периода времени, следует учесть следующие моменты, прежде чем перевести все почтовые ящики в организации в режим хранения для судебного разбирательства.
  - Если вы используете предыдущую команду для перевода всех почтовых ящиков в организации (или подмножества почтовых ящиков, соответствующих требованиям указанного фильтра получателей) в режим хранения для судебного разбирательства, на хранение помещаются только почтовые ящики, доступные на момент выполнения команды. Чтобы применить функцию хранения к позднее созданным почтовым ящикам, команду понадобится выполнить еще раз. Если вы часто создаете почтовые ящики, можно запланировать выполнение команды с необходимой частотой.
  - Перевод всех почтовых ящиков в режим хранения для судебного разбирательства может существенно повлиять на размер почтовых ящиков. В организации Exchange 2016 или Exchange 2019 запланируйте достаточное хранилище в соответствии с требованиями организации к сохранению.
  - Для этой папки размер хранилища предусмотрен отдельно, и потому увеличение количества элементов в ней не может привести к превышению ограничения для хранилища почтовых ящиков. Как упоминалось ранее, сохранение данных почтового ящика в течение длительного периода времени приведет к росту папки "Элементы с возможностью восстановления" в почтовом ящике и архиве пользователя. Рекомендуется периодически отслеживать размер этой папки с помощью командлета **Get-MailboxFolderStatistics** , чтобы убедиться, что она не достигает предела. Дополнительные сведения см. в разделе:
    - Get-MailboxFolderStatistics
    - Очистите или удалите элементы из папки "Элементы с возможностью восстановления".
- В предыдущей команде, которая переводит все почтовые ящики в режим хранения, используется фильтр получателей, возвращающий все почтовые ящики пользователей. Вы можете использовать другие свойства получателей,

чтобы вернуть список определенных почтовых ящиков, которые затем можно передать командлету **Set-Mailbox** для перевода этих почтовых ящиков в режим хранения для судебного разбирательства.

Вот несколько примеров использования командлетов **Get-Mailbox** и **Get-Recipient** для получения подмножества пользователей на основе общих свойств пользователей или почтовых ящиков. В этих примерах предполагается, что были заполнены соответствующие свойства почтового ящика (например , *CustomAttributeN* или *Department*).

PowerShell

```
Get-Mailbox -RecipientTypeDetails UserMailbox -ResultSize unlimited -
Filter 'CustomAttribute15 -eq "OneYearLitigationHold"'
```

PowerShell

```
Get-Recipient -RecipientTypeDetails UserMailbox -ResultSize unlimited -
Filter 'Department -eq "HR"'
```

PowerShell

```
Get-Recipient -RecipientTypeDetails UserMailbox -ResultSize unlimited -
Filter 'PostalCode -eq "98052"'
```

PowerShell

```
Get-Recipient -RecipientTypeDetails UserMailbox -ResultSize unlimited -
Filter 'StateOrProvince -eq "WA"'
```

PowerShell

```
Get-Mailbox -ResultSize Unlimited -Filter "RecipientTypeDetails -ne
'DiscoveryMailbox'"
```

Вы можете использовать в фильтре другие свойства, чтобы включать и исключать почтовые ящики. Подробные сведения см. в статье Filterable Properties for the -Filter Parameter.

Применение функции удержания ко всем почтовым ящикам

Статья • 04.04.2023

Вашей организации может потребоваться сохранить все данные почтового ящика в течение определенного периода. Для выполнения этого требования можно использовать удержание для судебного разбирательства или In-Place удержание. После помещения почтового ящика в удержание для судебного разбирательства или In-Place удержания элементы почтового ящика, которые были изменены или удалены без возможности восстановления, сохраняются в папке Элементы с возможностью восстановления в течение срока, указанного в удержании. Дополнительные сведения см. в разделе Удержание на месте и удержание для судебного разбирательства в Exchange Server.

Прежде чем применять ко всем почтовым ящикам в организации эти функции, обратите внимание на следующее:

- Если применить к почтовому ящику функцию хранения, она будет действовать и для содержимого архивного почтового ящика пользователя (если он включен).
- Применение функции хранения ко всем почтовым ящикам в организации может существенно увеличить их размер. В Exchange Server развертывании запланируйте достаточное хранилище в соответствии с требованиями организации к сохранению.
- Длительное хранение данных почтового ящика приведет к увеличению размера папки "Элементы с возможностью восстановления" в основном и архивном почтовых ящиках пользователя. Для этой папки размер хранилища предусмотрен отдельно, и потому увеличение количества элементов в ней не может привести к превышению ограничения для хранилища почтовых ящиков. В Exchange Server по умолчанию для папки "Элементы с возможностью восстановления" используется ограничение в 30 ГБ. Рекомендуется периодически отслеживать размер этой папки, чтобы убедиться, что она не достигает предела. Дополнительные сведения см. в разделе Папка "Элементы с возможностью восстановления" в Exchange Server.

Что выбрать: хранение для судебного разбирательства или хранение на месте?

Ниже приведены некоторые факторы, которые следует учитывать при выборе функции удержания, которая будет использоваться для всех почтовых ящиков в организации.

Назначение	**Применение хранения для судебного разбирательства**	**Применение хранения на месте**
Использование Центра администрирования Exchange	Да Для настройки удержания для судебного разбирательства EAC лучше всего подходит для быстрых разовых действий в нескольких почтовых ящиках. Мы рекомендуем использовать командную консоль Exchange для размещения удержания для судебного разбирательства для всех пользователей в вашей организации. Дополнительные сведения см. в разделе Размещение почтового ящика в удержании для судебного разбирательства.	Да Однако в Центре администрирования Exchange невозможно выбрать более 500 исходных почтовых ящиков. Дополнительные сведения см. в статье Создание или удаление In-Place удержания.
Использование командной консоли Exchange	Да	Да
Применение функции хранения к более 10 000 почтовых ящиков	Да Хранение для судебного разбирательства — это свойство почтового ящика. Вы можете поместить все почтовые ящики в организации на удержание с помощью командлета **Set-Mailbox**.	Да, используйте несколько объектов хранения на месте. Для одного объекта хранения на месте вы можете указать до 10 000 почтовых ящиков с помощью групп рассылки. Чтобы применить функцию хранения к дополнительным почтовым ящикам, создайте другие объекты хранения. Это потребует дополнительных затрат на управление. Хранение для судебного разбирательства упрощает удержание большого количества почтовых ящиков.

Назначение	Применение хранения для судебного разбирательства	Применение хранения на месте
Применение функции хранения к нескольким почтовым ящикам течение различных сроков.	Да Хранение для судебного разбирательства — это свойство почтового ящика. К каждому почтовому ящику (или наборам почтовых ящиков) вы можете применять функцию хранения в течение различных сроков. В разделе Дополнительные сведения приведены примеры того, как с помощью свойств получателей в фильтре можно применить хранение для судебного разбирательства к подмножеству почтовых ящиков.	Да Если вы создаете отдельные объекты хранения для тысячи почтовых ящиков, мы рекомендуем использовать хранение для судебного разбирательства. Однако если вы создаете удержания для определенных событий, в которых задействовано несколько пользователей (например, в судебном случае), используйте для группы пользователей одно удержание на месте. Не рекомендуется создавать отдельные удержания In-Place для каждого почтового ящика, так как это приведет к созданию множества запросов In-Place удержания. Это будет сложнее управлять, чем судебные удержания. Большое количество объектов удержания In-Place также может привести к снижению производительности в EAC при обновлении, создании или изменении In-Place объектов eDiscovery или In-Place удержания.

Назначение	Применение хранения для судебного разбирательства	Применение хранения на месте
Автоматическое применение функции хранения к новым почтовым ящикам	Нет После создания нового почтового ящика его необходимо поместить на хранение для судебного разбирательства. Для этого вы также можете запланировать выполнение команды или сценария с необходимой частотой.	Нет Необходимо добавить новый почтовый ящик к существующему удержанию In-Place, даже если вы указали группу рассылки при создании In-Place удержания. Для этого вы также можете запланировать выполнение команды или сценария с необходимой частотой. Мы рекомендуем проверять с помощью сценария, достигнуто ли ограничение в размере 10 000 почтовых ящиков для объекта хранения на месте, а затем при необходимости создавать новый.

Применение ко всем почтовым ящикам хранения для судебного разбирательства

Вы можете легко и быстро поместить все почтовые ящики на удержание на неопределенный срок или на указанный срок с помощью командной консоли Exchange. Эта команда помещает все почтовые ящики на удержание с длительностью удержания 2555 дней (около 7 лет).

PowerShell

```
Get-Mailbox -ResultSize Unlimited -Filter "RecipientTypeDetails -eq
'UserMailbox'" | Set-Mailbox -LitigationHoldEnabled $true -
LitigationHoldDuration 2555
```

В примере используется командлет Get-Mailbox и фильтр получателей для получения всех почтовых ящиков пользователей в организации, а затем передает список почтовых ящиков в командлет Set-Mailbox , чтобы включить удержание для судебного разбирательства и указать длительность удержания. Дополнительные сведения см. в разделе Размещение почтового ящика в удержании для судебного разбирательства.

Применение хранения на месте ко всем почтовым ящикам

С помощью EAC можно выбрать до 500 почтовых ящиков и поместить их на удержание. Дополнительные сведения см. в статье Создание или удаление In-Place удержания.

Чтобы разместить более 500 пользователей в In-Place удержание, используйте командную консоль Exchange. Дополнительные сведения см. в разделе New-MailboxSearch.

> **Совет**
>
> В гибридных средах можно использовать функцию неактивного почтового ящика в Exchange Online для хранения почтовых ящиков без использования лицензии или необходимости использования учетной записи для почтового ящика. Для функции неактивного почтового ящика требуется лицензия "Exchange Online план 2, Office 365 корпоративный E3 и E5". Если у вас есть лицензия Exchange Online плана 1, необходимо назначить отдельную лицензию "Exchange Online Archiving" почтовому ящику. Дополнительные сведения см **. в разделе Неактивный почтовый ящик**.

Дополнительные сведения

- Когда вы помещаете все почтовые ящики в организации на удержание, функция хранения применяется только к почтовым ящикам, существующим на момент выполнения команды. Чтобы применить функцию хранения к почтовым ящикам, созданным позднее, запустите команду еще раз. Если вы часто создаете новые почтовые ящики, можно запланировать выполнение команды с необходимой частотой.

- Размещение почтовых ящиков на удержание сохраняет данные, предотвращая удаление элементов в папке "Элементы с возможностью восстановления" до истечения указанного срока хранения элемента. Если удержание настроено для неограниченного хранения элементов, они не будут очищаться из почтового ящика. Кроме того, если почтовый ящик находится на удержании, исходная версия сообщения сохраняется перед изменением. Объедините удержание для судебного разбирательства или удержание In-Place с политикой хранения, которая может автоматически удалять сообщения (и перемещать их в папку "Элементы с возможностью восстановления") по

истечении указанного периода времени в соответствии с требованиями вашей организации к хранению электронной почты. Дополнительные сведения см. в разделе Теги хранения и политики хранения в Exchange Server.

- Команда командной консоли Exchange, используемая в этом разделе для размещения удержания для судебного разбирательства во всех почтовых ящиках, использует фильтр получателей, который возвращает все почтовые ящики пользователей. Вы можете использовать другие свойства получателей, чтобы получить список определенных почтовых ящиков, который можно передать командлету **Set-Mailbox**, чтобы применить функцию хранения для судебного разбирательства к этим почтовым ящикам.

  Вот несколько примеров использования командлетов **Get-Mailbox** и **Get-Recipient** для получения подмножества пользователей на основе общих свойств пользователей или почтовых ящиков. В этих примерах предполагается, что были заполнены соответствующие свойства почтового ящика (например , *CustomAttributeN* или *Department*).

  PowerShell

  ```
  Get-Mailbox -RecipientTypeDetails UserMailbox -ResultSize unlimited -Filter 'CustomAttribute15 -eq "OneYearLitigationHold"'
  ```

  PowerShell

  ```
  Get-Recipient -RecipientTypeDetails UserMailbox -ResultSize unlimited -Filter 'Department -eq "HR"'
  ```

  PowerShell

  ```
  Get-Recipient -RecipientTypeDetails UserMailbox -ResultSize unlimited -Filter 'PostalCode -eq "98052"'
  ```

  PowerShell

  ```
  Get-Recipient -RecipientTypeDetails UserMailbox -ResultSize unlimited -Filter 'StateOrProvince -eq "WA"'
  ```

  PowerShell

  ```
  Get-Mailbox -ResultSize Unlimited -Filter "RecipientTypeDetails -ne 'DiscoveryMailbox'"
  ```

Вы можете использовать в фильтре другие свойства, чтобы включать и исключать почтовые ящики. Подробные сведения см. в статье Filterable Properties for the -Filter Parameter.

Сохранение скрытых копий и получателей расширенной группы рассылки для обнаружения электронных данных

Статья • 04.04.2023

In-Place удержание и удержание для судебного разбирательства позволяет сохранять содержимое почтового ящика в соответствии с нормативными требованиями и требованиями к обнаружению электронных данных. Сведения о получателях, непосредственно адресованные в полях Кому и Копия сообщения, по умолчанию включаются во все сообщения, но вашей организации может потребоваться возможность поиска и воспроизведения сведений обо всех получателях сообщения. Это включает в себя

- **Получатели, адресованные с помощью поля СК сообщения**: получатели СК хранятся в сообщении в почтовом ящике отправителя, но не включаются в заголовки сообщения, доставляемого получателям.
- **Получатели расширенной группы рассылки**: получатели, которые получают сообщение, так как они являются членами группы рассылки, к которой было адресовано сообщение, в полях Кому, Копия или СК.

Exchange 2016 и Exchange 2019 сохраняют сведения о получателях ск и расширенных групп рассылки. Эти сведения можно найти с помощью функции электронного обнаружения и удержания.

Способы хранения получателей скрытой копии и расширенной группы рассылки

Как уже упоминалось, сведения о получателях в скрытой копии хранятся в сообщении в почтовом ящике отправителя. Эти сведения индексируются и доступны для обнаружения электронных данных и хранения на месте.

Сведения о получателях расширенной группы рассылки хранятся в сообщении после применения функции хранения на месте или хранения для судебного разбирательства к почтовому ящику. Участие в группе рассылки определяется на момент отправки сообщения. На расширенный список получателей, сохраненный в сообщении, не влияют изменения участия в группе после отправки сообщения.

Сведения о...	Хранится в...	Хранятся по умолчанию?	Доступен для...
Получатели в полях "Кому" и "Копия"	Свойствах сообщения в почтовых ящиках отправителя и получателей.	Да	Отправитель, получатели и ответственные за обеспечение соответствия требованиям
Получатели в поле "Скрытая копия"	Свойствах сообщения в почтовом ящике отправителя.	Да	Отправитель и ответственные за обеспечение соответствия требованиям
Получатели расширенной группы рассылки	Свойствах сообщения в почтовом ящике отправителя.	Нет. Сведения о получателях расширенной группы рассылки хранятся после применения функции хранения на месте или хранения для судебного разбирательства к почтовому ящику.	Ответственные за обеспечение соответствия требованиям

Поиск сообщений, отправленных получателям в скрытой копии или получателям расширенной группы рассылки

Результаты поиска для обнаружения электронных данных о сообщениях, отправленных пользователю, теперь включают сообщения, отправленные группе рассылки, в которую входит получатель. В таблице ниже показаны сценарии, в которых в результатах поиска для обнаружения электронных данных возвращаются сообщения, отправленные получателям в скрытой копии и получателям расширенной группы рассылки.

Сценарий 1. Джон является членом US-Sales группы рассылки. В этой таблице показаны результаты поиска eDiscovery, когда Боб прямо или косвенно отправляет сообщение Джону через группу рассылки.

При поиске отправленных сообщений в почтовом ящике Боба...	И сообщение отправляется с...	Результаты включают сообщение?
Кому: Павел	Павел в поле "Кому"	Да

При поиске отправленных сообщений в почтовом ящике Боба...	И сообщение отправляется с...	Результаты включают сообщение?
Кому: Павел	Отдел продаж в России в поле "Кому"	Да
Кому: Отдел продаж в России	Отдел продаж в России в поле "Кому"	Да
Копия: Павел	Павел в поле "Копия"	Да
Копия: Павел	Отдел продаж в России в поле "Копия"	Да
Копия: Отдел продаж в России	Отдел продаж в России в поле "Копия"	Да

Сценарий 2. Боб отправляет сообщение электронной почты Джону (Кому/Копия) и Джеку (ск) напрямую или косвенно через группу рассылки. В таблице ниже показаны результаты поиска eDiscovery.

При поиске...	Для отправленных сообщений...	Результаты включают сообщение?	Примечания
Почтовый ящик Ивана	Кому/Копия: Павел	Да	Указывает, что Виктор добавлен в поле "Скрытая копия"
Почтовый ящик Ивана	Скрытая копия: Виктор	Да	Указывает, что Виктор добавлен в поле "Скрытая копия"
Почтовый ящик Ивана	Скрытая копия: Виктор (через группу рассылки)	Да	Список участников группы рассылки в скрытой копии, расширенный при отправке сообщения, отображается в предварительном просмотре результатов поиска для обнаружения электронных данных, их экспорте и журналах.
Почтовый ящик Павла	Кому/Копия: Павел	Да	Получатели в скрытой копии не указываются

При поиске...	Для отправленных сообщений...	Результаты включают сообщение?	Примечания
Почтовый ящик Павла	Скрытая копия: Виктор (напрямую или через группу рассылки)	Нет	В сообщении, доставленном получателям, не хранятся сведения о поле "Скрытая копия". Нужно искать в почтовом ящике отправителя.
Почтовый ящик Виктора	Кому/Копия: Павел (напрямую или через группу рассылки)	Да	В сообщение, доставленное всем получателям, включены сведения о полях "Кому" и "Копия".
Почтовый ящик Виктора	Скрытая копия: Виктор (напрямую или через группу рассылки)	Нет	В сообщении, доставленном получателям, не хранятся сведения о поле "Скрытая копия". Нужно искать в почтовом ящике отправителя.

Вопросы и ответы

В. Когда и где хранятся сведения о получателе СК?

О. Сведения о получателях в поле "Скрытая копия" по умолчанию сохраняются в исходном сообщении в почтовом ящике отправителя. Если в качестве получателя в поле "Скрытая копия" указана группа рассылки, участие в ней расширяется, только если почтовый ящик отправителя находится на хранении.

В. Когда и где хранится список развернутых получателей группы рассылки?

О. Членство в группе расширяется во время отправки сообщения. Список расширенных членов группы рассылки хранится в исходном сообщении в почтовом ящике отправителя. Почтовый ящик отправителя должен находиться в In-Place удержании или удержании для судебного разбирательства.

В. Могут ли получатели to/cc увидеть, какие получатели были скакированы?

О. Нет. Заголовки сообщения не содержат этих сведений, а получатели в полях "Кому" и "Копия" их не видят. Отправитель может просматривать поле "Скрытая копия" в исходном сообщении, сохраненном в его почтовом ящике. Ответственные за обеспечение соответствия требованиям могут просматривать эти сведения во время поиска в почтовом ящике отправителя.

В. Как обеспечить постоянное сохранение получателей расширенной группы рассылки?

О. Сведения об этом см. в статье Place all mailboxes on hold.

В. Какие типы групп поддерживаются?

О. Поддерживаются группы рассылки, группы безопасности, поддерживающие почту, и динамические группы рассылки.

В. Существует ли ограничение на количество получателей группы рассылки, развернутых и хранящихся в сообщении?

О. Сохраняется не более 10 000 участников группы рассылки.

В. Поддерживаются ли вложенные группы рассылки?

О. Да, развернуты 25 уровней вложенных групп рассылки.

В. Где отображаются сведения о получателе ск и расширенной группы рассылки?

О. Сведения о получателях в скрытой копии и получателях расширенной группы рассылки отображаются для ответственных за обеспечение соответствия требованиям во время выполнения поиска с помощью функции обнаружения электронных данных. Получатели в скрытой копии и получатели расширенной группы рассылки включены в результаты поиска, скопированные в почтовый ящик найденных сообщений или экспортированные в PST-файл, а также в журнал обнаружения электронных данных, который входит в результаты поиска. Сведения о получателях в скрытой копии также доступны в предварительном просмотре результатов поиска.

В. Что произойдет, если член группы рассылки скрыт из глобального списка адресов организации?

О. Ничего. Даже если получатели скрыты в GAL, они входят в список получателей для расширенной группы рассылки.

In-Place обнаружение электронных данных в Exchange Server

Статья • 04.04.2023

Если ваша организация придерживается юридических требований обнаружения (связанных с политикой организации, соответствием требованиям или судебными исками), In-Place обнаружение электронных данных в Exchange Server может помочь вам выполнить поиск соответствующего содержимого в почтовых ящиках. Вы также можете использовать функцию обнаружения электронных данных на месте в гибридной среде Exchange для поиска в локальных и облачных почтовых ящиках с использованием одной и той же операции поиска.

> ⓘ **Важно!**
>
> In-Place обнаружение электронных данных — это мощная функция, которая позволяет пользователю с правильными разрешениями потенциально получить доступ ко всем записям обмена сообщениями, хранящимся в Exchange Server организации. Очень важно отслеживать и контролировать действия пользователей по обнаружению, в том числе по добавлению участников в группу ролей управления обнаружением и предоставлению доступа к почтовым ящикам найденных сообщений.

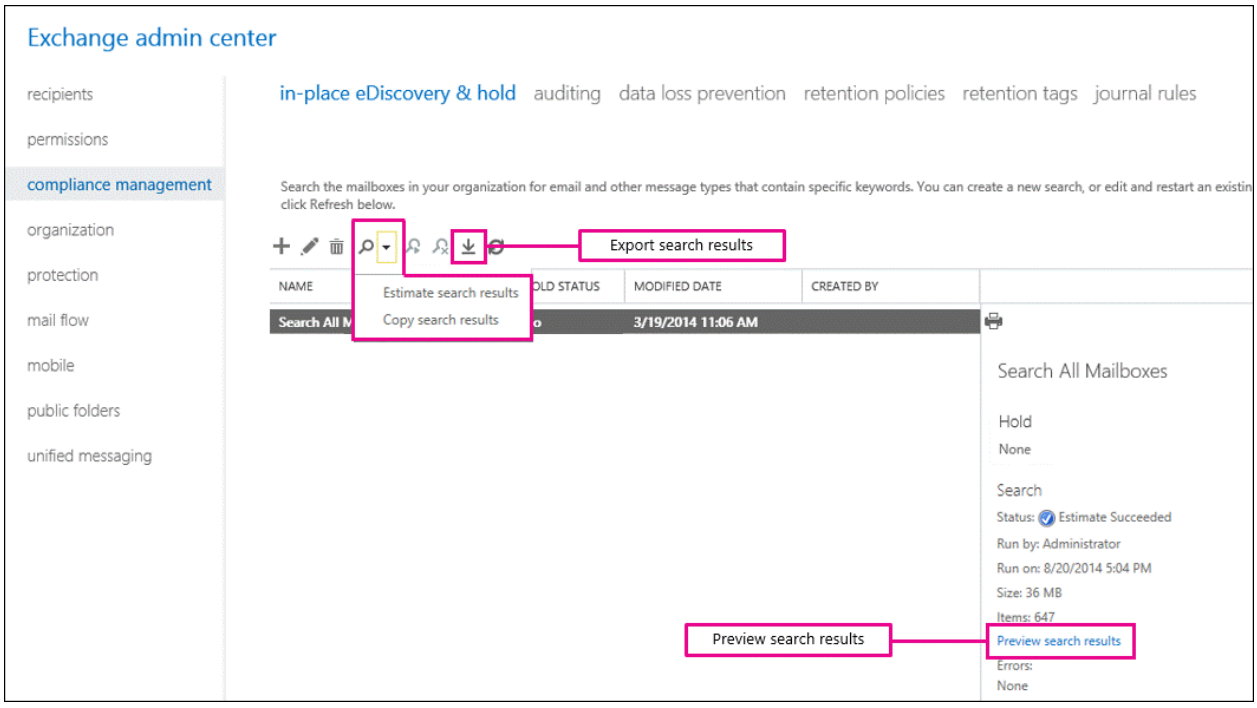
Принципы работы обнаружения электронных данных на месте

В электронном обнаружении на месте используются индексы содержимого, созданные службой поиска Exchange. Функция управления доступом на основе ролей (RBAC) позволяет группе ролей Управление обнаружением делегировать задачи обнаружения нетехническому персоналу без необходимости предоставлять пользователям расширенные права, с помощью которых они могут вносить изменения в конфигурацию Exchange. Центр администрирования Exchange (EAC) предоставляет простой в использовании интерфейс поиска для нетехнических сотрудников, таких как юристы и сотрудники по соответствию требованиям, менеджеры по записям и специалисты по персоналу.

Авторизованные пользователи могут выполнять обнаружение электронных данных на месте, выбирая почтовые ящики и указывая условия поиска, такие как ключевые слова, начальная и конечная дата, адреса отправителей и получателей, а также

типы сообщений. После завершения поиска авторизованные пользователи могут выбрать одно из следующих действий:

- **Оценка результатов поиска** . Этот параметр возвращает оценку общего размера и количества элементов, которые будут возвращены поиском на основе указанных условий.
- **Предварительный просмотр результатов поиска** . Этот параметр предоставляет предварительный просмотр результатов. Отображаются сообщения, возвращенные из каждого включенного в поиск почтового ящика.
- **Копировать результаты поиска** . Этот параметр позволяет копировать сообщения в почтовый ящик обнаружения.
- **Экспорт результатов поиска** . После копирования результатов поиска в почтовый ящик обнаружения их можно экспортировать в PST-файл.



In-Place eDiscovery использует язык запросов по ключевым словам (KQL). Пользователи, знакомые с KQL, могут создавать мощные поисковые запросы для поиска индексов контента. Дополнительные сведения о KQL см. в справочнике по синтаксису языка запросов ключевых слов.

In-Place разрешения на обнаружение электронных данных

Чтобы авторизованные пользователи выполняли поиск In-Place обнаружения электронных данных, необходимо добавить их в группу ролей Управление обнаружением . Эта группа ролей состоит из двух ролей управления: роли поиска почтовых ящиков, которая позволяет пользователю выполнять поиск In-Place eDiscovery, и роли удержания по юридическим причинам, которая позволяет пользователю разместить почтовый ящик в In-Place удержание и удержание для судебного разбирательства.

По умолчанию разрешения для выполнения задач, связанных с электронным обнаружением на месте, не назначаются пользователям или администраторам Exchange. Администраторы Exchange, входящие в группу роли управления организацией, могут добавлять пользователей в группу роли управления обнаружением и создавать настраиваемые группы ролей для сужения области менеджера по обнаружению до подмножества пользователей. Дополнительные сведения о добавлении пользователей в группу ролей "Управление обнаружением" см. в статье Назначение разрешений на обнаружение электронных данных в Exchange Server.

> ⓘ **Важно!**
>
> Если пользователь не добавлен в группу ролей "Управление обнаружением" или ему не назначена роль поиска почтовых ящиков, пользовательский интерфейс "**Удержание eDiscovery & на месте** " не отображается в EAC, а командлеты In-Place eDiscovery (***MailboxSearch**) недоступны в командной консоли Exchange.

Аудит изменений в роли RBAC, включенный по умолчанию, обеспечивает ведение соответствующих записей для отслеживания назначений группы ролей управления обнаружением. Отчет о группе ролей администраторов используется для поиска изменений в группах ролей администраторов. Подробнее см. в разделе Search the role group changes or administrator audit logs.

Использование обнаружения электронных данных на месте

Поиск методом обнаружения электронных данных на месте могут выполнять пользователи, которые были добавлены в группу ролей управления обнаружением. Поиск можно выполнить с помощью веб-интерфейса в EAC. Он облегчает нетехническому персоналу (делопроизводителям, должностным лицам, отвечающим за соблюдение нормативных требований, юристам или сотрудникам

отдела кадров) выполнение обнаружение электронных данных на месте. Для выполнения поиска также можно использовать командную консоль Exchange. Дополнительные сведения см. в статье Создание In-Place поиска eDiscovery в Exchange Server

The **In-Place eDiscovery & Hold** wizard in the EAC allows you to create an In-Place eDiscovery search and also use In-Place Hold to place search results on hold. When you create an In-Place eDiscovery search, a search object is created in the In-Place eDiscovery system mailbox. This object can be manipulated to start, stop, modify, and remove the search. After you create the search, you can choose to get an estimate of search results, which includes keyword statistics that help you determine query effectiveness. You can also do a live preview of items returned in the search, allowing you to view message content, the number of messages returned from each source mailbox and the total number of messages. You can use this information to further fine-tune your query if required.

Если результаты поиска соответствуют требованиям, вы можете скопировать их в почтовый ящик найденных сообщений. Чтобы экспортировать почтовый ящик найденных сообщений или часть его содержимого в PST-файл, можно воспользоваться Outlook или EAC.

При создании поиска методом обнаружения электронных данных на месте необходимо указать следующие параметры:

- **Имя** — имя поиска используется для идентификации поиска. При копировании результатов поиска в почтовый ящик обнаружения в почтовом ящике обнаружения создается папка с помощью имени поиска и метки времени для уникальной идентификации результатов поиска в почтовом ящике обнаружения.

- **Источники**. Вы можете выполнить поиск по всем почтовым ящикам в организации Exchange Server или указать почтовые ящики для поиска. Вы также можете выполнить поиск по всем общедоступным папкам. Если вы также хотите использовать тот же поиск для размещения элементов на удержании, необходимо указать почтовые ящики. Вы также можете поместить все общедоступные папки в In-Place удержание. Можно указать группу рассылки, включающую пользователей почтовых ящиков, которые являются членами этой группы. Членство в группе вычисляется один раз при создании поиска, а последующие изменения членства в группе автоматически не отражаются в поиске. Основной и архивный почтовые ящики пользователя включаются в поиск.

- **Поисковый запрос** . Вы можете либо включить все содержимое почтового ящика из указанных почтовых ящиков, либо использовать поисковый запрос для возврата элементов, которые более важны для дела или исследования. В поисковом запросе можно указать следующие параметры.

  - **Ключевые слова** . Вы можете указать ключевые слова и фразы для поиска содержимого сообщения. Кроме того, вы можете использовать логические операторы **AND**, **OR** и **NOT**. Кроме того, Exchange Server также поддерживает оператор **NEAR**, что позволяет искать слово или фразу, расположенные рядом с другим словом или фразой.

    Для поиска точного совпадения фразы из нескольких слов необходимо заключить фразу в кавычки. Например, при поиске фразы "план и конкуренция" будут возвращены сообщения, содержащие точное совпадение этой фразы, тогда как при указании фразы **план И конкуренция** будут возвращены сообщения, содержащие слова **план** и **конкуренция** в любой части сообщения.

    Exchange Server также поддерживает синтаксис языка запросов ключевых слов (KQL) для поиска In-Place обнаружения электронных данных. Дополнительные сведения о KQL см. в справочнике по синтаксису языка запросов ключевых слов.

    > ⓘ **Примечание**
    >
    > Электронное обнаружение на месте не поддерживает регулярные выражения.

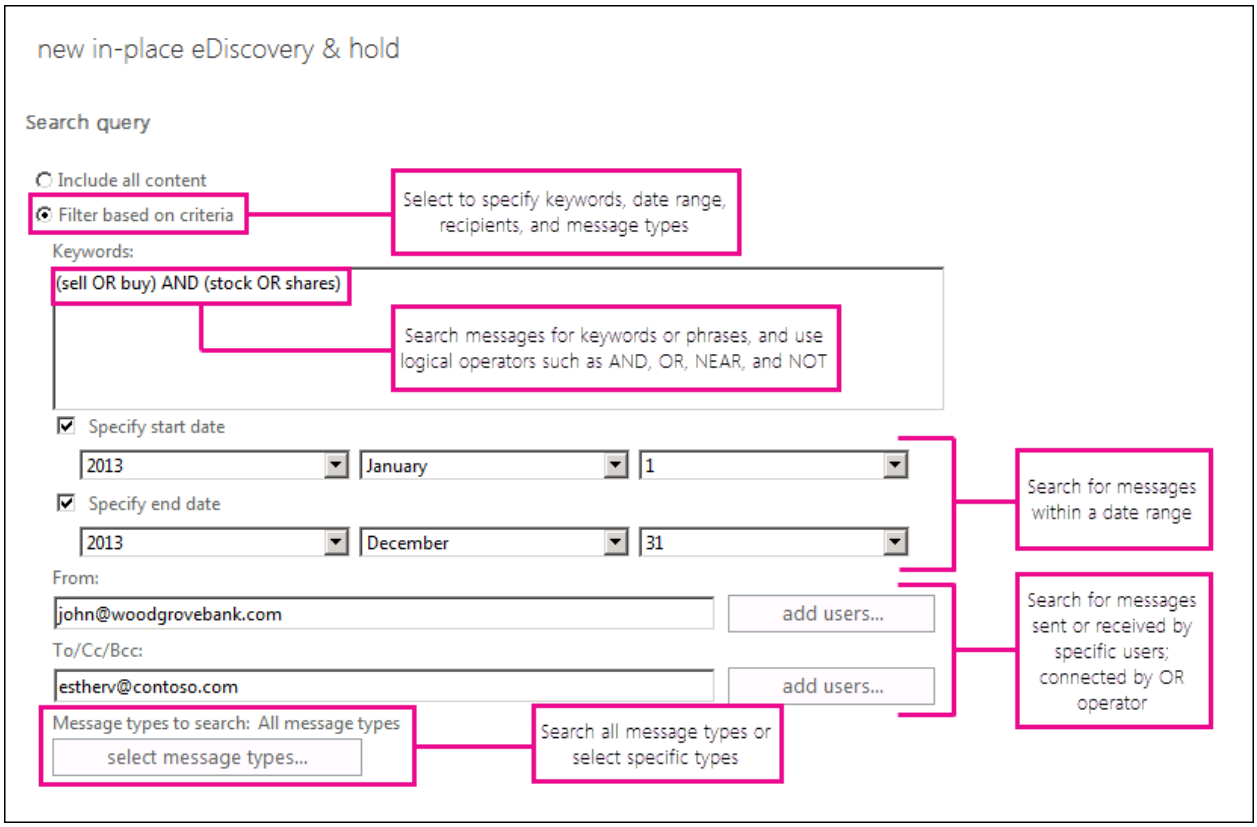
    You must capitalize logical operators such as **AND** and **OR** for them to be treated as operators instead of keywords. We recommend that you use explicit parenthesis for any query that mixes multiple logical operators to avoid mistakes or misinterpretations. For example, if you want to search for messages that contain either WordA or WordB AND either WordC or WordD, you must use **(WordA OR WordB) AND (WordC OR WordD)**.

  - **Даты начала и окончания** . По умолчанию In-Place обнаружение электронных данных не ограничивает поиск диапазоном дат. Чтобы найти сообщения, отправленные в определенный диапазон дат, можно сузить поиск, указав дату начала и окончания периода. Если не задать дату окончания, то в результатах поиска будут показываться последние результаты каждый раз, когда поиск осуществляется заново.

- **Отправители и получатели** . Чтобы сузить поиск, можно указать отправителей или получателей сообщений. Вы можете использовать адреса электронной почты, отображаемые имена или имя домена для поиска элементов, отправленных или полученных от всех пользователей домена. Например, чтобы найти адрес электронной почты отправителя или получателя в Contoso, Ltd, укажите **@contoso.com** в поле **От** или **Кому/ Скрытая копия** в EAC. Можно также указать **@contoso.com** в *параметрах Senders* или *Recipients* в командной консоли Exchange.

- **Типы сообщений** . По умолчанию выполняется поиск всех типов сообщений. Вы можете ограничить поиск, выбрав определенные типы сообщений, такие как электронная почта, контакты, документы, журнал, встречи, заметки и содержимое Lync.

На следующем снимке экрана показан пример поискового запроса в EAC.



При использовании обнаружения электронных данных на месте также необходимо учесть следующие факторы.

- **Вложения** — In-Place обнаружение электронных данных выполняет поиск вложений, поддерживаемых поиском Exchange. Дополнительные сведения см. в разделе Default Filters for Exchange Search. В локальных развертываниях вы можете добавить поддержку дополнительных форматов файлов, установив для необходимых типов файлов фильтры поиска (известные как iFilter) на серверах почтовых ящиков.

- **Неисхожимые элементы** — это элементы почтового ящика, которые не могут быть проиндексированы поиском Exchange. Причины, по которым они не могут быть проиндексированы, включают отсутствие установленного фильтра поиска для присоединенного файла, ошибку фильтра и зашифрованные сообщения. Для успешного поиска eDiscovery вашей организации может потребоваться включить такие элементы для проверки. При копировании результатов поиска в почтовый ящик обнаружения или их экспорте в PST-файл можно включать элементы, не доступные для поиска. Дополнительные сведения см. в разделе Unsearchable Items in Exchange eDiscovery.

- **Зашифрованные элементы** . Так как сообщения, зашифрованные с помощью S/MIME, не индексируются поиском Exchange, In-Place обнаружение электронных данных не выполняет поиск этих сообщений. Если выбран параметр включения в результаты поиска элементов, поиск в которых невозможен, сообщения с шифрованием S/MIME копируются в почтовый ящик найденных сообщений.

- **Отмена дублирования** . При копировании результатов поиска в почтовый ящик обнаружения или экспорте результатов поиска в PST-файл можно включить *отключение дублирования* результатов поиска, чтобы скопировать в почтовый ящик обнаружения только один экземпляр уникального сообщения. Дедупликация имеет следующие преимущества.

  - Более низкие требования к хранилищу и меньший размер почтового ящика обнаружения благодаря уменьшению количества копируемых сообщений.

  - Сокращение нагрузки на менеджеров по обнаружению, юрисконсультов и других лиц, занятых в проверке результатов поиска.

  - Сокращение расходов на электронное обнаружение в зависимости от количества повторяющихся элементов, исключенных из результатов поиска.

- **Элементы, защищенные IRM** . Сообщения, защищенные с помощью управления правами на доступ к данным (IRM), индексируются поиском Exchange и поэтому включаются в результаты поиска, если они соответствуют параметрам запроса. Сообщения должны быть защищены с помощью кластера служб Active Directory Rights Management Services (AD RMS) в том же лесу Active Directory, что и сервер почтовых ящиков. Дополнительные сведения см. в разделе Управление правами на доступ к данным в Exchange Server.

  Важно!

- Если службе поиска Exchange не удалось проиндексировать сообщение с защитой IRM по причине ошибки расшифровки или отключенной службы IRM, защищенное сообщение не добавляется в список элементов с ошибками. Если вы выбрали параметр для включения в результаты поиска элементов, поиск в которых невозможен, результаты поиска могут не содержать защищенные сообщения, расшифровать которые не удалось.

- Чтобы включить сообщения с защитой IRM в поиск, можно создать другой поиск, результаты которого будут содержать сообщения с вложениями в формате RPMSG. Строку `attachment:rpmsg` запроса можно использовать для поиска всех защищенных IRM сообщений в указанных почтовых ящиках независимо от того, успешно ли индексирован. Это может привести к дублированию некоторых результатов поиска в случаях, когда один поиск возвращает сообщения, соответствующие заданным критериям, включая сообщения с защитой IRM с успешно выполненной индексацией. При этом сообщения с защитой IRM, которые не удалось индексировать, не возвращаются.

- Результаты второго поиска всех сообщений с защитой IRM также содержат защищенные сообщения, успешно индексированные и возвращенные при первом поиске. Кроме того, сообщения с защитой IRM, возвращенные в результатах второго поиска, могут не соответствовать критериям поиска, например ключевым словам, заданным для первого поиска.

Оценка, предварительный просмотр и копирование результатов поиска

После завершения поиска In-Place eDiscovery можно просмотреть оценки результатов поиска в области Сведения в EAC. Оценка включает количество возвращаемых элементов и общий размер этих элементов. Вы также можете просмотреть статистику ключевых слов, которая возвращает сведения о количестве элементов, возвращаемых для каждого ключевого слова, используемого в поисковом запросе. Эти сведения полезны для определения эффективности запросов. Если запрос слишком широкий, он может вернуть гораздо больший набор данных, что может потребовать дополнительных ресурсов для проверки и повышения затрат на обнаружение электронных данных. Если запрос слишком узок, он может значительно уменьшить количество возвращаемых записей или вообще не возвращать записей. Оценки и статистика ключевых слов можно использовать для точной настройки запроса в соответствии с вашими требованиями.

> ⓘ **Примечание**
>
> В Exchange Server статистика ключевых слов также включает статистику свойств, не относящихся к ключевым словам, таких как даты, типы сообщений, а также отправителей и получателей, указанных в поисковом запросе.

Вы можете просмотреть результаты поиска, чтобы убедиться, что возвращенные сообщения содержат искомое содержимое, и при необходимости выполнить точную настройку запроса. При предварительном просмотре поиска методом обнаружения электронных данных отображается количество сообщений, возвращенных из каждого почтового ящика, поиск в котором осуществлялся, и общее количество сообщений, возвращенных поиском. Предварительный просмотр создается быстро, при этом вам не нужно копировать сообщения в почтовый ящик найденных сообщений.

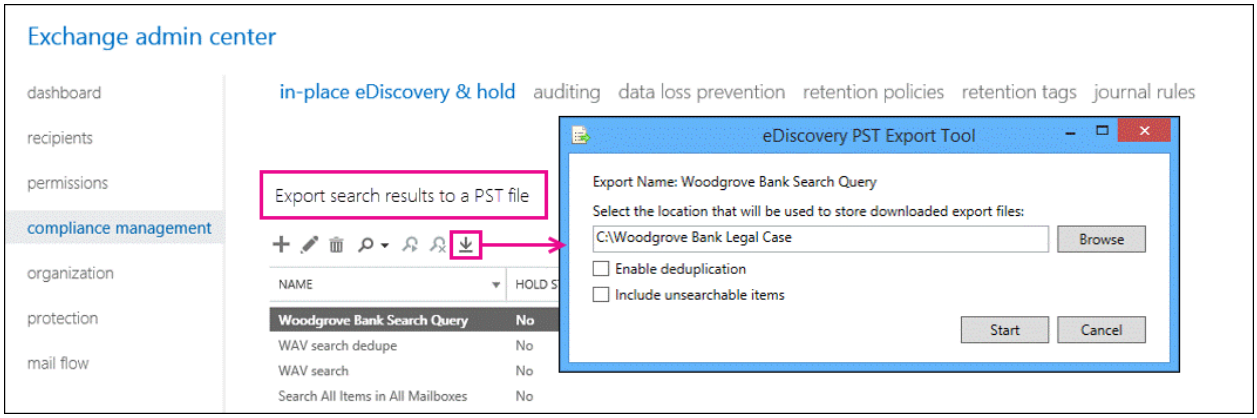
Если количество и качество результатов поиска вас удовлетворяет, их можно скопировать в почтовый ящик найденных сообщений. При копировании сообщений можно воспользоваться следующими параметрами.

- **Включить неискируемые элементы** . Дополнительные сведения о типах элементов, которые считаются недоступными для поиска, см. в разделе Рекомендации по поиску eDiscovery в предыдущем разделе.
- **Включение дедупликации** . Удаление дублирования сокращает набор данных, включив только один экземпляр уникальной записи, если в одном или нескольких почтовых ящиках найдено несколько экземпляров.
- **Включить полное ведение журнала** . По умолчанию при копировании элементов включено только базовое ведение журнала. Можно выбрать функцию полного ведения журнала, чтобы регистрировать сведения обо всех записях, возвращенных в поиске.
- **Отправка сообщения электронной почты по завершении копирования** . Поиск In-Place eDiscovery может возвращать большое количество записей. Копирование сообщений, возвращенных в почтовый ящик найденных сообщений, может занять много времени. Используйте этот параметр для получения почтового уведомления о завершении процесса копирования. Чтобы упростить доступ с помощью Outlook в Интернете, уведомление содержит ссылку на расположение в почтовом ящике обнаружения, куда копируются сообщения.

Дополнительные сведения см. в разделе Копирование результатов поиска с обнаружением электронных данных в почтовый ящик обнаружения.

Экспорт результатов поиска в PST-файл

После копирования результатов поиска в почтовый ящик найденных сообщений результаты поиска можно экспортировать в PST-файл.



После экспорта результатов поиска в PST-файл вы или другие пользователи можете открыть их в Outlook для просмотра или печати сообщений, представленных в результатах поиска. Дополнительные сведения см. в статье Экспорт результатов поиска eDiscovery в PST-файл.

Ведение журнала операций поиска при обнаружении электронных данных на месте

Существует два типа ведения журнала для поиска In-Place обнаружения электронных данных.

- **Базовое ведение журнала** . Базовое ведение журнала включено по умолчанию для всех In-Place поиска по обнаружению электронных данных. В нем регистрируются сведения о поиске и выполнившем его пользователе. Сведения, собираемые при обычном ведении журнала, включаются в текст сообщения электронной почты, которое отправляется в почтовый ящик, где хранятся результаты поиска. Это сообщение находится в папке, созданной для хранения результатов поиска.

- **Полное ведение журнала** . Полное ведение журнала включает сведения обо всех сообщениях, возвращаемых поиском. Эти сведения содержатся в CSV-файле, который вкладывается в сообщение электронной почты, содержащее сведения обычного ведения журнала. Для имени CSV-файла используется имя поиска. Эти сведения могут потребоваться для делопроизводства или

обеспечения соответствия требованиям. Чтобы включить полное ведение журнала, при копировании результатов поиска в почтовый ящик найденных сообщений в Центре администрирования Exchange выберите параметр **Включить полное ведение журнала**. Если вы используете командную консоль Exchange, укажите параметр полного ведения журнала с помощью параметра *LogLevel* .

> **Примечание**
>
> При использовании командной консоли Exchange для создания или изменения поиска In-Place обнаружения электронных данных можно также отключить ведение журнала.

Помимо журнала поиска, который включается при копировании результатов поиска в почтовый ящик обнаружения, Exchange также регистрирует командлеты, используемые EAC или командной консолью Exchange для создания, изменения или удаления In-Place поиска eDiscovery. Эта информация регистрируется в записях журнала аудита администратора. Дополнительные сведения см. в разделе Ведение журнала аудита администратора в Exchange Server.

Почтовые ящики обнаружения

После создания запроса на обнаружение электронных данных на месте результаты поиска можно скопировать в целевой почтовый ящик. Центр администрирования Exchange позволяет выбрать почтовый ящик найденных сообщений в качестве целевого. Почтовый ящик найденных сообщений — это специальный почтовый ящик, который предоставляет приведенные ниже возможности.

- **Более простой и безопасный выбор целевого почтового ящика** . Если вы используете EAC для копирования In-Place результатов поиска по обнаружению электронных данных, только почтовые ящики обнаружения становятся доступными в виде репозитория, в котором будут храниться результаты поиска. Это устраняет возможность случайного выбора диспетчером обнаружения почтового ящика другого пользователя или незащищенного почтового ящика, в котором будут храниться потенциально конфиденциальные сообщения.

- **Квота хранилища больших почтовых ящиков** . Целевой почтовый ящик должен иметь возможность хранить большой объем данных сообщений, которые могут быть возвращены In-Place поиска eDiscovery. По умолчанию

для почтовых ящиков обнаружения квота хранилища почтовых ящиков составляет 50 ГБ. Эту квоту увеличить нельзя.

- **Более безопасная по умолчанию** — как и все типы почтовых ящиков, почтовый ящик обнаружения имеет связанную учетную запись пользователя Active Directory. Однако по умолчанию эта учетная запись отключена. К почтовому ящику найденных сообщений имеют доступ только явно авторизованные пользователи. Участники группы ролей управления обнаружением имеют права на полный доступ к почтовому ящику найденных сообщений по умолчанию. Однако разрешения на доступ к дополнительным почтовым ящикам найденных сообщений не назначаются ни для каких пользователей.

- **Email доставка отключена** — пользователи не могут отправлять сообщения электронной почты в почтовый ящик обнаружения. Доставка электронной почты в почтовые ящики найденных сообщений запрещена с помощью ограничений доставки. Это сохраняет целостность результатов поиска, скопированных в почтовый ящик найденных сообщений. По умолчанию почтовые ящики обнаружения не отображаются в глобальном списке адресов вашей организации.

Exchange Server программа установки создает один почтовый ящик обнаружения с отображаемым именем **Почтовый ящик поиска обнаружения**. Вы можете использовать командную консоль Exchange для создания дополнительных почтовых ящиков обнаружения. По умолчанию создаваемые почтовые ящики найденных сообщений не имеют назначенных прав доступа к почтовым ящикам. Для доступа к сообщениям, скопированным в почтовый ящик найденных сообщений, менеджеру по обнаружению можно назначить права полного доступа Дополнительные сведения см. Дополнительные сведения см. в разделе Создание почтового ящика обнаружения .

Функция обнаружения электронных данных на месте также использует системные почтовые ящики с отображаемым именем **SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}** для хранения метаданных обнаружения электронных данных на месте. Системные почтовые ящики не отображаются в EAC или в списках адресов Exchange. Перед удалением базы данных почтовых ящиков, в которой находится In-Place системный почтовый ящик обнаружения электронных данных, необходимо переместить почтовый ящик в другую базу данных почтовых ящиков. Если почтовый ящик удален или поврежден, менеджеры по обнаружению не смогут выполнять поиски методом обнаружения электронных данных до тех пор, пока почтовый ящик не будет создан повторно. Дополнительные сведения см. в разделе Re-Create the Discovery System Mailbox.

Электронное обнаружение на месте и хранение на месте

При выполнении запросов на обнаружение электронных данных вам может потребоваться сохранять содержимое почтовых ящиков до завершения судебного процесса или расследования. Сообщения, удаленные или измененные пользователем почтового ящика или любыми процессами, также должны быть сохранены. В Exchange Server это достигается с помощью In-Place удержания. Дополнительные сведения см. в разделе Удержание на месте и удержание для судебного разбирательства в Exchange Server.

Мастер **удержания & электронных данных на месте** можно использовать для поиска элементов и их сохранения до тех пор, пока они необходимы для обнаружения электронных данных или для удовлетворения других бизнес-требований. When using the same search for both In-Place eDiscovery and In-Place Hold, be aware of the following:

- Вы не можете использовать параметр для удержания всех почтовых ящиков в вашей организации. Необходимо выбрать почтовые ящики или группы рассылки. Однако вы можете отложить все общедоступные fol ders в организации.
- Если поиск методом обнаружения электронных данных на месте также используется для хранения на месте, удалить этот поиск нельзя. Сначала необходимо отключить параметр хранения на месте, а затем удалить поиск.

Хранение почтовых ящиков для обнаружения электронных данных на месте

Когда сотрудник покидает организацию, обычно отключает или удаляет почтовый ящик. После отключения почтового ящика он отключается от учетной записи пользователя, но остается в почтовом ящике в течение определенного периода времени(по умолчанию 30 дней). Помощник по управляемым папкам не обрабатывает отключенные почтовые ящики, и политики хранения не применяются в течение этого периода. Вы не можете искать содержимое отключенного почтового ящика. По достижении срока хранения удаленного почтового ящика, настроенного для базы данных почтовых ящиков, почтовый ящик очищается из базы данных почтовых ящиков.

Если ваша организация требует, чтобы параметры хранения применялись к сообщениям сотрудников, которые больше не входят в организацию, или если вам

может потребоваться сохранить почтовый ящик бывшего сотрудника для текущего или будущего поиска eDiscovery, не отключайте и не удаляйте почтовый ящик. Чтобы убедиться в отсутствии доступа к почтовому ящику и доставки в него новых сообщений, выполните следующие действия.

1. Disable the Active Directory user account using **Active Directory Users & Computers** or other Active Directory or account provisioning tools or scripts. This prevents mailbox logon using the associated user account.

   > ⓘ **Важно!**
   >
   > Пользователи с разрешением полного доступа к почтовым ящикам по-прежнему могут обращаться к почтовому ящику. Чтобы предотвратить доступ других пользователей, необходимо удалить их разрешение полного доступа из почтового ящика. Сведения об удалении разрешений на полный доступ к почтовому ящику см. в разделе **Управление разрешениями для получателей**.

2. Задайте для максимального размера сообщений, которые могут отправляться пользователем почтового ящика или доставляться ему, очень низкое значение, например 1 КБ. Это предотвратит доставку новой почты в почтовый ящик и отправку почты из него. Дополнительные сведения см. в разделе Настройка ограничений на размер сообщений для почтового ящика.

3. Настройте ограничения на доставку для почтового ящика так, чтобы никто не мог отправлять в него сообщения. Дополнительные сведения см. в разделе Настройка ограничений доставки сообщений для почтового ящика.

> ⓘ **Важно!**
>
> Описанные действия необходимо выполнить вместе с другими процессами управления учетными записями, требуемыми для организации, но без отключения или удаления почтового ящика или удаления связанной учетной записи пользователя.

При планировании внедрения системы хранения почтовых ящиков для управления хранением сообщений (MRM) или электронного управления на месте необходимо принять во внимание текучесть кадров. Длительное хранение почтовых ящиков бывших сотрудников потребует дополнительного пространства для хранения на серверах почтовых ящиков и может привести к увеличению размера базы данных Active Directory, поскольку связанные учетные записи пользователей должны

храниться в течение того же периода. Кроме того, могут потребоваться изменения в процессах подготовки учетных записей и управления ими в организации.

Различные результаты поиска

Так как In-Place eDiscovery выполняет поиск по динамическим данным, возможно, два поиска из одного источника контента, которые используют один и тот же поисковый запрос, могут возвращать разные результаты. Ожидаемые результаты поиска также могут отличаться от фактических результатов, скопированных в почтовый ящик найденных сообщений. Это может произойти, даже если запустить один и тот же поиск в течение короткого промежутка времени. Существует несколько факторов, которые могут повлиять на согласованность результатов поиска.

- непрерывная индексация электронной почты в связи с тем, что функция поиска Exchange непрерывно обходит и индексирует базы данных почтовых ящиков вашей организации и контейнер транспорта;
- удаление сообщений электронной почты пользователями или автоматизированными процессами;
- массовый импорт большого количества электронной почты, индексирование которого занимает определенное время.

Если вы замечаете, что один и тот же поиск дает различные результаты, вы можете поставить почтовые ящики на хранение, чтобы сохранить содержимое, использовать поиск в периоды низкой загрузки и после импорта большого количества электронной почты ожидать определенное время, пока завершится индексирование.

Настраиваемые области управления для обнаружения электронных данных на месте

Пользовательская область управления позволяет определенным пользователям или группам использовать In-Place eDiscovery для поиска подмножества почтовых ящиков в Exchange Server организации. Например, вам может потребоваться разрешить менеджеру по обнаружению выполнять поиск только в почтовых ящиках пользователей, относящихся к определенному расположению или отделу. Для этого следует создать настраиваемую область управления, которая использует фильтр получателей для управления тем, в каких почтовых ящиках можно выполнять поиск. Области фильтра получателей используют фильтры для

выделения определенных получателей на основе типа или других свойств получателя.

Для обнаружения электронных данных на месте создать фильтр подключения настраиваемой области можно только с помощью членства в группе рассылки. Если вы используете другие свойства, такие как *CustomAttributeN*, *Department* или *PostalCode*, поиск завершается ошибкой, когда он выполняется членом группы ролей, которому назначена настраиваемая область. Подробнее см. в разделе Create a custom management scope for In-Place eDiscovery searches.

In-Place обнаружение электронных данных и поиск Exchange

В электронном обнаружении на месте используются индексы содержимого, созданные службой поиска Exchange. Служба поиска Exchange была модернизирована и теперь использует Microsoft Search Foundation, мощную платформу с более высокой производительностью индексации и запросов, а также улучшенным поиском. Так как Microsoft Search Foundation также используется другими продуктами Office, включая SharePoint Server, она обеспечивает более высокую совместимость и аналогичный синтаксис запросов в этих продуктах.

Благодаря единому механизму индексации содержимого для функции обнаружения электронных данных на месте не требуются дополнительные ресурсы для сканирования и индексации баз данных почтовых ящиков при получении ИТ-отделом запросов на электронное обнаружение.

Дополнительные сведения о форматах файлов, индексированных поиском Exchange, см. в разделе Форматы файлов, индексированные поиском Exchange.

Обнаружение электронных данных при гибридном развертывании Exchange

В гибридном развертывании, которое представляет собой среду, в которой некоторые почтовые ящики существуют на локальных серверах почтовых ящиков, а некоторые — в облачной организации, можно выполнять поиск In-Place обнаружения электронных данных в облачных почтовых ящиках с помощью EAC в локальной организации. Если вы планируете копировать сообщения в почтовый ящик обнаружения, необходимо выбрать локальный почтовый ящик обнаружения. В него будут копироваться сообщения из облачных почтовых ящиков,

возвращаемые в результатах поиска. Дополнительные сведения о гибридных развертываниях см. в разделе Exchange Server гибридных развертываний.

Чтобы успешно выполнять поиск по обнаружению электронных данных в Exchange Server гибридной организации, необходимо настроить проверку подлинности OAuth (открытая авторизация) между локальной средой Exchange и Exchange Online организациями, чтобы можно было использовать In-Place eDiscovery для поиска в локальных и облачных почтовых ящиках. Проверка подлинности OAuth — это протокол межсерверной проверки подлинности, который позволяет приложениям проверять подлинность друг друга.

Проверка подлинности OAuth поддерживает приведенные ниже сценарии обнаружения электронных данных при гибридном развертывании Exchange.

- Поиск локальных почтовых ящиков, использующих архивацию на базе Exchange Online для облачных архивных почтовых ящиков.
- Поиск в локальных и облачных почтовых ящиках в рамках одного сеанса обнаружения электронных данных.

Дополнительные сведения о сценариях обнаружения электронных данных, для которых требуется настроить проверку подлинности OAuth при гибридном развертывании Exchange, см. в разделе Using Oauth Authentication to Support eDiscovery in an Exchange Hybrid Deployment. Пошаговые инструкции по настройке проверки подлинности OAuth для поддержки обнаружения электронных данных см. в разделе Настройка проверки подлинности OAuth между Exchange и Exchange Online организациями.

Пошаговые инструкции по настройке проверки подлинности OAuth для поддержки обнаружения электронных данных см. в разделе Настройка проверки подлинности OAuth между Exchange и Exchange Online организациями.

Интеграция с SharePoint Server

Exchange Server предлагает интеграцию с SharePoint Server, позволяя диспетчеру обнаружения использовать Центр обнаружения электронных данных в SharePoint Server для выполнения следующих задач:

- **Поиск и сохранение содержимого из одного расположения** . Авторизованный диспетчер обнаружения может выполнять поиск и сохранение содержимого в SharePoint и Exchange, включая содержимое Lync, например беседы с мгновенными сообщениями и документы общих собраний, архивированные в почтовых ящиках Exchange.

- **Управление случаями** . Центр обнаружения электронных данных использует подход к управлению случаями для обнаружения электронных данных, позволяющий создавать случаи, а также искать и сохранять содержимое в разных репозиториях содержимого для каждого случая.

- **Экспорт результатов поиска** . Диспетчер обнаружения может использовать Центр обнаружения электронных данных для экспорта результатов поиска. Содержимое почтового ящика, включенное в результаты поиска, экспортируется в PST-файл.

SharePoint Server также использует Microsoft Search Foundation для индексирования содержимого и выполнения запросов. Независимо от того, использует ли менеджер по обнаружению EAC или центр обнаружения электронных данных для поиска содержимого Exchange, возвращается одно и то же содержимое почтового ящика.

Прежде чем использовать Центр обнаружения электронных данных в SharePoint Server для поиска почтовых ящиков Exchange, необходимо установить доверие между двумя приложениями. В Exchange и SharePoint для этого используется проверка подлинности OAuth. Сведения см. в разделе Configure Exchange for SharePoint eDiscovery Center. Поиск по обнаружению электронных данных, выполняемый из SharePoint, авторизован Exchange с помощью RBAC. Чтобы пользователь SharePoint мог выполнять поиск в почтовых ящиках Exchange для обнаружения электронных данных, ему должно быть назначено делегированное разрешение на управление обнаружением в Exchange. Чтобы иметь возможность предварительного просмотра содержимого почтового ящика, возвращаемого при поиске eDiscovery, выполненном с помощью SharePoint eDiscovery Center, у диспетчера обнаружения должен быть почтовый ящик в той же организации Exchange.

Ограничения и политики регулирования обнаружения электронных данных на месте

В Exchange Server ресурсы, In-Place использует обнаружение электронных данных, управляются политиками регулирования.

Политика регулирования по умолчанию содержит следующие параметры. Вы можете изменить значения по умолчанию в соответствии с требованиями организации, создав новую политику регулирования с областью организации и присвойте ей имя DiscoveryThrottlingPolicy.

Параметр	Описание	Значение по умолчанию
DiscoveryMaxConcurrency	Максимальное количество In-Place поиска электронных данных, которые пользователь может выполнять одновременно.	2
DiscoveryMaxMailboxes	Максимальное количество почтовых ящиков, в которых может быть выполнен поиск в ходе одного процесса обнаружения электронных данных на месте. Почтовые ящики общедоступных папок учитываются при подсчете максимального количества исходных почтовых ящиков.	10 000[1]
DiscoveryMaxStatsSearchMailboxes	Максимальное количество почтовых ящиков, в которых может быть выполнен поиск в ходе одного процесса обнаружения электронных данных на месте и просмотрена статистика ключевых слов.	100 **Примечание**. После выполнения оценки поиска обнаружения электронных данных можно просмотреть статистику по ключевым словам. Она содержит сведения о количестве элементов, возвращаемых для каждого ключевого слова в поисковом запросе. Если в поиск включено более 100 исходных почтовых ящиков, при попытке просмотра статистики ключевых слов будет возвращена ошибка.

Параметр	Описание	Значение по умолчанию
DiscoveryMaxKeywords	Максимальное количество ключевых слов, которое можно указать в одном процессе обнаружения электронных данных на месте.	500
DiscoveryPreviewSearchResultsPageSize	Максимальное количество элементов, отображаемых на одной странице в режиме предварительного просмотра результатов поиска методом обнаружения электронных данных на месте.	200
DiscoverySearchTimeoutPeriod	Количество минут, в течение которых будет выполняться поиск методом обнаружения электронных данных на месте до истечения времени ожидания.	10 минут

[1] Архивные почтовые ящики учитываются в пределах исходного почтового ящика. Это означает, что вы можете выполнить поиск не более 5000 почтовых ящиков, если соответствующий архивный почтовый ящик включен для всех 5000 почтовых ящиков.

Документация обнаружения электронных данных на месте

В следующей таблице содержатся ссылки на Exchange Server разделы, которые помогут вам узнать о In-Place eDiscovery и управлять ими.

Статья	Описание
Назначение разрешений на обнаружение электронных данных в Exchange Server	Узнайте, как предоставить пользователю доступ к использованию In-Place обнаружения электронных данных в EAC (и с помощью соответствующих командлетов) для поиска почтовых ящиков Exchange.
Создание In-Place поиска eDiscovery в Exchange Server	Узнайте, как создать поиск обнаружения электронных данных на месте, а также как оценивать и просматривать результаты обнаружения электронных данных на месте.
Копирование результатов поиска с обнаружением электронных данных в почтовый ящик обнаружения	Узнайте, как скопировать результаты поиска обнаружения электронных данных на месте в почтовый ящик обнаружения.
Экспорт результатов поиска при обнаружении электронных данных в PST-файл	Узнайте, как экспортировать результаты поиска обнаружения электронных данных на месте в PST-файл.
Свойства сообщений и операторы поиска для In-Place обнаружения электронных данных в Exchange Server	Узнайте, как свойства сообщений электронной почты можно искать с помощью обнаружения электронных данных на месте. В этом разделе представлены примеры синтаксиса для каждого свойства, сведения об операторах поиска, таких как **AND** и **OR**, и информация о других методах выполнения поисковых запросов, например использовании двойных кавычек (" ") и знаков подстановки в конце слова.
Поиск в общедоступных папках и их удержание с помощью обнаружения электронных данных на месте	Узнайте, как использовать In-Place eDiscovery для поиска и удержания всех общедоступных папок в организации.

Назначение разрешений на обнаружение электронных данных в Exchange Server

Статья • 04.04.2023

Если вы хотите, чтобы пользователи могли использовать Exchange Server In-Place обнаружения электронных данных, сначала необходимо добавить их в группу ролей Управление обнаружением. Члены группы ролей Управление обнаружением имеют полный доступ к почтовому ящику найденных сообщений по умолчанию, который называется **Почтовый ящик поиска методом обнаружения**.

> ⊗ **Внимание!**
>
> Члены группы ролей Управление обнаружением имеют доступ к конфиденциальному содержимому сообщений. В частности, они могут использовать обнаружение электронных данных на месте для поиска во всех почтовых ящиках организации Exchange, просматривать результаты поиска (и другие элементы почтового ящика), копировать их в почтовый ящик найденных сообщений и экспортировать в PST-файл. В большинстве организаций это разрешение предоставляется юристам, ответственным за обеспечение соответствия требованиям или специалистам отдела кадров.

Что нужно знать перед началом работы

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Группы ролей" в разделе Разрешения для управления ролями .
- По умолчанию в группе ролей Управление обнаружением нет членов. Поэтому администраторы с ролью Управление организацией не могут создавать поисковые запросы на обнаружение и управлять ими, если они не добавлены в группу ролей Управление обнаружением.
- В Exchange Server члены группы ролей "Управление организацией" могут создать In-Place удержание, чтобы поместить все содержимое почтового ящика на удержание. Однако чтобы создать запрет на удаление на основе

запроса, пользователь должен быть членом группы ролей Управление обнаружением или иметь роль "Поиск в почтовых ящиках".

- В группу ролей "Управление обнаружением" можно добавлять только *субъекты безопасности* (пользователей или группы, которым можно назначить разрешения). Например:
  - почтовые ящики пользователей;
  - пользователи почты;
  - Группы безопасности.
  - Другие группы ролей.
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

Добавление пользователя в группу ролей Управление обнаружением с помощью Центра администрирования Exchange

1. В EAC перейдите в **раздел Разрешения**>**Администратор роли**, выберите группу ролей **Управление обнаружением** и нажмите кнопку **Изменить**.✏️
2. На результирующей странице **Группа ролей** в разделе **Члены** щелкните **Добавить**➕
3. В появившемся диалоговом окне **Выбор членов** выберите доступного пользователя или группу и нажмите кнопку **Добавить**. Повторите этот шаг нужное количество раз. После этого нажмите кнопку **OK**.
4. На странице **Группа ролей** нажмите кнопку **Сохранить**.

Добавление пользователя в группу ролей Управление обнаружением с помощью Командная консоль Exchange

Чтобы добавить пользователя в группу ролей Управление обнаружением, используйте следующий синтаксис:

```
PowerShell
```

```
Add-RoleGroupMember -Identity "Discovery Management" -Member <Identity>
```

В этом примере в группу ролей Управление обнаружением добавляется пользователь Bsuneja.

PowerShell

```
Add-RoleGroupMember -Identity "Discovery Management" -Member Bsuneja
```

В этом примере добавляются члены в группу безопасности, поддерживающую почту, Contoso Compliance Management.

PowerShell

```
Add-RoleGroupMember -Identity "Discovery Management" -Member "Contoso
Compliance Management"
```

Дополнительные сведения см. в статье Add-RoleGroupMember.

Как проверить, все ли получилось?

Чтобы убедиться, что вы добавили пользователя в группу ролей Управление обнаружением, выполните одно из указанных ниже действий:

- В EAC перейдите в **раздел Разрешения**>**Администратор роли** и выберите группу ролей **Управление обнаружением**. Убедитесь, что пользователь указан в области сведений, в разделе **Члены**.
- В Командная консоль Exchange выполните следующую команду, чтобы просмотреть членов группы ролей Управление обнаружением.

  PowerShell

  ```
  Get-RoleGroupMember -Identity "Discovery Management"
  ```

Создание In-Place поиска eDiscovery в Exchange Server

Статья • 04.04.2023

Используйте In-Place поиск электронных данных для поиска содержимого во всех почтовых ящиках и общедоступных папках в Exchange Server организации. Дополнительные сведения об этих операциях поиска см. Дополнительные сведения об этих поисках см. в разделе Обнаружение электронных данных на месте в Exchange Server.

Перед началом работы

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Обнаружение электронных данных на месте" в разделе Политика обмена сообщениями и разрешения на соответствие требованиям Exchange Server.

- Для создания поиска eDiscovery необходимо иметь SMTP-адрес в организации, в которую вы создаете поисковые запросы. В гибридной организации Exchange локальный почтовый ящик Exchange должен иметь соответствующую учетную запись почтового пользователя в Microsoft 365 или Office 365 организации, например учетную запись администратора клиента. Этой учетной записи должна быть назначена лицензия Exchange Online. Дополнительные сведения о требованиях к лицензированию Microsoft 365 или Office 365 для поиска обнаружения электронных данных на месте см. в разделе Описание службы Exchange Online.

- Exchange Server программа установки создает почтовый ящик обнаружения с именем **Почтовый ящик поиска обнаружения** для копирования результатов поиска. Вы можете создать дополнительные почтовые ящики обнаружения. Дополнительные сведения см. в статье Создание почтового ящика обнаружения.

- Сообщения, возвращаемые в результатах поиска, не копируются автоматически в почтовый ящик найденных сообщений. После создания поиска вы можете оценить и просмотреть результаты поиска, скопировать их в почтовый ящик найденных сообщений или экспортировать в PST-файл, используя Центр администрирования Exchange (EAC). Дополнительные сведения см. в следующих статьях:

    - Использование Центра администрирования Exchange для оценки или предварительного просмотра результатов поиска (далее в этой статье)
    - Копирование результатов поиска с обнаружением электронных данных в почтовый ящик обнаружения
    - Экспорт результатов поиска при обнаружении электронных данных в PST-файл

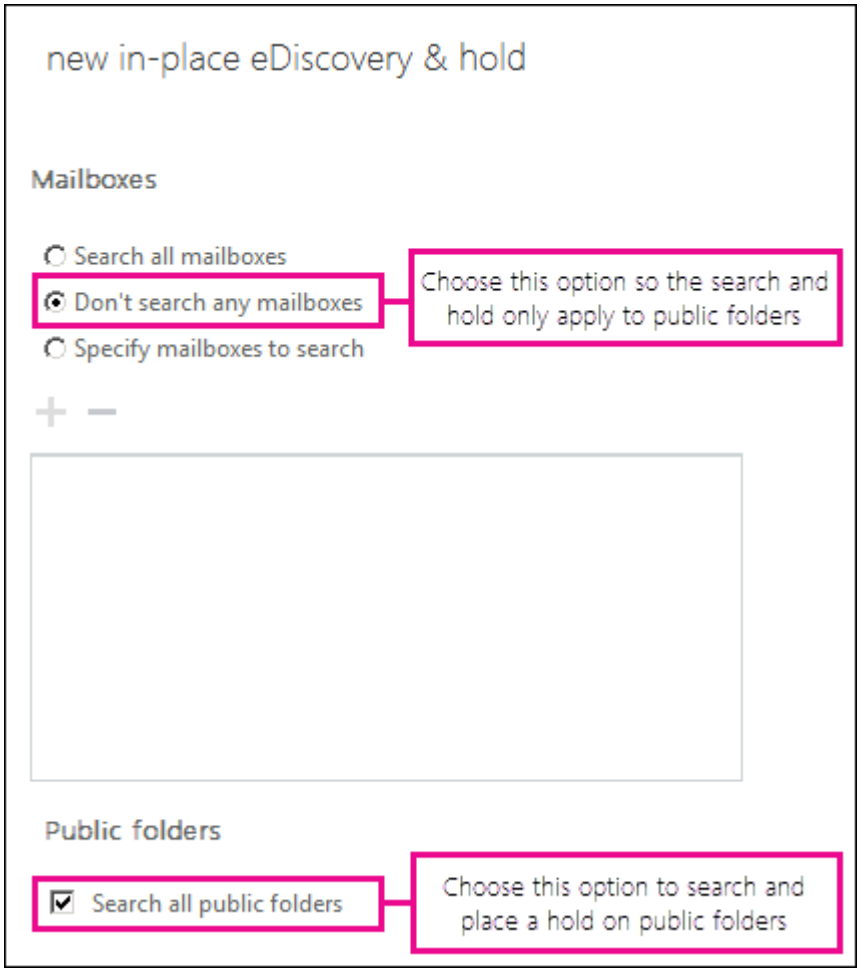
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

Создание поискового запроса с помощью Центра администрирования Exchange

Как объяснялось ранее, для создания поисков eDiscovery необходимо войти в учетную запись пользователя с адресом SMTP в вашей организации.

1. Перейдите в **раздел Управление соответствием**> на**месте eDiscovery Удержание &**и нажмите кнопку **Создать**➕
2. In the **New In-Place eDiscovery & Hold** window, on the **Name and description** page, type a name for the search, add an optional description, and then click **Next**.
3. На странице **Почтовые ящики и общедоступные папки** выберите источники контента для поиска:
    - Чтобы включить все почтовые ящики в поиск, выберите пункт **Поиск во всех почтовых ящиках**. При выборе этого варианта поиск будет выполняться без хранения данных на месте.
    - Чтобы исключить почтовые ящики из поиска и выполнить поиск только в общедоступных папках, нажмите кнопку **Не выполнять поиск в почтовых ящиках**.
    - Чтобы выполнить поиск в определенных почтовых ящиках, выберите пункт **Указать почтовые ящики для поиска**, а затем добавьте нужные почтовые ящики.
    - Чтобы включить общедоступные папки в поиск (или поместить их на хранение), нажмите кнопку **Поиск во всех общедоступных папках**. Дополнительные сведения о поиске общедоступных папок см. в статье

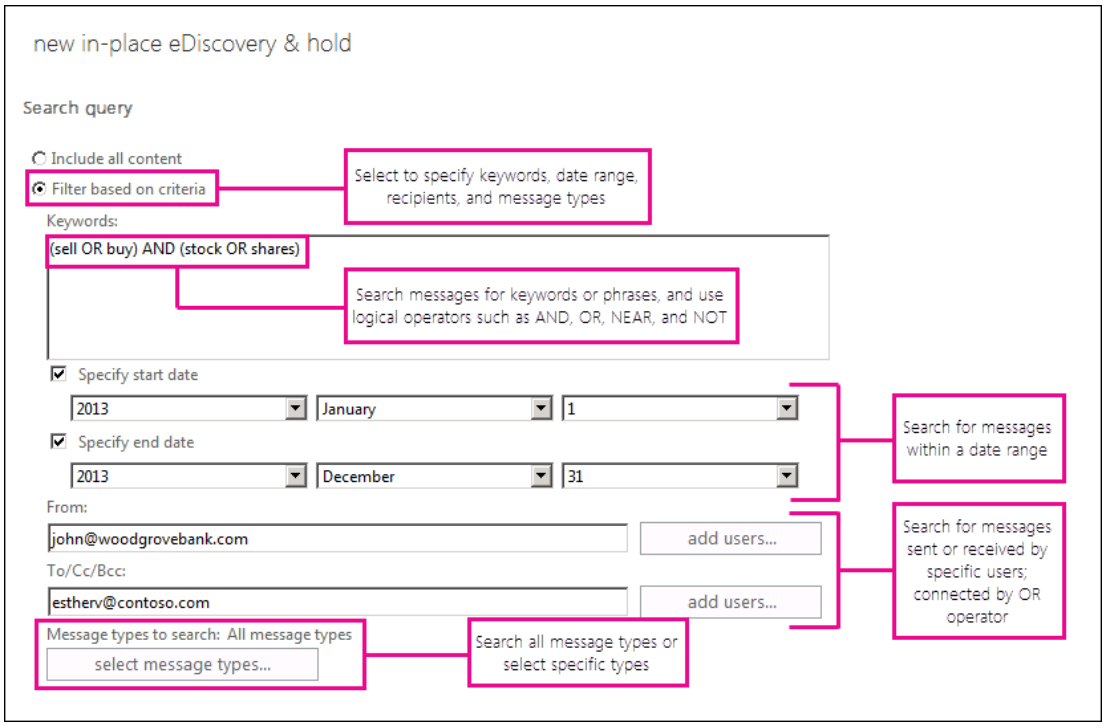
Поиск и удержание общедоступных папок с помощью In-Place обнаружения электронных данных.



4. На странице **Поисковый запрос** заполните следующие поля:

- **Включить все содержимое**. Выберите этот параметр, чтобы включить все содержимое в результаты поиска. Если выбрать этот вариант, указать дополнительные критерии поиска будет невозможно.

- **Фильтр на основе условий**. Выберите этот параметр, чтобы указать критерии поиска, включая ключевые слова, даты начала и окончания, адреса отправителей и получателей, а также типы сообщений. Дополнительные сведения о поисковых запросах см. в разделе Свойства сообщений и операторы поиска для In-Place обнаружения электронных данных в Exchange Server.



> ⓘ **Примечание**
>
> Поля **От:** и **Кому/копия/скрытая копия:** объединены с помощью оператора **ИЛИ** в поисковом запросе, который создается при запуске поиска. Это означает, что в результаты поиска включаются все сообщения, отправленные или полученные указанными пользователями (и соответствующие условиям поиска). Даты объединены с помощью оператора **И**.

5. На странице **Параметры хранения на месте** установите флажок **Поместить содержимое, соответствующее поисковому запросу в выбранных источниках, на удержание**, а затем выберите один из следующих вариантов хранения элементов на месте:

   - **Удержание на неопределенный срок**. Выберите этот параметр, чтобы поместить возвращенные элементы на неопределенное удержание. Такие элементы будут храниться, пока вы не удалите источник контента из поиска или не удалите поиск.

   - **Указать число дней для хранения элементов с даты получения** Используйте этот вариант для хранения элементов в течение указанного времени. Например, эту функцию можно использовать, если для вашей организации необходимо, чтобы все сообщения сохранялись на протяжении не менее семи лет. Можно использовать хранение на месте *на основе времени* вместе с политикой хранения, чтобы убедиться, что через семь лет элементы будут удалены.

> **ⓘ Важно!**
>
> Рекомендуем помещать источники контента или отдельные элементы на бессрочное хранение и отключать хранение после завершения судебного дела или расследования.

6. Нажмите кнопку **Готово**, чтобы сохранить поиск и получить оценку общего размера и количества элементов, которые будут возвращены на основании установленных критериев. Оценки отображаются в области сведений. Нажмите 🔄 чтобы обновить сведения, отображаемые в области сведений.

Создание поиска с помощью Командная консоль Exchange

Ниже приведены четыре примера использования командной консоли Exchange для поиска и удержания содержимого в почтовых ящиках и общедоступных папках. Подробные сведения о синтаксисе и параметрах об использовании командной консоли Exchange для создания поиска eDiscovery см. в статье New-MailboxSearch.

Пример 1

В этом примере создается запрос Discovery-CaseId012 на поиск элементов, содержащих ключевые слова **Contoso** и **ProjectA**. Результаты поиска помещаются на бессрочное хранение на месте. Поисковый запрос также включает следующие критерии:

- Дата начала: 1/1/2013
- Дата окончания: 12/31/2015
- Исходный почтовый ящик: Финансы группы рассылки
- Целевой почтовый ящик: Почтовый ящик поиска методом обнаружения
- Типы сообщений: Электронная почта
- Уровень ведения журнала: Полное

> **ⓘ Важно!**

Если не указать поисковый запрос, диапазон дат или тип сообщения, в результаты будут включены все элементы в исходных почтовых ящиках и общедоступных папках. Результаты будут такими же, как при выборе варианта **Включить все содержимое** на странице **Поисковый запрос** в Центре администрирования Exchange.

PowerShell

```
New-MailboxSearch "Discovery-CaseId012" -StartDate "01/01/2013" -EndDate "12/31/2015" -SourceMailboxes "DG-Finance" -TargetMailbox "Discovery Search Mailbox" -SearchQuery '"Contoso" AND "Project A"' -MessageTypes Email -IncludeUnsearchableItems -LogLevel Full -InPlaceHoldEnabled $true
```

PowerShell

```
Start-MailboxSearch "Discovery-CaseId012"
```

После использования командной консоли Exchange для создания поиска In-Place обнаружения электронных данных необходимо начать поиск с помощью командлета **Start-MailboxSearch** , чтобы скопировать сообщения в почтовый ящик обнаружения, указанный в *параметре TargetMailbox* . Дополнительные сведения см. в статье Copy eDiscovery search results to a discovery mailbox.

Примечание

Если используются параметры *StartDate* и *EndDate*, необходимо указать дату в формате мм/дд/гггг, даже если в настройках локального компьютера используется другой формат, например дд/мм/гггг. Например, чтобы найти сообщения, отправленные в период с 1 апреля 2015 г. по 1 июля 2015 г., укажите дату начала **04/01/2015** и дату окончания **07/01/2015**.

Пример 2

В этом примере создается поиск с обнаружением электронных данных на месте HRCase090116 для сообщений электронной почты, отправленных пользователем Alex Darrow пользователю Sara Davis в 2015 году.

PowerShell

```
New-MailboxSearch "HRCase090116" -StartDate "01/01/2015" -EndDate "12/31/2015" -SourceMailboxes alexd,sarad -SearchQuery 'From:alexd@contoso.com AND To:sarad@contoso.com' -MessageTypes Email -
```

```
TargetMailbox "Discovery Search Mailbox" -IncludeUnsearchableItems -LogLevel
Full
```

PowerShell

```
Start-MailboxSearch "HRCase090116"
```

Пример 3

В этом примере создается оценочный поиск элементов, отправленных между 1 января 2015 г. и 30 июня 2015 г. и содержащих фразу "patent infringement", во всех общедоступных папках в организации. В этот поиск не включаются почтовые ящики. Для запуска оценочного поиска используется командлет **Start-MailboxSearch**.

PowerShell

```
New-MailboxSearch -Name "Northwind Subpoena-All PFs" -AllPublicFolderSources
$true -AllSourceMailboxes $false -SearchQuery "patent infringement" -
StartDate "01/01/2015" -EndDate "06/30/2015" -TargetMailbox "Discovery
Search Mailbox" -EstimateOnly
```

PowerShell

```
Start-MailboxSearch "Northwind Subpoena-All PFs"
```

Пример 4

В этом примере во всех почтовых ящиках и общедоступных папках выполняется поиск содержимого со словами "прайс-лист" и "Contoso", которое было отправлено после 1 января 2015 г. Для запуска поиска и копирования его результатов в почтовый ящик найденных сообщений используется командлет **Start-MailboxSearch**.

PowerShell

```
New-MailboxSearch -Name "Contoso Litigation" -AllSourceMailboxes $true -
AllPublicFolderSources $true -SearchQuery '"price list" AND "contoso"' -
StartDate "01/01/2015" -TargetMailbox "Discovery Search Mailbox"
```

PowerShell

```
Start-MailboxSearch "Contoso Litigation"
```

Использование Центра администрирования Exchange для оценки или предварительного просмотра результатов поиска

Результаты поиска методом обнаружения электронных данных можно оценить и просмотреть в Центре администрирования Exchange. Если поиск создан с помощью командлета **New-MailboxSearch**, вы можете запустить его с помощью Командная консоль Exchange для оценки результатов.

1. Перейдите в раздел **Управление соответствием**> на**месте для обнаружения & электронных данных**.

2. В списке выберите поисковый запрос, а затем выполните одно из следующих действий:

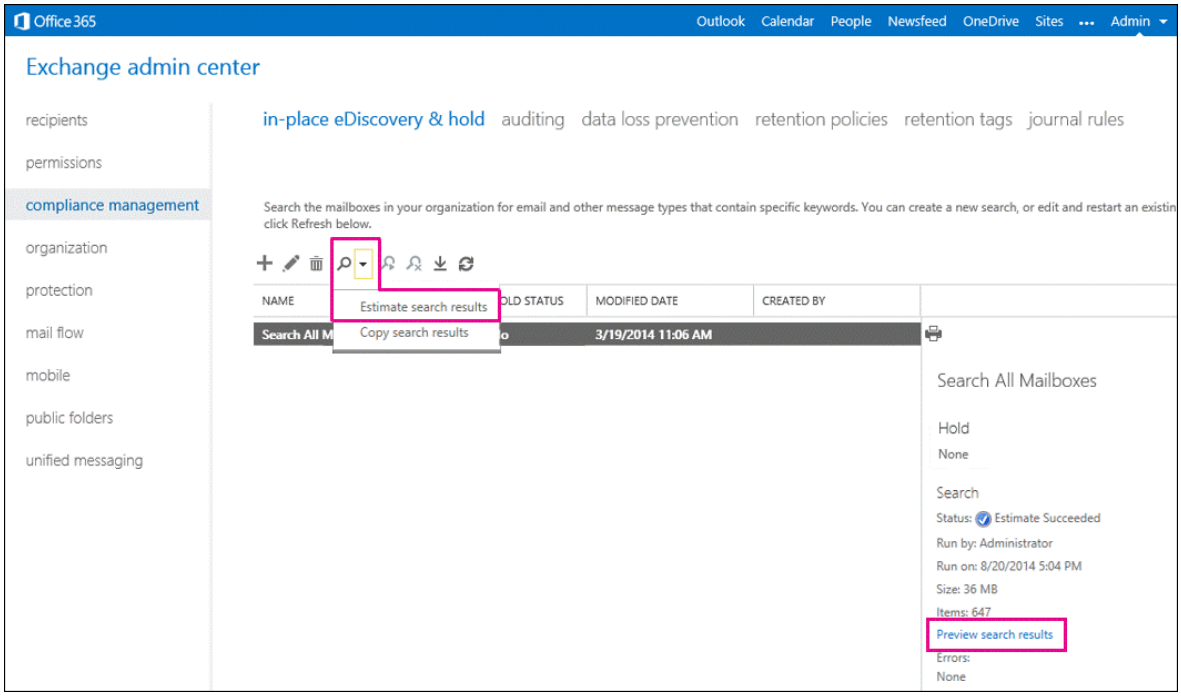
   - Щелкните **Значок Поиска**🔎>**Оцените результаты поиска**, чтобы получить оценку общего размера и количества элементов, которые будут возвращены поиском на основе указанных вами критериев. Этот параметр перезапускает поиск и выполняет оценку.

     Оценка результатов поиска отображается в области сведений. Нажмите 🔄 чтобы обновить сведения, отображаемые в области сведений.

   - Выберите элемент **Предварительный просмотр результатов поиска** в области сведений, чтобы просмотреть результаты после оценки. Если выбрать этот вариант, откроется окно **просмотра результатов поиска методом обнаружение электронных данных**. Отображаются все сообщения, найденные в почтовых ящиках или общедоступных папках, включенных в поиск.

     > ⓘ **Примечание**
     >
     > Почтовые ящики или общедоступные папки, включенные в поиск, отображаются на правой панели окна **просмотра результатов поиска методом обнаружение электронных данных**. Кроме того, отображается количество элементов, найденных в каждом источнике, и их общий размер. Все найденные элементы отображаются на правой панели и могут быть отсортированы по

дате. Элементы из каждого почтового ящика или общедоступной папки невозможно отобразить на правой панели, выбрав источник на левой панели. Чтобы просмотреть элементы из определенного почтового ящика или общедоступной папки, скопируйте результаты поиска и просмотрите их в почтовом ящике найденных сообщений.



Оценка результатов поиска с помощью Командная консоль Exchange

Вы можете использовать параметр *EstimateOnly* , чтобы получить оценку результатов поиска и не копировать результаты в почтовый ящик обнаружения. Необходимо запустить поиск только с оценкой с помощью командлета **Start-MailboxSearch**. Затем можно извлечь оценку результатов поиска, выполнив командлет **Get-MailboxSearch**. Командная консоль Exchange невозможно использовать для предварительного просмотра сообщений, возвращенных в результатах поиска.

Например, чтобы создать новый поиск, а затем отобразить оценку результатов поиска, выполните следующие команды:

PowerShell

```
New-MailboxSearch "FY15 Q2 Financial Results" -StartDate "04/01/2015" -
EndDate "06/30/2015" -SourceMailboxes "DG-Finance" -SearchQuery '"Financial"
AND "Fabrikam"' -EstimateOnly -IncludeKeywordStatistics
```

PowerShell

```
Start-MailboxSearch "FY15 Q2 Financial Results"
```

PowerShell

```
Get-MailboxSearch "FY15 Q2 Financial Results"
```

Чтобы отобразить определенную информацию об оценке результатов поиска с предыдущего примера, выполните следующую команду:

PowerShell

```
Get-MailboxSearch "FY15 Q2 Financial Results" | Format-List
Name,Status,LastRunBy,LastStartTime,LastEndTime,Sources,SearchQuery,ResultSi
zeEstimate,ResultNumberEstimate,Errors,KeywordHits
```

Дополнительные сведения

- После создания нового поиска eDiscovery можно скопировать результаты поиска в почтовый ящик найденных сообщений и экспортировать их в файл PST. Дополнительные сведения:
  - Копирование результатов поиска с обнаружением электронных данных в почтовый ящик обнаружения
  - Экспорт результатов поиска при обнаружении электронных данных в PST-файл
- После запуска оценки результатов поиска для обнаружения электронных данных (включительно со словами в условиях поиска), вы можете просмотреть статистику ключевых слов, щелкнув элемент **Просмотреть статистику ключевых слов** в области сведений для выбранного поиска. Она содержит сведения о количестве элементов, возвращаемых для каждого ключевого слова в поисковом запросе. Но если поиск включает более 100 исходных почтовых ящиков, при попытке просмотреть статистику ключевых слов возвращается ошибка. Для просмотра статистики ключевых слов поиск должен включать не более 100 исходных почтовых ящиков.
- Если вы используете **Get-MailboxSearch** в Exchange Online для получения сведений о поиске eDiscovery, необходимо указать имя поиска, чтобы вернуть полный список свойств поиска, например `Get-MailboxSearch "Contoso Legal`

`Case"`. Если запустить командлет **Get-MailboxSearch** без использования каких-либо параметров, не будут возвращены следующие свойства:

- `SourceMailboxes`
- `Sources`
- `PublicFolderSources`
- `SearchQuery`
- `ResultsLink`
- `PreviewResultsLink`
- `Errors`

  Это связано с тем, что для возврата этих свойств для всех поисковых запросов по обнаружению электронных данных в организации требуется много ресурсов.

Копирование результатов поиска по обнаружению электронных данных в почтовый ящик обнаружения в Exchange Server

Статья • 04.04.2023

После создания In-Place поиска eDiscovery в Exchange Server можно с помощью Центра администрирования Exchange (EAC) скопировать результаты в почтовый ящик обнаружения. Вы также можете использовать командную консоль Exchange для запуска поиска eDiscovery, созданного с помощью командлета **New-MailboxSearch** , который копирует результаты в почтовый ящик обнаружения, указанный при создании поиска.

Что нужно знать перед началом работы

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Обнаружение электронных данных на месте" в разделе Политика обмена сообщениями и разрешения на соответствие требованиям Exchange Server.
- Чтобы скопировать результаты поиска, необходимо создать поиск по обнаружению электронных данных с помощью EAC или командной консоли Exchange. Дополнительные сведения см. в статье Создание In-Place поиска eDiscovery в Exchange Server.
- Exchange Server программа установки создает почтовый ящик обнаружения с именем **Почтовый ящик поиска обнаружения** для копирования результатов поиска. Можно создать дополнительные почтовые ящики обнаружения. в разделе Create a Discovery Mailbox.
- Копирование результатов поиска в почтовый ящик найденных сообщений может занять 5 минут или больше времени, в зависимости от количества элементов почтовых ящиков, возвращенных в результатах.
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

Копирование результатов поиска с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел **Управление соответствием**> на**месте для обнаружения & электронных данных**.

2. В представлении списка выберите поиск при обнаружении электронных данных.

3. Щелкните **Значок поиска**🔎, а затем щелкните **Копировать результаты поиска** из раскрывающегося списка.

4. В окне **Копировать результаты поиска** выберите один из следующих вариантов:

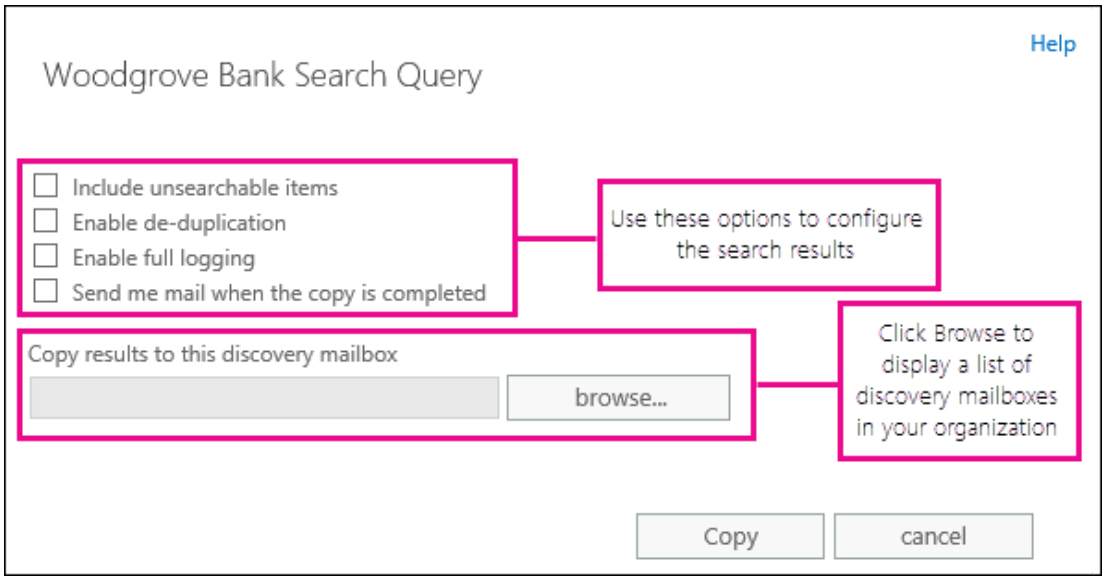
   - **Включить неискируемые элементы**. Установите этот флажок, чтобы включить элементы почтового ящика, которые не удалось найти (например, сообщения с вложениями типов файлов, которые не могут быть проиндексированы поиском Exchange). Дополнительные сведения см. в разделе Unsearchable Items in Exchange eDiscovery.

   - **Включить отмену дублирования**. Установите этот флажок, чтобы исключить повторяющиеся сообщения. В почтовый ящик найденных сообщений будет копироваться только один экземпляр сообщения.

   - **Включить полное ведение журнала**. Установите этот флажок, чтобы включить полный журнал в результаты поиска.

   - **Отправить мне сообщение по завершении копирования**. Установите этот флажок, чтобы получать уведомление по электронной почте о завершении поиска.

   - **Скопируйте результаты в этот почтовый ящик обнаружения**. Нажмите кнопку **Обзор** , чтобы выбрать почтовый ящик обнаружения, в который нужно скопировать результаты поиска.



5. Нажмите кнопку **Копировать**, чтобы начать процесс копирования результатов поиска в указанный почтовый ящик найденных сообщений.

6. Нажмите чтобы обновить сведения о состоянии копирования, которое отображается в области сведений.

7. После завершения копирования нажмите кнопку **Открыть**, чтобы открыть почтовый ящик найденных сообщений для просмотра результатов поиска.

Копирование результатов поиска с помощью Командная консоль Exchange

После использования командлета **New-MailboxSearch** для создания In-Place поиска eDiscovery необходимо начать поиск, чтобы скопировать сообщения в почтовый ящик обнаружения, указанный в *параметре TargetMailbox* . Сведения о создании поиска eDiscovery с помощью командной консоли Exchange см. в следующих разделах:

- Создание In-Place поиска eDiscovery в Exchange Server
- New-MailboxSearch

В следующем примере вы выполните следующую команду, чтобы запустить поиск по обнаружению электронных данных с именем *Fabrikam Investigation* , чтобы скопировать результаты поиска в почтовый ящик обнаружения, заданный параметром *TargetMailbox* при создании поиска.

PowerShell

```
Start-MailboxSearch "Fabrikam Investigation"
```

Если вы использовали параметр *EstimateOnly* для получения оценки результатов поиска, необходимо удалить этот параметр, прежде чем можно будет скопировать результаты поиска. Вам также нужно указать почтовый ящик найденных сообщений для копирования результатов поиска. Например, вы создали оценочный поиск с помощью следующей команды:

PowerShell

```
New-MailboxSearch "FY15 Q2 Financial Results" -StartDate "04/01/2015" -
EndDate "06/30/2015" -SourceMailboxes "DG-Finance" -SearchQuery '"Financial"
AND "Fabrikam"' -EstimateOnly -IncludeUnsearchableItems
```

Чтобы скопировать результаты поиска в почтовый ящик найденных сообщений, вам пришлось бы выполнить такие команды:

PowerShell

```
Set-MailboxSearch "FY15 Q2 Financial Results" -EstimateOnly $false -
TargetMailbox "Discovery Search Mailbox"
```

PowerShell

```
Start-MailboxSearch "FY15 Q2 Financial Results"
```

Дополнительные сведения об этих командлетах см. в следующих статьях:

- Set-Mailboxsearch
- Start-MailboxSearch

Дополнительные сведения

- После копирования результатов поиска в почтовый ящик обнаружения их также можно экспортировать в PST-файл. Дополнительные сведения см. в статье Экспорт результатов поиска eDiscovery в PST-файл. Обратите внимание, что результаты поиска можно экспортировать, не копируя их в почтовый ящик обнаружения. Вы можете создать поиск, доступный только для оценки, запустить его, а затем экспортировать результаты поиска.
- Дополнительные сведения об элементах, не включаемых в поиск, см. в разделе Unsearchable Items in Exchange eDiscovery.

- Если вы копируете все содержимое почтового ящика за определенный период (не указывая ключевые слова в условиях поиска), то все элементы, не включенные в поиск, за этот период будут автоматически включены в результаты поиска. Поэтому не устанавливайте флажок **Включить элементы, не включаемые в поиск** при копировании результатов поиска. В противном случае копия всех элементов, не включаемых в поиск, будет внесена в почтовый ящик найденных сообщений.

- Кроме копирования результатов поиска в почтовый ящик найденных сообщений вы также можете оценить или выполнить предварительный просмотр результатов поиска для выбранного поиска.

  - **Оценка результатов поиска**. Этот параметр возвращает оценку общего размера и количества элементов, которые будут возвращены поиском на основе указанных условий. Оценки отображаются в области сведений в EAC.

  - **Предварительный просмотр результатов поиска**. Этот параметр позволяет просматривать результаты поиска, возвращаемые поиском, а не копировать их в почтовый ящик обнаружения для просмотра. Это позволяет быстро определить, являются ли результаты поиска релевантными. После предварительного просмотра результатов можно изменить поисковый запрос, чтобы сузить результаты поиска и повторно запустить поиск. Элементы на странице предварительного просмотра являются версиями фактических результатов поиска только для чтения, поэтому вы не можете перемещать, изменять, удалять или пересылать страницу предварительного просмотра.

    Дополнительные сведения см. в разделе Использование Центра администрирования Exchange для оценки или предварительного просмотра результатов поиска.

Экспорт результатов поиска при обнаружении электронных данных в PST-файл

Статья • 04.04.2023

С помощью средства экспорта в Центр администрирования Exchange (EAC) вы можете экспортировать результаты поиска методом обнаружения электронных данных на месте в файл данных Outlook, который также называется PST-файлом. Результаты поиска будут содержать элементы из почтовых ящиков и общедоступных папок в зависимости от источников содержимого из поиска eDiscovery. Это позволяет распространять результаты поиска среди других сотрудников организации, таких как менеджер по персоналу или менеджер по работе с записями, а также для адвоката, выступающему в судебном деле. После экспорта результатов поиска в PST-файл вы или другие пользователи можете открыть их в Outlook для просмотра или печати сообщений, представленных в результатах поиска. PST-файлы также можно открывать в сторонних приложениях для обнаружения электронных данных или создания отчетов.

Что нужно знать перед началом работы

- Время, затраченное на экспорт результатов поиска, зависит от объема и размера результатов поиска, которые будут экспортированы.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Обнаружение электронных данных на месте" в разделе Политика обмена сообщениями и разрешения на соответствие требованиям Exchange Server.
- Вам потребуется активная учетная запись почты, присоединенная к учетной записи, которую вы хотите экспортировать.
- Компьютер, используемый для экспорта результатов поиска в PST-файл, должен соответствовать следующим требованиям к системе:
    - 32- и 64-разрядные версии Windows 7 и более поздних версий
    - Microsoft .NET Framework 4.7
    - поддерживаемый браузер:

- Internet Explorer 8 и более поздних версий

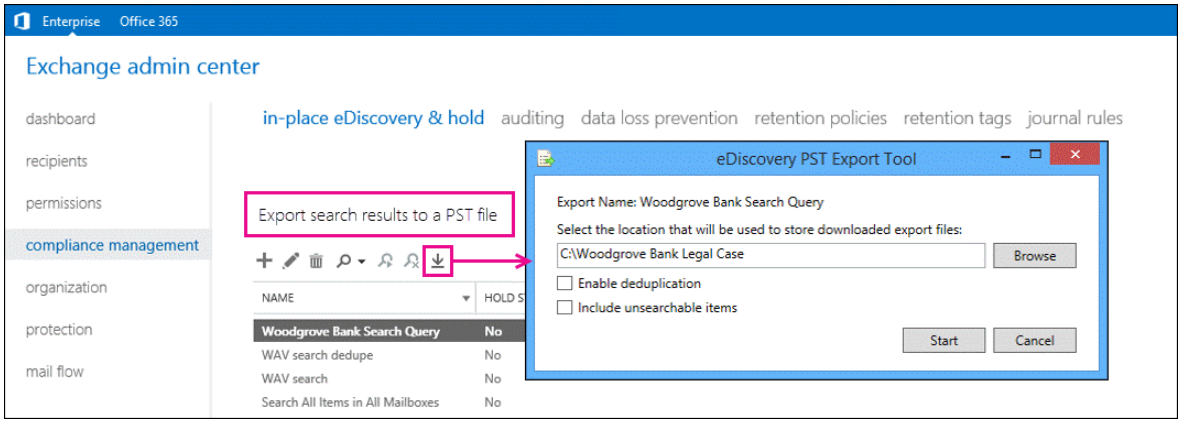
  ИЛИ

- Mozilla Firefox или Google Chrome с установленной надстройкой ClickOnce.

Использование EAC для экспорта результатов поиска In-Place eDiscovery в PST-файл

1. В EAC перейдите в раздел **Управление соответствием**> на**месте для обнаружения & электронных данных**.

2. В представлении списка выберите поиск обнаружения электронных данных, из которого вы хотите экспортировать результаты, и нажмите кнопку **Экспорт в PST-файл**.



3. В окне **Средства экспорта PST eDiscovery** выполните следующие действия:

   - Нажмите кнопку **Обзор**, чтобы указать, откуда нужно загрузить PST-файл.

   - Установите флажок **Включить дедупликацию**, чтобы исключить повторяющиеся сообщения. В PST-файл будет включен только один экземпляр сообщения.

   - Установите флажок **Включить неискируемые элементы** , чтобы включить элементы, которые не удалось найти (например, сообщения с вложениями типов файлов, которые не могут быть проиндексированы поиском Exchange). Недоступные для поиска элементы экспортируются в отдельный PST-файл.

   Примечание. Включение элементов, не доступных для поиска, при экспорте результатов поиска eDiscovery занимает больше времени, если почтовые

ящики или общедоступные папки содержат много элементов, недоступных для поиска. Чтобы сократить время для экспорта таких результатов поиска и не допустить создания больших PST-файлов, следуйте указанным далее рекомендациям.

- Создайте несколько поисков электронного обнаружения, каждый из которых выполняет поиск меньшего числа исходные почтовых ящиков.
- Создайте поиск eDiscovery, который включает только общедоступные папки.
- Если вы экспортируете все содержимое почтового ящика или общедоступной папки в пределах определенного диапазона дат (не указывая ключевые слова в критериях поиска), все элементы, недоступные для поиска, будут автоматически включены в результаты поиска. Поэтому не выбирайте флажок **Включить неискируемые элементы** .

4. Нажмите кнопку **Начать** для экспорта результатов поиска в PST-файл.

   Откроется окно со сведениями о состоянии процесса экспорта.

Дополнительные сведения

- Еще один способ уменьшить размер PST-файлов экспорта — экспортировать только неисхожие элементы для поиска eDiscovery. Для этого создайте или измените поиск, укажите начальную дату в будущем и удалите все ключевые слова в поле **Ключевые слова**. После этого поиск не будет возвращать результатов. Если при копировании или экспорте результатов установить флажок **Включить элементы, не поддерживающие поиск**, в почтовый ящик обнаружения или PST-файл будут добавлены только элементы, не поддерживающие поиск.
- Если включить дедупликацию, все результаты поиска экспортируются в один PST-файл. Если дедупликация не включена, экспортируется отдельный PST-файл для каждого почтового ящика (включая почтовые ящики общедоступных папок, если поиск включает общедоступные папки), содержащий результаты поиска. И, как уже упоминалось, недоступные для поиска элементы экспортируются в отдельный PST-файл.
- Кроме PST-файлов, содержащих результаты поиска, экспортируются также два других файла:

    - Файл конфигурации (.txt формате файла), содержащий сведения о запросе на экспорт PST, например имя экспортированного поиска eDiscovery, дату и время экспорта, включение дублирования и элементы, не доступные для поиска, поисковый запрос и источники контента, в котором был выполнен поиск.

    - Журнал результатов поиска (формат CSV), содержащий запись для каждого сообщения, возвращенного в результатах поиска. Каждая запись определяет источник содержимого, в котором находится сообщение. Если вы включили отключение дублирования, это поможет определить все почтовые ящики или общедоступные папки, содержащие повторяющиеся сообщения.

- В первой части каждого экспортированного файла используется имя поиска. Кроме того, дата и время запроса на экспорт добавляются к имени каждого PST-файла и журнала результатов.

- Вы не можете использовать средство экспорта PST с учетными записями, для которых требуется MULT-факторная проверка подлинности (MFA). Вместо этого необходимо создать пароль приложения для средства экспорта PST. Инструкции см. в статье Создание пароля приложения для Microsoft 365 .

Свойства сообщений и операторы поиска для In-Place обнаружения электронных данных в Exchange Server

Статья • 04.04.2023

В этом разделе описаны свойства сообщений электронной почты Exchange, которые можно искать с помощью In-Place удержания обнаружения & электронных данных в Exchange Server 2016 г. или Exchange Server 2019 г. The topic also describes Boolean search operators and other search query techniques that you can use to refine eDiscovery search results.

In-Place eDiscovery использует язык запросов по ключевым словам (KQL). Дополнительные сведения см. в справочнике по синтаксису языка запросов ключевых слов.

Свойства, доступные для поиска в Exchange

В следующей таблице перечислены свойства сообщений электронной почты, доступные для поиска при обнаружении электронных данных на месте или с помощью команды **New-MailboxSearch** или **Set-MailboxSearch**. Таблица содержит пример синтаксиса *property:value* для каждого свойства и описание результатов поиска, возвращаемых примерами.

Свойство	Описание свойства	Примеры	Результаты поиска, возвращаемые примерами

Свойство	Описание свойства	Примеры	Результаты поиска, возвращаемые примерами
Вложение	Имена файлов, вложенных в сообщение электронной почты.	вложение: annualreport.ppt вложение: ежегодно*	Сообщения с вложенным файлом с именем, соответствующим annualreport.ppt, например "annualreport.ppt" или "2017 annualreport.ppt". Во втором примере при использовании подстановочного знака возвращаются сообщения со вложениями, в названиях которых есть слово "annual".
Bcc	Поле "СК" электронного письма.[1]	Bcc: pilarp@contoso.com bcc:pilarp bcc:"Pilar Pinilla"	Все примеры возвращают сообщения, в поле "Скрытая копия" которых добавлен пользователь "Pilar Pinilla".
Category	Категории поиска. Категории могут быть определены пользователями с помощью Outlook или Outlook в Интернете (прежнее название — Outlook Web App). Допустимые значения: • blue • green • orange • purple • red • yellow	category:"Красная категория"	Сообщения, которым в исходных почтовых ящиках назначена красная категория.

Свойство	Описание свойства	Примеры	Результаты поиска, возвращаемые примерами
Cc	Поле "Копия" электронного письма.[1]	См3:pilarp@contoso.com cc:"Pilar Pinilla"	В обоих примерах возвращаются сообщения, в поле "Копия" которых указан пользователь "Pilar Pinilla".
From	Отправитель электронного письма.[1]	От:pilarp@contoso.com От: contoso.com	Сообщения, отправленные указанным пользователем или с указанного домена.
Importance	Важность сообщения, которую отправитель может указать при отправке. По умолчанию сообщения отправляются с обычной важностью, если отправитель не укажет **высокую** или **низкую** важность.	важность: высокая важность: средняя важность: низкая	Сообщения, которым назначена высокая, средняя или низкая важность.
Kind	Тип сообщений для поиска. Допустимые значения: • contacts • docs • email • faxes • im • journals • meetings • notes • posts • rssfeeds • tasks • voicemail	kind: email kind: email OR kind:im OR kind:voicemail	Сообщения, соответствующие критериям поиска. Второй пример возвращает сообщения электронной почты, сеансы обмена мгновенными сообщениями и голосовые сообщения, соответствующие критериям поиска.

Свойство	Описание свойства	Примеры	Результаты поиска, возвращаемые примерами
Participants	Все поля пользователей в электронном письме: "От", "Кому", "Копия" и "СК".[1]	Участников: garthf@contoso.com участники: contoso.com	Сообщения, отправленные или отправленные в garthf@contoso.com. Второй пример возвращает все сообщения, отправленные или полученные пользователем домена contoso.com.
Received	Дата получения сообщения адресатом.	получено: 15.04.2015 received>=01/01/2015 AND received<=03/31/2015	Сообщения, полученные 15 апреля 2014 г. Второй пример возвращает все сообщения, полученные с 1 января до 31 марта 2014 г.
Recipients	Все поля получателей в электронном письме: "Кому", "Копия" и "СК".[1]	Получателей: garthf@contoso.com получатели: contoso.com	Сообщения, отправленные в garthf@contoso.com. Второй пример возвращает сообщения, отправленные получателям на домене contoso.com.
Sent	Дата отправки сообщения отправителем.	отправлено: 01.07.2015 sent>=06/01/2015 AND sent<=07/01/2015	Сообщения, отправленные в указанный день или диапазон дат.

Свойство	Описание свойства	Примеры	Результаты поиска, возвращаемые примерами
Size	Размер элемента в байтах.	размер>26214400 size:1..1048576	Сообщения больше 25 МБ. Во втором примере возвращаются сообщения размером от 1 до 1 048 576 байт (1 МБ).
Subject	Текст в строке темы сообщения электронной почты.	subject:"Квартальное финансирование" тема: северный ветер	Сообщения, которые содержат точную фразу "Квартальное финансирование" в строке темы. Второй пример возвращает все сообщения, которые содержат слово northwind в строке темы.
Кому	Поле "Кому" электронного письма.[1]	Кому: annb@contoso.com to:annaye to: "Анна Ермолаева"	Все примеры возвращают сообщения, в поле "Кому" которых указано имя "Анна Ермолаева".

[1] В качестве значения свойства получателя вы можете использовать SMTP-адрес, отображаемое имя или псевдоним пользователя. Например, можно использовать annb@contoso.com, annb или "Ann Beebe", чтобы указать пользователя Ann Beebe.

Поддерживаемые операторы поиска

Логические операторы, например **AND**, **OR** и **NOT**, помогают задавать более определенные выражения для поиска в почтовых ящиках, включая какие-либо слова в поисковый запрос или исключая их из него. Другие методы, например использование операторов свойств (например, >= or ..), кавычек, скобок и подстановочных знаков, помогают уточнять поисковые запросы обнаружения

электронных данных. В следующей таблице перечислены операторы, позволяющие сократить или расширить область результатов поиска.

Оператор	Применение	Описание
И	keyword1 AND keyword2	Возвращает сообщения, включающие все указанные ключевые слова или `property: value` выражения.
+	keyword1 +keyword2 +keyword3	Возвращает элементы, содержащие *или* `keyword2` `keyword3`, *а* также содержащие `keyword1`. Таким образом, этот пример эквивалентен запросу `(keyword2 OR keyword3) AND keyword1`. Запрос `keyword1 + keyword2` (с пробелом после символа +) не совпадает с использованием оператора **AND** . Этот запрос будет эквивалентен `"keyword1 + keyword2"` и возвращает элементы с точной фазой `"keyword1 + keyword2"`.
ИЛИ	keyword1 OR keyword2	Возвращает сообщения, включающие одно или несколько указанных ключевых слов или `property: value` выражений.
NOT	keyword1 NOT keyword2 NOT from:"Анна Ермолаева"	Исключает сообщения, заданные ключевым словом или выражением `property: value` . Например, исключает сообщения, `NOT from:"Ann Beebe"` отправленные Энн Биб.
-	keyword1 -keyword2	Аналогичен оператору **NOT**. Этот запрос возвращает элементы, содержащие `keyword1` и исключающие элементы, содержащие `keyword2`.
NEAR	keyword1 NEAR(n) keyword2	Возвращает сообщения, в которых слова располагаются рядом друг с другом, где "n" означает количество слов по отдельности. Например, возвращает сообщения, `best NEAR(5) worst` в которых слово "худший" находится в пяти словах от "best". Если число не указано, расстояние по умолчанию — восемь слов.
:	свойство:значение	Двоеточие (:) в синтаксисе `property:value` указывает, что значение свойства, для которого выполняется поиск, равно указанному значению. Например, возвращает любое сообщение, `recipients:garthf@contoso.com` отправленное в garthf@contoso.com.
<	свойство<значение	Указывает, что значение искомого свойства меньше указанного значения. [1]

Оператор	Применение	Описание
>	свойство>значение	Указывает, что значение искомого свойства больше указанного значения.[1]
<=	свойство<=значение	Указывает, что значение искомого свойства меньше или равно указанному значению.[1]
>=	свойство>=значение	Указывает, что значение искомого свойства больше или равно указанному значению.[1]
..	property: value1.. value2	Указывает, что значение искомого свойства больше или равно значению 1 и меньше или равно значению 2.[1]
" "	"реальная стоимость" subject:"Квартальное финансирование"	Используйте двойные кавычки (" ") для поиска точной фразы или термина в ключевых словах и `property: value` поисковых запросах.
*	Кошка* subject:set*	Префикс поиска с подстановочными знаками (где звездочка помещается в конец слова) соответствует нулю или нескольким символам в ключевых словах или `property: value` запросах. Например, возвращает сообщения, `subject:set*` содержащие набор слов, установку и настройку (а также другие слова, начинающиеся с "set") в строке темы.
( )	(fair OR free) and from: contoso.com (IPO OR первичное) AND (биржа OR акции) (квартальное финансирование)	Круглые скобки группировать логические фразы, `property: value` элементы и ключевые слова. Например, возвращает элементы, `(quarterly financials)` содержащие слова квартальные и финансовые.

[1] Этот оператор используется для свойств, значения которых являются числами или датами.

[2] Логические операторы поиска необходимо указывать прописными буквами, например **AND**. В противном случае будет возвращена ошибка.

Неподдерживаемые символы в поисковых запросах

Как правило, при использовании неподдерживаемых символов в поисковом запросе возникает ошибка поиска или возвращаются неподходящие результаты. Как правило, неподдерживаемые символы скрыты и добавляются в запрос при его полном или частичном копировании из других приложений (например, Microsoft Word или Microsoft Excel) и вставке в поле ключевых слов на странице запроса поиска с помощью функции обнаружения электронных данных.

Ниже представлен список неподдерживаемых символов для поисковых запросов с использованием функции обнаружения электронных данных.

- **Интеллектуальные кавычки**. Интеллектуальные одиночные и *двойные кавычки (также называемые фигурными кавычками*) не поддерживаются. В поисковом запросе можно использовать только прямые кавычки.

- **Непечатаемые и управляющие символы**. Непечатаемые и управляющие символы не представляют собой письменный символ, например буквенно-цифровой символ. К непечатаемым и управляющим символам относятся символы, которые форматируют текст или разделяют его на строки.

- **Знаки слева направо и справа налево**. Эти символы являются контрольными знаками, используемыми для указания направления текста для языков слева направо (например, английского и испанского) и языков справа налево (например, арабского и иврита).

- **Логические операторы в нижнем регистре**. Как уже говорилось ранее, в поисковом запросе необходимо использовать логическое операторы верхнего регистра, такие как **AND** и **OR**. Синтаксис запроса часто указывает, что используется логический оператор, даже если могут использоваться операторы нижнего регистра; например, `(WordA or WordB) and (WordC or WordD)`.

Как предотвратить появление неподдерживаемых символов в поисковых запросах? Лучший способ избежать неподдерживаемых символов — просто ввести запрос в поле ключевых слов. Кроме того, вы можете скопировать запрос из Word или Excel, а затем вставить его в файл в обычном текстовом редакторе, например "Блокноте". После этого сохраните текстовый файл и выберите **ANSI** в раскрывающемся списке **Кодировка**. При этом будут удалены форматирование и неподдерживаемые символы. Затем вы можете скопировать запрос из текстового файла и вставить его в поле запроса по ключевым словам.

Советы по поиску

- Поиск по ключевым словам производится без учета регистра. Например, результаты поиска по словам **кот** и **КОТ** будут одинаковыми.

- Интервал между двумя ключевыми словами или двумя `property: value` выражениями такой же, как и при использовании **И**. Например, возвращает все сообщения, `from:"Sara Davis" subject:reorganization` отправленные Сарой Дэвис, которые содержат слово "**реорганизация** " в строке темы.

- Используйте синтаксис, соответствующий формату `property: value` . В значениях регистр не учитывается, а после оператора нельзя ставить пробел. При наличии пробела будет выполнен полнотекстовый поиск значения. Например, если указать **to: artemk**, будет выполнен поиск ключевого слова "artemk", а не сообщений, отправленных пользователю artemk.

- При поиске свойства получателя, например To, From, Cc или Recipients, можно использовать SMTP-адрес, псевдоним или отображаемое имя получателя. Например, можно использовать pilarp@contoso.com, pilarp или "Pilar Pinilla".

- Можно использовать только поиск с подстановочными знаками (например, ***cat** или ***set**). Поиск суффиксов с подстановочными знаками (cat*) или поиск с подстановочными знаками (*cat*) не поддерживается.

- Если искомое значение состоит из нескольких слов, то используйте двойные кавычки (" "). Например, **subject:budget Q1** возвращает сообщения, содержащие **бюджет** в строке темы и содержащие **Q1** в любом месте сообщения или в любом из свойств сообщения. Выражение **subject:"бюджет КВ1"** возвращает все сообщения, содержащие фразу **бюджет КВ1** в строке темы.

- Чтобы исключить из результатов поиска контент с определенным значением свойства, поставьте знак минус (-) перед именем свойства. Например, укажите **-from:"Sara Davis"**, чтобы исключить все сообщения, отправленные пользователем Sara Davis.

Поиск в общедоступных папках и их удержание с помощью обнаружения электронных данных на месте

Статья • 04.04.2023

Функцию обнаружения электронных данных на месте можно использовать для поиска и удержания содержимого в общедоступных папках. Подобно содержимому в почтовых ящиках пользователей содержимое общедоступных папок может пригодиться, если вашей организации приходится решать юридические вопросы, например во время судебных разбирательств или правовых расследований.

Перед началом работы

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Обнаружение электронных данных на месте" в разделе Политика обмена сообщениями и разрешения на соответствие требованиям Exchange Server.
- К почтовым ящикам и общедоступным папкам можно применить один и тот же поисковый запрос на обнаружение электронных данных.
- Удержание на месте можно использовать для удержания содержимого общедоступных папок. Но если выполняется поиск во всех почтовых ящиках организации, будет невозможно помещать источники контента на удержание.

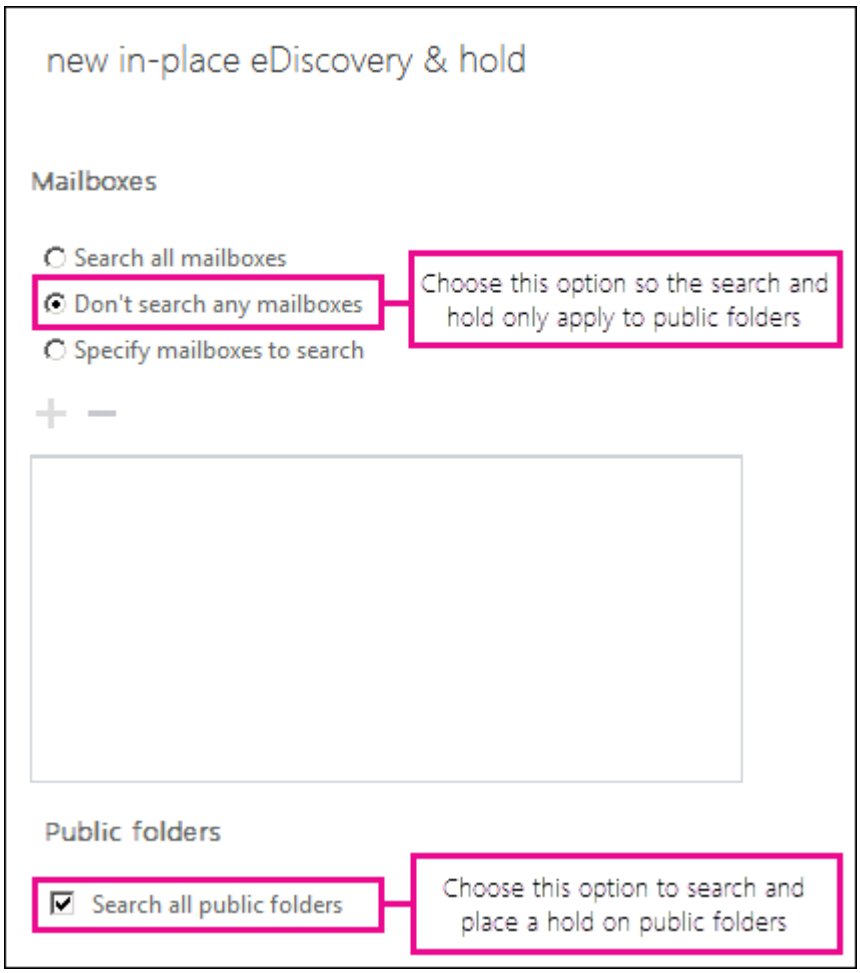
Использование Центра администрирования Exchange для поиска и хранения содержимого в общедоступных папках

1. Перейдите в **раздел Управление соответствием**> на**месте для обнаружения электронных данных&**.
2. Щелкните **Значок "Создать**+
3. На странице **Имя и описание** введите имя для поиска, добавьте описание (необязательно) и нажмите кнопку **Далее**.

4. На странице **Почтовые ящики и общедоступные папки** в разделе **Общедоступные папки** выберите **Поиск во всех общедоступных папках**. Кроме того, можно указать, следует ли выполнять поиск в почтовых ящиках:

   - Чтобы исключить почтовые ящики из поиска, выберите пункт **Не выполнять поиск в почтовых ящиках**.
   - Чтобы выполнить поиск в определенных почтовых ящиках, выберите пункт **Указать почтовые ящики для поиска**, а затем добавьте нужные почтовые ящики.

     > ⓘ **Примечание**
     >
     > Как описывалось ранее, если выбрать параметр **Поиск во всех почтовых ящиках**, будет невозможно включить удержание на месте для результатов поиска.



5. На странице **Поисковый запрос** заполните следующие поля:

   - **Включить все содержимое**. Выберите этот параметр, чтобы включить все содержимое в выбранные источники в результатах поиска. Если

выбрать этот вариант, указать дополнительные критерии поиска будет невозможно.

- **Фильтр на основе условий**. Выберите этот параметр, чтобы указать критерии поиска, включая ключевые слова, даты начала и окончания, адреса отправителей и получателей, а также типы сообщений.

6. На странице **Параметры хранения на месте** можно выбрать пункт **Поместить содержимое, совпадающее с запросом поиска, в выбранные почтовые ящики на хранение**, чтобы использовать для хранения все общедоступные папки в организации. Если этот флажок снят, содержимое не будет помещаться на хранение. Если необходимо поместить содержимое на хранение, выберите один из следующих вариантов, чтобы указать продолжительность хранения:

   - **Удержание на неопределенный срок**. Нажмите эту кнопку, чтобы поместить элементы, возвращенные поиском, на неопределенное удержание. Элементы на удержании будут сохраняться до исключения почтового ящика из поиска или до отмены поиска.

   - **Укажите количество дней хранения элементов относительно даты их получения**. Нажмите эту кнопку, чтобы хранить элементы в общедоступных папках в течение определенного периода. Например, эту функцию можно использовать, если для вашей организации необходимо, чтобы содержимое общедоступных папок сохранялось не менее семи лет.

7. Нажмите кнопку **Готово**, чтобы сохранить параметры поиска и получить оценочные сведения об общем размере и количестве элементов, которые будут возвращены операцией поиска или поставлены на удержание на основании указанных вами критериев.

   Estimates are displayed in the details pane on the **In-Place eDiscovery & Hold** page. Выберите поиск и нажмите кнопку **Обновить** чтобы обновить сведения о поиске, отображаемом в области сведений.

Поиск и удержание содержимого в общедоступных папках с помощью командной консоли Exchange

Ниже приведены три примера поиска и удержания содержимого общедоступных папок с помощью командной консоли Exchange.

Пример 1

В этом примере создается оценочный запрос поиска во всех общедоступных папках в организации для обнаружения элементов, которые были отправлены между 1 января 2015 г. и 30 июня 2015 г. и которые содержат фразу "нарушение патентных прав". В этот поиск не включаются почтовые ящики. Для запуска оценочного поиска используется командлет **Start-MailboxSearch**.

PowerShell

```
New-MailboxSearch -Name "Northwind Subpoena-All PFs" -AllPublicFolderSources $true -AllSourceMailboxes $false -SearchQuery "patent infringement" -StartDate "01/01/2015" -EndDate "06/30/2015" -TargetMailbox "Discovery Search Mailbox" -EstimateOnly
```

PowerShell

```
Start-MailboxSearch "Northwind Subpoena-All PFs"
```

Пример 2

В этом примере все содержимое помещено на хранение в общедоступные папки на неограниченное время. Для запуска поиска и помещения содержимого на хранение используется командлет **Start-MailboxSearch**.

PowerShell

```
New-MailboxSearch -Name "Hold for all PFs" -AllPublicFolderSources $true -AllSourceMailboxes $false -EstimateOnly -InPlaceHoldEnabled $true
```

PowerShell

```
Start-MailboxSearch "Hold for all PFs"
```

Пример 3

В этом примере во всех почтовых ящиках и общедоступных папках выполняется поиск содержимого со словами "прайс-лист" и "Contoso", которое было

отправлено после 1 января 2015 г. Для запуска поиска и копирования его результатов в почтовый ящик найденных сообщений используется командлет **Start-MailboxSearch**.

PowerShell

```
New-MailboxSearch -Name "Contoso Litigation" -AllSourceMailboxes $true -
AllPublicFolderSources $true -SearchQuery '"price list" AND "contoso"' -
StartDate "01/01/2015" -TargetMailbox "Discovery Search Mailbox"
```

PowerShell

```
Start-MailboxSearch "Contoso Litigation"
```

Дополнительные сведения

- Искать содержимое и помещать его на удержание можно только во всех общедоступных папках организации. Для поиска невозможно выбрать отдельные общедоступные папки.
- Если переместить общедоступные папки в другой почтовый ящик общедоступной папки, то это никак не повлияет на функцию поиска или постановки на удержание для перемещенных общедоступных папок.
- Почтовые ящики общедоступных папок идут в счет лимита на количество исходных почтовых ящиков для поиска электронных данных.
- Общедоступные папки, помещенные на удержание на месте, невозможно удалить. Чтобы удалить общедоступную папку, необходимо сначала отключить удержание.
- Включение поддержки почты для общедоступных папок не влияет на возможность обнаружения и хранения в них электронных данных. Выполнять поиск и удержание содержимого можно в общедоступных папках как с поддержкой почты, так и без нее.

Поиск соответствия требованиям для поиска по всем почтовым ящикам в Exchange Server

Статья • 04.04.2023

Функция поиска соответствия требованиям в Exchange Server позволяет выполнять поиск по всем почтовым ящикам в организации. В отличие от функции обнаружения электронных данных на месте (где максимальное количество почтовых ящиков, в которых можно выполнять поиск, составляет 10 000), в этом случае количество почтовых ящиков для одной операции поиска не ограничено. Если вам нужно выполнить поиск во всех почтовых ящиках организации, можно использовать командлет **New-ComplianceSearch**. В то же время с помощью функций рабочего процесса для обнаружения электронных данных на месте можно выполнять другие задачи, связанные с таким обнаружением, например помещать почтовые ящики на удержание или экспортировать результаты поиска. Предположим, вам нужно выполнить поиск во всех почтовых ящиках, чтобы определить те ящики, в которых хранятся сведения, имеющие отношение к судебному делу. Для этого можно использовать командлет **New-ComplianceSearch**. Почтовые ящики с такой информацией затем можно использовать в качестве исходных для обнаружения электронных данных на месте. С помощью функции обнаружения электронных данных на месте можно также поставить на удержание эти исходные почтовые ящики, скопировать результаты поиска в почтовый ящик найденных сообщений, а затем экспортировать их.

В этом разделе содержится скрипт, который можно запустить для создания поиска In-Place eDiscovery с помощью списка исходных почтовых ящиков и поискового запроса из поиска соответствия требованиям, созданного с помощью командлета **New-ComplianceSearch** .

Шаг 1. Запуск командлета New-ComplianceSearch для поиска по всем почтовым ящикам

Сначала воспользуйтесь консолью Командная консоль Exchange, чтобы создать операцию поиска соответствия по всем почтовым ящикам организации. Количество почтовых ящиков для одной операции поиска соответствия не ограничено. Укажите запрос по соответствующему ключевому слову (или запрос

по типам конфиденциальной информации), чтобы поиск возвратил только те исходные почтовые ящики, которые подходят для расследования. При необходимости уточните поисковый запрос, чтобы сузить область результатов поиска и исходных почтовых ящиков, которые будут возвращены.

> **ⓘ Примечание**
>
> Если поиск в исходных почтовых ящиках для обеспечения соответствия требованиям не возвращает результатов, операция обнаружения данных на месте не будет создана при выполнении скрипта, описанного для шага 3. Возможно, потребуется изменить поисковый запрос, а затем повторно выполнить поиск для обеспечения соответствия требованиям, чтобы возвратить результаты поиска.

Ниже приведен пример использования командлета **New-ComplianceSearch** для поиска по всем почтовым ящикам в организации. Этот поисковый запрос возвращает все сообщения, отправленные в период с 1 по 31 октября 2015 г. и содержащие фразу "financial report" (финансовый отчет) в строке темы. Первая команда создает запрос на поиск, а вторая выполняет его.

PowerShell

```
New-ComplianceSearch -Name "Search All-Financial Report" -ExchangeLocation all -ContentMatchQuery 'sent>=01/01/2015 AND sent<=06/30/2015 AND subject:"financial report"'
```

PowerShell

```
Start-ComplianceSearch -Identity "Search All-Financial Report"
```

Дополнительные сведения см. в статье New-ComplianceSearch.

> **ⓘ Важно!**
>
> When you create a compliance search by using the **New-ComplianceSearch** cmdlet, a shadow In-Place eDiscovery search is created (but not started) and displayed on the **In-Place eDiscovery & Hold** page in the Exchange admin center (EAC). It's also returned by using the **Get-MailboxSearch** cmdlet. Этот поиск в почтовом ящике называется **ComplianceSearchName -shadow**. We recommend that you delete the shadow In-Place eDiscovery search, and use the script in Step 3

to create the In-Place eDiscovery search. The functionality of creating a shadow search will be removed in a cumulative update for Exchange 2016.

Шаг 2 (необязательно). Проверка количества исходных почтовых ящиков в запросе на поиск для обеспечения соответствия требованиям

Запрос на поиск для обеспечения соответствия требованиям возвращает не более 500 исходных почтовых ящиков, содержащих результаты поиска. При наличии более 500 почтовых ящиков с данными, соответствующими поисковому запросу, в поиск соответствия, созданный на предыдущем шаге, включаются только первые 500, которые содержат наибольшее количество результатов поиска. Если результаты поиска содержат более 500 почтовых ящиков, некоторые из этих почтовых ящиков не будут включены в список исходных почтовых ящиков, которые были скопированы в новый запрос на поиск с обнаружением электронных данных на месте, созданный при выполнении шага 3.

Чтобы создать запрос на поиск для обеспечения соответствия требованиям, в который будет включено не более 500 исходных почтовых ящиков, выполните следующие действия. С их помощью можно выполнить скрипт, который покажет число исходных почтовых ящиков, содержащих результаты поиска и возвращенных при выполнении запроса на поиск для обеспечения соответствия требованиям (шаг 1).

1. Сохраните приведенный ниже текст в файле скрипта Windows PowerShell, используя суффикс .ps1 в имени файла. Этот файл можно назвать, например, SourceMailboxes.ps1.

```powershell
[CmdletBinding()]
Param(
     [Parameter(Mandatory=$True,Position=1)]
     [string]$SearchName
)
$search = Get-ComplianceSearch $SearchName
if ($search.Status -ne "Completed")
{
                "Please wait until the search finishes.";
                break;
}
```

```
$results = $search.SuccessResults;
if (($search.Items -le 0) -or ([string]::IsNullOrWhiteSpace($results)))
{
                "The compliance search " + $SearchName + " didn't
return any useful results.";
                break;
}
$mailboxes = @();
$lines = $results -split '[\r\n]+';
foreach ($line in $lines)
{
    if ($line -match 'Location: (\S+),.+Item count: (\d+)' -and
$matches[2] -gt 0)
    {
        $mailboxes += $matches[1];
    }
}
"Number of mailboxes that have search hits: " + $mailboxes.Count
```

2. В Командная консоль Exchange перейдите к папке, содержащей скрипт, созданный на предыдущем этапе, а затем запустите его. Например:

   PowerShell

   ```
   .\SourceMailboxes.ps1
   ```

3. При отображении запроса во время выполнения скрипта введите имя запроса на поиск для обеспечения соответствия требованиям, созданного при выполнении шага 1.

   Скрипт отобразит количество исходных почтовых ящиков, которые содержат результаты поиска.

При наличии более 500 исходных почтовых ящиков попробуйте создать два или более запроса на поиск для обеспечения соответствия требованиям. Например, разделите почтовые ящики организации на две половины и выполните в них поиск для обеспечения соответствия требованиям за две отдельные операции. Кроме того, можно изменить условия поиска, чтобы уменьшить количество почтовых ящиков, которые содержат результаты поиска. Например, можно указать диапазон дат или уточнить запрос по ключевому слову.

Шаг 3. Скрипт для создания запроса на поиск с обнаружением электронных данных

на месте на основе поиска для обеспечения соответствия требованиям

Теперь нужно запустить скрипт, который позволит преобразовать существующий запрос на поиск для обеспечения соответствия требованиям в запрос на поиск с обнаружением электронных данных на месте. Скрипт работает так:

- Запрашивает имя запроса на поиск для обеспечения соответствия требованиям, который требуется преобразовать.
- Проверяет, завершен ли поиск соответствия. Если поиск соответствия не возвращает результатов, поиск с обнаружением электронных данных на месте не будет создан.
- Сохраняет список исходных почтовых ящиков из поиска соответствия, которые содержат результаты поиска, в переменной.
- Создает поиск с обнаружением электронных данных на месте с указанными ниже свойствами. Обратите внимание, что новый поиск не запускается. Он запускается на шаге 4.
    - **Имя**: имя нового поиска использует следующий формат: *<Имя поиска> соответствия* требованиям_MBSearch1. Если вы снова запустите скрипт и используете тот же поиск по соответствию источнику, поиск будет называться *<Имя поиска> соответствия* требованиям_MBSearch2.
    - **Исходные почтовые ящики**: все почтовые ящики из поиска соответствия требованиям, содержащие результаты поиска.
    - **Поисковый запрос**. Новый поиск использует поисковый запрос из поиска соответствия требованиям. Если поиск соответствия включает все содержимое (при пустом поисковом запросе), новый поиск также будет иметь пустой поисковый запрос и включать все содержимое, найденное в исходных почтовых ящиках.
    - **Оценка только поиска**. Новый поиск помечается как поиск только для оценки. После выполнения такого поиска результаты не копируются в почтовый ящик найденных сообщений.

1. Сохраните приведенный ниже текст в файле скрипта Windows PowerShell, используя суффикс .ps1 в имени файла. Этот файл можно назвать, например, MBSearchFromComplianceSearch.ps1.

    ```
    PowerShell
    ```

```
[CmdletBinding()]
Param(
    [Parameter(Mandatory=$True,Position=1)]
    [string]$SearchName,
    [switch]$original,
    [switch]$restoreOriginal
)
$search = Get-ComplianceSearch $SearchName
if ($search.Status -ne "Completed")
{
   "Please wait until the search finishes";
   break;
}
$results = $search.SuccessResults;
if (($search.Items -le 0) -or ([string]::IsNullOrWhiteSpace($results)))
{
   "The compliance search " + $SearchName + " didn't return any useful
results";
   "A mailbox search object wasn't created";
   break;
}
$mailboxes = @();
$lines = $results -split '[\r\n]+';
foreach ($line in $lines)
{
    if ($line -match 'Location: (\S+),.+Item count: (\d+)' -and
$matches[2] -gt 0)
    {
        $mailboxes += $matches[1];
    }
}
$msPrefix = $SearchName + "_MBSearch";
$I = 1;
$mbSearches = Get-MailboxSearch;
while ($true)
{
    $found = $false;
    $mbsName = "$msPrefix$I";
    foreach ($mbs in $mbSearches)
    {
        if ($mbs.Name -eq $mbsName)
        {
            $found = $true;
            break;
        }
    }
    if (!$found)
    {
        break;
    }
    $I++;
}
$query = $search.KeywordQuery;
if ([string]::IsNullOrWhiteSpace($query))
```

```
{
    $query = $search.ContentMatchQuery;
}
if ([string]::IsNullOrWhiteSpace($query))
{
   New-MailboxSearch "$msPrefix$i" -SourceMailboxes $mailboxes -
EstimateOnly;
}
else
{
   New-MailboxSearch "$msPrefix$i" -SourceMailboxes $mailboxes -
SearchQuery $query -EstimateOnly;
}
```

2. В Командная консоль Exchange перейдите к папке, содержащей скрипт, созданный на предыдущем этапе, а затем запустите его. Например:

```
PowerShell

.\MBSearchFromComplianceSearch.ps1
```

3. При отображении запроса во время выполнения скрипта введите имя запроса на поиск для обеспечения соответствия требованиям, который необходимо преобразовать в запрос на поиск с обнаружением электронных данных на месте (например, запрос на поиск, созданный на шаге 1), и нажмите клавишу **Ввод**.

   При успешном выполнении сценария создается поиск с обнаружением электронных данных на месте с состоянием **NotStarted**. Выполните команду `Get-MailboxSearch <Name of compliance search>_MBSearch1 | FL`, чтобы отобразить свойства нового поиска.

Шаг 4. Запуск поиска с обнаружением электронных данных на месте

Сценарий, выполняемый на шаге 3, создает запрос на поиск с обнаружением электронных данных на месте, но не запускает его. Теперь необходимо запустить поиск, чтобы получить оценку его результатов.

1. В Центре администрирования Exchange (EAC) перейдите в раздел **Управление соответствием**> на**месте для хранения электронных & данных**.

2. В списке выберите поиск с обнаружением электронных данных на месте, созданный на шаге 3.

3. Щелкните **Поиск** (🔎>**Оцените результаты поиска**, чтобы начать поиск, и верните оценку общего размера и количества элементов, возвращаемых поиском.

   Оценка отображается в области сведений. Щелкните **Обновить** (🔄 Чтобы обновить сведения, отображаемые в области сведений.

4. Для предварительного просмотра результатов после завершения поиска нажмите кнопку **Предварительный просмотр результатов поиска** в области сведений.

> **Совет**
>
> Кроме того, можно использовать командную консоль Exchange для запуска поиска In-Place eDiscovery. например `Start-MailboxSearch -Identity <Name of compliance search>_MBSearch1`.

Действия после создания и запуска поиска с обнаружением электронных данных на месте

После создания и запуска поиска с обнаружением электронных данных на месте, который был создан с помощью сценария на шаге 3, можно выполнять различные стандартные действия над результатами поиска.

Создание хранения на месте

1. В EAC перейдите в раздел **Управление соответствием**> на**месте для обнаружения & электронных данных**.

2. В представлении списка выберите поиск In-Place eDiscovery, созданный на шаге 3, и нажмите кнопку **Изменить** (✏

3. На странице **Удержание на месте** установите флажок **Поставить содержимое выбранных почтовых ящиков, соответствующее поисковому запросу, на удержание**, а затем выберите один из следующих параметров:

   - **Держать на неопределенный срок**. Выберите этот параметр, чтобы поместить элементы, возвращенные поиском, на неопределенное

удержание. Такие элементы будут храниться до удаления почтового ящика из поиска или до удаления поиска.

- **Укажите количество дней для хранения элементов относительно даты их получения**. Выберите этот параметр, чтобы хранить элементы в течение определенного периода. Длительность будет вычислена с даты получения или создания элемента почтового ящика.

4. Нажмите кнопку **Сохранить**, чтобы создать запрос на удержание на месте, а затем повторите поиск.

Копирование результатов поиска

1. В EAC перейдите в раздел **Управление соответствием**> на**месте для обнаружения & электронных данных**.

2. В списке выберите поиск с обнаружением электронных данных на месте, созданный на шаге 3.

3. Щелкните **Поиск** (🔎 Затем выберите **Копировать результаты поиска** из раскрывающегося списка.

4. В окне **Копировать результаты поиска** выберите один из следующих вариантов:

   - **Включить неискируемые элементы**. Установите этот флажок, чтобы включить элементы почтового ящика, которые не удалось найти (например, сообщения с вложениями типов файлов, которые не могут быть проиндексированы поиском Exchange).

   - **Включить отмену дублирования**. Установите этот флажок, чтобы исключить повторяющиеся сообщения. В почтовый ящик найденных сообщений будет копироваться только один экземпляр сообщения.

   - **Включить полное ведение журнала**. Установите этот флажок, чтобы включить полный журнал в результаты поиска.

   - **Отправить мне сообщение по завершении копирования**. Установите этот флажок, чтобы получать уведомление по электронной почте о завершении поиска.

   - **Скопируйте результаты в этот почтовый ящик обнаружения**. Нажмите кнопку **Обзор** , чтобы выбрать почтовый ящик обнаружения, в который нужно скопировать результаты поиска.

5. Нажмите кнопку **Копировать**, чтобы начать процесс копирования результатов поиска в указанный почтовый ящик найденных сообщений.

6. Щелкните **Обновить** (Чтобы обновить сведения о состоянии копирования, отображаемые в области сведений.

7. После завершения копирования нажмите кнопку **Открыть**, чтобы открыть почтовый ящик найденных сообщений для просмотра результатов поиска.

Экспорт результатов поиска

1. В EAC перейдите в раздел **Управление соответствием**> на**месте для обнаружения & электронных данных**.

2. В списке выберите запрос на поиск с обнаружением электронных данных на месте, созданный на шаге 3, и нажмите кнопку **Экспорт в PST-файл**.

3. В списке выберите запрос на поиск методом обнаружения электронных данных на месте, результаты которого необходимо экспортировать, а затем нажмите **Экспортировать в PST-файл**.

4. В окне **Средства экспорта PST eDiscovery** выполните следующие действия:

    - Нажмите кнопку **Обзор**, чтобы указать, откуда нужно загрузить PST-файл.

    - Установите флажок **Включить дедупликацию**, чтобы исключить повторяющиеся сообщения. В PST-файл будет включен только один экземпляр сообщения.

    - Установите флажок **Включить элементы, недоступные для поиска**, чтобы добавить недоступные для поиска элементы почтовых ящиков (например, сообщения с вложенными файлами таких типов, которые не могут быть индексированы при поиске в Exchange). Недоступные для поиска элементы экспортируются в отдельный PST-файл.

5. Нажмите кнопку **Начать**, чтобы экспортировать результаты поиска в PST-файл.

   Откроется окно, содержащее сведения о состоянии экспорта.

Поиск и удаление сообщений в Exchange Server

Статья • 04.04.2023

Командлеты **New-ComplianceSearch** и **New-ComplianceSearchAction** можно использовать для поиска и удаления сообщения электронной почты из всех почтовых ящиков в организации. Это позволяет находить и удалять потенциально опасные сообщения, например:

- Сообщения, содержащие опасное вложение или вирус
- Фишинговые сообщения
- сообщения, содержащие конфиденциальные данные.

Зачем использовать командлеты New-ComplianceSearch и New-ComplianceSearchAction вместо командлета Search-Mailbox для удаления сообщений? В предыдущих версиях Exchange можно было выполнить `Search-Mailbox -DeleteContent` команду для поиска и удаления сообщений электронной почты. Это по-прежнему можно сделать в Exchange Server, но вы можете выполнить поиск только в 10 000 почтовых ящиков в одном поиске с помощью **командлета Search-Mailbox**. Для **New-ComplianceSearch** нет ограничений на количество почтовых ящиков в одном поиске. Это позволяет крупным организациям выполнять операции поиска и удаления в масштабах всей организации.

Ниже приведен рабочий процесс для процесса поиска и удаления.

Шаг 1. Создание и запуск поиска соответствия требованиям для поиска удаляемого сообщения

Шаг 2. Удаление сообщения

Описание того, что происходит с удаленными сообщениями, а также инструкции по отслеживанию состояния операции поиска и удаления см. в разделе More information.

> ⊗ **Внимание!**
>
> Поиск и удаление — это мощный инструмент, который позволяет всем пользователям с необходимыми разрешениями, удалять сообщения электронной почты из почтовых ящиков в организации.

Перед началом работы

- Чтобы использовать командлеты **New-ComplianceSearch** и **Start-ComplianceSearchAction** для создания и запуска поиска по соответствию, а также командлет **New-ComplianceSearchAction** для удаления сообщений, необходимо назначить роль управления поиском в почтовых ящиках. Эта роль не назначается администраторам по умолчанию. Чтобы назначить себе эту роль, чтобы можно было выполнять поиск в почтовых ящиках и удалять сообщения, добавьте себя в группу ролей Управление обнаружением. См. раздел Назначение разрешений на обнаружение электронных данных в Exchange Server.

- За один раз можно удалить не более 10 элементов в одном почтовом ящике. Так как возможность поиска и удаления сообщений предназначена для реагирования на инциденты, это ограничение обеспечивает быстрое удаление сообщений из почтовых ящиков. Эта возможность не предназначена для очистки почтовых ящиков пользователей.

Шаг 1. Создание и запуск поиска соответствия требованиям для поиска удаляемого сообщения

Первым шагом является создание и запуск поиска соответствия требованиям, чтобы найти сообщение, которое нужно удалить из почтовых ящиков в организации. Поиск можно создать, выполнив командлеты **New-ComplianceSearch** и **Start-ComplianceSearch** . Сообщения, соответствующие запросу для этого поиска, будут удалены с помощью командлета **New-ComplianceSearchAction** на шаге 2.

В этом примере команды создают и запускают поиск сообщения со словами "Обновить сведения об учетной записи" во всех почтовых ящиках в организации.

1. Откройте командную консоль Exchange.

2. Выполните следующие команды:

```
PowerShell

New-ComplianceSearch -Name "Remove Phishing Message" -ExchangeLocation
all -ContentMatchQuery 'subject:"Update your account information"'
```

```
PowerShell

Start-ComplianceSearch -Identity "Remove Phishing Message"
```

Сведения о создании поиска соответствия требованиям и настройке поисковых запросов см. в следующих разделах:

- New-ComplianceSearch
- Start-ComplianceSearch
- Свойства сообщений и операторы поиска для In-Place обнаружения электронных данных в Exchange Server

Советы по поиску сообщений для удаления

Цель поискового запроса — ограничить результаты поиска сообщениями, которые необходимо удалить. Ниже приведено несколько советов.

- Если вы знаете точный текст или фразу, используемую в строке темы сообщения, укажите в поисковом запросе свойство **Subject**.
- Если вы знаете точную дату (или диапазон дат) получения сообщения, укажите в поисковом запросе свойство **Received**.
- Если вы знаете, кто отправил сообщение, укажите в поисковом запросе свойство **From**.
- Просмотрите результаты поиска, чтобы убедиться, что возвращены только сообщения, которые необходимо удалить.
- Используйте статистику оценки поиска (с помощью командлета Get-ComplianceSearch), чтобы получить общее количество результатов поиска.

Ниже приведены два примера поиска подозрительных сообщений электронной почты.

- Этот запрос возвращает сообщения, полученные пользователями 13–14 апреля 2016 г., в которых есть слова "action" и "required" в строке темы.

```
PowerShell

(Received:4/13/2016..4/14/2016) AND (Subject:'Action required')
```

- Этот запрос возвращает сообщения, отправленные chatsuwloginsset12345@outlook.com и содержащие точную фразу "Обновить сведения об учетной записи" в строке темы.

```
PowerShell

(From:chatsuwloginsset12345@outlook.com) AND (Subject:"Update your account information")
```

Шаг 2. Удаление сообщения

После создания и уточнения поиска соответствия требованиям для возврата сообщения, которое требуется удалить, последним шагом будет выполнение **командлета New-ComplianceSearchAction** для удаления сообщения. Удаленные сообщения перемещаются в папку пользователя "Элементы с возможностью восстановления".

В этом примере команда удалит результаты поиска, возвращенные поиском по соответствию с именем "Удалить фишинговое сообщение".

1. Откройте командную консоль Exchange.
2. Выполните следующую команду.

```
PowerShell

New-ComplianceSearchAction -SearchName "Remove Phishing Message" -Purge -PurgeType SoftDelete
```

Дополнительные сведения

- **Что происходит после удаления сообщения?** Сообщение, которое удаляется с помощью `New-ComplianceSearchAction -Purge -PurgeType SoftDelete` команды , перемещается в папку Удаления в папке "Элементы с возможностью восстановления" пользователя. Она не удаляется из базы данных Exchange сразу. Пользователь может восстановить сообщения в папке "Удаленные" в течение периода хранения удаленных элементов, настроенного для почтового ящика. После истечения этого срока (или если пользователь очищает сообщение до его истечения) сообщение перемещается в папку "Очистка" и становится недоступным для пользователя. Попав в папку Очистка, сообщение снова сохраняется в течение срока хранения на основе периода

хранения удаленных элементов, настроенного для почтового ящика, если для почтового ящика включено восстановление отдельных элементов. (В Exchange восстановление одного элемента включено по умолчанию при создании нового почтового ящика.) По истечении срока хранения удаленного элемента сообщение помечается после окончательного удаления и будет очищено из базы данных Exchange при следующей обработке почтового ящика помощником по управляемым папкам.

- **Как узнать, что сообщения удаляются и перемещаются в папку "Элементы с возможностью восстановления"?** Если после удаления сообщения запустить тот же поиск соответствия требованиям, вы по-прежнему увидите то же количество результатов поиска (и может предположить, что сообщение не было удалено из почтовых ящиков пользователей). Это связано с тем, что поиск по соответствию выполняет поиск в папке "Элементы с возможностью восстановления", куда перемещается удаленное `New-ComplianceSearchAction -Purge -PurgeType SoftDelete` сообщение после выполнения команды. Чтобы убедиться, что сообщения перемещаются в папку "Элементы с возможностью восстановления", можно выполнить In-Place поиска eDiscovery (используя те же исходные почтовые ящики и критерии поиска, что и поиск соответствия требованиям, созданный на шаге 1), и скопировать результаты поиска в почтовый ящик обнаружения. Затем можно просмотреть результаты поиска в почтовом ящике найденных сообщений и проверить, перемещены ли сообщения в папку "Элементы с возможностью восстановления". Дополнительные сведения о создании In-Place поиска электронных данных, использующего список исходных почтовых ящиков и поисковый запрос из поиска соответствия требованиям, см. в статье Поиск соответствия требованиям для поиска по всем почтовым ящикам в Exchange Server.

- **Что произойдет, если сообщение будет удалено из почтового ящика, помещенного в In-Place удержание или удержание для судебного разбирательства?** После очистки сообщения (либо пользователем, либо по истечении срока хранения удаленных элементов) сообщение сохраняется до истечения срока удержания. Если период удержания не ограничен, элементы сохраняются до прекращения удержания или изменения периода удержания.

- **Как получить состояние операции поиска и удаления?** Запустите **Get-ComplianceSearchAction**: чтобы получить состояние операции удаления. Обратите внимание, что объект, который создается при выполнении командлета **New-ComplianceSearchAction** , именуется в следующем формате: `<name of Compliance Search>_Purge`.

Управление записями обмена сообщениями в Exchange Server

Статья • 04.04.2023

Пользователи каждый день отправляют и получают электронную почту. Если не обращать внимания на электронную почту, на пользователя может обрушиться целый поток создаваемых и принимаемых сообщений, что снижает производительность труда и подвергает организацию определенным рискам. Таким образом, управление жизненным циклом электронной почты имеет важнейшее значение для большинства организаций.

Управление записями сообщений (MRM) — это технология управления записями в Exchange Server, которая помогает организациям управлять жизненным циклом электронной почты и снизить юридические риски, связанные с электронной почтой. Развертывание этой технологии может пригодиться вашей организации по нескольким причинам.

- **Соответствие бизнес-требованиям**. В зависимости от политик обмена сообщениями в вашей организации может потребоваться хранить важные сообщения электронной почты в течение определенного периода времени. Например, почтовый ящик пользователя может содержать критически важные сообщения, связанные с бизнес-стратегией, транзакциями, разработкой продуктов или взаимодействием с клиентами.

- **Соответствие юридическим и нормативным требованиям**. Многие организации имеют юридические или нормативные требования для хранения сообщений в течение указанного периода и удаления сообщений старше этого периода. При хранении сообщений сверх этого срока могут возрасти правовые или финансовые риски организации.

- **Повышение производительности пользователей**. Если оставить неуправляемой, постоянно растущий объем электронной почты в почтовых ящиках пользователей также может повлиять на их производительность. Например, хотя подписки на информационные бюллетени и автоматические уведомления могут иметь информационную ценность при получении, пользователи могут не удалять их после чтения (часто они никогда не читаются). Многие из этих типов сообщений не имеют значения хранения в течение нескольких дней. Использование MRM для удаления таких сообщений может помочь уменьшить информационный беспорядок в почтовых ящиках пользователей, тем самым повышая производительность.

- **Улучшение управления хранилищем**. Из-за ожиданий, вызванных бесплатными службами электронной почты для потребителей, многие пользователи хранят старые сообщения в течение длительного периода времени или никогда не удаляют их. Обслуживание больших почтовых ящиков становится все более стандартной практикой, и пользователи не должны быть вынуждены изменять свои привычки работы на основе ограничительных квот почтовых ящиков. Однако хранение сообщений в течение периода, необходимого для бизнеса, юридических или нормативных причин, также увеличивает затраты на хранение.

Управление записями сообщений позволяет с необходимой гибкостью реализовать политику управления записями, которая максимально соответствует потребностям организации. Хорошее представление об управлении записями сообщений, архивировании и хранении на месте позволяет достичь целей управления хранением в почтовых ящиках и обеспечить соответствие нормативным требованиям к хранению.

MRM в Exchange Server

В Exchange Server mrM осуществляется за счет использования тегов хранения и политик хранения. Теги хранения используются для применения параметров хранения ко всему почтовому ящику и его стандартным папкам, таким как "Входящие" и "Удаленные". Вы также можете создавать и развертывать теги хранения, которые outlook 2010 и более поздних версий и Outlook в Интернете пользователи могут использовать для применения к папкам или отдельным сообщениям. После их создания вы добавляете теги хранения в политику хранения, а затем применяете политику к пользователям. Помощник по обслуживанию управляемых папок в почтовых ящиках обрабатывает почтовые ящики и применяет параметры хранения в политике хранения пользователя. Дополнительные сведения о политиках хранения см. в статье Теги хранения и политики хранения в Exchange Server.

По истечении срока хранения сообщения, который установлен в применимом теге хранения, помощник для управляемых папок выполняет действие по хранению, указанное в теге. Затем сообщения можно удалить окончательно или с возможностью восстановления. Если для пользователя подготовлен архив, с помощью тегов хранения также можно переместить элементы в локальный архив пользователя.

Стратегии управления записями сообщений

С помощью политик хранения можно применять основной срок хранения сообщений ко всему почтовому ящику или определенным папкам по умолчанию. Хотя существует несколько стратегий развертывания управления записями сообщений, ниже приведены самые распространенные из них.

Удаление всех сообщений по истечении указанного периода. В этой стратегии реализуется одна политика MRM, которая удаляет все сообщения по истечении определенного периода. В этой стратегии отсутствует классификация сообщений. Политику эту можно реализовать, создав единственный тег политики по умолчанию (DPT) для почтового ящика. Однако это не гарантирует, что сообщения будут храниться в течение указанного периода. Пользователи все еще могут удалять сообщения, прежде чем завершится срок хранения.

Перемещение сообщений в архивные почтовые ящики. В этой стратегии вы реализуете политики MRM, которые перемещают элементы в архивный почтовый ящик пользователя. Архивный почтовый ящик представляет собой дополнительное место для хранения старого и редко используемого содержимого. Теги хранения, отвечающие за перемещение элементов, также известны как *политики архивирования*. В одной политике хранения можно сочетать тег политики по умолчанию (DPT) и личные теги для перемещения элементов, а также тег политики по умолчанию (DPT), теги политики хранения (RPT) и личные теги для удаления элементов. Дополнительные сведения о политиках архивации см. в статье Архивация на месте в Exchange Server.

Удаление сообщений на основе расположения папки. В этой стратегии вы реализуете политики MRM на основе расположения электронной почты. Например, можно задать хранение сообщений в папке "Входящие" в течение одного года, а сообщений в папке "Нежелательная почта" — в течение 60-ти дней. Эту политику можно реализовать, используя сочетание тегов политики хранения (RPT) для каждой папки по умолчанию, которую требуется настроить, и тега политики по умолчанию (DPT) для всего почтового ящика. DPT применяется ко всем настраиваемым папкам и всем папкам по умолчанию, к которым не применяется RPT.

> ⓘ **Примечание**
>
> В Exchange Server можно создавать RPT для папок "Календарь" и "Задачи". Если вы не хотите, чтобы элементы в этих или других стандартных папках имели срок действия, можно создать для них отключенный тег хранения.

Разрешить пользователям классифицировать сообщения. В этой стратегии вы реализуете политики MRM, которые включают базовый параметр хранения для всех сообщений, но позволяют пользователям классифицировать сообщения на основе бизнес-требований или нормативных требований. В этом случае пользователи становятся важной частью вашей стратегии управления записями. Часто они лучше понимают значение хранения сообщения.

Пользователи могут применять различные параметры хранения к сообщениям, чтобы хранить их в течение различных периодов. Эту политику можно реализовать, используя сочетание следующих компонентов.

- DPT для почтового ящика
- Личные теги, которые пользователи могут применять к настраиваемым папкам или отдельным сообщениям
- Дополнительные теги политики хранения, определяющие истечение срока действия элементов в папках по умолчанию (необязательно)

Например, можно использовать политику хранения с личными тегами, которые имеют более короткий срок хранения (например, два дня, одна неделя или один месяц), а также личными тегами с более длительным сроком хранения (например, один год, два года или пять лет). Пользователи могут применять личные теги с более короткими сроками хранения для таких элементов, как подписки на информационные бюллетени, которые могут оказаться неактуальными через несколько дней после получения, а также теги с более длительными сроками с целью хранения важных для бизнеса элементов. Этот процесс также можно автоматизировать с помощью правил папки "Входящие" в Outlook, чтобы применить личный тег к сообщениям, которые соответствуют условиям правила.

Хранение сообщений для обнаружения электронных данных. В этой стратегии вы реализуете политики MRM, которые удаляют сообщения из почтовых ящиков по истечении указанного периода времени, но также сохраняют их в папке "Элементы с возможностью восстановления" для обнаружения электронных данных на месте в Exchange Server целях, даже если сообщения были удалены пользователем или другим процессом.

Это требование можно выполнить с помощью сочетания политик хранения и удержания на месте и удержания для судебного разбирательства в Exchange Server или судебного удержания. Политики хранения удаляют сообщения из почтового ящика по истечении указанного периода. Удержание на основе времени In-Place или удержание для судебного разбирательства сохраняет сообщения, которые были удалены или изменены до этого периода. Например, чтобы хранить

сообщения в течение семи лет, можно создать политику хранения с DPT, которая удаляет сообщения в течение семи лет, а удержание для судебного разбирательства для хранения сообщений в течение семи лет. Сообщения, которые не были удалены пользователями, будут удалены через семь лет; сообщения, удаленные пользователями до семилетнего периода, будут храниться в папке "Элементы с возможностью восстановления" в течение семи лет. Дополнительные сведения об этой папке см. в статье Папка "Элементы с возможностью восстановления" в Exchange Server.

Разрешить пользователям очищать свои почтовые ящики также можно с помощью тегов политики хранения (RPT) и личных тегов. Однако в этом случае хранение на месте и хранение для судебного разбирательства все еще будет действовать, поэтому удаленные сообщения будут храниться до завершения указанного срока.

> ⓘ **Примечание**
>
> Удержание на основе времени In-Place или удержание для судебного разбирательства похоже на то, что в Exchange 2010 неофициально называется *временным удержанием по юридическим* причинам. Такое удержание реализовывалось с помощью настройки периода хранения удаленных элементов в базе данных почтовых ящиков или отдельном почтовом ящике. При этом хранение удаленных элементов позволяло хранить удаленные и измененные элементы с учетом даты удаления. Удержание на месте и хранение для судебного разбирательства позволяют хранить элементы с учетом даты их получения или создания. Это гарантирует, что сообщения будут храниться по крайней мере в течение указанного периода.

Теги хранения и политики хранения в Exchange Server

Статья • 31.01.2025

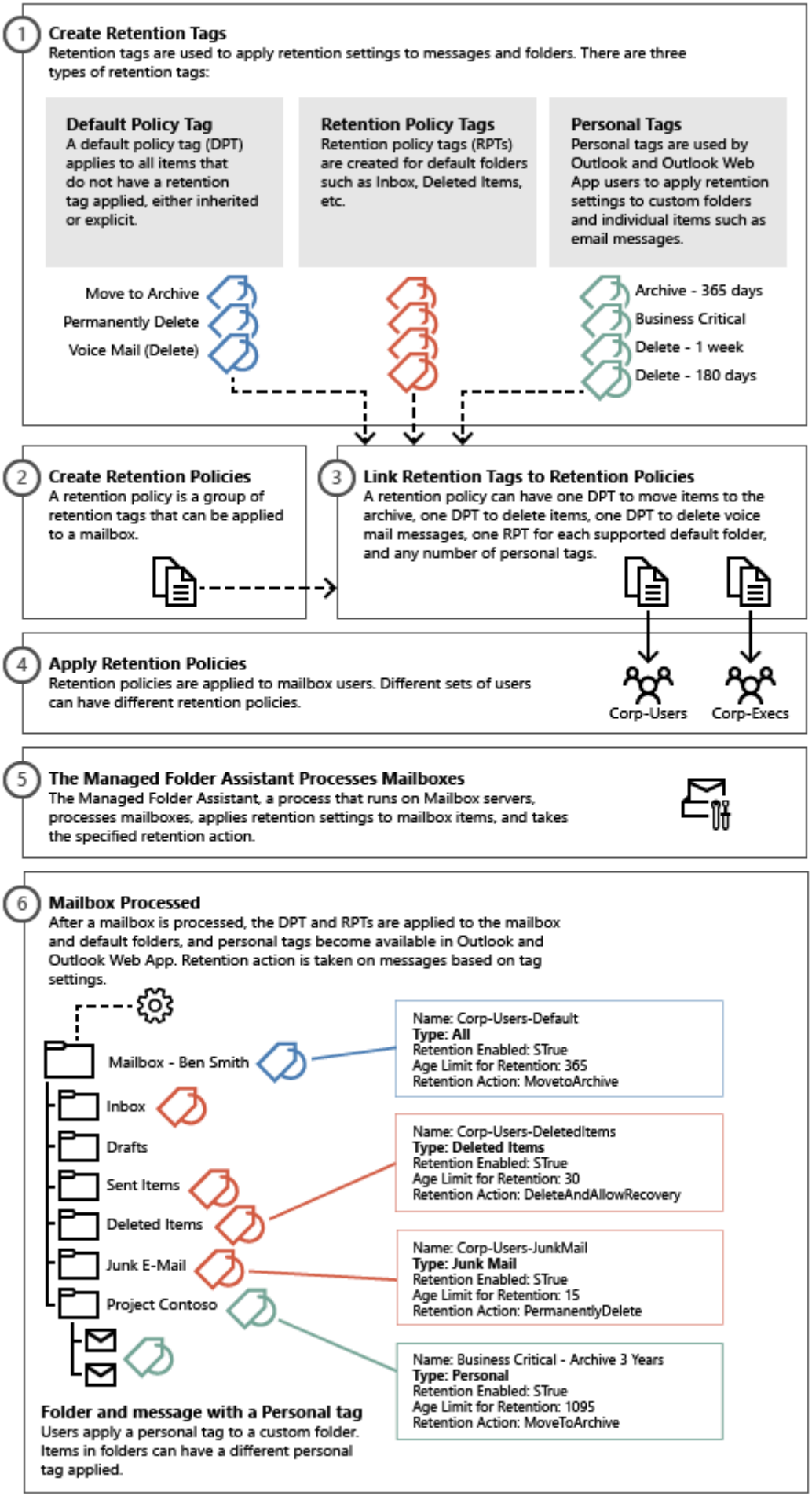
Технология "Управление записями сообщений" помогает организациям снизить юридические риски, связанные с электронной почтой и другими видами связи. Она позволяет хранить сообщения в соответствии с политикой компании или требованиями законодательства, а также удалять содержимое, не имеющее юридической или коммерческой ценности.

Стратегия управления записями сообщений

MrM в Exchange Server выполняется с помощью *тегов хранения* и *политик хранения*. Перед тем как подробно обсудить каждую из этих функций, давайте рассмотрим, как они используются в общей стратегии управления записями сообщений.

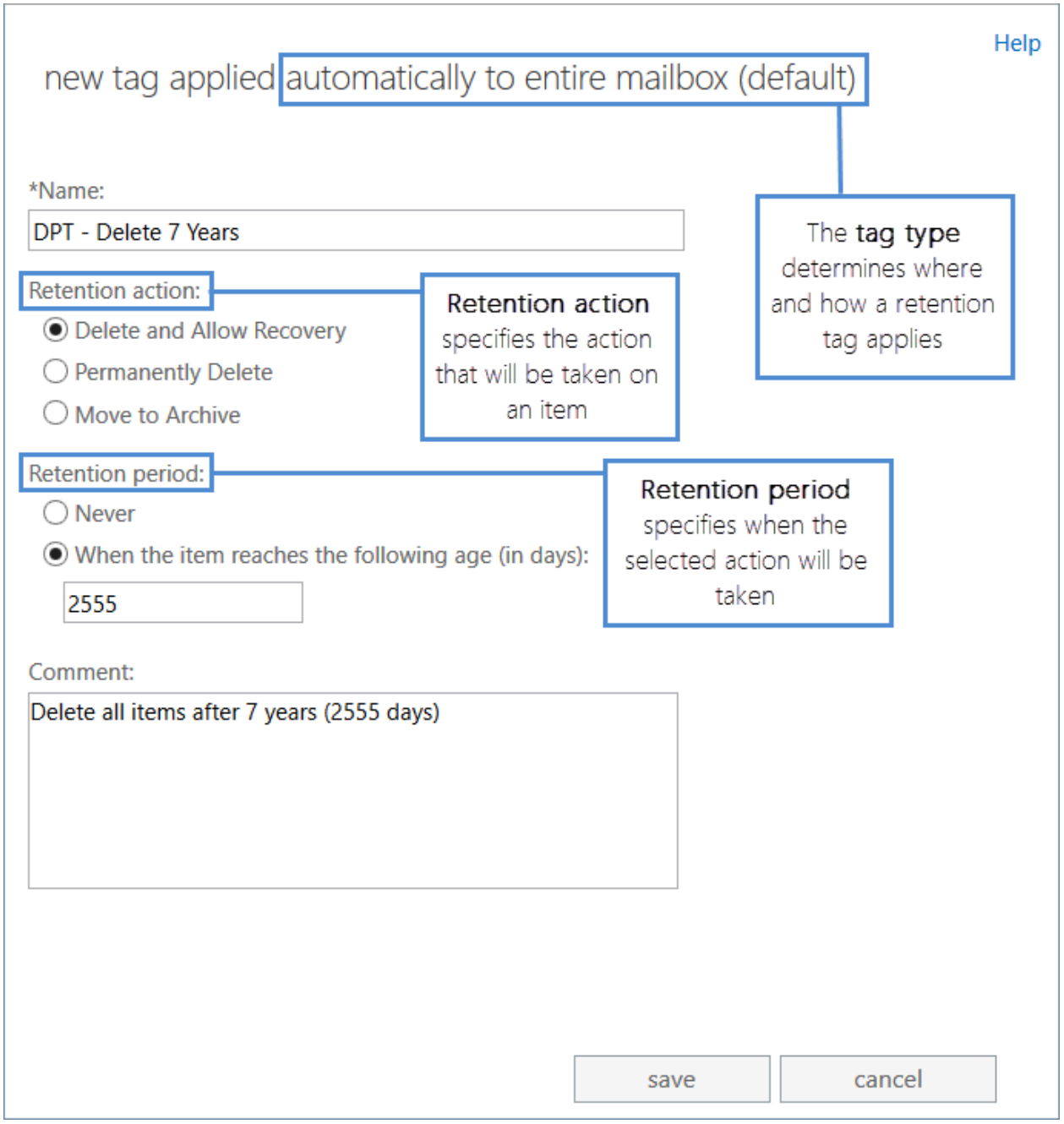
- Назначение *тегов политики хранения* (RPT) папкам по умолчанию, например папке "Входящие" и "Удаленные".
- Применение *тегов политики по умолчанию* (DPT) к почтовым ящикам для управления хранением всех элементов без тегов.
- Разрешение пользователю назначать *личные теги* настраиваемым папкам и отдельным элементам.
- Отделение функций управления записями сообщений от управления папками "Входящие" пользователей и обычных способов хранения файлов. Пользователи могут не применять требования хранения при хранении сообщений в управляемых папках. Отдельные сообщения могут иметь тег хранения, отличный от применяемого к папке, в которой они расположены.

На следующем рисунке показаны задачи, участвующие в реализации этой стратегии.


1
Create Retention Tags
Retention tags are used to apply retention settings to messages and folders. There are three types of retention tags:
Default Policy Tag
A default policy tag (DPT) applies to all items that do not have a retention tag applied, either inherited or explicit.
Retention Policy Tags
Retention policy tags (RPTs) are created for default folders such as Inbox, Deleted Items, etc.
Personal Tags
Personal tags are used by Outlook and Outlook Web App users to apply retention settings to custom folders and individual items such as email messages.
Move to Archive
Permanently Delete
Voice Mail (Delete)
Archive - 365 days
Business Critical
Delete - 1 week
Delete - 180 days
2
Create Retention Policies
A retention policy is a group of retention tags that can be applied to a mailbox.
3
Link Retention Tags to Retention Policies
A retention policy can have one DPT to move items to the archive, one DPT to delete items, one DPT to delete voice mail messages, one RPT for each supported default folder, and any number of personal tags.
4
Apply Retention Policies
Retention policies are applied to mailbox users. Different sets of users can have different retention policies.
Corp-Users
Corp-Execs
5
The Managed Folder Assistant Processes Mailboxes
The Managed Folder Assistant, a process that runs on Mailbox servers, processes mailboxes, applies retention settings to mailbox items, and takes the specified retention action.
6
Mailbox Processed
After a mailbox is processed, the DPT and RPTs are applied to the mailbox and default folders, and personal tags become available in Outlook and Outlook Web App. Retention action is taken on messages based on tag settings.
Mailbox - Ben Smith
Inbox
Drafts
Sent Items
Deleted Items
Junk E-Mail
Project Contoso
Name: Corp-Users-Default
Type: All
Retention Enabled: STrue
Age Limit for Retention: 365
Retention Action: MovetoArchive
Name: Corp-Users-DeletedItems
Type: Deleted Items
Retention Enabled: STrue
Age Limit for Retention: 30
Retention Action: DeleteAndAllowRecovery
Name: Corp-Users-JunkMail
Type: Junk Mail
Retention Enabled: STrue
Age Limit for Retention: 15
Retention Action: PermanentlyDelete
Name: Business Critical - Archive 3 Years
Type: Personal
Retention Enabled: STrue
Age Limit for Retention: 1095
Retention Action: MoveToArchive
Folder and message with a Personal tag
Users apply a personal tag to a custom folder. Items in folders can have a different personal tag applied.

Теги хранения

Как видите, теги хранения используются для применения параметров хранения к папкам и отдельным элементам, таким как сообщения электронной почты и голосовая почта. Эти параметры определяют, как долго сообщение остается в почтовом ящике, а также действие, которое необходимо выполнить, когда сообщение достигает указанного срока хранения. По истечении срока хранения сообщение перемещается в архив пользователя на месте или удаляется.



Теги хранения позволяют пользователям отмечать собственные папки почтовых ящиков и отдельные элементы для хранения. Теперь пользователи могут не применять требования к хранению элементов в управляемых папках, подготовленных администратором.

Типы тегов хранения

Теги хранения разделены на следующие три типа в зависимости от того, кто может их применять и где именно в почтовом ящике их можно применять.

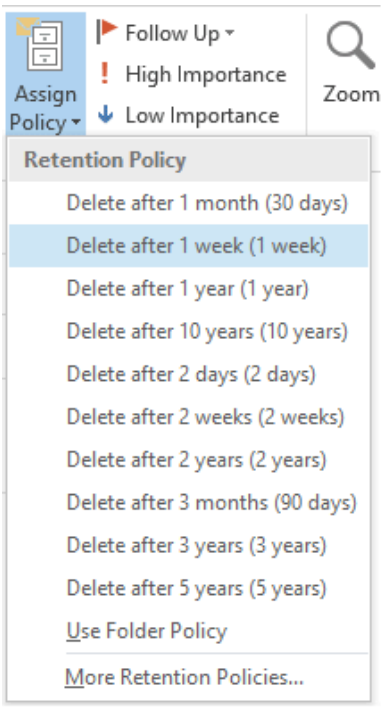
Развернуть таблицу

Тип тега хранения	Прикладной...	Кем применяется...	Доступные действия...	Сведения
Тег политики по умолчанию (DPT)	Автоматически ко всему почтовому ящику DPT применяется к *элементам без тегов* , которые являются элементами почтового ящика, к которым не применяется тег хранения напрямую или по наследованию из папки.	Администратор	Переместить в архив Удалить и разрешить восстановление Удалить окончательно	Пользователи не могут изменить теги DPT, примененные к почтовому ящику.
Тег политики хранения (RPT)	Автоматически к папке по умолчанию Папки по умолчанию — это папки, которые автоматически создаются во всех почтовых ящиках, например: **Входящие**, **Удаленные** и **Отправленные**. Список поддерживаемых папок по умолчанию см. в разделе Default folders that support Retention Policy Tags.	Администратор	Удалить и разрешить восстановление Удалить окончательно	Пользователи не могут изменить теги RPT, примененные к папке по умолчанию.

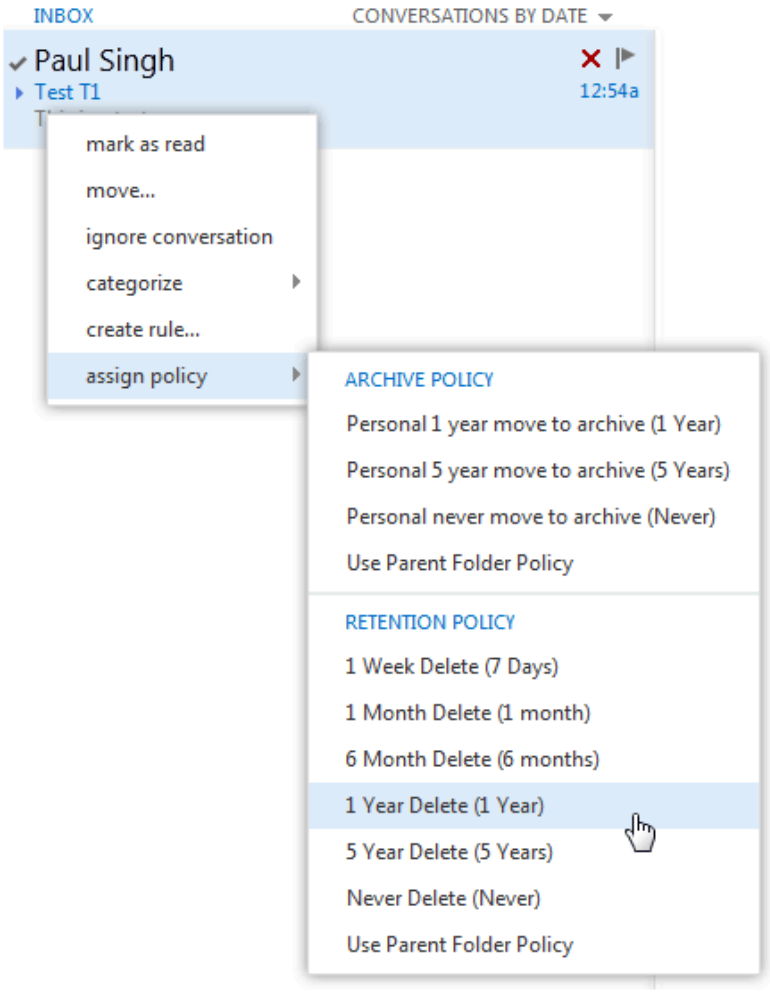
Тип тега хранения	Прикладной...	Кем применяется...	Доступные действия...	Сведения
Личный тег	Вручную к элементам и папкам Пользователи могут автоматизировать применение тегов, используя правила папки "Входящие", чтобы перемещать сообщение в папку, к которой применен определенный тег, или применять личный тег к сообщению.	Пользователи	Переместить в архив Удалить и разрешить восстановление Удалить окончательно	Личные теги позволяют пользователям определить, как долго будет храниться элемент. Например, к почтовому ящику может быть применен тег DPT для удаления элементов через семь лет, но пользователь может с помощью личного тега создать исключение для таких элементов, как информационные бюллетени и автоматические уведомления, чтобы удалять их через три дня.

Дополнительные сведения о личных тегах

Личные теги доступны пользователям Outlook и Outlook в Интернете в рамках их политики хранения. В Outlook и Outlook в Интернете личные теги с действием **Переместить в архив** представлены в списке **Политика архивации**, а личные теги с действиями **Удалить и разрешить восстановление** или **Окончательно удалить** — в списке **Политика хранения**, как показано ниже:



Outlook



Outlook on the web

Пользователи могут применять личные теги к папкам, которые они создают, или отдельным элементам. Сообщения с личными тегами всегда обрабатываются с учетом параметров этих тегов. Пользователи могут помечать личными тегами сообщения, чтобы те удалялись или перемещались до или после запланированного применения к их почтовому ящику параметров, указанных в тегах DPT или RPT. Также можно создавать личные теги с отключенной возможностью хранения. Это позволяет пользователям устанавливать теги на элементы, чтобы они никогда не переносились в архив и срок их действия никогда не истекал.

> ⓘ **Примечание**
>
> Пользователи могут применять политики архива к папкам по умолчанию, папкам и подпапкам, созданным пользователями, или отдельным элементам. Пользователи могут применять политику хранения к папкам или подпапкам, созданным пользователями, и отдельным элементам (в том числе к подпапкам и элементам в папке по умолчанию), но не к папкам по умолчанию.

Пользователи также могут использовать Центр администрирования Exchange (EAC) для выбора дополнительных личных тегов, которые не связаны с политикой хранения. Затем выбранные теги становятся доступными в Outlook и Outlook в Интернете. Чтобы пользователь мог выбирать дополнительные теги в Центре администрирования Exchange, необходимо добавить роль MyRetentionPolicies Role в его политику назначения ролей. Дополнительные сведения о политиках назначения ролей для пользователей см. в статье Understanding Management Role Assignment Policies. Если разрешить пользователям выбирать дополнительные личные теги, все личные теги в организации Exchange становятся доступными для них.

> ⓘ **Примечание**
>
> Личные теги — это расширенная функция. Для почтовых ящиков с политиками, содержащими эти теги (или как результат добавления пользователями этих тегов к своим почтовым ящикам), требуется корпоративная клиентская лицензия Exchange (CAL).

Период хранения

При включении тега хранения необходимо указать для него срок хранения. Этот срок определяет количество дней, в течение которых сообщение будет храниться в почтовом ящике пользователя после его доставки.

Расчет срока хранения для неповторяющихся элементов (таких как сообщения электронной почты) отличается от расчета для элементов, имеющих дату окончания, или повторяющихся элементов (таких как собрания и задачи). Сведения о том, как вычисляется срок хранения для различных типов элементов, см. в статье Как вычисляется срок хранения в Exchange Server.

Можно также создавать теги хранения с отключенной функцией хранения или отключать теги после их создания. Так как сообщения, к которым применен отключенный тег, не обрабатываются, действия хранения к ним не применяются. В результате можно использовать отключенный личный тег, например **Никогда не перемещать** или **Никогда не удалять**, для переопределения тега политики по умолчанию или тега политики хранения, которые в противном случае будут применяться к сообщению.

Действия сохранения

При создании или настройке тега хранения можно выбрать одно из следующих действий по истечении срока хранения элемента:

Развернуть таблицу

Действие сохранения	Принятые меры...	Кроме...
Переместить в архив	Перемещает сообщение в архивный почтовый ящик пользователя Доступно только для DPT и личных тегов Дополнительные сведения о архивации см. в статье Архивация на месте в Exchange Server.	Если у пользователя нет архивного почтового ящика, действие не выполняется.
Удаление и разрешение восстановления:	Аналогично ситуации, когда пользователь очищает папку "Удаленные". Элементы перемещаются в папку "Элементы с возможностью восстановления" в Exchange Server почтового ящика и сохраняются до истечения срока *хранения удаленных элементов*. Пользователь получает еще одну возможность восстановить элемент в диалоговом окне **Восстановление удаленных элементов** в Outlook или Outlook в Интернете.	Если срок хранения удаленных элементов равен нулю дней, элементы удаляются без возможности восстановления. Дополнительные сведения см. в разделе Настройка квот на хранение удаленных элементов и восстанавливаемых элементов.
Удалить без возможности восстановления	Окончательно удаляет сообщения. После этого сообщения не могут быть восстановлены.	Если почтовый ящик помещается на удержание на месте и удержание для судебного разбирательства в Exchange Server или судебного разбирательства, элементы сохраняются в папке "Элементы с возможностью восстановления" на основе параметров удержания. Обнаружение электронных данных на месте в Exchange Server по-

Действие сохранения	Принятые меры...	Кроме...
		прежнему будет возвращать эти элементы в результатах поиска.
Установить отметку "Срок хранения истек"	Помечает сообщение как просроченное. В Outlook и Outlook в Интернете элементы с истекшим сроком действия отображаются с уведомлением "Срок действия этого элемента истек" и "Срок действия этого элемента истек через 0 дней".	N. O.

> ⓘ **Примечание**
>
> Тег политики по умолчанию (DPT) с **действием Переместить в Архив** всегда перезаписывает тег политики хранения (RPT) или личный тег (PT), если предельный срок хранения DPT ниже RPT или PT.

Дополнительные сведения о создании тегов хранения см. в статье Создание политики хранения в Exchange Server.

Политики хранения

Чтобы применить один или несколько тегов хранения к почтовому ящику, необходимо добавить их в политику хранения, а затем применить политику к почтовым ящикам. Почтовый ящик не может иметь более одной политики хранения. Теги хранения можно связать с политикой хранения или отсоединить от нее в любое время, и изменения автоматически вступают в силу для всех почтовых ящиков, в которых применена политика.

Политика хранения может иметь следующие теги хранения.

Развернуть таблицу

Тип тега хранения	Теги в политике
Тег политики по умолчанию (DPT)	Один тег DPT с действием **Переместить в архив**

Тип тега хранения	Теги в политике
	Один DPT с действиями **"Удалить" и "Разрешить восстановление**" или **"Окончательное удаление"** Один тег DPT с действиями **Удалить и разрешить восстановление** или **Удалить окончательно** для сообщений голосовой почты
Теги политики хранения	Один тег политики хранения для каждой поддерживаемой папки по умолчанию **Примечание.** Нельзя связать несколько RPT для определенной папки по умолчанию (например **, Удаленные элементы**) с одной и той же политикой хранения.
Личные теги	Любое количество личных тегов **Примечание.** Многие личные теги в политике могут сбить пользователей с толку. Мы рекомендуем связывать с политикой хранения не более 10 личных тегов.

> ⓘ **Примечание**
>
> С политикой хранения можно не связывать теги хранения, но рекомендуется использовать такой сценарий. Если к почтовому ящику применена политика хранения, с которой не связаны теги хранения, срок хранения элементов этого почтового ящика будет не ограничен.

Политика хранения может включать в себя архивные теги (теги, перемещающие элементы в личный архивный почтовый ящик) вместе с тегами удаления (тегами, удаляющими элементы). К элементу почтового ящика также могут одновременно применяться эти два типа тегов. Архивные почтовые ящики не имеют отдельной политики хранения. К основному и архивному почтовым ящикам применяется одна политика хранения.

When planning to create retention policies, you must consider whether they'll include both archive and deletion tags. As mentioned earlier, a retention policy can have one DPT that uses the **Move to archive** action and one DPT that uses either the **Delete and allow recovery** or **Permanently delete** action. The DPT with the **Move to archive** action must have a lower retention age than the DPT with a deletion action. For example, you can use a DPT with the **Move to archive** action to move items to the archive mailbox in two years, and a DPT with a deletion action to remove items from the mailbox in seven years. Items in both primary and archive mailboxes will be deleted after seven years.

Политика хранения по умолчанию

Программа установки Exchange создает политику хранения **Default MRM Policy**. Политика автоматически применяется, если вы создаете архив для нового пользователя и не указываете политику хранения.

Вы можете изменить теги, включенные в политику MRM по умолчанию, например путем изменения срока хранения или действия хранения, отключения тега или изменения политики путем добавления или удаления тегов из него. Обновленная политика применяется к почтовым ящикам при следующей обработке помощником по управляемым папкам (MFA).

Дополнительные сведения, в том числе список тегов сохранения, связанных с политикой, см. в статье Default Retention Policy.

Помощник по работе с управляемыми папками

Помощник для управляемых папок — помощник по обслуживанию почтовых ящиков, работающий на серверах почтовых ящиков, — обрабатывает почтовые ящики, к которым применена политика хранения.

Помощник для управляемых папок применяет политику хранения путем проверки элементов в почтовом ящике и определения того, являются ли они субъектами хранения. Затем он помечает элементы, которые необходимо хранить, с помощью соответствующих тегов хранения и применяет указанное действие хранения к элементам с истекшим сроком хранения.

Помощник для управляемых папок функционирует на основе регулировки. Помощники такого типа работают непрерывно и не требуют планирования. Системные ресурсы, которые они могут расходовать, регулируются. Помощник для управляемых папок можно настроить на обработку всех почтовых ящиков на сервере почтовых ящиков в течение определенного периода (известного как *рабочий цикл*). Помимо этого, через заданный интервал времени в момент, называемый *контрольной точкой рабочего цикла*, помощник обновляет список обрабатываемых почтовых ящиков. В процессе обновления помощник добавляет вновь созданные или перемещенные почтовые ящики в очередь. Он также изменяет приоритеты для существующих почтовых ящиков, которые не были успешно обработаны из-за сбоев, и перемещает их на более высокое место в очереди, чтобы их можно было обработать за тот же рабочий цикл.

Чтобы запустить помощник вручную для обработки определенного почтового ящика, используйте командлет Start-ManagedFolderAssistant. Дополнительные

сведения см. в статье Настройка и запуск помощника по управляемым папкам в Exchange Server.

> ⓘ **Примечание**
>
> Помощник для управляемых папок не выполняет действия над сообщениями, которые не являются субъектами хранения (для которых отключены теги хранения). Можно также отключить тег хранения, чтобы временно приостановить обработку элементов с этим тегом.

Перемещение элементов между папками

Элемент почтового ящика, перемещенный из одной папки в другую, наследует все теги, примененные к папке, в которую он перемещен. Если элемент перемещен в папку, для которой не назначен тег хранения, к ней применяется тег DPT. Если элемент имеет явно назначенный тег, этот тег всегда имеет приоритет над тегами папок или тегом по умолчанию.

Применение тега хранения к папке в архиве

Когда пользователь применяет личный тег к папке в архиве, если папка с таким же именем существует в основном почтовом ящике и имеет другой тег, тег в этой папке в архиве изменяется в соответствии с тегом в основном почтовом ящике. Это позволяет избежать путаницы, связанной с элементами в папке в архиве, с поведением срока действия, отличным от того, что и в той же папке в основном почтовом ящике пользователя. Например, у пользователя есть папка с именем Project Contoso в основном почтовом ящике с тегом *Delete - 3 года* , а папка Project Contoso также существует в архивном почтовом ящике. Если пользователь применяет личный тег *Delete — 1 год* для удаления элементов в папке через 1 год. При повторной обработке почтового ящика папка возвращается к тегу Delete — 3 года.

Удаление тега хранения из политики хранения

После удаления тега хранения из примененной к почтовому ящику политики хранения этот тег становится недоступным пользователю и его невозможно применять к элементам почтового ящика.

Существующие элементы, помеченные этим тегом, будут по-прежнему обрабатываться помощником по работе с управляемыми папками на основе

параметров этого тега, а действие хранения, определенное в этом теге, будет применяться к соответствующим сообщениям.

Однако если тег удален, определение тега, сохраненное в службе каталогов Active Directory, также удаляется. Это приводит к тому, что помощнику для управляемых папок необходимо обработать все элементы в почтовом ящике и пометить повторно те из них, к которым применяется удаленный тег. В зависимости от количества почтовых ящиков и сообщений этот процесс может вызвать значительное потребление ресурсов на всех серверах почтовых ящиков, которые содержат почтовые ящики с политиками хранения, включающими в себя удаленный тег.

> ⓘ **Важно!**
>
> Если тег хранения удален из политики хранения, срок хранения всех элементов почтового ящика, к которым он применен, по-прежнему будет определяться его параметрами. Чтобы параметры тега не применялись к элементам, необходимо удалить тег. Удалив тег, вы удалите его из всех политик хранения, в которые он включен.

Отключение тега хранения

При отключении тега хранения помощник для управляемых папок пропустит элементы, к которым применен этот тег. Элементы с отключенным тегом хранения никогда не будут перемещаться или удаляться (в зависимости от указанного действия хранения). Так как эти элементы по-прежнему рассматриваются как элементы с тегами, тег политики по умолчанию не применяется к ним. Например, чтобы устранить неполадки с параметрами тегов хранения, можно временно отключить тег хранения, чтобы остановить обработку сообщений с этим тегом помощником по работе с управляемыми папками.

> ⓘ **Примечание**
>
> В поле срока хранения для отключенного тега пользователь видит значение **Никогда**. Если пользователь отметит элемент, который не следует удалять, включение тега в будущем может привести к непреднамеренному удалению элементов. Это также относится к тегам с действием **Переместить в архив**.

Удержание хранения

Параметры хранения можно применять к новым сообщениям пользователей, которые временно отсутствуют на работе и не могут просмотреть почту. В зависимости от политики хранения сообщения могут удаляться или перемещаться в личный архив пользователя. Действие политики хранения для почтового ящика можно приостановить. При этом вы также можете добавить комментарий для пользователя почтового ящика (или другого пользователя, имеющего доступ к этому почтовому ящику) о приостановке хранения, в том числе времени начала и окончания приостановки. Эти комментарии отображаются в поддерживаемых клиентах Outlook. Вы также можете локализовать комментарий на выбранный пользователем язык.

> ⓘ **Примечание**
>
> Приостановка хранения не влияет на то, как обрабатываются квоты на хранение почтовых ящиков. В зависимости от заполнения почтового ящика и применимых квот советуем временно увеличить квоту на хранение почтовых ящиков для пользователей в отпуске или без доступа к почте. Дополнительные сведения о квотах хранилища почтовых ящиков см. в разделе **Настройка квот хранилища для почтового ящика**.

За время отсутствия на работе в почтовых ящиках пользователей может накопиться большой объем электронной почты. В зависимости от объема электронной почты и продолжительности отсутствия разбор сообщений может занять несколько недель. Учитывайте этот фактор время перед отключением приостановки хранения.

Если ваша организация никогда не внедряла MRM и пользователи не знакомы с ее функциями, вы также можете использовать удержание на начальном этапе *подготовки и обучения* развертывания MRM. Можно создать и развернуть политики хранения и обучать пользователей работе с ними без риска перемещения или удаления элементов до овладения пользователями техникой установки тегов. За несколько дней до окончания периода разминки и обучения следует напомнить пользователям о крайнем сроке разминки. По истечении этого периода можно снять с почтовых ящиков пользователей удержание на хранение и разрешить помощнику для управляемых папок обрабатывать элементы почтовых ящиков и применять к ним указанные действия хранения.

Если вы используете гибридную среду Exchange, обратите внимание на следующее поведение: если в Microsoft 365 настроено удержание, `GUID` объект для этого удержания записывается `msExchUserHoldPolicies` в атрибут объекта пользователя, к которому применяется удержание. Затем этот атрибут синхронизируется обратно с

локальная служба Active Directory. Когда MFA обрабатывает почтовый ящик для элементов, которые можно очистить, он обнаруживает `msExchUserHoldPolicies` атрибут . Однако он не может получить сведения о настроенном удержании, так как они недоступны в Exchange Server локальной организации. Чтобы предотвратить удаление данных, которые может потребоваться сохранить, MFA пропускает очистку `DiscoveryHolds` этих элементов из папки в почтовом ящике. Со временем эта папка становится полной, что приводит к тому, что `Recoverable Items` папка достигает своей квоты. Инструкции по устранению этого поведения и рекомендации по настройке см. в статье о полной поддержке папки "Элементы с возможностью восстановления" локального почтового ящика .

Как вычисляется срок хранения в Exchange Server

Статья • 04.04.2023

Помощник для управляемых папок (MFA) — это один из многих вспомогательных процессов, которые выполняются на серверах почтовых ящиков. Его задача — обрабатывать почтовые ящики, к которым применяется политика хранения, добавлять к почтовому ящику теги хранения, включенные в политику, и обрабатывать элементы в почтовом ящике. Если элементы содержат тег хранения, помощник проверяет срок хранения этих элементов. Если заданный срок хранения элемента превышен, выполняется указанное действие хранения. В числе возможных действий перемещение элемента в архив пользователя, удаление элемента с возможностью восстановления или без него.

Дополнительные сведения см. в статье Теги хранения и политики хранения в Exchange Server.

Определение срока хранения элементов различного типа

Срок хранения элементов почтового ящика рассчитывается на основе даты доставки или даты создания (для таких элементов, как черновики, которые были созданы пользователем, но не были доставлены). Когда помощник для управляемых папок обрабатывает элементы в почтовом ящике, он помечает дату начала и дату окончания срока хранения для всех элементов, которые имеют теги хранения с действием хранения **Удалить и разрешить восстановление** или **Удалить навсегда**. Элементы с тегом архивации также помечаются датой перемещения.

Элементы в папке "Удаленные" и элементы, у которых может быть начальная и конечная дата, например элементы календаря (собрания и встречи), а также задачи обрабатываются по-разному, как показано в этой таблице.

Если тип элемента имеет значение ...	И элемент...	Срок хранения рассчитывается на основе...

Если тип элемента имеет значение ...	И элемент...	Срок хранения рассчитывается на основе...
Сообщение электронной почты Документ Факс Элемент дневника Приглашение на собрание, ответ или отмена приглашения Пропущенный вызов Примечания	Не в папке "Удаленные"	Дата доставки или создания
Сообщение электронной почты Документ Факс Элемент дневника Приглашение на собрание, ответ или отмена приглашения Пропущенный вызов Примечания	В папке "Удаленные"	Дата доставки или создания, если элемент не был удален из папки без унаследованного или явного тега хранения. Если элемент находится в папке без унаследованного или явного тега хранения, он не обрабатывается помощником для управляемых папок, следовательно, не содержит начальной даты. Если пользователь удаляет такой элемент, помощник для управляемых папок обрабатывает его в первый раз в папке "Удаленные" и задает текущую дату как начальную.

Если тип элемента имеет значение ...	И элемент...	Срок хранения рассчитывается на основе...
Календарь	Не в папке "Удаленные"	Срок действия неповторяющихся элементов календаря определяется конечной датой. Срок действия повторяющихся элементов календаря определяется конечной датой последнего повторения. Срок хранения повторяющихся элементов календаря, для которых конечная дата не задана, не ограничен.
Календарь	В папке "Удаленные"	Срок действия элемента календаря истекает в соответствии с , `message-received date` если он существует. Если элемент календаря не содержит `message-received date`, срок его действия истекает в соответствии с его `message-creation date`. Если элемент календаря не содержит ни , `message-received date` ни `message-creation date`, срок его действия не истекает.
Задача	Не в папке "Удаленные"	Неповторяющиеся задачи: • Срок действия неповторяющейся задачи истекает в соответствии с , `message-received date` если она существует. • Если у неповторяющейся задачи нет `message-received date`, срок ее действия истекает в соответствии с ее `message-creation date`. • Если у неповторяющейся задачи нет ни , `message-received date` ни `message-creation date`, срок действия не истекает. Срок действия повторяющейся задачи истекает в соответствии с значением `end date` последнего вхождения. Если у повторяющейся задачи нет `end date`, срок ее действия не истекает. Срок хранения восстанавливаемой задачи (повторяющейся задачи, которая создается повторно через указанное время после выполнения предыдущего экземпляра задачи) не ограничен.

Если тип элемента имеет значение ...	И элемент...	Срок хранения рассчитывается на основе...
Задача	В папке "Удаленные"	Срок действия задачи истекает в соответствии с , `message-received date` если она существует. Если задача не имеет `message-received date`, срок ее действия истекает в соответствии с ее `message-creation date`. Если задача не имеет ни , `message-received date` ни `message-creation date`, срок ее действия не истекает.
Contact	В любой папке	Для контактов не устанавливаются даты начала и окончания срока действия, поэтому их пропускает помощник для управляемых папок, а срок их действия не истекает.
Повреждено	В любой папке	Помощник для управляемых папок пропускает поврежденные элементы; срок их действия не ограничен.

Примеры

Если пользователь...	Теги хранения в папке...	Помощник по управляемым папкам...
Получает сообщение в папку "Входящие" 26.01.2016. Удаляет сообщение 27.02.2016.	"Входящие": удаление через 365 дней "Удаленные": удаление через 30 дней	Обрабатывает сообщение в папке "Входящие" 26.01.2016, маркирует его датой начала (26.01.2016) и датой окончания срока действия (26.01.2017). Еще раз обрабатывает сообщение в папке "Удаленные" 27.02.2016. Пересчитывает дату окончания срока действия с учетом той же даты начала (26.01.2016). Поскольку элемент старше 30 дней, срок его действия немедленно прекращается.
Получает сообщение в папку "Входящие" 26.01.2016. Удаляет сообщение 27.02.2016.	"Входящие": нет (наследованный или явный) "Удаленные": удаление через 30 дней	Обрабатывает сообщение в папке "Удаленные" 27.02.2016 и определяет, что элемент не имеет даты начала. Помечает текущую дату как дату начала, а 27.03.2016 — как дату окончания срока действия. Срок действия элемента истекает 27.03.2016, через 30 дней после его удаления или перемещения в папку "Удаленные".

Дополнительные сведения

Элементы в почтовых ящиках, для которых задана приостановка политики хранения, не удаляются, пока приостановка длится.

Если почтовый ящик помещается в In-Place удержание или хранение для судебного разбирательства, элементы с истекающим сроком действия удаляются из папки "Входящие", но сохраняются в папке "Элементы с возможностью восстановления", пока почтовый ящик не будет удален из удержания на месте и удержания для судебного разбирательства в Exchange Server.

В гибридных развертываниях в локальных и Exchange Online организациях должны существовать одни и те же теги хранения и политики хранения, чтобы обеспечить согласованное перемещение и истечение срока действия элементов в обеих организациях. Дополнительные сведения см. в разделе Export and import retention tags.

Создание политики хранения в Exchange Server

Статья • 04.04.2023

Узнайте, как использовать политики хранения для управления жизненным циклом электронной почты в Exchange 2016 и Exchange 2019. Политики хранения применяются путем создания тегов хранения, их добавления к политике хранения и применения этой политики к пользователям почтовых ящиков.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 30 минут
- Для процедур, описанных в этом разделе, требуются определенные разрешения. Сведения о разрешениях см. в каждой процедуре.
- Почтовые ящики, к которым вы применяете политики хранения, должны располагаться на серверах Exchange Server 2010 или более поздних версий.

Этап 1. Создание тега хранения

Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Управление записями обмена сообщениями" в разделе Политика обмена сообщениями и разрешения на соответствие требованиям Exchange Server.

Использование Центра администрирования Exchange для создания тега хранения

1. Перейдите в раздел**Теги хранения** управления >**соответствием**и щелкните **добавить**➕
2. Выберите один из приведенных ниже вариантов.
    - **Автоматически применяется ко всему почтовому ящику (по умолчанию):** создает тег политики по умолчанию (DPT). Теги DPT используются для создания политики удаления по умолчанию и политики архивации по умолчанию, применяемых ко всем элементам почтового ящика.

> ⓘ **Примечание**
>
> В Центре администрирования Exchange невозможно создать тег политики по умолчанию для удаления элементов голосовой почты. Создание таких тегов для удаления элементов голосовой почты показано в приведенном ниже примере кода для командной консоли Exchange.

- **Автоматически применяется к папке по умолчанию**. Создает тег политики хранения (RPT) для папки по умолчанию, например **папки "Входящие"** или **"Удаленные".**

  > ⓘ **Примечание**
  >
  > Создавать теги RPT можно только с действиями **Удалить и разрешить восстановление** или **Окончательно удалить**.

- **Применяется пользователями к элементам и папкам (личным):** создает личные теги. Эти теги позволяют пользователям Outlook и Outlook в Интернете применять параметры архивирования или удаления к сообщению или папкам, которые отличаются от параметров, применяемых к родительской папке или всему почтовому ящику.

3. Название и страницы **создания тега хранения** и параметры на ней различаются в зависимости от типа выбранного тега. Заполните следующие поля:

   - **Имя.** Укажите имя тега хранения. Имена тегов хранения отображаются для пользователей в Outlook и Outlook в Интернете вместе с периодом хранения.

   - **Примените этот тег к следующей папке по умолчанию**: Доступно, только если вы выбрали этот параметр на шаге 2.

   - **Действие хранения**. Выберите одно из следующих действий, которые необходимо выполнить после того, как элемент достигнет срока хранения:

   - **Удалить и разрешить восстановление**. Удаляет элементы, но разрешает пользователям восстанавливать их с помощью параметра **Восстановить удаленные элементы** в Outlook или Outlook в Интернете. Элементы хранятся до истечения периода хранения удаленных элементов,

настроенного для базы данных почтовых ящиков или пользователя почтового ящика.

- **Окончательное удаление**: безвозвратно удаляет элемент из базы данных почтовых ящиков.

  > ⓘ **Важно!**
  >
  > Почтовые ящики и элементы, которые подлежат удержанию на месте и удержанию для судебного разбирательства, хранятся, а также возвращаются поисковыми запросами на обнаружение электронных данных на месте. Дополнительные сведения см. **в статье Удержание на месте и удержание для судебного разбирательства в Exchange Server**.

- **Переместить в архив**. Доступно только при создании DPT или личного тега. Выберите это действие, чтобы переместить элементы в In-Place архив пользователя.

- **Период хранения**. Выберите один из следующих параметров:

- **Никогда**: указывает, что элементы никогда не должны удаляться или перемещаться в архив.

- **Когда элемент достигает следующего возраста (в днях):** указывает количество дней хранения элементов перед их перемещением или удалением. Срок хранения всех поддерживаемых элементов (кроме календаря и задач) начинается с даты их получения или создания. Срок хранения для элементов календаря и задач рассчитывается с учетом даты окончания.

- **Комментарий**: необязательное поле, используемое для административных заметок или примечаний. Поле не отображается для пользователей.

Использование командной консоли Exchange для создания тега хранения

Командлет **New-RetentionPolicyTag** используется для создания тега хранения. Различные параметры, доступные в командлетах, позволяют создавать разные типы тегов хранения. Используйте параметр *Type* для создания DPT (`All`), RPT (укажите тип папки по умолчанию, например `Inbox`) или личный тег (`Personal`).

Эта команда создает тег DPT для удаления всех сообщений из почтового ящика после 7 лет (2556 дней).

```
PowerShell

New-RetentionPolicyTag -Name "DPT-Corp-Delete" -Type All -
AgeLimitForRetention 2556 -RetentionAction DeleteAndAllowRecovery
```

Эта команда создает тег DPT для перемещения всех сообщений в личный архив после 2 лет (730 дней).

```
PowerShell

New-RetentionPolicyTag -Name "DPT-Corp-Move" -Type All -AgeLimitForRetention
730 -RetentionAction MoveToArchive
```

Эта команда создает тег DPT для удаления сообщений голосовой почты после 20 дней.

```
PowerShell

New-RetentionPolicyTag -Name "DPT-Corp-Voicemail" -Type All -MessageClass
Voicemail -AgeLimitForRetention 20 -RetentionAction DeleteAndAllowRecovery
```

Эта команда создает тег RPT для окончательного удаления сообщений из папки нежелательной почты после 30 дней.

```
PowerShell

New-RetentionPolicyTag -Name "RPT-Corp-JunkMail" -Type JunkEmail -
AgeLimitForRetention 30 -RetentionAction PermanentlyDelete
```

Эта команда создает личный тег для запрета на удаление сообщения.

```
PowerShell

New-RetentionPolicyTag -Name "Never Delete" -Type Personal -RetentionAction
DeleteAndAllowRecovery -RetentionEnabled $false
```

Этап 2. Создание политики хранения

Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Управление

записями обмена сообщениями" в разделе Политика обмена сообщениями и разрешения на соответствие требованиям Exchange Server.

Использование Центра администрирования Exchange для создания политики хранения

1. Перейдите в раздел**Политики хранения** управления >**соответствием**и щелкните **Добавить**➕

2. В области **Новая политика хранения** заполните следующие поля:

   - **Имя**. Введите имя для политики хранения.
   - **Теги хранения. Щелкните**➕ Чтобы выбрать теги, которые нужно добавить в эту политику хранения.

     Политика хранения может содержать перечисленные ниже теги хранения.

     - Один тег политики по умолчанию с действием **Переместить в архив**
     - Один тег DPT с действиями **Удалить и разрешить восстановление** или **Окончательно удалить**
     - Один тег DPT для голосовых сообщений с действиями **Удалить и разрешить восстановление** или **Окончательно удалить**
     - Один тег RPT для каждой папки по умолчанию (например, **Входящие**) для удаления элементов
     - Любое количество личных тегов

     > ⓘ **Примечание**
     >
     > Можно добавлять любое количество личных тегов в политику хранения, но наличие нескольких личных тегов с различными параметрами хранения может запутать пользователей. Рекомендуется связывать с политикой хранения не более десяти личных тегов.

   Можно создать политику хранения без тегов, но элементы в почтовом ящике, к которым данная политика применяется, не будут перемещены или удалены. Можно также добавлять и удалять теги хранения в такой политике после ее создания.

Использование командной консоли Exchange для создания политики хранения

В этом примере создается политика хранения RetentionPolicy-Corp и используется параметр *RetentionPolicyTagLinks* для связывания пяти тегов с политикой.

PowerShell

```
New-RetentionPolicy "RetentionPolicy-Corp" -RetentionPolicyTagLinks "DPT-Corp-Delete","DPT-Corp-Move","DPT-Corp-Voicemail","RPT-Corp-JunkMail","Never Delete"
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе New-RetentionPolicy.

Действие 3. Применение политики хранения к пользователям почтовых ящиков

После того как вы создали политику хранения, ее следует применить к пользователям почтовых ящиков. Вы можете применять разные политики хранения к различным группам пользователей. Подробные инструкции см. в статье Применение политики хранения к почтовым ящикам в Exchange Server.

Как убедиться, что это сработало?

После того как вы создали теги хранения, добавили их к политике, а политику применили к пользователям почтовых ящиков, помощник по обслуживанию почтовых ящиков управления записями сообщений при следующей обработке почтового ящика удалит или переместит сообщения согласно параметрам, заданным в тегах хранения.

Чтобы убедиться, что вы успешно применили политику хранения, выполните следующие действия.

1. Выполните приведенную ниже команду в командной консоли Exchange, чтобы вручную запустить помощник по управлению записями сообщений для одного почтового ящика.

   PowerShell

   ```
   Start-ManagedFolderAssistant -Identity <mailbox identity>
   ```

2. Войдите в почтовый ящик с помощью приложения Outlook или Outlook в Интернете и убедитесь, что сообщения удалены или перемещены в архив в соответствии с настройками политики.

Теги хранения и политики хранения в Exchange Server

Статья • 31.01.2025

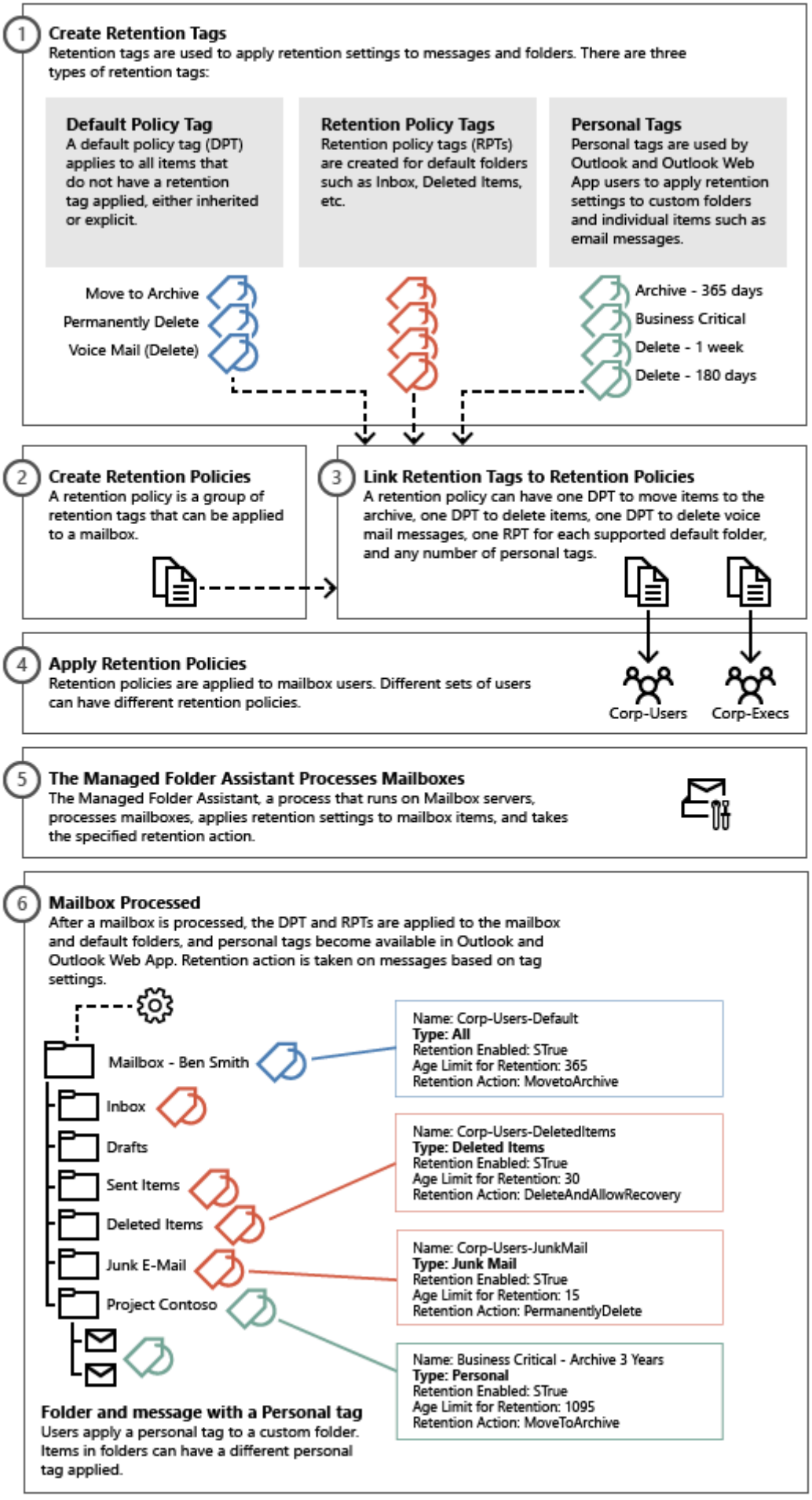
Технология "Управление записями сообщений" помогает организациям снизить юридические риски, связанные с электронной почтой и другими видами связи. Она позволяет хранить сообщения в соответствии с политикой компании или требованиями законодательства, а также удалять содержимое, не имеющее юридической или коммерческой ценности.

Стратегия управления записями сообщений

MrM в Exchange Server выполняется с помощью *тегов хранения* и *политик хранения*. Перед тем как подробно обсудить каждую из этих функций, давайте рассмотрим, как они используются в общей стратегии управления записями сообщений.

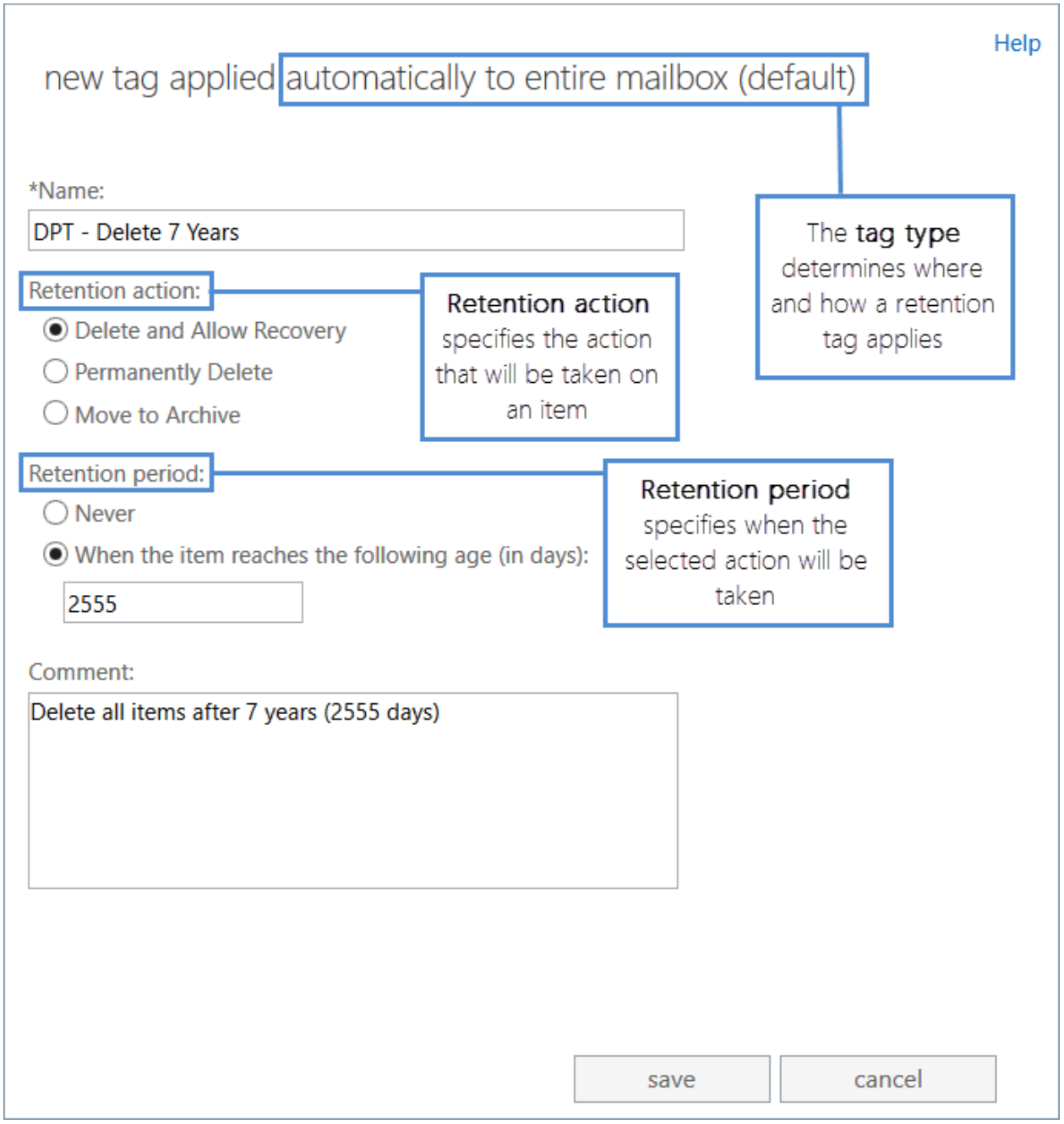
- Назначение *тегов политики хранения* (RPT) папкам по умолчанию, например папке "Входящие" и "Удаленные".
- Применение *тегов политики по умолчанию* (DPT) к почтовым ящикам для управления хранением всех элементов без тегов.
- Разрешение пользователю назначать *личные теги* настраиваемым папкам и отдельным элементам.
- Отделение функций управления записями сообщений от управления папками "Входящие" пользователей и обычных способов хранения файлов. Пользователи могут не применять требования хранения при хранении сообщений в управляемых папках. Отдельные сообщения могут иметь тег хранения, отличный от применяемого к папке, в которой они расположены.

На следующем рисунке показаны задачи, участвующие в реализации этой стратегии.


1
Create Retention Tags
Retention tags are used to apply retention settings to messages and folders. There are three types of retention tags:
Default Policy Tag
A default policy tag (DPT) applies to all items that do not have a retention tag applied, either inherited or explicit.
Retention Policy Tags
Retention policy tags (RPTs) are created for default folders such as Inbox, Deleted Items, etc.
Personal Tags
Personal tags are used by Outlook and Outlook Web App users to apply retention settings to custom folders and individual items such as email messages.
Move to Archive
Permanently Delete
Voice Mail (Delete)
Archive - 365 days
Business Critical
Delete - 1 week
Delete - 180 days
2
Create Retention Policies
A retention policy is a group of retention tags that can be applied to a mailbox.
3
Link Retention Tags to Retention Policies
A retention policy can have one DPT to move items to the archive, one DPT to delete items, one DPT to delete voice mail messages, one RPT for each supported default folder, and any number of personal tags.
4
Apply Retention Policies
Retention policies are applied to mailbox users. Different sets of users can have different retention policies.
Corp-Users
Corp-Execs
5
The Managed Folder Assistant Processes Mailboxes
The Managed Folder Assistant, a process that runs on Mailbox servers, processes mailboxes, applies retention settings to mailbox items, and takes the specified retention action.
6
Mailbox Processed
After a mailbox is processed, the DPT and RPTs are applied to the mailbox and default folders, and personal tags become available in Outlook and Outlook Web App. Retention action is taken on messages based on tag settings.
Mailbox - Ben Smith
Inbox
Drafts
Sent Items
Deleted Items
Junk E-Mail
Project Contoso
Name: Corp-Users-Default
Type: All
Retention Enabled: STrue
Age Limit for Retention: 365
Retention Action: MovetoArchive
Name: Corp-Users-DeletedItems
Type: Deleted Items
Retention Enabled: STrue
Age Limit for Retention: 30
Retention Action: DeleteAndAllowRecovery
Name: Corp-Users-JunkMail
Type: Junk Mail
Retention Enabled: STrue
Age Limit for Retention: 15
Retention Action: PermanentlyDelete
Name: Business Critical - Archive 3 Years
Type: Personal
Retention Enabled: STrue
Age Limit for Retention: 1095
Retention Action: MoveToArchive
Folder and message with a Personal tag
Users apply a personal tag to a custom folder. Items in folders can have a different personal tag applied.

Теги хранения

Как видите, теги хранения используются для применения параметров хранения к папкам и отдельным элементам, таким как сообщения электронной почты и голосовая почта. Эти параметры определяют, как долго сообщение остается в почтовом ящике, а также действие, которое необходимо выполнить, когда сообщение достигает указанного срока хранения. По истечении срока хранения сообщение перемещается в архив пользователя на месте или удаляется.



Теги хранения позволяют пользователям отмечать собственные папки почтовых ящиков и отдельные элементы для хранения. Теперь пользователи могут не применять требования к хранению элементов в управляемых папках, подготовленных администратором.

Типы тегов хранения

Теги хранения разделены на следующие три типа в зависимости от того, кто может их применять и где именно в почтовом ящике их можно применять.

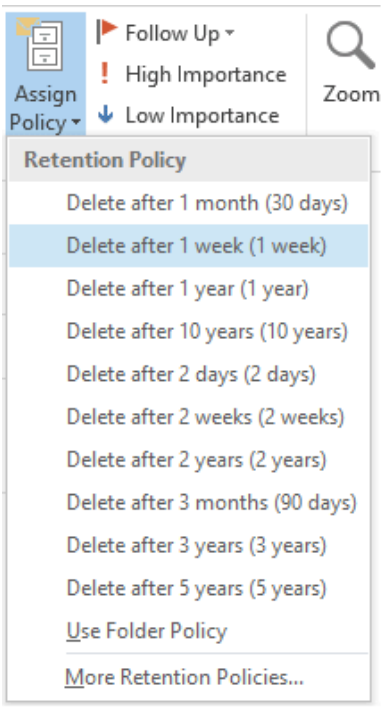
Развернуть таблицу

Тип тега хранения	Прикладной...	Кем применяется...	Доступные действия...	Сведения
Тег политики по умолчанию (DPT)	Автоматически ко всему почтовому ящику DPT применяется к *элементам без тегов* , которые являются элементами почтового ящика, к которым не применяется тег хранения напрямую или по наследованию из папки.	Администратор	Переместить в архив Удалить и разрешить восстановление Удалить окончательно	Пользователи не могут изменить теги DPT, примененные к почтовому ящику.
Тег политики хранения (RPT)	Автоматически к папке по умолчанию Папки по умолчанию — это папки, которые автоматически создаются во всех почтовых ящиках, например: **Входящие**, **Удаленные** и **Отправленные**. Список поддерживаемых папок по умолчанию см. в разделе Default folders that support Retention Policy Tags.	Администратор	Удалить и разрешить восстановление Удалить окончательно	Пользователи не могут изменить теги RPT, примененные к папке по умолчанию.

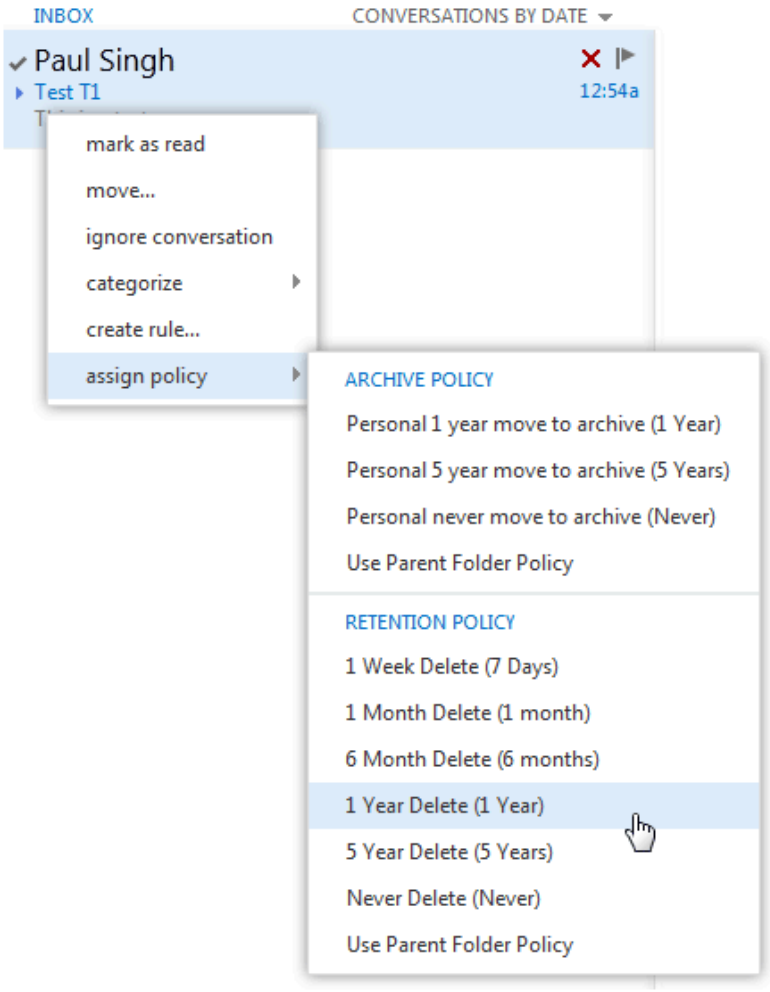
Тип тега хранения	Прикладной...	Кем применяется...	Доступные действия...	Сведения
Личный тег	Вручную к элементам и папкам Пользователи могут автоматизировать применение тегов, используя правила папки "Входящие", чтобы перемещать сообщение в папку, к которой применен определенный тег, или применять личный тег к сообщению.	Пользователи	Переместить в архив Удалить и разрешить восстановление Удалить окончательно	Личные теги позволяют пользователям определить, как долго будет храниться элемент. Например, к почтовому ящику может быть применен тег DPT для удаления элементов через семь лет, но пользователь может с помощью личного тега создать исключение для таких элементов, как информационные бюллетени и автоматические уведомления, чтобы удалять их через три дня.

Дополнительные сведения о личных тегах

Личные теги доступны пользователям Outlook и Outlook в Интернете в рамках их политики хранения. В Outlook и Outlook в Интернете личные теги с действием **Переместить в архив** представлены в списке **Политика архивации**, а личные теги с действиями **Удалить и разрешить восстановление** или **Окончательно удалить** — в списке **Политика хранения**, как показано ниже:



Outlook



Outlook on the web

Пользователи могут применять личные теги к папкам, которые они создают, или отдельным элементам. Сообщения с личными тегами всегда обрабатываются с учетом параметров этих тегов. Пользователи могут помечать личными тегами сообщения, чтобы те удалялись или перемещались до или после запланированного применения к их почтовому ящику параметров, указанных в тегах DPT или RPT. Также можно создавать личные теги с отключенной возможностью хранения. Это позволяет пользователям устанавливать теги на элементы, чтобы они никогда не переносились в архив и срок их действия никогда не истекал.

> ⓘ **Примечание**
>
> Пользователи могут применять политики архива к папкам по умолчанию, папкам и подпапкам, созданным пользователями, или отдельным элементам. Пользователи могут применять политику хранения к папкам или подпапкам, созданным пользователями, и отдельным элементам (в том числе к подпапкам и элементам в папке по умолчанию), но не к папкам по умолчанию.

Пользователи также могут использовать Центр администрирования Exchange (EAC) для выбора дополнительных личных тегов, которые не связаны с политикой хранения. Затем выбранные теги становятся доступными в Outlook и Outlook в Интернете. Чтобы пользователь мог выбирать дополнительные теги в Центре администрирования Exchange, необходимо добавить роль MyRetentionPolicies Role в его политику назначения ролей. Дополнительные сведения о политиках назначения ролей для пользователей см. в статье Understanding Management Role Assignment Policies. Если разрешить пользователям выбирать дополнительные личные теги, все личные теги в организации Exchange становятся доступными для них.

> ⓘ **Примечание**
>
> Личные теги — это расширенная функция. Для почтовых ящиков с политиками, содержащими эти теги (или как результат добавления пользователями этих тегов к своим почтовым ящикам), требуется корпоративная клиентская лицензия Exchange (CAL).

Период хранения

При включении тега хранения необходимо указать для него срок хранения. Этот срок определяет количество дней, в течение которых сообщение будет храниться в почтовом ящике пользователя после его доставки.

Расчет срока хранения для неповторяющихся элементов (таких как сообщения электронной почты) отличается от расчета для элементов, имеющих дату окончания, или повторяющихся элементов (таких как собрания и задачи). Сведения о том, как вычисляется срок хранения для различных типов элементов, см. в статье Как вычисляется срок хранения в Exchange Server.

Можно также создавать теги хранения с отключенной функцией хранения или отключать теги после их создания. Так как сообщения, к которым применен отключенный тег, не обрабатываются, действия хранения к ним не применяются. В результате можно использовать отключенный личный тег, например **Никогда не перемещать** или **Никогда не удалять**, для переопределения тега политики по умолчанию или тега политики хранения, которые в противном случае будут применяться к сообщению.

Действия сохранения

При создании или настройке тега хранения можно выбрать одно из следующих действий по истечении срока хранения элемента:

Развернуть таблицу

Действие сохранения	Принятые меры...	Кроме...
Переместить в архив	Перемещает сообщение в архивный почтовый ящик пользователя Доступно только для DPT и личных тегов Дополнительные сведения о архивации см. в статье Архивация на месте в Exchange Server.	Если у пользователя нет архивного почтового ящика, действие не выполняется.
Удаление и разрешение восстановления:	Аналогично ситуации, когда пользователь очищает папку "Удаленные". Элементы перемещаются в папку "Элементы с возможностью восстановления" в Exchange Server почтового ящика и сохраняются до истечения срока *хранения удаленных элементов*. Пользователь получает еще одну возможность восстановить элемент в диалоговом окне **Восстановление удаленных элементов** в Outlook или Outlook в Интернете.	Если срок хранения удаленных элементов равен нулю дней, элементы удаляются без возможности восстановления. Дополнительные сведения см. в разделе Настройка квот на хранение удаленных элементов и восстанавливаемых элементов.
Удалить без возможности восстановления	Окончательно удаляет сообщения. После этого сообщения не могут быть восстановлены.	Если почтовый ящик помещается на удержание на месте и удержание для судебного разбирательства в Exchange Server или судебного разбирательства, элементы сохраняются в папке "Элементы с возможностью восстановления" на основе параметров удержания. Обнаружение электронных данных на месте в Exchange Server по-

Действие сохранения	Принятые меры...	Кроме...
		прежнему будет возвращать эти элементы в результатах поиска.
Установить отметку "Срок хранения истек"	Помечает сообщение как просроченное. В Outlook и Outlook в Интернете элементы с истекшим сроком действия отображаются с уведомлением "Срок действия этого элемента истек" и "Срок действия этого элемента истек через 0 дней".	N. O.

> ⓘ **Примечание**
>
> Тег политики по умолчанию (DPT) с **действием Переместить в Архив** всегда перезаписывает тег политики хранения (RPT) или личный тег (PT), если предельный срок хранения DPT ниже RPT или PT.

Дополнительные сведения о создании тегов хранения см. в статье Создание политики хранения в Exchange Server.

Политики хранения

Чтобы применить один или несколько тегов хранения к почтовому ящику, необходимо добавить их в политику хранения, а затем применить политику к почтовым ящикам. Почтовый ящик не может иметь более одной политики хранения. Теги хранения можно связать с политикой хранения или отсоединить от нее в любое время, и изменения автоматически вступают в силу для всех почтовых ящиков, в которых применена политика.

Политика хранения может иметь следующие теги хранения.

Развернуть таблицу

Тип тега хранения	Теги в политике
Тег политики по умолчанию (DPT)	Один тег DPT с действием **Переместить в архив**

Тип тега хранения	Теги в политике
	Один DPT с действиями **"Удалить" и "Разрешить восстановление**" или **"Окончательное удаление"** Один тег DPT с действиями **Удалить и разрешить восстановление** или **Удалить окончательно** для сообщений голосовой почты
Теги политики хранения	Один тег политики хранения для каждой поддерживаемой папки по умолчанию **Примечание.** Нельзя связать несколько RPT для определенной папки по умолчанию (например **, Удаленные элементы**) с одной и той же политикой хранения.
Личные теги	Любое количество личных тегов **Примечание.** Многие личные теги в политике могут сбить пользователей с толку. Мы рекомендуем связывать с политикой хранения не более 10 личных тегов.

> ⓘ **Примечание**
>
> С политикой хранения можно не связывать теги хранения, но рекомендуется использовать такой сценарий. Если к почтовому ящику применена политика хранения, с которой не связаны теги хранения, срок хранения элементов этого почтового ящика будет не ограничен.

Политика хранения может включать в себя архивные теги (теги, перемещающие элементы в личный архивный почтовый ящик) вместе с тегами удаления (тегами, удаляющими элементы). К элементу почтового ящика также могут одновременно применяться эти два типа тегов. Архивные почтовые ящики не имеют отдельной политики хранения. К основному и архивному почтовым ящикам применяется одна политика хранения.

When planning to create retention policies, you must consider whether they'll include both archive and deletion tags. As mentioned earlier, a retention policy can have one DPT that uses the **Move to archive** action and one DPT that uses either the **Delete and allow recovery** or **Permanently delete** action. The DPT with the **Move to archive** action must have a lower retention age than the DPT with a deletion action. For example, you can use a DPT with the **Move to archive** action to move items to the archive mailbox in two years, and a DPT with a deletion action to remove items from the mailbox in seven years. Items in both primary and archive mailboxes will be deleted after seven years.

Политика хранения по умолчанию

Программа установки Exchange создает политику хранения **Default MRM Policy**. Политика автоматически применяется, если вы создаете архив для нового пользователя и не указываете политику хранения.

Вы можете изменить теги, включенные в политику MRM по умолчанию, например путем изменения срока хранения или действия хранения, отключения тега или изменения политики путем добавления или удаления тегов из него. Обновленная политика применяется к почтовым ящикам при следующей обработке помощником по управляемым папкам (MFA).

Дополнительные сведения, в том числе список тегов сохранения, связанных с политикой, см. в статье Default Retention Policy.

Помощник по работе с управляемыми папками

Помощник для управляемых папок — помощник по обслуживанию почтовых ящиков, работающий на серверах почтовых ящиков, — обрабатывает почтовые ящики, к которым применена политика хранения.

Помощник для управляемых папок применяет политику хранения путем проверки элементов в почтовом ящике и определения того, являются ли они субъектами хранения. Затем он помечает элементы, которые необходимо хранить, с помощью соответствующих тегов хранения и применяет указанное действие хранения к элементам с истекшим сроком хранения.

Помощник для управляемых папок функционирует на основе регулировки. Помощники такого типа работают непрерывно и не требуют планирования. Системные ресурсы, которые они могут расходовать, регулируются. Помощник для управляемых папок можно настроить на обработку всех почтовых ящиков на сервере почтовых ящиков в течение определенного периода (известного как *рабочий цикл*). Помимо этого, через заданный интервал времени в момент, называемый *контрольной точкой рабочего цикла*, помощник обновляет список обрабатываемых почтовых ящиков. В процессе обновления помощник добавляет вновь созданные или перемещенные почтовые ящики в очередь. Он также изменяет приоритеты для существующих почтовых ящиков, которые не были успешно обработаны из-за сбоев, и перемещает их на более высокое место в очереди, чтобы их можно было обработать за тот же рабочий цикл.

Чтобы запустить помощник вручную для обработки определенного почтового ящика, используйте командлет Start-ManagedFolderAssistant. Дополнительные

сведения см. в статье Настройка и запуск помощника по управляемым папкам в Exchange Server.

> ⓘ **Примечание**
>
> Помощник для управляемых папок не выполняет действия над сообщениями, которые не являются субъектами хранения (для которых отключены теги хранения). Можно также отключить тег хранения, чтобы временно приостановить обработку элементов с этим тегом.

Перемещение элементов между папками

Элемент почтового ящика, перемещенный из одной папки в другую, наследует все теги, примененные к папке, в которую он перемещен. Если элемент перемещен в папку, для которой не назначен тег хранения, к ней применяется тег DPT. Если элемент имеет явно назначенный тег, этот тег всегда имеет приоритет над тегами папок или тегом по умолчанию.

Применение тега хранения к папке в архиве

Когда пользователь применяет личный тег к папке в архиве, если папка с таким же именем существует в основном почтовом ящике и имеет другой тег, тег в этой папке в архиве изменяется в соответствии с тегом в основном почтовом ящике. Это позволяет избежать путаницы, связанной с элементами в папке в архиве, с поведением срока действия, отличным от того, что и в той же папке в основном почтовом ящике пользователя. Например, у пользователя есть папка с именем Project Contoso в основном почтовом ящике с тегом *Delete - 3 года* , а папка Project Contoso также существует в архивном почтовом ящике. Если пользователь применяет личный тег *Delete — 1 год* для удаления элементов в папке через 1 год. При повторной обработке почтового ящика папка возвращается к тегу Delete — 3 года.

Удаление тега хранения из политики хранения

После удаления тега хранения из примененной к почтовому ящику политики хранения этот тег становится недоступным пользователю и его невозможно применять к элементам почтового ящика.

Существующие элементы, помеченные этим тегом, будут по-прежнему обрабатываться помощником по работе с управляемыми папками на основе

параметров этого тега, а действие хранения, определенное в этом теге, будет применяться к соответствующим сообщениям.

Однако если тег удален, определение тега, сохраненное в службе каталогов Active Directory, также удаляется. Это приводит к тому, что помощнику для управляемых папок необходимо обработать все элементы в почтовом ящике и пометить повторно те из них, к которым применяется удаленный тег. В зависимости от количества почтовых ящиков и сообщений этот процесс может вызвать значительное потребление ресурсов на всех серверах почтовых ящиков, которые содержат почтовые ящики с политиками хранения, включающими в себя удаленный тег.

> ⓘ **Важно!**
>
> Если тег хранения удален из политики хранения, срок хранения всех элементов почтового ящика, к которым он применен, по-прежнему будет определяться его параметрами. Чтобы параметры тега не применялись к элементам, необходимо удалить тег. Удалив тег, вы удалите его из всех политик хранения, в которые он включен.

Отключение тега хранения

При отключении тега хранения помощник для управляемых папок пропустит элементы, к которым применен этот тег. Элементы с отключенным тегом хранения никогда не будут перемещаться или удаляться (в зависимости от указанного действия хранения). Так как эти элементы по-прежнему рассматриваются как элементы с тегами, тег политики по умолчанию не применяется к ним. Например, чтобы устранить неполадки с параметрами тегов хранения, можно временно отключить тег хранения, чтобы остановить обработку сообщений с этим тегом помощником по работе с управляемыми папками.

> ⓘ **Примечание**
>
> В поле срока хранения для отключенного тега пользователь видит значение **Никогда**. Если пользователь отметит элемент, который не следует удалять, включение тега в будущем может привести к непреднамеренному удалению элементов. Это также относится к тегам с действием **Переместить в архив**.

Удержание хранения

Параметры хранения можно применять к новым сообщениям пользователей, которые временно отсутствуют на работе и не могут просмотреть почту. В зависимости от политики хранения сообщения могут удаляться или перемещаться в личный архив пользователя. Действие политики хранения для почтового ящика можно приостановить. При этом вы также можете добавить комментарий для пользователя почтового ящика (или другого пользователя, имеющего доступ к этому почтовому ящику) о приостановке хранения, в том числе времени начала и окончания приостановки. Эти комментарии отображаются в поддерживаемых клиентах Outlook. Вы также можете локализовать комментарий на выбранный пользователем язык.

> ⓘ **Примечание**
>
> Приостановка хранения не влияет на то, как обрабатываются квоты на хранение почтовых ящиков. В зависимости от заполнения почтового ящика и применимых квот советуем временно увеличить квоту на хранение почтовых ящиков для пользователей в отпуске или без доступа к почте. Дополнительные сведения о квотах хранилища почтовых ящиков см. в разделе **Настройка квот хранилища для почтового ящика**.

За время отсутствия на работе в почтовых ящиках пользователей может накопиться большой объем электронной почты. В зависимости от объема электронной почты и продолжительности отсутствия разбор сообщений может занять несколько недель. Учитывайте этот фактор время перед отключением приостановки хранения.

Если ваша организация никогда не внедряла MRM и пользователи не знакомы с ее функциями, вы также можете использовать удержание на начальном этапе *подготовки и обучения* развертывания MRM. Можно создать и развернуть политики хранения и обучать пользователей работе с ними без риска перемещения или удаления элементов до овладения пользователями техникой установки тегов. За несколько дней до окончания периода разминки и обучения следует напомнить пользователям о крайнем сроке разминки. По истечении этого периода можно снять с почтовых ящиков пользователей удержание на хранение и разрешить помощнику для управляемых папок обрабатывать элементы почтовых ящиков и применять к ним указанные действия хранения.

Если вы используете гибридную среду Exchange, обратите внимание на следующее поведение: если в Microsoft 365 настроено удержание, `GUID` объект для этого удержания записывается `msExchUserHoldPolicies` в атрибут объекта пользователя, к которому применяется удержание. Затем этот атрибут синхронизируется обратно с

локальная служба Active Directory. Когда MFA обрабатывает почтовый ящик для элементов, которые можно очистить, он обнаруживает `msExchUserHoldPolicies` атрибут . Однако он не может получить сведения о настроенном удержании, так как они недоступны в Exchange Server локальной организации. Чтобы предотвратить удаление данных, которые может потребоваться сохранить, MFA пропускает очистку `DiscoveryHolds` этих элементов из папки в почтовом ящике. Со временем эта папка становится полной, что приводит к тому, что `Recoverable Items` папка достигает своей квоты. Инструкции по устранению этого поведения и рекомендации по настройке см. в статье о полной поддержке папки "Элементы с возможностью восстановления" локального почтового ящика .

Применение политики хранения к почтовым ящикам в Exchange Server

Статья • 04.04.2023

Политики хранения позволяют группировать один или несколько тегов хранения и применять их к почтовым ящикам для включения параметров хранения сообщений. Почтовый ящик не может иметь более одной политики хранения.

> ⊗ **Внимание!**
>
> Срок действия сообщений истекает на основании параметров, определенных тегами хранения, связанными с политикой. Эти параметры включают такие действия, как перемещение сообщений в архив или их окончательное удаление. Перед применением политики хранения к одному или нескольким почтовым ящикам рекомендуется проверить политику и каждый связанный с ней тег хранения.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Применение политик хранения" в разделе Политика обмена сообщениями и разрешения на соответствие требованиям Exchange Server.

Использование Центра администрирования Exchange для применения политики хранения к одному почтовому ящику

1. Перейдите в раздел **Почтовые ящики**>**получателей**.
2. В представлении списка выберите почтовый ящик, к которому требуется применить политику хранения, и нажмите кнопку **Изменить**.✎
3. В разделе **Почтовый ящик пользователя** выберите **Функции почтового ящика**.

4. В списке **Политика хранения** выберите политику, которую необходимо назначить почтовому ящику, и нажмите кнопку **Сохранить**.

Использование Центра администрирования Exchange для применения политики хранения к нескольким почтовым ящикам

1. Перейдите в раздел **Почтовые ящики**>**получателей**.
2. В представлении списка воспользуйтесь клавишами SHIFT или CTRL, чтобы выбрать несколько почтовых ящиков.
3. В области сведений щелкните **Дополнительные параметры**.
4. В разделе **Политика хранения** щелкните **Обновить**.
5. В разделе **Групповое назначение политики хранения** выберите необходимую политику хранения, а затем щелкните **Сохранить**.

Использование командной консоли Exchange для применения политики хранения к одному почтовому ящику

В этом примере показано применение политики хранения RP-Finance к почтовому ящику пользователя Morris.

PowerShell

```
Set-Mailbox "Morris" -RetentionPolicy "RP-Finance"
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Set-Mailbox.

Использование командной консоли Exchange для применения политики хранения к нескольким почтовым ящикам

В этом примере выполняется применение новой политики хранения New-Retention-Policy ко всем почтовым ящикам, для которых используется старая политика Old-Retention-Policy.

PowerShell

```
$OldPolicy=(Get-RetentionPolicy "Old-Retention-Policy").distinguishedName
Get-Mailbox -Filter "RetentionPolicy -eq '$OldPolicy'" -Resultsize Unlimited
| Set-Mailbox -RetentionPolicy "New-Retention-Policy"
```

В этом примере показано, как применить политику хранения RetentionPolicy-Corp для всех почтовых ящиков в организации Exchange.

PowerShell

```
Get-Mailbox -ResultSize unlimited | Set-Mailbox -RetentionPolicy
"RetentionPolicy-Corp"
```PowerShell

This example applies the retention policy RetentionPolicy-Finance to all
mailboxes in the Finance organizational unit.

```PowerShell
Get-Mailbox -OrganizationalUnit "Finance" -ResultSize Unlimited | Set-
Mailbox -RetentionPolicy "RetentionPolicy-Finance"
```

Дополнительные сведения о синтаксисе и параметрах см. в разделах Get-Mailbox и Set-Mailbox.

Как проверить, все ли получилось?

Чтобы убедиться, что вы применили политику хранения, выполните командлет Get-Mailbox для получения политики хранения почтового ящика или почтовых ящиков.

В этом примере возвращаются политики хранения для почтового ящика пользователя Morris.

PowerShell

```
Get-Mailbox Morris | Select RetentionPolicy
```

Эта команда возвращает все почтовые ящики, имеющие политику хранения RP-Finance.

PowerShell

```
Get-Mailbox -ResultSize unlimited | Where-Object {$_.RetentionPolicy -eq
"RP-Finance"} | Format-Table Name,RetentionPolicy -Auto
```

Настройка и запуск помощника по управляемым папкам в Exchange Server

Статья • 04.04.2023

Помощник по управляемым папкам (MFA) — это помощник по почтовым ящикам Exchange, который применяет и обрабатывает параметры хранения сообщений, настроенные в политиках хранения.

Как и в Exchange 2013, помощник по управляемым папкам в Exchange 2016 и Exchange 2019 — это всегда работающий помощник на основе регулирования. MFA не нуждается в планировании, и вы можете управлять объемом потребляемых им системных ресурсов. Помощник для управляемых папок можно настроить на обработку всех почтовых ящиков на сервере почтовых ящиков в течение определенного периода времени, называемого *рабочим циклом*. По умолчанию рабочий цикл MFA составляет один день (MFA ежедневно обрабатывает все почтовые ящики на сервере).

Вы также можете принудительно проверить указанный почтовый ящик с помощью MFA.

Что нужно знать перед началом работы

- Для выполнения этой процедуры можно использовать только PowerShell. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Хотя параметр *ManagedFolderAssistantSchedule* доступен в Exchange Server, он не работает на серверах Exchange 2016 или Exchange 2019. Он используется только для сосуществования с предыдущими версиями Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Управление записями обмена сообщениями" в разделе Политика обмена сообщениями и разрешения на соответствие требованиям Exchange Server.

Настройка помощника по обслуживанию управляемых папок

Чтобы настроить интервал обработки почтовых ящиков в MFA, необходимо выполнить два действия:

1. Настройка рабочего цикла MFA.
2. Применение нового значения рабочего цикла для MFA.

Этап 1. Настройка рабочего цикла помощника для управляемых папок с помощью командной консоли Exchange

Чтобы настроить рабочий цикл для MFA, используйте следующий синтаксис:

```
PowerShell

New-SettingOverride -Name "<UniqueOverrideName>" -Component
TimeBasedAssistants -Section ELCAssistant -Parameters @("WorkCycle=
<Timespan>") -Reason "<DescriptiveReason>" [-Server <ServerName>]
```

Примечания:

- Чтобы указать *<значение TimeSpan>* , используйте синтаксис `d.hh:mm:ss`, где *d = дни*, *чч = часы*, *мм = минуты* и *ss = секунды* .
- Чтобы настроить один рабочий цикл для MFA на всех серверах почтовых ящиков Exchange 2016 и Exchange 2019 в лесу Active Directory, не используйте параметр *Server* .
- Чтобы настроить рабочий цикл для MFA на определенном сервере почтовых ящиков Exchange 2016 и Exchange 2019, используйте параметр *Server* и имя сервера (не полное доменное имя или полное доменное имя). Применяйте этот метод, чтобы настроить разные рабочие циклы MFA на разных серверах Exchange Server.

В этом примере задается рабочий цикл MFA продолжительностью в два дня (MFA обрабатывает почтовые ящики каждые два дня). Так как мы не используем параметр *Server* , параметр применяется ко всем серверам почтовых ящиков Exchange 2016 и Exchange 2019 в организации.

- **Задание имени переопределения**: "MFA WorkCycle Override" (должно быть уникальным)
- **WorkCycle**: `2.00:00:00` (2 дня; обратите внимание, что значение `2`также работает)

- **Причина переопределения**: обработка почтовых ящиков каждые 2 дня

```
PowerShell

New-SettingOverride -Name "MFA WorkCycle Override" -Component
TimeBasedAssistants -Section ELCAssistant -Parameters
@("WorkCycle=2.00:00:00") -Reason "Process mailboxes every 2 days"
```

Эта команда указывает такой же 2-дневный рабочий цикл для MFA, но только на сервере Mailbox01.

```
PowerShell

New-SettingOverride -Name "Mailbox01 MFA WorkCycle Override" -Component
TimeBasedAssistants -Section ELCAssistant -Parameters
@("WorkCycle=2.00:00:00") -Reason "Process mailboxes every 2 days" -Server
Mailbox01
```

Этап 2. Применение нового значения рабочего цикла помощника для управляемых папок с помощью командной консоли Exchange

Чтобы применить новое значение рабочего цикла для MFA, используйте следующий синтаксис:

```
PowerShell

Get-ExchangeDiagnosticInfo -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh [-Server <ServerName>]
```

Примечания:

- Если вы не использовали параметр *Server* на шаге 1, не используйте его здесь. Если вы использовали параметр *Server* на шаге 1, используйте здесь то же имя сервера.
- Если вы удаляете собственное значение рабочего цикла для MFA с помощью командлета **Remove-SettingOverride**, вам все равно нужно выполнить эту команду, чтобы восстановить рабочий цикл по умолчанию (каждый день).

В этом примере применяется новое значение рабочего цикла для MFA на всех серверах почтовых ящиков Exchange 2016 и Exchange 2019 в организации.

PowerShell

```
Get-ExchangeDiagnosticInfo -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh
```

Эта команда применяет новое значение рабочего цикла для MFA на сервере Mailbox01.

PowerShell

```
Get-ExchangeDiagnosticInfo -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh -Server Mailbox01
```

Как проверить, все ли получилось?

Чтобы убедиться, что рабочий цикл помощника по управляемым папкам успешно настроен на одном или нескольких серверах, *замените*< *serverName*> именем сервера (а не полным доменным именем) и выполните следующую команду, чтобы проверить значение свойства **WorkCycle**:

PowerShell

```
[xml]$diag=Get-ExchangeDiagnosticInfo -Server <ServerName> -Process
MSExchangeMailboxAssistants -Component VariantConfiguration -Argument
"Config,Component=TimeBasedAssistants"
$diag.Diagnostics.Components.VariantConfiguration.Configuration.TimeBasedAss
istants.ElcAssistant
```

Запуск помощника для управляемых папок в определенном почтовом ящике с помощью командной консоли Exchange

Чтобы мгновенно обработать почтовый ящик с помощью MFA, используйте следующий синтаксис:

PowerShell

```
Start-ManagedFolderAssistant -Identity <MailboxIdentity>
```

В этом примере помощник для управляемых папок активируется для немедленной обработки почтового ящика пользователя Morris Cornejo.

PowerShell

```
Start-ManagedFolderAssistant -Identity morris.cornejo@contoso.com
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Start-ManagedFolderAssistant.

Использование ведения журнала аудита администратора в Exchange Server

Статья • 04.04.2023

Вы можете использовать ведение журнала аудита администратора в Exchange Server, чтобы регистрировать, когда пользователь или администратор вносит изменения в вашей организации. Вы можете отследить пользователя, который внес изменение, дополнить журналы изменений подробными сведениями о применении изменения, обеспечить соответствие нормативным требованиям и запросам на обнаружение, а также многое другое.

По умолчанию ведение журнала аудита администратора включено в новых установках Exchange Server.

Что подлежит аудиту

Аудиту подлежат командлеты, которые выполняются непосредственно в Командная консоль Exchange. Кроме того, операции, для выполнения которых используется Центр администрирования Exchange, также регистрируются в журнале, так как при этом запускаются командлеты в фоновом режиме.

В журнал заносятся командлеты, независимо от места их выполнения, если они находятся в списке аудита командлетов и один или несколько параметров этих командлетов находятся в списке аудита параметров. Журнал аудита в большей степени показывает, какие действия выполнялись для изменения объектов в организации Exchange, а не какие объекты были просмотрены.

Примечания.

- Командлет может быть не записан в журнал, если перед вызовом командлетом агента расширения командлета журнала аудита администратора произошла ошибка. Если ошибка произошла после вызова агента ведения журнала аудита администратора, командлет заносится в журнал вместе с соответствующей ошибкой. Дополнительные сведения см. в разделе агента журнала аудита Администратор далее в этом разделе.

- На компьютерах, на которых во время изменения конфигурации открыта Командная консоль Exchange, изменения конфигурации журнала аудита обновляются каждые 60 минут. Если изменения необходимо применить

немедленно, Командная консоль Exchange на каждом компьютере должна быть закрыта и снова открыта.

- После запуска команды может пройти до 15 минут, прежде чем она появится в результатах поиска журнала аудита. Это связано с тем, что перед поиском необходимо выполнить индексацию записей журнала аудита. Если команда не появляется в журнале аудита администратора, подождите несколько минут и снова выполните поиск.

Как настроить ведение журнала аудита действий администратора

По умолчанию, когда ведение журнала аудита администратора включено, запись журнала создается при каждом запуске любого командлета. Если аудит всех запускаемых командлетов не требуется, можно настроить аудит только необходимых командлетов и параметров. Ведение журнала аудита настраивается с помощью командлета **Set-AdminAuditLogConfig**. В этом командлете используются параметры, рассматриваемые в следующих разделах.

> ⓘ **Важно!**
>
> Изменения, вносимые в конфигурацию журнала аудита действий администратора, всегда фиксируются в журнале. Это происходит независимо от того, присутствует ли **Set-AdminAuditLogConfig** в списке командлетов для аудита и включено ли ведение журнала аудита.

При выполнении команды Exchange проверяет использованный командлет. Если выполняемый командлет соответствует любому из командлетов, предоставленных с параметром *AdminAuditLogCmdlets* , Exchange проверяет параметры, указанные в параметре *AdminAuditLogParameters* . Если в списке параметров найдено по крайней мере одно соответствие, Exchange заносит выполненный командлет в журнал. В следующих разделах приведены дополнительные сведения о каждом аспекте настройки ведения журнала аудита.

Дополнительные сведения об управлении конфигурацией ведения журнала аудита см. в статье Управление ведением журнала аудита администраторов.

Командлеты

Можно указать командлеты для которых необходимо осуществлять аудит, задав список командлетов и их параметров, записи о которых необходимо вносить в журнал. При настройке ведения журнала аудита можно указать для аудита каждый командлет или указать командлеты, которые требуется выполнить аудит, с помощью параметра *AdminAuditLogCmdlets* . Можно указать полные имена командлетов, например **New-Mailbox**, или указать частичные имена командлетов и заключить их в подстановочные знаки, такие как звездочка (`*`). Например, если требуется регистрировать при выполнении любого командлета, содержащего строку `Transport` , можно указать значение `*Transport*`. Можно использовать полные и частичные имена командлетов одновременно, чтобы настроить ведение журнала аудита необходимым образом.

Для аудита всех командлетов укажите только подстановочный знак (*). Это параметр по умолчанию.

Параметры

Кроме указания командлетов, записи о выполнении которых следует заносить в журнал, можно также указать, чтобы в журнал записывались командлеты, в которых используются определенные параметры. Используйте параметр *AdminAuditLogParameters* , чтобы указать, какие параметры следует регистрировать. Как и в случае с командлетами, можно указать полные имена параметров, например `Database`, или частичные имена параметров, заключенные в подстановочные знаки (`*`), например `*Address*`, или сочетание обоих.

Для аудита всех параметров укажите только подстановочный знак (*). Это параметр по умолчанию.

Срок хранения для журнала аудита действий администратора

По умолчанию записи в журнале аудита действий администратора хранятся в течение 90 дней. Через 90 дней запись удаляется. Ограничение на возраст журнала аудита можно изменить с помощью параметра *AdminAuditLogAgeLimit* . Например, чтобы изменить возрастной предел на 180 дней, используйте команду `Set-AdminAuditLogConfig -AdminAuditLogAgeLimit 180`. Кроме того, вы можете указать количество дней, часов, минут и секунд, в течение которых необходимо хранить записи журнала аудита. Чтобы указать значение, используйте формат `dd.hh:mm:ss` , в котором применяется следующее:

- **dd**: количество дней для хранения записи журнала аудита.

- **hh**: количество часов для хранения записи журнала аудита.
- **mm**: количество минут для хранения записи журнала аудита.
- **ss**: количество секунд для хранения записи журнала аудита.

С помощью `dd` поля необходимо указать несколько лет. Например, 365 дней соответствуют одному году; 730 дней — двум годам; 913 дней — двум годам и шести месяцам. Например, чтобы задать предельный срок действия журнала аудита в два года и шесть месяцев, используйте значение `913`.

Примечания.

- Вы можете сократить срок, в течение которого хранится журнал аудита действий администратора. В этом случае все записи журнала аудита, чей возраст превысит новое значение времени, будут удалены.
- Если для ограничения по возрасту задано значение 0, Exchange удаляет все записи в журнале аудита.
- Рекомендуем назначить разрешения, гарантирующие, что изменять время хранения журнала аудита могут только пользователи с высоким уровнем доверия.

Ведение подробного журнала

По умолчанию в журнал аудита действий администратора записываются только имя и параметры командлета (вместе с указанными значениями), сведения об измененном объекте, пользователе, который выполнил командлет, времени его выполнения и сервере, на котором он выполнен. В журнале аудита действий администратора не регистрируются сведения об измененных свойствах объекта. Если вы хотите, чтобы журнал аудита администратора также включал свойства объекта, который был изменен, можно включить подробное ведение журнала, задав для параметра *LogLevel* значение `Verbose`. В этом случае помимо сведений по умолчанию будут регистрироваться старые и новые значения измененных свойств объекта.

Командлеты с глаголом Test

По умолчанию командлеты, начинающиеся с глагола **Test**, не заносятся в журнал. Можно указать, что командлеты **Test** должны быть зарегистрированы, задав для параметра *TestCmdletLoggingEnabled* значение `$true`. Рекомендуем включать

ведение журнала аудита для командлетов проверки только на короткие периоды времени, так как при этом значительно увеличивается количество записей.

Журнал аудита действий администратора

При каждой регистрации командлета в журнале аудита действий администратора создается запись. Журнал аудита действий администратора хранится в выделенном почтовом ящике разрешения конфликтов, который скрыт и доступен только с помощью Центра администрирования Exchange, командлетов **Search-AdminAuditLog** и **New-AdminAuditLogSearch**. Содержание следующих разделов:

- Содержание журнала аудита действий администратора.
- Отчеты, доступные на странице **Аудит** в Центре администрирования Exchange.
- Командлеты поиска в журнале аудита действий администратора.

Содержимое журнала аудита

Каждая запись журнала аудита содержит сведения, описанные в приведенной ниже таблице. Журнал аудита содержит одну или несколько записей. Количество записей журнала аудита определяется ограничением по возрасту журнала аудита, указанным с помощью `Set-AdminAuditLogConfig -AdminAuditLogAgeLimit` команды . Все записи журнала аудита, время хранения которых истекло, удаляются.

Поля записей журнала аудита

Поле	Описание
`RunspaceId`	Это поле предназначено для внутреннего использования системой Exchange.
`ObjectModified`	Это поле содержит объект, измененный командлетом, указанным в `CmdletName` поле .
`CmdletName`	Это поле содержит имя командлета, который был запущен пользователем в `Caller` поле .
`CmdletParameters`	Это поле содержит параметры, указанные при выполнении командлета `CmdletName` в поле. В этом поле, при наличии, также хранится, но не отображается в выходных данных по умолчанию, значение, указанное с помощью параметра.

Поле	Описание
`ModifiedProperties`	Это поле содержит свойства, которые были изменены для объекта в `ObjectModified` поле . В этом поле также хранятся значения свойств — как старые, так и новые (сохраненные). **Важно!** Это поле заполняется только в том случае, если параметр *LogLevel* в командлете **Set-AdminAuditLogConfig** имеет значение `verbose`.
`Caller`	Это поле содержит учетную запись пользователя, который выполнил командлет в `CmdletName` поле .
`Succeeded`	Это поле указывает, успешно ли выполнен командлет в `CmdletName` поле. Значение равно или `True` `False`.
`Error`	Это поле содержит сообщение об ошибке, созданное в случае неудачного завершения командлета `CmdletName` в поле.
`RunDate`	Это поле содержит дату и время выполнения командлета `CmdletName` в поле. Дата и время хранятся в формате времени UTC.
`OriginatingServer`	Это поле указывает сервер, на котором был запущен командлет, указанный `CmdletName` в поле.
`Identity`	Это поле предназначено для внутреннего использования системой Exchange.
`IsValid`	Это поле предназначено для внутреннего использования системой Exchange.
`ObjectState`	Это поле предназначено для внутреннего использования системой Exchange.

Отчеты аудита Центра администрирования Exchange

На странице **Аудит** в Центре администрирования Exchange представлено несколько отчетов, содержащих сведения о различных типах изменений, касающийся соответствия требованиям и конфигурации администрирования. Следующие отчеты содержат сведения об изменениях конфигурации в организации:

- **Отчет о группе ролей администратора**. Этот отчет позволяет искать изменения в группах ролей управления, указанные в течение указанного периода времени. Полученные результаты содержат данные об измененных группах ролей, внесенных изменениях, а также о том, кто и когда внес эти изменения. Может быть возвращено не более 3000 записей. Если в результатах поиска выведено более 3000 записей, используйте отчет **Журнал аудита администратора** или командлет **Search-AdminAuditLog**.

- **Администратор отчет по журналу аудита**. Этот отчет позволяет просматривать записи в журнале аудита администратора, записанные в течение указанного периода времени. Вы также можете экспортировать их в XML-файл, а затем отправить этот файл по электронной почте указанному получателю. Дополнительные сведения о содержимом XML-файла см. в разделе Структура журнала аудита администратора.

Сведения об использовании этих отчетов см. в статье Поиск изменений группы ролей или журналы аудита администратора.

Командлет Search-AdminAuditLog

При запуске командлета **Search-AdminAuditLog** возвращаются все записи журнала аудита, которые соответствуют условиям поиска. Можно указать следующие условия поиска:

- **Командлеты**. Указывает командлеты, которые нужно найти в журнале аудита администратора.
- **Параметры**. Указывает параметры, разделенные запятыми, которые нужно найти в журнале аудита администратора. Поиск параметров возможен, только если указан командлет для поиска.
- **Дата окончания**: ограничивает результаты журнала аудита администратора записями, которые произошли на указанную дату или раньше.
- **Дата начала**: ограничивает результаты журнала аудита администратора записями, которые произошли на указанную дату или позже.
- **Идентификаторы объектов**. Указывает, что должны возвращаться только записи журнала аудита администратора, содержащие указанные измененные объекты.
- **Идентификаторы пользователей**. Указывает, что должны возвращаться только записи журнала аудита администратора, содержащие указанные идентификаторы пользователя, запустившего командлет.
- **Успешное завершение**. Указывает, должны ли возвращаться только записи журнала аудита администратора, указывающие на успех или сбой.

Каждая запись журнала аудита содержит сведения, описанные в таблице в разделе Содержимое журнала аудита. По умолчанию возвращается только первая 1000 записей журнала, которые соответствуют условиям поиска. Однако значение по умолчанию можно изменить с помощью параметра *ResultSize*. Можно указать

значение `Unlimited` с помощью параметра *ResultSize* , чтобы вернуть все записи журнала, соответствующие указанным условиям.

Сведения об использовании командлета **Search-AdminAuditLog** см. в разделе Поиск изменений группы ролей или журналы аудита администратора.

Командлет New-AdminAuditLogSearch

Командлет **New-AdminAuditLogSearch** выполняет поиск в журнале аудита действий администратора подобно командлету **Search-AdminAuditLog**. Однако вместо того, чтобы выводить результаты поиска в Командная консоль Exchange, командлет **New-AdminAuditLogSearch** выполняет поиск и отправляет результаты по электронной почте указанному получателю. Результаты включаются в электронное сообщение в виде XML-вложения.

С командлетом **New-AdminAuditLogSearch** можно использовать такие же условия поиска, как и с командлетом **Search-AdminAuditLog**. Список условий поиска см. в разделе Командлет Search-AdminAuditLog.

После выполнения командлета **New-AdminAuditLogSearch** для доставки отчета указанному получателю может потребоваться до 15 минут. Максимальный размер отчета в формате XML составляет 10 МБ. XML-файл содержит такие же сведения, что и таблица в разделе Содержимое журнала аудита. Дополнительные сведения о структуре XML-файла см. в разделе Структура журнала аудита администратора.

> ⓘ **Примечание**
>
> Outlook Web App не позволяет открывать XML-вложения по умолчанию. Вы можете настроить Exchange, чтобы разрешить просмотр XML-вложений с помощью Outlook Web App, или использовать другой почтовый клиент, например Microsoft Outlook, для просмотра вложения. Сведения о настройке Outlook Web App для просмотра XML-вложений см. **в статье Просмотр и настройка виртуальных каталогов Outlook в Интернете в Exchange Server**.

Сведения об использовании командлета **New-AdminAuditLogSearch** см. в разделе Поиск изменений группы ролей или журналы аудита администратора.

Как вносить записи в журнал аудита действий администратора вручную

Помимо ведения журнала командлетов Exchange при их запуске, Exchange Server позволяет вручную записывать записи журнала в журнал аудита. Exchange Server поддерживает это с помощью командлета **Write-AdminAuditLog**. Ниже перечислены ситуации, в которых может потребоваться добавить запись в журнал вручную.

- Пользовательский сценарий входа и выхода
- Сведения об изменении элемента управления
- Время начала и окончания обслуживания

С помощью командлета **Write-AdminAuditLog** можно указать строку текста для включения в журнал аудита с помощью параметра *Comment* . Параметр *Comment* принимает буквенно-цифровую строку длиной до 500 символов. В записи журнала аудита вручную вместе со строкой комментария содержатся все те же сведения, которые записываются при регистрации командлета Exchange. Описание полей, включенных в журнал аудита, см. в таблице из раздела Содержимое журнала аудита.

Записи журнала аудита, внесенные вручную, можно извлекать так же, как и любые другие записи журнала — с помощью страницы **аудита** Центра администрирования Exchange или командлетов **Search-AdminAuditLog** и **New-AdminAuditLogSearch**.

Сведения о том, как просмотреть содержимое параметра *Comment* в **командлете Write-AdminAuditLog** в записи журнала аудита вручную, см. в статье Поиск изменений группы ролей или журналов аудита администратора.

Репликация Active Directory

При ведении журнала аудита администратора используется репликация Active Directory для выполнения репликации параметров конфигурации, указанных для контроллеров домена в организации. В зависимости от параметров репликации выполненные изменения не сразу применяются ко всем серверам Exchange в организации.

Агент журнала аудита действий администратора

Встроенный агент расширения командлета журнала аудита Администратор выполняет ведение журнала аудита администратора для операций командлетов в

Exchange Server. Этот агент считывает конфигурацию журнала аудита и выполняет оценку каждого командлета, запускаемого в организации. Если критерий, указанный в конфигурации журнала аудита действий администратора, соответствует запускаемому командлету, агент создает запись.

Агент журнала аудита администратора включен по умолчанию, что необходимо для функции ведения журнала аудита действий администратора. Его невозможно отключить, и его приоритет невозможно изменить. Дополнительные сведения об агентах расширения командлета см. в статье Cmdlet Extension Agents.

Структура журнала аудита администратора в Exchange Server

Статья • 04.04.2023

Журналы аудита администратора содержат запись всех командлетов и параметров, которые были запущены в командной консоли Exchange и в Центре администрирования Exchange (EAC). Они создаются по запросу при запуске отчета журнала аудита администратора в Центре администрирования Exchange или при выполнении командлета **New-AdminAuditLogSearch** в командной консоли Exchange. Дополнительные сведения о журналах аудита см. в разделе Ведение журнала аудита администратора в Exchange Server.

Теги XML и атрибуты журнала аудита

Журналы аудита хранятся в файлах XML и могут содержать записи нескольких журналов. В следующей таблице описаны все теги XML и связанные с ними атрибуты.

Элемент	Атрибут	Описание
`<?xml version="1.0" encoding="utf-8"?>`	Недоступно	Это тег объявления документа XML. Он включается в каждый файл XML журнала аудита и содержит номер версии XML и значение типа кодировки символов.
`SearchResults`	Недоступно	В этом теге содержатся все записи журнала аудита в файле XML. Тег `Event` является дочерним для этого тега. Для КАЖДОГО XML-файла существует только один `SearchResults` тег.
`Event`		В этом теге содержится запись журнала аудита для отдельного командлета. Этот тег содержит атрибуты `Caller`, `Cmdlet`, `ObjectModified`, `RunDate`, `Succeeded`, `Error` и `OriginatingServer` . Теги `CmdletParameters` и `ModifiedProperties` являются дочерними элементами этого тега. Существует один `Event` тег для каждой записи журнала аудита.
	`Caller`	Этот атрибут содержит учетную запись пользователя, который выполнил командлет в атрибуте `Cmdlet` .

Элемент	Атрибут	Описание
	`Cmdlet`	Этот атрибут содержит имя командлета, который был запущен пользователем в атрибуте `Caller` .
	`ObjectModified`	Этот атрибут содержит объект, измененный командлетом, указанным в атрибуте `Cmdlet` . Тег `ModifiedProperties` показывает, какие свойства были изменены для этого объекта.
	`RunDate`	Этот атрибут содержит дату и время выполнения командлета в атрибуте `Cmdlet` .
	`Succeeded`	Этот атрибут указывает, успешно ли выполнен командлет в атрибуте `Cmdlet` . Значение равно или `True` `False`.
	`Error`	Этот атрибут содержит сообщение об ошибке, созданное в случае неудачного завершения командлета в атрибуте `Cmdlet` . Если ошибка не обнаружена, значение задается в `None`.
	`OriginatingServer`	Этот атрибут содержит сервер, на котором был запущен командлет, указанный в атрибуте `Cmdlet` .
`CmdletParameters`	Недоступно	В этом теге содержатся все параметры, заданные при запуске командлета. Тег `Parameter` является дочерним для этого тега. На каждый тег приходится по одному `CmdletParameters` тегу `Event` .
`Parameter`		В этом теге содержится отдельный параметр, заданный при запуске командлета. Этот тег содержит атрибуты `Name` и `Value` . На тег `CmdletParameters` может быть несколько `Parameter` тегов.
	`Name`	В этом атрибуте содержится имя параметра, заданного в командлете при его запуске.
	`Value`	Этот атрибут содержит значение, указанное в параметре, указанном в атрибуте `Name` .

Элемент	Атрибут	Описание
`ModifiedProperties`	Недоступно	В этом теге содержатся все свойства, которые были изменены в результате выполнения командлета. Тег `Property` является дочерним для этого тега. На каждый тег приходится по одному `ModifiedProperties` тегу `Event` . **Важно!** Этот тег заполняется только в том случае, если параметр *LogLevel* в командлете **Set-AdminAuditLogConfig** имеет значение `Verbose`.
`Property`		В этом теге содержится отдельное свойство, заданное при запуске командлета. Этот тег содержит атрибуты `Name`, `OldValue` и `NewValue` . На тег `ModifiedProperties` может быть несколько `Property` тегов.
	`Name`	В этом атрибуте содержится имя свойства, измененного в результате выполнения командлета.
	`OldValue`	Этот атрибут содержит значение, которое содержалось в свойстве, указанном в атрибуте `Name` до его изменения.
	`NewValue`	Этот атрибут содержит значение, на которое было изменено свойство в атрибуте `Name` .

Пример записи в журнале аудита действий администратора

Ниже приведен пример типичной записи в журнала аудита действий администратора.

XML

```
<?xml version="1.0" encoding="utf-8"?>
<SearchResults>
  <Event Caller="corp.e16.contoso.com/Users/Administrator" Cmdlet="Set-
Mailbox" ObjectModified="corp.e16.contoso.com/Users/david" RunDate="2015-10-
18T15:48:15-07:00" Succeeded="true" Error="None" OriginatingServer="WIN8MBX
(15.01.0396.030)">
    <CmdletParameters>
      <Parameter Name="Identity" Value="david" />
      <Parameter Name="ProhibitSendReceiveQuota" Value="10 GB
(10,737,418,240 bytes)" />
    </CmdletParameters>
    <ModifiedProperties>
      <Property Name="ProhibitSendReceiveQuota" OldValue="35 GB
```

```
(37,580,963,840 bytes)" NewValue="10 GB (10,737,418,240 bytes)" />
    </ModifiedProperties>
  </Event>
</SearchResults>
```

На основе данных в этой записи журнала мы знаем, что произошло следующее:

- 18.10.2017 в 15:48 по тихоокеанскому времени (UTC-7) пользователь `Administrator` выполнил командлет **Set-Mailbox**.
- При запуске командлета **Set-Mailbox** было задано два следующих параметра:
  - *Удостоверение* со значением `david`
  - *ProhibitSendReceiveQuota* со значением `10GB`
- Свойство *ProhibitSendReceiveQuota* объекта `david` было изменено новым значением `10GB`, которое заменило старое значение `35GB`.

  > ⓘ **Примечание**
  >
  > Измененные свойства сохраняются в журнале аудита, так как в этом примере *параметру LogLevel* в командлете `Set-AdminAuditLogConfig` было присвоено значение `Verbose` .

- Операция успешно завершена без ошибок.

Управление ведением журнала аудита администратора в Exchange Server

Статья • 04.04.2023

Ведение журнала аудита администратора в Exchange Server позволяет создавать запись журнала при каждом запуске указанного командлета. Записи журнала содержат сведения о том, какой командлет выполнялся, какие параметры использовались, кто выполнял командлет и какие объекты были затронуты. Дополнительные сведения о ведении журнала аудита администратора см. в разделе Ведение журнала аудита администратора в Exchange Server.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: менее 5 минут
- Для выполнения этой процедуры можно использовать только PowerShell.Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Ведение журнала аудита администратора" раздела "Инфраструктура Exchange и разрешения PowerShell ".
- При ведении журнала аудита действий администратора для репликации параметров конфигурации, указанных для контроллеров домена в организации, используется Active Directory. В зависимости от параметров репликации внесенные изменения могут быть применены не сразу ко всем серверам Exchange 2016 и Exchange 2019 в вашей организации.
- На компьютерах, на которых во время изменения конфигурации открыта Командная консоль Exchange, изменения конфигурации журнала аудита обновляются каждые 60 минут. Если изменения необходимо применить немедленно, Командная консоль Exchange на каждом компьютере должна быть закрыта и снова открыта.
- После запуска команды может пройти до 15 минут, прежде чем она появится в результатах поиска журнала аудита. Это связано с тем, что перед поиском

необходимо выполнить индексацию записей журнала аудита. Если команда не появляется в журнале аудита администратора, подождите несколько минут и снова выполните поиск.

Как задать командлеты для аудита

По умолчанию в журналах аудита создается запись для каждого выполняемого командлета. Если ведение журнала аудита включено впервые и необходимо, чтобы это действие выполнялось далее, список аудита командлетов изменять не требуется. Если вы ранее указали командлеты для аудита и теперь хотите выполнить аудит всех командлетов, вы можете выполнить аудит всех командлетов, указав подстановочный знак звездочки (*) с помощью параметра *AdminAuditLogCmdlets* в **командлете Set-AdminAuditLogConfig** , как показано в следующей команде.

PowerShell

```
Set-AdminAuditLogConfig -AdminAuditLogCmdlets *
```

Вы можете указать, какие командлеты следует выполнять аудит, предоставив список командлетов с помощью параметра *AdminAuditLogCmdlets* . При указании списка командлетов для аудита можно указать один командлеты, командлеты со звездочкой (*) подстановочными знаками или сочетание обоих командлетов. Записи в списке разделяются запятыми. Допустимы следующие значения:

- `New-Mailbox`
- `*TransportRule`
- `*Management*`
- `Set-Transport*`

В этом примере выполняется аудит командлетов, указанных в предыдущем списке.

PowerShell

```
Set-AdminAuditLogConfig -AdminAuditLogCmdlets New-Mailbox, *TransportRule,
*Management*, Set-Transport*
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Set-AdminAuditLogConfig.

Как задать параметры для аудита

По умолчанию в журналах аудита создается запись для каждого выполняемого командлета, независимо от указанных параметров. Если ведение журнала аудита включено впервые и необходимо, чтобы это действие выполнялось далее, список аудита параметров изменять не требуется. Если ранее вы указали параметры для аудита и теперь хотите выполнить аудит всех параметров, это можно сделать, указав подстановочный знак звездочки (*) с параметром *AdminAuditLogParameters* в **командлете Set-AdminAuditLogConfig** , как показано в следующей команде.

PowerShell

```
Set-AdminAuditLogConfig -AdminAuditLogParameters *
```

Вы можете указать параметры, которые требуется выполнить аудит, с помощью параметра *AdminAuditLogParameters* . При указании списка параметров для аудита можно указать отдельные параметры, параметры с подстановочными знаками звездочки (*) или сочетание обоих параметров. Записи в списке разделяются запятыми. Допустимы следующие значения:

- `Database`
- `*Address*`
- `Custom*`
- `*Region`

> ⓘ **Примечание**
>
> Для создания записи журнала аудита при выполнении команды команда должна включать по крайней мере один или несколько параметров, которые существуют по крайней мере в одном или нескольких командлетах, указанных с параметром *AdminAuditLogCmdlets* .

В этом примере выполняется аудит параметров, указанных в предыдущем списке.

PowerShell

```
Set-AdminAuditLogConfig -AdminAuditLogParameters Database, *Address*,
Custom*, *Region
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Set-AdminAuditLogConfig.

Как задать срок хранения для журнала аудита действий администратора

Время хранения журнала аудита определяет период, в течение которого будут храниться записи журнала аудита. При превышении времени хранения записи журнала она удаляется. Значение по умолчанию — 90 дней.

Вы можете указать возрастной предел в днях. Кроме того, можно указать количество дней, часов, минут и секунд, в течение которых должны храниться записи журнала аудита. Чтобы указать значение, более конкретное, чем дни, используйте формат dd.hh.mm:ss, где применяется следующее:

- **dd**: количество дней для хранения записи журнала аудита
- **hh**: количество часов для хранения записи в журнале аудита
- **mm**: количество минут для хранения записи журнала аудита
- **ss**: количество секунд для хранения записи журнала аудита.

> ⊗ **Внимание!**
>
> Для времени хранения журнала аудита можно установить меньшее значение по сравнению с текущим временем хранения. При этом все записи журнала аудита, длительность хранения которых превысит новое время хранения, будут удалены. > Если для ограничения по возрасту задано значение 0, Exchange удаляет все записи в журнале аудита. > Рекомендуется назначать разрешения, чтобы настроить ограничение на возраст журнала аудита только для пользователей с высоким уровнем доверия.

В этом примере указывается время хранения, равное двум годам и шести месяцам.

PowerShell

```
Set-AdminAuditLogConfig -AdminAuditLogAgeLimit 913
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Set-AdminAuditLogConfig.

Как включить или отключить ведение журнала для командлетов с глаголом Test

По умолчанию командлеты, начинающиеся с глагола **Test**, не заносятся в журнал. Причиной этого является то, что командлеты **Test** могут создавать большой объем данных за короткий период времени. Включать ведение журнала командлетов **Test** рекомендуется только на короткий период времени.

Эта команда включает ведение журнала командлетов **Test**.

```
PowerShell

Set-AdminAuditLogConfig -TestCmdletLoggingEnabled $true
```

Эта команда отключает ведение журнала командлетов **Test**.

```
PowerShell

Set-AdminAuditLogConfig -TestCmdletLoggingEnabled $false
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Set-AdminAuditLogConfig.

Как отключить ведение журнала аудита действий администратора

Чтобы отключить ведение журнала аудита действий администратора, используйте указанную ниже команду.

```
PowerShell

Set-AdminAuditLogConfig -AdminAuditLogEnabled $false
```

Как включить ведение журнала аудита действий администратора

Чтобы включить ведение журнала аудита действий администратора, используйте указанную ниже команду.

```
PowerShell
```

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $true
```

Как просмотреть параметры, касающиеся ведения журнала аудита действий администратора

Чтобы просмотреть параметры, касающиеся ведения журнала аудита действий администратора, которые вы настроили в организации, используйте указанную ниже команду.

PowerShell

```
Get-AdminAuditLogConfig
```

Ведение журнала аудита почтового ящика в Exchange Server

Статья • 04.04.2023

Так как почтовые ящики могут содержать конфиденциальную информацию с высоким влиянием на бизнес (HBI) и личную информацию (PII), важно отслеживать, кто входит в почтовые ящики в вашей организации и какие действия выполняются. Особенно важно отслеживать доступ к почтовым ящикам пользователей, отличных от владельца почтового ящика. Эти пользователи называются *пользователями делегатов*.

С помощью *функции ведения журнала аудита почтового ящика* можно регистрировать доступ владельцев, делегатов (в том числе администраторов с полными разрешениями на доступ к почтовому ящику) и администраторов к почтовым ящикам.

При включении функции ведения журнала аудита для почтового ящика можно указать, какие именно действия (например, доступ к почтовому ящику, перемещение или удаление сообщений) должны регистрироваться для соответствующих типов учетных записей для входа (администратор, делегированный пользователь или владелец). В записях журнала аудита также содержатся другие важные сведения, такие как IP-адрес клиента, имя узла, процесс или клиент, использованные для получения доступа к почтовому ящику. Для перемещенных сообщений также указывается имя папки назначения.

Ведение журнала аудита почтовых ящиков

Для всех почтовых ящиков, для которых включено ведение журнала аудита, создаются журналы аудита. Записи журнала хранятся во вложенной папке "Аудиты" папки "Элементы с возможностью восстановления" в отслеживаемом почтовом ящике. Это обеспечивает централизованный доступ ко всем записям журнала аудита независимо от того, каков способ клиентского доступа к почтовому ящику или какой сервер (либо компьютер) администратор использует для доступа к журналу аудита почтовых ящиков. При перемещении почтового ящика на другой сервер также перемещаются хранящиеся в нем журналы аудита.

По умолчанию записи журнала аудита хранятся в почтовом ящике 90 дней, после чего удаляются. Время хранения можно изменить, используя параметр *AuditLogAgeLimit* в командлете Set-Mailbox. Если почтовый ящик хранится на месте или хранится для судебного разбирательства, записи журнала аудита сохраняются

до истечения периода хранения журналов аудита для этого почтового ящика. Чтобы сохранить журналы аудита на более длительный срок, следует увеличить период хранения, изменив значение параметра *AuditLogAgeLimit*. Вы также можете экспортировать записи журнала аудита до истечения периода хранения. Дополнительные сведения см. в разделе:

- Экспорт журналов аудита почтовых ящиков
- Создание поиска по журналу аудита почтового ящика

Включение ведения журнала аудита почтовых ящиков

Ведение журнала аудита включено для каждого почтового ящика. С помощью командлета **Set-Mailbox** можно включить или отключить ведение журнала аудита почтовых ящиков. Дополнительные сведения см. в разделе Включение или отключение ведения журнала аудита почтовых ящиков для почтового ящика.

При включении ведения журнала аудита почтового ящика операции доступа к почтовому ящику, а также некоторые действия администраторов и делегатов записываются по умолчанию. Для записи действий владельца почтового ящика необходимо указать, какие именно действия должны записываться.

Действия, которые регистрируются в журналах аудита почтовых ящиков

В приведенной ниже таблице перечислены действия, записываемые в журнале аудита почтового ящика, а также типы учетных записей вошедших пользователей, для которых эти действия можно зарегистрировать. Обратите внимание на то, что администратор, которому предоставлены разрешения на полный доступ к почтовому ящику пользователя, считается делегированным пользователем.

Для отключения записи определенных действий, выполняемых в почтовом ящике, необходимо изменить параметры ведения журнала аудита почтового ящика. Существующие записи в журнале аудита удаляются после истечения заданного срока хранения.

Действие	Описание	Администратор	Делегат	Владелец
Копировать	Сообщение скопировано в другую папку.	Да	Нет	Нет

Действие	Описание	Администратор	Делегат	Владелец
Создание	В папке "Календарь", "Контакты", "Заметки" или "Задачи" почтового ящика создан элемент, например новое приглашение на собрание. Учтите, что создание сообщений и папок при этом не регистрируется.	Да[1]	Да[1]	Да
FolderBind	Папка почтового ящика была открыта.	Да[1]	Да[2]	Нет
HardDelete	Элемент удален из папки "Элементы для восстановления" без возможности восстановления.	Да[1]	Да[1]	Да
MailboxLogin	Пользователь выполнил вход в свой почтовый ящик.	Нет	Нет	Да[3]
MessageBind	Сообщение открыто или просматривается в области просмотра.	Да	Нет	Нет
Move	Сообщение перемещено в другую папку.	Да[1]	Да	Да
MoveToDeletedItems	Сообщение перемещено в папку "Удаленные".	Да[1]	Да	Да
SendAs	Сообщение отправлено с использованием разрешений "Отправить как".	Да[1]	Да[1]	Нет
SendOnBehalf	Сообщение отправлено с использованием разрешений "Отправить от имени".	Да[1]	Да	Нет
SoftDelete	Сообщение удалено из папки "Удаленные".	Да[1]	Да[1]	Да
Update	Параметры элемента обновлены.	Да[1]	Да[1]	Да

[1] Аудит по умолчанию, если аудит включен для почтового ящика.

[2] Записи для действий привязки папок, выполняемых делегатами, объединяются. За 24 часа в журнале создается одна запись для доступа к отдельной папке.

[3] Аудит для входа владельца в почтовый ящик работает только для имен входа POP3, IMAP4 или OAuth. Он не поддерживается для входа в почтовый ящик с использованием NTLM или Kerberos.

Поиск в журнале аудита почтового ящика

Для поиска записей в журнале аудита можно использовать следующие способы.

- **Синхронный поиск в одном почтовом ящике**. Вы можете использовать командлет Search-MailboxAuditLog для синхронного поиска записей журнала аудита почтовых ящиков для одного почтового ящика. Командлет отображает результаты поиска в окне командной консоли Exchange. Дополнительные сведения см. в разделе Search Mailbox Audit Log for a Mailbox.

- **Асинхронный поиск в одном или нескольких почтовых ящиках**. Вы можете создать поиск по журналам аудита почтовых ящиков для асинхронного поиска по журналам аудита почтовых ящиков для одного или нескольких почтовых ящиков, а затем отправить результаты поиска на указанный адрес электронной почты. Результаты поиска отправляются в виде вложения XML. Для выполнения поиска используйте командлет New-MailboxAuditLogSearch. Дополнительные сведения см. в разделе Create a Mailbox Audit Log Search.

- **Использование отчетов аудита в Центре администрирования Exchange (EAC).** Вы можете использовать вкладку **Аудит** в Центре администрирования Exchange для запуска отчета о доступе к почтовому ящику, не являющегося владельцем (содержит записи для действий администратора и удаления) или экспорта записей, не являющихся владельцами, из журнала аудита почтовых ящиков. Дополнительные сведения см. в следующих статьях:

  - Запуск отчета о доступе к чужим почтовым ящикам
  - Экспорт журналов аудита почтовых ящиков

Записи журнала аудита почтовых ящиков

В следующей таблице описываются поля, заполняемые в журнале аудита почтовых ящиков.

Поле	Заполняется
Операция	Одно из следующих действий: Copy Create FolderBind HardDelete MailboxLogin MessageBind Move MoveToDeletedItems SendAs SendOnBehalf SoftDelete Update
OperationResult	Один из следующих результатов: Failed Частичносоздало Succeeded
LogonType	Тип учетной записи для входа пользователя, выполняющего действие. Типы учетных записей для входа: Владелец Делегат Администратор
DestFolderId	Идентификатор GUID папки назначения для операций перемещения.
DestFolderPathName	Путь к папке назначения для операций перемещения.
FolderId	Идентификатор GUID папки.
FolderPathName	Путь к папке.
ClientInfoString	Сведения для идентификации клиента или компонента Exchange, выполняющего эту операцию.
ClientIPAddress	IP-адрес клиентского компьютера.
ClientMachineName	Имя клиентского компьютера.
ClientProcessName	Имя процесса клиентского приложения.
ClientVersion	Версия клиентского приложения.
InternalLogonType	Тип внутреннего пользователя (сотрудника организации), выполнившего операцию. Для этого поля допускаются те же значения, что и для поля **LogonType**.

Поле	Заполняется
MailboxOwnerUPN	Имя участника-пользователя (UPN) владельца почтового ящика.
MailboxOwnerSid	Идентификатор безопасности владельца почтового ящика (SID).
DestMailboxOwnerUPN	Имя участника-пользователя владельца почтового ящика назначения, выполняющего действия в нескольких почтовых ящиках.
DestMailboxOwnerSid	Идентификатор безопасности владельца почтового ящика назначения, выполняющего действия в нескольких почтовых ящиках.
DestMailboxOwnerGuid	Идентификатор GUID владельца почтового ящика назначения.
CrossMailboxOperation	Запись сведений об операции, выполненной в нескольких почтовых ящиках (например, копирование или перемещение сообщений в другие почтовые ящики).
LogonUserDisplayName	Отображаемое имя пользователя, выполнившего вход.
DelegateUserDisplayName	Отображаемое имя пользователя-делегата.
LogonUserSid	Идентификатор безопасности пользователя, выполнившего вход.
SourceItems	Идентификатор ItemID элементов почтового ящика, в котором выполнено записанное действие (например, перемещение или удаление). Для действий, выполненных для нескольких элементов, данное поле отображается как совокупность элементов.
SourceFolders	Идентификатор GUID исходной папки.
ItemId	Идентификатор элемента.
ItemSubject	Тема элемента.
MailboxGuid	Идентификатор GUID почтового ящика
MailboxResolvedOwnerName	Имя пользователя почтового ящика разрешено в формате *DOMAIN\ SamAccountName*.
LastAccessed	Время выполнения действия.
Identity	Идентификатор записи журнала аудита.

Дополнительные сведения

- **Доступ администратора к почтовым ящикам**. Считается, что доступ к почтовым ящикам будет осуществляться администратором только в следующих сценариях:
  - Для поиска в почтовом ящике используется обнаружение электронных данных на месте.
  - Использование командлета New-MailboxExportRequest для экспорта почтового ящика.
  - Microsoft Exchange Server для доступа к почтовому ящику используются объекты данных клиента MAPI и объектов данных для совместной работы.
- **Обход ведения журнала аудита почтовых ящиков**. Доступ к почтовым ящикам авторизованными автоматизированными процессами, такими как учетные записи, используемые сторонними средствами или учетными записями, используемыми для законного мониторинга, может создать большое количество записей журнала аудита почтовых ящиков и не представляет интереса для вашей организации. Регистрацию сведений о таких учетных записях в журнале аудита можно отключить. Дополнительные сведения см. в разделе Bypass a User Account From Mailbox Audit Logging.
- **Ведение журнала действий владельца почтового ящика**. Для почтовых ящиков, таких как почтовый ящик поиска обнаружения, который может содержать более конфиденциальные сведения, рассмотрите возможность включения ведения журнала аудита почтового ящика для действий владельца почтового ящика, таких как удаление сообщений.

Включение или отключение ведения журнала аудита почтовых ящиков для почтового ящика в Exchange Server

Статья • 04.04.2023

С помощью ведения журнала аудита почтового ящика в Exchange Server вы можете отслеживать входы в почтовый ящик, а также какие действия выполняются во время входа пользователя в систему. Если ведение журнала аудита почтового ящика включено, некоторые действия, выполняемые администраторами и делегатами, записываются по умолчанию. Действия, выполняемые владельцем почтового ящика, по умолчанию не записываются. Дополнительные сведения о ведении журнала аудита почтовых ящиков и действиях, которые можно регистрировать, см. в статье Ведение журнала аудита почтовых ящиков в Exchange Server.

> ⊗ **Внимание!**
>
> Аудит действий владельца почтового ящика может создать большое количество записей в журнале и поэтому по умолчанию отключен. Рекомендуем включать аудит только для определенных действий владельца.

Что нужно знать перед началом работы

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Ведение журнала аудита почтовых ящиков" в разделе Политика обмена сообщениями и разрешения на соответствие требованиям Exchange Server.
- По умолчанию записи в журнале аудита почтового ящика хранятся в течение 90 дней. Сроки хранения записей см. в разделе Дополнительные сведения.
- Вы не можете использовать центр администрирования Exchange (EAC), чтобы включить или отключить ведение журнала аудита почтовых ящиков. Необходимо использовать командную консоль Exchange. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

- Администратор, которому предоставлены разрешения на полный доступ к почтовому ящику пользователя, считается делегированным пользователем.
- Считается, что администраторы получают доступ к почтовым ящикам только в следующих случаях:
  - Для поиска в почтовом ящике используется обнаружение электронных данных на месте.
  - Для экспорта почтового ящика используется командлет **New-MailboxExportRequest**.
  - Для доступа к почтовому ящику используется Редактор MAPI Microsoft Exchange Server.

Включение и отключение ведения журнала аудита почтовых ящиков

Для включения или отключения ведения журнала аудита почтового ящика можно использовать Командная консоль Exchange. С ее помощью можно включить или отключить запись всех операций, указанных для администратора, делегатов и владельца почтового ящика.

В этом примере включается ведение журнала аудита почтового ящика пользователя Ben Smith.

PowerShell

```
Set-Mailbox -Identity "Ben Smith" -AuditEnabled $true
```

В этом примере мы включили ведение журнала аудита для почтовых ящиков всех пользователей в организации.

PowerShell

```
Get-Mailbox -ResultSize Unlimited -Filter "RecipientTypeDetails -eq
'UserMailbox'" | Select PrimarySmtpAddress | ForEach {Set-Mailbox -Identity
$_.PrimarySmtpAddress -AuditEnabled $true}
```

В этом примере отключается ведение журнала аудита почтового ящика пользователя Ben Smith.

PowerShell

```
Set-Mailbox -Identity "Ben Smith" -AuditEnabled $false
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе Set-Mailbox.

Настройка ведения журнала аудита почтовых ящиков для доступа администратора, делегата и владельца

Если для почтового ящика включено ведение журнала аудита почтовых ящиков, только действия администратора, делегата и владельца, указанные в конфигурации ведения журнала аудита, заносятся в журнал.

В этом примере указывается, что `MessageBind` действия и `FolderBind` , выполняемые администраторами, будут регистрироваться в почтовом ящике Бена Смита.

PowerShell

```
Set-Mailbox -Identity "Ben Smith" -AuditAdmin MessageBind,FolderBind -
AuditEnabled $true
```

В этом примере указывается, что `SendAs` действия или `SendOnBehalf` , выполняемые пользователями-делегатами, будут регистрироваться в почтовом ящике Бена Смита.

PowerShell

```
Set-Mailbox -Identity "Ben Smith" -AuditDelegate SendAs,SendOnBehalf -
AuditEnabled $true
```

В этом примере указывается, что действие, `HardDelete` выполненное владельцем почтового ящика, будет зарегистрировано в почтовом ящике Бена Смита.

PowerShell

```
Set-Mailbox -Identity "Ben Smith" -AuditOwner HardDelete -AuditEnabled $true
```

Подробные сведения о синтаксисе и параметрах см. в разделе Set-Mailbox.

Как проверить, все ли получилось?

Чтобы убедиться, что ведение журнала аудита почтовых ящиков включено и указаны правильные настройки ведения журнала для доступа администратора, делегата и владельца, используйте командлет Get-Mailbox для извлечения параметров ведения журнала аудита для этого почтового ящика.

В этом примере извлекаются параметры почтового ящика Бена Смита (Ben Smith) и передаются параметры аудита, в том числе срок хранения записей журнала, в командлет **Format-List**.

PowerShell

```
Get-Mailbox "Ben Smith" | Format-List Audit*
```

Значение `True` свойства **AuditEnabled** проверяет, включено ли ведение журнала аудита.

В этом примере показано получение параметров аудита для почтовых ящиков всех пользователей в организации.

PowerShell

```
Get-Mailbox -ResultSize Unlimited -Filter "RecipientTypeDetails -eq
'UserMailbox'" | Format-List Name,Audit*
```

Дополнительные сведения

При запуске командлета **Get-Mailbox** могут не отображаться все действия для каждого типа пользователей. Но вы можете выполнить приведенные ниже команды, чтобы просмотреть все действия для определенного типа входа пользователя.

PowerShell

```
Get-Mailbox <identity of mailbox> | Select-Object -ExpandProperty AuditAdmin
```

PowerShell

```
Get-Mailbox <identity of mailbox> | Select-Object -ExpandProperty
AuditDelegate
```

PowerShell

```
Get-Mailbox <identity of mailbox> | Select-Object -ExpandProperty AuditOwner
```

По умолчанию записи в журнале аудита почтового ящика хранятся в течение 90 дней. Когда срок хранения записи превышает 90 дней, она удаляется. С помощью командлета **Set-Mailbox** можно изменить этот параметр, чтобы элементы хранились в течение большего (или меньшего) периода времени.

В этом примере срок хранения записей в журнале аудита почтового ящика пользователя Pilar Pinilla увеличивается до 180 дней.

PowerShell

```
Set-Mailbox -Identity "Pilar Pinilla" -AuditLogAgeLimit 180
```

В этом примере срок хранения записей в журнале аудита почтовых ящиков всех пользователей в организации уменьшается до 60 дней.

PowerShell

```
Get-Mailbox -ResultSize Unlimited -Filter "RecipientTypeDetails -eq
'UserMailbox'" | Set-Mailbox -AuditLogAgeLimit 60
```

Запуск отчета об обращениях к почтовым ящикам со стороны пользователей, не являющихся их владельцами

Статья • 04.04.2023

В отчете о доступе к почтовому ящику, не являющемуся владельцем, в Центре администрирования Exchange (EAC) перечислены почтовые ящики, доступ к которым был предоставлен другому пользователю, не являющемуся владельцем почтового ящика. Когда не владелец обращается к почтовому ящику, Exchange регистрирует сведения об этом действии. Exchange сохраняет этот журнал аудита почтового ящика в виде сообщения электронной почты в скрытой папке в проверенном почтовом ящике. В отчете отображаются записи из этого журнала в виде результатов поиска и содержатся все почтовые ящики, к которым обращается не владелец, который обращается к каждому почтовому ящику и когда, действия, выполненные не владельцами, а также успешно ли они были выполнены.

Exchange регистрирует определенные действия, не являющиеся владельцами, включая администраторов и пользователей, которым назначены разрешения для почтового ящика (которые называются *делегированными пользователями*). Вы также можете ограничить поиск пользователями из вашей организации или людьми со стороны. По умолчанию Exchange хранит записи в журнале аудита почтового ящика в течение 90 дней.

Ведение журнала аудита почтового ящика можно включить в командной консоли Exchange.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Ведение журнала аудита почтовых ящиков" в статье Политика обмена сообщениями и разрешения на соответствие требованиям Exchange Server.

- Сведения о сочетаниях клавиш, которые могут применяться к процедурам, описанным в этой статье, см. в разделе Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Шаг 1. Включение ведения журнала аудита почтовых ящиков с помощью командной консоли Exchange

Ведение журнала аудита необходимо включить для каждого почтового ящика, который вы хотите видеть в отчете о доступе к чужим почтовым ящикам. Если этого не сделать, создать отчет не получится.

Чтобы включить ведение журнала аудита почтового ящика для одного почтового ящика, выполните следующую команду в командной консоли Exchange:

PowerShell

```
Set-Mailbox <Identity> -AuditEnabled $true
```

Например, чтобы включить аудит почтовых ящиков для пользователя Николая Грачева, выполните следующую команду:

PowerShell

```
Set-Mailbox "Florence Flipo" -AuditEnabled $true
```

Чтобы включить аудит почтовых ящиков для всех почтовых ящиков пользователей в организации, выполните следующие команды:

PowerShell

```
$UserMailboxes = Get-mailbox -Filter "RecipientTypeDetails -eq
'UserMailbox'"
```

PowerShell

```
$UserMailboxes | ForEach {Set-Mailbox $_.Identity -AuditEnabled $true}
```

Как проверить, все ли получилось?

Чтобы убедиться, что ведение журнала аудита почтового ящика настроено успешно, выполните следующую команду:

PowerShell

```
Get-Mailbox | Format-List Name,AuditEnabled
```

Значение `True` свойства *AuditEnabled* проверяет, включено ли ведение журнала аудита.

Шаг 2. Использование EAC для запуска отчета о доступе к почтовому ящику, не являющегося владельцем

1. В EAC перейдите в раздел **Аудит управления соответствием**> требованиям.
2. Выберите команду **Запустить отчет о доступе к почтовым ящикам со стороны пользователей, не являющихся владельцами**.

   По умолчанию служба Exchange создает отчет о доступе к чужим почтовым ящикам в организации за последние две недели. В результатах поиска отображаются почтовые ящики, для которых включено ведение журнала аудита.
3. Чтобы просмотреть отчет о доступе к определенному почтовому ящику со стороны пользователей, не являющихся владельцами, выберите этот почтовый ящик со списка почтовых ящиков. Просмотрите результаты поиска в области сведений.

Примечания.

- Нужно сузить поиск? Выберите начальную и конечные даты и конкретные почтовые ящики для поиска. Нажмите кнопку **Поиск** , чтобы повторно запустить отчет.

- Вы также можете указать, какой тип доступа (тип входа) нужно искать. Доступны следующие варианты:
    - **Все пользователи, не являющиеся владельцами**. Найдите доступ администраторов и делегированных пользователей в организации. Сюда также входят обращения пользователей за пределами организации.
    - **Внешние пользователи**: поиск доступа для пользователей за пределами организации.
    - **Администраторы и делегированные пользователи**. Найдите доступ администраторов и делегированных пользователей в организации.
    - **Администраторы**. Найдите доступ администраторов в вашей организации.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно выполнили отчет о доступе к почтовому ящику, не являющегося владельцем, проверьте область результатов поиска. В области результатов отображаются почтовые ящики, для которые вы запустили отчет, будь то отдельный пользователь или группа почтовых ящиков. Если для определенного почтового ящика нет результатов, возможно, в указанном диапазоне дат не было доступа, не являющегося владельцем, или не было доступа, не являющегося владельцем. Как мы уже рекомендовали ранее, убедитесь, что вы включили ведение журнала аудита для почтовых ящиков, к которым вы хотите найти доступ не владельцев.

Что записывается в журнале аудита почтовых ящиков?

При запуске отчета о доступе к почтовому ящику, не являющегося владельцем, в результатах поиска EAC отображаются записи из журнала аудита почтовых ящиков. Каждая запись в отчете содержит следующие сведения:

- Кто открывал почтовый ящик и когда.
- Действия, выполненные этим пользователем.
- Затронутое сообщение и его папка.
- Было ли действие успешным.

В таблице ниже перечислены типы регистрируемых действий, а также указано, регистрируются ли они по умолчанию для доступа администраторов и делегированных пользователей. Если вы хотите отслеживать действия, не регистрируемые по умолчанию, включите их регистрацию с помощью командной консоли Exchange.

Действие	Описание	Администраторы	Пользователи-делегаты
Обновление	Сообщение было изменено.	Да	Да
Копирование	Сообщение было скопировано в другую папку.	Нет	Нет
Перемещение	Сообщение было перемещено в другую папку.	Да	Нет
Перемещение в папку "Удаленные"	Сообщение было перемещено в папку "Удаленные".	Да	Нет
Удаление с возможностью восстановления	Сообщение было удалено из папки "Удаленные".	Да	Да
Удаление без возможности восстановления	Сообщение очищено из папки "Элементы с возможностью восстановления".	Да	Да
FolderBind	Была открыта папка почтового ящика.	Да	Нет
"Отправить как"	Сообщение было отправлено с помощью разрешения SendAs. Это означает, что другой пользователь отправил сообщение от лица владельца почтового ящика.	Да	Да
Отправка от имени	Сообщение отправлено с помощью разрешения SendOnBehalf. Это означает, что другой пользователь отправил сообщение от лица владельца почтового ящика. В сообщении будет указано, от чьего лица и кем было отправлено сообщение.	Да	Нет
MessageBind	Сообщение открывалось или просматривалось в области просмотра.	Нет	Нет

Защита от потери данных в Exchange Server

Статья • 04.04.2023

Защита от потери данных (DLP) важна в Exchange Server, так как критически важные для бизнеса сообщения электронной почты часто включают конфиденциальные данные. Функции защиты от потери данных делают управление конфиденциальными данными в сообщениях электронной почты проще, чем когда-либо прежде, благодаря балансировке требований к соответствию без лишних препятствий для производительности рабочих. В следующем видео представлен концептуальный обзор DLP.
https://www.microsoft.com/ru-ru/videoplayer/embed/31f2b48e-93ed-4be3-b46d-e7230c0fed8f?autoplay=false&postJsllMsg=true&autoCaptions=ru-ru

Политики защиты от потери данных — это простые пакеты, которые представляют собой коллекции правил потока обработки почты (также известных как правила транспорта), содержащие конкретные условия, действия и исключения, которые фильтруют сообщения и вложения на основе их содержимого. Вы можете создать политику защиты от потери данных, но не активировать ее. Это позволяет проверить политики без ущерба для потока почты. Дополнительные сведения см. в разделе Тестирование правила потока обработки почты.

Политики защиты от потери данных могут использовать все возможности правил потока обработки почты для обнаружения и последующего действия с сообщениями при передаче. Например, правило потока обработки почты может выполнять глубокий анализ содержимого с помощью совпадений ключевых слов, совпадений словаря, совпадений текстовых шаблонов с помощью регулярных выражений и других методов проверки содержимого, чтобы обнаружить содержимое, которое нарушает политики защиты от потери данных в организации. Дактилоскопия документов также доступна для обнаружения конфиденциальной информации в стандартных формах. Дополнительную информацию см. в следующих статьях:

- Отпечаток документа
- Правила потока обработки почты в Exchange Server
- Интеграция правил классификации с правилами потока обработки почты

Помимо настраиваемых политик защиты от потери данных, вы также можете информировать отправителей электронной почты о том, что они собираются

нарушить одну из ваших политик, даже до отправки сообщения, содержащего конфиденциальную информацию. Это можно сделать, настроив советы по политике. Советы по политике содержат краткое примечание о возможных нарушениях политики в Outlook 2013 или более поздней версии, Outlook в Интернете (ранее — Outlook Web App) и Outlook в Интернете для устройств. Дополнительные сведения см. в статье Policy Tips.

Примечания:

- Защита от потери данных — дополнительная возможность, для использования которой требуется корпоративная клиентская лицензия (CAL) на Exchange. Дополнительные сведения о клиентских лицензиях и лицензировании серверов см. в разделе Часто задаваемые вопросы о лицензировании Exchange.
- В гибридных средах, где некоторые почтовые ящики находятся в локальной среде Exchange, а некоторые — в Exchange Online, политики защиты от потери данных применяются только в Exchange Online. Для сообщений, отправляемых между локальными пользователями, политики защиты от потери данных не применяются, так как сообщения не покидают локальную среду.

Ищете задачи управления, связанные с предотвращением потери данных? См. раздел Процедуры защиты от потери данных.

Создание политик для защиты конфиденциальных данных

Предотвращение потери данных помогает идентифицировать и отслеживать множество категорий конфиденциальной информации, которые были определены в рамках политики, например личные идентификационные номера или номера кредитных карт. Вы можете определить собственные настраиваемые политики и правила потока обработки почты или использовать шаблоны политик защиты от потери данных, включенные в Exchange, чтобы быстро приступить к работе. *Шаблон политики* — это модель, которая включает в себя ряд условий, правил и действий, которые можно выбрать для создания и сохранения фактической политики защиты от потери данных, которая поможет вам проверять сообщения. Дополнительные сведения о включенных шаблонах политик см. в статье Шаблоны политик защиты от потери данных, предоставляемые в Exchange.

Существует три различных метода, которые можно использовать для реализации защиты от потери данных:

- **Применить встроенный шаблон, предоставленный в Exchange**. Самый быстрый способ приступить к использованию политик защиты от потери данных — создать и реализовать новую политику с помощью шаблона. Это позволит сэкономить усилия на создании нового набора правил с нуля. Вы должны знать, какой тип данных вы хотите проверить, или какой нормативный акт соответствия вы пытаетесь решить. Кроме того, необходимо знать ожидания вашей организации в отношении обработки этих данных. Дополнительные сведения см. в разделах Шаблоны политик защиты от потери данных в Exchange и Создание политики защиты от потери данных из шаблона.

- **Импорт предварительно созданного файла политики извне организации**. Вы можете импортировать политики, созданные независимыми поставщиками программного обеспечения. Таким образом вы можете расширить решение защиты от потери данных в соответствии с бизнес-требованиями. Дополнительные сведения см. в разделах Определение собственных шаблонов защиты от потери данных и типов сведений и Импорт политики защиты от потери данных из файла.

- **Создание пользовательской политики без каких-либо предварительных условий**. Ваше предприятие может иметь собственные требования к мониторингу определенных типов данных, которые, как известно, существуют в системе обмена сообщениями. Вы можете создать настраиваемую политику самостоятельно, чтобы находить уникальные данные сообщений и действовать на ней. Необходимо знать требования и ограничения среды, в которой будет применяться политика защиты от потери данных для создания эффективных настраиваемых политик. Дополнительные сведения см. в статье Создание настраиваемой политики защиты от потери данных.

После добавления политики можно просмотреть и изменить ее правила, отключить политику или полностью удалить ее. Дополнительные сведения см. в разделе Управление политиками защиты от потери данных.

Типы конфиденциальной информации в политиках DLP

При создании или изменении политик защиты от потери данных можно включать правила, которые ищут конфиденциальную информацию. Типы конфиденциальной информации, перечисленные в разделе Типы конфиденциальной информации в Exchange Server, доступны для использования в политиках. Вы можете настроить условия в политике, например количество раз, которое необходимо найти перед

выполнением действия, или действие, которое необходимо выполнить. Дополнительные сведения о создании политик DLP см. в разделе Create a Custom DLP Policy. Дополнительные сведения о правилах потока обработки почты см. в разделе Правила потока обработки почты в Exchange Server.

Чтобы упростить использование правил, которые ищут конфиденциальную информацию, Exchange поставляется с шаблонами политик, которые уже включают некоторые типы конфиденциальной информации. Вы не можете добавить условия для всех типов конфиденциальной информации, так как шаблоны предназначены для того, чтобы помочь вам сосредоточиться на наиболее распространенных типах данных, связанных с соответствием требованиям в вашей организации. Дополнительные сведения о готовых шаблонах см. в разделе Шаблоны политик защиты от потери данных, предоставляемые в Exchange.

Вы можете создать множество политик защиты от потери данных для своей организации и включить их все, чтобы искать различные типы информации. Вы также можете создать политику защиты от потери данных, которая не основана на существующем шаблоне. Сведения о создании такой политики см. в статье Создание настраиваемой политики защиты от потери данных. Дополнительные сведения о доступных типах конфиденциальной информации см. в разделе Типы конфиденциальной информации в Exchange Server.

Определение важных данный в форме с помощью функции создания отпечатков документов

Exchange позволяет использовать отпечатки документов , чтобы легко создать тип конфиденциальной информации, основанный на стандартной форме.

Подсказки политик уведомляют пользователей о конфиденциальном контенте

Сообщения в подсказках политик можно использовать для информирования отправителей сообщений электронной почты о возможных проблемах с соблюдением норм при составлении сообщений электронной почты. При настройке подсказки политики в политике защиты от потери данных уведомление будет отображаться только в том случае, если что-то в сообщении электронной почты отправителя соответствует условиям, описанным в политике. Советы по

политике похожи на подсказки, представленные в Exchange 2010. Подробнее см. в разделе Policy Tips.

Обнаружение конфиденциальной информации наряду с классификацией обычных сообщений

Ключевым фактором надежности решения защиты от потери данных является возможность правильно определять конфиденциальное или конфиденциальное содержимое, которое может быть уникальным для вашей организации, нормативных требований, географического расположения или других бизнес-потребностей. Архитектура DLP Exchange использует глубокий анализ содержимого в сочетании с критериями обнаружения, которые устанавливаются с помощью правил в политиках защиты от потери данных. Чтобы предотвратить потерю данных в Exchange, необходимо настроить соответствующий набор правил конфиденциальной информации, которые обеспечивают высокую степень защиты, сводя к минимуму перебои в потоке обработки почты, вызванные ложноположительными и отрицательными результатами. Эти типы правил (которые называются в сведениях о защите от потери данных как *обнаружение конфиденциальной информации*) функционируют в рамках правил потока обработки почты, чтобы включить возможности защиты от потери данных. Дополнительные сведения об этих функциях см. в статье Интеграция правил конфиденциальной информации с правилами потока обработки почты.

Вы по-прежнему можете применять традиционные классификации сообщений к сообщениям и объединять эти классификации с обнаружением конфиденциальной информации. Эти функции можно использовать вместе в рамках одной политики защиты от потери данных или управлять ими независимо (параллельно). Дополнительные сведения о традиционных классификациях сообщений Exchange 2010 см. в статье Основные сведения о классификациях сообщений.

Сведения о сообщениях, обработанных в DLP

Сведения о сообщениях, содержащих обнаружения политики защиты от потери данных в вашей среде, см. в разделах Просмотр отчетов об обнаружении политики защиты от потери данных и Создание отчетов об инцидентах для обнаружения политик защиты от потери данных. Данные, связанные с обнаружением защиты от потери данных, тесно интегрированы в отчеты о доставке.

Дополнительные сведения

- Политика обмена сообщениями и соответствие требованиям в Exchange Server
- DLP Procedures
- Просмотр отчетов об обнаружении политики защиты от потери данных)
- Создание отпечатка документа

Типы конфиденциальной информации в Exchange Server

Статья • 04.04.2023

Защита от потери данных включает 80 типов конфиденциальной информации, готовых к использованию в соответствующих политиках. В этой статье перечислены все эти типы конфиденциальной информации и показано, каким именно образом политика защиты от потери данных выявляет каждый тип. Тип конфиденциальной информации определяется шаблоном, который можно идентифицировать регулярным выражением или функцией. Кроме того, для идентификации типа конфиденциальной информации могут использоваться подкрепляющие доказательства, такие как ключевые слова и контрольные суммы. Уровень вероятности и расположение слов и знаков также используются в процессе оценки.

Код банка ABA

Формат: девять цифр, которые могут иметь форматированный или неформатированный шаблон.

Шаблон:

Форматированные:

- четыре цифры, начиная с 0, 1, 2, 3, 6, 7 или 8;
- дефис;
- четыре цифры;
- дефис;
- цифра.

Неформатировано: девять последовательных цифр, начиная с 0, 1, 2, 3, 6, 7 или 8

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_aba_routing` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_ABA_Routing`.

```
<!-- ABA Routing Number -->
<Entity id="cb353f78-2b72-4c3c-8827-92ebe4f69fdf" patternsProximity="300" recommendedConfidence="75">
      <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_aba_routing" />
        <Match idRef="Keyword_ABA_Routing" />
      </Pattern>
 </Entity>
```

Ключевые слова:

Keyword_ABA_Routing

Keyword_ABA_Routing
Aba aba# aba routing # aba routing number Aba # abarouting # aba number abaroutingnumber american bank association routing # american bank association routing number americanbankassociationrouting # americanbankassociationroutingnumber bank routing number маршрутизация банка # bank routing number routing transit number Rtn

Номер внутреннего удостоверения личности для Аргентины (DNI)

Формат: восемь цифр, разделенных точками

Шаблон: восемь цифр:

- две цифры;
- точка;
- три цифры;
- точка;
- три цифры;

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_argentina_national_id` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_argentina_national_id`.

```
<!-- Argentina National Identity (DNI) Number -->
<Entity id="eefbb00e-8282-433c-8620-8f1da3bffdb2" recommendedConfidence="75" patternsProximity="300">
   <Pattern confidenceLevel="75">
      <IdMatch idRef="Regex_argentina_national_id"/>
      <Match idRef="Keyword_argentina_national_id"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_argentina_national_id
Argentina National Identity number Удостоверение Удостоверение личности Dni Национальный реестр лиц NIC Documento Nacional de Identidad Registro Nacional de las Personas Identidad Identificación

Номер банковского счета для Австралии

Формат: 6–10 цифр с номером банковского государственного филиала или без нее

Шаблон: номер счета — 6–10 цифр. Номер филиала государственного банка Австралии

- Три цифры
- дефис;
- Три цифры

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_australia_bank_account_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_australia_bank_account_number`.
- Регулярное выражение `Regex_australia_bank_account_number_bsb` находит содержимое, соответствующее шаблону.

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_australia_bank_account_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_australia_bank_account_number`.

```
<!-- Australia Bank Account Number -->
<Entity id="74a54de9-2a30-4aa0-a8aa-3d9327fc07c7" patternsProximity="300" recommendedConfidence="75">
  <Pattern confidenceLevel="85">
        <IdMatch idRef="Regex_australia_bank_account_number" />
        <Match idRef="Keyword_australia_bank_account_number" />
        <Match idRef="Regex_australia_bank_account_number_bsb" />
  </Pattern>
  <Pattern confidenceLevel="75">
        <IdMatch idRef="Regex_australia_bank_account_number" />
        <Match idRef="Keyword_australia_bank_account_number" />
  </Pattern>
 </Entity>
```

Ключевые слова:

Keyword_australia_bank_account_number
swift bank code correspondent bank base currency usa account holder address bank address information account fund transfers bank charges bank details banking information full names Идея

Номер водительского удостоверения для Австралии

Формат: девять букв и цифр

Шаблон: девять букв и цифр:

- две цифры или буквы (без учета регистра);

- две цифры;
- пять цифр или букв (без учета регистра).

  ИЛИ

- 1–2 дополнительные буквы (без учета регистра);
- 4–9 цифр.

  ИЛИ

- девять цифр или букв (без учета регистра).

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_australia_drivers_license_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_australia_drivers_license_number`.
- Ключевое слово из не `Keyword_australia_drivers_license_number_exclusions` найдено.

```
<!-- Australia Drivers License Number -->
<Entity id="1cbbc8f5-9216-4392-9eb5-5ac2298d1356" patternsProximity="300" recommendedConfidence="75">
   <Pattern confidenceLevel="75">
        <IdMatch idRef="Regex_australia_drivers_license_number" />
        <Match idRef="Keyword_australia_drivers_license_number" />
        <Any minMatches="0" maxMatches="0">
          <Match idRef="Keyword_australia_drivers_license_number_exclusions" />
        </Any>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_australia_drivers_license_number	**Keyword_australia_drivers_license_number_exclusions**

Keyword_australia_drivers_license_number	Keyword_australia_drivers_license_number_exclusions
international driving permits	Aaa
australian automobile association	DriverLicense
Сидней nsw	DriverLicenses
international driving permit	Driver License
DriverLicence	Driver Licenses
DriverLicences	ДрайверыЛицензии
Driver Lic	ДрайверыЛицензии
Driver Licence	Drivers License
Driver Licences	Drivers Licenses
DriversLic	Водительские права
ДрайверыЛицензация	Водительские лицензии
ДрайверыЛицензии	Driver' License
Drivers Lic	Driver' Licenses
Drivers Lics	Лицензия драйвера
Drivers Licence	Лицензии драйвера
Drivers Licences	Driver's License
Driver'Lic	Driver's Licenses
Driver'Lics	DriverLicense #
Водительские права	DriverLicenses #
Водительские права	Driver License#
Driver' Lic	Driver Licenses#
Driver' Lics	ДрайверыЛицензии #
Driver' Licence	ДрайверыЛицензии #
Driver' Licences	Drivers License#
Driver'sLic	Drivers Licenses#
Driver'sLics	Водительские права #
Водительская лицензия	Водительские лицензии #
Лицензий драйверов	Driver' License#
Driver's Lic	Driver' Licenses#
Driver's Lics	Лицензия драйвера #
Driver's Licence	Лицензии драйвера #
Driver's Licences	Driver's License#
DriverLic #	Driver's Licenses#
DriverLics #	
DriverLicence #	
DriverLicences #	
Driver Lic#	
Driver Lics#	
Driver Licence#	
Driver Licences#	
DriversLic #	
DriversLics #	
ДрайверыЛицензация #	
ДрайверыЛицензии #	
Drivers Lic#	
Drivers Lics#	
Drivers Licence#	
Drivers Licences#	
Driver'Lic #	
Driver'Lics #	
Водительские права #	
Водительские права #	
Driver' Lic#	
Driver' Lics#	
Driver' Licence#	
Driver' Licences#	
Driver'sLic #	
Driver'sLics #	
Водительская лицензия #	
Лицензий драйверов #	
Driver's Lic#	
Driver's Lics#	
Driver's Licence#	
Driver's Licences#	

Номер карты медицинского страхования для Австралии

Формат: 10–11 цифр

Шаблон: 10–11 цифр:

- Первая цифра находится в диапазоне 2–6.
- Девятая цифра — проверочная.
- Десятая цифра — цифра серии.
- Одиннадцатая цифра (необязательно) — индивидуальный номер.

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 95 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_australian_medical_account_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_Australia_Medical_Account_Number`.
- контрольная сумма проходит проверку.

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_australian_medical_account_number` находит содержимое, соответствующее шаблону.
- Контрольная сумма проходит проверку.

```
<!-- Australia Medical Account Number -->
<Entity id="104a99a0-3d3b-4542-a40d-ab0b9e1efe63" recommendedConfidence="85" patternsProximity="300">
    <Pattern confidenceLevel="95">
     <IdMatch idRef="Func_australian_medical_account_number"/>
     <Any minMatches="1">
     <Match idRef="Keyword_Australia_Medical_Account_Number"/>
     </Any>
  </Pattern>
<Pattern confidenceLevel="85">
     <IdMatch idRef="Func_australian_medical_account_number"/>
     <Any minMatches="0" maxMatches="0">
  <Match idRef="Keyword_Australia_Medical_Account_Number"/>
     </Any>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_Australia_Medical_Account_Number
bank account details medicare payments mortgage account bank payments information branch credit card loan department of human services local service Medicare

Номер паспорта гражданина Австралии

Формат: буква, за которой следует семь цифр.

Шаблон: буква (без учета регистра), за которой следуют семь цифр.

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_australia_passport_number` находит содержимое, соответствующее шаблону.
- Найдено ключевое слово из `Keyword_passport` или `Keyword_australia_passport_number` .

```
<!-- Australia Passport Number -->
<Entity id="29869db6-602d-4853-ab93-3484f905df50" patternsProximity="300" recommendedConfidence="75">
  <Pattern confidenceLevel="75">
        <IdMatch idRef="Regex_australia_passport_number" />
        <Any minMatches="1">
          <Match idRef="Keyword_passport" />
          <Match idRef="Keyword_australia_passport_number" />
        </Any>
   </Pattern>
</Entity>
```

Ключевые слова:

Keyword_passport	Keyword_australia_passport_number
Passport Number	Паспорт
Passport No	passport details
Passport#	immigration and citizenship
Паспорт #	commonwealth of australia
PassportID	department of immigration
Passportno	residential address
passportnumber	department of immigration and citizenship
パスポート	Визы
パスポート番号	national identity card
パスポートのNum	passport number
パスポート#	travel document
Numéro de passeport	issuing authority
Passeport n °	
Passeport Non	
Passeport#	
Passeport #	
PasseportNon	
Passeportn °	

Номер налогоплательщика для Австралии

Формат: 8–9 цифр

Шаблон: 8–9 цифры обычно представлены пробелами следующим образом:

- Три цифры
- Необязательный пробел
- Три цифры
- Необязательный пробел
- 2–3 цифры, причем последняя цифра — контрольная

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 95 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_australian_tax_file_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_Australia_Tax_File_Number`.
- Ключевое слово из не `Keyword_number_exclusions` найдено.
- контрольная сумма проходит проверку.

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_australian_tax_file_number` находит содержимое, соответствующее шаблону.
- Ключевое слово из `Keyword_Australia_Tax_File_Number` или `Keyword_number_exclusions` не найдено.
- Контрольная сумма проходит проверку.

```
<!-- Australia Tax File Number -->
<Entity id="e29bc95f-ff70-4a37-aa01-04d17360a4c5" patternsProximity="300" recommendedConfidence="85">
    <Pattern confidenceLevel="95">
        <IdMatch idRef="Func_australian_tax_file_number" />
        <Any minMatches="1">
          <Match idRef="Keyword_Australia_Tax_File_Number" />
        </Any>
        <Any minMatches="0" maxMatches="0">
          <Match idRef="Keyword_number_exclusions" />
        </Any>
  </Pattern>
  <Pattern confidenceLevel="85">
        <IdMatch idRef="Func_australian_tax_file_number" />
        <Any minMatches="0" maxMatches="0">
          <Match idRef="Keyword_Australia_Tax_File_Number" />
          <Match idRef="Keyword_number_exclusions" />
        </Any>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_Australia_Tax_File_Number	Keyword_number_exclusions
australian business number	00000000
marginal tax rate	11111111
medicare levy	22222222
portfolio number	33333333
service veterans	44444444
withholding tax	55555555
individual tax return	66666666
tax file number	77777777
	88888888
	99999999
	000000000
	111111111
	222222222
	333333333
	444444444
	555555555
	666666666
	777777777
	888888888
	999999999
	0000000000
	1111111111
	2222222222
	3333333333
	4444444444
	5555555555
	6666666666
	7777777777
	8888888888
	9999999999

Внутренний идентификационный номер гражданина Бельгии

Формат: 11 цифр плюс разделители

Шаблон: 11 цифр плюс разделители:

- шесть цифр и две точки в формате ГГ.ММ.ДД для даты рождения;

- дефис;
- три последовательные цифры (нечетные для мужчин, четные для женщин);
- точка;
- две проверочные цифры.

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_belgium_national_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_belgium_national_number`.
- Контрольная сумма проходит проверку.

```
<!-- Belgium National Number -->
  <Entity id="fb969c9e-0fd1-4b18-8091-a2123c5e6a54" recommendedConfidence="75" patternsProximity="300">
   <Pattern confidenceLevel="75">
     <IdMatch idRef="Func_belgium_national_number"/>
     <Match idRef="Keyword_belgium_national_number"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_belgium_national_number
Удостоверение Регистрация Идентификации Идентификатор Identiteitskaart Registratie nummer Identificatie nummer Identiteit Registratie Идентификация Carte d'identité numéro d'immatriculation numéro d'identification identité Надпись Идентификация Identifizierung Identifikationsnummer Personalausweis Registrierung Registrationsnummer

Номер юридического лица для Бразилии (CNPJ)

Формат: 14 цифр, включая регистрационный номер, номер ветви и контрольные цифры, а также разделители

Шаблон: 14 цифр, плюс разделители:

- две цифры;
- точка;
- три цифры;
- точка;
- три цифры (эти первые восемь цифр — регистрационный номер);

- косая черта;
- номер отделения из четырех цифр;
- дефис;
- Две цифры, которые являются контрольными цифрами

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_brazil_cnpj` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_brazil_cnpj`.
- Контрольная сумма проходит проверку.

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_brazil_cnpj` находит содержимое, соответствующее шаблону.
- Контрольная сумма проходит проверку.

```
<!-- Brazil Legal Entity Number (CNPJ) -->
<Entity id="9b58b5cd-5e90-4df6-b34f-1ebcc88ceae4" recommendedConfidence="85" patternsProximity="300">
   <Pattern confidenceLevel="85">
     <IdMatch idRef="Func_brazil_cnpj"/>
     <Match idRef="Keyword_brazil_cnpj"/>
  </Pattern>
  <Pattern confidenceLevel="75">
     <IdMatch idRef="Func_brazil_cnpj"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_brazil_cnpj
CNPJ CNPJ/MF CNPJ-MF National Registry of Legal Entities Taxpayers Registry Legal entity Legal entities Registration Status Для бизнеса Организация CNPJ Cadastro Nacional da Pessoa Jurídica Cadastro Geral de Contribuintes CGC Pessoa jurídica Pessoas jurídicas Situação cadastral Inscrição Empresa

Номер CPF для Бразилии

Формат: 11 цифр, которые включают контрольную цифру и могут быть отформатированы или отформатированы.

Шаблон:

Форматированные:

- три цифры;
- точка;
- три цифры;
- точка;
- три цифры;
- дефис;
- две проверочные цифры.

Неформатировано: 11 цифр, где последние две цифры являются контрольными.

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_brazil_cpf` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_brazil_cpf`.
- Контрольная сумма проходит проверку.

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_brazil_cpf` находит содержимое, соответствующее шаблону.
- Контрольная сумма проходит проверку.

```
<!-- Brazil CPF Number -->
<Entity id="78e09124-f2c3-4656-b32a-c1a132cd2711" recommendedConfidence="85" patternsProximity="300">
  <Pattern confidenceLevel="85">
     <IdMatch idRef="Func_brazil_cpf"/>
     <Match idRef="Keyword_brazil_cpf"/>
  </Pattern>
  <Pattern confidenceLevel="75">
     <IdMatch idRef="Func_brazil_cpf"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_brazil_cpf
Cpf Идентификации Регистрация Доходов Cadastro de Pessoas Físicas Imposto Identificação Inscrição Receita

Номер внутреннего удостоверения личности для Бразилии (RG)

Формат:

- Registro Geral (старый формат): девять цифр плюс разделители
- Registro de Identidade (RIC) (новый формат): 11 цифр плюс дефис

Шаблон:

Registro Geral (старый формат):

- две цифры;
- точка;
- три цифры;
- точка;
- три цифры;
- дефис;
- одна цифра — проверочная.

Registro de Identidade (RIC) (новый формат):

- 10 цифр;
- дефис;
- одна цифра — проверочная.

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_brazil_rg` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_brazil_rg`.
- Контрольная сумма проходит проверку.

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_brazil_rg` находит содержимое, соответствующее шаблону.
- Контрольная сумма проходит проверку.

```
<!-- Brazil National ID Card (RG) -->
<Entity id="486de900-db70-41b3-a886-abdf25af119c" recommendedConfidence="85" patternsProximity="300">
  <Pattern confidenceLevel="85">
     <IdMatch idRef="Func_brazil_rg"/>
     <Match idRef="Keyword_brazil_rg"/>
  </Pattern>
  <Pattern confidenceLevel="75">
     <IdMatch idRef="Func_brazil_rg"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_brazil_rg
National ID Регистрация Cédula de identidade Registro Geral Rg Registro de Identidade Рик Número de registo Registro

Номер банковского счета для Канады

Формат: семь или двенадцать цифр

Шаблон: номер банковского счета в Канаде — семь или двенадцать цифр. Транзитный номер банковского счета в Канаде имеет указанный ниже формат.

- пять цифр;
- дефис;
- три цифры.

  ИЛИ

- ноль "0";
- Восемь цифр

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_canada_bank_account_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_canada_bank_account_number`.
- Регулярное выражение `Regex_canada_bank_account_transit_number` находит содержимое, соответствующее шаблону.

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_canada_bank_account_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_canada_bank_account_number`.

```
<!-- Canada Bank Account Number -->
<Entity id="552e814c-cb50-4d94-bbaa-bb1d1ffb34de" patternsProximity="300" recommendedConfidence="75">
  <Pattern confidenceLevel="85">
        <IdMatch idRef="Regex_canada_bank_account_number" />
        <Match idRef="Keyword_canada_bank_account_number" />
        <Match idRef="Regex_canada_bank_account_transit_number" />
   </Pattern>
   <Pattern confidenceLevel="75">
        <IdMatch idRef="Regex_canada_bank_account_number" />
        <Match idRef="Keyword_canada_bank_account_number" />
   </Pattern>
</Entity>
```

Ключевые слова:

Keyword_canada_bank_account_number

Keyword_canada_bank_account_number
canada savings bonds canada revenue agency canadian financial institution direct deposit form canadian citizen legal representative notary public commissioner for oaths child care benefit universal child care canada child tax benefit income tax benefit harmonized sales tax social insurance number income tax refund child tax benefit territorial payments institution number deposit request banking information direct deposit

Номер водительского удостоверения для Канады

Формат: зависит от провинции

Шаблон: различные узоры, охватывающие Альберту, Британскую Колумбию, Манитобу, Нью-Брансуик, Ньюфаундленд/Лабрадор, Новую Шотландию, Онтарио, остров Принца Эдуарда, Квебек и Саскачеван

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_[province_name]_drivers_license_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_[province_name]_drivers_license_name`.
- обнаружено ключевое слово из `Keyword_canada_drivers_license`.

```
<!-- Canada Driver's License Number -->
    <Entity id="37186abb-8e48-4800-ad3c-e3d1610b3db0" patternsProximity="300" recommendedConfidence="75">
      <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_alberta_drivers_license_number" />
        <Match idRef="Keyword_alberta_drivers_license_name" />
        <Match idRef="Keyword_canada_drivers_license" />
      </Pattern>
      <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_british_columbia_drivers_license_number" />
        <Match idRef="Keyword_british_columbia_drivers_license_name" />
        <Match idRef="Keyword_canada_drivers_license" />
      </Pattern>
      <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_manitoba_drivers_license_number" />
        <Match idRef="Keyword_manitoba_drivers_license_name" />
        <Match idRef="Keyword_canada_drivers_license" />
      </Pattern>
      <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_new_brunswick_drivers_license_number" />
        <Match idRef="Keyword_new_brunswick_drivers_license_name" />
        <Match idRef="Keyword_canada_drivers_license" />
      </Pattern>
      <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_newfoundland_labrador_drivers_license_number" />
        <Match idRef="Keyword_newfoundland_labrador_drivers_license_name" />
        <Match idRef="Keyword_canada_drivers_license" />
      </Pattern>
      <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_nova_scotia_drivers_license_number" />
```

```
      <Match idRef="Keyword_nova_scotia_drivers_license_name" />
      <Match idRef="Keyword_canada_drivers_license" />
    </Pattern>
    <Pattern confidenceLevel="75">
      <IdMatch idRef="Func_ontario_drivers_license_number" />
      <Match idRef="Keyword_ontario_drivers_license_name" />
      <Match idRef="Keyword_canada_drivers_license" />
    </Pattern>
    <Pattern confidenceLevel="75">
      <IdMatch idRef="Func_prince_edward_island_drivers_license_number" />
      <Match idRef="Keyword_prince_edward_island_drivers_license_name" />
      <Match idRef="Keyword_canada_drivers_license" />
    </Pattern>
    <Pattern confidenceLevel="75">
      <IdMatch idRef="Func_quebec_drivers_license_number" />
      <Match idRef="Keyword_quebec_drivers_license_name" />
      <Match idRef="Keyword_canada_drivers_license" />
    </Pattern>
    <Pattern confidenceLevel="75">
      <IdMatch idRef="Func_saskatchewan_drivers_license_number" />
      <Match idRef="Keyword_saskatchewan_drivers_license_name" />
      <Match idRef="Keyword_canada_drivers_license" />
    </Pattern>
  </Entity>
```

Ключевые слова:

Keyword_[province_name]_drivers_license_name	**Keyword_canada_drivers_license**
Аббревиатура провинции, например AB. Название провинции, например Альберта.	Dl Dls Cdl CDLS DriverLic DriverLics DriverLicense DriverLicenses DriverLicence DriverLicences Driver Lic Driver Lics Driver License Driver Licenses Driver Licence Driver Licences DriversLic DriversLics ДрайверыЛицензация ДрайверыЛицензии ДрайверыЛицензии ДрайверыЛицензии Drivers Lic Drivers Lics Drivers License Drivers Licenses Drivers Licence Drivers Licences Driver'Lic Driver'Lics Водительские права Водительские лицензии Водительские права Водительские права Driver' Lic Driver' Lics Driver' License Driver' Licenses Driver' Licence Driver' Licences Driver'sLic Driver'sLics Лицензия драйвера Лицензии драйвера Водительская лицензия Лицензий драйверов Driver's Lic

Keyword_[province_name]_drivers_license_name	Keyword_canada_drivers_license
	Driver's Lics
	Driver's License
	Driver's Licenses
	Driver's Licence
	Driver's Licences
	Permis de Conduire
	id
	ids
	idcard number
	idcard numbers
	idcard#
	idcard #s
	idcard card
	idcard cards
	idcard
	identification number
	identification numbers
	identification #
	identification #s
	identification card
	identification cards
	Идентификации
	Dl #
	Dls #
	Cdl #
	CDLS #
	DriverLic #
	DriverLics #
	DriverLicense #
	DriverLicenses #
	DriverLicence #
	DriverLicences #
	Driver Lic#
	Driver Lics#
	Driver License#
	Driver Licenses#
	Driver License#
	Driver Licences#
	DriversLic #
	DriversLics #
	ДрайверыЛицензии #
	ДрайверыЛицензии #
	ДрайверыЛицензация #
	ДрайверыЛицензии #
	Drivers Lic#
	Drivers Lics#
	Drivers License#
	Drivers Licenses#
	Drivers Licence#
	Drivers Licences#
	Driver'Lic #
	Driver'Lics #
	Водительские права #
	Водительские лицензии #
	Водительские права #
	Водительские права #
	Driver' Lic#
	Driver' Lics#
	Driver' License#
	Driver' Licenses#
	Driver' Licence#
	Driver' Licences#
	Driver'sLic #
	Driver'sLics #
	Лицензия драйвера #
	Лицензии драйвера #
	Водительская лицензия #
	Лицензий драйверов #
	Driver's Lic#
	Driver's Lics#
	Driver's License#
	Driver's Licenses#
	Driver's Licence#

Keyword_[province_name]_drivers_license_name	Keyword_canada_drivers_license
	Driver's Licences# Permis de Conduire# Id # Идентификаторы # idcard card# idcard cards# idcard # identification card# identification cards# Идентификации #

Номер службы здравоохранения для Канады

Формат: 10 цифр

Шаблон: 10 цифр

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_canada_health_service_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_canada_health_service_number`.

```
<!-- Canada Health Service Number -->
<Entity id="59c0bf39-7fab-482c-af25-00faa4384c94" patternsProximity="300" recommendedConfidence="75">
  <Pattern confidenceLevel="75">
        <IdMatch idRef="Regex_canada_health_service_number" />
        <Any minMatches="1">
          <Match idRef="Keyword_canada_health_service_number" />
        </Any>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_canada_health_service_number
personal health number patient information health services speciality services automobile accident patient hospital Психиатр workers compensation Инвалидности

Номер паспорта гражданина Канады

Формат: две прописные буквы, за которыми следуют шесть цифр.

Шаблон: две прописные буквы, за которыми следуют шесть цифр

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_canada_passport_number` находит содержимое, соответствующее шаблону.

- Найдено ключевое слово из `Keyword_canada_passport_number` или `Keyword_passport` .

```
<!-- Canada Passport Number -->
<Entity id="14d0db8b-498a-43ed-9fca-f6097ae687eb" patternsProximity="300" recommendedConfidence="75">
  <Pattern confidenceLevel="75">
        <IdMatch idRef="Regex_canada_passport_number" />
        <Any minMatches="1">
          <Match idRef="Keyword_canada_passport_number" />
          <Match idRef="Keyword_passport" />
        </Any>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_canada_passport_number	Keyword_passport
canadian citizenship canadian passport passport application passport photos certified translator canadian citizens processing times renewal application	Passport Number Passport No Passport# Паспорт # PassportID Passportno passportnumber パスポート パスポート番号 パスポートのNum パスポート# Numéro de passeport Passeport n ° Passeport Non Passeport# Passeport # PasseportNon Passeportn °

Персональный идентификационный номер службы здравоохранения для Канады (PHIN)

Формат: девять цифр

Шаблон: девять цифр

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_canada_phin` находит содержимое, соответствующее шаблону.
- Найдено по крайней мере два ключевых слова из `Keyword_canada_phin` или `Keyword_canada_provinces` ..

```
<!-- Canada PHIN -->
<Entity id="722e12ac-c89a-4ec8-a1b7-fea3469f89db" patternsProximity="300" recommendedConfidence="75">
  <Pattern confidenceLevel="75">
        <IdMatch idRef="Regex_canada_phin" />
        <Any minMatches="2">
          <Match idRef="Keyword_canada_phin" />
          <Match idRef="Keyword_canada_provinces" />
        </Any>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_canada_phin	Keyword_canada_provinces
social insurance number	Нунавут
health information act	Квебек
income tax information	Northwest Territories
manitoba health	Онтарио
health registration	British Columbia
prescription purchases	Альберта
benefit eligibility	Саскачеван
personal health	Манитоба
power of attorney	Юкон
registration number	Newfoundland and Labrador
personal health number	New Brunswick
practitioner referral	Nova Scotia
wellness professional	Prince Edward Island
patient referral	Канада
health and wellness	

Номер карты социального страхования для Канады

Формат: девять цифр с необязательными дефисами или пробелами

Шаблон:

Форматированные:

- Три цифры
- Дефис или пробел
- Три цифры
- Дефис или пробел
- Три цифры

Неформатировано: девять цифр

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_canadian_sin` находит содержимое, соответствующее шаблону.
- По крайней мере два из следующих сочетаний:
  - обнаружено ключевое слово из `Keyword_sin`.
  - обнаружено ключевое слово из `Keyword_sin_collaborative`.
  - Функция `Func_eu_date` находит дату в правильном формате даты.
- Контрольная сумма проходит проверку.

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_unformatted_canadian_sin` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_sin`.
- Контрольная сумма проходит проверку.

```
<!-- Canada Social Insurance Number -->
<Entity id="a2f29c85-ecb8-4514-a610-364790c0773e" patternsProximity="300" recommendedConfidence="75">
  <Pattern confidenceLevel="85">
        <IdMatch idRef="Func_canadian_sin" />
```

```
        <Any minMatches="2">
          <Match idRef="Keyword_sin" />
          <Match idRef="Keyword_sin_collaborative" />
          <Match idRef="Func_eu_date" />
        </Any>
  </Pattern>
  <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_unformatted_canadian_sin" />
        <Match idRef="Keyword_sin" />
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_sin	Keyword_sin_collaborative
sin	driver's license
social insurance	drivers license
numero d'assurance sociale	driver's licence
Грехи	drivers licence
Ssn	Dob
ssns	Birthdate
social security	Birthday
numero d'assurance social	Date of Birth
national identification number	
national id	
Грех #	
soc ins	
social ins	

Номер удостоверения личности для Чили

Формат: 7–8 цифр плюс разделители контрольной цифры или буквы

Шаблон: 7–8 цифр плюс разделители:

- 1 или 2 цифры;
- точка;
- три цифры;
- точка;
- три цифры;
- тире;
- одна цифра или буква (без учета регистра) — проверочная.

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_chile_id_card` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_chile_id_card`.
- Контрольная сумма проходит проверку.

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_chile_id_card` находит содержимое, соответствующее шаблону.
- Контрольная сумма проходит проверку.

```
<!-- Chile Identity Card Number -->
<Entity id="4e979794-49a0-407e-a0b9-2c536937b925" recommendedConfidence="85" patternsProximity="300">
  <Pattern confidenceLevel="85">
     <IdMatch idRef="Func_chile_id_card"/>
     <Match idRef="Keyword_chile_id_card"/>
  </Pattern>
  <Pattern confidenceLevel="75">
     <IdMatch idRef="Func_chile_id_card"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_chile_id_card
National Identification Number Identity card Идентификатор Идентификации Rol Único Nacional Запустить Rol Único Tributario Колею Cédula de Identidad Número De Identificación Nacional Tarjeta de identificación Identificación

Номер удостоверения личности жителя Китая (KHP)

Формат: 18 цифр

Шаблон: 18 цифр:

- шесть цифр — код адреса;
- Восемь цифр в форме ГГГГММДД, которые являются датой рождения
- Три цифры, которые являются кодом заказа
- Одна цифра, которая является контрольной цифрой

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_china_resident_id` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_china_resident_id`.
- Контрольная сумма проходит проверку.

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_china_resident_id` находит содержимое, соответствующее шаблону.
- Контрольная сумма проходит проверку.

```
<!-- China Resident Identity Card (PRC) Number -->
<Entity id="c92daa86-2d16-4871-901f-816b3f554fc1" recommendedConfidence="85" patternsProximity="300">
  <Pattern confidenceLevel="85">
     <IdMatch idRef="Func_china_resident_id"/>
     <Match idRef="Keyword_china_resident_id"/>
  </Pattern>
  <Pattern confidenceLevel="75">
     <IdMatch idRef="Func_china_resident_id"/>
```

```
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_china_resident_id
Resident Identity Card Knp National Identification Card 身份证 居民 身份证 居民身份证 鉴定 身分證 居民 身份證 鑑定

Номер кредитной карты

Формат: 14 цифр, которые могут быть отформатированы или неформатированы (dddddd) и должны пройти тест Luhn.

Шаблон: очень сложный и надежный шаблон, который обнаруживает карты всех основных брендов по всему миру, включая Visa, MasterCard, Discover Card, JCB, American Express, подарочные карты и закусочные карты.

Контрольная сумма: Да, контрольная сумма Luhn

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_credit_card` находит содержимое, соответствующее шаблону.
- Верно одно из условий ниже:
  - обнаружено ключевое слово из `Keyword_cc_verification`.
  - обнаружено ключевое слово из `Keyword_cc_name`.
  - Функция `Func_expiration_date` находит дату в правильном формате даты.
- Контрольная сумма проходит проверку.

Политика защиты от потери данных с вероятностью в 65 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, отдаленном не более чем на 300 знаков:

- Функция `Func_credit_card` находит содержимое, соответствующее шаблону.
- Контрольная сумма проходит проверку.

```
<!-- Credit Card Number -->
<Entity id="50842eb7-edc8-4019-85dd-5a5c1f2bb085" patternsProximity="300" recommendedConfidence="85">
  <Pattern confidenceLevel="85">
        <IdMatch idRef="Func_credit_card" />
        <Any minMatches="1">
          <Match idRef="Keyword_cc_verification" />
          <Match idRef="Keyword_cc_name" />
          <Match idRef="Func_expiration_date" />
        </Any>
  </Pattern>
  <Pattern confidenceLevel="65">
        <IdMatch idRef="Func_credit_card" />
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_cc_verification	Keyword_cc_name

Keyword_cc_verification	Keyword_cc_name
card verification	Amex
card identification number	american express
Cvn	americanexpress
cid	Визы
cvc2	Mastercard
cvv2	master card
pin block	Mc
security code	masters
security number	master cards
security no	diner's Club
issue number	diners club
issue no	dinersclub
криптограмма	discover card
numéro de sécurité	discovercard
numero de securite	discover cards
kreditkartenprüfnummer	Jcb
kreditkartenprufnummer	japanese card bureau
prüfziffer	carte blanche
prufziffer	Картбланш
sicherheits Kode	credit card
sicherheitscode	См3 #
sicherheitsnummer	cc#:
verfalldatum	expiration date
codice di verifica	exp date
Трески. sicurezza	expiry date
cod sicurezza	date d'expiration
n autorizzazione	date d'exp
código	date expiration
codigo	bank card
Трески. Seg	банковская карта
cod seg	card number
código de segurança	card num
codigo de seguranca	cardnumber
codigo de segurança	cardnumbers
código de seguranca	card numbers
cód. segurança	кредитная карта
Трески. seguranca треска. segurança	credit cards
cód. seguranca	кредитные карты
cód segurança	Ccn
cod seguranca cod segurança	card holder
cód seguranca	Карточки
número de verificação	card holders
numero de verificacao	Держателей карт
ablauf	check card
gültig bis	checkcard
gültigkeitsdatum	check cards
gultig bis	контрольные знаки
gultigkeitsdatum	debit card
scadenza	дебетовая карта
data scad	debit cards
fecha de expiracion	дебетовые карты
fecha de venc	atm card
vencimiento	atmcard
válido hasta	atm cards
valido hasta	atmcards
vto	Пути
data de expiração	en route
data de expiracao	card type
data em que expira	carte bancaire
validade	carte de crédit
Доблести	carte de credit
vencimento	numéro de carte
Венк	numero de carte
	nº de la carte
	nº de carte
	kreditkarte
	karte
	karteninhaber
	karteninhabers
	kreditkarteninhaber
	kreditkarteninstitut
	kreditkartentyp
	eigentümername

Keyword_cc_verification	Keyword_cc_name
	kartennr kartennummer kreditkartennummer kreditkarten-nummer carta di credito carta credito N. Carta n carta Nr. Carta nr carta numero carta numero della carta numero di carta tarjeta credito tarjeta de credito tarjeta crédito tarjeta de crédito tarjeta de atm tarjeta atm tarjeta debito tarjeta de debito tarjeta débito tarjeta de débito nº de tarjeta Нет. de tarjeta no de tarjeta numero de tarjeta número de tarjeta tarjeta no tarjetahabiente cartão de crédito cartão de credito cartao de crédito cartao de credito cartão de débito cartao de débito cartão de debito cartao de debito débito automático debito automatico número do cartão numero do cartão número do cartao numero do cartao número de cartão numero de cartão número de cartao numero de cartao nº do cartão nº do cartao n º. do cartão no do cartão no do cartao Нет. do cartão Нет. do cartao

Номер идентификационной карты гражданина Хорватии

Формат: девять цифр

Шаблон: девять последовательных цифр

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_croatia_id_card` находит содержимое, соответствующее шаблону.

- обнаружено ключевое слово из `Keyword_croatia_id_card`.

```
<!--Croatia Identity Card Number-->
<Entity id="ff12f884-c20a-4189-b185-34c8e7258d47" recommendedConfidence="75" patternsProximity="300">
  <Pattern confidenceLevel="75">
     <IdMatch idRef="Func_croatia_id_card"/>
     <Match idRef="Keyword_croatia_id_card"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_croatia_id_card
Croatian identity card Osobna iskaznica

Персональный идентификационный номер (OIB) гражданина Хорватии

Формат: 10 цифр

Шаблон: 10 цифр:

- Шесть цифр в форме ДДММГГ, которые являются датой рождения
- четыре цифры, где последняя цифра — проверочная.

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_croatia_oib_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_croatia_oib_number`.
- Контрольная сумма проходит проверку.

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_croatia_oib_number` находит содержимое, соответствующее шаблону.
- Контрольная сумма проходит проверку.

```
<!-- Croatia Personal Identification (OIB) Number -->
<Entity id="31983b6d-db95-4eb2-a630-b44bd091968d" recommendedConfidence="85" patternsProximity="300">
  <Pattern confidenceLevel="85">
     <IdMatch idRef="Func_croatia_oib_number"/>
     <Match idRef="Keyword_croatia_oib_number"/>
  </Pattern>
  <Pattern confidenceLevel="75">
     <IdMatch idRef="Func_croatia_oib_number"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_croatia_oib_number
Personal Identification Number Osobni identifikacijski broj OIB

Номер внутренней идентификационной карты гражданина Чехии

Формат: 10 цифр, содержащих косую черту

Шаблон: 10 цифр:

- Шесть цифр, которые являются датой рождения
- косая черта;
- четыре цифры, где последняя цифра — проверочная.

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_czech_id_card` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_czech_id_card`.
- Контрольная сумма проходит проверку.

```
<!-- Czech National Identity Card Number -->
<Entity id="60c0725a-4eb6-455b-9dda-05d8a7396497" recommendedConfidence="85" patternsProximity="300">
  <Pattern confidenceLevel="85">
     <IdMatch idRef="Func_czech_id_card"/>
     <Match idRef="Keyword_czech_id_card"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_czech_id_card
Czech national identity card Občanský průka

Персональный идентификационный номер гражданина Дании

Формат: 10 цифр, содержащих дефис

Шаблон: 10 цифр:

- Шесть цифр в формате ДДММГГ, которые являются датой рождения
- дефис;
- четыре цифры, где последняя цифра — проверочная.

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_denmark_id` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_denmark_id`.
- Контрольная сумма проходит проверку.

```
<!-- Denmark Personal Identification Number -->
<Entity id="6c4f2fef-56e1-4c00-8093-88d7a01cf460" recommendedConfidence="75" patternsProximity="300">
```

```
  <Pattern confidenceLevel="75">
     <IdMatch idRef="Regex_denmark_id"/>
     <Match idRef="Keyword_denmark_id"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_denmark_id
Personal Identification Number Cpr Det Centrale Personregister Personnummer

Номер Управления по борьбе с наркотиками США (DEA)

Формат: две буквы, за которыми следуют семь цифр

Шаблон: шаблон должен включать все следующие компоненты:

- Одна буква (без учета регистра) из следующего набора: abcdefghjklmnprstux, представляющая собой код регистрирующегося лица
- Одна буква (без учета регистра), представляющая собой первую букву фамилии регистрирующегося лица
- Семь цифр, последняя из которых — контрольная

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_dea_number` находит содержимое, соответствующее шаблону.
- Контрольная сумма проходит проверку.

```
<!-- DEA Number -->
<Entity id="9a5445ad-406e-43eb-8bd7-cac17ab6d0e4" recommendedConfidence="85" patternsProximity="300">
  <Pattern confidenceLevel="85">
     <IdMatch idRef="Func_dea_number"/>
  </Pattern>
</Entity>
```

Ключевые слова: None

Номер банковской карты, Европейский союз

Формат: 16 цифр

Шаблон: очень сложный и надежный шаблон

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_eu_debit_card` находит содержимое, соответствующее шаблону.
- Верно по меньшей мере одно из условий ниже:
  - обнаружено ключевое слово из `Keyword_eu_debit_card`.
  - обнаружено ключевое слово из `Keyword_card_terms_dict`.

- обнаружено ключевое слово из `Keyword_card_security_terms_dict`.
- обнаружено ключевое слово из `Keyword_card_expiration_terms_dict`.
- Функция `Func_eu_date1` находит дату в правильном формате даты.
- Функция `Func_eu_date2` находит дату в правильном формате даты.

- Контрольная сумма проходит проверку.

```
<!-- EU Debit Card Number -->
<Entity id="0e9b3178-9678-47dd-a509-37222ca96b42" patternsProximity="300" recommendedConfidence="85">
  <Pattern confidenceLevel="85">
        <IdMatch idRef="Func_eu_debit_card" />
        <Any minMatches="1">
          <Match idRef="Keyword_eu_debit_card" />
          <Match idRef="Keyword_card_terms_dict" />
          <Match idRef="Keyword_card_security_terms_dict" />
          <Match idRef="Keyword_card_expiration_terms_dict" />
          <Match idRef="Func_expiration_date" />
          <Match idRef="Func_eu_date" />
          <Match idRef="Func_eu_date1" />
          <Match idRef="Func_eu_date2" />
        </Any>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_eu_debit_card	**Keyword_card_terms_dict**	**Keyword_card_security_terms_dict**	**Keyword_card_expiration_terms_dict**
account number	acct nbr	card identification number	ablauf
card number	acct num	card verification	data de expiracao
card no.	acct no	cardi la verifica	data de expiração
security number	american express	cid	data del exp
См3 #	americanexpress	cod seg	data di exp
	americano espresso	cod seguranca	data di scadenza
	Amex	cod segurança	data em que expira
	atm card	cod sicurezza	data scad
	atm cards	Трески. Seg	data scadenza
	atm kaart	Трески. seguranca	date de validité
	atmcard	Трески. segurança	datum afloop
	atmcards	Трески. sicurezza	datum van exp
	atmkaart	codice di sicurezza	de afloop
	atmkaarten	codice di verifica	espira
	bancontact	codigo	espira
	bank card	codigo de seguranca	exp date
	bankkaart	codigo de segurança	exp datum
	card holder	криттограмма	Истечения срока действия
	card holders	криптограмма	Истекает
	card num	криптограмма	Истекает
	card number	cv2	Истечения
	card numbers	Cvc	fecha de expiracion
	card type	cvc2	fecha de venc
	cardano numerico	Cvn	gultig bis
	Карточки	Cvv	gultigkeitsdatum
	Держателей карт	cvv2	gültig bis
	cardnumber	cód seguranca	gültigkeitsdatum
	cardnumbers	cód segurança	la scadenza
	carta bianca	cód. seguranca	scadenza
	carta credito	cód. segurança	valable
	carta di credito	código	validade
	cartao de credito	código de seguranca	valido hasta
	cartao de crédito	código de segurança	Доблести
	cartao de debito	de kaart controle	venc
	cartao de débito	geeft nr uit	vencimento
	carte bancaire	issue no	vencimiento
	carte blanche	issue number	verloopt
	carte bleue	kaartidentificatienummer	vervaldag
	carte de credit	kreditkartenprufnummer	vervaldatum
	carte de crédit	kreditkartenprüfnummer	vto
	carte di credito	kwestieaantal	válido hasta
	Картбланш	Нет. dell'edizione	

Keyword_eu_debit_card	Keyword_card_terms_dict	Keyword_card_security_terms_dict	Keyword_card_expiration_terms_dict
	cartão de credito	Нет. di sicurezza	
	cartão de crédito	numero de securite	
	cartão de debito	numero de verificacao	
	cartão de débito	numero dell'edizione	
	Cb	numero di identificazione della scheda	
	Ccn	numero di sicurezza	
	check card	numero van veiligheid	
	check cards	numéro de sécurité	
	checkcard	nº autorizzazione	
	контрольные знаки	número de verificação	
	chequekaart	perno il blocco	
	Cirrus	pin block	
	cirrus-edc-maestro	prufziffer	
	controlekaart	prüfziffer	
	controlekaarten	security code	
	credit card	security no	
	credit cards	security number	
	кредитная карта	sicherheits kode	
	кредитные карты	sicherheitscode	
	debetkaart	sicherheitsnummer	
	debetkaarten	speldblok	
	debit card	veiligheid nr	
	debit cards	veiligheidsaantal	
	дебетовая карта	veiligheidscode	
	дебетовые карты	veiligheidsnummer	
	debito automatico	verfalldatum	
	diners club		
	dinersclub		
	Обнаружить		
	discover card		
	discover cards		
	discovercard		
	карты обнаружения		
	débito automático		
	Edc		
	eigentümername		
	european debit card		
	hoofdkaart		
	hoofdkaarten		
	in viaggio		
	japanese card bureau		
	japanse kaartdienst		
	Jcb		
	kaart		
	kaart num		
	kaartaantal		
	kaartaantallen		
	kaarthouder		
	kaarthouders		
	karte		
	karteninhaber		
	karteninhabers		
	kartennr		
	kartennummer		
	kreditkarte		
	kreditkarten-nummer		
	kreditkarteninhaber		
	kreditkarteninstitut		
	kreditkartennummer		
	kreditkartentyp		
	Маэстро		
	master card		
	master cards		
	Mastercard		
	masters		
	Mc		
	mister cash		
	n carta		
	N. Carta		
	no de tarjeta		
	no do cartao		
	no do cartão		
	Нет. de tarjeta		

Keyword_eu_debit_card	Keyword_card_terms_dict	Keyword_card_security_terms_dict	Keyword_card_expiration_terms_dict
	Нет. do cartao Нет. do cartão nr carta Nr. Carta numeri di scheda numero carta numero de cartao numero de carte numero de cartão numero de tarjeta numero della carta numero di carta numero di scheda numero do cartao numero do cartão numéro de carte nº carta nº de carte nº de la carte nº de tarjeta nº do cartao nº do cartão n º. do cartão número de cartao número de cartão número de tarjeta número do cartao scheda dell'assegno scheda dell'atmosfera scheda dell'atmosfera scheda della banca scheda di controllo scheda di debito scheda matrice schede dell'atmosfera schede di controllo schede di debito schede matrici scoprono la scheda scoprono le schede Индивидуальные supporti di scheda supporto di scheda Переключатель tarjeta atm tarjeta credito tarjeta de atm tarjeta de credito tarjeta de debito tarjeta debito tarjeta no tarjetahabiente tipo della scheda ufficio giapponese della scheda v pay v-pay Визы visa plus visa electron Visto visum vpay		

Национальный идентификационный номер гражданина Финляндии

Формат: шесть цифр плюс символ, указывающий столетие плюс три цифры плюс контрольная цифра

Шаблон: шаблон должен включать все следующие компоненты:

- Шесть цифр в формате ДДММГГ, которые являются датой рождения

- Маркер века (символы "-" и "+" или буква "a")
- Трехзначный личный идентификационный номер
- Цифра или буква (без учета регистра) — проверочная.

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_finnish_national_id` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_finnish_national_id`.
- Контрольная сумма проходит проверку.

```
<!-- Finnish National ID-->
<Entity id="338FD995-4CB5-4F87-AD35-79BD1DD926C1" patternsProximity="300" recommendedConfidence="85">
  <Pattern confidenceLevel="85">
          <IdMatch idRef="Func_finnish_national_id" />
          <Match idRef="Keyword_finnish_national_id" />
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_finnish_national_id
Sosiaaliturvatunnus SOTU Henkilötunnus HETU Personbeteckning Personnummer

Номер паспорта гражданина Финляндии

Формат: сочетание девяти букв и цифр

Шаблон: сочетание девяти букв и цифр:

- две буквы (без учета регистра);
- семь цифр.

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_finland_passport_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_finland_passport_number`.

```
<!-- Finland Passport Number -->
<Entity id="d1685ac3-1d3a-40f8-8198-32ef5669c7a5" recommendedConfidence="75" patternsProximity="300">
  <Pattern confidenceLevel="75">
     <IdMatch idRef="Regex_finland_passport_number"/>
     <Match idRef="Keyword_finland_passport_number"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_finland_passport_number
Паспорт Passi

Номер водительского удостоверения для Франции

Формат: 12 цифр

Шаблон: 12 цифр с проверкой для скидки на аналогичные шаблоны, такие как французские телефонные номера

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, отдаленном не более чем на 300 знаков:

- Функция `Func_french_drivers_license` находит содержимое, соответствующее шаблону.
- Верно по меньшей мере одно из условий ниже:
  - обнаружено ключевое слово из `Keyword_french_drivers_license`.
  - Функция `Func_eu_date` находит дату в правильном формате даты.

```
<!-- France Driver's License Number -->
<Entity id="18e55a36-a01b-4b0f-943d-dc10282a1824" patternsProximity="300" recommendedConfidence="75">
  <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_french_drivers_license" />
        <Any minMatches="1">
          <Match idRef="Keyword_french_drivers_license" />
          <Match idRef="Func_eu_date" />
        </Any>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_french_drivers_license
drivers licence drivers license driving licence driving license permis de conduire licence number license number licence numbers license numbers

Национальная идентификационная карта гражданина Франции (CNI)

Формат: 12 цифр

Шаблон: 12 цифр

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных на 65 % уверена, что обнаружен этот тип конфиденциальной информации, если в пределах 300 символов регулярное выражение `Regex_france_cni` находит содержимое, соответствующее шаблону.

```
<!-- France CNI -->
<Entity id="f741ac74-1bc0-4665-b69b-f0c7f927c0c4" patternsProximity="300" recommendedConfidence="65">
```

```
  <Pattern confidenceLevel="65">
        <IdMatch idRef="Regex_france_cni" />
  </Pattern>
</Entity>
```

Ключевые слова: None

Номер паспорта гражданина Франции

Формат: девять цифр и букв

Шаблон: девять цифр и букв:

- Две цифры
- Две буквы (без учета регистра)
- Пять цифр

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_fr_passport` находит содержимое, соответствующее шаблону.
- Ключевое слово из `Keyword_passport` найдено..

```
<!-- France Passport Number -->
<Entity id="3008b884-8c8c-4cd8-a289-99f34fc7ff5d" patternsProximity="300" recommendedConfidence="75">
  <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_fr_passport" />
        <Match idRef="Keyword_passport" />
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_passport
Passport Number Passport No Passport# Паспорт # PassportID Passportno Соединенного Королевства パスポート パスポート番号 パスポートのNum パスポート# Numéro de passeport Passeport n ° Passeport Non Passeport# Passeport # PasseportNon Passeportn °

Номер социального страхования для Франции (INSEE)

Формат: 15 цифр

Шаблон:

Должен соответствовать одному из двух шаблонов:

- 13 цифр, за которыми идет пробел, а потом еще две цифры;
- 15 последовательных цифр.

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 95 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_french_insee` или `Func_fr_insee` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_fr_insee`.
- контрольная сумма проходит проверку.

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_french_insee` или `Func_fr_insee` находит содержимое, соответствующее шаблону.
- Ключевое слово из не `Keyword_fr_insee` найдено.
- Контрольная сумма проходит проверку.

```
<!-- France INSEE -->
<Entity id="71f62b97-efe0-4aa1-aa49-e14de253619d" patternsProximity="300" recommendedConfidence="85">
  <Pattern confidenceLevel="95">
        <IdMatch idRef="Func_french_insee" />
        <Match idRef="Func_fr_insee" />
        <Any minMatches="1">
          <Match idRef="Keyword_fr_insee" />
        </Any>
  </Pattern>
  <Pattern confidenceLevel="85">
        <IdMatch idRef="Func_french_insee" />
        <Match idRef="Func_fr_insee" />
        <Any minMatches="0" maxMatches="0">
          <Match idRef="Keyword_fr_insee" />
        </Any>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_fr_insee
Insee securité sociale securite sociale national id national identification numéro d'identité no d'identité Нет. d'identité numero d'identite no d'identite Нет. d'identite social security number social security code social insurance number le numéro d'identification nationale d'identité nationale numéro de sécurité sociale le code de la sécurité sociale numéro d'assurance sociale numéro de sécu code sécu

Номер водительского удостоверения для Германии

Формат: сочетание 11 цифр и букв

Шаблон: 11 цифр и букв (без учета регистра):

- Одна цифра или буква
- Две цифры
- Шесть цифр или букв
- Одна цифра
- Одна цифра или буква

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_german_drivers_license` находит содержимое, соответствующее шаблону.
- Верно по меньшей мере одно из условий ниже:
  - обнаружено ключевое слово из `Keyword_german_drivers_license_number`.
  - обнаружено ключевое слово из `Keyword_german_drivers_license_collaborative`.
  - обнаружено ключевое слово из `Keyword_german_drivers_license`.
- Контрольная сумма проходит проверку.

```
<!-- German Driver's License Number -->
<Entity id="91da9335-1edb-45b7-a95f-5fe41a16c63c" patternsProximity="300" recommendedConfidence="75">
  <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_german_drivers_license" />
        <Any minMatches="1">
          <Match idRef="Keyword_german_drivers_license_number" />
          <Match idRef="Keyword_german_drivers_license_collaborative" />
          <Match idRef="Keyword_german_drivers_license" />
        </Any>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_german_drivers_license_number	Keyword_german_drivers_license_collaborative	Keyword_german_drivers_license

Keyword_german_drivers_license_number	Keyword_german_drivers_license_collaborative	Keyword_german_drivers_license
Führerschein	Nr-Führerschein	ausstellungsdatum
Fuhrerschein	Nr-Fuhrerschein	ausstellungsort
Fuehrerschein	Nr-Fuehrerschein	ausstellende behöde
Führerscheinnummer	No-Führerschein	ausstellende behorde
Fuhrerscheinnummer	No-Fuhrerschein	ausstellende behoerde
Fuehrerscheinnummer	No-Fuehrerschein	
Führerschein-	N-Führerschein	
Fuhrerschein-	N-Fuhrerschein	
Fuehrerschein-	N-Fuehrerschein	
FührerscheinnummerNr	Nr-Führerschein	
FuhrerscheinnummerNr	Nr-Fuhrerschein	
FuehrerscheinnummerNr	Nr-Fuehrerschein	
FührerscheinnummerKlasse	No-Führerschein	
FuhrerscheinnummerKlasse	No-Fuhrerschein	
FuehrerscheinnummerKlasse	No-Fuehrerschein	
Führerschein- Nr	N-Führerschein	
Fuhrerschein- Nr	N-Fuhrerschein	
Fuehrerschein- Nr	N-Fuehrerschein	
Führerschein- Klasse		
Fuhrerschein- Klasse		
Fuehrerschein- Klasse		
FührerscheinnummerNr		
FuhrerscheinnummerNr		
FuehrerscheinnummerNr		
FührerscheinnummerKlasse		
FuhrerscheinnummerKlasse		
FuehrerscheinnummerKlasse		
Führerschein- Nr		
Fuhrerschein- Nr		
Fuehrerschein- Nr		
Führerschein- Klasse		
Fuhrerschein- Klasse		
Fuehrerschein- Klasse		
Dl		
Dls		
Driv Lic		
Driv Licen		
Driv License		
Driv Licenses		
Driv Licence		
Driv Licences		
Driv Lic		
Driver Licen		
Driver License		
Driver Licenses		
Driver Licence		
Driver Licences		
Drivers Lic		
Drivers Licen		
Drivers License		
Drivers Licenses		
Drivers Licence		
Drivers Licences		
Driver's Lic		
Driver's Licen		
Driver's License		
Driver's Licenses		
Driver's Licence		
Driver's Licences		
Driving Lic		
Driving Licen		
Driving License		
Driving Licenses		
Driving Licence		
Driving Licences		

Номер удостоверения личности для Германии

Формат:

- С 1 ноября 2010 года: девять букв и цифр
- С 1 апреля 1987 года по 31 октября 2010 года: 10 цифр

Шаблон:

С 1 ноября 2010 г.:

- одна буква (без учета регистра);
- Восемь цифр

С 1 апреля 1987 года по 31 октября 2010 года: 10 цифр

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 65 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, отдаленном не более чем на 300 знаков:

- Регулярное выражение `Regex_germany_id_card` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_germany_id_card`.

```
<!-- Germany Identity Card Number -->
<Entity id="e577372f-c42e-47a0-9d85-bebed1c237d4" recommendedConfidence="65" patternsProximity="300">
  <Pattern confidenceLevel="65">
     <IdMatch idRef="Regex_germany_id_card"/>
     <Match idRef="Keyword_germany_id_card"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_germany_id_card
Identity Card Идентификатор Идентификации Personalausweis Identifizierungsnummer Ausweis Идентификация

Номер паспорта гражданина Германии

Формат: 10 цифр или букв

Шаблон: шаблон должен включать все следующие компоненты:

- Первый символ — цифра или буква из следующего набора: C, F, G, H, J, K.
- Три цифры
- Пять цифр или букв из следующего набора: C, F-H, J-N, P, R, T, V-Z
- Одна цифра

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_german_passport` находит содержимое, соответствующее шаблону.
- находится любое ключевое слово из пяти соответствующих списков;

- контрольная сумма проходит проверку.

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_german_passport_data` находит содержимое, соответствующее шаблону.
- находится любое ключевое слово из пяти соответствующих списков;
- контрольная сумма проходит проверку.

```
<!-- German Passport Number -->
<Entity id="2e3da144-d42b-47ed-b123-fbf78604e52c" patternsProximity="300" recommendedConfidence="75">
  <Pattern confidenceLevel="85">
        <IdMatch idRef="Func_german_passport" />
        <Any minMatches="1">
          <Match idRef="Keyword_german_passport" />
          <Match idRef="Keyword_german_passport_collaborative" />
          <Match idRef="Keyword_german_passport_number" />
          <Match idRef="Keyword_german_passport1" />
          <Match idRef="Keyword_german_passport2" />
        </Any>
  </Pattern>
  <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_german_passport_data" />
        <Any minMatches="1">
          <Match idRef="Keyword_german_passport" />
          <Match idRef="Keyword_german_passport_collaborative" />
          <Match idRef="Keyword_german_passport_number" />
          <Match idRef="Keyword_german_passport1" />
          <Match idRef="Keyword_german_passport2" />
        </Any>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_german_passport	Keyword_german_passport_collaborative	Keyword_german_passport_number	Keyword_german_passport1	Keyword_gern
reisepass reisepasse reisepassnummer Паспорт Паспорта	geburtsdatum ausstellungsdatum ausstellungsort	No-Reisepass Nr-Reisepass	Reisepass-Nr	bnationalit.t

Национальная идентификационная карта гражданина Греции

Формат: сочетание 7–8 букв и цифр плюс тире

Шаблон:

Семь букв и чисел (старый формат):

- одна буква (любая буква греческого алфавита);
- тире;
- шесть цифр.

Восемь букв и чисел (новый формат):

- две буквы, которые в прописном виде есть как в греческом, так и латинском алфавите (ABEZHIKMNOPTYX);
- тире;
- шесть цифр.

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_greece_id_card` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_greece_id_card`.

```
<!-- Greece National ID Card -->
<Entity id="82568215-1da1-46d3-874a-d2294d81b5ac" recommendedConfidence="85" patternsProximity="300">
  <Pattern confidenceLevel="85">
     <IdMatch idRef="Regex_greece_id_card"/>
     <Match idRef="Keyword_greece_id_card"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_greece_id_card
Greek identity Card Ταυτοτητα Δελτίο αστυνομικής ταυτότητας Ταυτότητα

Номер удостоверения личности для Гонконга (HKID)

Формат: сочетание 8–9 букв и цифр, а также необязательные круглые скобки вокруг конечного символа

Шаблон: сочетание из 8–9 букв:

- 1–2 буквы (без учета регистра);
- шесть цифр;
- последний символ (любая цифра или буква "A") является проверочной цифрой и заключен в скобки (необязательно).

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_hong_kong_id_card` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_hong_kong_id_card`.
- Контрольная сумма проходит проверку.

Политика защиты от потери данных с вероятностью в 65 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, отдаленном не более чем на 300 знаков:

- Функция `Func_hong_kong_id_card` находит содержимое, соответствующее шаблону.
- Контрольная сумма проходит проверку.

```
<!-- Hong Kong Identity Card (HKID) number -->
<Entity id="e63c28a7-ad29-4c17-a41a-3d2a0b70fd9c" recommendedConfidence="75" patternsProximity="300">
  <Pattern confidenceLevel="75">
     <IdMatch idRef="Func_hong_kong_id_card"/>
     <Match idRef="Keyword_hong_kong_id_card"/>
  </Pattern>
  <Pattern confidenceLevel="65">
     <IdMatch idRef="Func_hong_kong_id_card"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_hong_kong_id_card
Hong Kong Identity Card HKID ID card 香港身份證 香港永久性居民身份證

Идентификационный номер налогоплательщика для Индии

Формат: 10 букв или цифр

Шаблон: 10 букв или цифр:

- пять букв (без учета регистра);
- четыре цифры;
- Буква, которая является проверочным числом в алфавитном порядке.

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_india_permanent_account_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_india_permanent_account_number`.
- Контрольная сумма проходит проверку.

```
<!-- India Permanent Account Number -->
<Entity id="2602bfee-9bb0-47a5-a7a6-2bf3053e2804" recommendedConfidence="85" patternsProximity="300">
  <Pattern confidenceLevel="85">
     <IdMatch idRef="Regex_india_permanent_account_number"/>
     <Match idRef="Keyword_india_permanent_account_number"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_india_permanent_account_number
Permanent Account Number Пан

Индивидуальный идентификационный номер (Aadhaar) для Индии

Формат: 12 цифр, содержащих необязательные пробелы или дефисы.

Шаблон: 12 цифр:

- четыре цифры;
- необязательный пробел или тире;
- четыре цифры;
- необязательный пробел или тире;
- Последняя цифра, которая является контрольной цифрой

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_india_aadhaar` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_india_aadhar`.
- Контрольная сумма проходит проверку.

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_india_aadhaar` находит содержимое, соответствующее шаблону.
- Контрольная сумма проходит проверку.

```
<!-- India Unique Identification (Aadhaar) number -->
<Entity id="1ca46b29-76f5-4f46-9383-cfa15e91048f" recommendedConfidence="85" patternsProximity="300">
  <Pattern confidenceLevel="85">
     <IdMatch idRef="Func_india_aadhaar"/>
     <Match idRef="Keyword_india_aadhar"/>
  </Pattern>
  <Pattern confidenceLevel="75">
     <IdMatch idRef="Func_india_aadhaar"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_india_aadhar
Аадхар Аадхаар UID आधार

Номер удостоверения личности (KTP) для Индонезии

Формат: 16 цифр, содержащих необязательные точки

Шаблон: 16 цифр:

- две цифры (код провинции);
- точка (необязательно);
- две цифры (код округа или города);
- две цифры (код района);
- точка (необязательно);
- Шесть цифр в формате ДДММГГ, которые являются датой рождения
- точка (необязательно);
- четыре цифры.

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_indonesia_id_card` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_indonesia_id_card`.

Политика защиты от потери данных на 75 % уверена, что обнаружен этот тип конфиденциальной информации, если в пределах 300 символов регулярное выражение `Regex_indonesia_id_card` находит содержимое, соответствующее шаблону.

```
<!-- Indonesia Identity Card (KTP) Number -->
<Entity id="da68fdb0-f383-4981-8c86-82689d3b7d55" recommendedConfidence="85" patternsProximity="300">
  <Pattern confidenceLevel="85">
     <IdMatch idRef="Regex_indonesia_id_card"/>
     <Match idRef="Keyword_indonesia_id_card"/>
  </Pattern>
  <Pattern confidenceLevel="75">
     <IdMatch idRef="Regex_indonesia_id_card"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_indonesia_id_card
Ktp Kartu Tanda Penduduk Nomor Induk Kependudukan

Международный номер банковского счета (IBAN)

Формат: код страны (две буквы) плюс контрольные цифры (две цифры) плюс число bban (до 30 символов)

Шаблон:

Шаблон должен включать в себя все указанные ниже элементы.

- Двухбуквенный код страны
- Две проверочные цифры (после которых может следовать пробел)
- 1–7 групп из четырех букв или цифр (могут разделяться пробелами)
- 1–3 буквы или цифры

Формат для названия каждой из стран немного отличается. Тип конфиденциальной информации IBAN охватывает следующие 60 стран: объявление, ae, al, at, az, ba, be, bg, bh, ch, cr, cy, cz, de, dk, do, ee, es, fi, fo, fr, gb, ge, gi, gl, gr, hr, hu, ie, il, is, it, kw, lb, li, lt, lu, lv, mc, md, me, mk, mr, mt, mu, nl, no, pl, pt, ro, rs, sa, se, si, sk, sm, tn, tr, vg

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_iban` находит содержимое, соответствующее шаблону.
- Контрольная сумма проходит проверку.

```
<Entity id="e7dc4711-11b7-4cb0-b88b-2c394a771f0e" patternsProximity="300" recommendedConfidence="85">
  <Pattern confidenceLevel="85">
        <IdMatch idRef="Func_iban" />
  </Pattern>
</Entity>
```

Ключевые слова: None

IP-адрес

Формат: IPv4 или IPv6-адрес

Шаблон:

- IPv4: сложный шаблон, который учитывает форматированные (точки) и неформатированные (без периодов) версии IPv4-адресов.
- IPv6: сложный шаблон, который учитывает форматированные числа IPv6 (которые включают двоеточия).

Контрольная сумма: Нет

Определение:

В случае с протоколом IPv4 политика защиты от потери данных с вероятностью в 95 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, отдаленном не более чем на 300 знаков:

- Регулярное выражение `Regex_ipv4_address` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_ipaddress`.

В случае с протоколом IPv6 политика защиты от потери данных с вероятностью в 95 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, отдаленном не более чем на 300 знаков:

- Регулярное выражение `Regex_ipv6_address` находит содержимое, соответствующее шаблону.
- Ключевое слово из не `Keyword_ipaddress` найдено.

В случае с протоколом IPv4 политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, отдаленном не более чем на 300 знаков:

- Регулярное выражение `Regex_ipv4_address` находит содержимое, соответствующее шаблону.
- Ключевое слово из не `Keyword_ipaddress` найдено.

В случае с протоколом IPv6 политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, отдаленном не более чем на 300 знаков:

- Регулярное выражение `Regex_ipv6_address` находит содержимое, соответствующее шаблону.
- Ключевое слово из не `Keyword_ipaddress` найдено.

```
<Entity id="1daa4ad5-e2dd-4ca4-a788-54722c09efb2" patternsProximity="300" recommendedConfidence="85">
    <Pattern confidenceLevel="95">
        <IdMatch idRef="Regex_ipv4_address" />
        <Any minMatches="1">
          <Match idRef="Keyword_ipaddress" />
        </Any>
    </Pattern>
    <Pattern confidenceLevel="95">
        <IdMatch idRef="Regex_ipv6_address" />
        <Any minMatches="1">
          <Match idRef="Keyword_ipaddress" />
        </Any>
    </Pattern>
    <Pattern confidenceLevel="85">
        <IdMatch idRef="Regex_ipv4_address" />
        <Any minMatches="0" maxMatches="0">
          <Match idRef="Keyword_ipaddress" />
        </Any>
    </Pattern>
    <Pattern confidenceLevel="85">
        <IdMatch idRef="Regex_ipv6_address" />
        <Any minMatches="0" maxMatches="0">
          <Match idRef="Keyword_ipaddress" />
        </Any>
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_ipaddress
ip address internet protocol כתובת ה-IP

Индивидуальный социальный номер (PPS) для Ирландии

Формат:

- Новый формат (1 января 2013 г. и более поздние): семь цифр, за которыми следуют две буквы
- Старый формат (31 декабря 2012 года и более ранние): семь цифр, за которыми следуют 1-2 буквы

Шаблон:

Новый формат (1 января 2013 г. и более поздние версии)

- семь цифр;
- буква (без учета регистра), которая является алфавитным проверочным символом;
- буква "A" или "H" (без учета регистра).

Старый формат (31 декабря 2012 г. и более ранние версии)

- семь цифр;
- 1–2 буквы (без учета регистра).

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_ireland_pps` находит содержимое, соответствующее шаблону.
- Верно одно из условий ниже:
  - обнаружено ключевое слово из `Keyword_ireland_pps`.
  - Функция `Func_eu_date` находит дату в правильном формате даты.
- Контрольная сумма проходит проверку.

Политика защиты от потери данных с вероятностью в 65 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, отдаленном не более чем на 300 знаков:

- Функция `Func_ireland_pps` находит содержимое, соответствующее шаблону.
- Контрольная сумма проходит проверку.

```
<!-- Ireland Personal Public Service (PPS) Number -->
<Entity id="1cdb674d-c19a-4fcf-9f4b-7f56cc87345a" recommendedConfidence="85" patternsProximity="300">
  <Pattern confidenceLevel="85">
     <IdMatch idRef="Func_ireland_pps"/>
     <Any minMatches="1">
  <Match idRef="Keyword_ireland_pps"/>
  <Match idRef="Func_eu_date"/>
     </Any>
  </Pattern>
  <Pattern confidenceLevel="65">
     <IdMatch idRef="Func_ireland_pps"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_ireland_pps

Keyword_ireland_pps
Personal Public Service Number PPS Number PPS Num PPS No. PPS # Pps # PPSN Public Services Card Uimhir Phearsanta Seirbhíse Poiblí Уим. Psp Psp

Номер банковского счета для Израиля

Формат: 13 цифр

Шаблон:

Форматированные:

- Две цифры
- Тире
- Три цифры
- Тире
- Восемь цифр

Неформатировано: 13 последовательных цифр

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_israel_bank_account_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_israel_bank_account_number`.

```
<!-- Israel Bank Account Number -->
<Entity id="7d08b2ff-a0b9-437f-957c-aeddbf9b2b25" patternsProximity="300" recommendedConfidence="75">
    <Pattern confidenceLevel="75">
        <IdMatch idRef="Regex_israel_bank_account_number" />
        <Any minMatches="1">
          <Match idRef="Keyword_israel_bank_account_number" />
        </Any>
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_israel_bank_account_number
Bank Account Number Bank Account Account Number מספר חשבון בנק

Национальный идентификатор для Израиля

Формат: девять цифр

Шаблон: девять последовательных цифр

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_israeli_national_id_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_Israel_National_ID`.
- Контрольная сумма проходит проверку.

```
<!-- Israel National ID Number -->
<Entity id="e05881f5-1db1-418c-89aa-a3ac5c5277ee" patternsProximity="300" recommendedConfidence="75">
    <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_israeli_national_id_number" />
        <Any minMatches="1">
          <Match idRef="Keyword_Israel_National_ID" />
        </Any>
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_Israel_National_ID
מספר זהות National ID Number

Номер водительского удостоверения для Италии

Формат: сочетание 10 букв и цифр

Шаблон: сочетание 10 букв и цифр:

- Одна буква (без учета регистра)
- Буква "A" или "V" (без учета регистра)
- Семь букв (без учета регистра), цифр или символов подчеркивания
- Одна буква (без учета регистра)

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_italy_drivers_license_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_italy_drivers_license_number`.

```
<!-- Italy Driver's license Number -->
<Entity id="97d6244f-9157-41bd-8e0c-9d669a5c4d71" patternsProximity="300" recommendedConfidence="75">
    <Pattern confidenceLevel="75">
        <IdMatch idRef="Regex_italy_drivers_license_number" />
        <Any minMatches="1">
          <Match idRef="Keyword_italy_drivers_license_number" />
        </Any>
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_italy_drivers_license_number
numero di patente di guida patente di guida

Номер банковского счета для Японии

Формат: семь или восемь цифр

Шаблон:

Номер банковского счета: семь или восемь цифр

Код филиала для банковского счета.

- Четыре цифры
- Пробел или тире (необязательно)
- Три цифры

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_jp_bank_account` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_jp_bank_account`.
- Верно одно из условий ниже:
  - Функция `Func_jp_bank_account_branch_code` находит содержимое, соответствующее шаблону.
  - обнаружено ключевое слово из `Keyword_jp_bank_branch_code`.

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_jp_bank_account` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_jp_bank_account`.

```
<!-- Japan Bank Account Number -->
<Entity id="d354f95b-96ee-4b80-80bc-4377312b55bc" patternsProximity="300" recommendedConfidence="75">
  <Version minEngineVersion="15.01.0131.000">
    <Pattern confidenceLevel="85">
          <IdMatch idRef="Func_jp_bank_account" />
          <Match idRef="Keyword_jp_bank_account" />
          <Any minMatches="1">
            <Match idRef="Func_jp_bank_account_branch_code" />
            <Match idRef="Keyword_jp_bank_branch_code" />
          </Any>
      </Pattern>
  </Version>
     <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_jp_bank_account" />
        <Match idRef="Keyword_jp_bank_account" />
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_jp_bank_account	Keyword_jp_bank_branch_code

Keyword_jp_bank_account	Keyword_jp_bank_branch_code
Checking Account Number Checking Account Checking Account # Checking Acct Number Checking Acct # Checking Acct No. Checking Account No. Bank Account Number Bank Account Bank Account # Bank Acct Number Bank Acct # Bank Acct No. Bank Account No. Savings Account Number Savings Account Savings Account # Savings Acct Number Savings Acct # Savings Acct No. Savings Account No. Debit Account Number Debit Account Debit Account # Debit Acct Number Debit Acct # Debit Acct No. Debit Account No. 口座番号を当座預金口座の確認 ＃アカウントの確認、勘定番号の確認 #勘定の確認 勘定番号の確認 口座番号の確認 銀行口座番号 銀行口座 銀行口座＃ 銀行の勘定番号 銀行のacct# 銀行の勘定いいえ 銀行口座番号 普通預金口座番号 預金口座 貯蓄口座＃ 貯蓄勘定の数 貯蓄勘定＃ 貯蓄勘定番号 普通預金口座番号 引き落とし口座番号 口座番号 口座番号＃ デビットのacct番号 デビット勘定＃ デビットACCTの番号 デビット口座番号	Отемачи

Номер водительского удостоверения для Японии

Формат: 12 цифр

Шаблон: 12 последовательных цифр

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_jp_drivers_license_number` находит содержимое, соответствующее шаблону.

- обнаружено ключевое слово из `Keyword_jp_drivers_license_number`.

```
<!-- Japan Driver's License Number -->
<Entity id="c6011143-d087-451c-8313-7f6d4aed2270" patternsProximity="300" recommendedConfidence="75">
    <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_jp_drivers_license_number" />
        <Match idRef ="Keyword_jp_drivers_license_number" />
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_jp_drivers_license_number
driver license drivers license driver's license drivers licenses driver's licenses driver licenses DI # Dls # Lic # lics # 運転免許証 運転免許 免許証 免許 運転免許証番号 運転免許番号 免許証番号 免許番号 運転免許証ナンバー 運転免許ナンバー 免許証ナンバー 運転免許証No. 運転免許No. 免許証No. 免許No. 運転免許証 # 運転免許 # 免許証 # 免許 #

Номер паспорта гражданина Японии

Формат: две буквы, за которыми следуют семь цифр

Шаблон: две буквы (без учета регистра), за которыми следует семь цифр.

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_jp_passport` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_jp_passport`.

```
<!-- Japan Passport Number -->
<Entity id="75177310-1a09-4613-bf6d-833aae3743f8" patternsProximity="300" recommendedConfidence="75">
    <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_jp_passport" />
        <Match idRef="Keyword_jp_passport" />
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_jp_passport
パスポート パスポート番号 パスポートのNum パスポート#

Номер регистрации резидента Японии

Формат: 11 цифр

Шаблон: 11 последовательных цифр

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_jp_resident_registration_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_jp_resident_registration_number`.

```
<!-- Japan Resident Registration Number -->
<Entity id="01c1209b-6389-4faf-a5f8-3f7e13899652" patternsProximity="300" recommendedConfidence="75">
    <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_jp_resident_registration_number" />
        <Match idRef ="Keyword_jp_resident_registration_number" />
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_jp_resident_registration_number
Resident Registration Number Resident Register Number Residents Basic Registry Number Resident Registration No. Resident Register No. Residents Basic Registry No. Basic Resident Register No. 住民登録番号、登録番号をレジデント 住民基本登録番号、登録番号 住民基本レジストリ番号を常駐 登録番号を常駐住民基本台帳登録番号

Номер карты социального страхования для Японии (SIN)

Формат: 7–12 цифр

Шаблон: 7–12 цифр:

- Четыре цифры
- Дефис (необязательно)
- Шесть цифр

  ИЛИ

- 7–12 последовательных цифр.

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_jp_sin` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_jp_sin`.

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_jp_sin_pre_1997` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_jp_sin`.

```
<!-- Japan Social Insurance Number -->
<Entity id="c840e719-0896-45bb-84fd-1ed5c95e45ff" patternsProximity="300" recommendedConfidence="75">
    <Pattern confidenceLevel="85">
        <IdMatch idRef="Func_jp_sin" />
        <Match idRef="Keyword_jp_sin" />
    </Pattern>
    <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_jp_sin_pre_1997" />
        <Match idRef="Keyword_jp_sin" />
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_jp_sin
Social Insurance No. Social Insurance Num Social Insurance Number 社会保険のテンキー 社会保険番号

Номер удостоверения личности для Малайзии

Формат: 12 цифр, содержащих необязательные дефисы

Шаблон: 12 цифр:

- Шесть цифр в формате ГГММДД, которые являются датой рождения
- дефис (необязательно);
- код места рождения из двух букв;
- дефис (необязательно);
- три случайные цифры;
- код пола из одной цифры.

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_malaysia_id_card_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_malaysia_id_card_number`.

```
<!-- Malaysia ID Card Number -->
</Entity>
      <Entity id="7f0e921c-9677-435b-aba2-bb8f1013c749" patternsProximity="300" recommendedConfidence="85">
        <Pattern confidenceLevel="85">
            <IdMatch idRef="Regex_malaysia_id_card_number" />
            <Match idRef="Keyword_malaysia_id_card_number" />
        </Pattern>
</Entity>
```

Ключевые слова:

Keyword_malaysia_id_card_number
MyKad Identity Card ID Card Identification Card Digital Application Card Kad Akuan Diri Kad Aplikasi Digital

Номер гражданской службы для Нидерландов (BSN)

Формат: 8–9 цифр, содержащих необязательные пробелы

Шаблон: 8–9 цифр:

- три цифры;
- пробел (необязательно);
- три цифры;
- пробел (необязательно);
- 2–3 цифры.

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_netherlands_bsn` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_netherlands_bsn`.
- Функция `Func_eu_date` находит дату в правильном формате даты.
- Контрольная сумма проходит проверку.

Политика защиты от потери данных с вероятностью в 65 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, отдаленном не более чем на 300 знаков:

- Функция `Func_netherlands_bsn` находит содержимое, соответствующее шаблону.
- Контрольная сумма проходит проверку.

```
<!-- Netherlands Citizen's Service (BSN) Number -->
<Entity id="c5f54253-ef7e-44f6-a578-440ed67e946d" recommendedConfidence="85" patternsProximity="300">
  <Pattern confidenceLevel="85">
     <IdMatch idRef="Func_netherlands_bsn"/>
     <Match idRef="Keyword_netherlands_bsn"/>
     <Match idRef="Func_eu_date"/>
  </Pattern>
  <Pattern confidenceLevel="65">
     <IdMatch idRef="Func_netherlands_bsn"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_netherlands_bsn
Citizen service number Bsn Burgerservicenummer Sofinummer Persoonsgebonden nummer Persoonsnummer

Номер министерства здравоохранения для Новой Зеландии

Формат: три буквы, пробел (необязательно) и четыре цифры

Шаблон: три буквы (без учета регистра) пробел (необязательно) четыре цифры

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_new_zealand_ministry_of_health_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_nz_terms`.
- Контрольная сумма проходит проверку.

```
<!-- New Zealand Health Number -->
<Entity id="2b71c1c8-d14e-4430-82dc-fd1ed6bf05c7" patternsProximity="300" recommendedConfidence="85">
    <Pattern confidenceLevel="85">
        <IdMatch idRef="Func_new_zealand_ministry_of_health_number" />
        <Any minMatches="1">
          <Match idRef="Keyword_nz_terms" />
        </Any>
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_nz_terms
Nhi Новая Зеландия Работоспособность Лечения

Идентификационный номер для Норвегии

Формат: 11 цифр

Шаблон: 11 цифр:

- Шесть цифр в формате ДДММГГ, которые являются датой рождения
- индивидуальный номер из трех цифр;
- две проверочные цифры.

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_norway_id_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_norway_id_number`.
- Контрольная сумма проходит проверку.

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_norway_id_numbe` находит содержимое, соответствующее шаблону.
- Контрольная сумма проходит проверку.

```
<!-- Norway Identification Number -->
<Entity id="d4c8a798-e9f2-4bd3-9652-500d24080fc3" recommendedConfidence="85" patternsProximity="300">
  <Pattern confidenceLevel="85">
     <IdMatch idRef="Func_norway_id_number"/>
     <Match idRef="Keyword_norway_id_number"/>
  </Pattern>
  <Pattern confidenceLevel="75">
     <IdMatch idRef="Func_norway_id_number"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_norway_id_number
Personal identification number Norwegian ID Number ID Number Идентификации Personnummer Fødselsnummer

Единый многофункциональный идентификационный номер для Филиппин

Формат: 12 цифр, разделенных дефисами

Шаблон: 12 цифр:

- четыре цифры;
- дефис;
- семь цифр;
- дефис;
- одна цифра.

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_philippines_unified_id` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_philippines_id`.

```
<!-- Philippines Unified Multi-Purpose ID number -->
<Entity id="019b39dd-8c25-4765-91a3-d9c6baf3c3b3" recommendedConfidence="75" patternsProximity="300">
  <Pattern confidenceLevel="75">
     <IdMatch idRef="Regex_philippines_unified_id"/>
     <Match idRef="Keyword_philippines_id"/>
```

```
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_philippines_id
Unified Multi-Purpose ID УМИД Identity Card Pinag-isang Multi-Layunin ID

Удостоверение личности гражданина Польши

Формат: три буквы и шесть цифр

Шаблон: три буквы (без учета регистра), за которыми следует шесть цифр

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_polish_national_id` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_polish_national_id_passport_number`.
- Контрольная сумма проходит проверку.

```
<!-- Poland Identity Card-->
<Entity id="25E64989-ED5D-40CA-A939-6C14183BB7BF" patternsProximity="300" recommendedConfidence="85">
      <Pattern confidenceLevel="85">
          <IdMatch idRef="Func_polish_national_id" />
          <Match idRef="Keyword_polish_national_id_passport_number" />
      </Pattern>
</Entity>
```

Ключевые слова:

Keyword_polish_national_id_passport_number
Nazwa i nr dowodu tożsamości Dowód Tożsamości Dow. Os.

Национальный идентификационный номер гражданина Польши (PESEL)

Формат: 11 цифр

Шаблон: 11 последовательных цифр

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_pesel_identification_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_pesel_identification_number`.
- Контрольная сумма проходит проверку.

```
<!-- Poland National ID (PESEL) -->
<Entity id="E3AAF206-4297-412F-9E06-BA8487E22456" patternsProximity="300" recommendedConfidence="85">
      <Pattern confidenceLevel="85">
          <IdMatch idRef="Func_pesel_identification_number" />
          <Match idRef="Keyword_pesel_identification_number" />
      </Pattern>
</Entity>
```

Ключевые слова:

Keyword_pesel_identification_number
Nr PESEL PESEL

Паспорт гражданина Польши

Формат: две буквы и семь цифр

Шаблон: две буквы (без учета регистра), за которыми следует семь цифр.

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_polish_passport_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_polish_national_id_passport_number`.
- Контрольная сумма проходит проверку.

```
<!-- Poland Passport Number -->
<Entity id="03937FB5-D2B6-4487-B61F-0F8BFF7C3517" patternsProximity="300" recommendedConfidence="85">
      <Pattern confidenceLevel="85">
          <IdMatch idRef="Func_polish_passport_number" />
          <Match idRef="Keyword_polish_national_id_passport_number" />
      </Pattern>
</Entity>
</Version>
```

Ключевые слова:

Keyword_polish_national_id_passport_number
Nazwa i nr dowodu tożsamości Dowód Tożsamości Dow. Os.

Номер карты гражданина Португалии

Формат: восемь цифр

Шаблон: восемь цифр

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_portugal_citizen_card` находит содержимое, соответствующее шаблону.

- обнаружено ключевое слово из `Keyword_portugal_citizen_card`.

```
<!-- Portugal Citizen Card Number -->
<Entity id="91a7ece2-add4-4986-9a15-c84544d81ecd" recommendedConfidence="85" patternsProximity="300">
  <Pattern confidenceLevel="85">
     <IdMatch idRef="Regex_portugal_citizen_card"/>
     <Match idRef="Keyword_portugal_citizen_card"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_portugal_citizen_card
Citizen Card National ID Card CC Cartão de Cidadão Bilhete de Identidade

Национальный идентификатор для Саудовской Аравии

Формат: 10 цифр

Шаблон: 10 последовательных цифр

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_saudi_arabia_national_id` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_saudi_arabia_national_id`.

```
<!-- Saudi Arabia National ID -->
<Entity id="8c5a0ba8-404a-41a3-8871-746aa21ee6c0" patternsProximity="300" recommendedConfidence="75">
    <Pattern confidenceLevel="75">
        <IdMatch idRef="Regex_saudi_arabia_national_id" />
        <Any minMatches="1">
          <Match idRef="Keyword_saudi_arabia_national_id" />
        </Any>
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_saudi_arabia_national_id
Identification Card I card number ID number الوطنية الهوية بطاقة رقم

Номер внутреннего удостоверения личности гражданина Сингапура (NRIC)

Формат: девять букв и цифр

Шаблон: девять букв и цифр:

- буква "F", "G", "S" или "T" (без учета регистра);

- семь цифр;
- алфавитный проверочный символ.

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_singapore_nric` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_singapore_nric`.
- Контрольная сумма проходит проверку.

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_singapore_nric` находит содержимое, соответствующее шаблону.
- Контрольная сумма проходит проверку.

```
<!-- Singapore National Registration Identity Card (NRIC) Number -->
<Entity id="cead390a-dd83-4856-9751-fb6dc98c34da" recommendedConfidence="75" patternsProximity="300">
  <Pattern confidenceLevel="85">
     <IdMatch idRef="Regex_singapore_nric"/>
     <Match idRef="Keyword_singapore_nric"/>
  </Pattern>
  <Pattern confidenceLevel="75">
     <IdMatch idRef="Regex_singapore_nric"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_singapore_nric
National Registration Identity Card Identity Card Number NRIC Ic Foreign Identification Number Плавник 身份证 身份證

Идентификационный номер для Южной Африки

Формат: 13 цифр, которые могут содержать пробелы

Шаблон: 13 цифр:

- Шесть цифр в формате ГГММДД, которые являются датой рождения
- четыре цифры;
- индикатор гражданства в виде одной цифры;
- цифра "8" или "9";
- Одна цифра, которая является контрольной суммой

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_south_africa_identification_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_south_africa_identification_number`.
- Контрольная сумма проходит проверку.

```
<!-- South Africa Identification Number -->
<Entity id="e2adf7cb-8ea6-4048-a2ed-d89eb65f2780" recommendedConfidence="85" patternsProximity="300">
  <Pattern confidenceLevel="85">
     <IdMatch idRef="Func_south_africa_identification_number"/>
     <Match idRef="Keyword_south_africa_identification_number"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_south_africa_identification_number
Identity card Идентификатор Идентификации

Регистрационный номер жителя Южной Кореи

Формат: 13 цифр, содержащих дефис

Шаблон: 13 цифр:

- Шесть цифр в формате ГГММДД, которые являются датой рождения
- дефис;
- одна цифра (определяет век и пол);
- код региона рождения из четырех цифр;
- одна цифра, используемая для разграничения людей, у которых предшествующие цифры совпадают;
- проверочная цифра.

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_south_korea_resident_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_south_korea_resident_number`.
- Контрольная сумма проходит проверку.

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_south_korea_resident_number` находит содержимое, соответствующее шаблону.
- Контрольная сумма проходит проверку.

```
<!-- South Korea Resident Registration Number -->
<Entity id="5b802e18-ba80-44c4-bc83-bf2ad36ae36a" recommendedConfidence="85" patternsProximity="300">
  <Pattern confidenceLevel="85">
     <IdMatch idRef="Func_south_korea_resident_number"/>
     <Match idRef="Keyword_south_korea_resident_number"/>
  </Pattern>
  <Pattern confidenceLevel="75">
     <IdMatch idRef="Func_south_korea_resident_number"/>
```

```
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_south_korea_resident_number
National ID card Citizen's Registration Number Jumin deungnok beonho RRN 주민등록번호

Номер социального страхования Испании (SSN)

Формат: 11–12 цифр

Шаблон: 11–12 цифр:

- Две цифры
- Косая черта (необязательно)
- 7–8 цифр
- Косая черта (необязательно)
- Две цифры

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_spanish_social_security_number` находит содержимое, соответствующее шаблону.
- Контрольная сумма проходит проверку.

```
<!-- Spain SSN -->
<Entity id="5df987c0-8eae-4bce-ace7-b316347f3070" patternsProximity="300" recommendedConfidence="85">
    <Pattern confidenceLevel="85">
        <IdMatch idRef="Func_spanish_social_security_number" />
    </Pattern>
</Entity>
```

Ключевые слова: None

Национальный идентификационный номер гражданина Швеции

Формат: 10 или 12 цифр и необязательный разделитель

Шаблон: 10 или 12 цифр и необязательный разделитель:

- 2–4 цифры (необязательно)
- Шесть цифр в формате даты ГГММДД.
- Разделитель - или + (необязательно)
- четыре цифры.

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_swedish_national_identifier` находит содержимое, соответствующее шаблону.
- Контрольная сумма проходит проверку.

```
<!-- Sweden National ID -->
<Entity id="f69aaf40-79be-4fac-8f05-fd1910d272c8" patternsProximity="300" recommendedConfidence="85">
    <Pattern confidenceLevel="85">
        <IdMatch idRef="Func_swedish_national_identifier" />
    </Pattern>
</Entity>
```

Ключевые слова: None

Номер паспорта гражданина Швеции

Формат: восемь цифр

Шаблон: восемь последовательных цифр

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_sweden_passport_number` находит содержимое, соответствующее шаблону.
- Верно одно из условий ниже:
  - обнаружено ключевое слово из `Keyword_passport`.
  - обнаружено ключевое слово из `Keyword_sweden_passport`.

```
<!-- Sweden Passport Number -->
<Entity id="ba4e7456-55a9-4d89-9140-c33673553526" patternsProximity="300" recommendedConfidence="75">
    <Pattern confidenceLevel="75">
        <IdMatch idRef="Regex_sweden_passport_number" />
        <Any minMatches="1">
          <Match idRef="Keyword_passport" />
          <Match idRef="Keyword_sweden_passport" />
        </Any>
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_sweden_passport	**Keyword_passport**

Keyword_sweden_passport	Keyword_passport
visa requirements Alien Registration Card Schengen visas Schengen visa Visa Processing Visa Type Single Entry Multiple Entry G3 Processing Fees	Passport Number Passport No Passport# Паспорт # PassportID Passportno Соединенного Королевства パスポート パスポート番号 パスポートのNum パスポート＃ Numéro de passeport Passeport n ° Passeport Non Passeport# Passeport # PasseportNon Passeportn °

Код SWIFT

Формат: четыре буквы, за которыми следуют 5–31 буквы или цифры

Шаблон: четыре буквы, за которыми следуют 5–31 буквы или цифры:

- Четырехбуквенный код банка (без учета регистра)
- Необязательный пробел
- 4–28 букв или цифр (основной номер банковского счета, BBAN)
- Необязательный пробел
- 1–3 буквы или цифры (оставшаяся часть BBAN)

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_swift` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_swift`.

```
<Entity id="cb2ab58c-9cb8-4c81-baf8-a4e106791df4" patternsProximity="300" recommendedConfidence="75">
<Pattern confidenceLevel="75">
        <IdMatch idRef="Regex_swift" />
        <Match idRef="Keyword_swift" />
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_swift

Keyword_swift
international organization for standardization 9362 iso 9362 iso9362 Swift # swift code swift number swiftroutingnumber swift code swift number # swift routing number bic number bic code bic# Bic # bank identifier code 標準化9362 迅速 # SWIFTコード SWIFT番号 迅速なルーティング番号 BIC番号 BICコード 銀行識別コードのための国際組織 Organisation internationale de normalisation 9362 rapide # code SWIFT le numéro de swift swift numéro d'acheminement le numéro BIC # BIC code identificateur de banque

Национальный идентификатор, Тайвань

Формат: одна буква (на английском языке), за которой следуют девять цифр

Шаблон: одна буква (на английском языке), за которой следует девять цифр:

- Один символ (на английском языке, без учета регистра)
- Цифра 1 или 2
- Восемь цифр

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_taiwanese_national_id` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_taiwanese_national_id`.
- Контрольная сумма проходит проверку.

```
<!-- Taiwanese National ID -->
<Entity id="4C7BFC34-8DD1-421D-8FB7-6C6182C2AF03" patternsProximity="300" recommendedConfidence="85">
      <Pattern confidenceLevel="85">
          <IdMatch idRef="Func_taiwanese_national_id" />
          <Match idRef="Keyword_taiwanese_national_id" />
      </Pattern>
</Entity>
```

Ключевые слова:

Keyword_taiwanese_national_id
身份證字號 身份證 身份證號碼 身份證號 身分證字號 身分證 身分證號碼 身份證號 身分證統一編號 國民身分證統一編號 簽名 蓋章 簽名或蓋章 簽章

Номер паспорта гражданина Тайваня

Формат:

- Номер биометрического паспорта: девять цифр
- Небиометрический номер паспорта: девять цифр

Шаблон:

- Номер биометрического паспорта:
  - цифра "3";
  - Восемь цифр
- Небиометрический номер паспорта: девять цифр

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_taiwan_passport` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_taiwan_passport`.

```
<!-- Taiwan Passport Number -->
<Entity id="e7251cb4-4c2c-41df-963e-924eb3dae04a" recommendedConfidence="75" patternsProximity="300">
  <Pattern confidenceLevel="75">
     <IdMatch idRef="Regex_taiwan_passport"/>
     <Match idRef="Keyword_taiwan_passport"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_taiwan_passport
ROC passport number Passport number Passport no Passport Num Passport # 护照 中華民國護照 Zhōnghuá Mínguó hùzhào

Номер удостоверения жителя Тайваня (ARC/TARC)

Формат: 10 букв и цифр

Шаблон: 10 букв и цифр:

- две буквы (без учета регистра);
- Восемь цифр

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_taiwan_resident_certificate` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_taiwan_resident_certificate`.

```
<!-- Taiwan Resident Certificate (ARC/TARC) -->
<Entity id="48269fec-05ea-46ea-b326-f5623a58c6e9" recommendedConfidence="75" patternsProximity="300">
  <Pattern confidenceLevel="75">
     <IdMatch idRef="Regex_taiwan_resident_certificate"/>
     <Match idRef="Keyword_taiwan_resident_certificate"/>
  </Pattern>
</Entity>
```

Ключевые слова:

Keyword_taiwan_resident_certificate
Resident Certificate Resident Cert Resident Cert. Identification card Alien Resident Certificate ARC Taiwan Area Resident Certificate TARC 居留證 外僑居留證 台灣地區居留證

Номер водительского удостоверения для Соединенного Королевства

Формат: сочетание 18 букв и цифр в указанном формате

Шаблон: 18 букв и цифр:

- Пять букв (без учета регистра) или цифра 9 вместо буквы
- Одна цифра
- Пять цифр в формате даты ДДММГ, представляющие собой дату рождения
- Две буквы (без учета регистра) или цифра 9 вместо буквы
- Пять цифр

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_uk_drivers_license` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_uk_drivers_license`.

- Контрольная сумма проходит проверку.

```
<!-- U.K. Driver's License Number -->
<Entity id="f93de4be-d94c-40df-a8be-461738047551" patternsProximity="300" recommendedConfidence="75">
    <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_uk_drivers_license" />
        <Match idRef="Keyword_uk_drivers_license" />
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_uk_drivers_license
DVLA light vans Квадроциклы motor cars 125cc Коляской Трициклов Мотоциклов Лицензия на фотокарту learner drivers licence holder licence holders driving licences driving licence dual control car

Регистрационный номер избирателя для Соединенного Королевства

Формат: две буквы, за которыми следуют 1–4 цифры

Шаблон: две буквы (без учета регистра), за которыми следуют 1–4 цифры

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_uk_electoral` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_uk_electoral`.

```
<!-- U.K. Electoral Number -->
<Entity id="a3eea206-dc0c-4f06-9e22-aa1be3059963" patternsProximity="300" recommendedConfidence="75">
    <Pattern confidenceLevel="75">
        <IdMatch idRef="Regex_uk_electoral" />
        <Any minMatches="1">
          <Match idRef="Keyword_uk_electoral" />
        </Any>
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_uk_electoral
council nomination nomination form electoral register electoral roll

Номер национальной службы здравоохранения для Соединенного Королевства

Формат: 10–17 цифр, разделенных пробелами

Шаблон: 10–17 цифр:

- 3 или 10 цифр
- Пробел
- Три цифры
- Пробел
- Четыре цифры

Контрольная сумма: Да

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_uk_nhs_number` находит содержимое, соответствующее шаблону.
- Верно одно из условий ниже:
  - обнаружено ключевое слово из `Keyword_uk_nhs_number`.
  - обнаружено ключевое слово из `Keyword_uk_nhs_number1`.
  - обнаружено ключевое слово из `Keyword_uk_nhs_number_dob`.
- Контрольная сумма проходит проверку.

```
<!-- U.K. NHS Number -->
<Entity id="3192014e-2a16-44e9-aa69-4b20375c9a78" patternsProximity="300" recommendedConfidence="85">
    <Pattern confidenceLevel="85">
        <IdMatch idRef="Func_uk_nhs_number" />
        <Any minMatches="1">
          <Match idRef="Keyword_uk_nhs_number" />
          <Match idRef="Keyword_uk_nhs_number1" />
          <Match idRef="Keyword_uk_nhs_number_dob" />
        </Any>
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_uk_nhs_number	Keyword_uk_nhs_number1	Keyword_uk_nhs_number_dob
national health service	идентификатор пациента	Gp
Nhs	patient identification	Dob
health services authority	patient no	D.O.B
health authority	patient number	Date of Birth
		Birth Date

Номер карты национального страхования для Соединенного Королевства (NINO)

Формат: девять букв и цифр, каждая пара букв и цифр при необходимости разделена пробелами или дефисами.

Шаблон: девять букв и цифр, каждая пара букв и цифр при необходимости разделена пробелами или дефисами:

- Две любые буквы (без учета регистра), кроме D, F, I, Q, U или V. Кроме того, в качестве второй буквы невозможно использовать O. Не допускаются также следующие сочетания: BG, GB, KN, NK, NT, TN и ZZ.

- Шесть цифр
- Пробел или тире (необязательно)
- Две цифры
- Пробел или тире (необязательно)
- Две цифры
- Пробел или тире (необязательно)
- Две цифры
- Одна буква (A, B, C или D) или один пробел.

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_uk_nino` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_uk_nino`.

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_uk_nino` находит содержимое, соответствующее шаблону.
- Ключевое слово из не `Keyword_uk_nino` найдено.

```
<!-- U.K. NINO -->
<Entity id="16c07343-c26f-49d2-a987-3daf717e94cc" patternsProximity="300" recommendedConfidence="75">
    <Pattern confidenceLevel="85">
        <IdMatch idRef="Func_uk_nino" />
        <Any minMatches="1">
          <Match idRef="Keyword_uk_nino" />
        </Any>
    </Pattern>
     <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_uk_nino" />
        <Any minMatches="0" maxMatches="0">
          <Match idRef="Keyword_uk_nino" />
        </Any>
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_uk_nino
national insurance number national insurance contributions protection act Страхование social security number insurance application medical application social insurance medical attention social security great britain Страхование

Номер паспорта гражданина США и/или Соединенного Королевства

Формат: девять цифр

Шаблон: девять последовательных цифр

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_usa_uk_passport` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_passport`.

```
<Entity id="178ec42a-18b4-47cc-85c7-d62c92fd67f8" patternsProximity="300" recommendedConfidence="75">
    <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_usa_uk_passport" />
        <Match idRef="Keyword_passport" />
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_passport
Passport Number Passport No Passport# Паспорт # PassportID Passportno Соединенного Королевства パスポート パスポート番号 パスポートのNum パスポート# Numéro de passeport Passeport n ° Passeport Non Passeport# Passeport # PasseportNon Passeportn °

Номер банковского счета для США

Формат: 4–17 цифр

Шаблон: 4–17 последовательных цифр

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Регулярное выражение `Regex_usa_bank_account_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_usa_Bank_Account`.

```
<!-- U.S. Bank Account Number -->
<Entity id="a2ce32a8-f935-4bb6-8e96-2a5157672e2c" patternsProximity="300" recommendedConfidence="75">
    <Pattern confidenceLevel="75">
        <IdMatch idRef="Regex_usa_bank_account_number" />
        <Match idRef="Keyword_usa_Bank_Account" />
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_США_Bank_Account
Checking Account Number Checking Account Checking Account # Checking Acct Number Checking Acct # Checking Acct No. Checking Account No. Bank Account Number Bank Account # Bank Acct Number Bank Acct # Bank Acct No. Bank Account No. Savings Account Number Savings Account. Savings Account # Savings Acct Number Savings Acct # Savings Acct No. Savings Account No. Debit Account Number Debit Account Debit Account # Debit Acct Number Debit Acct # Debit Acct No. Debit Account No.

Номер водительского удостоверения для США

Формат: зависит от состояния

Шаблон: зависит от штата, например, Нью-йорк:

- Подойдут девять цифр в формате ццц ццц ццц.
- Не подойдут девять цифр в формате ццццццццц.

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_new_york_drivers_license_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_[state_name]_drivers_license_name`.
- обнаружено ключевое слово из `Keyword_us_drivers_license`.

Политика защиты от потери данных с вероятностью в 65 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, отдаленном не более чем на 300 знаков:

- Функция `Func_new_york_drivers_license_number` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_[state_name]_drivers_license_name`.
- обнаружено ключевое слово из `Keyword_us_drivers_license_abbreviations`.
- Ключевое слово из не `Keyword_us_drivers_license` найдено.

```
<Pattern confidenceLevel="75">
        <IdMatch idRef="Func_new_york_drivers_license_number" />
        <Match idRef="Keyword_new_york_drivers_license_name" />
        <Match idRef="Keyword_us_drivers_license" />
```

```
    </Pattern>
    <Pattern confidenceLevel="65">
        <IdMatch idRef="Func_new_york_drivers_license_number" />
        <Match idRef="Keyword_new_york_drivers_license_name" />
        <Match idRef="Keyword_us_drivers_license_abbreviations" />
        <Any minMatches="0" maxMatches="0">
          <Match idRef="Keyword_us_drivers_license" />
        </Any>
    </Pattern>
```

Ключевые слова:

Keyword_us_drivers_license_abbreviations	Keyword_us_drivers_license	Keyword_[state_name]_drivers_license_name
Dl	DriverLic	Аббревиатура штата (например, NY)
Dls	DriverLics	Название штата (например, New York)
Cdl	DriverLicense	
CDLS	DriverLicenses	
Идентификатор	Driver Lic	
Идентификаторы	Driver Lics	
Dl #	Driver License	
Dls #	Driver Licenses	
Cdl #	DriversLic	
CDLS #	DriversLics	
Id #	ДрайверыЛицензии	
Идентификаторы #	ДрайверыЛицензии	
ID number	Drivers Lic	
ID numbers	Drivers Lics	
Lic	Drivers License	
Lic #	Drivers Licenses	
	Driver'Lic	
	Driver'Lics	
	Водительские права	
	Водительские лицензии	
	Driver' Lic	
	Driver' Lics	
	Driver' License	
	Driver' Licenses	
	Driver'sLic	
	Driver'sLics	
	Лицензия драйвера	
	Лицензии драйвера	
	Driver's Lic	
	Driver's Lics	
	Driver's License	
	Driver's Licenses	
	identification number	
	identification numbers	
	identification #	
	ID card	
	Удостоверения личности	
	identification card	
	identification cards	
	DriverLic #	
	DriverLics #	
	DriverLicense #	
	DriverLicenses #	
	Driver Lic#	
	Driver Lics#	
	Driver License#	
	Driver Licenses#	
	DriversLic #	
	DriversLics #	
	ДрайверыЛицензии #	
	ДрайверыЛицензии #	
	Drivers Lic#	
	Drivers Lics#	
	Drivers License#	
	Drivers Licenses#	
	Driver'Lic #	
	Driver'Lics #	
	Водительские права #	
	Водительские лицензии #	
	Driver' Lic#	

Keyword_us_drivers_license_abbreviations	Keyword_us_drivers_license	Keyword_[state_name]_drivers_license_name
	Driver' Lics# Driver' License# Driver' Licenses# Driver'sLic # Driver'sLics # Лицензия драйвера # Лицензии драйвера # Driver's Lic# Driver's Lics# Driver's License# Driver's Licenses# Удостоверение личности # Удостоверения личности # identification card# identification cards#	

Идентификационный номер налогоплательщика для США (ITIN)

Формат: девять цифр, которые начинаются с "9" и содержат "7" или "8" в качестве четвертой цифры, при необходимости отформатированные пробелами или дефисами.

Шаблон:

Форматированные:

- Цифра 9
- Две цифры
- Пробел или тире
- Цифра 7 или 8
- Одна цифра
- Пробел или тире
- Четыре цифры

Неформатированный:

- Цифра 9
- Две цифры
- Цифра 7 или 8
- Пять цифр

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_formatted_itin` находит содержимое, соответствующее шаблону.
- Верно по меньшей мере одно из условий ниже:
  - обнаружено ключевое слово из `Keyword_itin`.
  - Функция `Func_us_address` находит адрес в правильном формате даты.
  - Функция `Func_us_date` находит дату в правильном формате даты.
  - обнаружено ключевое слово из `Keyword_itin_collaborative`.

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_unformatted_itin` находит содержимое, соответствующее шаблону.
- Верно по меньшей мере одно из условий ниже:
  - обнаружено ключевое слово из `Keyword_itin_collaborative`.
  - Функция `Func_us_address` находит адрес в правильном формате даты.
  - Функция `Func_us_date` находит дату в правильном формате даты.

```
<!-- U.S. Individual Taxpayer Identification Number (ITIN) -->
<Entity id="e55e2a32-f92d-4985-a35d-a0b269eb687b" patternsProximity="300" recommendedConfidence="75">
    <Pattern confidenceLevel="85">
        <IdMatch idRef="Func_formatted_itin" />
        <Any minMatches="1">
          <Match idRef="Keyword_itin" />
          <Match idRef="Func_us_address" />
          <Match idRef="Func_us_date" />
          <Match idRef="Keyword_itin_collaborative" />
        </Any>
    </Pattern>
    <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_unformatted_itin" />
        <Match idRef="Keyword_itin" />
        <Any minMatches="1">
          <Match idRef="Keyword_itin_collaborative" />
          <Match idRef="Func_us_address" />
          <Match idRef="Func_us_date" />
        </Any>
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_itin	Keyword_itin_collaborative
Налогоплательщик	Лицензия
налоговый идентификатор	Dl
tax identification	Dob
itin	Birthdate
Ssn	Birthday
Олова	Date of Birth
social security	
tax payer	
itins	
за рулем	
individual taxpayer	

Страховой номер для США (SSN)

Формат: девять цифр, которые могут иметь форматированный или неформатированный шаблон

> ⓘ **Примечание**
>
> Есть SSN выдан до середины 2011 г., он отличается строгим форматированием, при котором определенные части номера должны входить в указанные диапазоны (при этом нет контрольной суммы).

Шаблон. Четыре функции ищут сети SSN в четырех разных шаблонах:

- `Func_ssn` находит сети SSN с строгим форматированием до 2011 года, отформатированными с помощью дефисов или пробелов (ddd-dd-dddd OR ddd dddd)
- `Func_unformatted_ssn` находит сети SSN со строгим форматированием до 2011 года, которые не отформатированы в виде девяти последовательных цифр (ddddddddddd)
- `Func_randomized_formatted_ssn` находит сети SSN после 2011 года, отформатированные с помощью дефисов или пробелов (ddd-ddd-dddd OR ddd dddd)

- `Func_randomized_unformatted_ssn` находит сети SSN после 2011 года, которые не отформатированы как девять последовательных цифр (ddddddddd)

Контрольная сумма: Нет

Определение:

Политика защиты от потери данных с вероятностью в 85 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_ssn` находит содержимое, соответствующее шаблону.
- Верно по меньшей мере одно из условий ниже:
  - обнаружено ключевое слово из `Keyword_ssn`.
  - Функция `Func_us_date` находит дату в правильном формате даты.
  - Функция `Func_us_address` находит адрес в правильном формате даты.

Политика защиты от потери данных с вероятностью в 75 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, не отдаленном более чем на 300 знаков:

- Функция `Func_unformatted_ssn` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_ssn`.
- Верно по меньшей мере одно из условий ниже:
  - Функция `Func_us_date` находит дату в правильном формате даты.
  - Функция `Func_us_address` находит адрес в правильном формате даты.

Политика защиты от потери данных с вероятностью в 65 % верно обнаруживает этот тип конфиденциальной информации, если в расположении, отдаленном не более чем на 300 знаков:

- Функция `Func_randomized_formatted_ssn` находит содержимое, соответствующее шаблону.
- Функция `Func_ssn` не находит содержимое, соответствующее шаблону.
- Верно по меньшей мере одно из условий ниже:
  - обнаружено ключевое слово из `Keyword_ssn`.
  - Функция `Func_us_date` находит дату в правильном формате даты.
  - Функция `Func_us_address` находит адрес в правильном формате даты.

Политика защиты от потери данных с вероятностью в 55 % верно обнаружила этот тип конфиденциальной информации, если в пределах ближайших 300 знаков:

- Функция `Func_randomized_unformatted_ssn` находит содержимое, соответствующее шаблону.
- обнаружено ключевое слово из `Keyword_ssn`.
- Функция `Func_unformatted_ssn` не находит содержимое, соответствующее шаблону.
- Верно по меньшей мере одно из условий ниже:
  - Функция `Func_us_date` находит дату в правильном формате даты.
  - Функция `Func_us_address` находит адрес в правильном формате даты.

```
<!-- U.S. Social Security Number (SSN) -->
<Entity id="a44669fe-0d48-453d-a9b1-2cc83f2cba77" patternsProximity="300" recommendedConfidence="75">
    <Pattern confidenceLevel="85">
        <IdMatch idRef="Func_ssn" />
        <Any minMatches="1">
          <Match idRef="Keyword_ssn" />
          <Match idRef="Func_us_date" />
          <Match idRef="Func_us_address" />
```

```
        </Any>
    </Pattern>
    <Pattern confidenceLevel="75">
        <IdMatch idRef="Func_unformatted_ssn" />
        <Match idRef="Keyword_ssn" />
        <Any minMatches="1">
          <Match idRef="Func_us_date" />
          <Match idRef="Func_us_address" />
        </Any>
    </Pattern>
    <Pattern confidenceLevel="65">
        <IdMatch idRef="Func_randomized_formatted_ssn" />
        <Any minMatches="0" maxMatches="0">
          <Match idRef="Func_ssn" />
        </Any>
        <Any minMatches="1">
          <Match idRef="Keyword_ssn" />
          <Match idRef="Func_us_date" />
          <Match idRef="Func_us_address" />
        </Any>
    </Pattern>
    <Pattern confidenceLevel="55">
        <IdMatch idRef="Func_randomized_unformatted_ssn" />
        <Match idRef="Keyword_ssn" />
        <Any minMatches="0" maxMatches="0">
          <Match idRef="Func_unformatted_ssn" />
        </Any>
        <Any minMatches="1">
          <Match idRef="Func_us_date" />
          <Match idRef="Func_us_address" />
        </Any>
    </Pattern>
</Entity>
```

Ключевые слова:

Keyword_ssn
Social Security Social Security# Soc Sec Ssn SSNS Ssn # Ss # SSID

Управление правами на доступ к данным в Exchange Server

Статья • 04.04.2023

Каждый день люди используют электронную почту для обмена конфиденциальными отчетами и информацией. Так как электронная почта доступна практически где угодно, почтовые ящики превратились в хранилища большого количества потенциально конфиденциальной информации. Таким образом, утечка информации представляет серьезную угрозу для организаций. Чтобы предотвратить утечку информации, Exchange Server включает функции управления правами на доступ к данным (IRM), которые обеспечивают постоянную защиту сообщений электронной почты и вложений в сети и в автономном режиме. Эти функции IRM по сути остались такими же, какими были в Exchange 2013.

Понятие утечки информации

Утечка информации — это раскрытие конфиденциальной информации неавторизованным пользователям. Утечка информации может дорого стоить организации и иметь масштабные последствия для бизнеса, сотрудников, клиентов и партнеров. Чтобы не нарушать действующие нормы, организациям необходимо защитить себя от случайной или преднамеренной утечки информации.

Ниже приведены некоторые последствия, к которым может привести утечка информации.

- **Финансовый ущерб**. Организация может понести потерю бизнеса, штрафы или негативное освещение в средствах массовой информации.
- **Ущерб имиджу и авторитету**. Утечка сообщений электронной почты может стать источником смущения для отправителя и организации.
- **Потеря конкурентного преимущества**: это одно из самых серьезных последствий. Раскрытие стратегических планов хозяйственной деятельности или слияний и поглощений может привести к снижению доходов или рыночной капитализации компании. Среди других угроз для конкурентного преимущества можно выделить потерю данных исследований, аналитических данных и другой интеллектуальной собственности.

Традиционные решения для защиты от утечки информации

Традиционные решения для защиты от утечки информации могут предотвратить доступ к данным на начальном этапе, но часто они не обеспечивают постоянную защиту. В следующей таблице описаны некоторые традиционные решения.

Решение	Описание	Ограничения
Протокол TLS	TLS — это стандартный интернет-протокол, используемый для шифрования сетевых соединений. В среде обмена сообщениями протокол TLS используется для шифрования соединений "сервер-сервер" и "клиент-сервер". По умолчанию Exchange использует TLS для всех внутренних передач сообщений. STARTTLS также включен по умолчанию для сеансов SMTP с внешними узлами (сначала выполняется попытка шифрования TLS, но если оно недоступно, разрешается незашифрованное соединение). Вы также можете настроить безопасность домена, чтобы применять протокол Mutual TLS для сеансов с внешними организациями.	Протокол TLS обеспечивает защиту сеанса SMTP только между двумя узлами SMTP. Другими словами, TLS защищает данные при передаче, но не обеспечивает защиту на уровне сообщений или данных в местах хранения. Сообщения в почтовых ящиках отправителей и получателей остаются незащищенными, если они не шифруются другим методом. Запрашивать шифрование по протоколу TLS можно только для первого прыжка электронной почты, отправляемой за пределы организации. После того как сообщение получит удаленный узел SMTP, он может передать его на другой узел SMTP по незашифрованному соединению. Так как протокол TLS — это технология транспортного уровня, используемая в потоке обработки почты, он не может контролировать действия получателя с сообщением.

Решение	Описание	Ограничения
Шифрование сообщений	Для шифрования сообщений пользователи могут использовать различные технологии, например S/MIME.	Пользователи сами решают, необходимо ли шифровать сообщение. Шифрование подразумевает дополнительные расходы на развертывание инфраструктуры открытых ключей (PKI) и сопутствующие затраты на управление сертификатами для пользователей и защиту закрытых ключей. После расшифровки сообщения действия получателя с информацией не контролируются. Расшифрованная информация может быть скопирована, распечатана или переслана. По умолчанию сохраненные вложения не защищены. Серверы обмена сообщениями не могут открывать и проверять сообщения, зашифрованные с помощью протокола S/MIME. Поэтому они не могу применять политики обмена сообщениями, проверять сообщения на вирусы и выполнять другие действия, для которых необходим доступ к содержимому сообщений.

И наконец, традиционные решения часто не позволяют применять единые политики обмена сообщениями для предотвращения утечки информации. Например, пользователь помечает сообщение как **Для служебного пользования** и **Не пересылать**. После доставки получателю ни отправитель, ни организация больше не контролируют сообщение. Получатель может умышленно или случайно переслать сообщение (используя правила автоматической пересылки) на внешние учетные записи электронной почты, подвергая организацию существенному риску утечки информации.

IRM в Exchange

IRM в Exchange помогает:

- предотвратить пересылку, изменение, печать, отправку по факсу, сохранение и копирование уполномоченными получателями содержимого, защищенного службой IRM;
- обеспечить для вложений в поддерживаемых форматах такой же уровень защиты, что и для сообщения;
- поддерживать функцию управления сроком действия сообщений и вложений с защитой IRM, которая не позволяет просматривать их по истечении указанного периода;
- предотвратить копирование содержимого, защищенного службой IRM, с помощью средства "Ножницы" в Windows.

Однако IRM в Exchange не может предотвратить раскрытие информации следующими способами:

- создание снимков экрана с помощью программ сторонних производителей;
- фотографирование защищенного IRM содержимого, которое отображается на экране;
- запоминание или переписывание информации пользователями.

IRM использует службы Active Directory Rights Management Services (AD RMS), технологию защиты информации в Windows Server, которая использует сертификаты и лицензии на основе XrML для сертификации компьютеров и пользователей, а также для защиты содержимого. Когда документ или сообщение защищено с помощью AD RMS, к нему прикрепляется лицензия XrML, содержащая права уполномоченных пользователей на содержимое. Чтобы получить доступ к защищенному IRM содержимому, приложения с поддержкой AD RMS должны получить лицензию на использование для уполномоченного пользователя с сервера AD RMS. Приложения Office, такие как Word, Excel, PowerPoint и Outlook, поддерживают RMS и могут использоваться для создания и использования защищенного содержимого.

> ⓘ **Примечание**
>
> Агент предварительной лицензии Exchange присоединяет лицензию на использование к сообщениям, защищенным сервером AD RMS в вашей организации. Дополнительные сведения см. в разделе **Предварительное лицензирование** далее в этой статье.

Дополнительные сведения о службах Active Directory Rights Management см. в статье Службы Active Directory Rights Management Services.

Шаблоны политик прав служб Active Directory Rights Management

Серверы AD RMS предоставляют веб-службу, используемую для перечисления и получения шаблонов политики прав на основе XrML, которые позволяют применять защиту IRM к сообщениям. Применяя соответствующий шаблон политики прав, вы указываете, разрешено ли получателю отвечать на сообщение, отвечать всем, пересылать его, извлекать из него информацию, сохранять или печатать.

По умолчанию Exchange поставляется с шаблоном "**Не пересылать** ". Если к сообщению применен этот шаблон, расшифровать его могут только пользователи, которым оно адресовано. Получатели не могут переслать сообщение, скопировать из него содержимое или распечатать. Вы можете создавать дополнительные шаблоны RMS на серверах AD RMS организации для своих нужд.

Дополнительные сведения о шаблонах политик прав см. в статье Рекомендации по шаблонам политики AD RMS.

Дополнительные сведения о создании шаблонов политик прав AD RMS см. в разделе Пошаговое руководство по развертыванию шаблонов политики прав AD RMS.

Применение защиты IRM к сообщениям

По умолчанию организация Exchange включает IRM, но чтобы применить защиту IRM к сообщениям, необходимо использовать один или несколько из следующих методов:

- **Вручную пользователями в Outlook**. Пользователи могут защищать сообщения с помощью IRM в Outlook с помощью доступных им шаблонов политики прав AD RMS. Этот процесс использует функции IRM в Outlook, а не Exchange. Дополнительные сведения об использовании IRM в Outlook см. в статье Общие сведения об использовании IRM для сообщений электронной почты.
- **Вручную пользователями в Outlook в Интернете**. Когда администратор включает IRM в Outlook в Интернете (ранее — Outlook Web App), пользователи могут защищать отправляемые ими сообщения с правами на

доступ к данным и просматривать полученные сообщения с защитой IRM. Дополнительные сведения об IRM в Outlook в Интернете см. в статье Общие сведения об IRM в Outlook Web App.

- **Вручную пользователям в Exchange ActiveSync**. Когда администратор включает IRM в Exchange ActiveSync пользователи могут просматривать, отвечать на сообщения, пересылать и создавать сообщения, защищенные IRM, на устройствах ActiveSync. Дополнительные сведения см. в статье Understanding Information Rights Management in Exchange ActiveSync.

- **Автоматически в Outlook**. Администраторы могут создавать правила защиты Outlook для автоматической защиты сообщений с правами на доступ к данным. Правила защиты Outlook автоматически развертываются на клиентах Outlook, а защита IRM применяется Outlook, когда пользователь создает сообщение. Дополнительные сведения см. в статье Правила защиты Outlook.

- **Автоматически на серверах почтовых ящиков**. Администраторы могут создавать правила потока обработки почты (также называемые правилами транспорта), чтобы автоматически защищать сообщения с правами на доступ к данным, которые соответствуют указанным условиям. Дополнительную информацию можно узнать в статье Understanding Transport Protection Rules.

  > ⓘ **Примечание**
  >
  > Защита IRM не применяется к сообщениям, которые уже защищены IRM. Например, если пользователь IRM защищает сообщение в Outlook или Outlook в Интернете, правило защиты транспорта не будет применять защиту IRM к тому же сообщению.

Сценарии для защиты IRM

В этой таблице описаны сценарии отправки сообщений и указано, доступна ли защита IRM.

Сценарий	Поддерживается ли отправка сообщений с защитой IRM?	Требования

Сценарий	Поддерживается ли отправка сообщений с защитой IRM?	Требования
Отправка сообщений в одной локальной организации Exchange	Да	Сведения о требованиях см. в разделе Требования к IRM далее в этом разделе.
Отправка сообщений между различными лесами Active Directory в локальной организации.	Да	Требования см. в статье Настройка AD RMS для интеграции с Exchange Server 2010 в нескольких лесах.
Отправка сообщений между локальной организацией Exchange и Microsoft 365 или Office 365 организацией в гибридном развертывании.	Да	Дополнительные сведения см. в разделе IRM в гибридных развертываниях Exchange.
Отправка сообщений внешним получателям	Нет	Exchange не включает решение для отправки защищенных IRM сообщений внешним получателям в не федеративных организациях. Сведения о создании федеративного доверия между двумя лесами Active Directory с помощью службы федерации Active Directory (AD FS) (AD FS) см. в статье Общие сведения о политиках доверия AD RMS.

Расшифровка защищенных IRM сообщений для применения политик обмена сообщениями

Чтобы применить политики обмена сообщениями и обеспечить соответствие нормативным требованиям, Exchange требуется доступ к содержимому зашифрованных сообщений. В соответствии с требованиями по обнаружению электронных данных в связи с судебным разбирательством, нормативно-правовыми проверками или внутренними расследованиями специалист по аудиту также должен иметь возможность искать информацию в зашифрованных

сообщениях. Чтобы помочь в выполнении этих задач, Exchange включает следующие функции расшифровки:

- **Расшифровка транспорта**. Разрешает доступ к содержимому сообщений агентами транспорта, установленными на серверах Exchange. Дополнительные сведения см. в разделе Общие сведения о расшифровке транспорта.

- **Расшифровка отчетов журналов**. Позволяет вести журналы уровня "Стандартный" или "Премиум" для сохранения в отчетах журнала чистого текста защищенных IRM сообщений. Дополнительные сведения см. в разделе Включение расшифровки отчетов журнала.

- **Расшифровка IRM для поиска Exchange**. Позволяет поиску Exchange индексировать содержимое в сообщениях, защищенных IRM. Когда диспетчер обнаружения выполняет поиск In-Place eDiscovery, в результатах поиска возвращаются защищенные IRM сообщения, которые были проиндексированы. Дополнительные сведения см. в статье Настройка IRM для поиска Exchange и In-Place обнаружения электронных данных.

Чтобы включить эти функции расшифровки, необходимо добавить почтовый ящик федерации (системный почтовый ящик, созданный Exchange) в группу Суперпользователей на сервере AD RMS. Инструкции см. в статье Add the Federation Mailbox to the AD RMS Super Users Group.

Предварительная лицензирования

Чтобы разрешить авторизованным пользователям просматривать защищенные IRM сообщения и вложения, Exchange автоматически присоединяет предварительную лицензию к защищенным сообщениям. Это предотвращает многократное обращение клиента к серверу AD RMS за лицензией на использование и позволяет просматривать защищенные IRM сообщения в автономном режиме. Предварительная лицензизация также позволяет пользователям просматривать сообщения, защищенные IRM, в Outlook в Интернете. При включении функций IRM предварительное лицензирование включается по умолчанию.

Агенты управления правами на доступ к данным

Функции IRM используют встроенные агенты транспорта, существующие в транспортной службе на серверах почтовых ящиков. Большинство встроенных

агентов транспорта невидимы и неуправляемы командлетами управления агентами транспорта в командной консоли Exchange (***-TransportAgent**).

Встроенные агенты транспорта, связанные с IRM, описаны в этой таблице:

Имя агента	**Управляемость**	**Событие SMTP или классификатора**	**Описание**
Агент расшифровки отчетов журнала	Нет	**OnCategorizedMessage**	Предоставляет текстовую копию защищенных IRM сообщений, которые прикреплены к отчетам журнала.
Агент предварительного лицензирования	Нет	**OnRoutedMessage**	Присоединяет предварительную лицензию к сообщениям, защищенным службой IRM.
Агент расшифровки RMS	Нет	**OnSubmittedMessage**,	Расшифровывает защищенные IRM сообщения, чтобы предоставить доступ к их содержимому агентам транспорта.
Агент шифрования RMS	Нет	**OnRoutedMessage**	Применяет защиту IRM к сообщениям, помеченным агентом транспорта, и повторно шифрует расшифрованные сообщения транспорта.
Агент расшифровки протокола RMS	Нет	**OnEndOfData**	Расшифровывает защищенные IRM сообщения, чтобы предоставить доступ к их содержимому агентам транспорта.
Агент правил транспорта	Да	**OnRoutedMessage**	Помечает сообщения, соответствующие условиям в правиле защиты транспорта, для применения защиты IRM агентом шифрования RMS.

Дополнительные сведения об агентах транспорта см. в разделе Транспортные агенты в Exchange Server.

Требования к управлению правами на доступ к данным

По умолчанию организация Exchange включает IRM. Чтобы фактически реализовать IRM в Exchange Server организации, развертывание должно соответствовать требованиям, описанным в этой таблице.

Сервер	Требования
Кластер AD RMS	*Кластер AD RMS* — термин, использующийся для обозначения любого развертывания AD RMS, в том числе одного сервера AD RMS. AD RMS — это веб-служба, поэтому вам не нужно настраивать отказоустойчивый кластер Windows Server. Чтобы обеспечить высокий уровень доступности и балансировку нагрузки, в кластере можно развернуть несколько серверов AD RMS и использовать балансировку сетевой нагрузки (NLB). **Точка подключения службы**. Приложения с поддержкой AD RMS, такие как Exchange, используют точку подключения службы, зарегистрированную в Active Directory, для обнаружения кластера и URL-адресов AD RMS. В лесу Active Directory есть только одна точка подключения службы для AD RMS. Вы можете зарегистрировать точку подключения службы во время установки AD RMS или после нее. **Разрешения.** Разрешения на чтение и выполнение конвейера сертификации сервера AD RMS (`ServerCertification.asmx` файл по адресу `\inetpub\wwwroot\_wmcs\certification\`) должны быть назначены следующим субъектам безопасности: • Группа Exchange Servers или отдельные серверы Exchange. • группа службы AD RMS на серверах AD RMS. Дополнительные сведения см. в разделе Установка разрешений для конвейера сертификации сервера AD RMS. **Суперпользователей AD RMS**. Чтобы включить расшифровку транспорта, расшифровку отчетов журнала, IRM в Outlook в Интернете и расшифровку IRM для поиска Exchange, необходимо добавить почтовый ящик федерации в группу суперпользователей на сервере AD RMS. Дополнительные сведения см. в разделе Добавление федеративного почтового ящика в группу суперпользователей службы управления правами Active Directory.
Exchange	Требуется Exchange 2010 или более поздней версии. В рабочей среде установка AD RMS и Exchange на одном сервере не поддерживается.
Outlook	Шаблоны AD RMS для защиты сообщений доступны в Outlook 2007 или более поздних версиях. Для правил защиты Outlook в Exchange требуется Outlook 2010 или более поздней версии.

Сервер	Требования
Exchange ActiveSync	IRM доступен для мобильных приложений и устройств, поддерживающих протокол Exchange ActiveSync версии 14.1 или более поздней, а также включенный тег **RightsManagementInformation** (как представленный в Exchange 2010 с пакетом обновления 1). Пользователи с поддерживаемыми устройствами могут использовать ActiveSync для просмотра, ответа на сообщения, пересылки и создания сообщений, защищенных IRM, без подключения к компьютеру для активации устройства для IRM. Дополнительные сведения см. в статье Understanding Information Rights Management in Exchange ActiveSync.

Функции Exchange IRM поддерживают форматы файлов Office. Вы можете расширить защиту IRM на другие форматы файлов, развернув пользовательские средства защиты. Дополнительные сведения о пользовательских предохранителях найдите Information Protection и партнеры по управлению на странице поставщиков решений Майкрософт.

Настройка и проверка IRM

Для настройки функций IRM в Exchange используется командная консоль Exchange. Инструкции см. в статье Managing Rights Protection.

После установки и настройки сервера почтовых ящиков можно выполнить сквозные испытания развертывания IRM с помощью командлета **Test-IRMConfiguration**. Командлет выполняет следующие тесты:

- Проверяет конфигурацию IRM для организации Exchange.
- Проверяет сервер службы AD RMS на предмет сведений о версии и исправлениях.
- Проверяет, можно ли активировать сервер Exchange Server для RMS, получая сертификат учетной записи прав (RAC) и сертификат лицензиара клиента.
- Получает шаблоны политики прав службы AD RMS с сервера службы AD RMS.
- Проверяет способность указанного отправителя отправлять сообщения, защищенные службой IRM.
- Получает для указанного получателя лицензию на использование суперпользователя.
- Получает для указанного получателя предварительную лицензию.

Дополнительные сведения см. в статье Test-IRMConfiguration.

Ведение журнала в Exchange Server

Статья • 04.04.2023

Ведение журнала в Exchange Server может помочь вашей организации реагировать на юридические, нормативные и организационные требования к соответствию, записывая все или целевые сообщения электронной почты. Ведение журнала в Exchange Server практически не изменилось с Exchange Server 2010 года.

Exchange предоставляет следующие варианты параметров я.ов..

- **Стандартное ведение журнала. Занесение** в журнал всех сообщений, отправляемых и полученных почтовыми ящиками в определенной базе данных почтовых ящиков. Чтобы регистрировать все сообщения в организации, необходимо настроить ведение журнала во всех базах данных почтовых ящиков на всех серверах Exchange.

- **Ведение журнала уровня "Премиум".** Используйте *правила журнала* для записи сообщений на основе получателей (все получатели или указанные получатели) и области (внутренние сообщения, внешние сообщения или все сообщения). Для лицензирования уровня "Премиум" требуются клиентские лицензии (CAL) Exchange Enterprise. Дополнительные сведения о клиентских лицензиях см. в разделе Часто задаваемые вопросы о лицензировании Exchange.

Чтобы настроить ведение журнала, см. статью Процедуры журналирования в Exchange Server.

Для хранения сообщений и обеспечения соответствия требованиям необходимо иметь представление о функции ведения журнала и о том, как она соотносится с корпоративными политиками соответствия.

Важность ведения журнала

Во-первых, важно понимать разницу между ведением журнала и архивированием, когда дело доходит до сообщений электронной почты:

- *Ведение журнала* — это запись сообщений электронной почты в рамках стратегии хранения электронной почты в организации.

- *Архивация* — это удаление сообщений электронной почты из исходного расположения (например, почтового ящика пользователя) и их сохранение в другом месте.

Многие организации должны хранить сообщения электронной почты своих сотрудников. Ведение журнала Exchange можно применять как средство стратегии архивирования или хранения электронной почты.

Хотя нормативные требования могут не требовать ведения журнала, ведение журналов Exchange может помочь вашей организации обеспечить соответствие нормативным требованиям. Например, в некоторых финансовых сферах должностные лица несут ответственность за то, что их сотрудники заявляют клиентам. Менеджеры по управлению соответствием могут пользоваться ведением журнала для сбора и регулярной проверки сообщений электронной почты, отправленных клиентам сотрудниками, в рамках проверки коммуникации между сотрудниками и клиентами. Далее менеджеры по управлению соответствием могут сообщить о положительном результате проверки уполномоченному сотруднику, который затем подаст регулятивному органу отчет о соответствии требованиям.

В следующем списке приведены некоторые из более известных американских и международных правил, в которых ведение журнала Exchange может помочь в рамках ваших стратегий соответствия требованиям:

- Акт Сарбейнс-Оксли от 2002 г. (SOX)
- Правило комиссии по бирже ценных бумаг 17a-4 (правило SEC 17 A-4)
- National Association of Securities Dealers 3010 & 3110 (NASD 3010 & 3110)
- Акт Грэмма-Лича-Блайли (Gramm-Leach-Bliley) (Акт финансовой модернизации)
- Акт 2001 года о защите конфиденциальности данных в финансовых учреждениях
- Акт 2003 года о защите конфиденциальности данных в финансовых учреждениях
- Акт 1996 года о передаче и защите данных учреждений здравоохранения (HIPAA)
- Акт 2001 года об объединении и усилении Америки за счет предоставления надлежащих средств, необходимых для предотвращения терроризма (Патриотический акт)
- Директива по защите данных Европейского союза
- Акт о защите личной информации в Японии

Агент ведения журнала

Агент общения — это встроенный транспортный агент Exchange, который обрабатывает сообщения по мере их передачи через транспортную службу на серверах почтовых ящиков. Параметры конфигурации журнала хранятся в Active Directory и считываются агентом журналов. Агент ведения журнала зарегистрирован в событиях классификатора **OnSubmittedMessage** и **OnRoutedMessage** на транспортном конвейере. Дополнительные сведения о транспортном конвейере см. в статье Mail flow and the transport pipeline.

Командлеты управления агентами транспорта (***-TransportAgent**) не видят большую часть встроенных агентов транспорта и не могут ими управлять.

Отчеты журнала

Отчет журнала — это сообщение, записанное в журнале. Отчет журнала содержит исходное сообщение в виде неотправленного вложения файла. Текст отчета журнала содержит сводную информацию из исходного сообщения (например, адрес электронной почты отправителя, тема сообщения, **идентификатор сообщения** и адреса электронной почты получателя). Этот тип журнала называется *журналированием конвертов* и является единственным методом, поддерживаемым Exchange.

Отчеты журнала и сообщения, защищенные службой управления правами на доступ к данным

Необходимо учитывать влияние сообщений, защищенных IRM, на отчеты журнала. Сторонние системы архивации без встроенной поддержки RMS не могут расшифровывать защищенные IRM сообщения в отчетах журнала, что негативно влияет на поиск и обнаружение содержимого в журналах. В Exchange можно настроить расшифровку отчета журнала, чтобы сохранить копию сообщения в отчете журнала с открытым текстом. Дополнительные сведения см. в разделе Включение расшифровки отчетов журнала.

Правила журнала

Ниже перечислены базовые компоненты правила журнала.

- **Получатель журнала**. Укажите, чьи сообщения нужно записывать в журнал.

- **Область действия правила журнала**. Укажите, какие сообщения нужно записывать в журнал.
- **Почтовый ящик журналов**. Укажите, где нужно хранить записанные в журнал сообщения.

Получатель журнала

Компонент *Получатель журнала* указывает, чьи сообщения нужно записывать в журнал. Сообщения, отправленные или полученные получателем журнала записываются в журнал (направление не имеет значения). Вы можете настроить правило журнала для регистрации сообщений для всех отправителей и получателей в организации Exchange или ограничить правило журнала почтовым ящиком, группой, пользователем почты или почтовым контактом Exchange. Если вы укажете группу рассылки, ведение журнала будет включено для *участников* группы рассылки, а не для самой группы.

Указывая определенных получателей или группы получателей, вы сможете настроить среду ведения журнала в соответствии с юридическими и нормативными требованиями организации. Это также позволит снизить расходы на хранение больших объемов данных.

Получатели журнала, для которых включена единая система обмена сообщениями в Exchange 2016

По умолчанию, если ваша организация Exchange 2016 использует единую систему обмена сообщениями (UM) для консолидации инфраструктуры электронной почты, голосовой почты и факсов, Exchange настраивается для записи уведомлений голосовой почты и сообщений уведомлений о пропущенных звонках. Можно отключить ведение журнала для этих типов сообщений, но сообщения, которые содержат факсы, сгенерированные единой системой обмена сообщениями, будут всегда записываться в журнал.

Сведения о том, как отключить ведение журнала для уведомлений о пропущенных звонках и поступлении голосовой почты, см. в разделе Включение или отключение ведения журнала голосовой почты и уведомлений о пропущенных звонках.

> ⓘ **Примечание**
>
> Единая система обмена сообщениями не доступна в Exchange 2019.

Область действия правил журнала

Когда вы укажете, чьи сообщения нужно записывать, необходимо указать, какие именно сообщения нужно записывать. Допустимы следующие варианты:

- **Только внутренние сообщения**. Источник или назначение сообщения находится в организации Exchange.
- **Только внешние сообщения**. Источник или назначение сообщения находится за пределами организации Exchange.
- **Все сообщения**: источник или назначение сообщения не имеет значения. Обратите внимание, что применение правила журнала с такой областью действий может привести к записи в журнал сообщений, которые уже были записаны на основании других правил журнала.

Почтовый ящик журналов

Сообщения, записанные в журнал, будут доставлены в почтовый ящик журналов. Настройка почтового ящика журналов зависит от требований политик, юридических и нормативных требований, применяемых в организации. Например, может быть достаточно настройки только одного почтового ящика журналов для всех правил журнала в организации, а может потребоваться использование различных почтовых ящиков журналов для разных правил журнала.

Примечания.

- Почтовые ящики журналов содержат конфиденциальную информацию, поэтому их необходимо защитить. Сообщения в почтовом ящике журналов могут касаться судопроизводства или подпадать под нормативные требования. Мы рекомендуем создать и применить четко определенные политики, указывающие, кто именно должен иметь доступ к почтовому ящику журналов. Проконсультируйтесь с юристами, чтобы убедиться, что система ведения журнала соответствует всем законам и нормативам, действующим для организации.
- Почтовый ящик Microsoft 365 или Office 365 нельзя использовать в качестве почтового ящика журнала. Если вы выполняете гибридное развертывание между локальной средой Exchange и Microsoft 365 или Office 365, вы можете назначить локальные почтовые ящики журналов для microsoft 365 или Office 365 и локальных организаций. Вы также можете отправлять сообщения, записанные в журнал, в локальную систему архивации электронной почты или стороннюю службу архивации.

- Почтовые ящики журналов должны принимать сообщения максимального размера, допустимого в вашей организации. Учитывайте максимальные размеры сообщений, настроенные для отдельных почтовых ящиков. Дополнительные сведения см. в разделе Настройка ограничений на размер сообщений для почтового ящика.

- Рекомендуется настроить почтовый ящик журнала так, чтобы он принимал только сообщения от получателя Microsoft Exchange (единственного отправителя отчетов журнала). Обратите внимание, что это можно сделать только в командной консоли Exchange. Дополнительные сведения см. в статье Настройка ограничений доставки сообщений для почтового ящика.

- Мы рекомендуем отключить ограничения квоты хранилища для почтового ящика журналов. Дополнительные сведения см. в разделе Настройка квот хранилища для почтового ящика.

Альтернативный почтовый ящик журналов

Как и другие сообщения, отчеты о недоставленных журналах помещаются в очередь, а доставка периодически повторяется до истечения срока действия сообщения (значение по умолчанию — два дня и настраивается параметром *MessageExpirationTimeout* в **командлете Set-TransportService**). В отличие от других сообщений, отчеты журнала с истекшим сроком действия не могут быть возвращены отправителю в отчете о недоставке (также известном как сообщение о недоставке или отказе), так как отправитель является получателем Microsoft Exchange. Отчеты журнала с истекшим сроком действия не могут быть восстановлены.

Если вы хотите избежать постановки в очередь и истечения срока действия недоставленных отчетов журнала, можете указать *альтернативный почтовый ящик журналов*, который будет принимать отчеты о недоставке для *всех* недоставленных отчетов журнала в случае, если эти отчеты не удается доставить *ни на один* почтовый ящик журналов (достаточно одного альтернативного почтового ящика журналов на все почтовые ящики журналов в организации). Исходный отчет журнала будет отправляться вместе с отчетом о недоставке в качестве вложения. Когда почтовый ящик журнала снова станет доступен, вы можете использовать функцию **повторной отправки этого сообщения** в Outlook для отчетов о недоставке в альтернативном почтовом ящике журнала для отправки неотмененных отчетов о доставке в почтовый ящик журнала.

Перед настройкой альтернативного почтового ящика журналов обратитесь к уполномоченным юристам. Законами или нормами, применимыми к вашей

организации, может быть запрещено хранить все сообщения журнала в одном почтовом ящике.

При настройке альтернативного почтового ящика журналов необходимо использовать те же критерии, что и при создании почтового ящика журналов.

Примечания.

- Если альтернативный почтовый ящик журналов становится недоступен и отклоняет отчеты о недоставке отчетов журнала, исходные отчеты журналов удаляются без возможности восстановления.
- Альтернативный почтовый ящик журналов необходимо рассматривать как специальный почтовый ящик. Правила журнала, правила для папки "Входящие" и правила потока обработки почты (также известные как правила транспорта), включающие альтернативный почтовый ящик журналов, будут игнорироваться.

Репликация правил журнала

Поскольку правила журнала хранятся в Active Directory, они считываются и применяются службой транспорта на всех серверах почтовых ящиков в организации. При создании, изменении или удалении правила журнала это действие реплицируется между всеми контроллерами домена в организации. Это позволяет Exchange предоставлять согласованный набор правил журнала в организации.

Примечания.

- Репликация между контроллерами домена зависит от факторов, которые не контролируются Exchange (например, количество сайтов Active Directory и скорость сетевых каналов). Соответственно, при реализации правил журнала в организации следует учесть задержки репликации. Дополнительные сведения о репликации Active Directory см. в статье Общие сведения о репликации Active Directory и управлении топологией с помощью Windows PowerShell.
- Каждый сервер почтовых ящиков кэширует расширенные группы рассылки, чтобы избежать повторных запросов Active Directory на определение членства в группах. По умолчанию записи в кэше расширенных групп действительны в течение четырех часов. Таким образом, изменения в составе участников группы не будут применяться к правилам журнала до обновления кэша развернутых групп. Чтобы принудительно обновить кэш на сервере

почтовых ящиков, перезапустите службу транспорта Microsoft Exchange. Эту службу необходимо перезапустить на каждом сервере почтовых ящиков, где требуется принудительно обновить кэш.

Устранение неполадок

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server. Если у вас возникли проблемы с альтернативным почтовым ящиком журнала, см. статью KB2829319.

Ведение журнала в Exchange Server

Статья • 04.04.2023

Ведение журнала в Exchange Server записывает входящие и исходящие сообщения электронной почты. Дополнительные сведения см. в разделе Ведение журнала в Exchange Server.

В этой статье описано, как настроить возможности ведения журнала стандартные (запись сообщений со всех почтовых ящиков, находящихся в базе данных почтовых ящиков) и расширенные (использование правил журнала для указания получателей, чьи сообщения нужно записывать). Одни параметры доступны только в Центре администрирования Exchange, другие — только в командной консоли Exchange.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Ведение журнала" в разделе Политика обмена сообщениями и разрешения на соответствие требованиям Exchange Server.
- Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**. Если у вас возникли проблемы с почтовым ящиком **JournalingReportDNRTo**, просмотрите статью **Правила транспорта и почтовых ящиков в Exchange Online работают некорректно**.

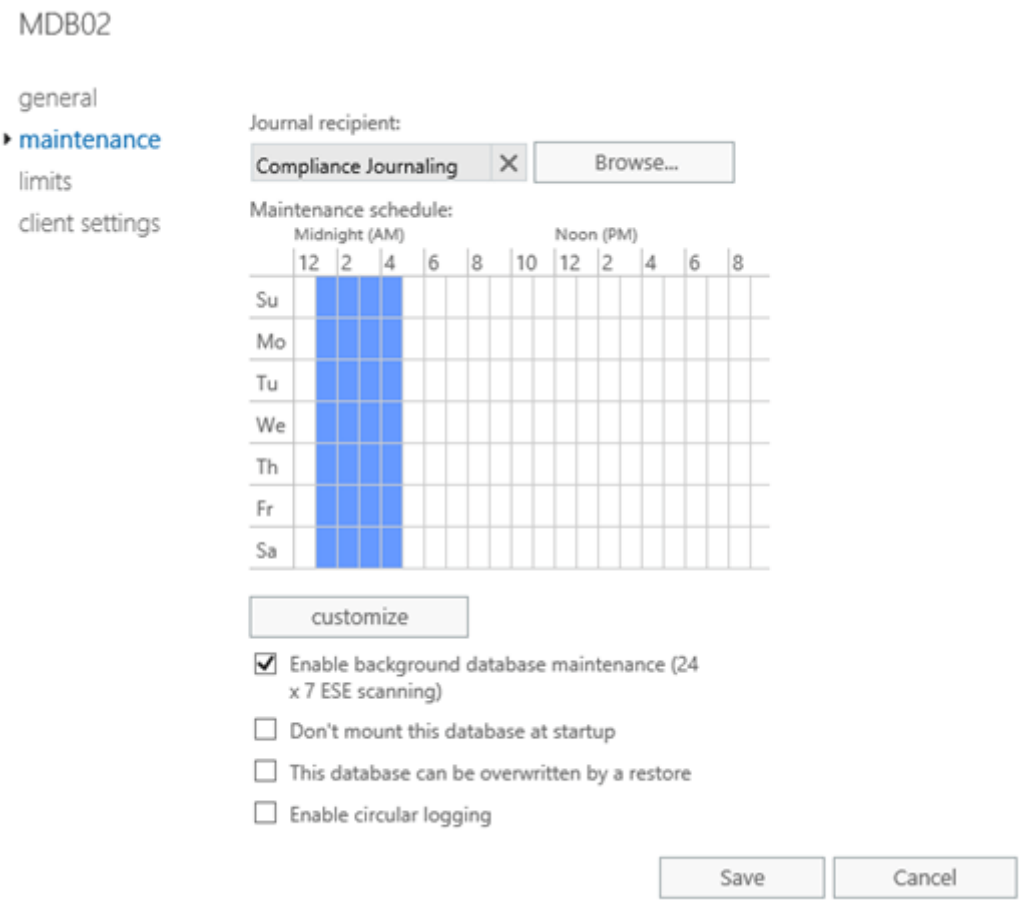
Процедура стандартного ведения журнала

При стандартном ведении журнала выполняется запись всех сообщений, отправленных и полученных всеми почтовыми ящиками в конкретной базе данных почтовых ящиков. Чтобы включить ведение журнала, нужно указать почтовый ящик журналов (почтовый ящик, в котором будут храниться зарегистрированные сообщения) для базы данных. Чтобы отключить ведение журнала для базы данных, очистите значение почтового ящика журналов в базе данных почтовых ящиков. Дополнительные сведения о настройке почтового ящика журналов см. в разделе Почтовый ящик журналов.

> ⊗ **Внимание!**
>
> Отключение ведения журнала для базы данных почтовых ящиков может привести к несоблюдению в организации применимых политик хранения сообщений.

Как включить или отключить ведение журнала для баз данных почтовых ящиков с помощью Центра администрирования Exchange

1. В EAC выберите **Серверы**>**Базы данных**.
2. Выберите базу данных почтовых ящиков и нажмите кнопку **Изменить** (✎
3. В появившемся окне со свойствами базы данных почтовых ящиков откройте вкладку **Обслуживание** и выполните одну из следующих процедур:
    - **Включить ведение журнала**. Нажмите кнопку **Обзор** рядом с полем **Получатель журнала** . В открывшемся диалоговом окне выберите почтовый ящик для хранения внесенных в журнал сообщений, а затем нажмите кнопку **ОК**.
    - **Отключить ведение журнала**. Нажмите кнопку **Удалить X** рядом со значением в поле **Получатель журнала** .



По завершении нажмите кнопку **Сохранить**.

Как с помощью командной консоли Exchange включить или отключить ведение журнала для баз данных почтовых ящиков

Чтобы включить ведение журнала для базы данных почтовых ящиков, используйте указанный ниже синтаксис.

```
Set-MailboxDatabase -Identity <MailboxDatabaseIdentity> -JournalRecipient
<JournalMailboxIdentity>
```

В этом примере показано, как включить ведение журнала для базы данных почтовых ящиков, названной Sales Database, и настроить почтовый ящик, названный Sales Database Journal Mailbox, в качестве почтового ящика журналов, чтобы хранить в нем зарегистрированные сообщения.

```
Set-MailboxDatabase -Identity "Sales Database" -JournalRecipient "Sales
Database Journal Mailbox"
```

Чтобы отключить ведение журнала для базы данных почтовых ящиков, используйте указанный ниже синтаксис.

```
Set-MailboxDatabase -Identity <MailboxDatabaseIdentity> -JournalRecipient
$null
```

В этом примере показано, как отключить ведение журнала для базы данных почтовых ящиков, названной Sales Database.

```
Set-MailboxDatabase -Identity "Sales Database" -JournalRecipient $null
```

В этом примере показано, как отключить ведение журнала для всех баз данных почтовых ящиков в организации Exchange.

```
Get-MailboxDatabase | Set-MailboxDatabase -JournalRecipient $null
```

Как проверить, все ли получилось?

Чтобы убедиться в том, что ведение журнала для базы данных почтовых ящиков успешно включено или отключено, выполните любую из приведенных ниже процедур.

- В EAC перейдите в раздел **Серверы**>**Базы данных**> выберите **пункт Изменить** базу данных > (✎>**Обслуживание** и проверка заполнения поля **Получатель журнала** (ведение журнала включено) или пустого (ведение журнала отключено).
- В командной консоли Exchange выполните приведенную ниже команду, чтобы проверить значение свойства **JournalRecipient** для всех баз данных почтовых ящиков в организации.

  ```
  ```

```
Get-MailboxDatabase | Format-Table -Auto Name,JournalRecipient
```

- Отправьте сообщение в почтовый ящик из базы данных, откройте почтовый ящик журналов в Outlook или Outlook Web App (предыдущее название — Outlook в Интернете) и проверьте, доставлено ли зарегистрированное сообщение (отчет журнала) в почтовый ящик журналов.

Расширенные возможности ведения журнала

Расширенные возможности ведения журнала позволяют использовать *правила журнала*, чтобы записывать сообщения с учетом нужных получателей (указывая всех или выбранных) и необходимых областей (добавляя сообщения внутренние, внешние или все). Для лицензирования уровня "Премиум" требуются клиентские лицензии (CAL) Exchange Enterprise. Дополнительные сведения о клиентских лицензиях см. в разделе Часто задаваемые вопросы о лицензировании Exchange.

Создание правил журнала

Ниже перечислены базовые компоненты правила журнала.

- **Получатель журнала**. Укажите, чьи сообщения нужно записывать в журнал. Можно выбрать все сообщения или сообщения, полученные или отправленные определенными пользователями (в том числе членами групп рассылки).

- **Область действия правила журнала**. Что нужно регистрировать: только внутренние сообщения, только внешние сообщения или внутренние и внешние сообщения.

- **Почтовый ящик журналов**. Укажите, где нужно хранить записанные в журнал сообщения.

Как создавать правила журнала с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел**Правила журналауправления**> соответствием и нажмите кнопку **Добавить** (+

2. В открывшемся окне **Новое правило журнала** настройте указанные ниже параметры.

    - **Отправка отчетов журнала по адресу**: Введите псевдоним или адрес электронной почты почтового ящика журнала, куда будут доставлены сообщения журнала (отчеты журнала).

    - **Имя**. Введите уникальное описательное имя для правила журнала.

    - **Если сообщение отправлено или получено от**: укажите получателя журнала (которого вы хотите записывать в журнал). Щелкните стрелку раскрывающегося списка и выберите любое из указанных ниже значений.

    - **Конкретный пользователь или группа**. В открывшемся диалоговом окне выберите одного получателя и нажмите кнопку **OK** по завершении.

    - **Применить ко всем сообщениям**.

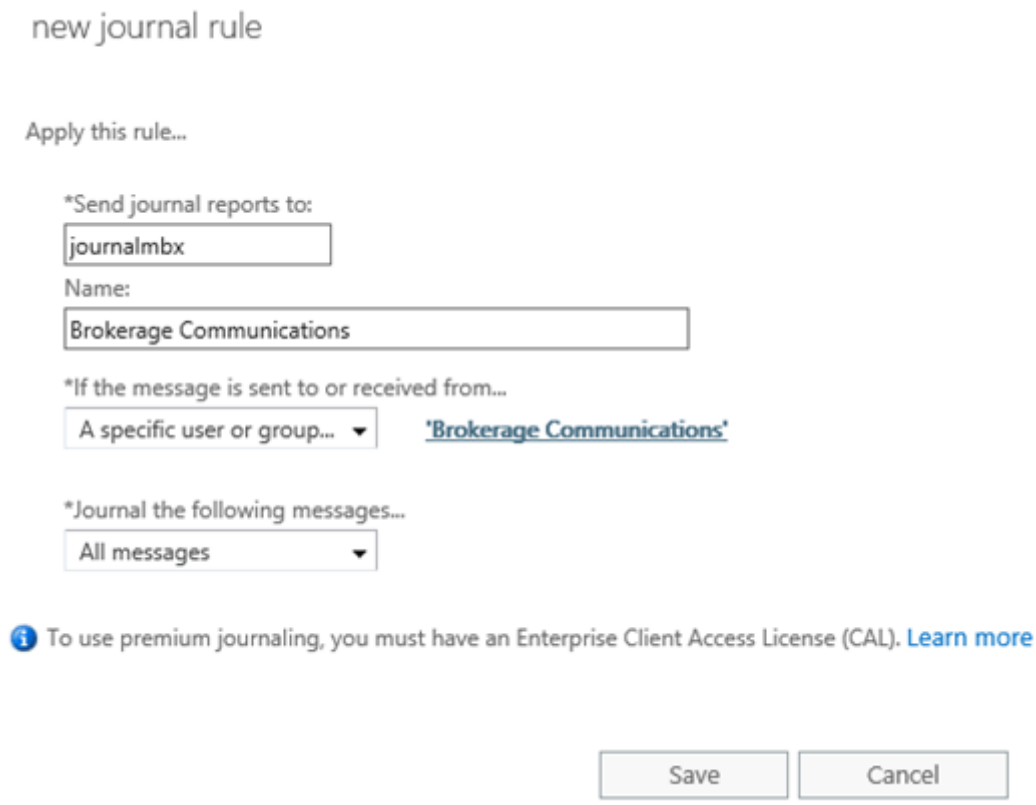
    - **Записывать в журнал следующие сообщения**. Укажите область действия для правила журнала. Щелкните стрелку раскрывающегося списка и выберите одно из доступных значений:

    - **Все сообщения**;

    - **Только внутренние сообщения**;

    - **Только внешние сообщения**.

    По завершении нажмите кнопку **Сохранить**.



Как создавать правила журнала с помощью командной консоли Exchange

Для создания правил журнала в командной консоли Exchange используйте указанный ниже синтаксис.

```
New-JournalRule -Name <RuleName> -JournalEmailAddress
<JournalMailboxIdentity> [-Recipient <JournalRecipientEmailAddress>] [-Scope
<Global | Internal | External>] [-Enabled <$true | $false>]
```

В этом примере показано, как создать правило журнала, названное Regulation 123, с указанными ниже параметрами.

- **Получатель журнала**: пользователь Конни Майр, адрес электронной почты которого — cmayr@contoso.com.
- **Область правила журнала**: внутренние и внешние сообщения (мы не использовали параметр *Scope* , а значение по умолчанию — `Global`).
- **Почтовый ящик журнала**: почтовый ящик с именем Почтовый ящик журнала.
- Правило журнала включено (мы не использовали параметр *Enabled* , а значение по умолчанию — `$true`).

```
New-JournalRule -Name "Regulation 123" -JournalEmailAddress "Journal
Mailbox" -Recipient cmayr@contoso.com
```

Примечание. Чтобы создать правило журнала, которое применяется ко всем получателям, не используйте параметр *Recipient* .

Подробные сведения о синтаксисе и параметрах см. в статье New-JournalRule.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно создали правило журнала, выполните одну из приведенных ниже процедур.

- В EAC перейдите в раздел**Правила журналауправления**> соответствием и убедитесь, что новое правило журнала, созданное вами, указано в списке.
- Чтобы с помощью командной консоли Exchange проверить, есть ли новое правило журнала в списке, выполните указанную ниже команду.

  ```
  Get-JournalRule | Format-Table -Auto
  Name,Recipient,JournalEmailAddress,Scope,Enabled
  ```

- Отправьте сообщение получателю, входящему в область действия правила журнала, откройте в Outlook или Outlook Web App почтовый ящик журналов и проверьте, доставлено ли в него зарегистрированное сообщение (отчет журнала).

Включение или отключение правил журнала

По умолчанию при создании правила журнала в EAC или командной консоли Exchange это правило включено. Командная консоль Exchange может использоваться только для создания отключенного правила журнала (значение параметра *Enabled* находится `$false` в команде **New-JournalRule**).

Создав правило журнала, можно включать или отключать это правило в Центре администрирования Exchange или командной консоли Exchange.

> ⓘ **Важно!**

Если это правило отключено, сообщения, которые должны были бы вноситься в журнал с его помощью, записываться не будут. Убедитесь, что отключением правила журнала вы не нарушаете нормы и требования вашей организации.

Как с помощью Центра администрирования Exchange включать или отключать правила журнала

1. В EAC перейдите в раздел**Правила журналауправления соответствием**>.
2. В представлении списка выберите правило журнала. В столбце **Вкл.** снимите флажок, чтобы отключить правило, или установите его, чтобы включить правило.

Как с помощью командной консоли Exchange включать или отключать правила журнала

Для включения или отключения правил журнала в Командная консоль Exchange используйте указанный ниже синтаксис.

```
<Disable-JournalRule | Enable-JournalRule> -Identity <JournalRuleIdentity>
```

В этом примере показано, как отключить правило журнала под названием Contoso Legal.

```
Disable-JournalRule -Identity "Contoso Legal"
```

В этом примере показано, как включить правило журнала под названием Contoso Legal.

```
Enable-JournalRule -Identity "Contoso Legal"
```

Как проверить, что все получилось?

Чтобы убедиться, что правило журнала успешно включено или выключено, выполните одну из указанных ниже процедур.

- В EAC перейдите в раздел**Правила журналауправления**> соответствием и проверьте состояние флажка в столбце **Вкл**. для правила.
- В командной консоли Exchange выполните приведенную ниже команду, чтобы проверить значение свойства **Enabled** для всех правил журнала.

```
Get-JournalRule | Format-Table -Auto Name,Enabled
```

- Отправьте сообщение получателю, который входит в область действия правила журнала. Затем в Outlook или Outlook Web App откройте почтовый ящик журналов и проверьте, доставлено ли в него зарегистрированное сообщение (отчет журнала).

Изменение правил журнала

При изменении правила журнала никакие дополнительные параметры не используются. В этом случае доступны те же параметры, что и при создании правила.

- **EAC**: перейдите в**раздел Правила журналауправления**> соответствием и нажмите кнопку **Изменить** (✎ Доступные параметры те же, что и при создании правила. Дополнительные сведения см. в разделе Создание правил журнала с помощью EAC .
- **Командная консоль Exchange**: синтаксис для изменения правила журнала:

```
Set-JournalRule -Identity <JournalRuleIdentity> [-Name <RuleName>] [-
JournalEmailAddress <JournalMailboxIdentity>] [-Recipient
<JournalRecipientEmailAddress | $null>] [-Scope <Global | Internal |
External>]
```

Вы не можете использовать командлет **Set-Journal** для включения или отключения правила (параметр *Enabled* отсутствует). Чтобы включить или отключить правило, используйте командлеты **Enable-JournalRule** и **Disable-JournalRule**, как описано в разделе Включение или отключение правил журнала.

Подробные сведения о синтаксисе и параметрах см. в статье Set-JournalRule.

Удаление правил журнала

Как удалять правила журнала с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел**Правила журналауправления соответствием**>.
2. В представлении списка выберите правило или правила, которые нужно удалить, а затем нажмите кнопку **Удалить** (🗑

Как удалять правила журнала с помощью командной консоли Exchange

Для удаления правил журнала в командной консоли Exchange используйте указанный ниже синтаксис.

```
Remove-JournalRule -Identity <JournalRuleIdentity>
```

В этом примере показано удаление правила журнала под названием Brokerage Journal Rule.

```
Remove-JournalRule "Brokerage Journal Rule"
```

Подробные сведения о синтаксисе и параметрах см. в статье Remove-JournalRule.

Как проверить, все ли получилось?

Чтобы убедиться, что правило журнала успешно удалено, выполните одну из указанных ниже процедур.

- В EAC перейдите в раздел**Правила журналауправления**> соответствием и убедитесь, что удаляемое правило больше не указано в списке.
- В командной консоли Exchange выполните указанную ниже команду, чтобы проверить удаление правила.

  ```
  Get-JournalRule | Format-Table -Auto Name
  ```

- Отправьте сообщение получателю, который входил в область действия только что удаленного правила журнала. Затем в Outlook или Outlook Web App откройте почтовый ящик журналов и убедитесь, что зарегистрированное сообщение (отчет журнала) в него не доставлено.

Включение или отключение ведения журнала для уведомлений о голосовой почте и пропущенных звонках

По умолчанию в журнале уровня "Премиум" регистрируются уведомления голосовой почты и сообщения уведомления об пропущенных звонках, созданные единой системой обмена сообщениями (UM) в Exchange 2016. Однако вы можете отключить ведение журнала для этих сообщений. Обратите внимание, что даже если вы отключите ведение журнала для уведомлений от службы единой системы обмена сообщениями, сообщения с факсами, созданные этой службой, все равно будут записываться в журнал.

> ⓘ **Примечание**
>
> Единая система обмена сообщениями не доступна в Exchange 2019.

Этот параметр можно изменить только в командной консоли Exchange.

Чтобы отключить ведение журнала для уведомлений о голосовой почте и пропущенных звонках, выполните указанную ниже команду.

```
Set-TransportConfig -VoicemailJournalingEnabled $false
```

Чтобы включить ведение журнала для уведомлений о голосовой почте и пропущенных звонках, выполните указанную ниже команду.

```
Set-TransportConfig -VoicemailJournalingEnabled $true
```

Как проверить, все ли получилось?

Чтобы убедиться, что ведение журнала для уведомлений о голосовой почте и пропущенных звонках успешно включено или отключено, проверьте значение свойства **VoicemailJournalingEnabled**, выполнив указанную ниже команду.

```
Get-TransportConfig | Format-List VoicemailJournalingEnabled
```

Указание альтернативного почтового ящика журналов

Для заполнения журнала уровня "Премиум" можно указать *альтернативный почтовый ящик журнала* , который принимает отчеты о недоставке (также известные как NDR или сообщения о недоставке) для *всех* отчетов журнала, которые невозможно выполнить, если *любой* почтовый ящик журнала недоступен (один альтернативный почтовый ящик журнала для всех почтовых ящиков журнала в вашей организации). Дополнительные сведения см. в разделе Альтернативный почтовый ящик журнала.

> ⊗ **Внимание!**
>
> Если альтернативный почтовый ящик журналов также недоступен и отклоняет сообщения возврата отчетов журнала, исходные отчеты журнала удаляются без возможности восстановления.

Как указать альтернативный почтовый ящик журналов с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел**Правила журналауправления соответствием**>.
2. Щелкните **Выбрать адрес** рядом с элементом **Отправлять недоставленные отчеты журнала по адресу**.
3. В открывшемся окне **Отчеты о недоставке для недоставленных отчетов журнала** нажмите кнопку **Обзор**, в новом окне выберите почтовый ящик, затем последовательно нажмите кнопки **OK** и **Сохранить**.

Примечание. Чтобы удалить функциональность альтернативного почтового ящика журнала, щелкните адрес электронной почты рядом **с полем Отправка отчетов о недоставленных журналах**. В открывавшемся окне In the **NDR for undeliverable journal reports (В отчетах о недоставленных журналах**) нажмите кнопку **Удалить X** рядом с адресом электронной почты, а затем нажмите кнопку **Сохранить**.

Как указать альтернативный почтовый ящик журналов с помощью командной консоли Exchange

Чтобы указать альтернативный почтовый ящик журналов с помощью командной консоли Exchange, используйте приведенный ниже синтаксис.

```
Set-TransportConfig -JournalingReportNdrTo <MailboxEmailAddress | $null>
```

В этом примере указывается почтовый ящик с адресом altjournalingmbx@contoso.com электронной почты в качестве альтернативного почтового ящика журнала.

```
Set-TransportConfig -JournalingReportNdrTo altjournalingmbx@contoso.com
```

В этом примере показано, как отключить альтернативный почтовый ящик журналов.

```
Set-TransportConfig -JournalingReportNdrTo $null
```

Как проверить, что все получилось?

Чтобы убедиться в том, что альтернативный почтовый ящик журналов успешно указан, выполните любую из приведенных ниже процедур.

- В EAC перейдите в**раздел Правила журналауправления**> соответствием и проверьте значение **параметра Отправить отчеты о недоставленных журналах**.
- В командной консоли Exchange выполните приведенную ниже команду, чтобы проверить значение свойства **JournalingReportNdrTo**.

  ```
  Get-TransportConfig | Format-List JournalingReportNdrTo
  ```

Как включить расшифровку отчетов журнала

Расшифровка отчетов журнала позволяет вести **журнал уровня "Премиум"** , чтобы сохранить в отчетах журналов защищенную IRM копию сообщений с открытым текстом (вместе с исходным сообщением, защищенным IRM). Если сообщение содержит любые вложения, которые были защищены с помощью кластера AD RMS в организации, вложения также расшифровываются.

Чтобы включить расшифровку отчетов журнала, выполните указанные ниже действия.

1. Настройте группу суперпользователей AD RMS. Инструкции см. в статье Add the Federation Mailbox to the AD RMS Super Users Group.
2. Выполните следующую команду в Командная консоль Exchange:

```
Set-IRMConfiguration -JournalReportDecryptionEnabled $true
```

Дополнительные сведения см. в статье Включение и отключение расшифровки отчета журнала.

Правила потока обработки почты в Exchange Server

Статья • 04.04.2023

Правила потока обработки почты (также известные как правила транспорта) можно использовать для идентификации сообщений, проходящих через конвейер транспорта, и принятия действий с сообщениями в организации Exchange 2016 и Exchange 2019. Правила потока обработки почты похожи на правила папки "Входящие", доступные в Outlook и Outlook в Интернете (прежнее название — Outlook Web App). Основное отличие заключается в том, что правила потока обработки почты выполняют действия с сообщениями во время их передачи, а не после доставки сообщения в почтовый ящик. Правила потока обработки почты включают более широкий спектр условий, исключений и действий, позволяющих реализовать политики обмена сообщениями многих типов.

В данной статье описываются компоненты правил потока обработки почты и принципы их работы.

Для управления правилами потока обработки почты можно использовать Центр администрирования Exchange (EAC) или командную консоль Exchange. Инструкции по управлению правилами потока обработки почты см. в разделе Процедуры для правил потока обработки почты в Exchange Server.

Каждое правило можно применить принудительно или тестировать (с уведомлением отправителя или без него). Дополнительные сведения о параметрах тестирования см. в разделах Тестирование правила потока обработки почты и Советы по политике.

Указания по реализации определенных политик обмена сообщениями см. в следующих статьях:

- Заявления об отказе от ответственности, подписи, нижние колонтитулы или заголовки в Exchange Server
- Распространенные сценарии утверждения сообщений
- Использование правил потока обработки почты для проверки вложений сообщений

Компоненты правила обработки почтового потока

Правило состоит из условий, исключений, действий и свойств.

- **Условия**. Определите сообщения, к которым нужно применить действия. Некоторые условия проверяют поля заголовков сообщений (например, поля "Кому", "От" или "Копия"). Другие условия проверяют свойства сообщений (например, тему, текст, вложения, размер или классификацию сообщения). Для большинства условий требуется указать оператор сравнения (например, "равно", "не равно" или "содержит"), а также значение для сравнения. Если условий или исключений нет, правило применяется ко всем сообщениям.

  Полный список условий правил потока обработки почты см. в разделе Условия и исключения (предикаты) правил потока обработки почты в Exchange Server.

- **Исключения**. При необходимости определите сообщения, к которым не должны применяться действия. В исключениях доступны те же идентификаторы сообщений, что и в условиях. Исключения переопределяют условия и запрещают применение действий правила к сообщению, даже если оно соответствует всем настроенным условиям.

- **Действия**. Укажите, что следует делать с сообщениями, которые соответствуют условиям правила и не соответствуют ни одному из исключений. Доступно множество действий, таких как отклонение, удаление и перенаправление сообщений, добавление получателей, добавление префиксов к теме сообщения и вставка заявления об отказе в текст сообщения.

  Полный список доступных действий с правилами потока обработки почты см. в разделе Действия правил потока обработки почты в Exchange Server.

- **Свойства**. Укажите другие параметры правил, которые не являются условиями, исключениями или действиями. Например, они могут указывать, следует ли принудительно применять правило или проверять его, а также период, в течение которого применяется правило. Дополнительные сведения см. в разделе Свойства правил обработки почтового потока этой статьи.

Несколько условий, исключений и действий

В приведенной ниже таблице показан принцип обработки нескольких условий, значений условий, исключений и действий в правиле.

Компонент	Логический оператор	Комментарии
Несколько условий	И	Сообщение должно соответствовать всем условиям правила. Если требуется соответствие одному из условий, используйте отдельные правила для каждого условия. Например, если требуется добавлять одно и то же заявление об отказе к сообщениям с вложениями и сообщениям, содержащим определенный текст, создайте отдельное правило для каждого из условий. В Центре администрирования Exchange очень легко скопировать правило.
Одно условие с несколькими значениями	ИЛИ	В некоторых условиях можно указать несколько значений. Сообщение должно соответствовать любому (не обязательно всем) указанным значениям. Например, если тема сообщения — Сведения о курсах акций, а в условии **Тема содержит любое из этих слов** указаны слова Contoso и акций, то условие выполняется, так как тема содержит одно из указанных значений.
Несколько исключений	ИЛИ	Если сообщение соответствует какому-либо из исключений, к нему не применяются действия. Сообщение может соответствовать не всем исключениям.
Если сообщение соответствует любому из исключений, действия не обрабатываются. Сообщение не должно соответствовать всем исключениям.	И	С сообщениями, соответствующими условиям правила, выполняются все действия, указанные в правиле. Например, если выбраны действия **Добавить в начало темы сообщения** и **Добавить получателей в поле "Скрытая копия"**, к сообщению применяются оба действия. Необходимо помнить, что некоторые действия, например **Удалить сообщение без уведомления**, препятствуют последующей обработке сообщения другими правилами. Другие действия, например **Переслать сообщение**, запрещают дополнительные действия. Кроме того, вы можете задать для правила действие, которые останавливает применение последующих правил к сообщению.

Свойства правил обработки почтового потока

В представленной ниже таблице описываются свойства, доступные в правилах потока обработки почты.

Имя свойства в Центре администрирования Exchange	**Имя параметра в командной консоли Exchange**	**Описание**
Приоритет	*Priority*	Указывает порядок применения правил к сообщениям. Приоритет, заданный по умолчанию, зависит от времени создания правила (чем старше правило, тем выше приоритет), а проверка в случае правил с высоким приоритетом выполняется раньше, чем в случае правил с низким приоритетом. Чтобы изменить приоритет правила в Центре администрирования Exchange, переместите его вверх или вниз в списке правил. В командной консоли Exchange вы задаете номер приоритета (0 является наивысшим приоритетом). Например, если одно правило отклоняет сообщения с номером кредитной карты, а второе требует подтверждения, необходимо, чтобы правило отклонения применялось первым и останавливало обработку других правил. Дополнительные сведения см. в разделе Установка приоритета для правил потока обработки почты.
Проверять выполнение этого правила со степенью серьезности	*SetAuditSeverity*	Задает уровень серьезности отчета об инциденте и соответствующую запись, которая записывается в журнал отслеживания сообщений, если сообщения нарушают политики защиты от потери данных. Допустимые значения: DoNotAudit, Low, Medium и High.

Имя свойства в Центре администрирования Exchange	Имя параметра в командной консоли Exchange	Описание
Режим	*Mode*	Вы можете сразу начать применять правило к сообщениям или проверить его, не оказывая влияния на доставку сообщений (как с подсказками политики защиты от потери данных, так и без них). Советы по политике похожи на подсказки и могут быть настроены для представления краткой заметки в Outlook или Outlook в Интернете, которая предоставляет сведения о возможных нарушениях политики для пользователя, создающего сообщение. Дополнительные сведения см. в разделе Советы по политике. Дополнительные сведения о режимах см. в разделе Тестирование правила потока обработки почты.
Активировать это правило начиная с **Отключить это правило начиная с**	*ActivationDate* *ExpiryDate*	Задает диапазон дат для работы правила.
Флажок **Вкл** установлен или снят	Новые правила: *параметр Enabled* в командлете **New-TransportRule** . Существующие правила: используйте командлет **Enable-TransportRule** или **Disable-TransportRule**. Значение отображается в свойстве **State** правила.	Вы можете создать отключенное правило и включить его, когда будете готовы его проверить. Кроме того, вы можете отключить правило, не удаляя его, чтобы сохранить параметры. Сведения о том, как это сделать, см. в разделе Включение и отключение правил потока обработки почты.
Отложить сообщение, если не завершена обработка правил	*RuleErrorAction*	Вы можете указать, как должно обрабатываться сообщение, если не удается завершить обработку правила. По умолчанию правило игнорируется, но при желании сообщение можно отправлять на повторную обработку.

Имя свойства в Центре администрирования Exchange	Имя параметра в командной консоли Exchange	Описание
Соответствие адреса отправителя в сообщении	*SenderAddressLocation*	Если в правиле используются условия или исключения, проверяющие электронный адрес отправителя, нужное значение можно искать в заголовке, конверте сообщения или одновременно в заголовке и конверте. Дополнительные сведения см. в разделе Отправители.
Остановить обработку других правил	*SenderAddressLocation*	Это действие для правила, но в Центре администрирования Exchange оно отображается как свойство. Вы можете остановить применение других правил к сообщению после его обработки данным правилом.
Комментарии	*Comments*	**Комментарии** Вы можете ввести описательные примечания к правилу.

Как применяются правила обработки почтового потока

Правила потока обработки почты применяются агентом транспорта на серверах почтовых ящиков и пограничных транспортных серверах. На серверах почтовых ящиков правила применяет агент правил транспорта. На пограничных транспортных серверах правила применяет агент пограничных правил. Хотя эти агенты обладают схожими наборами функций, между ними есть некоторые отличия. В приведенной ниже таблице представлена сводка важных отличий.

Агент транспорта	Событие SMTP или классификатора при применении правил	Место хранения правил
Агент правил транспорта на серверах почтовых ящиков	Событие классификатора **OnResolvedMessage**. В Exchange 2010 агент правила транспорта был вызван для события классификатора **OnRoutedMessage** . Переход на событие **OnResolvedMessage** позволил использовать новые действия правил, которые могут управлять маршрутизацией приложения (например, требовать протокол TLS).	В Active Directory. Правила доступны всем серверам почтовых ящиков в лесу Active Directory.

Агент транспорта	Событие SMTP или классификатора при применении правил	Место хранения правил
Агент пограничных правил на пограничных транспортных серверах	Событие **SMTP OnEndOfData**	В локальном экземпляре служб Active Directory облегченного доступа к каталогам (AD LDS) на сервере. Правила применяются только к сообщениям, проходящим через локальный сервер.

Дополнительные сведения об агентах транспорта см. в разделе Транспортные агенты в Exchange Server.

Различия обработки в зависимости от типа сообщения

Через организацию проходят сообщения нескольких типов. Типы сообщений, которые могут быть обработаны правилами транспорта, описаны в таблице ниже.

Тип сообщения	Можно ли применить правило?
Обычные сообщения. Сообщения, которые содержат обычный текст либо текст в формате RTF или HTML. Кроме того, текст может содержать составной или альтернативный набор форматов.	Да
Зашифрованные S/MIME-сообщения	Правила могут получать доступ к заголовкам конвертов и обрабатывать сообщения только при соблюдении условий, проверяющих эти заголовки. Правила с условиями, требующими проверки содержимого сообщения, или действиями, которые меняют содержимое сообщения, не могут обрабатываться.

Тип сообщения	Можно ли применить правило?
Защищенные сообщения RMS. Сообщения, защищенные с помощью шаблона политики прав active Directory Rights Management Services (AD RMS).	Правила всегда могут получать доступ к заголовкам конвертов и обрабатывать сообщения в зависимости от условий, которые проверяют эти заголовки. Чтобы правило проверял или изменял содержимое защищенного сообщения, необходимо: • установить параметр **Обязательно** или **Необязательно** для транспортной расшифровки. По умолчанию выбран параметр **Необязательно**; • Ключ шифрования .
Сообщения с открытой подписью. Сообщения, которые были подписаны, но не зашифрованы.	Да
Сообщения единой системы обмена сообщениями: сообщения, созданные или обрабатываемые службой единой системы обмена сообщениями в Exchange 2016, такие как голосовая почта, факс, уведомления о пропущенных звонках и сообщения, созданные или пересылаемые с помощью голосового доступа Microsoft Outlook. (**Примечание**. Единая система обмена сообщениями недоступна в Exchange 2019.)	Да
Анонимные сообщения: сообщения, отправленные анонимными отправителями.	Да
Чтение отчетов. Отчеты, созданные в ответ на запросы на чтение уведомлений от отправителей. Отчеты чтения имеют класс `IPM.Note*.MdnRead` сообщений или `IPM.Note*.MdnNotRead`.	Да

Хранение и репликация правил

Правила потока обработки почты, которые вы создаете и настраиваете на серверах почтовых ящиков, хранятся в Active Directory и считываются и применяются транспортной службой на всех серверах почтовых ящиков в организации. При

создании, изменении или удалении правила потока обработки почты изменение реплицируется между контроллерами домена в вашей организации. Это позволяет Exchange предоставлять согласованный набор правил потока обработки почты в организации.

Примечания.

- Репликация между контроллерами домена зависит от факторов, которые не контролируются Exchange (например, количество сайтов Active Directory и скорость сетевых каналов). Следовательно, при реализации правил потока обработки почты в организации следует учитывать задержки репликации. Дополнительные сведения о репликации Active Directory см. в статье Общие сведения о репликации Active Directory и управлении топологией с помощью Windows PowerShell.

- Каждый сервер почтовых ящиков кэширует расширенные группы рассылки, чтобы избежать повторных запросов Active Directory на определение членства в группах. По умолчанию записи в кэше расширенных групп действительны в течение четырех часов. Следовательно, правила потока обработки почты не обнаруживают членство в группах, пока кэш расширенных групп не будет обновлен. Чтобы принудительно обновить кэш на сервере почтовых ящиков, перезапустите службу транспорта Microsoft Exchange. Эту службу необходимо перезапустить на каждом сервере почтовых ящиков, где требуется принудительно обновить кэш.

Правила потока обработки почты, создаваемые и настраиваемые на пограничных транспортных серверах, хранятся в локальном экземпляре служб AD LDS на сервере. На пограничных транспортных серверах не происходит автоматическая репликация правил потока обработки почты. Правила на пограничном транспортном сервере применяются только к сообщениям, проходящим через локальный сервер. Если один и тот же набор правил потока обработки почты требуется применить на нескольких пограничных транспортных серверах, вы можете клонировать конфигурацию пограничного транспортного сервера либо экспортировать, а затем импортировать правила потока обработки почты. Дополнительные сведения см. в статье Edge Transport Server Cloned Configuration и разделе Импорт и экспорт коллекций правил потока обработки почты.

Каждый раз, когда служба транспорта на сервере почтовых ящиков или пограничном транспортном сервере обнаруживает измененное правило потока обработки почты, соответствующее событие записывается в журнал приложений в средстве просмотра событий (код события 4002 на серверах почтовых ящиков и 16028 на пограничных транспортных серверах).

Репликация и хранение правила в смешанных средах

Существует два типичных сценария смешанной среды:

- **Гибридные развертывания, в которых часть организации находится в Microsoft 365 или Office 365**

  В гибридной среде репликация правил между локальной организацией Exchange и Microsoft 365 или Office 365 не выполняется. Поэтому при создании правила в Exchange необходимо создать соответствующее правило в Microsoft 365 или Office 365. Правила, создаваемые в Microsoft 365 или Office 365, хранятся в облаке, а правила, создаваемые в локальной организации, хранятся локально в Active Directory. При управлении правилами в гибридной среде необходимо синхронизировать два набора правил, внося изменения в обоих местах или внося изменения в одну среду, а затем экспортировать правила и импортировать их в другую среду.

  Важно! Несмотря на существенное перекрытие условий и действий, доступных в Microsoft 365 или Office 365 и Exchange Server, существуют различия. Если вы планируете создавать одно и то же правило в обеих средах, убедитесь, что нужные действия доступны. Список доступных условий и действий, доступных в Microsoft 365 или Office 365, см. в следующих разделах:

  Условия и исключения (предикаты) правил для потока обработки почты в Exchange Online

  Действия правил потока почты в Exchange Online

- **Совместная работа с Exchange 2010**

  > ⓘ **Примечание**
  >
  > Этот раздел относится только к Exchange 2016.

  При совместном использовании Exchange 2010 все правила потока обработки почты хранятся в Active Directory и реплицируются в вашей организации независимо от Exchange Server версии, используемой для создания правил. Однако все правила потока обработки почты связаны с версией сервера Exchange Server, которая использовалась для их создания, и хранятся в контейнере для конкретной версии в Active Directory. При первом развертывании Exchange 2016 в организации все существующие правила импортируются в Exchange 2016 в процессе установки. Однако все последующие изменения потребуется вносить в обе версии. Например, если

изменить существующее правило в Exchange 2016 (командная консоль Exchange или EAC), то же самое изменение необходимо внести в Exchange 2010 (командная консоль Exchange или консоль управления Exchange).

Exchange 2010 не может обрабатывать правила, имеющие значение **Version** или **RuleVersion** 15. *n*. *n*. *n*. Чтобы убедиться, что все правила могут быть обработаны, используйте только правила со значением 14. *n*. *n*. *n*.

Условия и исключения (предикаты) правил потока обработки почты в Exchange Server

Статья • 14.08.2024

Условия и исключения в правилах потока обработки почты (также называемых правилами транспорта) определяют, к каким сообщениям правило применяется, а к каким — нет. Например, если правило добавляет к сообщениям заявление об отказе, вы можете настроить это правило так, чтобы оно применялось только к сообщениям от определенных пользователей, содержащим указанные слова, или ко всем сообщениям, кроме тех, которые были отправлены участникам определенной группы. В совокупности условия и исключения в правилах потока обработки почты также *называются предикатами*, так как для каждого условия существует соответствующее исключение, использующее одинаковые параметры и синтаксис. Единственное отличие заключается в том, что условия указывают, к каким сообщениям правило применяется, а исключения — наоборот.

Большинство условий и исключений содержат только одно свойство, принимающее одно или несколько значений. Например, для условия **Отправитель** необходимо указать отправителя сообщения. У некоторых условий есть два свойства. Например, для условия **Заголовок сообщения включает любое из этих слов** необходимо указать в одном свойстве поле заголовка сообщения, а в другом — искомый текст. У некоторых условий и исключений нет свойств. Например, условие **В любом вложении есть исполняемое содержимое** просто ищет в сообщениях вложения с исполняемым содержимым.

Дополнительные сведения о правилах потока обработки почты в Exchange Server, включая обработку нескольких условий, исключений или многозначных условий и исключений, см. в статье Правила потока обработки почты в Exchange Server.

Дополнительные сведения об условиях и исключениях в правилах потока обработки почты в Exchange Online Protection или Exchange Online см. в статье Условия и исключения (предикаты) правил потока обработки почты в Exchange Online.

Условия и исключения для правил потока обработки почты на серверах почтовых ящиков

В следующих разделах представлены таблицы, описывающие условия и исключения, доступные в правилах потока обработки почты на серверах почтовых ящиков. Типы свойств описываются в разделе Типы свойств.

Отправители

Получатели

Тема или текст сообщения

Вложения

Все получатели

Типы конфиденциальной информации, значения в полях "Кому" и "Копия", размер и кодировки сообщений

Отправитель и получатель

Свойства сообщения

Заголовки сообщений

> 7 **Примечание**

- Когда вы выберете условие или исключение в Центре администрирования Exchange (EAC), значение, которое в итоге отобразится в поле **Применить это правило, если** или **Кроме случаев, когда**, скорее всего, будет короче указанного (если вы составляли его из частей). Кроме того, при создании правил на основе шаблона (отфильтрованного списка сценариев) часто можно не составлять условие из частей, а выбрать для него краткое имя. Краткие имена и полные названия условий и исключений представлены в столбцах с данными по Центру администрирования Exchange.
- Если в Центре администрирования Exchange выбрано условие **[Применить ко всем сообщениям]**, указывать другие условия невозможно. В командной консоли Exchange для создания такого правила достаточно не указывать никаких параметров условий.
- Условия и исключения содержат одни и те же параметры и свойства, поэтому в выходных данных командлета **Get-TransportRulePredicate** исключения не указываются отдельно. Кроме того, имена некоторых предикатов, возвращаемые этим командлетом, отличаются от имен соответствующих параметров, а в предикате может потребоваться указать несколько параметров.

Отправители

Для условий и исключений, проверяющих адрес отправителя, можно указать, где правило будет искать этот адрес.

В центре администрирования EAC в разделе **Свойства этого правила** выберите **Сопоставить адрес отправителя в сообщении**. Для просмотра этого параметра может потребоваться выбрать **Дополнительные параметры** . В командной консоли Exchange параметром является *SenderAddressLocation*. Ниже представлены возможные значения.

- **Заголовок**: проверяет только отправителей в заголовках сообщений (например, поля **"От"**, **"Отправитель"** или **"Ответить** на"). Это значение по умолчанию и способ работы правил потока обработки почты до Exchange 2013 с накопительным обновлением 1 (CU1).
- **Конверт**. Проверьте только отправителей из конверта сообщения (значение **MAIL FROM** , которое использовалось при передаче SMTP, которое обычно хранится в поле **Return-Path**). Поиск конвертов сообщений доступен только для следующих условий (и соответствующих исключений):
  - **Отправитель (***Om*)
  - **Отправитель является членом** (*FromMemberOf*)
  - **Адрес отправителя включает** (*FromAddressContainsWords*)
  - **Адрес отправителя совпадает** (*FromAddressMatchesPatterns*)
  - **Домен отправителя —** (*SenderDomainIs*)
- **Заголовок или конверт** (`HeaderOrEnvelope`): проверьте отправителей в заголовке сообщения и конверте сообщения.

Развернуть таблицу

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
Отправитель... **Отправитель>это человек**	*From* *ExceptIfFrom*	`Addresses`	Сообщения, отправленные указанными почтовыми ящиками, почтовыми пользователями или почтовыми контактами в организации Exchange.	Exchange 2010 или более поздней версии

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
Расположение отправителя **Отправитель>является внешним или внутренним**	*FromScope* *ExceptIfFromScope*	`UserScopeFrom`	Сообщения от внутренних или внешних отправителей.	Exchange 2010 или более поздней версии
Отправитель входит в группу **Отправитель>является членом этой группы**	*FromMemberOf* *ExceptIfFromMemberOf*	`Addresses`	Сообщения, отправленные участником заданной группы.	Exchange 2010 или более поздней версии
Адрес отправителя содержит **Отправитель>адрес включает любое из этих слов**	*FromAddressContainsWords* *ExceptIfFromAddressContainsWords*	`Words`	Сообщения, электронный адрес отправителя которых содержит указанные слова.	Exchange 2010 или более поздней версии
Адрес отправителя совпадает с **Отправитель>адрес соответствует любому из этих текстовых шаблонов**	*FromAddressMatchesPatterns* *ExceptIfFromAddressMatchesPatterns*	`Patterns`	Сообщения, электронный адрес отправителя которых содержит текстовые шаблоны, соответствующие указанным регулярным выражениям.	Exchange 2010 или более поздней версии
Указанные свойства отправителя включают любое из этих слов **Отправитель>имеет определенные свойства, включая любое из этих слов**	*SenderADAttributeContainsWords* *ExceptIfSenderADAttributeContainsWords*	Первое свойство: `ADAttribute` Второе свойство: `Words`	Сообщения, в которых заданный атрибут Active Directory отправителя содержит любые из указанных слов. Для атрибута **Country** требуется двухбуквенный код страны (например, DE для Германии).	Exchange 2010 или более поздней версии
Указанные свойства отправителя совпадают с этими текстовыми шаблонами **Отправитель>имеет определенные свойства, соответствующие этим текстовым шаблонам**	*SenderADAttributeMatchesPatterns* *ExceptIfSenderADAttributeMatchesPatterns*	Первое свойство: `ADAttribute` Второе свойство: `Patterns`	Сообщения, в которых заданный атрибут Active Directory отправителя содержит текстовые шаблоны, соответствующие указанным регулярным выражениям.	Exchange 2010 или более поздней версии
Отправитель переопределил подсказку политики **Отправитель>переопределен совет политики**	*HasSenderOverride* *ExceptIfHasSenderOverride*	Н/д	Сообщения, в которых отправитель решил переопределить политику защиты от потери данных (DLP). Дополнительные сведения о политиках защиты от потери данных см. в статье Защита от потери данных в Exchange Server.	Exchange 2013 или более поздней версии

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
IP-адрес отправителя находится в диапазоне **Отправитель>IP-адрес находится в любом из этих диапазонов или точно соответствует**	*SenderIPRanges* *ExceptIfSenderIPRanges*	`IPAddressRanges`	Сообщения, IP-адрес отправителя которых совпадает с указанным IP-адресом или находится в указанном диапазоне IP-адресов.	Exchange 2013 или более поздней версии
Домен отправителя... **Отправитель>domain is is**	*SenderDomainIs* *ExceptIfSenderDomainIs*	`DomainName`	Сообщения, в которых домен электронного адреса отправителя совпадает с указанным значением. Если необходимо найти домены отправителя, *содержащие* указанный домен (например, любой поддомен домена), используйте условие **Соответствие адреса отправителя** (*FromAddressMatchesPatterns*) и укажите домен с помощью синтаксиса : `'\.domain\.com$'`.	Exchange 2013 или более поздней версии

Получатели

Развернуть таблицу

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
Получатель **Получатель>это человек**	*SentTo* *ExceptIfSentTo*	`Addresses`	Сообщения, одним из получателей которых является указанный почтовый ящик, почтовый пользователь или почтовый контакт в организации Exchange. Получатели могут быть указаны в поле **To**, **Cc** или **Bcc** сообщения. **Примечание**. Нельзя указать группы рассылки или группы безопасности с поддержкой почты. Если необходимо выполнить действия с сообщениями, отправляемыми в группу, используйте вместо этого условие **To contains** (*AnyOfToHeader*).	Exchange 2010 или более поздней версии
Расположение получателя	*SentToScope* *ExceptIfSentToScope*	`UserScopeTo`	Сообщения, отправленные внутренним получателям, внешним получателям,	Exchange 2010 или более

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
Получатель>имеет значение external/external			внешним получателям из партнерских организаций или внешним получателям из организаций, не являющихся партнерскими.	поздней версии
Получатель входит в группу **Получатель>является членом этой группы**	*SentToMemberOf* *ExceptIfSentToMemberOf*	`Addresses`	Сообщения, у которых есть получатели, являющиеся членами указанной группы. Группа может быть указана в поле **To**, **Cc** или **Bcc** сообщения.	Exchange 2010 или более поздней версии
Адрес получателя содержит **Получатель>адрес включает любое из этих слов**	*RecipientAddressContainsWords* *ExceptIfRecipientAddressContainsWords*	`Words`	Сообщения, электронный адрес получателя которых содержит указанные слова. **Примечание.** Это условие или исключение не учитывает сообщения, отправляемые на прокси-адреса получателей. Он соответствует только сообщениям, отправленным основной адрес электронной почты получателя.	Exchange 2010 или более поздней версии
Адрес получателя соответствует **Получатель>адрес соответствует любому из этих текстовых шаблонов**	*RecipientAddressMatchesPatterns* *ExceptIfRecipientAddressMatchesPatterns*	`Patterns`	Сообщения, электронный адрес получателя которых содержит текстовые шаблоны, соответствующие указанным регулярным выражениям. **Примечание.** Это условие или исключение не учитывает сообщения, отправляемые на прокси-адреса получателей. Он соответствует только сообщениям, отправленным основной адрес электронной почты получателя.	Exchange 2010 или более поздней версии
Указанные свойства получателя содержат любое из следующих слов **Получатель>имеет определенные свойства, включая любое из этих слов**	*RecipientADAttributeContainsWords* *ExceptIfRecipientADAttributeContainsWords*	Первое свойство: `ADAttribute` Второе свойство: `Words`	Сообщения, в которых заданный атрибут Active Directory получателя содержит любое из указанных слов. Для атрибута **Country** требуется двухбуквенный код страны (например, DE для Германии).	Exchange 2010 или более поздней версии
Указанные свойства получателя соответствуют этим текстовым шаблонам **Получатель>имеет определенные свойства, соответствующие**	*RecipientADAttributeMatchesPatterns* *ExceptIfRecipientADAttributeMatchesPatterns*	Первое свойство: `ADAttribute` Второе свойство: `Patterns`	Сообщения, в которых заданный атрибут Active Directory получателя содержит текстовые шаблоны, соответствующие указанным регулярным выражениям.	Exchange 2010 или более поздней версии

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
этим текстовым шаблонам				
Домен получателя... **Получатель>domain is is**	*RecipientDomainIs* *ExceptIfRecipientDomainIs*	`DomainName`	Сообщения, в которых домен электронного адреса получателя совпадает с указанным значением. Если вам нужно найти домены получателей, *содержащие* указанный домен (например, любой поддомен домена), используйте условие **Адреса получателя** (*RecipientAddressMatchesPatterns*) и укажите домен с помощью синтаксиса `'\.domain\.com$'`.	Exchange 2013 или более поздней версии

Тема или текст сообщения

> 7 **Примечание**
>
> Поиск слов или текстовых шаблонов в теме или других полях заголовка в сообщении происходит *после* того, как сообщение было декодировано из метода кодирования передачи содержимого MIME, который использовался для передачи двоичного сообщения между SMTP-серверами в тексте ASCII. Нельзя использовать условия или исключения для поиска необработанных (как правило, Base64) значений темы или других полей заголовка в сообщениях.

Развернуть таблицу

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
Тема или текст содержат **Тема или текст>тема или текст включает любое из этих слов**	*SubjectOrBodyContainsWords* *ExceptIfSubjectOrBodyContainsWords*	`Words`	Сообщения, в которых поле **Subject** или текст содержит указанные слова.	Exchange 2010 или более поздней версии
Тема или основной текст соответствует **Тема или текст>Тема или текст соответствуют этим текстовым шаблонам**	*SubjectOrBodyMatchesPatterns* *ExceptIfSubjectOrBodyMatchesPatterns*	`Patterns`	Сообщения, в которых поле **Subject** или текст содержит текстовые шаблоны, соответствующие указанным регулярным выражениям.	Exchange 2010 или более поздней версии
Тема содержит **Тема или текст>тема включает любое из этих слов**	*SubjectContainsWords* *ExceptIfSubjectContainsWords*	`Words`	Сообщения, в которых поле **Subject** содержит указанные слова.	Exchange 2010 или более поздней версии

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
Тема соответствует **Тема или текст>Тема соответствует этим текстовым шаблонам**	*SubjectMatchesPatterns* *ExceptIfSubjectMatchesPatterns*	`Patterns`	Сообщения, в которых поле **Subject** содержит текстовые шаблоны, соответствующие указанным регулярным выражениям.	Exchange 2010 или более поздней версии

Вложения

Дополнительные сведения о том, как правила потока обработки почты проверяют вложения сообщений, см. в статье Использование правил потока обработки почты для проверки вложений сообщений.

Развернуть таблицу

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
Содержимое любого вложения включает **Любое вложение>содержимое включает любое из этих слов**	*AttachmentContainsWords* *ExceptIfAttachmentContainsWords*	`Words`	Сообщения, вложения которых содержат указанные слова.	Exchange 2010 или более поздней версии
Содержимое любого вложения совпадает с **Любое вложение>содержимое соответствует этим текстовым шаблонам**	*AttachmentMatchesPatterns* *ExceptIfAttachmentMatchesPatterns*	`Patterns`	Сообщения, вложения которых содержат текстовые шаблоны, соответствующие указанным регулярным выражениям. **Примечание.** Проверяются только первые 150 КБ каждого вложения.	Exchange 2010 или более поздней версии
Невозможно проверить содержимое каких-либо вложений **Любое вложение>содержимое не может быть проверено**	*AttachmentIsUnsupported* *ExceptIfAttachmentIsUnsupported*	Н/д	Сообщения, в которых вложения изначально не распознаны Exchange, а необходимый IFilter не установлен на сервере почтовых ящиков. Дополнительные сведения см. в разделе Регистрация IFilters пакета фильтров с помощью Exchange Server.	Exchange 2010 или более поздней версии

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
Любое имя вложенного файла, соответствующее **Любое вложение>имя файла соответствует этим текстовым шаблонам**	*AttachmentNameMatchesPatterns* *ExceptIfAttachmentNameMatchesPatterns*	`Patterns`	Сообщения, в которых имя файла вложения содержит текстовые шаблоны, соответствующие указанным регулярным выражениям.	Exchange 2010 или более поздней версии
Расширение файла любого вложения соответствует **Любое вложение>расширение файла включает эти слова**	*AttachmentExtensionMatchesWords* *ExceptIfAttachmentExtensionMatchesWords*	`Words`	Сообщения, в которых расширение файла вложения совпадает с любым из указанных свойств.	Exchange 2013 или более поздней версии
Любое вложение размером не менее **Любое вложение > Имеет размер не меньше**	*AttachmentSizeOver* *ExceptIfAttachmentSizeOver*	`Size`	Сообщения, содержащие вложения, размер которых равен заданному или превышает его. В Центре администрирования Exchange указать размер можно только в килобайтах (КБ).	Exchange 2010 или более поздней версии
Сообщение не завершило сканирование **Любое вложение>не завершена проверка**	*AttachmentProcessingLimitExceeded* *ExceptIfAttachmentProcessingLimitExceededed*	Н/д	Сообщения, для которых обработчику правил не удалось завершить сканирование вложений. С помощью этого условия можно создавать правила, которые совместно определяют и обрабатывают сообщения, содержимое которых не полностью прошло сканирование.	Exchange 2013 или более поздней версии
Любое вложение содержит исполняемое содержимое **Любое вложение>содержит исполняемое содержимое**	*AttachmentHasExecutableContent* *ExceptIfAttachmentHasExecutableContent*	Н/д	Сообщения, которые содержат вложения, являющиеся исполняемыми файлами. Система просматривает свойства файла, а не	Exchange 2013 или более поздней версии

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
			только его расширение.	
Любое вложение защищено паролем **Любое вложение>защищен паролем**	*AttachmentIsPasswordProtected* *ExceptIfAttachmentIsPasswordProtected*	Н/Д	Сообщения с вложениями, защищенными паролем (такие файлы нельзя проверить). Обнаружение паролей работает только для документов Office, .zip файлов и файлов .7Z.	Exchange 2013 или более поздней версии
имеет следующие свойства, включая любое из этих слов **Любое вложение>имеет эти свойства, включая любое из этих слов**	*AttachmentPropertyContainsWords* *ExceptIfAttachmentPropertyContainsWords*	Первое свойство: `DocumentProperties` Второе свойство: `Words`	Сообщения, в которых заданное свойство вложенного документа Office содержит указанные слова. Это условие помогает интегрировать правила потока обработки почты с SharePoint, инфраструктурой классификации файлов (FCI) в Windows Server 2012 R2 или более поздней версии или сторонней системой классификации. Вы можете выбрать встроенное свойство из списка или указать настраиваемое свойство.	Exchange 2016 или более поздней версии

Все получатели

Условия и исключения в этом разделе предоставляют уникальную возможность, которая влияет на *всех* получателей, когда сообщение содержит хотя бы одного из указанных получателей. Например, предположим, что у вас есть правило, которое отклоняет сообщения. Если вы используете условие получателя из раздела Получатели , сообщение отклоняется только для указанных получателей. Например, если правило находит указанного получателя в сообщении, но оно содержит пять других получателей. Сообщение отклоняется для этого получателя и доставляется пяти другим получателям.

Если добавить условие для получателей из данного радела, сообщение будет отклонено как для обнаруженного получателя, так и для пяти остальных пользователей.

И наоборот, исключение получателя из этого раздела *предотвращает* применение действия правила ко *всем* получателям сообщения, а не только к обнаруженным получателям.

> 7 **Примечание**
>
> Это условие или исключение не учитывает сообщения, отправляемые на прокси-адреса получателя. Он соответствует только сообщениям, отправленным основной адрес электронной почты получателя.

Развернуть таблицу

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
Адрес какого-либо получателя содержит **Любой получатель>адрес включает любое из этих слов**	*AnyOfRecipientAddressContainsWords* *ExceptIfAnyOfRecipientAddressContainsWords*	`Words`	Сообщения, в которых поле **To**, **Cc** или **Bcc** содержит указанные слова.	Exchange 2013 или более поздней версии
Адрес какого-либо получателя соответствует **Любой получатель>адрес соответствует любому из этих текстовых шаблонов**	*AnyOfRecipientAddressMatchesPatterns* *ExceptIfAnyOfRecipientAddressMatchesPatterns*	`Patterns`	Сообщения, в которых поле **To**, **Cc** или **Bcc** содержит текстовые шаблоны, соответствующие указанным регулярным выражениям.	Exchange 2013 или более поздней версии

Типы конфиденциальной информации, значения в полях "Кому" и "Копия", размер и кодировки сообщений

Условия в этом разделе, которые ищут значения в полях **Кому** и **Копия** , ведут себя так же, как условия в разделе Любые получатели (правило влияет на *всех* получателей сообщения, а не только на обнаруженных получателей).

> 7 **Примечание**
>
> Условия получателя в этом разделе не учитывают сообщения, отправляемые на прокси-адреса получателя. Они соответствуют только сообщениям, отправленным основной адрес электронной почты получателя.

Развернуть таблицу

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
Сообщение содержит конфиденциальные сведения **Сообщение>содержит любой из этих типов**	*MessageContainsDataClassifications* *ExceptIfMessageContainsDataClassifications*	`SensitiveInformationTypes`	Сообщения, которые содержат конфиденциальную информацию, определенную в политиках защиты	Exchange 2013 или более поздней версии

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
конфиденциальной информации;			от потери данных (DLP). Это условие требуется для правил, использующих действие **Уведомить отправителя с помощью подсказки политики** (*NotifySender*).	
Поле "Кому" содержит **Сообщение**>**В поле содержится этот человек**	*AnyOfToHeader* *ExceptIfAnyOfToHeader*	`Addresses`	Сообщения, в которых поле **To** содержит какого-либо из указанных получателей.	Exchange 2010 или более поздней версии
Поле "Кому" содержит члена группы **Сообщение**>**В поле содержится член этой группы**	*AnyOfToHeaderMemberOf* *ExceptIfAnyOfToHeaderMemberOf*	`Addresses`	Сообщения, в которых поле **To** содержит получателя, являющегося членом указанной группы.	Exchange 2010 или более поздней версии
Поле "Копия" содержит **Сообщение**>**Поле "Копия" содержит этого человека**	*AnyOfCcHeader* *ExceptIfAnyOfCcHeader*	`Addresses`	Сообщения, в которых поле **Cc** содержит какого-либо из указанных получателей.	Exchange 2010 или более поздней версии
Поле "Копия" содержит члена группы **Сообщение**>**содержит члена этой группы**	*AnyOfCcHeaderMemberOf* *ExceptIfAnyOfCcHeaderMemberOf*	`Addresses`	Сообщения, в которых поле **Cc** содержит получателя, являющегося членом указанной группы.	Exchange 2010 или более поздней версии
Поле "Кому" или "Копия" содержит **Сообщение**>**Поле "Кому" или "Копия" содержит этого человека**	*AnyOfToCcHeader* *ExceptIfAnyOfToCcHeader*	`Addresses`	Сообщения, в которых поле **To** или **Cc** содержит какого-либо из указанных получателей.	Exchange 2010 или более поздней версии
Поле "Кому" или "Копия" содержит члена группы **Сообщение**>**Поле "Кому" или "Копия"**	*AnyOfToCcHeaderMemberOf* *ExceptIfAnyOfToCcHeaderMemberOf*	`Addresses`	Сообщения, в которых поле **To** или **Cc** содержит получателя, являющегося членом указанной группы.	Exchange 2010 или более поздней версии

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
содержит члена этой группы				
Размер сообщения превышает или равен **Сообщение>размер больше или равен**	*MessageSizeOver* *ExceptIfMessageSizeOver*	`Size`	Сообщения, общий размер которых (сообщение и вложения) равен заданному или превышает его. В Центре администрирования Exchange указать размер можно только в килобайтах (КБ). **Примечание**. Ограничения на размер сообщений в почтовых ящиках оцениваются перед правилами потока обработки почты. Сообщение, слишком большое для почтового ящика, отклоняется до того, как правило с этим условием сможет действовать с сообщением.	Exchange 2013 или более поздней версии
Имя набора символов включаем любое из этих слов **Сообщение>имя набора символов включает любое из этих слов**	*ContentCharacterSetContainsWords* *ExceptIfContentCharacterSetContainsWords*	`CharacterSets`	Сообщения с какими-либо из указанных кодировок.	Exchange 2013 или более поздней версии

Отправитель и получатель

Развернуть таблицу

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
Отправитель приходится получателю **Отправитель и получатель>отношение**	*SenderManagementRelationship* *ExceptIfSenderManagementRelationship*	`ManagementRelationship`	Сообщения, в которых либо отправитель является менеджером получателя, либо	Exchange 2010 или более поздней версии

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
отправителя к получателю —			отправитель управляется получателем.	
сообщение пересылается между членами этих групп **Отправитель и получатель>сообщение находится между участниками этих групп**	*BetweenMemberOf1* и *BetweenMemberOf2* *ExceptIfBetweenMemberOf1* и *ExceptIfBetweenMemberOf2*	`Addresses`	Сообщения, отправляемые между участниками заданных групп.	Exchange 2010 или более поздней версии
Руководитель отправителя или получателя **Отправитель и получатель>этот человек является руководителем отправителя или получателя**.	*ManagerForEvaluatedUser* и *ManagerAddress* *ExceptIfManagerForEvaluatedUser* и *ExceptIfManagerAddress*	Первое свойство: `EvaluatedUser` Второе свойство: `Addresses`	Сообщения, отправители или получатели которых являются подчиненными указанного пользователя.	Exchange 2010 или более поздней версии
Сравнение свойства отправителя со свойством какого-либо получателя дает результат **Отправитель и получатель>свойства отправителя и получателя сравниваются как**	*ADAttributeComparisonAttribute* и *ADComparisonOperator* *ExceptIfADAttributeComparisonAttribute* и *ExceptIfADComparisonOperator*	Первое свойство: `ADAttribute` Второе свойство: `Evaluation`	Сообщения, в которых у отправителя и получателя совпадают или не совпадают значения указанного атрибута Active Directory.	Exchange 2010 или более поздней версии

Свойства сообщений

Развернуть таблицу

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
Тип сообщения **Свойства**> сообщения **включить тип сообщения**	*MessageTypeMatches* *ExceptIfMessageTypeMatches*	`MessageType`	Сообщения указанного типа. **Примечание.** Если Outlook или Outlook в Интернете настроены для пересылки сообщения, в сообщение добавляется свойство **ForwardingSmtpAddress**. Тип сообщения не изменяется на `AutoForward`.	Exchange 2010 или более поздней версии
Сообщение классифицировано как **Свойства**> сообщения	*HasClassification* *ExceptIfHasClassification*	`MessageClassification`	Сообщения с указанной классификацией. Это пользовательская классификация сообщений,	Exchange 2010 или более

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
включить эту классификацию			которую можно создать в организации с помощью командлета **New-MessageClassification**.	поздней версии
Сообщению не присвоена какая-либо классификация **Свойства**> сообщения **не включать какие-либо классификации**	*HasNoClassification* *ExceptIfHasNoClassification*	Н/д	Сообщения, у которых нет классификации.	Exchange 2010 или более поздней версии
Сообщение имеет значение вероятности нежелательной почты не менее **Свойства**> сообщения **включить SCL больше или равен**	*SCLOver* *ExceptIfSCLOver*	`SCLValue`	Сообщения, которым назначена вероятность нежелательной почты, равная указанному значению или превышающая его.	Exchange 2010 или более поздней версии
Важность сообщения имеет значение **Свойства**> сообщения **включить уровень важности**	*WithImportance* *ExceptIfWithImportance*	`Importance`	Сообщения с указанным уровнем важности.	Exchange 2010 или более поздней версии

Заголовки сообщений

> **7 Примечание**
>
> Поиск слов или текстовых шаблонов в теме или других полях заголовка в сообщении происходит *после* того, как сообщение было декодировано из метода кодирования передачи содержимого MIME, который использовался для передачи двоичного сообщения между SMTP-серверами в тексте ASCII. Нельзя использовать условия или исключения для поиска необработанных (как правило, Base64) значений темы или других полей заголовка в сообщениях.

Развернуть таблицу

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
Заголовок сообщения включает **Заголовок**> сообщения **включает любое из этих слов**	*HeaderContainsMessageHeader* и *HeaderContainsWords* *ExceptIfHeaderContainsMessageHeader* и *ExceptIfHeaderContainsWords*	Первое свойство: `MessageHeaderField` Второе свойство: `Words`	Сообщения, которые содержат указанное поле заголовка. Значение этого поля содержит указанные слова. Имя поля заголовка и значение этого поля всегда	Exchange 2010 или более поздней версии

Условие или исключение в Центре администрирования Exchange	Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
			используются вместе.	
Заголовок сообщения соответствует **Заголовок**> сообщения **соответствует этим текстовым шаблонам**	*HeaderMatchesMessageHeader* и *HeaderMatchesPatterns* *ExceptIfHeaderMatchesMessageHeader* и *ExceptIfHeaderMatchesPatterns*	Первое свойство: `MessageHeaderField` Второе свойство: `Patterns`	Сообщения, которые содержат указанное поле заголовка. Значение этого поля содержит указанные регулярные выражения. Имя поля заголовка и значение этого поля всегда используются вместе.	Exchange 2010 или более поздней версии

Условия и исключения для правил потока обработки почты на пограничных транспортных серверах

В правилах потока обработки почты на пограничных транспортных серверах доступны только некоторые из условий и исключений, доступных на серверах почтовых ящиков. На пограничных транспортных серверах недоступен Центр администрирования Exchange, поэтому управлять правилами потока обработки почты на локальном пограничном транспортном сервере можно только с помощью командной консоли Exchange. В представленной ниже таблице описываются эти условия и исключения. Типы свойств описываются в разделе Типы свойств.

Развернуть таблицу

Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
AnyOfRecipientAddressContainsWords *ExceptIfAnyOfRecipientAddressContainsWords*	`Words`	Сообщения, в которых поля **To**, **Cc** или **Bcc** содержат указанные слова. Если сообщение содержит указанного получателя, действие правила применяется (или не применяется) ко *всем* получателям сообщения. Например, сообщение отклоняется для всех получателей сообщения, а не только для указанного пользователя.	Exchange 2013 или более поздней версии
AnyOfRecipientAddressMatchesPatterns *ExceptIfAnyOfRecipientAddressMatchesPatterns*	`Patterns`	Сообщения, в которых поле **To**, **Cc** или **Bcc** содержит текстовые шаблоны, соответствующие указанным регулярным выражениям. Если сообщение содержит указанного получателя, действие правила применяется (или не применяется) ко *всем* получателям сообщения. Например, сообщение отклоняется для всех получателей сообщения, а не только для указанного пользователя.	Exchange 2013 или более поздней версии

Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
AttachmentSizeOver *ExceptIfAttachmentSizeOver*	`Size`	Сообщения, содержащие вложения, размер которых равен заданному или превышает его.	Exchange 2010 или более поздней версии
FromAddressContainsWords *ExceptIfFromAddressContainsWords*	`Words`	Сообщения, электронный адрес отправителя которых содержит указанные слова.	Exchange 2010 или более поздней версии
FromAddressMatchesPatterns *ExceptIfFromAddressMatchesPatterns*	`Patterns`	Сообщения, электронный адрес отправителя которых содержит текстовые шаблоны, соответствующие указанным регулярным выражениям.	Exchange 2010 или более поздней версии
FromScope *ExceptIfFromScope*	`UserScopeFrom`	Сообщения от внутренних или внешних отправителей.	Exchange 2010 или более поздней версии
HeaderContainsMessageHeader и *HeaderContainsWords* *ExceptIfHeaderContainsMessageHeader* и *ExceptIfHeaderContainsWords*	Первое свойство: `MessageHeaderField` Второе свойство: `Words`	Сообщения, которые содержат указанное поле заголовка. Значение этого поля содержит указанные слова. Имя поля заголовка и значение этого поля всегда используются вместе.	Exchange 2010 или более поздней версии
HeaderMatchesMessageHeader и *HeaderMatchesPatterns* *ExceptIfHeaderMatchesMessageHeader* и *ExceptIfHeaderMatchesPatterns*	Первое свойство: `MessageHeaderField` Второе свойство: `Patterns`	Сообщения, которые содержат указанное поле заголовка. Значение этого поля содержит указанные регулярные выражения. Имя поля заголовка и значение этого поля всегда используются вместе.	Exchange 2010 или более поздней версии
MessageSizeOver *ExceptIfMessageSizeOver*	`Size`	Сообщения, общий размер которых (сообщение и вложения) равен заданному или превышает его.	Exchange 2013 или более поздней версии
SCLOver *ExceptIfSCLOver*	`SCLValue`	Сообщения, которым назначена вероятность нежелательной почты, равная указанному значению или превышающая его.	Exchange 2010 или более поздней версии
SubjectContainsWords *ExceptIfSubjectContainsWords*	`Words`	Сообщения, в которых поле **Subject** содержит указанные слова.	Exchange 2010 или более поздней версии
SubjectMatchesPatterns *ExceptIfSubjectMatchesPatterns*	`Patterns`	Сообщения, в которых поле **Subject** содержит текстовые шаблоны, соответствующие указанным регулярным выражениям.	Exchange 2010 или более поздней версии

Параметры условий и исключений в командной консоли Exchange	Тип свойства	Описание	Доступен в
SubjectOrBodyContainsWords *ExceptIfSubjectOrBodyContainsWords*	`Words`	Сообщения, в которых поле **Subject** или текст содержит указанные слова.	Exchange 2010 или более поздней версии
SubjectOrBodyMatchesPatterns *ExceptIfSubjectOrBodyMatchesPatterns*	`Patterns`	Сообщения, в которых поле **Subject** или текст содержит текстовые шаблоны, соответствующие указанным регулярным выражениям.	Exchange 2010 или более поздней версии

Типы свойств

В представленной ниже таблице описываются типы свойств, используемые в условиях и исключениях.

> 7 **Примечание**
>
> Примечание. Квота запрета отправки и получения фактически определяет максимальный размер почтового ящика.

Развернуть таблицу

Тип свойства	Допустимые значения	Описание
`ADAttribute`	Выберите из встроенного списка атрибутов Active Directory	Вы можете проверка к любому из следующих атрибутов Active Directory: • **City** • **Company** • **Страна** • **CustomAttribute1 — CustomAttribute15** • **Department** • **DisplayName** • **Отправить сообщение** • **FaxNumber** • **FirstName** • **HomePhoneNumber** • **Initials** • **LastName** • **Сотрудник** • **MobileNumber** • **Примечания**. • **Office** • **OtherFaxNumber** • **OtherHomePhoneNumber** • **OtherPhoneNumber** • **PagerNumber** • **PhoneNumber** • **Pobox** • **Состояние** • **Улице** • **Title** • **UserLogonName** • **Почтовый индекс** В EAC, чтобы указать несколько слов или текстовых шаблонов для

Тип свойства	Допустимые значения	Описание
		одного атрибута, разделите значения запятыми. Например, значение `San Francisco,Palo Alto` атрибута **City** ищет значение "City равно Сан-Франциско" или City равно Пало-Альто". В командной консоли Exchange используйте синтаксис `"AttributeName1:Value1,Value 2 with spaces,Value3...","AttributeName2:Word4,Value 5 with spaces,Value6..."`, где `Value` — это слово или текстовый шаблон, который требуется сопоставить. Например, `"City:San Francisco,Palo Alto"` или `"City:San Francisco,Palo Alto"`, `"Department:Sales,Finance"`. Если указано несколько атрибутов (или несколько значений для одного атрибута), используется оператор **or**. Не используйте значения с пробелами в начале или в конце. Для атрибута **Country** требуется двухбуквенный код страны ISO 3166-1 (например, DE для Германии). Дополнительные сведения см. в разделе Коды стран — ISO 3166.
`Addresses`	Получатели в Exchange	В зависимости от характера условия или исключения вы можете указать любой объект с поддержкой почты в организации (например, условия, связанные с получателем) или ограничиться определенным типом объекта (например, группы для условий членства в группах). Кроме того, условие или исключение может потребовать одного значения или разрешить несколько значений. В командной консоли Exchange разделите несколько значений запятыми. **Примечание.** Это условие или исключение не учитывает сообщения, отправляемые на прокси-адреса получателей. Он соответствует только сообщениям, отправленным основной адрес электронной почты получателя.
`CharacterSets`	Массив имен кодировок	Одна или несколько кодировок содержимого, присутствующих в сообщении. Например: • `Arabic/iso-8859-6` • `Chinese/big5` • `Chinese/euc-cn` • `Chinese/euc-tw` • `Chinese/gb2312` • `Chinese/iso-2022-cn` • `Cyrillic/iso-8859-5` • `Cyrillic/koi8-r` • `Cyrillic/windows-1251` • `Greek/iso-8859-7` • `Hebrew/iso-8859-8` • `Japanese/euc-jp` • `Japanese/iso-022-jp` • `Japanese/shift-jis` • `Korean/euc-kr` • `Korean/johab` • `Korean/ks_c_5601-1987` • `Turkish/windows-1254` • `Turkish/iso-8859-9` • `Vietnamese/tcvn`

Тип свойства	Допустимые значения	Описание
`DocumentProperties`	Массив настраиваемых или встроенных свойств документа	Указывает встроенное или настраиваемое свойство документа. Встроенные свойства документов: • **Влияние на бизнес**; • **Комплиантность** • **Конфиденциальность** • **Department** • **Влияние** • **Интеллектуальная собственность**; • **Личные сведения**; • **Персональные данные**; • **Личное использование**; • **Необходимое разрешение**; • **PHI** • **PII** • **Проект** • **Защищенная медицинская информация**. Каждое свойство содержит одно значение. При указании нескольких свойств используется оператор **или** . Командная консоль Exchange использует синтаксис : `"<PropertyName1>:<PropertyValue1>","<PropertyName2>:<PropertyValue2>"`, где `<PropertyValue>` — это слово, которое нужно сопоставить. Синтаксис для этого параметра — `"PropertyName:Word"`. Чтобы указать несколько свойств или несколько слов для одного свойства, используйте следующий синтаксис: `"PropertyName1:Word1,Phrase with spaces,word2...","PropertyName2:Word3,Phrase with spaces,word4...`. Не добавляйте пробелы в начале и в конце. Если указано несколько свойств (или несколько значений для одного свойства), используется оператор **or**.
`DomainName`	Массив доменов SMTP	Например, `contoso.com` или `eu.contoso.com`. В командной консоли Exchange можно указать несколько доменов, разделенных запятыми.
`EvaluatedUser`	Одно значение: **Sender** или **Recipient**	Указывает, чьего руководителя ищет правило: отправителя или получателя.
`Evaluation`	Одно значение **Равно** или **Не равно** (`NotEqual`)	При сравнении атрибута Active Directory отправителя и получателей этот оператор указывает, должны ли совпадать значения.
`Importance`	Одно значение: **Низкий** (Low), **Обычный** (Normal) или **Высокий** (High)	Уровень важности, назначенный сообщению отправителем в Outlook или Outlook в Интернете.
`IPAddressRanges`	Массив IP-адресов или диапазонов адресов	Введите IPv4-адреса, используя следующий синтаксис: • **Один IP-адрес**: например. `192.168.1.1` • **Диапазон IP-адресов**: например, `192.168.0.1-192.168.0.254`. • **Диапазон IP-адресов бесклассовой междоменной маршрутизации (CIDR):** например, `192.168.0.1/25`. В командной консоли Exchange можно указать несколько IP-адресов или диапазонов, разделенных запятыми.

Тип свойства	Допустимые значения	Описание
`ManagementRelationship`	Одно значение **Manager** или **Direct report**(`DirectReport`)	Задает отношение между отправителем и любым получателем. Правило проверяет атрибут **Manager** в Active Directory, чтобы узнать, является ли отправитель руководителем или подчиненным получателя.
`MessageClassification`	Одна классификация сообщения	В центре администрирования EAC вы выбираете из списка созданных классификаций сообщений. В командной консоли Exchange для идентификации классификации сообщений используется командлет **Get-MessageClassification** . Например, выполните следующую команду, чтобы найти сообщения с классификацией `Company Internal` и добавить к теме сообщения значение `CompanyInternal`: `New-TransportRule "Rule Name" -HasClassification @(Get-MessageClassification "Company Internal").Identity -PrependSubject "CompanyInternal"`
`MessageHeaderField`	Одиночная строка	Задает имя поля заголовка. Имя поля заголовка всегда связано со значением в поле заголовка (совпадение слов или текста). *Заголовок сообщения* — это коллекция обязательных и необязательных полей заголовка для сообщения. Примеры полей заголовков: **To**, **From**, **Received** и **Content-Type**. Официальные поля заголовков определены в стандарте RFC 5322. Неофициальные поля заголовков начинаются с **X-** и называются *X-заголовками*.
`MessageType`	Одно значение типа сообщения	Задает один из следующих типов сообщений: • **Автоматический ответ** (`OOF`) • **Автоматическая пересылка** (`AutoForward`) • **С шифрованием** • **Календаря** • **Управление разрешениями** (`PermissionControlled`) • **Голосовая почта** • **Подписал** • **Запрос на утверждение** (`ApprovalRequest`) • **Уведомление о прочтении** (`ReadReceipt`) **Примечание.** Если Outlook или Outlook в Интернете настроены для пересылки сообщения, в сообщение добавляется свойство **ForwardingSmtpAddress**. Тип сообщения не изменяется на `AutoForward`.
`Patterns`	Массив регулярных выражений	Указывает одно или несколько регулярных выражений, используемых для идентификации текстовых шаблонов в значениях. Дополнительные сведения см. в разделе Синтаксис регулярных выражений. В командной консоли Exchange вы указываете несколько регулярных выражений, разделенных запятыми, и заключаете каждое регулярное выражение в кавычки ().
`SCLValue`	Одно из указанных ниже значений: • **Обход фильтрации нежелательной почты** (`-1`) • Целые числа от 0 до 9.	Указывает вероятность нежелательной почты, назначенную сообщению. Чем больше ее значение, тем вероятнее, что сообщение окажется спамом.

Тип свойства	Допустимые значения	Описание
`SensitiveInformationTypes`	Массив типов конфиденциальной информации	Задает один или несколько типов конфиденциальной информации, определенных в организации. Список встроенных типов конфиденциальной информации см. в разделе Типы конфиденциальной информации в Exchange Server. В командной консоли Exchange используйте синтаксис `@{<SensitiveInformationType1>},@{<SensitiveInformationType2>},...`. Например, чтобы найти содержимое, содержащее по крайней мере два номера кредитов карта и по крайней мере один номер маршрутизации ABA, используйте значение `@{Name="Credit Card Number"; minCount="2"},@{Name="ABA Routing Number"; minCount="1"}`.
`Size`	Одно значение размера	Задает размер вложения или всего сообщения. В Центре администрирования Exchange указать размер можно только в килобайтах (КБ). В командной консоли Exchange при вводе значения укажите значение с помощью одной из следующих единиц: • `B` (байт) • `KB` (килобайты) • `MB` (мегабайты) • `GB` (гигабайт) Например, `20MB`. TB (терабайт)
`UserScopeFrom`	Одно значение **Внутри организации** (`InOrganization`) или **Вне организации** (`NotInOrganization`)	Считается, что отправитель находится в организации, если выполняются следующие условия: • Отправитель — это почтовый ящик, почтовый пользователь, группа или общедоступная папка с поддержкой почты, которая существует в Active Directory организации. • Адрес электронной почты отправителя находится в принятом домене, который настроен в качестве доверенного домена или домен внутренней ретрансляции *и* сообщение было отправлено или получено через подключение, прошедшее проверку подлинности. Дополнительные сведения о принятых доменах см. в разделе Принятые домены в Exchange Server. Отправитель считается вне организации, если выполняется одно из следующих условий: • Адрес электронной почты отправителя не находится в принятом домене. • Адрес электронной почты отправителя находится в принятом домене, настроенном как домен внешнего ретранслятора. **Примечание.** Чтобы определить, считаются ли почтовые контакты внутри организации или за ее пределами, адрес отправителя сравнивается с принятыми доменами организации.
`UserScopeTo`	Одно из указанных ниже значений: • **Внутри организации** (`InOrganization`) • **Вне организации** (`NotInOrganization`)	Получатель считается внутри организации, если выполняется одно из следующих условий: • Получатель — это почтовый ящик, почтовый пользователь, группа или общедоступная папка с поддержкой почты, которая существует в Active Directory организации. • Адрес электронной почты получателя находится в принятом домене, который не настроен как домен внешнего

Тип свойства	Допустимые значения	Описание
	• **Во внешней партнерской организации** (`ExternalPartner`) • **Во внешней организации, не относящейся к партнерам** (`ExternalNonPartner`)	ретранслятора , *и* сообщение было отправлено или получено через подключение, прошедшее проверку подлинности. Получатель считается вне организации, если выполняется одно из следующих условий: • Адрес электронной почты получателя не находится в принятом домене, и в то же время адрес электронной почты получателя не находится в удаленном домене, для которого свойству `IsInternal` присвоено значение true. • Электронный адрес получателя находится на обслуживаемом домене, настроенном в качестве домена внешней ретрансляции. Внешние партнерские организации — это внешние домены, на которых параметры безопасности домена (взаимная проверка подлинности TLS) настроены на отправку почты. Внешние не партнерские организации — это все остальные внешние домены, которые не считаются партнерскими доменами.
`Words`	Массив строк	Указывает одно или несколько слов для поиска. Слова не чувствительны к регистру и могут быть окружены пробелами и знаками препинания. Подстановочные знаки и частичные совпадения не поддерживаются. Например, по запросу «contoso» будет найден текст « Contoso.». Тем не менее, если текст окружен другими символами, то соответствия не будет. Например, "contoso" не соответствует следующим значениям: • Acontoso • Contosoa • Acontosob Звездочка (*) обрабатывается как литеральный символ и не используется в качестве подстановочного знака.

Дополнительные сведения

Действия правил потока обработки почты в Exchange Server

Условия и исключения (предикаты) правил для потока обработки почты в Exchange Online

Действия правил потока обработки почты в Exchange Server

Статья • 04.04.2023

Действия в правилах потока обработки почты (их еще зовут правилами транспорта) указывают, что делать с сообщениями, которые соответствуют условиям правила. Например, вы можете создать правило, которое пересылает сообщения от определенных отправителей модератору либо добавляет оговорку или персонализированную подпись ко всем исходящим сообщениям.

Действия обычно требуют дополнительных свойств. Например, если правило перенаправляет сообщение, необходимо указать, куда следует перенаправить сообщение. Некоторые действия имеют несколько доступных или обязательных свойств. Например, когда правило добавляет поле заголовка в заголовок сообщения, необходимо указать имя и значение заголовка. Когда правило добавляет в сообщения заявление об отказе от ответственности, необходимо указать текст заявления об отказе, но вы также можете указать, куда вставить текст или что делать, если заявление об отказе не удается добавить в сообщение. Как правило, в правиле можно настроить несколько действий, но некоторые действия являются монопольными. Например, одно правило не может отклонить и перенаправить одно и то же сообщение.

Дополнительные сведения о правилах потока обработки почты в Exchange Server, включая обработку нескольких действий, см. в статье Правила потока обработки почты в Exchange Server.

Дополнительные сведения об условиях и исключениях в правилах потока обработки почты см. в статье Условия и исключения (предикаты) правил потока обработки почты в Exchange Server.

Действия для правил потока обработки почты на серверах почтовых ящиков

В представленной ниже таблице описаны действия, доступные для правил потока обработки почты на серверах почтовых ящиков. Допустимые значения для каждого свойства описаны в разделе Значения свойств[Значения свойств].

Примечания.

- После выбора действия в Центре администрирования Exchange (EAC) значение, которое в конечном итоге отображается в поле **Выполнение следующего действия** , часто отличается от выбранного пути щелчка. Кроме того, при создании новых правил иногда (в зависимости от выбранных вариантов) можно выбрать короткое имя действия из шаблона (отфильтрованный список действий) вместо того, чтобы следовать полному пути щелчка. Короткие имена и значения пути полного щелчка отображаются в столбце EAC таблицы.
- Названия некоторых действий, которые возвращает командлет **Get-TransportRuleAction**, отличаются от имен соответствующих параметров, а для действия может потребоваться указать несколько параметров.

Действие в Центре администрирования Exchange	Параметр action в командной консоли Exchange	Свойство	Описание	Доступен в
Переслать сообщение для утверждения этим пользователям **Пересылка сообщения для утверждения>этим людям**	*ModerateMessageByUser*	`Addresses`	Переадресует определенным модераторам сообщение в приложении к запросу об утверждении. Дополнительные сведения см. в разделе Общие сценарии утверждения сообщений. В качестве модератора невозможно указать группу рассылки.	Exchange 2010 или более поздней версии

Действие в Центре администрирования Exchange	Параметр action в командной консоли Exchange	Свойство	Описание	Доступен в
Переслать сообщение для утверждения диспетчеру отправителя **Пересылка сообщения для утверждения>диспетчеру отправителя**	*ModerateMessageByManager*	н/д	Пересылает сообщение для утверждения руководителю отправителя. Это действие работает только в том случае, если атрибут **диспетчера** отправителя определен в Active Directory. В противном случае сообщение доставляется получателям без модерации.	Exchange 2010 или более поздней версии
Перенаправить сообщение этим получателям **Перенаправление сообщения на>эти получатели**	*RedirectMessageTo*	`Addresses`	Перенаправляет сообщение указанным получателям. Сообщение не доставлено исходным получателям, при этом никакие уведомления не отправляются ни отправителю, ни исходным получателям.	Exchange 2010 или более поздней версии
Отклонить сообщение с пояснением **Блокировка сообщения>отклонить сообщение и включить объяснение**	*RejectMessageReasonText*	`String`	Возвращает сообщение отправителю в отчете о недоставке, или сообщении возврата, с указанием причины отклонения в заданном тексте. Адресат не получает ни исходного сообщения, ни уведомления. Используемый по умолчанию расширенный код состояния — `5.7.1`. При создании или изменении правила в командной консоли Exchange можно указать код DSN с помощью параметра *RejectMessageEnhancedStatusCode* .	Exchange 2010 или более поздней версии
Отклонить сообщение с расширенным кодом состояния **Блокировка сообщения>отклонить сообщение с расширенным кодом состояния**	*RejectMessageEnhancedStatusCode*	`DSNEnhancedStatusCode`	Возвращает сообщение отправителю в отчете о недоставке с указанным расширенным кодом уведомления о доставке (DSN). Адресат не получает ни исходного сообщения, ни уведомления. Допустимые коды DSN : `5.7.1` или `5.7.900` через `5.7.999`. Используемый текст причины по умолчанию — `Delivery not authorized, message refused`. При создании или изменении правила в командной консоли Exchange можно указать текст причины отклонения с помощью параметра *RejectMessageReasonText* .	Exchange 2010 или более поздней версии

Действие в Центре администрирования Exchange	Параметр action в командной консоли Exchange	Свойство	Описание	Доступен в
Удалить сообщение, не отправляя уведомлений **Блокировка сообщения>удалить сообщение без уведомления**	*DeleteMessage*	н/д	Удаляет сообщение, не отправляя уведомление ни получателю, ни отправителю.	Exchange 2010 или более поздней версии
Добавлять получателей в поле "СК" **Добавление получателей>в поле СК**	*BlindCopyTo*	`Addresses`	Добавляет одного или нескольких получателей в поле **Bcc** сообщения. Исходные получатели не уведомляются, и им не видны дополнительные адреса.	Exchange 2010 или более поздней версии
Добавлять получателей в поле "Кому" **Добавление получателей>в поле To**	*AddToRecipients*	`Addresses`	Добавляет одного или нескольких получателей в поле **To** сообщения. Дополнительные адреса видны исходным получателям.	Exchange 2010 или более поздней версии
Добавлять получателей в поле "Копия" **Добавление получателей>в поле Копия**	*CopyTo*	`Addresses`	Добавляет одного или нескольких получателей в поле **Cc** сообщения. Добавленный адрес виден для исходных получателей.	Exchange 2010 или более поздней версии
Добавить руководителя отправителя в качестве получателя **Добавление получателей>добавление диспетчера отправителя в качестве получателя**	*AddManagerAsRecipientType*	`AddedManagerAction`	Добавляет руководителя отправителя к сообщению в качестве получателя указанного типа (**To**, **Cc**, **Bcc**) или перенаправляет сообщение руководителю отправителя, не уведомляя ни отправителя, ни получателя. Это действие работает только в том случае, если атрибут **диспетчера** отправителя определен в Active Directory.	Exchange 2010 или более поздней версии
Добавить в сообщение заявление об отказе **Применение заявления об отказе от ответственности к сообщению>добавление заявления об отказе от ответственности**	*ApplyHtmlDisclaimerText* *ApplyHtmlDisclaimerFallbackAction* *ApplyHtmlDisclaimerTextLocation*	Первое свойство: `DisclaimerText` Второе свойство: `DisclaimerFallbackAction` Третье свойство (только командная оболочка Exchange): `DisclaimerTextLocation`	Добавляет указанную оговорку в формате HTML в конец сообщения. При создании или изменении правила в командной консоли Exchange используйте параметр *ApplyHtmlDisclaimerTextLocation* со значением `Append`.	Exchange 2010 или более поздней версии
Предварить заявлением об отказе **Применение заявления об отказе от ответственности к сообщению>добавление заявления об отказе от ответственности**	*ApplyHtmlDisclaimerText* *ApplyHtmlDisclaimerFallbackAction* *ApplyHtmlDisclaimerTextLocation*	Первое свойство: `DisclaimerText` Второе свойство: `DisclaimerFallbackAction` Третье свойство (только командная оболочка Exchange): `DisclaimerTextLocation`	Добавляет указанную оговорку в формате HTML в начало сообщения. При создании или изменении правила в командной консоли Exchange используйте параметр *ApplyHtmlDisclaimerTextLocation* со значением `Prepend`.	Exchange 2010 или более поздней версии

Действие в Центре администрирования Exchange	Параметр action в командной консоли Exchange	Свойство	Описание	Доступен в
Удалить этот заголовок **Изменение свойств**> сообщения **удаление заголовка сообщения**	*RemoveHeader*	`MessageHeaderField`	Удаляет указанное поле из заголовка сообщения.	Exchange 2010 или более поздней версии
Установить для заголовка сообщения значение **Изменение свойств**> сообщения **Установка заголовка сообщения**	*SetHeaderName* *SetHeaderValue*	Первое свойство: `MessageHeaderField` Второе свойство: `String`	Добавляет или изменяет указанное поле в заголовке сообщения и устанавливает для этого поля заданное значение.	Exchange 2010 или более поздней версии
Применить классификацию сообщений **Изменение свойств**> сообщения **применение классификации сообщений**	*ApplyClassification*	`MessageClassification`	Применяет к сообщению указанную классификацию сообщений.	Exchange 2010 или более поздней версии
Задать значение для вероятности нежелательной почты **Изменение свойств**> сообщения **установка уровня достоверности нежелательной почты (SCL)**	*SetSCL*	`SCLValue`	Задает указанное значение вероятности нежелательной почты для сообщения.	Exchange 2010 или более поздней версии
Применить защиту прав к сообщению с **Изменение безопасности**> сообщений **применение защиты прав**	*ApplyRightsProtectionTemplate*	`RMSTemplate`	Применяет к сообщению указанный шаблон службы управления правами (RMS). Для каждого почтового ящика RMS требуются клиентские лицензии (CAL) Exchange Enterprise. Дополнительные сведения о клиентских лицензиях см. в разделе Часто задаваемые вопросы о лицензировании Exchange.	Exchange 2010 или более поздней версии
Требовать шифрование TLS **Изменение безопасности**> сообщений **требовать шифрование TLS**	*RouteMessageOutboundRequireTls*	`n/a`	Принудительно маршрутизирует исходящие сообщения с применением подключения, зашифрованного с помощью TLS.	Exchange 2013 или более поздней версии

Действие в Центре администрирования Exchange	Параметр action в командной консоли Exchange	Свойство	Описание	Доступен в
Добавить в начало темы сообщения	*PrependSubject*	`String`	Добавляет указанный текст в начало поля **Subject** сообщения. Рекомендуем добавить пробел или двоеточие (:) в конце указанного текста, чтобы отделить его от исходного текста темы. Чтобы предотвратить добавление одной и той же строки в сообщения, которые уже содержат текст в теме (например, ответы), добавьте в правило исключение **Тема включает** (*ExceptIfSubjectContainsWords*).	Exchange 2010 или более поздней версии
Уведомить отправителя подсказкой политики	*NotifySender* *RejectMessageReasonText* *RejectMessageEnhancedStatusCode* (только командная консоль Exchange)	Первое свойство: `NotifySenderType` Второе свойство: `String` Третье свойство (только командная оболочка Exchange): `DSNEnhancedStatusCode`	Уведомляет отправителя или блокирует сообщение, если оно соответствует политике защиты от потери данных. При использовании этого действия необходимо использовать условие **Сообщение содержит конфиденциальную информацию** (*MessageContainsDataClassification*). При создании или изменении правила в командной консоли Exchange параметр *RejectMessageReasonText* является необязательным. Если этот параметр не используется, используется текст `Delivery not authorized, message refused` по умолчанию. В командной консоли Exchange можно также использовать параметр *RejectMessageEnhancedStatusCode* , чтобы указать расширенный код состояния. Если этот параметр не используется, используется код `5.7.1` расширенного состояния по умолчанию. Это действие ограничивает остальные условия, исключения и действия, которые можно настроить для правила.	Exchange 2013 или более поздней версии
Создать отчет об инциденте и отправить его	*GenerateIncidentReport* *IncidentReportContent*	Первое свойство: `Addresses` Второе свойство: `IncidentReportContent`	Отправляет указанным получателям отчет об инциденте с заданным содержимым. Отчет об инциденте создается для сообщений, которые соответствуют политикам защиты от потери данных, используемым в организации.	Exchange 2013 или более поздней версии

Действие в Центре администрирования Exchange	Параметр action в командной консоли Exchange	Свойство	Описание	Доступен в
Уведомление получателя сообщением	*GenerateNotification*	`NotificationMessageText`	Задает текст, HTML-теги и ключевые слова, которые необходимо включить в сообщения уведомления, отправляемые получателям. Например, вы можете сообщить получателям, что сообщение было отклонено правилом или отмечено как спам и доставлено в папку "Нежелательная почта".	Exchange 2016 или более поздней версии
Свойства этого правила . >**Аудит этого правила с уровнем серьезности**	*SetAuditSeverity*	`AuditSeverityLevel`	Указывает, следует ли: • запретить создание отчета об инциденте и соответствующей записи в журнале отслеживания сообщений; • создать отчет об инциденте и соответствующую запись в журнале отслеживания сообщений с указанной степенью серьезности (низкой, средней или высокой).	Exchange 2013 или более поздней версии
Свойства этого раздела> правила **Остановить обработку дополнительных правил** **Дополнительные параметры**>**Свойства этого раздела**> правила **Остановить обработку дополнительных правил**	*StopRuleProcessing*	н/д	Указывает, что после применения правила к сообщению его не обрабатывают другие правила.	Exchange 2013 или более поздней версии

Действия для правил потока обработки почты на пограничных транспортных серверах

Небольшое подмножество действий, доступных на серверах почтовых ящиков, также доступно на пограничных транспортных серверах, но есть и некоторые действия, доступные только на пограничных транспортных серверах. На пограничных транспортных серверах недоступен Центр администрирования Exchange, поэтому управлять правилами потока обработки почты на локальном пограничном транспортном сервере можно только с помощью командной консоли Exchange. Действия описаны в следующей таблице. Типы свойств описаны в разделе Значения свойств .

Параметр action в командной консоли Exchange	Свойство	Описание	Поддерживаемые серверы	Доступен в
AddToRecipients	`Addresses`	Добавляет одного или нескольких получателей в поле **To** сообщения. Дополнительные адреса видны исходным получателям.	Серверы почтовых ящиков и пограничные транспортные серверы	Exchange 2010 или более поздней версии
BlindCopyTo	`Addresses`	Добавляет одного или нескольких получателей в поле **Bcc** сообщения. Исходные получатели не уведомляются, и им не видны дополнительные адреса.	Серверы почтовых ящиков и пограничные транспортные серверы	Exchange 2010 или более поздней версии

Параметр action в командной консоли Exchange	Свойство	Описание	Поддерживаемые серверы	Доступен в
CopyTo	`Addresses`	Добавляет одного или нескольких получателей в поле **Cc** сообщения. Дополнительный адрес виден исходным получателям.	Серверы почтовых ящиков и пограничные транспортные серверы	Exchange 2010 или более поздней версии
DeleteMessage	н/д	Удаляет сообщение, не отправляя уведомление ни получателю, ни отправителю.	Серверы почтовых ящиков и пограничные транспортные серверы	Exchange 2010 или более поздней версии
Disconnect	н/д	Разрывает SMTP-соединение между сервером-отправителем и пограничным транспортным сервером, при этом отчет о недоставке не создается.	Только пограничные транспортные серверы	Exchange 2010 или более поздней версии
LogEventText	`String`	Создает событие с указанным текстом в журнале приложений на локальном пограничном транспортом сервере. Запись содержит следующие сведения: • **Уровень**: `Information` • **Источник**: `MSExchange Messaging Policies` • **Идентификатор события**: `4000` • **Категория задачи**: `Rules` • **EventData**: `The following message is logged by an action in the rules: <text you specify>.`	Только пограничные транспортные серверы	Exchange 2010 или более поздней версии
PrependSubject	`String`	Добавляет указанный текст в начало поля **Subject** сообщения. Рекомендуем добавить пробел или двоеточие (:) в конце указанного текста, чтобы отделить его от исходной темы.	Серверы почтовых ящиков и пограничные транспортные серверы	Exchange 2010 или более поздней версии
Карантин	н/д	Доставляет сообщение в почтовый ящик карантина, определенный в конфигурации фильтрации содержимого на пограничном транспортном сервере. Дополнительные сведения см. в разделе Настройка почтового ящика карантина нежелательной почты. Если почтовый ящик карантина не настроен, сообщение возвращается отправителю в отчете о недоставке.	Только пограничные транспортные серверы	Exchange 2010 или более поздней версии
RedirectMessageTo	`Addresses`	Перенаправляет сообщение указанным получателям. Сообщение не доставлено исходным получателям, при этом никакие уведомления не отправляются ни отправителю, ни исходным получателям.	Серверы почтовых ящиков и пограничные транспортные серверы	Exchange 2010 или более поздней версии
RemoveHeader	`MessageHeaderField`	Удаляет указанное поле из заголовка сообщения.	Серверы почтовых ящиков и пограничные транспортные серверы	Exchange 2010 или более поздней версии

Параметр action в командной консоли Exchange	Свойство	Описание	Поддерживаемые серверы	Доступен в
SetHeaderName *SetHeaderValue*	Первое свойство: `MessageHeaderField` Второе свойство: `String`	Добавляет или изменяет указанное поле в заголовке сообщения и устанавливает для этого поля заданное значение.	Серверы почтовых ящиков и пограничные транспортные серверы	Exchange 2010 или более поздней версии
SetSCL	`SCLValue`	Задает указанное значение вероятности нежелательной почты для сообщения.	Серверы почтовых ящиков и пограничные транспортные серверы	Exchange 2010 или более поздней версии
SmtpRejectMessageRejectText *SmtpRejectMessageRejectStatusCode*	Первое свойство: `String` Второе свойство: `SMTPStatusCode`	Разрывает SMTP-соединение между сервером-отправителем и пограничным транспортным сервером, при этом добавляется указанный код состояния SMTP и указанный текст с описанием причины отклонения. Адресат не получает ни исходного сообщения, ни уведомления. Допустимыми значениями для кода состояния SMTP являются целые числа от до `400` `500` , как определено в RFC 3463. Если указать текст отклонения без указания кода состояния SMTP, используется код `550` по умолчанию. Если указать код состояния SMTP без указания текста отклонения, используемым текстом будет `Delivery not authorized, message refused`.	Только пограничные транспортные серверы	Exchange 2010 или более поздней версии
StopRuleProcessing	н/д	Указывает, что после применения правила к сообщению его не обрабатывают другие правила.	Серверы почтовых ящиков и пограничные транспортные серверы	Exchange 2013 или более поздней версии

Значения свойств

В приведенной ниже таблице представлены значения свойств, которые можно указать для действий в правилах потока обработки почты.

Свойство	Допустимые значения	Описание
`AddedManagerAction`	Одно из указанных ниже значений: • **To** • **Cc** • **Bcc** • **Redirect**	Определяет, как указывать руководителя отправителя в сообщениях. Если выбрано значение **Кому**, **Копия** или **СК**, то руководитель отправителя добавляется в качестве получателя в указанном поле. Если выбрано значение **Перенаправить**, сообщение доставляется только руководителю отправителя, а отправитель и получатель не получают уведомлений. Это действие работает только в том случае, если атрибут **диспетчера** отправителя определен в Active Directory.

Свойство	Допустимые значения	Описание
`Addresses`	Получатели в Exchange	В зависимости от нужного действия, в организации можно указать либо любой объект, поддерживающий почту, либо только объект определенного типа. Как правило, вы можете выбрать нескольких получателей, но отчет об инциденте можно отправить только одному из них.
`AuditSeverityLevel`	Одно из указанных ниже значений: • Снимите **флажок Аудит этого правила с уровнем серьезности** или выберите **Аудит этого правила с уровнем серьезности** со значением **Не указано** (`DoNotAudit`). • **Низкая** • **Средний** • **Высокий**	Значения **Низкая**, **Средняя** и **Высокая** задают степень серьезности, назначаемой отчету об инциденте и соответствующей записи в журнале отслеживания сообщений. Другое значение запрещает создание отчета об инциденте и добавление соответствующей записи в журнал отслеживания сообщений.
`DisclaimerFallbackAction`	Одно из указанных ниже значений: • **Wrap** • **Ignore** • **Reject**	Указывает действие на случай, если к сообщению не удастся добавить оговорку. В некоторых случаях содержимое сообщения не удается изменить (например, если сообщение зашифровано). Ниже указаны доступные резервные действия. • **Обертывание**. Исходное сообщение упаковывается в новый конверт сообщения, а текст заявления об отказе вставляется в новое сообщение. Это значение используется по умолчанию. ◦ Последующие правила потока обработки почты применяются к конверту нового сообщения, а не к исходному сообщению. Поэтому настройте эти правила с более низким приоритетом, чем другие правила. ◦ Если исходное сообщение невозможно перенести в конверт нового сообщения, то исходное сообщение не доставляется. Оно возвращается отправителю в отчете о недоставке. • **Игнорировать**: правило игнорируется, и сообщение доставляется без заявления об отказе от ответственности. • **Отклонить**: сообщение возвращается отправителю в отчете о недоставке.
`DisclaimerText`	Строка HTML	Задает текст оговорки, который может включать HTML-теги, встроенные теги каскадной таблицы стилей (CSS) и изображения, указанные с помощью тега IMG. Максимальная длина (включая теги) составляет 5000 символов.
`DisclaimerTextLocation`	Одно значение: `Append` или `Prepend`	В командной консоли Exchange *используется applyHtmlDisclaimerTextLocation* , чтобы указать расположение текста заявления об отказе в сообщении. `Append`: добавьте заявление об отказе в конец текста сообщения. Это значение используется по умолчанию. `Prepend`: добавьте заявление об отказе в начале текста сообщения.

Свойство	Допустимые значения	Описание
`DSNEnhancedStatusCode`	Одно значение кода DSN: • `5.7.1` • `5.7.900`–`5.7.999`	Задает используемый код DSN. Вы можете создавать собственные уведомления о доставке с помощью командлета **New-SystemMessage**. Если вы не указываете текст причины отклонения вместе с кодом DSN, используемый текст причины по умолчанию — `Delivery not authorized, message refused`. При создании или изменении правила в командной консоли Exchange можно указать текст причины отклонения с помощью параметра *RejectMessageReasonText* .

Свойство	Допустимые значения	Описание
`IncidentReportContent`	Одно или несколько из следующих значений: • **Sender** • **Получатели** • **Тема** • **Получатели cc'd** (`Cc`) • **Получатели СК** (`Bcc`) • **Серьезность** • **Сведения о переопределении отправителя** (`Override`) • **Правила сопоставления** (`RuleDetections`) • **Ложноположительные отчеты** (`FalsePositive`) • **Обнаруженные классификации данных** (`DataClassifications`) • **Совпадающее содержимое** (`IdMatch`) • **Исходная почта** (`AttachOriginalMail`)	Задает свойства исходного сообщения, которые необходимо включить в отчет об инциденте. Вы можете указать любое сочетание этих свойств. Помимо указанных свойств, всегда добавляется идентификатор сообщения. Ниже перечислены доступные свойства. **Sender**: отправитель исходного сообщения. **Получатели**, **получатели cc'd** и **получатели СК**: все получатели сообщения или только получатели в полях **Копия** или **СК** . Для каждого свойства в отчет об инциденте включаются только первые 10 получателей. **Тема**: поле **Тема** исходного сообщения. **Серьезность. Серьезность** аудита серьезности активированного правила. Журналы отслеживания сообщений включают все уровни серьезности аудита и могут фильтроваться по серьезности аудита. Если в EAC снимите флажок **Аудит этого правила с уровнем серьезности** (в командной консоли Exchange значение `DoNotAudit` параметра *SetAuditSeverity*), совпадения с правилами не будут отображаться в отчетах о правилах. Если сообщение обработано несколькими правилами, в отчет об инциденте включаются данные о наивысшей степени серьезности. **Сведения о переопределении отправителя**. Переопределение, если отправитель решил переопределить подсказку политики. Если отправитель указал обоснование, также включаются первые 100 символов текста с этим обоснованием. **Правила сопоставления**. Список правил, активированных сообщением. **Ложноположительные отчеты**: ложноположительный результат, если отправитель помечает сообщение как ложноположительный результат для подсказки политики. **Обнаруженные классификации данных**. Список типов конфиденциальной информации, обнаруженных в сообщении. **Совпадающее содержимое**. Обнаруженный тип конфиденциальной информации, точно совпадающее содержимое сообщения и 150 символов до и после сопоставления конфиденциальной информации. **Исходная почта**: все сообщение, активировавшее правило, прикрепляется к отчету об инциденте. В командной консоли Exchange укажите несколько значений, разделенных запятыми.
`MessageClassification`	Объект классификации одиночного сообщения	В Центре администрирования Exchange нужно выбрать в списке одну из доступных классификаций сообщений. В командной консоли Exchange используйте командлет **Get-MessageClassification** , чтобы просмотреть доступные объекты классификации сообщений.

Свойство	Допустимые значения	Описание
`MessageHeaderField`	Одиночная строка	Указывает добавляемое, удаляемое или изменяемое поле SMTP-заголовка сообщения. *Заголовок сообщения* — это коллекция обязательных и необязательных полей заголовка для сообщения. Примеры полей заголовков: **To**, **From**, **Received** и **Content-Type**. Официальные поля заголовков определены в стандарте RFC 5322. Неофициальные поля заголовков начинаются с **X-** и называются *X-заголовками*.
`NotificationMessageText`	Любое сочетание обычного текста, HTML-тегов и ключевых слов	Задает текст, который нужно добавить в сообщение уведомления для получателей. Помимо обычного текста и HTML-тегов, вы можете указать следующие ключевые слова, в которых используются значения из исходного сообщения: • `%%From%%` • `%%To%%` • `%%Cc%%` • `%%Subject%%` • `%%Headers%%` • `%%MessageDate%%`
`NotifySenderType`	Одно из указанных ниже значений: • **Уведомление отправителя, но разрешение на отправку** (`NotifyOnly`) • **Блокировать сообщение** (`RejectMessage`) • **Блокировать сообщение, если оно не является ложноположительным** (`RejectUnlessFalsePositiveOverride`) • **Заблокируйте сообщение, но разрешите отправителю переопределить и отправить** (`RejectUnlessSilentOverride`) • **Заблокируйте сообщение, но разрешите отправителю переопределить бизнес-обоснование и отправить** (`RejectUnlessExplicitOverride`)	Задает тип подсказки политики, которую получает отправитель, если сообщение нарушает политику защиты от потери данных. Эти параметры перечислены в приведенном ниже списке. • **Уведомление отправителя, но разрешение на отправку**: отправитель получает уведомление, но сообщение доставляется в обычном режиме. • **Блокировать сообщение**: сообщение отклоняется, а отправитель получает уведомление. • **Блокировать сообщение, если оно не является ложноположительным**. Сообщение отклоняется, если отправитель не помечает его как ложноположительное. • **Заблокировать сообщение, но разрешить отправителю переопределить и отправить**: сообщение отклоняется, если отправитель не решил переопределить ограничение политики. • **Блокировать сообщение, но разрешать отправителю переопределять бизнес-обоснование и отправлять**. Это значение похоже на **Блокировать сообщение, но позволяет отправителю переопределять и отправлять**, но отправитель также предоставляет обоснование для переопределения ограничения политики. При использовании этого действия необходимо указать условие **Сообщение содержит конфиденциальную информацию** (*MessageContainsDataClassification*).

Свойство	Допустимые значения	Описание
`RMSTemplate`	Один объект шаблона RMS	Задает шаблон RMS, применяемый к сообщению. В Центре администрирования Exchange выберите шаблон RMS из списка. В командной консоли Exchange используйте командлет **Get-RMSTemplate** , чтобы просмотреть доступные шаблоны RMS. Для каждого почтового ящика RMS требуются клиентские лицензии (CAL) Exchange Enterprise. Дополнительные сведения о клиентских лицензиях см. в разделе Часто задаваемые вопросы о лицензировании Exchange.
`SCLValue`	Одно из указанных ниже значений: • **Обход фильтрации нежелательной почты** (`-1`) • Целые числа от 0 до 9.	Указывает вероятность нежелательной почты, назначенную сообщению. Чем больше ее значение, тем вероятнее, что сообщение окажется спамом.
`String`	Одиночная строка	Задает текст, добавляемый в указанное поле заголовка сообщения, отчет о недоставке или запись журнала событий. В командной консоли Exchange, если значение содержит пробелы, заключите значение в кавычки (").

Дополнительные сведения

Условия и исключения (предикаты) правил потока обработки почты в Exchange Server

Заявления об отказе от ответственности, подписи, нижние колонтитулы или заголовки в Exchange Server

Статья • 04.04.2023

В верхнюю или нижнюю часть электронных сообщений, поступающих в организацию или исходящих из нее, можно добавить предупреждение, юридическую оговорку, заявление о раскрытии информации, подпись или другие сведения. Это может понадобиться в связи с юридическими, корпоративными или нормативными требованиями, для определения потенциально небезопасных сообщений или по другим причинам, характерным для вашей организации.

Чтобы создать отказ от ответственности, создайте правило потока обработки почты (также известное как правило транспорта) с действием, которое добавляет указанный текст в сообщения электронной почты. Вы можете настроить правило для применения заявления об отказе от ответственности ко всем сообщениям (без условий) или определить условия, определяющие, когда добавляется заявление об отказе (например, когда отправитель является членом определенной группы, когда сообщение содержит определенные слова или текстовые шаблоны или только исходящие сообщения). Вы также можете определить исключения, которые препятствуют добавлению заявления об отказе от ответственности в сообщения (например, сообщения от определенных отправителей, сообщения, отправленные определенным получателям или сообщения, которые уже содержат заявление об отказе от ответственности). Чтобы применить несколько отказов к одному сообщению, необходимо использовать несколько правил. Дополнительные сведения о правилах потока обработки почты см. в разделе Правила потока обработки почты в Exchange Server.

Ищете процедуры? См. статью Процедуры для правил потока обработки почты в Exchange Server.

Примеры

Примечание. Примеры в этом разделе не предназначены для использования как есть. Измените их в соответствии со своими потребностями.

Тип	Пример добавляемого текста

Тип	Пример добавляемого текста
Юридическая оговорка для исходящих сообщений	Это сообщение и любые передаваемые в нем файлы конфиденциальны и предназначены исключительно для использования адресатом. Если вы получили его по ошибке, уведомите системного администратора.
Юридическая оговорка для входящих сообщений	Сотрудники обязуются не делать клеветнических заявлений и не нарушать авторские или другие права, а также не допускать такого нарушения в сообщениях электронной почты. В случае получения подобных сообщений необходимо немедленно уведомить своего руководителя.
Уведомление об отправке сообщения псевдониму	Это сообщение отправлено группе обсуждений по продажам.
Подпись (уникальные данные для каждого сотрудника)	Кэтлин Майер Отдел продаж Contoso www.contoso.com kathleen@contoso.com cell: 111-222-1234
Реклама	Специальные предложения за март см. здесь

Расположение оговорки

Можно выбрать, куда вставить оговорку — в начало или в конец сообщения.

В центре администрирования EAC вы выбираете действие **Добавить заявление об ответственности** или **Применить заявление об отказе к сообщению**>,**предшествующему отказу от ответственности**.

В командной консоли Exchange используйте параметр *ApplyHtmlDisclaimerTextLocation* со значением `Append` (по умолчанию) или `Prepend`.

Форматирование оговорки

Ниже указано форматирование, которое можно использовать для текста оговорки.

Тип сведений	Описание
обычный текст	Максимальная длина: 5000 символов, в том числе HTML-теги и встроенные каскадные таблицы стилей (CSS).

Тип сведений	Описание
HTML и встроенные CSS	Для форматирования текста можно использовать стили HTML и встроенные CSS. Например, используйте `<HR>` тег, чтобы добавить строку перед заявлением об отказе. Текст заявления об отказе также поддерживает следующие ключевые слова, использующие значения отправителя: • %%City%% • %%Company%% • %%CountryOrRegion%% • %%Отдел%% • %%DisplayName%% • %%Fax%% • %%FirstName%% • %%HomePhone%% • %%Initials%% • %%LastName%% • %%Manager%% • %%MobilePhone%% • %%Notes%% • %%Office%% • %%Pager%% • %%Phone%% • %%Почтовый код%% • %%PostOfficeBox%% • %%StateOrProvince%% • %%StreetAddress%% • %%Title%% • %%UserPrincipalName%% • %%WindowsEmailAddress%% HTML игнорируется, если оговорка добавляется к сообщению с обычным текстом.
изображения;	Используйте тег , `<IMG>` чтобы указать изображение, доступное в Интернете. Например, `<IMG src="http://contoso.com/images/companylogo.gif" alt="Contoso logo">`. По умолчанию Outlook и Outlook в Интернете (предыдущее имя — Outlook Web App) блокируют внешнее веб-содержимое, в том числе изображения. Пользователи должны подтвердить и скачать заблокированное внешнее содержимое. Мы рекомендуем протестировать заявления об отказе с `IMG` тегами, чтобы убедиться, что они отображаются так, как вы хотите.

Тип сведений	Описание
Сведения о пользователях для персонализированных подписей	Маркеры можно использовать для добавления уникальных атрибутов из учетной записи Active Directory отправителя: • %%City%% • %%Company%% • %%CountryOrRegion%% • %%Отдел%% • %%DisplayName%% • %%Fax%% • %%FirstName%% • %%HomePhone%% • %%Initials%% • %%LastName%% • %%Manager%% • %%MobilePhone%% • %%Notes%% • %%Office%% • %%Pager%% • %%Phone%% • %%Почтовый код%% • %%PostOfficeBox%% • %%StateOrProvince%% • %%StreetAddress%% • %%Title%% • %%UserPrincipalName%% • %%WindowsEmailAddress%%

Ниже приведен пример html-заявления об отказе от ответственности, который включает в себя сигнатуру `IMG` , тег и внедренный CSS.

HTML

```
<div style="font-size:9pt;  font-family: 'Calibri',sans-serif;">
%%displayname%%<br/>
%%title%%<br/>
%%company%%<br/>
%%street%%<br/>
%%city%%, %%state%% %%zipcode%%</div>
 <br/>
<div style="background-color:#D5EAFF; border:1px dotted #003333;
padding:.8em; ">
<div><img alt="Fabrikam"  src="http://fabrikam.com/images/fabrikamlogo.png">
</div>
<span style="font-size:12pt;  font-family: 'Cambria','times new
roman','garamond',serif; color:#ff0000;">HTML Disclaimer Title</span><br/>
<p style="font-size:8pt; line-height:10pt; font-family: 'Cambria','times
roman',serif;">This message contains confidential information and is
intended only for the individual(s) addressed in the message. If you aren't
```

```
the named addressee, you should not disseminate, distribute, or copy this e-
mail. If you aren't the intended recipient, you aren'tified that disclosing,
distributing, or copying this e-mail is strictly prohibited.  </p>
<span style="padding-top:10px; font-weight:bold; color:#CC0000; font-
size:10pt; font-family: 'Calibri',Arial,sans-serif; "><a
href="http://www.fabrikam.com">Fabrikam, Inc. </a></span><br/><br/>
</div>
```

Резервные варианты для правил оговорок

Exchange не может изменять содержимое некоторых сообщений (например, зашифрованных). В правилах, добавляющих оговорку в сообщения, укажите действие, которое следует выполнить, если добавить оговорку не удается. Эта непредвиденность называется *резервным вариантом* для правила заявления об отказе от ответственности. Доступные резервные варианты указаны ниже.

- **Оболочка**: создается новое сообщение, и исходное сообщение добавляется в него в виде вложения. Текст заявления об отказе добавляется в новое сообщение, которое доставляется получателям. Это значение используется по умолчанию.
  - Последующие правила потока обработки почты, которые проверяют свойства сообщения (например, тему сообщения или текст в тексте сообщения), будут проверять новое сообщение, а не исходное сообщение (которое теперь является вложением в новом сообщении). Если вы хотите, чтобы другие правила проверяли исходное сообщение и действовали над этим сообщением, убедитесь, что эти правила применяются *перед* правилом об отказе от ответственности, используя более низкий приоритет для правила заявления об отказе от ответственности и более высокий приоритет для других правил.
  - Если процесс вставки исходного сообщения в качестве вложения в новое сообщение завершается ошибкой, исходное сообщение не доставляется. Исходное сообщение возвращается отправителю в отчете о недоставке (также известном как недоставка или сообщение о отказе).

- **Игнорировать**: правило игнорируется, а исходное сообщение доставляется без заявления об отказе.

- **Отклонить**. Исходное сообщение возвращается отправителю в отчете о недоставке.

В Центре администрирования Exchange выбирайте резервный вариант в действиях для правила. В командной консоли Exchange используйте параметр *ApplyHtmlDisclaimerFallbackAction* .

Область применения оговорки

Используя оговорки, следует учитывать, к каким сообщениям они будут применяться. Например, можно указать разные оговорки для внутренних и внешних сообщений или для сообщений, отправляемых пользователями в конкретных отделах. Чтобы оговорка применялась только к первому сообщению в беседе, добавьте исключение, которое запрещает многократно применять текст оговорки к одним и тем же сообщениям.

Ниже приведены примеры возможных условий и исключений.

Описание	**Условия и исключения в Центре администрирования Exchange (EAC)**	**Условия и исключения в командной консоли Exchange для командлетов New-TransportRule или Set-TransportRule**
Получатель находится вне вашей организации Exchange. Исключение настроено так, что к сообщениям, которые уже содержат текст оговорки CONTOSO LEGAL NOTICE, оговорка повторно не применяется.	Условие: **получатель находится**>**за пределами организации** Исключение: **тема или текст**>**темы или текста соответствует этим текстовым шаблонам**> CONTOSO LEGAL NOTICE	`-FromScope NotInOrganization -ExceptIf -SubjectOrBodyMatches "CONTOSO LEGAL NOTICE"`
Входящие сообщения с исполняемыми файлами во вложениях	Условие 1. **Отправитель находится**>**за пределами организации** Условие 2. **Любое вложение**>**содержит исполняемое содержимое**	`-FromScope NotInOrganization -AttachmentHasExecutableContent`
Отправитель находится в отделе маркетинга	Условие: **отправитель**>**является членом этой группы**>.	`-FromMemberOf "Marketing Team"`

Описание	Условия и исключения в Центре администрирования Exchange (EAC)	Условия и исключения в командной консоли Exchange для командлетов New-TransportRule или Set-TransportRule
Сообщения от внешнего отправителя группе обсуждений по продажам	Условие 1. **Отправитель находится>за пределами организации** Условие 2. **Поле "Кому>" или "Копия" содержит***имя группы* пользователя >	`-FromScope NotInOrganization -SentTo "Sales Discussion Group"`
Добавление рекламы в исходящие сообщения на один месяц	Условие 1. **Получатель находится>за пределами организации** Укажите даты в полях **Активировать это правило начиная с** или **Отключить это правило начиная с**.	`-ApplyHtmlDisclaimerLocation Prepend -SentToScope NotInOrganization -ActivationDate '03/1/2016' -ExpiryDate '03/31/2016'`

Полный список условий и исключений, которые можно использовать для целей заявления об отказе от ответственности, см. в статье Условия и исключения (предикаты) правил потока обработки почты в Exchange Server.

Ограничения подписей в масштабах организации

Exchange Server сигнатуры не могут выполнять следующие сценарии:

- Вставьте подпись непосредственно под последним ответом или пересылаемой электронной почтой.
- Отображение подписей электронной почты на стороне сервера в папках отправленных пользователей.
- Пропустите строки, содержащие переменные, которые не удалось обновить (например, если значение не было предоставлено пользователю).

Чтобы получить эти и другие возможности, используйте стороннее средство. Выполните поиск **в Интернете программного обеспечения для подписи**

электронной почты. Некоторые из этих поставщиков являются партнерами Microsoft Gold, и их программное обеспечение предоставляет эти возможности.

Дополнительные сведения

Заявления об отказе от ответственности, подписи, нижние колонтитулы и заголовки в Exchange 2013

Процедуры для правил потока обработки почты в Exchange Server

Статья • 04.04.2023

Правила потока обработки почты (также называемые правилами транспорта) определяют и принимают меры с сообщениями, которые передаются через организацию Exchange. Дополнительные сведения о правилах потока обработки почты см. в разделе Правила потока обработки почты в Exchange Server.

На серверах почтовых ящиков для управлениями правилами потока обработки почты можно использовать Центр администрирования Exchange (EAC) и командную консоль Exchange. На пограничных транспортных серверах можно использовать только командную консоль Exchange.

> **Совет**
>
> Убедитесь, что правила работают надлежащим образом. Тщательно тестируйте все правила и взаимодействия между ними.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут.
- Дополнительные сведения о EAC см. в разделе Центр администрирования Exchange в Exchange Server. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Правила потока обработки почты" в разделе Политика обмена сообщениями и разрешения на соответствие требованиям в Exchange Server (Exchange Server) или в разделе Разрешения компонентов в Exchange Online.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Создание правил транспорта

- При создании правил потока обработки почты в первую очередь следует руководствоваться поставленными задачами. Примеры см. в следующих статьях:
  - Использование правил потока обработки почты для проверки вложений сообщений
  - Заявления об отказе от ответственности, подписи, нижние колонтитулы или заголовки в Exchange Server
  - Управление утверждением сообщений
- Политики защиты от потери данных (DLP) — это коллекции правил потока обработки почты. Сведения о создании политик защиты от потери данных см. в разделе Exchange Server процедуры защиты от потери данных.

Создание правил потока обработки почты с помощью Центра администрирования Exchange

В Центре администрирования Exchange можно создавать правила потока обработки почты с помощью шаблона (отфильтрованного списка условий и действий), копируя существующие правила или создавая их с нуля.

1. В EAC перейдите в раздел**Правилапотока обработки**> почты и выберите один из следующих параметров:
   - Чтобы создать правило на основе шаблона, щелкните **Добавить** (➕) и выберите шаблон (значение, отличное от **Создать правило**).
   - Чтобы скопировать правило, выберите правило и выберите **Копировать** (📄 Обратите внимание, что возможность копирования правил доступна только в Центре администрирования Exchange.
   - Чтобы создать новое правило с нуля, **выберите Добавить** (➕ Затем выберите **Создать новое правило**.
2. На открывшейся странице **Новое правило** настройте следующие параметры:

- **Имя**. Введите уникальное описательное имя правила.
- **Примените это правило, если**: выберите условие для правила. Если правило должно применяться ко всем сообщениям, выберите пункт **[Применить ко всем сообщениям]**. Описание доступных условий см. в статье Условия и исключения (предикаты) правил потока обработки почты в Exchange Server.
- **Выполните следующие действия**. Выберите действие для правила. Действие применяется к сообщениям, которые соответствуют условиям. Описание доступных условий см. в разделе Действия правил потока почты в Exchange Server.

Необязательные свойства:

- **Аудит этого правила с уровнем серьезности**. Для политик защиты от потери данных этот параметр указывает, как данные соответствия правил отображаются в отчетах об обнаружении политики защиты от потери данных. Дополнительные сведения см. в статье View DLP policy detection reports. Если снять этот флажок или выбрать значение **Не указано**, совпадения с правилом не будут отображаться в соответствующих отчетах.
- **Выберите режим для этого правила**. Для тестирования правила можно использовать один из двух режимов тестирования, не влияя на поток обработки почты. В обоих тестовых режимах в журнал отслеживания сообщений добавляется запись. Выберите одно из следующих значений:
- **Принудительное применение**. Это правило включается и немедленно начинается обработка сообщений. Выполняются все действия в правиле. Это значение используется по умолчанию.
- **Тестирование с помощью подсказок политики**. Это включает правило, и все действия подсказки политики (**уведомление отправителя с помощью подсказки политики**) будут отправлены, но никакие действия, связанные с доставкой сообщений, выполняться не будут. Для использования этого режима необходимо настроить защиту от потери данных. Дополнительные сведения см. в статье Policy Tips.
- **Тестирование без советов по политике**. Для политик защиты от потери данных будет принудительно применяться только **отчет о создании инцидента и его отправке в** действие. Не выполняется никаких действий, связанных с доставкой сообщений.

3. Вы можете создать правило, нажав кнопку **Сохранить**, или выбрать **Дополнительные параметры**, чтобы настроить следующие дополнительные параметры:

    - Чтобы добавить условия, нажмите **Добавить условие**. Если у вас несколько условий, можно удалить условие, нажав кнопку **Удалить X**. Обратите внимание, что после нажатия кнопки **Дополнительные параметры** доступны дополнительные условия.

    - Чтобы добавить условия, нажмите **Добавить условие**. Если у вас есть несколько действий, можно удалить действие, нажав кнопку **Удалить X**. Обратите внимание, что после нажатия кнопки **Дополнительные параметры** доступны дополнительные действия.

    - Чтобы добавить исключения из правила, нажмите **Добавить исключение**, а затем выберите исключение в раскрывающемся списке **Кроме случаев, когда**. Вы можете удалить исключение, нажав **Удалить X**.

    - **Активируйте это правило в следующую дату**: укажите дату начала, если вы хотите, чтобы правило влось в силу после определенной даты. Обратите внимание, что правило будет включено и до наступления этой даты, но не будет обрабатываться.

    - **Отключите это правило в следующую дату**: укажите дату окончания, если вы хотите, чтобы правило прекратило обработку сообщений в определенную дату. Обратите внимание, что после этой даты правило останется включенным, но не будет обрабатываться.

    - **Остановить обработку дополнительных правил**. Установите этот флажок, чтобы избежать применения дополнительных правил после обработки этим правилом сообщения.

    - **Отложить сообщение, если обработка правила не завершена**. Установите этот флажок, чтобы повторно отправить сообщение для обработки. По умолчанию правило будет игнорироваться, а доставка сообщения продолжится в обычном режиме.

    - **Сопоставление адреса отправителя в сообщении**. Для условий и исключений, которые проверяют адрес отправителя, можно указать, где правило ищет адрес отправителя: в заголовке сообщения (по умолчанию), конверте сообщения или в заголовке и конверте. Дополнительные сведения см. в разделе Отправители.

    - **Примечания**. Укажите описательное примечание для правила.

По завершении нажмите кнопку **Сохранить**.

Создание правил потока обработки почты с помощью командной консоли Exchange

В командной консоли Exchange для новых правил потока обработки почты есть два параметра, недоступных в Центре администрирования Exchange (пока правило не будет создано):

- Создание нового правила как отключено (*включено* `$false`)
- Задайте приоритет правила (*номер>приоритета<*).

Для создания правил потока обработки почты в командной консоли Exchange используйте следующий синтаксис:

PowerShell

```
New-TransportRule -Name <RuleName> [<Conditions>] [<Exceptions>] <Actions>
[<Properties>]
```

В этом примере создается правило со следующими параметрами:

- **Имя**: пометка сообщений из Интернета в отдел продаж DG.
- **Conditions**
  - Сообщения от внешних отправителей.

    И

  - Сообщения, отправленные группе рассылки Sales Department.
- **Действие**: перед полем **Subject** сообщения добавляется значение `"External message to Sales DG: "`. Двоеточие и пробел в конце этого значения помогают отделить добавленный текст от исходного значения.

PowerShell

```
New-TransportRule -Name "Mark messages from the Internet to Sales DG" -
FromScope NotInOrganization -SentTo "Sales Department" -PrependSubject
"External message to Sales DG: "
```

Дополнительные сведения о синтаксисе и параметрах см. в статье New-TransportRule.

Примечание. Условия и действия в примере предназначены только для иллюстрации. Просмотрите доступные условия, исключения и действия правил потока обработки почты, чтобы определить, какие из них соответствуют вашим требованиям.

Как проверить, что все получилось?

Чтобы проверить, успешно ли создано правило потока обработки почты, выполните одно из указанных ниже действий.

- В EAC перейдите в раздел**Правилапотока обработки**> почты и убедитесь, что созданное правило находится в списке.
- В командной консоли Exchange используйте любую из представленных ниже процедур.
  - Выполните следующую команду, чтобы увидеть новое правило в списке правил:

```
PowerShell

Get-TransportRule
```

  - Замените <*RuleName*> именем правила и выполните следующую команду, чтобы просмотреть сведения о правиле:

```
PowerShell

Get-TransportRule -Identity "<RuleName>" | Format-List
```

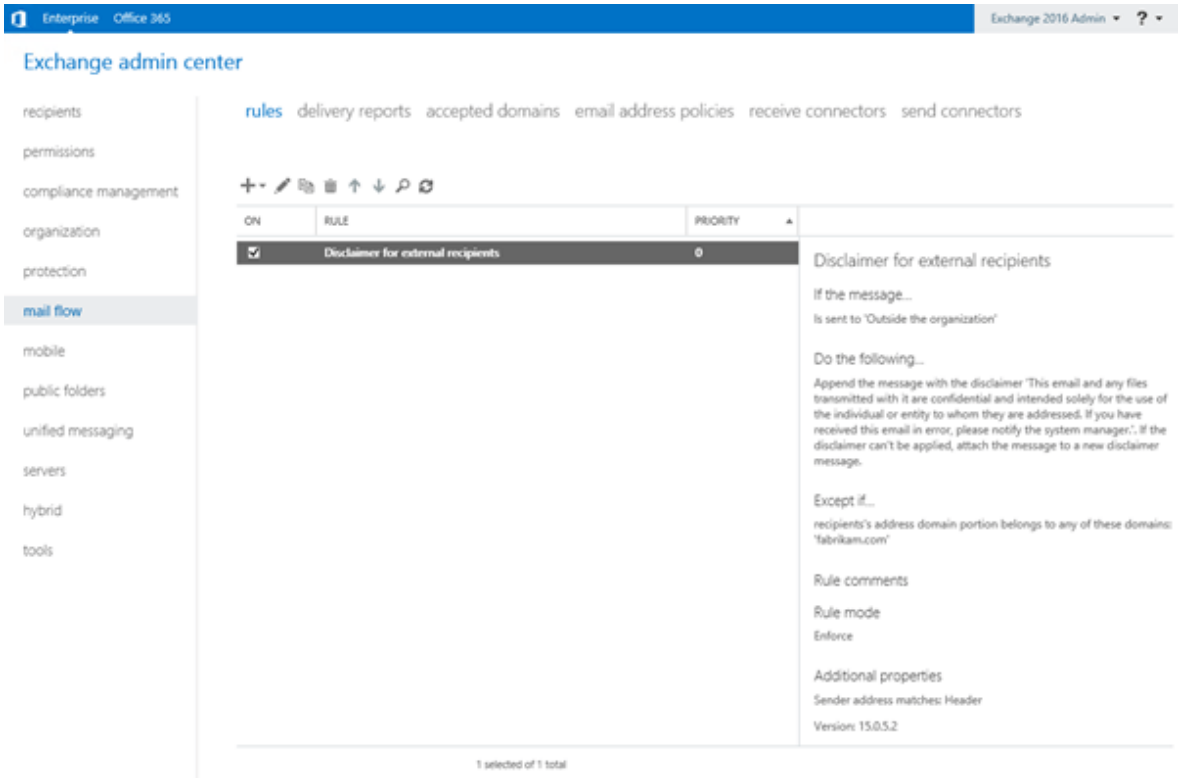
Просмотр правил потока обработки почты

Правила потока обработки почты, созданные на сервере почтовых ящиков, хранятся в Active Directory, поэтому при просмотре правил на таком сервере отображаются все правила, определенные в организации. При просмотре правил потока обработки почты на пограничном транспортном сервере с помощью командной консоли Exchange отображаются правила, хранящиеся на локальном сервере.

Просмотр правил потока обработки почты с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел**Правилапотока обработки**> почты.

2. При выборе правила сведения о нем отображаются в области сведений. Чтобы просмотреть дополнительные сведения о правиле, щелкните **Изменить** (✎).



В Центре администрирования Exchange свойство **Версия** отображается только в области сведений. Это свойство указывает на совместимость правила с предыдущими версиями Exchange (14). *n*. *n*. *n* — Exchange 2010, 15.0. *n*. *n* — Exchange 2013).

Просмотр правил потока обработки почты с помощью командной консоли Exchange

Чтобы получить сводный список всех правил потока обработки почты, выполните следующую команду:

PowerShell

```
Get-TransportRule
```

Чтобы получить подробные сведения об определенном правиле, используйте следующий синтаксис:

PowerShell

```
Get-TransportRule -Identity "<RuleName>" | Format-List [<Specific properties to view>]
```

В этом примере возвращаются значения всех свойств правила под названием "Sender is a member of marketing".

PowerShell

```
Get-TransportRule -Identity "Sender is a member of marketing" | Format-List
```

В этом примере возвращаются только указанные свойства правила.

PowerShell

```
Get-TransportRule -Identity "Sender is a member of marketing" | Format-List
Name,State,Mode,Priority,Comments,Conditions,Exceptions,RuleVersion
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Get-TransportRule.

Просмотр доступных условий и исключений (предикатов) для правил потока обработки почты с помощью командной консоли Exchange

Условия и исключения в правилах потока обработки почты в совокупности *называются предикатами* , так как для каждого условия существует соответствующее исключение, использующее одинаковые параметры и синтаксис. Единственное отличие заключается в том, что условия указывают, к каким сообщениям правило применяется, а исключения — наоборот. Просмотреть список условий и исключений можно только в командной консоли Exchange.

Чтобы просмотреть условия и исключения, доступные в правилах потока обработки почты, выполните следующую команду:

PowerShell

```
Get-TransportRulePredicate
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Get-TransportRulePredicate.

Примечания.

- Исключения не отличаются от условий.

- На пограничных транспортных серверах доступны только некоторые из предикатов, доступных на серверах почтовых ящиков. Дополнительные сведения см. в разделе Условия и исключения правил обработки почты (предикаты) в Exchange Server.

- Имена некоторых предикатов отличаются от имен соответствующих параметров условий и исключений в командлетах **New-TransportRule** и **Set-TransportRule**. Кроме того, у некоторых предикатов есть несколько обязательных параметров.

Просмотр доступных действий для правил потока обработки почты с помощью Командная консоль Exchange

Просмотреть список действий можно только в командной консоли Exchange.

Чтобы просмотреть список действий, доступных в правилах потока обработки почты, выполните следующую команду:

```
PowerShell

Get-TransportRuleAction
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Get-TransportRuleAction.

Примечания.

- На пограничных транспортных серверах доступны только некоторые из действий, доступных на серверах почтовых ящиков, но также существуют действия, доступные только на пограничных транспортных серверах. Дополнительные сведения см. в статье Действия правил потока обработки почты в Exchange Server.

- Имена некоторых действий отличаются от имен соответствующих параметров действий в командлетах **New-TransportRule** и **Set-TransportRule**. Кроме того, у некоторых действий есть несколько обязательных параметров.

Изменение правил потока обработки почты

Изменение правил потока обработки почты с помощью Центра администрирования Exchange

При изменении правила потока обработки почты в Центре администрирования Exchange не используется никаких дополнительных параметров. В этом случае доступны те же параметры, что и при создании правила.

1. В EAC перейдите в раздел**Правилапотока обработки**> почты.
2. Выберите правило и нажмите кнопку **Изменить** (✎ Обратите внимание, что отображаются все свойства правила (ссылка **Дополнительные параметры** недоступна). Дополнительные сведения о свойствах правил см. в разделе Создание правил потока обработки почты с помощью Центра администрирования Exchange этой статьи.

Изменение правил потока обработки почты с помощью командной консоли Exchange

При изменении правила потока обработки почты в командной консоли Exchange его нельзя отключить или включить (в **командлете Set-TransportRule** нет параметра *Enabled*). Вместо этого используйте командлеты **Disable-TransportRule** и **Enable-TransportRule**, как описано далее в этой статье.

Для изменения правил потока обработки почты в командной консоли Exchange используйте следующий синтаксис:

PowerShell

```
Set-MailFlowRule -Identity "<RuleName>" [<Conditions>] [<Exceptions>]
[<Actions>] [<Properties>]
```

В этом примере к правилу под названием "Sender is a member of marketing" добавляется исключение, чтобы правило не применялось к сообщениям от пользователя Kelly Rollin.

PowerShell

```
Set-TransportRule -Identity "Sender is a member of marketing" -ExceptIfFrom
"Kelly Rollin"
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Set-TransportRule.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли изменено правило потока обработки почты, выполните одно из указанных ниже действий.

- В EAC перейдите в**раздел Правилапотока обработки**> почты, выберите правило и просмотрите сведения в области сведений. Чтобы просмотреть другие параметры, нажмите кнопку **Изменить** (✎

- В командной консоли Exchange замените <*RuleName*> именем правила и выполните следующую команду:

  PowerShell

  ```
  Get-TransportRule -Identity "<RuleName>" | Format-List
  ```

Установка приоритета для правил потока обработки почты

По умолчанию правилам потока обработки почты присваивается приоритет, основанный на порядке их создания (новые правила имеют более низкий приоритет, чем старые). Более низкий приоритет указывает на более высокий приоритет правила, а правила обрабатываются в порядке приоритета (правила с более высоким приоритетом обрабатываются перед правилами с более низким приоритетом). Два правила не могут иметь одинаковый приоритет.

Примечания.

- Вы можете предотвратить выполнение сообщения последующими правилами с более низким приоритетом, включив в правило действие **Остановить обработку дополнительных правил** (*StopRuleProcessing* `$true`).

- В Центре администрирования Exchange изменить приоритет правила можно только после его создания. В командной консоли Exchange можно переопределить заданный по умолчанию приоритет при создании правила (это может повлиять на приоритеты существующих правил).

Установка приоритета правил потока обработки почты с помощью Центра администрирования Exchange

В Центре администрирования Exchange правила обрабатываются в том же порядке, в котором они отображаются (для первого правила в свойстве **Приоритет** задано значение 0). Чтобы изменить приоритет правила, переместите правило вверх или вниз в списке (вы также можете напрямую изменить номер **приоритета** , изменив правило в EAC).

1. В EAC перейдите в раздел**Правилапотока обработки**> почты.
2. Выберите правило, а затем нажмите кнопку **Переместить вверх** (🡅) или **Переместить вниз** (🡇), чтобы переместить правило вверх или вниз в списке.

Установка приоритета для правил потока обработки почты с помощью командной консоли Exchange

Максимальный приоритет, который можно задать для правила, — 0. Минимальное значение зависит от количества правил. Например, если у вас есть пять правил, вы можете использовать значения 0–4. Изменение приоритета существующего правила оказывает каскадное влияние на другие правила. Например, если вы измените приоритет правила на 2, когда у вас есть пять правил (с приоритетами от 0 до 4), то для существующего правила с приоритетом 2 будет задан приоритет 3, а для правила с приоритетом 3 будет задан приоритет 4.

Чтобы задать приоритет правила в командной консоли Exchange, используйте следующий синтаксис:

PowerShell

```
Set-TransportRule -Identity "<RuleName>" -Priority <Number>
```

В этом примере для правила под названием "Sender is a member of marketing" задается приоритет 2. Все правила с приоритетом не больше 2 понижаются на один ранг (значения приоритета увеличиваются на 1).

PowerShell

```
Set-TransportRule -Identity "Sender is a member of marketing" -Priority 2
```

Примечание. Чтобы задать приоритет нового правила при его создании, используйте параметр *Priority* командлета **New-TransportRule**.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли изменен приоритет правила потока обработки почты, выполните одно из указанных ниже действий.

- В EAC перейдите в раздел**Правилапотока обработки**> почты и проверьте значение **Приоритет** правила в списке.
- В командной консоли Exchange используйте любую из представленных ниже процедур.
  - Выполните следующую команду, чтобы просмотреть список правил и соответствующих значений **Priority**:

```
PowerShell

Get-TransportRule
```

  - Замените <*RuleName*> именем правила и выполните следующую команду:

```
PowerShell

Get-TransportRule -Identity "<RuleName>" | Format-List Name,Priority
```

Включение и отключение правил потока обработки почты

Отключение правила позволяет предотвратить его применение к сообщениям, сохранив параметры правила.

По умолчанию правила потока обработки почты включены при их создании в EAC или командной консоли Exchange, но для создания отключенного правила можно использовать командную консоль Exchange (используйте параметр *Enabled* со значением `$false`).

Включение и отключение правил потока обработки почты с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел**Правилапотока обработки**> почты.
2. Выберите правило в списке, а затем настройте один из следующих параметров:
   - **Отключите правило**. Снимите флажок в столбце **Включено** .

- **Включить правило**. Установите флажок в столбце **Включено** .

Включение и отключение правил потока обработки почты с помощью командной консоли Exchange

Для включения и отключения правил потока обработки почты в командной консоли Exchange используйте следующий синтаксис:

```
PowerShell

<Enable-TransportRule | Disable-TransportRule> -Identity "<RuleName>"
```

В этом примере отключается правило потока обработки почты под названием "Sender is a member of marketing".

```
PowerShell

Disable-TransportRule "Sender is a member of marketing"
```

В этом примере включается правило потока обработки почты под названием "Sender is a member of marketing".

```
PowerShell

Enable-TransportRule "Sender is a member of marketing"
```

Дополнительные сведения о синтаксисе и параметрах см. в статьях Enable-TransportRule и Disable-TransportRule.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли включено или отключено правило потока обработки почты, выполните одно из указанных ниже действий.

- В EAC перейдите в раздел**Правилапотока обработки**> почты и в списке правил проверьте состояние флажка в столбце **Вкл**.
- В командной консоли Exchange используйте любую из представленных ниже процедур.
  - Выполните следующую команду, чтобы просмотреть список правил и соответствующих значений **State**:

    ```
    
    ```

```
PowerShell

Get-TransportRule
```

- Замените <*RuleName*> именем правила и выполните следующую команду:

```
PowerShell

Get-TransportRule -Identity "<RuleName>" | Format-List Name,State
```

Удаление правил потока обработки почты

Удаление правил потока обработки почты с помощью Центра администрирования Exchange

1. В EAC перейдите в**раздел Правилапотока обработки**> почты.
2. Выберите правило, которое нужно удалить из списка, и нажмите кнопку **Удалить** (🗑

Удаление правил потока обработки почты с помощью командной консоли Exchange

Для удаления правил потока обработки почты в командной консоли Exchange используйте следующий синтаксис:

```
PowerShell

Remove-TransportRule -Identity "<RuleName>"
```

В этом примере удаляется правило потока обработки почты под названием "Sender is a member of marketing".

```
PowerShell

Remove-TransportRule -Identity "Sender is a member of marketing"
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Remove-TransportRule.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли удалено правило потока обработки почты, выполните одно из указанных ниже действий.

- В EAC перейдите в раздел**Правилапотока обработки**> почты и убедитесь, что удаляемого правила больше нет в списке.
- В командной консоли Exchange выполните указанную ниже команду, чтобы проверить удаление правила.

```
PowerShell

Get-TransportRule
```

Импорт и экспорт коллекций правил потока обработки почты

Вы можете импортировать коллекцию правил потока обработки почты, ранее экспортированную в качестве резервной копии, или импортировать правила, экспортированные из предыдущей версии Exchange.

Примечания.

- В Центре администрирования Exchange невозможно импортировать и экспортировать коллекции правил потока обработки почты. Можно использовать только командную консоль Exchange.
- Невозможно импортировать коллекцию правил потока обработки почты в Exchange 2010, если эта коллекция правил была экспортирована из Exchange 2013 или более поздней версии.

Экспорт коллекции правил потока обработки почты с помощью командной консоли Exchange

1. Выполните следующую команду:

```
PowerShell

$File = Export-TransportRuleCollection
```

2. Используйте следующий синтаксис:

```
PowerShell
```

```
[System.IO.File]::WriteAllBytes('<OutputFile>', $File.FileData)
```

Например, чтобы сохранить экспортированную коллекцию правил потока обработки почты в файл C:\My Documents\Exported Rules.xml, выполните следующую команду:

```
PowerShell

[System.IO.File]::WriteAllBytes('C:\My Documents\Exported Rules.xml',
$File.FileData)
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Export-TransportRuleCollection.

Импорт коллекции правил потока обработки почты с помощью командной консоли Exchange

1. Используйте следующий синтаксис.

```
PowerShell

$Data = [System.IO.File]::ReadAllBytes('<OutputFile>')
```

Например, чтобы импортировать коллекцию правил потока обработки почты из файла C:\My Documents\Exported Rules.xml, выполните следующую команду:

```
PowerShell

$Data = [System.IO.File]::ReadAllBytes('C:\My Documents\Exported
Rules.xml')
```

2. Выполните следующую команду:

```
PowerShell

Import-TransportRuleCollection -FileData $Data
```

Дополнительные сведения о синтаксисе и параметрах см. в статье Import-TransportRuleCollection.

Нужна дополнительная помощь?

- Ресурсы для Exchange Server:
  - Правила потока обработки почты в Exchange Server
  - Условия и исключения (предикаты) правил потока обработки почты в Exchange Server
  - Действия правил потока обработки почты в Exchange Server

Регистрация IFilters пакета фильтров в Exchange Server

Статья • 11.02.2025

Правила потока обработки почты с условиями сканирования вложений выполняют извлечение текста при анализе содержимого вложений. Exchange Server могут проверять наиболее часто используемые типы вложений в собственном коде. Дополнительные типы вложений можно включить, зарегистрировав IFilters в Exchange Server. В этой статье показано, как зарегистрировать IFilters, выпущенные корпорацией Майкрософт и внешними поставщиками.

После регистрации IFilter для определенного типа файлов правила потока обработки почты с условиями обработки вложений могут сканировать эти вложения. В результате эти типы файлов больше не активируют условие *AttachmentIsUnsupported* .

> **⚠ Предупреждение**
>
> В процедуры, приведенные в этой теме, входит изменение реестра на серверах Exchange. Неправильное изменение реестра может привести к серьезным проблемам, которые могут потребовать переустановки операционной системы. Проблемы, возникающие в результате неправильного изменения реестра, могут быть не устранены. Перед внесением изменений в реестр выполните резервное копирование всех важных данных.
>
> Для выполнения данных процедур также необходимо остановить и перезапустить транспортную службу Microsoft Exchange на серверах почтовых ящиков.

Дополнительные задачи управления, связанные с правилами потока обработки почты, см. в разделе Процедуры для правил потока обработки почты в Exchange Server.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут на сервер.

- Перед выполнением этой процедуры или процедур вам должны быть назначены разрешения. Сведения о необходимых разрешениях см. в записи "Параметры конфигурации сервера Exchange" в статье о разрешениях для инфраструктуры Exchange и PowerShell .
- На серверах, на которых уже установлена роль сервера почтовых ящиков Exchange Server, необходимо выполнить следующие процедуры. При добавлении дополнительных серверов почтовых ящиков после выполнения этих процедур их необходимо снова выполнить на новых подготовленных серверах.
- Сведения о сочетаниях клавиш, которые могут применяться к процедурам, описанным в этой статье, см. в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по **адресу Exchange Server** .

Регистрация пакета фильтров Microsoft Office 2010

Если вы используете сборку Exchange Server раньше, чем Exchange Server 2019 CU15 (2025H1), по умолчанию правила потока обработки почты Exchange не поддерживают следующие типы файлов Office:

- Office OneNote
- Office Publisher

Для поддержки этих файлов необходимо развернуть пакет фильтров Microsoft Office 2010. Этот пакет фильтра не развертывается во время установки Exchange Server и не является предварительным условием для развертывания.

Развертывание пакета фильтров Microsoft Office 2010

Развертывание пакета фильтров Office 2010 состоит из двух основных этапов:

- Скачайте и установите пакет фильтров, который регистрирует IFilters в Windows (поиск).
- Изменение реестра таким образом, чтобы IFilters также регистрировались в Exchange Server. Этот шаг позволяет Exchange поддерживать сканирование вложений для форматов файлов.

> ⓘ **Важно!**
>
> Эту процедуру необходимо выполнить на каждом сервере почтовых ящиков в организации.

1. Скачайте и сохраните пакет фильтров Microsoft Office 2010 (`FilterPack64bit.exe`) из Центра загрузки Майкрософт.
2. `FilterPack64bit.exe` Запустите файл на сервере почтовых ящиков и следуйте инструкциям, чтобы завершить установку.
3. Запустите редактор реестра и перейдите к приведенному ниже подразделу реестра.

   PowerShell

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ExchangeServer\v15\HubTransportRole\CLSID
   ```

4. В разделе **CLSID** добавьте подраздел для файлов OneNote следующим образом.

   a. Щелкните правой кнопкой мыши **CLSID**, наведите указатель мыши на **пункт Создать**, а затем выберите **Ключ**.

   b. Измените имя нового ключа на `{B8D12492-CE0F-40AD-83EA-099A03D493F1}`.

   c. Выберите созданный ключ и задайте значение **(по умолчанию)** в том месте, где установлен пакет фильтров Office 2010. По умолчанию пакет фильтров устанавливается в `C:\Program Files\Common Files\Microsoft Shared\Filters\ONIFilter.dll`.

   d. Щелкните **правой кнопкой мыши {B8D12492-CE0F-40AD-83EA-099A03D493F1}**, наведите указатель мыши на **пункт Создать** и выберите **Строковое значение**.

e. Назовите новое строковое значение `ThreadingModel` и задайте для него значение `Both`.

5. В разделе **CLSID** добавьте подраздел для файлов Publisher следующим образом.

   a. Щелкните правой кнопкой мыши **CLSID**, наведите указатель мыши на **пункт Создать**, а затем выберите **Ключ**.

   b. Измените имя нового ключа на `{A7FD8AC9-7ABF-46FC-B70B-6A5E5EC9859A}`.

   c. Выберите созданный ключ и задайте значение **(по умолчанию)** в том месте, где установлен пакет фильтров Office 2010. По умолчанию пакет фильтров устанавливается в `C:\Program Files\Common Files\Microsoft Shared\Filters\PUBFILT.dll`.

   d. Щелкните правой кнопкой мыши **{A7FD8AC9-7ABF-46FC-B70B-6A5E5EC9859A}**, наведите указатель на пункт **Создать** и выберите **Строковое значение**.

   e. Назовите новое строковое значение `ThreadingModel` и задайте для него значение `Both`.

6. Откройте следующий раздел реестра:

```
PowerShell

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ExchangeServer\v15\HubTransportRo
le\filters
```

7. В разделе **фильтры** добавьте подраздел для `.one` расширений, как показано ниже.

   a. Щелкните правой кнопкой мыши **фильтры**, наведите указатель мыши на пункт **Создать**, а затем выберите **Пункт Ключ**.

   b. Измените имя нового ключа на `.one`.

   c. Выберите созданный ключ и задайте для параметра **(по умолчанию)** значение `{B8D12492-CE0F-40AD-83EA-099A03D493F1}`.

8. В разделе **фильтры** добавьте подраздел для расширений PUB следующим образом.

a. Щелкните правой кнопкой мыши **фильтры**, наведите указатель мыши на **пункт Создать** , а затем выберите **пункт Ключ**.

b. Измените имя нового ключа на `.pub`.

c. Выберите созданный ключ и задайте для параметра **(по умолчанию)** значение `{A7FD8AC9-7ABF-46FC-B70B-6A5E5EC9859A}`.

9. Закройте редактор реестра.

10. На сервере почтовых ящиков остановите и перезапустите приведенные ниже службы в указанном порядке.

a. Остановите службу транспорта Microsoft Exchange

b. Остановите службу Microsoft Filtering Management Service.

c. Запустите службу Microsoft Filtering Management Service.

d. Запустите службу транспорта Microsoft Exchange.

Как узнать, что пакет фильтров Microsoft Office 2010 успешно развернут?

Чтобы убедиться, что вы успешно зарегистрировали IFilters пакета фильтров Microsoft Office 2010, сделайте следующее:

1. Создайте правило потока обработки почты со следующими свойствами. Подробные инструкции по созданию правил потока обработки почты см. в разделе Процедуры для правил потока обработки почты в Exchange Server.

   - Отправителем является ваш почтовый ящик.
   - Содержимое любого вложения включает "Фильтры IFilter проверки".
   - Создайте отчет об инциденте и отправьте его в свой почтовый ящик.

2. Создайте файл OneNote, содержащий фразу "Фильтры IFilter проверки", вложите его в новое сообщение электронной почты и отправьте на свой адрес.

3. Убедитесь, что вы получили отчет об инциденте правила потока обработки почты для созданного правила. Этот шаг подтверждает, что обработчик правил смог проанализировать содержимое файла OneNote.

4. Повторите шаги 2 и 3 с файлом Publisher.

Регистрация сторонних IFilters для поддержки других форматов файлов

Вы можете расширить возможность сканирования вложений для файлов других типов, зарегистрировав другие сторонние IFilters. Необходимо установить и зарегистрировать IFilter типа файла на каждом из серверов почтовых ящиков.

> **ⓘ Важно!**
>
> Корпорация Майкрософт не тестирует сторонние IFilters с правилами потока обработки почты, поэтому перед развертыванием в рабочей среде рекомендуется развернуть и протестировать сторонние IFilters в тестовой среде.

Развертывание фильтра Adobe PDF IFilter

В этой процедуре показано, как развернуть IFilter Adobe PDF для поддержки обработки вложений PDF в правилах потока обработки почты.

> **ⓘ Примечание**
>
> По умолчанию Exchange Server поддерживает сканирование PDF-файлов в правилах потока обработки почты. Пример PDF здесь просто используется, чтобы проиллюстрировать, как можно расширить поддержку файлов других типов с помощью сторонних IFilters.

1. Скачайте IFilter Adobe PDF и следуйте инструкциям по установке.
2. Запустите редактор реестра и перейдите к приведенному ниже подразделу.

   Консоль

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ExchangeServer\v15\HubTransportRo
   le\CLSID
   ```

3. В разделе **CLSID** добавьте подраздел для PDF-файлов следующим образом.
   a. Щелкните правой кнопкой мыши **CLSID**, наведите указатель мыши на **пункт Создать**, а затем выберите **Ключ**.
   b. Измените имя нового ключа на `{E8978DA6-047F-4E3D-9C78-CDBE46041603}`.

> ⓘ **Примечание**
>
> Каждый фильтр IFilter имеет идентификатор уникального класса (CLSID). CISID можно найти в документации по установке для регистрируемого IFilter или в разделе реестра для поиска расширения `HKEY_CLASSES_ROOT\CLSID` файла.

c. Выберите созданный ключ и задайте значение **(по умолчанию)** в том месте, где вы установили PDF-фильтр IFilter. По умолчанию IFilter PDF устанавливается в `C:\Program Files\Adobe\Adobe PDF IFilter 9 for 64-bit platforms\bin\PDFFilter.dll`.

4. Откройте следующий раздел реестра:

```
Консоль

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ExchangeServer\v15\HubTransportRo
le\filters
```

5. В разделе **фильтры** добавьте подраздел для `.pdf` расширений следующим образом:

a. Щелкните правой кнопкой мыши **фильтры**, наведите указатель мыши на пункт **Создать**, а затем выберите **Пункт Ключ**.

b. Измените имя нового ключа на `.pdf`.

c. Выберите созданный ключ и задайте для параметра **(по умолчанию)** значение `{E8978DA6-047F-4E3D-9C78-CDBE46041603}`.

6. Закройте редактор реестра.

7. На сервере почтовых ящиков остановите и перезапустите приведенные ниже службы в указанном порядке.

a. Остановите службу транспорта Microsoft Exchange.

b. Остановите службу Microsoft Filtering Management Service.

c. Запустите службу Microsoft Filtering Management Service.

d. Запустите службу транспорта Microsoft Exchange.

Как узнать, что вы успешно зарегистрировали сторонние IFilters для поддержки других форматов файлов?

Используйте ту же процедуру, описанную выше в этой статье Как узнать, что вы успешно развернули пакет фильтров Microsoft Office 2010? Замените файлы Publisher файлами Adobe PDF.

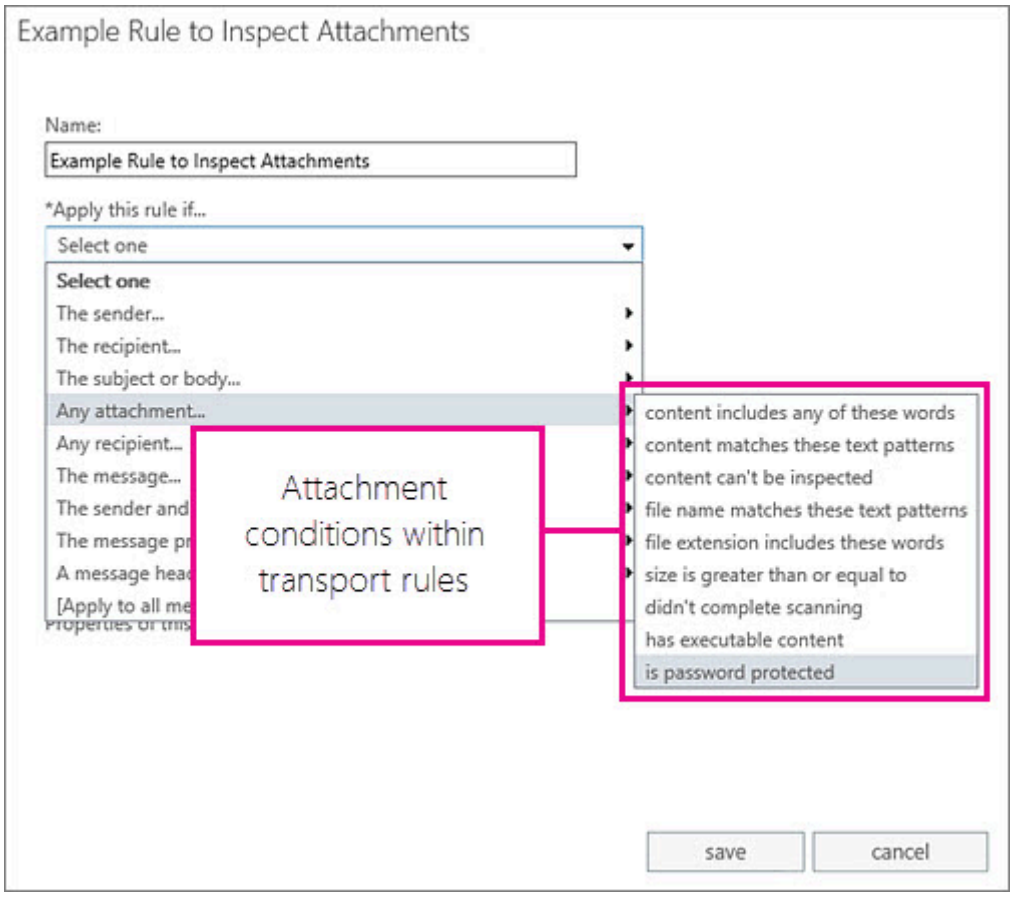
Использование правил потока обработки почты для проверки вложений сообщений

Статья • 11.02.2025

Вы можете проверить вложения электронной почты в организации, настроив правила потока обработки почты (также известные как правила транспорта). Exchange предлагает правила потока обработки почты, которые предоставляют возможность просматривать вложения электронной почты в рамках требований к безопасности и соответствию требованиям к обмену сообщениями. Проверив вложения, вы можете с учетом их содержимого или характеристик выполнить действия над соответствующими сообщениями. Ниже перечислены некоторые задачи, связанные с вложениями, которые можно выполнять при помощи правил транспорта.

- Поиск файлов в сжатых вложениях, таких как `.zip` и `.rar` , и, если есть текст, соответствующий указанному шаблону, добавьте заявление об отказе в конце сообщения.
- Изучение содержимого вложений и перенаправление сообщения модератору на утверждение перед доставкой, если во вложении найдены указанные ключевые слова.
- Проверка наличия сообщения с вложениями, которые невозможно изучить, и блокировка отправки всего сообщения.
- Проверьте наличие вложений, размер которых превышает определенный размер, а затем сообщите отправителю о проблеме, если вы решили предотвратить доставку сообщения.
- Создание уведомлений для пользователей, отправляющих сообщение, которое подпадает под действие правила потока обработки почты.
- Блокирование всех сообщений с вложениями. Примеры см. в статье Common attachment blocking scenarios.

Администраторы Exchange могут создавать правила потока обработки почты, перейдя в раздел**Правилапотока обработки почты**>**в Центре**> администрирования Exchange. Для выполнения этой процедуры необходимы соответствующие разрешения. После создания нового правила можно просмотреть полный список условий, связанных с вложением, выбрав **Дополнительные параметры**>**Любое вложение** в разделе **Применить это правило, если**. Параметры, связанные с вложениями, показаны на следующем рисунке.



Дополнительные сведения о правилах потока обработки почты, включая полный набор условий и действий, которые можно выбрать, см. в статье Правила потока обработки почты (правила транспорта) в Exchange Server. Exchange Online Protection (EOP) и гибридные клиенты могут воспользоваться правилами потока обработки почты, приведенными в разделе Рекомендации по настройке EOP. Если вы готовы приступить к созданию правил, см. статью Процедуры для правил потока обработки почты в Exchange Server.

Проверка содержимого вложений

Проверять содержимое почты можно с помощью условий правил транспорта, указанных в приведенной ниже таблице. При этом анализируются только первые 150 КБ вложения. Чтобы начать использовать эти условия при проверке сообщений, необходимо добавить их в правило потока обработки почты. Сведения о создании или изменении правил см. в статье Процедуры для правил потока обработки почты в Exchange Server.

Развернуть таблицу

Имя условия в Центре администрирования Exchange	Имя условия в командной консоли	Описание
Содержимое вложения содержит любое из этих слов	`AttachmentContainsWords`	Это условие сопоставляет сообщения с поддерживаемыми типами файлов вложений, содержащими заданную строку или группу символов.
Все содержимое вложения соответствует эти текстовые шаблоны	`AttachmentMatchesPatterns`	Это условие сопоставляет сообщения с поддерживаемыми типами файлов вложений, которые содержат текстовый шаблон, соответствующий заданному регулярному выражению.

Имена командной консоли Exchange для перечисленных здесь условий являются параметрами `TransportRule` , для которых требуется командлет .

- Дополнительные сведения о командлете см. в статье New-TransportRule.
- Дополнительные сведения о типах свойств для этих условий см. в статье Условия правил потока обработки почты и исключения (предикаты) в Exchange Server.

Правила потока обработки почты могут проверять только содержимое поддерживаемых типов файлов. Если агент правил потока обработки почты обнаруживает вложение, которое отсутствует в списке поддерживаемых типов файлов, `AttachmentIsUnsupported` активируется условие. Поддерживаемые типы файлов перечислены в следующем разделе. Любой файл, не указанный в списке `AttachmentIsUnsupported` , активирует условие .

Сжатые архивные файлы

Если сообщение содержит сжатый архивный файл, например `.zip` файл или `.cab` , агент правил потока обработки почты проверит файлы, содержащиеся в этом вложении. Такие сообщения обрабатываются способом, схожим с обработкой сообщений с несколькими вложениями. Свойства сжатых архивных файлов не проверяются. Например, если тип файла-контейнера поддерживает примечания, это поле не просматривается.

Поддерживаемые типы файлов для проверки содержимого с помощью правил транспорта

В следующей таблице перечислены типы файлов, поддерживаемые правилами потока обработки почты. Система автоматически обнаруживает типы файлов, проверяя свойства файла, а не фактическое расширение имени файла. Такое поведение помогает предотвратить обход фильтрации правил потока почты хакерами путем переименования расширения файла. Список типов файлов с исполняемым кодом, которые можно проверить в контексте правил потока обработки почты, приведен далее в этом разделе.

Начиная с выпуска Exchange Server 2019 CU15 (2025H1), Exchange Server использует DocParser вместо Oracle Outside In Technology. В этом обновлении также добавлена поддержка дополнительных типов файлов. Если вы используете Exchange Server 2019 CU15 или более поздней версии, можно проверить следующие типы файлов:

Развернуть таблицу

Категория	Расширение файла	Примечания
Adobe PDF	PDF	Нет
Сжатые архивные файлы	`.arj, .bz2, .cab, .chm, .gz, .gzip, .lha, .lzh, .lzma, .mhtml, .msp, .rar, .rar4, .tar, .xar, .xz, .zip, .7z`	Нет
HTML	`.ascx, .asp, .aspx, .css, .hta, .htm, .html, .htw, .htx, .jhtml`	Нет
JSON	`.adaptivecard, .json, .messagecard`	Нет
Почта	`.eml, .msg, .nws`	Нет
Microsoft Office	`.doc, .docb, .docm, .docx, .dot, .dotm, .dotx, .obd, .obt, .one, .pot, .potm, .potx, .ppa, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .xlb, .xlc, .xlm, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw`	Содержимое любых внедренных частей в файлах этих типов также проверяется. Однако объекты, которые не внедренные (например, связанные документы), не проверяются. Содержимое в пользовательских свойствах также сканируется.

Категория	Расширение файла	Примечания
Microsoft Office xml	`.excelml, .powerpointml, .wordml`	Нет
Microsoft Visio	`.vdw, .vdx, .vsd, .vsdm, .vsdx, .vss, .vssm, .vssx, .vst, .vstm, .vstx, .vsx, .vtx`	Нет
OpenDocument	`.odp, .ods, .odt`	Части ODF-файлов не обрабатываются. Например, если ODF-файл содержит внедренный документ, содержимое внедренного документа не просматривается.
Прочее	`.dfx, .dxf, .encoffmetro, .fluid, .mime, .pointpub, .pub, .rtf, .vtt, .xps`	Нет
Текст	`.asm, .bat, .c, .class, .cmd, .cpp, .cs, .csv, .cxx, .def, .dic, .h, .hpp, .hxx, .ibq, .idl, .inc, .inf, .ini, .inx, .java, .js, .json, .lnk, .log, .m3u, messagestorage, .mpx, .php, .pl, .pos, .tsv, .txt, .vcf, .vcs`	Сканируются и другие текстовые файлы. Этот список является репрезентативным.
XML	`.infopathml, .jsp, .mspx, .xml`	Нет

Если вы используете версию, более раннюю, чем Exchange Server 2019 CU15 (2025H1), можно проверить следующие типы файлов:

Развернуть таблицу

Категория	Расширение файла	Примечания
Office 2013, Office 2010 и Office 2007	`.docm, .docx, .pptm, .pptx, .pub, .one, .xlsb, .xlsm, .xlsx`	Файлы Microsoft OneNote и Microsoft Publisher не поддерживаются по умолчанию. Поддержку этих типов файлов можно включить с помощью интеграции IFilter. Дополнительные сведения см. в разделе Регистрация пакетов фильтров IFilters в Exchange Server. Содержимое любых внедренных частей в файлах этих типов также проверяется. Однако объекты, которые не внедренные

Категория	Расширение файла	Примечания
		(например, связанные документы), не проверяются.
Office 2003	`.doc, .ppt, .xls`	Нет
Дополнительные файлы Office	`.rtf, .vdw, .vsd, .vss, .vst`	Нет
Adobe PDF	`.pdf`	Нет
HTML	`.html`	Нет
XML	`.xml`	Нет
Текст	`.txt, .asm, .bat, .c, .cmd, .cpp, .cxx, .def, .dic, .h, .hpp, .hxx, .ibq, .idl, .inc, inf, .ini, inx, .js, .log, .m3u, .pl, .rc, .reg, .vbs, .wt`	Нет
OpenDocument	`.odp, .ods, .odt`	Части ODF-файлов не обрабатываются. Например, если ODF-файл содержит внедренный документ, содержимое внедренного документа не просматривается.
Чертеж AutoCAD	`.dxf`	Файлы AutoCAD 2013 не поддерживаются. **Заметка:** Типы файлов больше не могут проверяться после установки su Exchange Server марта 2024 г.
Image	`.jpg, .tiff`	Проверяется только текст метаданных, связанный с этими файлами изображений. Оптическое распознавание символов отсутствует. **Заметка:** Типы файлов больше не могут проверяться после установки su Exchange Server марта 2024 г.

Проверка свойств файла вложения

Следующие условия правила потока обработки почты проверяют свойства файла, вложенного в сообщение. Чтобы начать использовать эти условия при проверке сообщений, необходимо добавить их в правило потока обработки почты. Список

поддерживаемых типов файлов с исполняемым кодом, которые можно проверить в контексте правил потока обработки почты, приведен здесь. Дополнительные сведения о создании или изменении правил см. в разделе Процедуры для правил потока обработки почты в Exchange Server.

Развернуть таблицу

Имя условия в Центре администрирования Exchange	Имя условия в командной консоли	Описание
Имя любого файла вложения соответствует этим текстовым шаблонам	`AttachmentNameMatchesPatterns`	Это условие сопоставляет сообщения с поддерживаемыми типами файлов вложений, если имя таких вложений содержит указанные символы.
Расширение любого файла вложения включает эти слова	`AttachmentExtensionMatchesWords`	Это условие сопоставляет сообщения с поддерживаемыми типами файлов вложений, если расширение имени файла соответствует указанному.
Размер любого вложения равен или превышает	`AttachmentSizeOver`	Это условие соответствует сообщениям с поддерживаемыми типами файлов вложений, если их размер больше указанного.
Любое вложение, проверка которого не завершена	`AttachmentProcessingLimitExceeded`	Это условие соответствует сообщениям, если вложение не проверяется агентом правил потока обработки почты.
Любое вложение содержит исполняемое содержимое	`AttachmentHasExecutableContent`	Это условие сопоставляет сообщения, которые содержат исполняемые файлы в виде вложений. В этом разделе перечислены поддерживаемые типы файлов.
Любое вложение защищено паролем	`AttachmentIsPasswordProtected`	Это условие соответствует сообщениям с поддерживаемыми типами

Имя условия в Центре администрирования Exchange	Имя условия в командной консоли	Описание
		файлов вложений, если они защищены паролем.

Имена командной консоли Exchange для перечисленных здесь условий являются параметрами `TransportRule` , для которых требуется командлет .

- Дополнительные сведения о командлете см. в статье New-TransportRule.
- Дополнительные сведения о типах свойств для этих условий см. в статье Условия правил потока обработки почты и исключения (предикаты) в Exchange Server.

Поддерживаемые типы исполняемых файлов для проверки правилами транспорта

Агент транспорта использует обнаружение подлинных типов, изучая свойства, а не только расширение файла. Это позволяет предотвратить обход правила хакерами путем переименования расширения файла. В таблице ниже перечислены типы исполняемых файлов, которые поддерживают эти условия. Если найден файл, не указанный здесь, `AttachmentIsUnsupported` активируется условие.

Развернуть таблицу

Тип файла	Собственное расширение
32-разрядный исполняемый файл Windows с расширением библиотеки динамической компоновки.	`.dll`
Самораспаковывающийся исполняемый файл.	`.exe`
Исполняемый файл для удаления.	`.exe`
Файл ярлыка программы.	`.exe`
32-разрядный исполняемый файл Windows.	`.exe`
Файл документа Microsoft Visio в формате XML.	`.vxd`
Файл операционной системы OS/2.	`.os2`
16-разрядный исполняемый файл Windows.	`.w16`

Тип файла	Собственное расширение
Файл дисковой операционной системы.	`.dos`
Стандартный файл антивирусной проверки Европейского Института исследования Антивирусных Программ.	`.com`
Файл сведений о программе Windows.	`.pif`
Исполняемый файл Windows.	`.exe`

> **ⓘ Важно!**
>
> `.rar` (самораспаковывающиеся архивные файлы, созданные с помощью архивировщика WinRAR), `.jar` (архивные файлы Java) и `.obj` (скомпилированные файлы исходного кода, трехмерные объекты или файлы последовательностей) **не** считаются исполняемыми типами файлов. Чтобы заблокировать эти файлы, можно использовать правила потока обработки почты, которые ищут файлы с этими расширениями, как описано выше в этой статье.

Расширение количества поддерживаемых типов файлов

Поддерживаемые типы файлов, перечисленные в этом разделе, можно изменить в любое время с помощью интеграции IFilter. Дополнительные сведения см. в разделе Регистрация пакетов фильтров IFilters в Exchange Server.

Типы файлов, добавляемых с помощью этого процесса, становятся поддерживаемыми типами файлов и больше не активируют `AttachmentIsUnsupported` условие.

Политики защиты от потери данных и правила потока обработки почты для вложений

Чтобы упростить управление важными бизнес-данными в электронной почте, вы можете добавить любые связанные с вложениями условия вместе с правилами политики защиты от потери данных (DLP). Например, можно разрешить отправку

сообщений с номерами паспортов, только если эти данные находятся во вложении, защищенном паролем. Для этого выполните следующие действия.

- Создайте политику DLP, которая проверяет сообщения на наличие конфиденциальных данных, связанных с паспортами. Дополнительные сведения см. в статье Защита от потери данных в Exchange Server.
- Добавьте исключение **Любое вложение, защищенное паролем**, в область Правила потока обработки почты **Кроме если...**
- Определите действие, выполняемое с почтой, содержащей номера паспортов, которых нет в защищенном файле.

Политики защиты от потери данных и условия, связанные с вложениями, могут помочь вам обеспечить соблюдение бизнес-потребностей, определив их как условия правил потока обработки почты, исключения и действия. При включении проверки конфиденциальной информации в политику защиты от потери данных все вложения к сообщениям проверяются только на наличие этой информации. Однако условия, связанные с вложением, такие как размер или тип файла, не включаются до тех пор, пока вы не добавите условия, перечисленные в этом разделе. Защита от потери данных доступна не во всех версиях Exchange; Дополнительные сведения см. в разделе Защита от потери данных.

Папка "Элементы с возможностью восстановления" в Exchange Server

Статья • 04.04.2023

Чтобы защититься от случайного или злонамеренного удаления и упростить усилия по обнаружению, обычно предпринимаемые до или во время судебного разбирательства или расследования, Exchange Server и Exchange Online использовать папку "Элементы с возможностью восстановления". Папка "Элементы с возможностью восстановления" заменяет функцию, которая в более ранних версиях Exchange называлась *мусорной корзиной* . Папку "Элементы с возможностью восстановления" используют следующие функции Exchange:

- Хранение удаленного элемента
- Восстановление отдельных элементов
- Хранение на месте
- Хранение для судебного разбирательства
- Ведение журнала аудита почтового ящика
- Журнал календаря

Терминология

Знание следующих терминов поможет получить общее представление о сведениях, приводимых в этом разделе.

Удаление

> Описывает операцию, при которой элемент перемещается из какой-либо папки в папку "Удаленные", настроенную по умолчанию.

Обратимое удаление

> Описывает, когда элемент удаляется из папки по умолчанию "Удаленные" и помещается в папку "Элементы с возможностью восстановления". Также описывается, когда пользователь Outlook удаляет элемент, нажав клавиши SHIFT+DELETE, который обходит папку "Удаленные" и помещает элемент непосредственно в папку "Элементы с возможностью восстановления".

Необратимое удаление

> Описывает операцию, при которой элемент помечается для удаления из базы данных почтовых ящиков. Такое действие также называется *необратимым удалением из хранилища*.

Папка "Элементы с возможностью восстановления"

Каждый почтовый ящик состоит из обычных, видимых папок, например "Входящие", Календарь и "Отправленные" и внутренних данных, параметров и других рабочих данных о почтовом ящике. Папка "Элементы с возможностью восстановления" относится к последним. Они не видны пользователям, работающим с Outlook, Outlook в Интернете или другими почтовыми клиентами.

Указанное изменение архитектуры обеспечивает следующие преимущества.

- Если почтовый ящик перемещается в другую базу данных почтовых ящиков, папка корзины перемещается вместе с ним.
- Папка "Элементы с возможностью восстановления" индексируется службой поиска Exchange и может быть обнаружена с помощью обнаружения электронных данных на месте.
- Папка "Элементы с возможностью восстановления" имеет свою собственную квоту хранения данных.
- Сервер Exchange может препятствовать удалению данных из папки корзины.
- На сервере Exchange доступно отслеживание изменений определенного содержимого.

Папка "Элементы с возможностью восстановления" содержит следующие подпапки.

- **Удаления**. Эта вложенная папка содержит все элементы, удаленные из папки "Удаленные". (В Outlook пользователь может обратимо удалить элемент, нажав клавиши SHIFT+DELETE.) Эта вложенная папка предоставляется пользователям с помощью функции Восстановить удаленные элементы в Outlook и Outlook в Интернете.
- **Версии**. Если включена In-Place удержание или удержание для судебного разбирательства, эта вложенная папка содержит исходные и измененные

копии удаленных элементов. Эта папка не отображается для конечных пользователей.

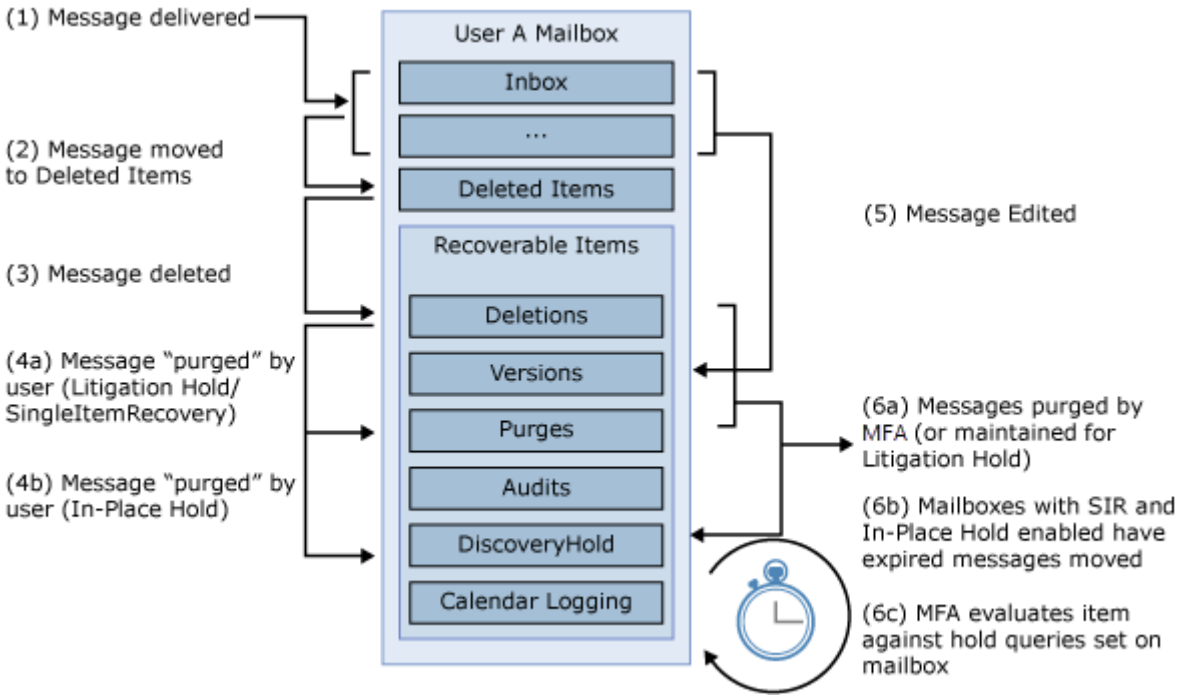
- **Очистки**. Если включена поддержка судебного разбирательства или восстановление одного элемента, эта вложенная папка содержит все элементы, которые жестко удалены. Эта папка не отображается для конечных пользователей.

- **Аудиты**. Если ведение журнала аудита почтового ящика включено для почтового ящика, эта вложенная папка содержит записи журнала аудита. Дополнительные сведения о ведении журнала аудита почтовых ящиков см. в статье Ведение журнала аудита почтовых ящиков в Exchange Server.

- **DiscoveryHolds**: если включено In-Place удержание, эта вложенная папка содержит все элементы, которые соответствуют параметрам запроса на удержание и жестко удаляются.

- **Ведение журнала календаря**. Эта вложенная папка содержит изменения календаря, происходящие в почтовом ящике. Эта папка не отображается для пользователей.

На следующем рисунке показаны подпапки в папке корзины. Кроме того, указаны хранение удаленных элементов, восстановление отдельных элементов и рабочие процессы хранения, описанные в следующих разделах.



Хранение удаленного элемента

Элемент считается обратимо удаленным в следующих случаях.

- Пользователь удаляет один или все элементы из папки "Удаленные".
- Пользователь нажимает сочетание клавиш SHIFT+DELETE, чтобы удалить элемент из любой другой папки почтового ящика.

Элементы, к которым было применено обратимое удаление, перемещаются в подпапку "Удаленные" папки "Элементы для восстановления". Это обеспечивает дополнительный уровень защиты, поэтому пользователи могут восстановить удаленные элементы, не прибегая к помощи службы поддержки. Пользователи могут использовать функцию "Восстановление удаленных элементов" в Outlook или Outlook в Интернете для восстановления удаленного элемента. Эту же функцию можно использовать для окончательного удаления элемента. Дополнительные сведения см. в разделе:

- Восстановление удаленных элементов в Outlook для Windows
- Восстановление удаленных элементов или электронных сообщений в Outlook в Интернете

Элементы остаются в подпапке "Удаленные" до тех пор, пока не истечет период их хранения. По умолчанию период хранения удаленных элементов в базе данных почтовых ящиков равен 14 дням. Указанное значение можно изменить для всей базы данных или конкретного почтового ящика. Помимо периода хранения удаленных элементов, в отношении папки корзины применяются квоты. Дополнительные сведения см. в статье Квоты почтовых ящиков с возможностью восстановления далее в этом разделе.

По истечении срока хранения удаленного элемента элемент полностью удаляется из Exchange Server.

Параметр *Не удалять элементы без возможности восстановления, пока не будет создана резервная копия базы данных* , может повлиять на это поведение. Если этот параметр не включен (по умолчанию), для удаления элементов из вложенной папки Удаления считается только период хранения удаленных элементов. Если этот параметр включен и достигнут срок хранения удаленных элементов, элементы не удаляются до тех пор, пока не будет создана резервная копия базы данных почтовых ящиков, в которой находится почтовый ящик.

Дополнительные сведения об этих параметрах и способах их изменения см. в статье Настройка хранения удаленных элементов и квот на элементы с возможностью восстановления.

Восстановление отдельных элементов

Если элемент удаляется из вложенной папки Удаления, либо пользователем, очищающим элемент с помощью функции "Восстановить удаленные элементы", либо автоматическим процессом, например помощником по управляемым папкам (например, тег хранения, для удаления навсегда), пользователь не сможет восстановить элемент. В более ранних версиях Exchange для восстановления таких элементов администратору требовалось восстановить из резервных копий базу данных почтовых ящиков или отдельный почтовый ящик. Такие действия, как правило, задерживали процедуру восстановления на несколько минут или часов в зависимости от используемого механизма резервного копирования.

В Exchange Server можно использовать *восстановление одного элемента* для восстановления элементов без использования носителя резервного копирования для восстановления баз данных почтовых ящиков. Это приводит к значительно более коротким периодам восстановления. Если для почтового ящика включено восстановление одного элемента, любой элемент, удаленный из вложенной папки Deletes до периода хранения удаленного элемента, перемещается во вложенную папку Очистки. Когда помощник по управляемым папкам обрабатывает папку "Элементы с возможностью восстановления" для почтового ящика с включенным восстановлением одного элемента, любой элемент во вложенной папке Очистки не очищается, если срок хранения удаленных элементов не истек для этого элемента.

В следующей таблице перечислены данные и действия, которые можно выполнять в папке корзины, если включена функция восстановления отдельных элементов.

Папка корзины и восстановление отдельных элементов

Состояние восстановления отдельных элементов	**Папка "Элементы с возможностью восстановления" содержит обратимо удаленные элементы**	**Папка "Элементы для восстановления" содержит необратимо удаленные элементы**	**Пользователи могут удалять элементы из папки "Элементы с возможностью восстановления"**	**Помощник для управляемых папок автоматически удаляет элементы из папки корзины**

Состояние восстановления отдельных элементов	Папка "Элементы с возможностью восстановления" содержит обратимо удаленные элементы	Папка "Элементы для восстановления" содержит необратимо удаленные элементы	Пользователи могут удалять элементы из папки "Элементы с возможностью восстановления"	Помощник для управляемых папок автоматически удаляет элементы из папки корзины
Включена	Да	Да	Нет	Да. По умолчанию все элементы удаляются через 14 дней за исключением элементов календаря, которые удаляются через 120 дней.
Отключено	Да	Нет	Да	Да. По умолчанию все элементы удаляются через 14 дней за исключением элементов календаря, которые удаляются через 120 дней. Если до истечения периода хранения удаленных элементов достигается квота предупреждения элементов для восстановления, сообщения удаляются в порядке их поступления (ФИФО).

В Exchange Server восстановление одного элемента по умолчанию не включено для новых почтовых ящиков или почтовых ящиков, перемещенных из предыдущей версии Exchange. Необходимо использовать командную консоль Exchange, чтобы включить восстановление одного элемента для почтового ящика, а затем настроить или изменить период хранения удаленных элементов. Дополнительные сведения о восстановлении одного элемента см. в разделе Восстановление удаленных сообщений в почтовом ящике пользователя.

Удержание на месте и хранение для судебного разбирательства

В Exchange Server и Exchange Online диспетчеры обнаружения могут использовать In-Place обнаружения электронных данных с делегированными разрешениями группы ролей Управления обнаружением для выполнения поиска содержимого почтового ящика. В Exchange Server и Exchange Online можно использовать удержание In-Place для сохранения элементов почтовых ящиков, соответствующих параметрам запроса, и защиты элементов от удаления пользователями или автоматизированными процессами. Вы также можете использовать удержание для судебного разбирательства для сохранения всех элементов в почтовых ящиках пользователей и защиты элементов от удаления пользователями или автоматизированными процессами.

Помещение почтового ящика в In-Place удержание или удержание для судебного разбирательства не позволяет помощнику по управляемым папкам автоматически очищать сообщения из вложенных папок DiscoveryHolds, Удаления и Очистки. Кроме того, для почтового ящика также включена защита страницы копирования при записи. Защита страницы копирования при записи создает копию исходного элемента перед записью изменений в хранилище Exchange. После удаления почтового ящика из удержания помощник по управляемым папкам возобновляет автоматическую очистку.

> ⓘ **Примечание**
>
> Если вы помещаете почтовый ящик как на In-Place удержание, так и на удержание для судебного разбирательства, то предпочтение отдается удержанию всего почтового ящика.

В следующей таблице перечислены данные и действия, которые можно выполнять в папке корзины, если включено хранение для судебного разбирательства.

Папка корзины и хранение

Состояние хранения	Папка "Элементы с возможностью восстановления" содержит обратимо удаленные элементы	Папка "Элементы для восстановления" содержит измененные и необратимо удаленные элементы	Пользователи могут удалять элементы из папки "Элементы с возможностью восстановления"	Помощник для управляемых папок автоматически удаляет элементы из папки корзины
Включена	Да	Да	Нет	Нет
Отключено	Да	Нет	Да	Да

Дополнительные сведения об обнаружении электронных данных на месте, хранении на месте и хранении для судебного разбирательства см. в следующих статьях:

- Обнаружение электронных данных на месте в Exchange Server
- Удержание на месте и удержание для судебного разбирательства в Exchange Server

Защита страниц от копирования при записи и измененные элементы

Если пользователь, для которого включено хранение на месте или хранение для судебного разбирательства, изменяет конкретные свойства элемента почтового ящика, перед сохранением изменений создается копия исходного элемента почтового ящика. Исходная копия сохраняется в подпапке "Версии". Такой процесс называется *защитой страниц на основе копирования при записи*. Защита страниц от копирования при записи применяется к элементам, находящимся в любой папке почтового ящика. Подпапка "Версии" не отображается для пользователей.

В следующей таблице перечислены свойства сообщений, которые включают функцию защиты страниц от копирования при записи.

Свойства, активирующие функцию защиты страниц на основе копирования при записи

Тип элемента	Свойства, активирующие функцию защиты страниц на основе копирования при записи

Тип элемента	Свойства, активирующие функцию защиты страниц на основе копирования при записи
Сообщения (IPM.Note*) Сообщения (IPM.Post*)	Subject • Текст сообщения • Вложения • Отправители и получатели • Даты отправки и получения
Элементы, отличные от сообщений	Любые изменения видимых свойств за исключением следующих: • Расположение элемента (когда элемент перемещается между папками) • Изменение состояния элемента (прочитан или не прочитан) • Изменения тега хранения, применяемого к элементу
Элементы в папке "Черновики" по умолчанию	Нет. На элементы в папке "Черновики" не распространяется действие функции защиты страниц от копирования при записи.

> ⓘ **Важно!**
>
> Функция защиты страниц от копирования при записи не сохраняет версию собрания, если его организатор получает ответы от участников и обновляются сведения об отслеживании собрания. Кроме того, функцией защиты страниц от копирования при записи не фиксируются изменения в RSS-каналах.

Когда почтовый ящик больше не находится на хранении на месте или хранении для судебного разбирательства, копии измененных элементов, которые хранятся в папке "Версии", удаляются.

Квоты почтового ящика элементов для восстановления

Когда элемент перемещается в папку корзины, его размер вычитается из квоты почтового ящика и добавляется к размеру этой папки. В Exchange Server базы данных почтовых ящиков имеют настраиваемую квоту предупреждений о восстанавливаемых элементах (*мягкое ограничение*) в размере 20 ГБ и квоту на восстанавливаемые элементы (*жесткое ограничение*) в 30 ГБ. По умолчанию указанные предельные значения наследуются всеми почтовыми ящиками в базе данных. Тем не менее можно настроить отдельные почтовые ящики с другими

квотами. Дополнительные сведения см. в статье Настройка хранения удаленных элементов и квот на элементы с возможностью восстановления.

В Exchange Online ограничения по умолчанию для квоты элементов с возможностью восстановления такие же, как и Exchange Server: мягкое ограничение в 20 ГБ и жесткое ограничение в 30 ГБ. Однако при помещении почтового ящика на хранение для судебного разбирательства или хранение на месте, квоты папки элементов для восстановления автоматически увеличиваются до 90 и 100 ГБ соответственно.

Когда размер папки корзины почтового ящика достигает соответствующей квоты, в ней будет невозможно сохранять дополнительные элементы. Это влияет на функции почтового ящика следующим образом.

- Пользователи почтового ящика не могут удалять элементы.
- Помощник для управляемых папок не может удалять элементы на основе тега хранения или параметров управляемых папок.
- В случае почтовых ящиков, для которых задано хранение для судебного разбирательства, хранение на месте или восстановление отдельных элементов, защита страниц на основе копирования при записи не обеспечивает поддержку версий элементов, изменяемых пользователем.
- Для почтовых ящиков с включенным ведением журнала аудита в подпапке "Аудиты" невозможно сохранить записи журнала аудита почтового ящика.

Если почтовый ящик не помещен на хранение на месте или хранение для судебного разбирательства, помощник по обслуживанию управляемых папок автоматически очищает содержимое папки "Элементы с возможностью восстановления" после окончания срока хранения удаленных элементов. Если для папки достигнуто ограничение по квоте предупреждения, помощник автоматически удаляет элементы в порядке ФИФО.

Когда папка "Элементы с возможностью восстановления" достигает мягкого и жесткого предела по умолчанию, вы получите уведомление с помощью журнала событий и оповещения Microsoft System Center Operations Manager. Такое предупреждение появляется, когда размер папки "Элементы для восстановления" впервые достигает установленных по умолчанию строгих и нестрогих квот, а затем выводится один раз в день.

В следующей таблице перечислены события, регистрируемые в журнале, когда размер папки корзины достигает установленных по умолчанию строгих и нестрогих квот.

Предупреждения и ошибки, связанные с квотой элементов для восстановления

Идентификатор события	Тип	Source	Сообщение
10024	Предупреждение	Хранилище почтовых ящиков MSExchangeIS	Почтовый ящик *для пользователя> почтового ящика (GUID) превысил квоту предупреждений для элементов, доступных для*< восстановления.>< Удалите эти элементы или увеличьте квоту. Если будет превышена квота элементов для восстановления, пользователь не сможет удалять элементы из почтового ящика.
10023	Ошибка	Хранилище почтовых ящиков MSExchangeIS	Почтовый ящик для *<пользователя> почтового ящика* (<*GUID*>) превысил максимальную квоту элементов с возможностью восстановления. Удалять элементы из этого почтового ящика невозможно. Необходимо как можно скорее сообщить об этом владельцу почтового ящика. Удалите элементы с возможностью восстановления или увеличьте квоту.

Идентификатор события	Тип	Source	Сообщение
10023	Предупреждение	MSExchangeMailboxAssistants	В почтовом ящике *<mailbox user>* превышено ограничение по квоте предупреждения на размер папки "Элементы с возможностью восстановления". Чтобы не допустить сбоя в почтовом ящике, элементы с возможностью восстановления удалены. Квота предупреждения элементов для восстановления: 20 ГБ (21 474 836 480 байт); исходный размер папки "Элементы с возможностью восстановления": 21475005311; текущий размер папки "Элементы с возможностью восстановления": 21474823820; статистика папки: - Обработанные папки: RecoverableItemsRoot, RecoverableItemsVersions, RecoverableItemsPurges, RecoverableItemsDeletions; исходные размеры папок: 21391661934, 55190914, 1987247, 26157788 (число элементов: 276828, 400, 84, 646); текущие размеры папок: 21391480443, 55190914, 1987247, 26157788 (число элементов: 276817, 400, 84, 646)

Если почтовый ящик помещен на хранение на месте или хранение для судебного разбирательства, защита страниц на основе копирования при записи недоступна.

Чтобы версии измененных элементов сохранялись, необходимо сократить размер папки "Элементы с возможностью восстановления". Вы можете скопировать сообщения из папки "Элементы с возможностью восстановления" в почтовый ящик найденных сообщений с помощью командлета Search-Mailbox, а затем удалить их. Кроме того, вы можете увеличить квоту элементов для восстановления для почтового ящика. Дополнительные сведения см. в статье Очистка или удаление элементов из папки "Элементы с возможностью восстановления".

Дополнительные сведения

- Копирование при записи возможно, только если к почтовому ящику применено хранение на месте или хранение для судебного разбирательства.
- Если пользователям требуется восстановить удаленные элементы из папки корзины, рекомендуем ознакомиться со следующими статьями:
  - Восстановление удаленных элементов в Outlook для Windows
  - Восстановление удаленных элементов или электронной почты в Outlook в Интернете

Удаление элементов из папки "Элементы с возможностью восстановления"

Статья • 04.04.2023

Папка "Элементы с возможностью восстановления" (известная в более ранних версиях Exchange как *контейнер*) существует для защиты от случайного или злонамеренного удаления и для облегчения усилий по обнаружению, обычно проводимых до или во время судебного разбирательства или расследования.

Процедура очистки папки "Элементы с возможностью восстановления" зависит от того, находится ли почтовый ящик на хранении на месте или хранении для судебного разбирательства и включено ли для него восстановление отдельных элементов.

- Если эти функции отключены, вы можете просто удалить элементы из папки "Элементы с возможностью восстановления". После этого восстановление отдельных элементов будет невозможно.
- Если эти функции включены, важно сохранить данные почтовых ящиков до их отключения. В этом случае для очистки папки "Элементы с возможностью восстановления" необходимо выполнить более сложные действия.

Дополнительные сведения о удержании In-Place и удержании для судебного разбирательства см. в статье Удержание на месте и удержание для судебного разбирательства в Exchange Server. Дополнительные сведения о восстановлении одного элемента см. в разделе Восстановление одного элемента в папке "Элементы с возможностью восстановления" в Exchange Server.

Что нужно знать перед началом работы

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Удаление содержимого почтового ящика" в разделе Политика обмена сообщениями и разрешения соответствия требованиям в Exchange Server.
- Так как некорректная очистка папки элементов для восстановления может привести к потере данных, важно ознакомиться с принципом работы этой папки и последствиями удаления ее содержимого. Перед выполнением этой

процедуры рекомендуется просмотреть сведения в папке "Элементы с возможностью восстановления" в Exchange Server.

- Для выполнения этих процедур нельзя использовать Центр администрирования Exchange. Необходимо использовать командную консоль Exchange. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: Exchange Server, Exchange Online или Exchange Online Protection.

Удаление элементов из папки "Элементы с возможностью восстановления" для почтовых ящиков, для которых не включено хранение или восстановление отдельных элементов, с помощью Командная консоль Exchange

В этом примере элементы удаляются из папки "Элементы с возможностью восстановления" пользователя Gurinder Singh, а также копируются в папку GurinderSingh-RecoverableItems в почтовом ящике Discovery Search Mailbox (почтовый ящик найденных сообщений, созданный программой установки Exchange).

PowerShell

```
Search-Mailbox -Identity "Gurinder Singh" -SearchDumpsterOnly -TargetMailbox "Discovery Search Mailbox" -TargetFolder "GurinderSingh-RecoverableItems" -DeleteContent
```

Примечание

Чтобы удалить элементы из почтового ящика, не копируя их в другой почтовый ящик, используйте предыдущую команду без параметров *TargetMailbox* и *TargetFolder* .

Дополнительные сведения о синтаксисе и параметрах см. в разделе Search-Mailbox.

Очистка папки "Элементы с возможностью восстановления" для почтовых ящиков, для которых включено хранение или восстановление отдельных элементов, с помощью командной консоли Exchange

Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Удаление содержимого почтового ящика" в разделе Политика обмена сообщениями и разрешения соответствия требованиям в Exchange Server.

Если для почтового ящика достигнуто ограничение по квоте элементов для восстановления, рекомендуем увеличить квоту и не удалять элементы из папки. Вы также можете отслеживать события, связанные с квотой предупреждения элементов для восстановления, в журнале приложений и предпринимать необходимые меры, например увеличивать квоту или анализировать увеличение размера папки "Элементы с возможностью восстановления" в почтовых ящиках.

Если ограничения хранилища или аналогичные проблемы не позволяют увеличить квоту на элементы с возможностью восстановления, рекомендуется сначала скопировать данные из папки "Элементы с возможностью восстановления" пользователя в другой почтовый ящик перед удалением сообщений. Если вы удаляете элементы из-за ограничений хранилища на одном томе, вы можете скопировать элементы в почтовый ящик, расположенный на томе с достаточным объемом хранилища.

В этой процедуре элементы копируются из папки "Элементы с возможностью восстановления" пользователя Gurinder Singh в папку GurinderSingh-RecoverableItems в почтовом ящике Discovery Search Mailbox. Прежде чем копировать и удалять элементы из папки "Элементы с возможностью восстановления", убедитесь, что элементы не удалены из указанной папки. После копирования элементов в почтовый ящик найденных сообщений или резервный почтовый ящик и очистки папки можно вернуться к предыдущим параметрам почтового ящика.

1. Получите значения следующих параметров квоты. Обязательно запишите значения, чтобы можно было вернуть их после очистки папки элементов для

восстановления:

- *RecoverableItemsQuota*
- *RecoverableItemsWarningQuota*
- *ProhibitSendQuota*
- *ProhibitSendReceiveQuota*
- *UseDatabaseQuotaDefaults*
- *RetainDeletedItemsFor*
- *UseDatabaseRetentionDefaults*

> ⓘ **Примечание**
>
> Если для параметра *UseDatabaseQuotaDefaults* задано значение `$true`, предыдущие параметры квоты не применяются. Соответствующие параметры квоты, настроенные в базе данных почтовых ящиков, применяются даже в том случае, если заполнены параметры отдельных почтовых ящиков.

PowerShell

```
Get-Mailbox "Gurinder Singh" | Format-List
*Quota*,RetainDeletedItemsFor,UseDatabaseRetentionDefaults
```

2. Получите параметры доступа к почтовому ящику. Обязательно запишите их значения для последующей настройки.

PowerShell

```
Get-CASMailbox "Gurinder Singh" | Format-List EwsEnabled,
ActiveSyncEnabled, MAPIEnabled, OWAEnabled, ImapEnabled, PopEnabled
```

3. Получите текущий размер папки элементов для восстановления. Запишите размер, чтобы можно было поднять квоты на шаге 6.

PowerShell

```
Get-MailboxFolderStatistics "Gurinder Singh" -FolderScope
RecoverableItems | Format-List Name,FolderAndSubfolderSize
```

4. Отключите клиентский доступ к почтовому ящику, чтобы обеспечить невозможность внесения изменений в данные почтового ящика на время данной процедуры.

```
PowerShell

Set-CASMailbox "Gurinder Singh" -EwsEnabled $false -ActiveSyncEnabled
$false -MAPIEnabled $false -OWAEnabled $false -ImapEnabled $false -
PopEnabled $false
```

5. Чтобы запретить удаление элементов из папки «Элементы для восстановления», увеличьте для этой папки стандартную квоту и квоту предупреждения, а для периода хранения удаленных элементов установите значение, которое превышает текущий размер пользовательской папки элементов для восстановления. Это особенно важно для сохранения сообщений из почтовых ящиков, к которым применено хранение для судебного разбирательства или хранение на месте. Рекомендуется увеличить значения этих параметров вдвое.

```
PowerShell

Set-Mailbox "Gurinder Singh" -RecoverableItemsQuota 50Gb -
RecoverableItemsWarningQuota 50Gb -RetainDeletedItemsFor 3650 -
ProhibitSendQuota 50Gb -ProhibitSendReceiveQuota 50Gb -
UseDatabaseQuotaDefaults $false -UseDatabaseRetentionDefaults $false
```

6. Остановите службу помощников по почтовым ящикам Microsoft Exchange и запретите ее запуск на сервере почтовых ящиков, выполнив следующие команды:

```
PowerShell

Stop-Service MSExchangeMailboxAssistants; Set-Service
MSExchangeMailboxAssistants -StartupType Disabled
```

Результатом этой команды является остановка помощника по управляемым папкам на сервере почтовых ящиков.

> ⓘ **Важно!**
>
> Если почтовый ящик находится в базе данных почтовых ящиков в группе обеспечения доступности баз данных (DAG), то необходимо отключить помощник для управляемых папок для каждого члена группы DAG, в

котором размещается копия этой базы данных. Если база данных переходит на другой сервер при сбое, то это предотвращает удаление данных почтовых ящиков помощником для управляемых папок на этом сервере.

7. Отключите функцию восстановления отдельных элементов и снимите почтовый ящик с хранения для судебного разбирательства.

```
PowerShell

Set-Mailbox "Gurinder Singh" -SingleItemRecoveryEnabled $false -
LitigationHoldEnabled $false
```

> ⓘ **Важно!**
>
> Когда команда запущена, включение восстановления отдельных элементов или хранения для судебного разбирательства может занять до одного часа. Переходить к следующему шагу рекомендуется только после завершения этого этапа.

8. Скопируйте элементы из папки элементов для восстановления в папку почтового ящика поиска на обнаружение и удалите содержимое исходного почтового ящика.

```
PowerShell

Search-Mailbox -Identity "Gurinder Singh" -SearchDumpsterOnly -
TargetMailbox "Discovery Search Mailbox" -TargetFolder "GurinderSingh-
RecoverableItems" -DeleteContent
```

Если необходимо удалить только сообщения, которые соответствуют указанным условиям, используйте параметр *SearchQuery* для указания условий. В этом примере выполняется удаление строки «Your bank statement» в поле **Тема**.

```
PowerShell

Search-Mailbox -Identity "Gurinder Singh" -SearchQuery "Subject:'Your
bank statement'" -SearchDumpsterOnly -TargetMailbox "Discovery Search
Mailbox" -TargetFolder "GurinderSingh-RecoverableItems" -DeleteContent
```

> ⓘ **Примечание**
>
> Копировать элементы в почтовый ящик поиска на обнаружение не требуется. Сообщения можно копировать в любой почтовый ящик. Тем не менее, чтобы запретить доступ к потенциально конфиденциальным данным почтовых ящиков, рекомендуется копировать сообщения в тот почтовый ящик, доступ к которому имеют только авторизованные диспетчеры записей. По умолчанию круг пользователей, имеющих доступ к почтовому ящику поиска на обнаружение по умолчанию, ограничен членами группы ролей управления обнаружением. Дополнительные сведения см. **в разделе Обнаружение электронных данных на месте в Exchange Server**.

9. Если к этому почтовому ящику ранее применялось хранение для судебного разбирательства или восстановление отдельных элементов, снова включите эти функции.

```
PowerShell

Set-Mailbox "Gurinder Singh" -SingleItemRecoveryEnabled $true -
LitigationHoldEnabled $true
```

> ⓘ **Важно!**
>
> Когда команда запущена, включение восстановления отдельных элементов или хранения для судебного разбирательства может занять до одного часа. Включать помощник для управляемых папок и разрешать клиентский доступ (шаги 11 и 12) рекомендуется только после завершения этого этапа.

10. Верните прежние значения квот, записанные на шаге 1:

    - *RecoverableItemsQuota*
    - *RecoverableItemsWarningQuota*
    - *ProhibitSendQuota*
    - *ProhibitSendReceiveQuota*
    - *UseDatabaseQuotaDefaults*

- *RetainDeletedItemsFor*
- *UseDatabaseRetentionDefaults*

В этом примере выполняется снятие почтового ящика с судебного удержания, для периода хранения удаленных элементов устанавливается значение 14 дней, а для квоты "Элементы с возможностью восстановления" настраивается использование того же значения, что и для базы данных почтовых ящиков. Если значения, указанные на шаге 1, отличаются, необходимо использовать предыдущие параметры, чтобы указать каждое значение и задать для параметра *UseDatabaseQuotaDefaults* значение `$false`. Если для параметров *RetainDeletedItemsForand UseDatabaseRetentionDefaults* ранее были заданы другие значения, то им также необходимо вернуть значения, записанные на шаге 1.

PowerShell

```
Set-Mailbox "Gurinder Singh" -RetentionHoldEnabled $false -
RetainDeletedItemsFor 14 -RecoverableItemsQuota unlimited -
UseDatabaseQuotaDefaults $true
```

11. Настройте службу помощников по почтовым ящикам Microsoft Exchange для автоматического запуска на сервере почтовых ящиков, выполнив следующие команды:

PowerShell

```
Set-Service MSExchangeMailboxAssistants -StartupType Automatic; Start-
Service MSExchangeMailboxAssistants
```

12. Включите клиентский доступ к почтовому ящику, выполнив следующую команду:

PowerShell

```
Set-CASMailbox -ActiveSyncEnabled $true -EwsEnabled $true -MAPIEnabled
$true -OWAEnabled $true -ImapEnabled $true -PopEnabled $true
```

Подробные сведения о синтаксисе и параметрах см. в таких разделах:

- Get-Mailbox
- Get-CASMailbox

- Get-MailboxFolderStatistics
- Set-CASMailbox
- Set-Mailbox
- Search-Mailbox

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно очистили папку "Элементы с возможностью восстановления" почтового ящика, используйте командлет Get-MailboxFolderStatistics , чтобы проверить размер папки "Элементы с возможностью восстановления".

В этом примере возвращается значение, указывающее размер этой папки и ее вложенных папок, а также число элементов в папке и каждой вложенной папке.

PowerShell

```
Get-MailboxFolderStatistics -Identity "Gurinder Singh" -FolderScope
RecoverableItems | Format-Table
Name,FolderAndSubfolderSize,ItemsInFolderAndSubfolders -Auto
```

S/MIME для подписи и шифрования сообщений

Статья • 04.04.2023

Как администратор в Exchange Server вы можете включить безопасные и многоцелевые расширения электронной почты (S/MIME) для своей организации. S/MIME — это общепринятый способ, а точнее протокол для передачи зашифрованных сообщений с цифровой подписью. S/MIME позволяет шифровать электронные письма и добавлять к ним цифровую подпись. При использовании S/MIME получатели могут быть уверены, что:

- сообщение в их почтовом ящике — точная копия отправленного;
- сообщение поступило от определенного отправителя, а не от мошенника.

Для этого S/MIME предоставляет службы криптографической безопасности, такие как проверка подлинности, обеспечение целостности сообщений и неотрекаемости источника (с помощью цифровых подписей). Протокол S/MIME также помогает повысить конфиденциальность и безопасность обмена электронными сообщениями (с помощью шифрования).

Для применения S/MIME требуется сертификат и инфраструктура публикации, которая часто используется при взаимодействии с корпоративными клиентами и конечными потребителями. Пользователь управляет криптографическими ключами в S/MIME и может выбрать, будут ли они применяться для каждого отправляемого сообщения. Почтовые программы, такие как Outlook, выполняют поиск в расположении доверенного корневого центра сертификации для добавления цифровой подписи и ее проверки.

Полный обзор истории и архитектуры S/MIME в контексте электронной почты см. в этой статье.

Поддерживаемые сценарии и технические особенности S/MIME

S/MIME можно настроить для работы со следующими конечными точками:

- Outlook 2010 или более поздней версии;
- Outlook в Интернете (предыдущее название — Outlook Web App);

- Exchange ActiveSync (EAS).

Действия по настройке S/MIME для каждой из этих конечных точек несколько различаются. Ниже приведены общие инструкции.

1. Установите центр сертификации на основе Windows и настройте инфраструктуру открытых ключей для выдачи сертификатов S/MIME. Поддерживаются сертификаты, выданные сторонними поставщиками сертификатов. Дополнительные сведения см. в статье Общие сведения о развертывании сертификатов сервера.

2. Опубликуйте сертификат пользователя в учетной записи доменных служб локальная служба Active Directory (AD DS) в **атрибутах UserSMIMECertificate** и (или**) UserCertificate**. Ad DS должны находиться на компьютерах в физическом расположении, которое вы контролируете, а не в удаленном объекте или облачной службе в Интернете. Дополнительные сведения об AD DS см. в разделе Обзор доменные службы Active Directory.

3. Настройте коллекцию виртуальных сертификатов для проверки S/MIME. Эта информация используется Outlook в Интернете при проверке подписи сообщения электронной почты для подтверждения того, что оно было подписано доверенным сертификатом.

4. Настройте конечную точку Outlook или EAS для использования S/MIME.

Настройка S/MIME для Outlook в Интернете

Настройка S/MIME для Outlook в Интернете состоит из следующих этапов:

1. Параметры S/MIME для Outlook в Интернете в Exchange Server.

2. Set up Virtual Certificate Collection to Validate S/MIME

Сведения об отправке зашифрованного сообщения S/MIME в Outlook в Интернете см. в разделе Шифрование сообщений с помощью S/MIME в Outlook в Интернете.

Технологии шифрования сообщений

Различные технологии шифрования используются совместно для обеспечения защиты сообщений, хранящихся в почтовых ящиках и при пересылке. Протокол S/MIME может работать одновременно со следующими технологиями, но не зависит от них:

- **Безопасность транспортного уровня (TLS):** шифрует туннель или маршрут между почтовыми серверами, чтобы предотвратить перехват и перехват, а также шифрует подключение между клиентами электронной почты и серверами.

  > ⓘ **Примечание**
  >
  > Теперь для шифрования данных, которыми обмениваются компьютерные системы, используется протокол TLS вместо протокола SSL. Они настолько тесно связаны, что термины "SSL" и "TLS" (без версий) часто используются взаимозаменяемо. Из-за этого сходства ссылки на "SSL" в разделах Exchange, Центре администрирования Exchange и командной консоли Exchange часто используются для охвата протоколов SSL и TLS. Как правило, термин "SSL" обозначает именно протокол SSL только в тех случаях, когда указан номер версии (например, SSL 3.0). Чтобы узнать, почему следует отключить протокол SSL и переключиться на TLS, см. **статью Защита от уязвимости SSL 3.0**.

- **BitLocker**. Шифрует данные на жестком диске в центре обработки данных, чтобы, если кто-то получил несанкционированный доступ, он не смог прочитать их. Дополнительные сведения см. в статье BitLocker: развертывание на Windows Server 2012 и более поздних версий.

Параметры S/MIME для Outlook в Интернете в Exchange Server

Статья • 04.04.2023

Администратор Exchange может настроить Outlook в Интернете (прежнее название — Outlook Web App), чтобы разрешить отправку и получение сообщений, защищенных S/MIME. Используйте командлеты **Get-SmimeConfig** и **Set-SmimeConfig** для просмотра этой функции и управления ею в командной консоли Exchange. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.

Подробные сведения о синтаксисе и параметрах см. в разделах Get-SmimeConfig и Set-SmimeConfig.

S/MIME в Outlook в Интернете в Exchange 2019 поддерживается в Internet Explorer, Edge, Edge с Chromium и Google Chrome.

Рекомендации по Chrome

Чтобы использовать S/MIME в Outlook в Интернете в веб-браузере Google Chrome, вам (или другому администратору) необходимо задать и настроить политику Chromium **с именем ExtensionInstallForcelist** для установки расширения Microsoft S/MIME в Chrome. Значение политики — `maafgiompdekodanheihhgilkjchcakm;https://outlook.office.com/owa/SmimeCrxUpdate.ashx`. Обратите внимание, что для применения этой политики требуются присоединенные к домену компьютеры, поэтому для использования S/MIME в Chrome фактически требуются компьютеры, присоединенные к домену.

Дополнительные сведения о политике **ExtensionInstallForcelist** см. в разделе ExtensionInstallForcelist.

Этот шаг является предварительным условием для использования Chrome. он не заменяет элемент управления S/MIME, установленный пользователями. Пользователям предлагается скачать и установить элемент управления S/MIME в Outlook в Интернете во время первого использования S/MIME. Кроме того, пользователи могут заранее перейти к **S/MIME** в параметрах Outlook в Интернете, чтобы получить ссылку для скачивания элемента управления.

Высокий уровень доступности и устойчивость сайта в Exchange Server

Статья • 04.04.2023

Вы можете защитить базы данных почтовых ящиков Exchange Server и содержащиеся в них данные, настроив серверы и базы данных Exchange для обеспечения высокой доступности и устойчивости сайта. Exchange Server минимизирует затраты и сложность развертывания высокодоступного и отказоустойчивого решения для обмена сообщениями, обеспечивая высокий уровень доступности служб и данных, а также поддержку очень больших почтовых ящиков.

Exchange Server позволяет клиентам всех размеров и сегментов экономично развертывать службу непрерывности обмена сообщениями в своей организации, используя собственные возможности репликации и архитектуру высокого уровня доступности, представленные в Exchange 2010. Список изменений, внесенных после версии Exchange 2010, см. в статье Changes to high availability and site resilience over previous versions.

Основные термины

Следующие ключевые понятия важно понимать высокой доступности и устойчивости сайта:

Активный диспетчер

> Внутренний компонент Exchange, который запускается в службе репликации Microsoft Exchange и отвечает за мониторинг сбоев и действие по исправлению путем отработки отказа в группе обеспечения доступности баз данных.

AutoDatabaseMountDial

> Значение свойства сервера почтовых ящиков, которое определяет, будет ли Копия пассивной базы данных будут автоматически подключены в качестве новой активной копии, в зависимости от количества файлов журнала, отсутствует копия быть подключен.

Непрерывная репликация — режим блокировки

> В режиме блокировки при каждой записи обновления в буфер активного журнала активной копии базы данных обновление также передается в буфер журнала каждой пассивной копии почтового ящика. После заполнения буфера журнала каждая копия базы данных строит, проверяет и создает следующий файл журнала по порядку номера версии.

Непрерывная репликация — режим файла

> В файловом режиме, закрытые файлы журнала транзакций переносятся из активной копии базы данных в одну или несколько пассивных копий базы данных.

Группа доступности базы данных

> Группа из 16 серверов Exchange, на котором размещается набор реплицированных баз данных.

Мобильность баз данных

> Возможность репликации базы данных почтовых ящиков Exchange Server на другие серверы Exchange и подключения к ней.

Datacenter

> Обычно это относится к сайту Active Directory; однако он также может ссылаться на физический сайт. В контексте этой документации центр обработки данных равен сайту Active Directory.

Режим координации активации центра данных

> Свойство параметра группы обеспечения доступности баз данных, при включении которого обеспечивается получение службой репликации Microsoft Exchange разрешения на подключение баз данных при запуске.

Аварийное восстановление

> Любой процесс, используемый для ручного восстановления после сбоя. Это может быть сбой, затрагивающий как отдельный объект, так и все физическое расположение.

Интерфейс API Exchange для сторонней репликации

> Представленный в Exchange интерфейс API, который позволяет использовать для группы обеспечения доступности баз данных стороннюю синхронную репликацию вместо непрерывной.

Высокая доступность

> Решение, которое обеспечивает доступность служб и данных, а также автоматическое восстановление после сбоев, затрагивающих службы или данные (например, сбой сети, хранилища или сервера).

Добавочное развертывание

> Возможность развертывания высокого уровня доступности и устойчивости сайта после установки Exchange Server.

Изолированная копия базы данных почтовых ящиков

> Пассивная копия базы данных почтовых ящиков, у которой время запаздывания преобразования журнала больше нуля.

Копия базы данных почтовых ящиков

> База данных почтовых ящиков (файл EDB и журналы), которая находится в активном или пассивном состоянии.

Устойчивость почтовых ящиков

> Имя единого решения для обеспечения высокого уровня доступности и устойчивости сайта в Exchange Server.

Управляемая доступность

> Набор внутренних процессов, который состоит из зондов, мониторов и отвечающих устройств, обеспечивающих мониторинг и высокую доступность для всех ролей сервера и протоколов.

**over* (произносится "star over")

> Сокращение от терминов *переключение* (switchover) и *отработка отказа* (failover). Переключение представляет собой ручную активацию одной или нескольких копий базы данных. Отработка отказа представляет собой автоматическую активацию одной или нескольких копий базы данных после сбоя.

Система безопасности

> Ранее известная как контейнер транспорта, это функция транспортной службы, которая хранит копию всех сообщений в течение *X* дней. Значение по умолчанию: 2 дня.

теневая избыточность

> Функция транспортного сервера, обеспечивающая избыточность для сообщений на всем протяжении их пересылки.

Устойчивость сайта к сбоям

> Конфигурацию, которая расширяет инфраструктуру обмена сообщениями на несколько сайтов Active Directory, чтобы обеспечить бесперебойное функционирование для системы обмена сообщениями в случае сбоя, затрагивающего один из сайтов.

Группы доступности базы данных

DAG — это базовый компонент платформы высокого уровня доступности и устойчивости сайта, встроенной в Exchange Server. DAG — это группа из 16 серверов Exchange, которая размещает набор баз данных и обеспечивает автоматическое восстановление на уровне базы данных после сбоев, влияющих на отдельные базы данных, сети или серверы. На любом сервере в группе обеспечения доступности баз данных можно разместить копию базы данных почтовых ящиков с любого другого сервера в группе обеспечения доступности баз данных. Если сервер добавлен в группу обеспечения доступности баз данных, он вместе с другими серверами в этой группе обеспечивает автоматическое восстановление после сбоев, затрагивающих базы данных почтовых ящиков, например сбоев дисков или серверов. Дополнительные сведения о группах доступности баз данных см. в разделе Группы доступности баз данных.

Копии базы данных почтовых ящиков

Функции обеспечения высокой доступности и устойчивости сайта, впервые представленные в Exchange 2010, используются в Exchange Server для создания и обслуживания копий базы данных. Exchange Server также использует концепцию мобильности баз данных, которая представляет собой отработку отказа на уровне базы данных, управляемой Exchange.

Функция мобильности базы данных обеспечивает отключение баз данных от серверов и добавление поддержки до 16 копий одной базы данных. Она также отвечает за взаимодействие при создании копий базы данных.

Настройка копии базы данных в качестве активной базы данных почтовых ящиков называется *переключением*. Ситуация, когда происходит сбой, затрагивающий базу данных, а новая база данных становится активной копией, называется *отработкой отказа*. Этот процесс также затрагивает сбой сервера, при котором один или несколько серверов переводят в оперативный режим базы данных, которые ранее находились на неисправном сервере. При переключении или отработке отказа другие серверы Exchange почти сразу же становятся осведомлены о переключении и перенаправляют трафик клиента и обмена сообщениями в новую активную базу данных.

Например, если происходит сбой активной базы данных в группе обеспечения доступности баз данных из-за сбоя соответствующего хранилища, активный диспетчер выполняет автоматическое восстановление, переходя на копию базы данных на другом сервере в группе обеспечения доступности баз данных. В Exchange Server управляемая доступность обеспечивает поведение для восстановления после потери доступа по протоколу к базе данных, включая повторное использование пулов рабочих ролей приложений, перезапуск служб и серверов и инициализацию отработки отказа базы данных.

Дополнительные сведения о копиях баз данных почтовых ящиков см. в разделе Копии базы данных почтовых ящиков.

Active Manager

Exchange Server использует Active Manager для управления работоспособностью, состоянием, непрерывной репликацией и другими аспектами высокого уровня доступности. Дополнительные сведения о компоненте Active Manager см. в разделе Active Manager.

Устойчивость сайта к сбоям

В Exchange 2010 можно было развернуть группу обеспечения доступности баз данных в двух центрах обработки данных, в третьем разместить следящий сервер и включить отработку отказа для роли сервера почтовых ящиков в каждом центре обработки данных. Но вы не получили отработку отказа для самого решения, так как пространство имен по-прежнему необходимо вручную изменить для ролей сервера, не являющихся почтовыми ящиками.

В Exchange 2016 и Exchange 2019 пространство имен не нужно перемещать с помощью DAG. Exchange использует отказоустойчивость, встроенную в пространство имен через несколько IP-адресов, распределения нагрузки (и в случае необходимости, возможность введения серверов в эксплуатацию и их выведения из эксплуатации). Современные HTTP-клиенты работают с этой избыточностью автоматически. Стек HTTP может принимать несколько IP-адресов для полного доменного имени (FQDN), и если первый IP-адрес, который он пытается выполнить, не удается (то есть не удается подключиться), он попытается получить следующий IP-адрес в списке. При обратимом сбое (подключение теряется после установки сеанса, возможно, из-за периодических сбоев в службе, когда, например, устройство удаляет пакеты и должно быть удалено из службы), пользователю может потребоваться обновить браузер.

Это означает, что пространство имен больше не является единой точкой отказа, как в Exchange 2010. В Exchange 2010, пожалуй, основная критической точки отказа системы обмена сообщениями-это полное доменное имя, которое вы даете пользователям, поскольку это говорит пользователь куда идти. В парадигме Exchange 2010 изменить полное доменное имя для обозначения адресата не так просто, поскольку необходимо изменить DNS, а затем обработать задержки DNS, что иногда является трудной задачей. Кроме того, также в обработке нуждаются кэши имен в браузерах, что обычно занимает около 30 минут или более.

В Exchange Server клиенты имеют несколько мест. Почти все протоколы клиентского доступа в Exchange Server основаны на HTTP. Примеры — Outlook, EAS, EWS, Outlook в Интернете и Центр администрирования Exchange. У всех поддерживаемых клиентов HTTP имеется возможность использовать несколько IP-адресов, что позволяет выполнить отработку отказов на стороне клиента. Вы можете настроить DNS для передачи нескольких IP-адресов клиенту в процессе разрешения имен. Клиент запрашивает mail.contoso.com и получает, например, 2 или 4 IP-адреса. Клиент использует все полученные им IP-адреса. Это повышает эффективность работы клиента, так как при сбое одного из IP-адресов у клиента будет еще один или несколько IP-адресов, по которым он может попытаться подключиться. Если клиенту не удается подключиться по одному из IP-адресов, он

ожидает приблизительно 20 секунд, а затем пытается использовать следующий IP-адрес в списке. Таким образом, если вы потеряете виртуальный IP-адрес для массива служб клиентского доступа, то восстановление для клиентов будет выполнено автоматически приблизительно через 21 секунду.

Ниже перечислены связанные с этим преимущества.

- В Exchange Server, если вы потеряете подсистему балансировки нагрузки на основном сайте, вы просто отключите его (или, возможно, отключите виртуальный ip-адрес) и восстановите или замените его. В клиентах, в которых уже не используется виртуальный IP-адрес в дополнительном центре обработки данных, будет выполнена автоматическая отработка отказа на дополнительный важный компонент без изменения пространства имен и DNS. Благодаря этому не только отпадает необходимость в переключении, но и экономится время, которое обычно тратится на переключение центра обработки данных. В Exchange 2010 приходилось обрабатывать задержку DNS (поэтому рекомендовалось установить срок жизни [TTL] в 5 минут, а также ввести URL-адрес для обработки отказа). В Exchange 2016 и Exchange 2019 это не требуется, так как вы получаете быструю отработку отказа (20 секунд) пространства имен между ВИРТУАЛЬНЫми IP-адресами (центрами обработки данных).

- Благодаря быстрой обработке пространства имен между центрами обработки данных все, что требуется для обработки отказа центра обработки данных, — механизм обработки отказа роли сервера почтовых ящиков в центрах обработки данных. Для автоматической обработки отказа для группы обеспечения доступности баз данных необходимо просто разработать решение, при котором группа равномерно распределяется между двумя центрами обработки данных, а затем разместить следящий сервер в третьем расположении для его арбитража членами группы обеспечения доступности баз данных в каждом центре обработки данных (вне зависимости от состояния сети между центрами обработки данных с членами этой группы). Если у вас есть только два центра обработки данных и третье физическое расположение недоступно, вы можете разместить следящий сервер на виртуальной машине Microsoft Azure. Дополнительные сведения см. в разделе Using a Microsoft Azure VM as a DAG witness server.

- В этом сценарии администратор пытается просто решить проблему, а не восстановить службу. При этом просто ошибка просто исправляется; служба продолжает работать, и сохраняется целостность данных. При восстановлении службы вы ощущаете намного меньшие стресс и нехватку времени, чем при

ремонте неисправного устройства. Работа пользователя и администратора значительно упрощается.

Вы можете разрешить отработку отказа без необходимости обратного подключения (иногда это действие ошибочно называется восстановлением размещения). Если вы потеряете серверы в главном центре обработки данных, что приведет к 20-секундному перерыву в работе клиентов, можно даже не заботиться о восстановлении после сбоя. На данный момент основная задача состоит в решении ключевой проблемы (например, замене вышедшей из строя подсистемы балансировки нагрузки). После того как она подключится к сети и продолжит работу, одни клиенты начнут ее использование, а другие будут функционировать через второй центр обработки данных.

Exchange Server также предоставляет функциональные возможности, позволяющие администраторам справляться с периодическими сбоями. Прерывистый сбой происходит, если, например, ничего не происходит после установки начального TCP-соединения. Непредвиденный сбой требует некоторой дополнительной административные взыскания, так как это может быть в результате ввода в эксплуатацию нового устройства. В ходе восстановления устройство может быть включено и принимать некоторые запросы, но оно фактически не готово к обслуживанию клиентов, пока не будут выполнены необходимые действия по настройке. В этом сценарии, администратор может выполнять пространства имен, просто удалив VIP переключение для заменяемого устройства от DNS. Затем в течение этого периода, нет клиентов будут пытаться подключиться к нему. После замены администратор может добавить важный компонент обратно в DNS, а клиенты в конечном итоге начнут использовать его.

Дополнительные сведения о планировании и развертывании устойчивости сайта см. в разделах Планирование высокого уровня доступности и устойчивости сайта и Развертывание высокого уровня доступности и устойчивости сайта.

сторонний интерфейс API репликации

Exchange Server включает сторонний API репликации, который позволяет организациям использовать сторонние решения для синхронной репликации вместо встроенной функции непрерывной репликации. Корпорация Майкрософт поддерживает решения сторонних производителей, использующие этот API, если решение содержит необходимые функции, заменяющие все встроенные функции непрерывной репликации, которые отключены из-за использования API. Поддержка решений обеспечивается, только когда API используется в группе обеспечения доступности баз данных для управления и активации копий базы

данных почтовых ящиков. Использование интерфейса API для других целей не поддерживается. Кроме того, решение должно удовлетворять соответствующим требованиям к поддержке оборудования Windows. (Для поддержки не требуется тестовая проверка.)

При развертывании решения, использующего встроенный интерфейс API репликации сторонних производителей, учтите, что поставщик решения несет ответственность за основную поддержку решения. Майкрософт поддерживает данные Exchange для решений с репликацией и без нее. Решения, использующие репликацию данных, должны соответствовать политике поддержки Майкрософт для репликации данных. Кроме того, решения, использующие модель ресурсов Windows Failover Cluster должны отвечать требованиям кластеров Windows согласно статье базы знаний 943984, Политика поддержки отказоустойчивых кластеров Майкрософт для Windows Server 2008 и Windows Server 2008 R2 или Политика поддержки отказоустойчивых кластеров Майкрософт для Windows 2012.

Политика Майкрософт в области поддержки резервного копирования и восстановления для развертываний, использующих решения по репликации на основе интерфейсов API сторонних производителей, аналогична политике для развертываний со встроенной непрерывной репликацией.

Партнеры корпорации Майкрософт могут получить сведения о стороннем интерфейсе API в любом местном представительстве.

Документация высоким уровнем доступности и устойчивости сайта

В следующей таблице содержатся ссылки на разделы, которые помогут вам узнать о dag и управлении ими, копиями баз данных почтовых ящиков, а также резервным копированием и восстановлением для Exchange Server.

Статья	Описание
Группы обеспечения доступности баз данных	Сведения о группах DAG, активном диспетчере, режиме DAC и копиях базы данных почтовых ящиков.
Планирование высокого уровня доступности и устойчивости сайта	Сведения об общих требованиях, включая требования к оборудованию, сети, программному обеспечению, следящему серверу и другим компонентам, а также рекомендации для групп обеспечения доступности баз данных.

Статья	Описание
Развертывание с высоким уровнем доступности и устойчивости сайта	Исследовать пример сценария развертывания для развертывания и настройки групп DAG.
Управление высокой доступностью и устойчивостью сайтов	Подробнее о задачах управления DAG, переключениями и отработками отказа, и режим обслуживания.
Мониторинг групп доступности баз данных	Описание встроенных командлетов и сценариев для группы доступности базы данных и копии базы данных наблюдения.
Резервное копирование, восстановление и аварийное восстановление	Сведения о резервном копировании и восстановлении баз данных Exchange, восстановления базы данных, и восстановления серверов.

Изменения в высокой доступности и устойчивости сайта по сравнению с предыдущими версиями Exchange Server

Статья • 04.04.2023

Exchange Server 2013 и более поздних версиях используют группы доступности и копии баз данных почтовых ящиков (наряду с другими функциями, такими как восстановление отдельных элементов, политики хранения и отложенные копии баз данных) для обеспечения высокой доступности, устойчивости сайта и собственной защиты данных Exchange. Платформа высокого уровня доступности, хранилище сведений о Exchange и расширяемое ядро хранилища (ESE) были усовершенствованы с exchange 2010, чтобы обеспечить доступность и менее сложное управление, а также сократить затраты. Эти усовершенствования включают в себя:

- **Сокращение операций ввода-вывода в секунду**. Это позволяет максимально эффективно использовать диски большего размера с точки зрения емкости и операций ввода-вывода в секунду.

- **Управляемая доступность**. Благодаря управляемой доступности функции внутреннего мониторинга и восстановления тесно интегрированы для предотвращения сбоев, упреждающего восстановления служб и автоматического запуска отработки отказа сервера или оповещения администраторов о принятии мер. Основное внимание уделяется мониторингу и управлению взаимодействием с пользователями, а не только отслеживанию времени работы серверов и компонентов для поддержания непрерывной доступности системы.

- **Управляемое хранилище**. Управляемое хранилище — это имя переписанных процессов хранилища сведений в Exchange 2013 или более поздней версии. Управляемое хранилище написано на языке C# и тесно интегрировано со службой репликации Microsoft Exchange (MSExchangeRepl.exe) для повышения доступности за счет повышения устойчивости.

- **Поддержка нескольких баз данных на диск**. Усовершенствования позволяют поддерживать несколько баз данных (сочетание активных и пассивных копий) на одном диске, тем самым максимально эффективно используя диски

большего размера с точки зрения емкости и операций ввода-вывода в секунду.

- **AutoReseed**: функция автоматического повторного изменения позволяет быстро восстановить избыточность базы данных после сбоя диска. В случае сбоя диска копия базы данных, сохраненная на диске, копируется из активной копии базы данных на резервный диск того же самого сервера. Если на отказавшем диске хранилось несколько копий баз данных, их можно автоматически повторно заполнить на свободном диске. Это ускоряет повторное заполнение, так как активные базы данных, скорее всего, располагаются на нескольких серверах и данные копируются параллельно.

- **Автоматическое восстановление после сбоев хранилища**. Эта функция продолжает внедрение инноваций в Exchange 2010, позволяющих системе восстанавливаться после сбоев, влияющих на устойчивость или избыточность. Exchange теперь включает в себя больше операций восстановления для длительных операций ввода-вывода, чрезмерного потребления памяти MSExchangeRepl.exe и тяжелых случаев, когда система находится в таком плохом состоянии, что потоки не могут быть запланированы.

- **Улучшения отставленного копирования**. Отставленные копии теперь могут в определенной степени заботиться о себе с помощью автоматического воспроизведения журналов. Отстающие копии автоматически будут воспроизводить файлы журналов в различных ситуациях, таких как исправление страниц и мало места на диске. Если система обнаружит, что для отстающей копии требуется исправление страницы, журналы будут автоматически воспроизводиться в отстающую копию, чтобы выполнить исправление страницы. Отстающие копии также используют это автоматическое воспроизведение при достижении нижнего порога доступного дискового пространства или обнаружении того, что эта копия является единственной доступной копией в течение определенного времени. Кроме того, отстающие копии могут использовать Safety Net, что значительно упрощает восстановление или активацию.

- **Усовершенствования оповещений о едином копировании. Оповещение** о едином копировании, представленное в Exchange 2010, больше не является отдельным запланированным скриптом. Теперь оно интегрируется с компонентами управляемой доступности системы и входит в состав Exchange.

- **Автоматическая настройка сети DAG**. Сети DAG могут быть автоматически настроены системой на основе параметров конфигурации. Помимо вариантов ручной настройки, группы обеспечения доступности баз данных могут

различать сети MAPI и сети репликации, а также автоматически настраивать сети групп.

Сокращение операций ввода-вывода в секунду

В Exchange 2010 пассивные копии базы данных имеют низкую глубину контрольных точек, что требуется для быстрой отработки отказа. Кроме того, пассивная копия выполняет агрессивное предварительное чтение данных, чтобы не отставать от глубины контрольной точки в 5 мб. В результате использования низкой глубины контрольных точек и выполнения этих агрессивных операций предварительного чтения операции ввода-вывода в секунду для пассивной копии базы данных равны операциям ввода-вывода в секунду для активной копии в Exchange 2010.

В Exchange 2013 или более поздней версии система может обеспечить быструю отработку отказа, используя большую глубину контрольных точек для пассивной копии (100 МБ). Поскольку пассивные копии имеют глубину контрольных точек 100 МБ, они повторно настроены на менее агрессивное выполнение операций. В результате увеличения глубины контрольной точки и отмены настройки агрессивных операций предварительного чтения число операций ввода-вывода в секунду для пассивной копии составляет около 50 процентов активных операций ввода-вывода в секунду.

Наличие более высокой глубины контрольных точек для пассивной копии также приводит к другим изменениям. В переключаемых в Exchange 2010, кэш очищается база данных, в которой содержится база данных преобразуется из пассивной копии на активную копию. Начиная с Exchange 2013 ведение журнала ESE перезаписывается, чтобы кэш сохранялся при переходе от пассивного к активному. Поскольку подсистеме ESE не нужно очищать кэш, выполняется быстрая отработка отказа.

Было внесено еще одно изменение, относящееся к процессу фонового обслуживания баз данных (BDM). BDM теперь обрабатывает около 1-2 МБ в секунду для каждой копии.

В результате этих изменений Exchange теперь обеспечивает значительное сокращение операций ввода-вывода в секунду по сравнению с Exchange 2010.

Управляемая доступность

Управляемая доступность — это интеграция встроенного активного мониторинга и платформы высокого уровня доступности Exchange. Благодаря управляемой доступности система может определить время для отработки отказа базы данных на основе работоспособности службы. Управляемая доступность — это внутренняя инфраструктура, развернутая в службах клиентского доступа (интерфейсных) и внутренних службах на серверах почтовых ящиков. Управляемая доступность включает три основных асинхронных компонента, которые постоянно выполняют работу:

1. Первым компонентом является модуль пробы, отвечающий за выполнение измерений на сервере и сбор данных. Результаты этих измерений поступают во второй компонент — монитор.

2. Монитор содержит всю используемую системой бизнес-логику на основе того, что считается работоспособным состоянием собранных данных. Подобно подсистеме распознавания шаблонов, монитор ищет различные шаблоны среди всех собранных измерений, а затем принимает решение, можно ли считать компонент работоспособным.

3. Наконец, есть обработчик ответчика, который отвечает за действия по восстановлению.

Если что-то не работает, первое действие — попытка восстановления соответствующего компонента. Это может включать в себя многоэтапные действия по восстановлению; Например:

1. Перезапустите пул приложений.

2. Перезапустите службу.

3. Перезапустите сервер.

4. Переведите сервер в автономный режим, чтобы он больше не принимал трафик.

Если действия по восстановлению не помогают, система уведомляет о проблеме оператора-человека через журнал.

Управляемая доступность реализуется в форме две службы:

- **Exchange Health Manager Service (MSExchangeHMHost.exe)**: это процесс контроллера, который используется для управления рабочими процессами. Он используется для построения, выполнения, запуска и остановки рабочих процессов по мере необходимости. Он также используется для

восстановления рабочих процессов при сбоях, чтобы рабочие процессы не становились единственной точкой отказа.

- **Рабочий процесс диспетчера работоспособности Exchange (MSExchangeHMWorker.exe)**: это рабочий процесс, отвечающий за выполнение задач среды выполнения.

Управляемая доступность использует постоянное хранилище для выполнения своих функций:

- XML-файл конфигурации используются для инициализации определений рабочих элементов при запуске рабочего процесса.
- Реестр используется для хранения данных среды выполнения, например закладок.
- Инфраструктура журнала событий канала Crimson используется для хранения результатов рабочих элементов.

Дополнительные сведения об управляемой доступности см. в статье Управляемое доступность.

Управляемое хранилище

Exchange 2010 и более ранних версий поддерживают запуск одного экземпляра процесса хранилища сведений (Store.exe) в роли сервера почтовых ящиков. В этом едином хранилище размещены все базы данных на сервере: активные, пассивные, изолированные и базы данных восстановления. В этих архитектурах Exchange между различными базами данных, размещенными на сервере почтовых ящиков, существует небольшая изоляция, если она есть. Проблемы с единой базой данных почтовых ящиков могут негативно сказаться на всех остальных базах данных, а аварийное завершение в результате повреждения почтового ящика может повлиять на работу служб для всех пользователей, базы данных которых размещены на таком сервере.

Еще одна проблема, связанная с одним экземпляром Store, связана с отсутствием масштабируемости процессора с помощью расширяемого обработчика хранилища (ESE). ESE хорошо масштабируется до 8–12 ядер процессора, но помимо этого проблемы с взаимодействием между процессорами и синхронизацией кэша приводят к снижению производительности. Учитывая сегодняшние серверы с более чем 16 ядрами, это вызовет административную задачу управления сходством 8–12 ядер для ESE и использования других ядер для процессов, отличных от Store (например, Помощники, Search Foundation, Управляемая доступность и т. д.). Кроме

того, предыдущая архитектура ограничивала увеличение масштаба для процессов хранилища.

За многие годы процесс Store.exe был значительно усовершенствован, как и Exchange Server, но в конечном итоге его масштабируемость как одного процесса ограничена и представляет единственную точку отказа. Из-за этих ограничений Store.exe были удалены в Exchange 2013 и заменены управляемым хранилищем.

Дополнительные сведения см. в разделе Управляемое хранилище.

Несколько баз данных на том

Хотя улучшения хранилища в Exchange предназначены в основном для нескольких конфигураций дисков (JBOD), они доступны для использования всеми поддерживаемыми конфигурациями хранилища. Одной из таких функций является возможность размещения нескольких баз данных на одном и том же томе. Эта функция предназначена для больших дисков о Exchange оптимизация. Эти улучшения позволяют использовать большие диски по емкости с гораздо большей эффективностью в показателях емкости, количества операций ввода-вывода в секунду и времени повторного заполнения, а также призваны устранить следующие проблемы, связанные с выполнением задач в конфигурации хранилища JBOD.

- Необходимость управления размерами баз данных.
- Операции повторного заполнения должны быть быстрыми и надежными.
- Хотя емкость хранилища увеличивается, количество операций ввода-вывода в секунду не растет.
- Диски, на которых размещены пассивные копии базы данных, используются недостаточно эффективно в показателях количества операций ввода-вывода в секунду.
- Изолированные копии имеют асимметричные требования к хранилищу.
- Гибкость ограничивается для восстановления в условиях нехватки места на диске.

Тенденция увеличения емкости хранилища продолжается. Например, рекомендация по Exchange для максимального размера базы данных (2 терабайта) на 8-терабайтовом диске означает, что вы будете тратить более 5 терабайт дискового пространства.

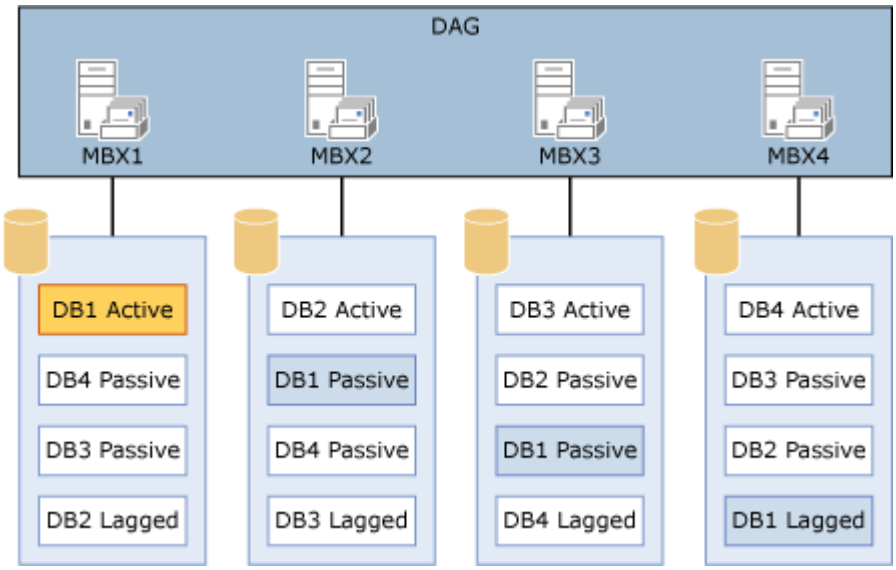
Решением было бы увеличение размера баз данных, но это препятствует управляемости, так как это может привести к длительному повторному просмотру (включая неуправляемое время повторного копирования) и скомпрометировать надежность копирования этого объема данных по сети.

Кроме того, в модели Exchange 2010 диск, на котором хранится пассивная копия, используется не в полной мере в плане количества операций ввода-вывода в секунду. В случае с изолированной пассивной копией, диск не только используется недостаточно эффективно с точки зрения количества операций ввода-вывода в секунду, но и является асимметричным в плане размера относительно дисков, используемых для хранения активных и неизолированных пассивных копий.

Exchange 2013 и более поздних версий оптимизирован для более эффективного использования больших дисков (8 ТБ) в конфигурации JBOD. С несколькими базами данных на диск теперь можно использовать диски одинакового размера, в которых хранится несколько копий баз данных, включая отстающие копии. Цель состоит в том, чтобы максимально способствовать распределению пользователей по существующим томам и обеспечить симметричный дизайн, при котором во время обычных операций в каждом члене группы обеспечения доступности баз данных размещается ряд активных, пассивных и дополнительных изолированных копий в одном томе.

Пример конфигурации, в которой используется несколько баз данных на томе представлен ниже.

Конфигурация, в которой используется несколько баз данных на том



Конфигурация на схеме обеспечивает симметричную структуру. Все четыре базы данных четырех серверах установлены одинаковые все размещены на одном диске на каждый сервер. Ключевой момент — количество копий каждой имеющейся базы данных равно числу копий базы данных на диск.

В конфигурации на схеме есть четыре копии каждой базы данных: одна активная копия, две пассивные копии и одна отстаиваемая копия. Поскольку каждая база данных имеет четыре копии, правильной считается конфигурация с четырьмя копиями на том.

Кроме того, приоритет активации сбалансирован в группе обеспечения доступности баз данных и на каждом сервере. Например:

- Активная копия будет иметь предпочтительное значение активации 1.
- Первая пассивная копия будет иметь предпочтительное значение активации 2.
- Вторая пассивная копия будет иметь предпочтительное значение активации 3.
- Отложенная копия будет иметь предпочтительное значение активации 4.

Помимо более эффективного распределения пользователей по существующим томам, еще одним преимуществом использования нескольких баз данных на диск является сокращение времени на восстановление защиты данных от сбоев, требующих повторного выполнения (например, сбоя диска).

По мере увеличения размера базы данных повторное ее заполнение занимает больше времени. Например, повторное заполнение базы данных на 2 ТБ может занять 23 часа, а базы данных на 8 ТБ — 93 часа (почти 4 дня). В обоих случаях повторное заполнение выполняется со скоростью около 20 МБ в секунду. Обычно это значит, что очень большую базу данных невозможно заполнить в разумный срок.

Если используется сценарий с одной копией базы данных на диск, операция заполнения эффективно связана с источником, поскольку диск постоянно заполняется из одного источника.

Вследствие разделения тома на несколько копий базы данных и наличия активной копии пассивных баз данных на определенном томе, который хранится у отдельных членов группы обеспечения доступности баз данных, система больше не будет связанной с источником в контексте повторного заполнения диска. При замене неисправного диска, он может быть повторно заполнен из нескольких источников. Это позволяет системе выполнить повторное заполнение и возобновить защиту данных для этих баз данных в более короткий срок.

При использовании нескольких баз данных на том рекомендуется следовать следующим рекомендациям и требованиям:

- Следует использовать один раздел логического диска на физический диск. Не создавайте на диске несколько разделов. Каждая копия базы данных и ее сопровождающие файлы (например, журналы транзакций и индекс контента) должны размещаться в уникальном каталоге на отдельном разделе.
- Число копий базы данных, созданных в том должно быть равно числу копий каждой базы данных. Например, если имеется четыре копии базы данных, необходимо использовать четыре копии базы данных на том.
- Копии базы данных должны иметь одних соседей. (Например, они все должны размещаться на одном диске на каждом сервере).
- Приоритет активации в группе обеспечения доступности баз данных должен быть сбалансирован таким образом, чтобы каждая копия базы данных на заданном диске имела уникальное значение приоритета активации.

AutoReseed

Автоматическое повторное восстановление (также известное как AutoReseed) — это замена действия, обычно управляемого администратором, в ответ на сбой диска, событие повреждения базы данных или другую проблему, которая требует повторного изменения копии базы данных. Функция Autoreseed была создана для автоматического восстановления избыточности базы данных после сбоя диска с помощью запасных дисков, настроенных в системе.

Дополнительные сведения см. в разделе AutoReseed. Подробные инструкции по настройке функции AutoReseed см. в разделе Configure AutoReseed for a database availability group.

Автоматическое восстановление после сбоев для хранения

Автоматическое восстановление после сбоев хранилища позволяет системе восстанавливаться после сбоев, влияющих на устойчивость или избыточность. В дополнение к поведению проверки ошибок, появившихся в Exchange 2010, Exchange теперь включает дополнительные варианты восстановления для длительных операций ввода-вывода, чрезмерного потребления памяти службой репликации Microsoft Exchange (MSExchangeRepl.exe) и серьезных случаев, когда невозможно запланировать потоки.

Даже в средах JBOD могут возникнуть проблемы с контроллерами массивов хранения, такие как сбой или зависание. В следующей таблице перечислены функции, предоставляющие функции обнаружения и восстановления зависающего ввода-вывода, которые обеспечивают повышенную устойчивость.

Имя	Проверка	Действие	Порог
Обнаружение зависания ввода-вывода базы данных ESE	Проверка незавершенных операций ввода-вывода с помощью обработчика ESE	Создание элемента сбоя в канале Crimson для перезапуска сервера	240 с
Периодический сигнал канала элемента сбоя	Обеспечение возможности записи и чтения отказавших элементов в канале Crimson	Служба репликации сервера периодического сигнала канала Crimson на сбои и перезапуск	30 с
Периодический сигнал системного диска	Проверка состояния диска серверной системы	Периодическая отправка небуферизованных операций ввода-вывода на системный диск; перезапуск сервера по истечении времени ожидания периодического сигнала	120 с

Exchange 2013 и более поздних версий повышает устойчивость сервера и хранилища, включая поведение для других серьезных условий. Эти условия и режимы описаны в таблице ниже.

Имя	Проверка	Действие	Порог
Неправильное состояние системы	Нет потоков, включая неуправляемые потоки, которые можно запланировать	Перезапустите сервер	302 с
Длительное время операций ввода-вывода	Измерения задержки операций ввода-вывода	Перезапустите сервер	41 с

Имя	Проверка	Действие	Порог
Использование памяти службы репликации	Измерение рабочего множества MSExchangeRepl.exe	1. Регистрация события 4395 в канале crimson с запросом на завершение службы 2. Инициирование прекращения MSExchangeRepl.exe 3. Если завершение службы завершается сбоем, перезапустите сервер.	4 гигабайта (ГБ)
Системное событие 129 (сброс шины)	Проверка наличия записи о событии 129 в журнале системных событий	Перезапустите сервер	Время события
Зависание базы данных кластера	Обновления диспетчера глобального обновления заблокированы	Перезапустите сервер	Время события

Повышения изолированной копии

Улучшения изолированной копии включают в себя интеграцию изолированной копии с функцией "страховочной сети" и автоматическое воспроизведение файлов журнала в определенных сценариях. Служба Safety Net появилась в Exchange 2013, чтобы заменить функцию Exchange 2010, известную как транспортная мусорная корзина. Safety Net похожа на контейнер транспорта, так как это очередь доставки, связанная со службой транспорта на сервере почтовых ящиков. Магазины копий сообщения в этой очереди, были успешно переданы на активной базы данных почтовых ящиков на сервере почтовых ящиков. У каждой активной базы данных почтовых ящиков есть своя очередь на сервере почтовых ящиков, в которой хранятся копии доставленных сообщений. Можно указать, как долго функция "страховочной сети" хранит копии успешно доставленных сообщений до истечения их срока действия и автоматического удаления.

Функция "страховочной сети" частично отвечает за теневую избыточность в средах с группами обеспечения доступности баз данных. В этих средах для обеспечения теневой избыточности не нужно хранить другую копию доставленного сообщения в теневой очереди, пока ожидается репликация доставленного сообщения в пассивных копиях баз данных почтовых ящиков на других серверах почтовых ящиков в группе обеспечения доступности баз данных. Копия отправленного сообщения уже хранится в "страховочной сети", поэтому теневая избыточность позволяет при необходимости повторно доставить сообщение из "страховочной сети".

С помощью Safety Net активация отстающей копии базы данных становится проще. Например, рассмотрим изолированную копию с 2-дневной задержкой преобразования. В этом случае "страховочную сеть" необходимо настроить на срок в 2 дня. Если вы столкнулись с ситуацией, в которой вам нужно использовать отстающую копию, вы можете:

1. Приостановите репликацию к нему.
2. Скопируйте его дважды (чтобы сохранить отстающий характер базы данных и создать дополнительную копию в случае необходимости).
3. Создайте копию и удалите все файлы журнала, кроме файлов в требуемом диапазоне.
4. Подключите копию, после чего в функции "страховочной сети" запустится автоматический запрос на повторную доставку почты в последние два дня.

Благодаря "страховочной сети" отпадает необходимость отслеживания точки повреждения. Пользователь получает почту за последние два дня за исключением данных, которые обычно теряются при отработке отказа, вызвавшей потерю данных.

Теперь изолированные копии могут позаботиться о себе сами, вызывая автоматическое воспроизведение журналов в определенных сценариях:

- При достижении порога нехватки места на диске.
- Если изолированная копия физически повреждена и требуется исправить страницу.
- При наличии менее трех доступных работоспособных копий (активных или пассивных; изолированные копии не учитываются) в течение более 24 часов.

В Exchange 2010 не поддерживалось исправление страниц для изолированных копий. В Exchange 2013 или более поздней версии исправление страниц доступно для отстающих копий с помощью этой функции автоматического воспроизведения. Если возникнет необходимость в исправлении страниц для изолированной копии, в последней будут автоматически воспроизведены журналы, что позволит исправить страницы. Эта функция автоматического воспроизведения также запускается в изолированных копиях, если достигается нижний порог доступного дискового пространства или обнаружено, что изолированная копия является единственной доступной копией в течение определенного времени.

Воспроизведение изолированных копий по умолчанию отключено. Его можно включить с помощью следующей команды.

PowerShell

```
Set-DatabaseAvailabilityGroup <DAGName> -ReplayLagManagerEnabled $true
```

После включения воспроизведение происходит при наличии менее трех копий. Можно изменить значение по умолчанию, равное 3, изменив следующее значение DWORD в реестре.

HKLM\Software\Microsoft\ExchangeServer\v15\Replay\Parameters\ReplayManagerNumAvailableCopies

Чтобы включить воспроизведение для нижних порогов доступного дискового пространства, необходимо настроить следующую запись реестра.

HKLM\Software\Microsoft\ExchangeServer\v15\Replay\Parameters\ReplayLagLowSpacePlaydownThresholdInMB

После настройки какого-либо из этих параметров реестра перезапустите службу управления DAG Microsoft Exchange, чтобы изменения вступили в силу.

В качестве примера рассмотрим среду, в которой заданная база данных имеет четыре копии (три копии с высоким уровнем доступности и одна копия с отставанием), а параметр по умолчанию используется для *ReplayLagManagerNumAvailableCopies*. Если неизолированная копия по какой-либо причине недоступна (например, приостановлена и т. д.), то изолированная копия автоматически воспроизводит файлы журналов через 24 часа.

Усовершенствования оповещений для отдельных копий

Обеспечение надежной работы серверов и работоспособности копий базы данных почтовых ящиков является основной задачей ежедневных операций обмена сообщениями Exchange. Необходимо вести активное наблюдение за оборудованием, операционной системой Windows и службами Exchange.

Но в среде обеспечения устойчивости почтовых ящиков Exchange важно отслеживать работоспособность и состояние группы доступности баз данных и копий базы данных почтовых ящиков. Особенно важно управлять рисками избыточности данных и выполнять мониторинг в течение периодов, когда реплицированная база данных имеет только одну копию. Это критически важно в средах, которые не используют избыточный массив независимых дисков (RAID) и вместо этого развертывают конфигурации JBOD. В среде RAID сбой одного диска

не повлияет на активную копию базы данных почтовых ящиков. Однако в среде JBOD сбой одного диска вызовет отработку отказа базы данных.

Скрипт CheckDatabaseRedundancy.ps1 появился в Exchange 2010. Он позволяет отследить избыточность реплицированных баз данных почтовых ящиков путем проверки наличия по крайней мере двух настроенных, работоспособных и актуальных копий, а также оповещает администратора с помощью журнала событий, если существует только одна работоспособная копия реплицированной базы данных. В этом случае при определении избыточности учитываются и активная, и пассивные копии.

Условия для создания единого хранилища включают следующие варианты, но не ограничиваются ими.

- Ошибка репликации активной копии в любую пассивную копию.
- Сбой всех пассивных копий, включая состояния FailedAndSuspended и Failed, а также работоспособные состояния, когда копия не принимает участия в копировании или воспроизведении журналов. Отставание копий не учитывается, если они в течение 10 минут при воспроизведении журналов в период задержки.
- Сбой системы при определении создания текущего журнала активной копии.

Поскольку администраторы в первую очередь должны знать, когда осталась единственная работоспособная копия базы данных, сценарий CheckDatabaseRedundancy.ps1 заменен на встроенные интегрированные функции, которые входят в набор для контроля работоспособности DataProtection управляемой доступности.

Собственная функциональность по-прежнему оповещает администраторов с помощью уведомлений журнала событий. Для отличия оповещений Exchange 2013 или более поздних версий от Exchange 2010 Exchange теперь использует следующие идентификаторы событий:

- Событие 4138 (Red Alert)
- Событие 4139 (Green Alert)

Собственная функциональность была улучшена, чтобы уменьшить шум оповещений, возникающий при входе нескольких баз данных на одном сервере в одно условие копирования. В Exchange 2010 предупреждения об одной копии создавались на уровне отдельной базы данных. В результате проблема на уровне сервера, затрагивающая несколько баз данных и несколько копий баз данных,

может вызвать бурю оповещений. Так как несколько сбоев на уровне сервера (например, проблемы с контроллером или памятью), существует хорошая вероятность того, что для каждого инцидента с сервером возникнет буря оповещений.

Оповещения теперь создаются для каждого сервера. Если сбой влияет на весь сервер, а избыточность данных становится подверженной риску для нескольких копий базы данных, создается одно оповещение для каждого сервера.

Автоматическая настройка сети DAG

Сеть DAG состоит из одной или нескольких подсетей, используемых для трафика репликации или трафика MAPI. Каждая группа DAG содержит не более одной сети MAPI и 0 или более сетей репликации.

В Exchange 2010 начальные сети DAG (например, DAGNetwork01 и DAGNetwork02) были созданы системой на основе подсетей, которые были перечислены службой кластеров. Если у вас несколько сетей и интерфейсы для указанной сети (например, сети MAPI) находились в одной подсети, дополнительная настройка не требовалась. Однако если интерфейсы для указанной сети находились в нескольких подсетях, необходимо выполнить задачу, известную как сворачивание сетей DAG.

В Exchange 2013 или более поздней версии сворачивание сетей DAG больше не требуется. Exchange по-прежнему использует те же механизмы обнаружения для различия между сетями MAPI и репликации, но теперь автоматически сворачивает сети DAG по мере необходимости.

Кроме того, теперь по умолчанию сетями DAG автоматически управляет система. Чтобы просмотреть сетевые свойства DAG с помощью Центра администрирования Exchange (EAC), необходимо настроить daG для управления сетью вручную, изменив свойства DAG с помощью центра администрирования Exchange или **командлета Set-DatabaseAvailabilityGroup** , чтобы задать *параметру ManualDagNetworkConfiguration* значение `$true`.

Изменения процесса выбора оптимальной копии

Выбор оптимальной копии (BCS) — это внутренний алгоритм поиска наилучшей копии отдельной базы данных для активации при наличии списка потенциальных копий, их работоспособности и состояния. Активный диспетчер выбирает лучшую

доступную (и незаблокированную) копию в качестве новой активной копии базы данных, если существующая активная копия базы данных не работает или администратор выполняет переключение без целевой точки. В Exchange 2010 процесс BCS оценивал ряд свойств всех копий баз данных, чтобы определить "оптимальную" для активации копию. К ним относятся:

- длина очереди копирования;
- длина очереди воспроизведения;
- состояние базы данных;
- состояние индекса содержимого.

В Exchange 2013 или более поздней версии Active Manager выполняет те же проверки и этапы BCS для определения работоспособности репликации, но теперь также включает в себя использование ограничения убывающего порядка состояний работоспособности. В результате таких изменений алгоритм BCS теперь называется и выбором оптимальной копии и сервера (BCSS).

BCSS включает несколько новых проверок работоспособности, которые теперь являются частью встроенных компонентов управляемого мониторинга доступности в Exchange. Существует четыре дополнительные проверки, выполняемые Active Manager (перечислены в порядке их выполнения):

1. **Все работоспособные**. Проверяет наличие сервера, на котором размещена копия затронутой базы данных, которая содержит все компоненты мониторинга в работоспособном состоянии.
2. **До нормальной работоспособности**. Проверяет наличие сервера, на котором размещена копия затронутой базы данных, которая содержит все компоненты мониторинга с приоритетом "Обычный" в работоспособном состоянии.
3. **Все лучше, чем источник**. Проверяет наличие сервера, на котором размещена копия затронутой базы данных с компонентами мониторинга в состоянии, которое лучше, чем текущий сервер, на котором размещена затронутая копия.
4. **То же самое, что источник**: проверяет наличие сервера, на котором размещена копия затронутой базы данных, в состоянии которого находятся компоненты мониторинга, в том же состоянии, что и на текущем сервере, на котором размещена затронутая копия.

Если BCSS запускается в результате отработки отказа, которая инициируется компонентом мониторинга управляемой доступности (например, с помощью

отвечающего устройства отработки отказов), применяется дополнительное принудительное ограничение, согласно которому работоспособность компонента целевого сервера должна превышать работоспособность компонента сервера, на котором выполнялась отработка отказа. Например, если сбой Outlook в Интернете (ранее известный как Outlook Web App) активирует управляемую отработку отказа через средство отработки отказа, СЛУЖБА BCSS должна выбрать сервер, на котором размещена копия затронутой базы данных, на котором Outlook в Интернете работоспособна.

Служба управления группой обеспечения доступности баз данных (DAG)

Exchange 2013 CU2 или более поздней версии включает службу управления DAG Microsoft Exchange (MSExchangeDAGMgmt). Эта служба содержит внутренние функции мониторинга DAG, которые ранее находились в службе репликации Microsoft Exchange (MSExchangeRepl).

Группы обеспечения доступности баз данных без административной точки доступа кластера

Всем dag на серверах Exchange под управлением Windows Server 2008 R2 или Windows Server 2012 требуется по крайней мере один IP-адрес в каждой подсети, входящей в сеть MAPI. IP-адреса, назначенные группе обеспечения доступности баз данных, используются кластером этой группы с административной точкой доступа кластера (которая также называется сетевым именем кластера), чтобы включить разрешение имен и подключение к кластеру (или, что более точно, подключение к элементу кластера, который в настоящее время владеет группой ресурсов ядра кластера) с использованием имени кластера.

Windows Server 2012 R2 или более поздней версии позволяет создать отказоустойчивый кластер без административной точки доступа. Отказоустойчивые кластеры Windows без административных точек доступа отличаются приведенными ниже характеристиками.

- Кластеру не назначается IP-адрес, поэтому в группе основных ресурсов кластера нет ресурса IP-адреса.
- Кластеру не назначается сетевое имя, поэтому в группе основных ресурсов кластера нет ресурса сетевого имени.

- Имя кластера не зарегистрировано в DNS, и имя кластера не разрешается в сети.
- Объект имени кластера (CNO) не создается в Active Directory.
- Вы не можете управлять отказоустойчивый кластер Windows с помощью средства управления отказоустойчивости кластеров. Вместо этого необходимо использовать Windows PowerShell и выполнить командлеты PowerShell для отдельных членов кластера.

Exchange 2013 с пакетом обновления 1 (SP1) или более поздней версии в Exchange на Windows Server 2012 R2 или более поздней версии позволяет создать daG без точки доступа администратора кластера. Дополнительные сведения см. в разделах Создание групп доступности базданных и Создание группы доступности базы данных.

Группы доступности базы данных

Статья • 04.04.2023

Группа доступности базы данных (DAG) — это базовый компонент платформы высокой доступности и устойчивости сайта сервера почтовых ящиков, встроенной в Microsoft Exchange Server. Группа обеспечения доступности баз данных — это группа серверов почтовых ящиков (до 16 серверов), которая содержит набор баз данных и обеспечивает автоматическое восстановление на уровне базы данных после сбоя, затрагивающего отдельные серверы и базы данных.

> ⓘ **Важно!**
>
> На всех серверах в группе обеспечения доступности баз данных должна быть установлена одна и та же версия Exchange. Например, нельзя смешивать серверы Exchange 2013 и серверы Exchange 2016 в одной группе daG.

Группа обеспечения доступности баз данных — единый объект для репликации базы данных почтовых ящиков, переключений базы данных и сервера, отработок отказа и внутреннего компонента, который называется *Active Manager*. Active Manager работает на каждом сервере почтовых ящиков, управляя переключениями и отработкой отказов в группах обеспечения доступности баз данных. Дополнительные сведения о компоненте Active Manager см. в разделе Active Manager.

На любом сервере в группе обеспечения доступности баз данных можно разместить копию базы данных почтовых ящиков с любого другого сервера в группе обеспечения доступности баз данных. Если сервер добавлен в группу обеспечения доступности баз данных, он вместе с другими серверами в этой группе обеспечивает автоматическое восстановление после сбоев, затрагивающих базы данных почтовых ящиков, например после сбоев дисков, серверов или сетей.

> ⓘ **Примечание**
>
> Дополнительные сведения о создании групп обеспечения доступности баз данных, управлении членством в группах, настройке свойств групп, создании и наблюдении за состоянием копий баз данных почтовых ящиков и выполнении переключения см. в разделе **Управление высокой доступностью и устойчивостью сайтов**.

Database availability group lifecycle

Группы доступности баз данных используют концепцию *добавочного развертывания*, которая представляет собой возможность развертывания службы и доступности данных для всех серверов почтовых ящиков и баз данных после установки Exchange. После развертывания Exchange Server серверов почтовых ящиков можно создать DAG, добавить серверы почтовых ящиков в DAG, а затем реплицировать базы данных почтовых ящиков между членами DAG.

> **Примечание**
>
> Поддерживается создание daG, содержащего сочетание физических серверов почтовых ящиков и виртуализированных серверов почтовых ящиков при условии, что серверы и решение соответствуют **требованиям к системе Exchange Server** и требованиям, изложенным в **Exchange Server виртуализации**. Как и в случае любых других конфигураций обеспечения высокой доступности Exchange необходимо следить за тем, чтобы все серверы почтовых ящиков в группе обеспечения доступности баз данных имели конфигурацию, подходящую для обработки необходимой нагрузки во время запланированных и незапланированных отключений.

Группа обеспечения доступности баз данных создается с помощью командлета New-DatabaseAvailabilityGroup. Изначально группа обеспечения доступности баз данных создается как пустой объект в Active Directory. Этот объект каталога используется для хранения необходимых сведений о группе обеспечения доступности баз данных, например сведений о членстве сервера и некоторых параметров конфигурации групп обеспечения доступности баз данных. При добавлении первого сервера в группу доступности баз данных для нее автоматически создается отказоустойчивый кластер. Этот отказоустойчивый кластер используется исключительно для группы обеспечения доступности баз данных; кластер должен быть выделен для этой группы. Поддержка этого кластера для любых других целей не поддерживается.

В дополнение к созданию отказоустойчивого кластера инициируется инфраструктура, которая отслеживает серверы на наличие сбоев сети или сервера. Механизм периодических сигналов о подтверждении соединения с отказоустойчивым кластером и база данных кластера затем используются для отслеживания и обработки информации о группе доступности, которая может быстро изменяться, например о состоянии подключения базы данных, состоянии репликации и о последнем подключении.

При создании каждая группа обеспечения доступности баз данных получает уникальное имя, а также один или несколько статических IP-адресов, настраивается для использования протокола DHCP или создается без точки административного доступа кластера. DaG без административной точки доступа можно создавать только на серверах под управлением Exchange 2019, Exchange 2016 или Exchange 2013 с пакетом обновления 1 (SP1) или более поздней версии с Windows Server 2012 R2 Standard или Datacenter Edition. Группы обеспечения доступности баз данных без точки административного доступа кластера обладают следующими характеристиками:

- кластеру или группе обеспечения доступности баз данных не назначается IP-адрес, поэтому в группе основных ресурсов кластера отсутствует ресурс "IP-адрес";
- кластеру не назначается сетевое имя, поэтому в группе основных ресурсов кластера отсутствует ресурс "Сетевое имя";
- имя кластера/группы обеспечения доступности баз данных не зарегистрировано в DNS, оно неразрешимо в сети;
- в Active Directory не создается объект имени кластера (CNO);
- управлять кластером с помощью средства управления отказоустойчивым кластером нельзя. Управлять им нужно с помощью Windows PowerShell, а командлеты Windows PowerShell должны выполняться в отношении отдельных элементов кластера;

В этом примере показано, как использовать Командная консоль Exchange для создания группы обеспечения доступности баз данных с точкой административного доступа кластера, которая будет иметь три сервера. Два сервера (EX1 и EX2) находятся в одной подсети (10.0.0.0), а третий сервер (EX3) расположен в другой подсети (192.168.0.0).

PowerShell

```
New-DatabaseAvailabilityGroup -Name DAG1 -WitnessServer EX4 -
DatabaseAvailabilityGroupIPAddresses 10.0.0.5,192.168.0.5
Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer EX1
Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer EX2
Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer EX3
```

Команды для создания группы обеспечения доступности баз данных без точки административного доступа кластера очень похожи.

PowerShell

```
New-DatabaseAvailabilityGroup -Name DAG1 -WitnessServer EX4 -
DatabaseAvailabilityGroupIPAddresses ([System.Net.IPAddress])::None
Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer EX1
Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer EX2
Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer EX3
```

При добавлении сервера EX1 в группу обеспечения доступности баз данных создается кластер для группы DAG1. В ходе создания кластера командлет **Add-DatabaseAvailabilityGroupServer** получает IP-адреса, настроенные для серверов группы обеспечения доступности баз данных, и игнорирует те из них, которые не соответствуют ни одной подсети, указанной на сервере EX1. В первом примере выше для группы DAG1 создается кластер с IP-адресом 10.0.0.5, а адрес 192.168.0.5 — игнорируется. Во втором примере выше значение параметра *DatabaseAvailabilityGroupIPAddresses* вызывает задачу создания отказоустойчивого кластера для группы обеспечения доступности баз данных, у которой нет административной точки доступа. Таким образом, в группе основных ресурсов кластера создается кластер с ресурсом "IP-адрес" или "Сетевое имя".

Затем добавляется сервер EX2 и командлет **Add-DatabaseAvailabilityGroupServer** снова получает IP-адреса, указанные в конфигурации группы обеспечения доступности баз данных. IP-адреса кластера не изменяются, поскольку серверы EX2 и EX1 находятся в одной подсети.

Затем добавляется сервер EX3 и командлет **Add-DatabaseAvailabilityGroupServer** снова получает IP-адреса, указанные в конфигурации группы обеспечения доступности баз данных. Поскольку на сервере EX3 присутствует подсеть, соответствующая IP-адресу 192.168.0.5, IP-адрес 192.168.0.5 добавляется в качестве ресурса IP-адреса в кластерной группе. Дополнительно для каждого ресурса IP-адреса автоматически настраивается зависимость **OR** для ресурса сетевого имени. При перемещении группы основных ресурсов кластера на сервер EX3 кластер будет использовать адрес 192.168.0.5.

При переводе ресурса сетевого имени в оперативный режим средство отказоустойчивости кластеров Windows регистрирует IP-адреса кластера в службе DNS для групп обеспечения доступности баз данных с точками административного доступа кластера. Кроме того, когда к кластеру добавляется EX1, в Active Directory создается объект имени кластера (CNO). Для функций DAG сетевое имя, IP-адрес (IP-адреса) и CNO кластера не используются. Администраторам и конечным пользователям нет необходимости обращаться или подключаться к кластеру/имени группы обеспечения доступности баз данных или IP-адресу. Некоторые сторонние приложения подключаются к точке доступа администратора кластера

для выполнения задач управления, таких как резервное копирование или мониторинг. Если вы не используете сторонние приложения, которым требуется точка доступа администрирования кластера, и daG работает под управлением Exchange 2016 или Exchange 2019 на Windows Server 2012 R2, рекомендуется создать daG без административной точки доступа. Такой подход упрощает настройку DAG, устраняет необходимость в одном или нескольких IP-адресах и сокращает площадь атаки DAG.

Группы обеспечения доступа к базам данных также настраиваются для использования следящего сервера и следящего каталога. Следящий сервер и следящий каталог либо автоматически настраиваются системой, либо настраиваются администратором вручную. В приведенных выше примерах выполняется настройка EX4 (сервера, который не входит и не будет входить в DAG) в качестве следящего сервера DAG.

По умолчанию группа обеспечения доступности баз данных предназначена для использования встроенной функции непрерывной репликации для репликации баз данных почтовых ящиков между серверами в группе обеспечения доступности баз данных. Если вы используете стороннюю репликацию данных, которая поддерживает API репликации сторонних поставщиков в Exchange Server, необходимо создать daG в режиме репликации сторонних производителей с помощью командлета New-DatabaseAvailabilityGroup с параметром *ThirdPartyReplication*. После включения этот режим нельзя отключить.

После создания группы обеспечения доступности баз данных можно добавить серверы почтовых ящиков. После добавления в группу обеспечения доступности баз данных первого сервера для группы создается кластер. Группы обеспечения доступности баз данных используют функции, предоставляемые технологией отказоустойчивой кластеризации Windows: пульс кластера, сети кластера и база данных кластера (для хранения изменяющихся данных, например изменений состояния базы данных с активного на пассивное или наоборот либо с подключенного состояния на отключенное и наоборот). По мере добавления в группу обеспечения доступности баз данных серверы присоединяются к базовому кластеру, система Exchange автоматически настраивает модель кворума кластера, и серверы добавляются в объект группы обеспечения доступности баз данных в Active Directory.

После добавления серверов почтовых ящиков в группу обеспечения доступности баз данных можно настроить различные свойства группы обеспечения доступности баз данных, например указать, требуется ли шифрование и сжатие в сети при репликации базы данных в группе обеспечения доступности баз данных. Кроме того, можно настроить сети групп обеспечения доступности баз данных и

при необходимости создать дополнительные сети групп обеспечения доступности баз данных.

После добавления членов в группу обеспечения доступности баз данных и настройки группы можно реплицировать активные базы данных почтовых ящиков на каждом сервере на других членов группы обеспечения доступности баз данных. Для отслеживания работоспособности и состояния созданных копий баз данных почтовых ящиков используются различные встроенные средства наблюдения. Кроме того, при необходимости можно выполнять переключение базы данных и сервера.

Модели кворума группы обеспечения доступности баз данных

Каждая группа обеспечения доступности баз данных основана на отказоустойчивом кластере Windows. Отказоустойчивые кластеры используют концепцию кворума, в которой согласованность участников кворума применяется для обеспечения того, что одновременно функционирует только одно подмножество членов кластера (куда могут входить все члены или большинство членов). Кворум не является новой концепцией для Exchange Server. Высокодоступные серверы почтовых ящиков в предыдущих версиях Exchange также работали в отказоустойчивых кластерах с использованием концепции кворума. Кворум представляет общее представление членов и ресурсов, а сам термин «кворум» также используется для описания физических данных, которые представляют конфигурацию в кластере, совместно используемую всеми членами кластера. В результате все группы обеспечения доступности баз данных требуют от базового отказоустойчивого кластера наличия кворума. Если кластер теряет кворум, все операции группы обеспечения доступности баз данных завершаются, а все подключенные базы данных, размещенные в этой группе, отключаются. В этом случае для исправления проблемы с кворумом и восстановления выполнения операций группы обеспечения доступности баз данных требуется вмешательство администратора.

Кворум очень важен для обеспечения согласованности, разрешения конфликтов с целью предотвращения разделения и обеспечения отклика кластера.

- **Обеспечение согласованности**. Основное требование для отказоустойчивого кластера Windows заключается в том, что каждый из членов всегда имеет представление кластера, согласованное с другими членами. Куст кластера выполняет роль всеобъемлющего репозитория всех конфигурационных данных, имеющих отношение к этому кластеру. Если куст кластера не может

быть загружен локально на члене группы обеспечения доступности баз данных, служба кластера не запускается, так как не может гарантировать согласованность представления кластера на этом члене представлению кластера на всех остальных членах.

- **Выступая в качестве разбиения связей**: ресурс свидетеля кворума используется в DAG с четным числом членов, чтобы избежать сценариев синдрома разделения мозга и убедиться, что только одна коллекция членов в DAG считается официальной. Если для кворума нужен сервер-свидетель, любой член группы обеспечения доступности может связаться с сервером-свидетелем и поместить блокировку SMB на файл witness.log этого сервера. Член группы обеспечения доступности, который блокирует сервер-свидетель (называется *блокирующим узлом*) сохраняет дополнительный голос для кворума. Члены группы обеспечения доступности баз данных, поддерживающие связь с блокирующим узлом, представляют собой большинство и тем самым поддерживают кворум. Любые члены группы обеспечения доступности баз данных, которые не могут связаться с блокирующим узлом, являются меньшинством и теряют кворум.

- **Обеспечение скорости реагирования**. Чтобы обеспечить скорость реагирования, модель кворума гарантирует, что при каждом запуске кластера достаточное количество членов распределенной системы являются операционными и коммуникативными, и по крайней мере одна реплика текущего состояния кластера может быть гарантирована. Не требуется дополнительного времени для установки связи с членами или для определения наличия определенной реплики.

Группы доступности баз данных с четным количеством членом используют режим кворума большинства узлов и общих файловых ресурсов, в котором разрешением конфликтов занимается внешний сервер-свидетель. В этом режиме кворума каждый член группы обеспечения доступности баз данных получает один голос. Кроме того, используется следящий сервер для предоставления одному члену группы взвешенный голос (то есть он получает два голоса вместо одного). Данные кворума кластера сохраняются по умолчанию на системном диске каждого члена группы обеспечения доступности баз данных и поддерживается в согласованном состоянии на всех дисках. Однако копия данных кворума не сохраняется на следящем сервере. Файл на следящем сервере используется для отслеживания того, какой член имеет наиболее обновленную копию данных, но сам следящий сервер не имеет копию данных кворума кластера. В этом режиме большинство голосующих членов (члены группы обеспечения доступности и сервер-свидетель) должны находиться в рабочем состоянии и поддерживать связь друг с другом для обеспечения кворума. Если большинство голосующих не может связаться друг с

другом, кластер группы обеспечения доступности теряет кворум и группа обеспечения доступности баз данных будет нуждаться во вмешательстве администратора, чтобы снова стать работоспособной. Дополнительные сведения см. в разделах Переключения центров обработки данных и Restore-DatabaseAvailabilityGroup.

Группы обеспечения доступности баз данных с нечетных количеством членов используют режим кворума большинства узлов. В этом режиме каждый член получает голос, локальный системный диск каждого члена используется для хранения данных кворума кластера. При изменении конфигурации группы обеспечения доступности это изменение отражается на всех дисках. Изменение считается вступившим в силу и согласованным, если был внесено на дисках половины членов (с округлением в сторону понижения) плюс один. Например, в группе обеспечения доступности баз данных с пятью членами изменение должно быть внесено на двух членах плюс один, то есть на трех членах.

Кворум собирается большинством голосующих членов, которые могут поддерживать связь друг с другом. Рассмотрим группу обеспечения доступности баз данных, состоящую из четырех членов. Так как эта группа имеет четное количество членов, внешний следящий сервер используется для предоставления одному из членов кластера пятого голоса для разрешения конфликтов. Чтобы обеспечить большинство голосующих (и, следовательно, наличие кворума), хотя бы три голосующих члена должны поддерживать связь друг с другом. В любое время не более двух голосующих члена может находиться в автономном режиме, не влияя на работу службы и доступа к данным. Если три и более голосующих члена находятся в автономном режиме, группа обеспечения доступности баз данных теряет кворум, служба и данные перестают быть доступными до устранения проблемы.

Exchange Server Active Manager

Статья • 04.04.2023

Microsoft Exchange Server включает компонент *Active Manager*, который управляет платформой высокого уровня доступности, которая включает в себя группу доступности базы данных (DAG) и копии базы данных почтовых ящиков. Active Manager выполняется внутри службы репликации Microsoft (MSExchangeRepl.exe) на всех серверах почтовых ящиков. На серверах почтовых ящиков, которые не входят в DAG, существует единая роль Active Manager: *Standalone Active Manager*.

На серверах, которые являются участниками группы обеспечения доступности баз данных, существуют две роли Active Manager: *Primary Active Manager* (PAM) и *Standby Active Manager* (SAM). Роль PAM — это экземпляр Active Manager в группе обеспечения доступности баз данных, принимающий решения о том, какие копии будут пассивными, а какие — активными. PAM отвечает за получение уведомлений об изменении топологии и реакцию на сбои серверов. Член группы обеспечения доступности баз данных, которому принадлежит роль PAM, всегда является текущим владельцем ресурса кворума кластера (кластерной группы по умолчанию). Если на сервере-владельце ресурса кворума кластера происходит сбой, роль PAM автоматически перемещается на оставшийся сервер, который становится новым владельцем ресурса кворума кластера. Кроме того, если сервер, на котором размещен ресурс кворума кластера, необходимо перевести в автономный режим для обслуживания или обновления, сначала следует перенести роль PAM на другой сервер группы обеспечения доступности баз данных. Роль PAM контролирует все передвижения активных назначений между копиями баз данных. (Только одна копия в любой момент времени может быть активной, и она может быть подключенной или отключенной.) Роль PAM также выполняет функции роли SAM на локальном компьютере (обнаружение сбоев локальных баз данных и банка данных).

Роль SAM предоставляет сведения о том, на каком сервере размещается активная копия базы данных почтовых ящиков, другим компонентам Exchange, использующим клиентский компонент Active Manager (например, службе клиентского доступа или транспортной службе). Роль SAM обнаруживает сбои локальных баз данных и локального банка данных. Она реагирует на сбои, запрашивая у роли PAM отработку отказа (если база данных реплицирована). Роль SAM не определяет целевой сервер отработки отказа и не обновляет состояние расположения базы данных в роли PAM. Она обращается к состоянию расположения активной копии базы данных для ответа на получаемые запросы активной копии базы данных.

ⓘ Примечание

Exchange Server не является кластеризованным приложением. Вместо этого функции библиотеки кластеризации clusapi.dll используются для реализации функциональности кластера, групп, сети кластера (пульса), управления узлами, реестра кластера и ряда задач управления. Кроме этого, служба Active Manager хранит сведения о текущем состоянии базы данных почтовых ящиков (данные об активных и пассивных копиях, а также о подключении) в базе данных кластера (также называется реестром кластера). Хотя эти сведения хранятся непосредственно в базе данных кластера, к ним не обращаются напрямую никакие другие компоненты.

В Exchange Server служба репликации Microsoft Exchange периодически отслеживает работоспособность всех подключенных баз данных. Кроме этого, она также отслеживает ошибки и сбои ввода-вывода подсистемы ESE. Если служба обнаруживает сбой, она уведомляет о нем службу Active Manager. Затем Active Manager определяет, какую копию базы данных следует подключить, и что для этого необходимо. Кроме того, она отслеживает активную копию базы данных почтовых ящиков (на основании сведений о копии базы данных, подключенной последней) и предоставляет сведения о результатах отслеживания службам клиентского доступа на сервере почтовых ящиков, к которому подключен клиент.

Лучший выбор копирования

При возникновении сбоя, препятствующего доступу к активной копии реплицированной базы данных почтовых ящиков, Active Manager выбирает оптимальную пассивную копию сбойной базы данных, которая будет активирована. Этот процесс был известен как выбор лучшей копии (BCS) в более ранних версиях Exchange, а в Exchange 2016 и Exchange 2019 он известен как выбор лучшей копии и сервера (BCSS). Общий процесс выглядит следующим образом:

1. Компонент «Управляемая доступность» или Active Manager определяет сбой или администратор инициирует переключение без цели.

2. PAM запускает внутренний алгоритм BCSS.

3. Выполняется процесс, называемый *попыткой копирования последних журналов* (ACLL), в ходе которого предпринимается попытка скопировать с сервера все отсутствующие файлы журналов, находившиеся в активной копии базы данных до отказа или переключения.

4. После завершения процесса ACLL значение *AutoDatabaseMountDial* для серверов почтовых ящиков, на которых хранятся копии базы данных, сравнивается с длиной очереди копирования базы данных, которая активируется. На этом этапе выполняется одно из следующих действий:

    - количество отсутствующих файлов журнала равно или меньше значения *AutoDatabaseMountDial*, в таком случае выполняется шаг 5; или

    - количество отсутствующих файлов журнала превышает значение *AutoDatabaseMountDial*, в таком случае Active Manager попытается активировать следующую наиболее доступную копию, если такая существует.

5. PAM создает запрос на установку в банк данных Microsoft Exchange через удаленный вызов процедур (RPC). На этом этапе выполняется одно из следующих действий:

    - база данных подключается и становится доступной для клиентов; или

    - база данных не подключается, и PAM выполняет действия 3 и 4 для следующей оптимальной копии (если она доступна).

В более ранних версиях Exchange процесс BCS оценивал ряд свойств всех копий баз данных, чтобы можно было определить оптимальную для активации копию. К ним относятся:

- длина очереди копирования;

- длина очереди воспроизведения;

- состояние базы данных;

- состояние индекса содержимого.

В Exchange Server Active Manager выполняет все те же проверки и этапы BCS, но теперь он также включает в себя использование ограничения убывающей последовательности состояний работоспособности. В частности, BCSS включает несколько новых проверок работоспособности, которые входят в состав встроенных компонентов мониторинга управляемой доступности в Exchange Server. Active Manager теперь выполняет четыре дополнительных проверки (перечисление в порядке выполнения):

1. **Все работоспособные**. Проверяет наличие сервера, на котором размещена копия затронутой базы данных, которая содержит все компоненты мониторинга в работоспособном состоянии.

2. **До нормальной работоспособности**. Проверяет наличие сервера, на котором размещена копия затронутой базы данных, которая содержит все компоненты мониторинга с приоритетом "Обычный" в работоспособном состоянии.

3. **Все лучше, чем источник**. Проверяет наличие сервера, на котором размещена копия затронутой базы данных с компонентами мониторинга в состоянии, которое лучше, чем текущий сервер, на котором размещена затронутая копия.

4. **То же самое, что источник**: проверяет наличие сервера, на котором размещена копия затронутой базы данных, в состоянии которого находятся компоненты мониторинга, в том же состоянии, что и на текущем сервере, на котором размещена затронутая копия.

Если BCSS будет вызвано в результате отработки отказа, активированного компонентом наблюдения (т. е. через отвечающее устройство отработки отказов), вводится в действие дополнительное обязательное ограничение, устанавливающее, что работоспособность компонента целевого сервера должна быть выше, чем у сервера, на котором произошел сбой. Например, если отказ Outlook в Интернете активирует отработку отказа через отвечающее устройство отработки отказов, BCSS должен выбрать сервер с копией отказавшей базы данных, на котором Outlook в Интернете работоспособен.

Процесс выбора оптимальной копии

По отношению к отказам базы данных (не отказам компонентов) Active Manager начинает процесс выбора оптимальной копии с создании списка копий базы данных, которые являются потенциальными кандидатами для активации. Все недоступные или административно заблокированные для активации копии базы данных игнорируются и не используются во время процесса выбора. Порядок расположения копий в списке зависит от значения *AutoDatabaseMountDial*:

- Если *параметр AutoDatabaseMountDial* настроен с любым значением, отличным `Lossless` от всех серверов, на которых размещена копия базы данных, Active Manager сортирует результирующий список, используя длину очереди копирования в качестве первичного ключа. Вычисление выполняется на основании LastLogInspected (с точки зрения копии), поэтому список потенциальных копий сортируется по наибольшему значению LastLogInspected (копия с наименьшей длиной очереди копирования). Если необходимо, Active Manager сортирует список второй раз, используя значение предпочтения активации в качестве вторичного ключа, чтобы разорвать все условия связывания, при которых две или больше пассивных копии имеют

одинаковую длину очереди копирования. Копия с наименьшим значением предпочтения активации имеет наибольший приоритет в списке.

- Если *параметр AutoDatabaseMountDial* настроен со значением `Lossless` на любом сервере, на котором размещена копия базы данных, Active Manager сортирует результирующий список в порядке возрастания, используя значение параметра активации в качестве первичного ключа. Кроме того, когда администратор выполняет переключение базы данных или сервера без потерь, не указывая цель, Active Manager также сортирует список результатов по возрастанию, используя значение предпочтения активации в качестве первичного ключа.

Далее Active Manager пытается найти в списке копию базы данных почтовых ящиков в состоянии Healthy, DisconnectedAndHealthy, DisconnectedAndResynchronizing или SeedingSource и оценивает потенциал активации каждой копии в списке на основе упорядоченного набора из десяти условий. Active Manager определяет, отвечает ли какой-либо кандидат для активации первому набору условий:

- Индекс содержимого имеет состояние Healthy (исправен).
- Длина очереди копирования файлов журнала меньше 10.
- Длина очереди преобразования файлов журнала меньше 50.

Если ни одна копия базы данных не отвечает первому набору условий, Active Manager пытается найти копию базы данных, отвечающую второму набору условий:

- Индекс содержимого имеет состояние Crawling (сканирование).
- Длина очереди копирования файлов журнала меньше 10.
- Длина очереди преобразования файлов журнала меньше 50.

Если ни одна копия базы данных не отвечает второму набору условий, Active Manager пытается найти копию базы данных, отвечающую третьему набору условий:

- Индекс содержимого имеет состояние Healthy (исправен).
- Длина очереди преобразования файлов журнала меньше 50.

Если ни одна копия базы данных не отвечает третьему набору условий, Active Manager пытается найти копию базы данных, отвечающую четвертому набору

условий:

- Индекс содержимого имеет состояние Crawling (сканирование).
- Длина очереди преобразования файлов журнала меньше 50.

Если ни одна копия базы данных не отвечает четвертому набору условий, Active Manager пытается найти копию базы данных, отвечающую пятому набору условий:

- Длина очереди преобразования файлов журнала меньше 50.

Если ни одна копия базы данных не отвечает пятому набору условий, Active Manager пытается найти копию базы данных, отвечающую шестому набору условий:

- Индекс содержимого имеет состояние Healthy (исправен).
- Длина очереди копирования файлов журнала меньше 10.

Если ни одна копия базы данных не отвечает шестому набору условий, Active Manager пытается найти копию базы данных, отвечающую седьмому набору условий:

- Индекс содержимого имеет состояние Crawling (сканирование).
- Длина очереди копирования файлов журнала меньше 10.

Если ни одна копия базы данных не отвечает седьмому набору условий, Active Manager пытается найти копию базы данных, отвечающую восьмому набору условий:

- Индекс содержимого имеет состояние Healthy (исправен).

Если ни одна копия базы данных не отвечает восьмому набору условий, Active Manager пытается найти копию базы данных, отвечающую девятому набору условий:

- Индекс содержимого имеет состояние Crawling (сканирование).

Если ни одна копия базы данных не отвечает девятому набору условий, Active Manager пытается активировать любую копию базы данных в состоянии Healthy, DisconnectedAndHealthy, DisconnectedAndResynchronizing или SeedingSource (десятый набор условий). Если копии, отвечающие десятому набору условий, не удается найти, автоматическая активация копии базы данных невозможна.

Как только будут найдены одна или несколько копий, отвечающих хотя бы одному набору условий, процесс ACLL копирует все файлы журналов из источника в потенциальную новую активную копию. По завершении этого процесса PAM выдает запрос на подключение, и либо база данных подключается и становится доступной для клиентов, либо база данных не подключается и PAM ищет следующую оптимальную копию (если она доступна).

Режим координации активации центра обработки данных в Exchange Server

Статья • 04.04.2023

Режим координации активации центра данных DAC (Datacenter Activation Coordination) — это свойство группы доступности базы данных DAG (Database Availability Group). Режим DAC отключен по умолчанию и должен включаться для всех групп обеспечения доступности базы данных (DAG), в которых используется непрерывная репликация. Необходимо отключить режим DAC для групп DAG, использующих режим сторонней репликации, если обратное не указано сторонним поставщиком.

Режим DAC используется для управления подключением баз данных при запуске групп DAG. Это средство позволяет предотвратить разделение вычислительных мощностей на уровне баз данных при смене центра обработки данных. *Разделение вычислительных мощностей* — это состояние, которое приводит к тому, что база данных подключается в качестве активной копии к двум членам одной группы DAG, которые не могут связаться друг с другом. Этого можно избежать с помощью режима DAC, так как этот режим требует, чтобы члены групп DAG получали разрешение на подключение баз данных.

Например, когда основной центр обработки данных содержит двух членов группы DAG и следящий сервер, а второй центр содержит двух других членов группы DAG, группа DAG не находится в режиме DAC. Когда основной центр обработки данных теряет питание, вы активируете DAG во втором центре. Когда питание основного центра восстанавливается, члены группы DAG в основном центре обработки данных, обладающие кворумом до перебоя питания, будут запущены и подключены к базам данных. Так как основной центр обработки данных был восстановлен без сетевого подключения ко второму центру, а группа DAG не находилась в режиме DAC, в активных базах данных группы DAG произошло разделение вычислительных мощностей.

Как работает режим DAC

Режим DAC включает протокол DACP (Datacenter Activation Coordination Protocol). В режиме DAC члены группы DAG не будут автоматически подключать базы данных, даже если обладают кворумом. Вместо этого с помощью DACP определяется

текущее состояние группы DAG и необходимость подключения баз данных с помощью диспетчера Active Manager.

Режим DAC можно представить как уровень приложения кворума для подключения баз данных. Чтобы понять назначение протокола DACP и принцип его работы, важно изучить основной сценарий, для работы с которым предназначен этот протокол. Рассмотрим сценарий для двух центров обработки данных, описанный выше. Предположим, что в основном центре произошел полный сбой питания. В этом случае нарушается работа всех серверов и глобальной сети, поэтому организация принимает решение активировать резервный центр обработки данных. Почти во всех таких сценариях восстановления, когда возобновляется питание основного центра обработки данных, подключение к глобальной сети обычно восстанавливается не сразу. Это означает, что члены группы DAG в основном центре подключаются к питанию, но они не могут установить связь с членами DAG в активированном резервном центре обработки данных. Основной центр обработки данных должен всегда содержать большинство участников кворума DAG, что означает: когда возобновляется питание, даже если отсутствует подключение глобальной сети к членам DAG в резервном центре обработки данных, члены DAG в основном центре имеют большинство и, как результат, кворум. Это представляет собой проблему, так как при наличии кворума эти серверы могут подключаться к своим базам данных, что будет приводить к расхождению с текущими активными базами данных, которые теперь подключены в активированном резервном центре обработки данных.

Протокол DACP был создан для решения этой проблемы. Диспетчер Active Manager хранит бит в памяти (0 либо 1), который указывает, разрешено ли группе DAG подключать локальные базы данных, которые назначены в качестве активных на сервере. Когда группа DAG работает в режиме DAC, при каждом запуске диспетчера Active Manager задается значение 0, которое означает, что ей не разрешено подключать базы данных. Так как сервер находится в режиме DAC, он должен установить связь со всеми известными ему другими участниками DAG, чтобы сообщить другому участнику DAG о том, можно ли подключать локальные базы данных, которые назначены в качестве активных. Ответ поступает в форме битового параметра для других диспетчеров Active Manager в группе DAG. Если другой сервер отвечает, что бит равен 1, то это означает, что серверам разрешено подключаться к базам данных, поэтому при запуске сервера для бита устанавливается значение 1 и подключаются его базы данных.

Но при восстановлении после сбоя питания основного центра данных, когда серверы восстанавливаются, но подключение к глобальной сети не восстановлено, все участники DAG в основном центре получают нулевое значение бита DACP; поэтому ни один из серверов, начинающих архивацию в восстановленном

основном центре, не подключит базы данных, так как ни один из них не может установить связь с участником DAG, имеющим значение бита DAG, равное 1.

Режим DAC для DAG с двумя участниками

Группы DAG с двумя членами наследуют ограничения, которые предотвращают обеспечение полной защиты от синдрома разделенности на уровне приложения только битом DACP. В группах DAG только с двумя членами режим DAC также использует время загрузки следящего сервера группы для определения возможности подключения баз данных при запуске. Время загрузки следящего сервера сравнивается со временем, когда бит DACP имел значение 1.

- Если время установки бита DACP предшествует времени загрузки следящего сервера, система предполагает, что член группы DAG и следящий сервер были перезагружены одновременно (возможно, из-за отключения питания основного центра обработки данных), и члену группы DAG не разрешается подключать базы данных.
- Если время установки бита DACP значительно предшествует времени загрузки следящего сервера, система предполагает, что член группы DAG был перезагружен по другой причине (возможно, из-за запланированного отключения для обслуживания или в результате сбоя системы или отключения питания на сервере группы DAG), и члену группы DAG разрешается подключить базы данных.

> ⓘ **Важно!**
>
> Так как время загрузки следящего сервера используется для определения возможности подключения участником группы DAG своих активных баз данных при запуске, следящий сервер и единственного участника группы DAG нельзя перезагружать одновременно. В противном случае участник группы обеспечения доступности баз данных может остаться в состоянии, в котором он не сможет подключать базы данных при запуске. В этом случае необходимо запустить командлет **Restore-DatabaseAvailabilityGroup** в группе обеспечения доступности баз данных. При этом будет переустановлен бит DACP, что позволит члену группы DAG подключить базы данных.

Другие преимущества режима DAC

Помимо защиты от синдрома разделенности на уровне приложения режим DAC позволяет использовать встроенные командлеты для устойчивости сайтов для переключения центра обработки данных. например:

- Stop-DatabaseAvailabilityGroup
- Restore-DatabaseAvailabilityGroup
- Start-DatabaseAvailabilityGroup

Выполнение переключения центра обработки данных для групп доступности базы данных, которые не входят в режим DAC, предполагает использование сочетания средств Exchange и средств управления кластером. Дополнительные сведения см. в разделе Переключения центров обработки данных.

Включение режима DAC

Режим DAC можно включить только в командной консоли Exchange. В частности, для включения режима DAC можно использовать командлет Set-DatabaseAvailabilityGroup, как это проиллюстрировано в следующем примере.

PowerShell

```
Set-DatabaseAvailabilityGroup -Identity DAG2 -DatacenterActivationMode
DagOnly
```

В предыдущем примере режим DAC включается для группы обеспечения доступности баз данных DAG2.

Дополнительные сведения о включении режима DAC см. в разделах Настройка свойств группы обеспечения доступности баз данных и Set-DatabaseAvailabilityGroup.

Копии базы данных почтовых ящиков в Exchange Server

Статья • 04.04.2023

Microsoft Exchange Server использует концепцию мобильности базы данных, которая представляет собой отработку отказа на уровне базы данных, управляемой Exchange. Функция мобильности баз данных устраняет привязку баз данных к серверам, обеспечивает поддержку до 16 копий одной базы данных и предлагает собственную систему добавления копий базы данных.

Основные характеристики

Ниже перечислены основные характеристики копий базы данных почтовых ящиков.

- На нескольких серверах почтовых ящиков можно создать до 16 копий базы данных почтовых ящиков Exchange Server при условии, что серверы группируются в группу доступности базы данных (DAG), которая является границей для непрерывной репликации. Exchange Server базы данных почтовых ящиков можно реплицировать только на серверы почтовых ящиков Exchange той же версии в daG. Невозможно реплицировать базу данных за пределами DAG, а также базу данных почтовых ящиков Exchange 2016 или Exchange 2019 на сервер под управлением Exchange 2013 или более ранней версии. Подробные сведения о группах доступности баз данных см. в разделе Группы доступности баз данных.

- Все серверы почтовых ящиков в группе обеспечения доступности баз данных должны находиться в одном домене Active Directory.

- Копии базы данных почтовых ящиков поддерживают концепции времени запаздывания преобразования и времени запаздывания усечения. Перед включением этих функций необходимо выполнить надлежащее планирование.

- Для любой копии базы данных можно создать резервную копию с помощью приложения резервного копирования на основе службы теневого копирования томов (VSS), совместимого с Exchange.

- Копии баз данных могут создаваться только на серверах почтовых ящиков, где не размещаются активные копии базы данных. При этом нельзя создать две

копии одной базы данных на одном и том же сервере.

- Все копии базы данных используют один и тот же путь на всех серверах, где хранятся копии. Пути баз данных и файлов журналов копий баз данных на всех серверах почтовых ящиков не должны конфликтовать с путями других баз данных.

- Копии баз данных можно создавать в одном и том же сайте Active Directory или в разных сайтах, а также в одной и той же или разных подсетях.

- Копии баз данных не поддерживаются на серверах почтовых ящиков, задержка сетевого кругового пути между которыми превышает 500 миллисекунд.

Копии базы данных почтовых ящиков

Копию базы данных почтовых ящиков можно создать в любое время. Копии баз данных почтовых ящиков можно распределять по серверам почтовых ящиков гибко и детализованно.

Вы можете создать копию базы данных почтовых ящиков с помощью мастера **добавления копирования базы данных почтовых ящиков** в Центре администрирования Exchange или с помощью командлета **Add-MailboxDatabaseCopy** в командной консоли Exchange.

При создании копии базы данных почтовых ящиков укажите следующие параметры.

- *Identity*: этот параметр указывает имя копируемых баз данных. Имена баз данных должны быть уникальными в пределах организации Exchange.

- *MailboxServer*: этот параметр указывает имя сервера почтовых ящиков, на котором будет размещена копия базы данных. Сервер должен входить в ту же группу обеспечения доступности баз данных и не может уже содержать копию этой базы данных.

Дополнительно можно указать следующие параметры.

- *ActivationPreference*: этот параметр указывает номер предпочтения активации, который используется в процессе выбора оптимального копирования Active Manager. Он также используется для перераспределения активных баз данных почтовых ящиков в группе обеспечения доступности баз данных при использовании сценария RedistributeActiveDatabases.ps1. Значение приоритета активации — это число, равное или больше 1, где 1 означает

самый высокий приоритет. Номер позиции не может быть больше числа копий базы данных почтовых ящиков.

- *ReplayLagTime*: этот параметр указывает время ожидания службы репликации Microsoft Exchange перед воспроизведением файлов журнала, скопированных в копию базы данных. Параметр имеет следующий формат: (дни.часы:минуты:секунды). По умолчанию для этого параметра используется значение 0 секунд. Максимальное допустимое значение — 14 дней. Минимально допустимое значение равно 0 секунд. Если задать для него значение 0, задержка преобразования журнала будет отключена.

- *TruncationLagTime*: этот параметр указывает время ожидания службы репликации Microsoft Exchange перед усечением файлов журнала, которые были воспроизведены в копии базы данных. Отсчет времени начинается с момента успешного преобразования журнала в копию базы данных. Параметр имеет следующий формат: (дни.часы:минуты:секунды). По умолчанию для этого параметра используется значение 0 секунд. Максимальное допустимое значение — 14 дней. Минимально допустимое значение равно 0 секунд. Если задать для него значение 0, задержка усечения журнала будет отключена.

- *SeedingPostponed*: этот параметр указывает, что задача не должна автоматически заполнять копию базы данных на указанном сервере почтовых ящиков. Данный параметр обычно используется, когда требуется заполнять новую копию базы данных почтовых ящиков на основе существующей пассивной копии (например, при добавлении второй копии определенной базы данных в удаленное расположение). При использовании этого параметра необходимо вручную заполнить копию базы данных при помощи командлета Update-MailboxDatabaseCopy.

Дополнительные сведения о создании, использовании и управлении копиями базы данных почтовых ящиков см. в разделе Управление копиями базы данных почтовых ящиков.

Сведения об автоматическом использовании

Статья • 04.04.2023

Автоматическое повторное повторение или автоматическое восстановление — это функция, которая заменяет стандартные действия, выполняемые администраторами в ответ на сбой диска, событие повреждения базы данных или другую проблему, для чего требуется повторное заполнение копии базы данных.

Общие сведения о функции Autoreseed

В конфигурации AutoReseed используется стандартизованная структура представления хранилища и администратор выбирает начальную точку. Функция AutoReseed позволяет после сбоя диска восстановить избыточность как можно скорее. Это включает использование точек подключения для предварительного сопоставления набора томов (включая запасные тома) и баз данных. Если произошел сбой диска, когда диск больше недоступен для операционной системы или больше не доступен для записи, система выделяет резервный том, а затронутые копии базы данных повторно заполняются автоматически.

1. Служба репликации Microsoft Exchange периодически выполняет сканирование на наличие копий в состоянии FailedAndSuspended. Если все копии базы данных на томе, настроенном для autoReseed, находятся в состоянии FailedandSuspended в течение 15 минут подряд, запускается рабочий процесс AutoReseed.

2. AutoReseed попытается возобновить неудачные и приостановленные копии до трех раз, с 5-минутным спящем режимом между каждой попыткой. Иногда после возобновления копирования базы данных FailedandSuspended копия остается в состоянии Сбоя. Это может произойти по разным причинам, поэтому этот шаг предназначен для обработки таких случаев; Функция AutoReseed автоматически приостановит копию базы данных, которая завершилась ошибкой в течение 10 минут подряд, чтобы сохранить рабочий процесс. Если действия приостановки и возобновления не приводят к работоспособной копии базы данных, рабочий процесс продолжается.

3. При поиске копии с таким состоянием выполняется ряд проверок предварительных требований. Например, будет проверено, достаточно ли на диске свободного пространства, находятся ли база данных и файлы журналов

в одном томе и в допустимых расположениях, соответствующих соглашениям об именах.

4. Если проверка готовности успешно пройдена, функция Восстановления дисков в службе репликации Microsoft Exchange выделяет, сопоставляет и форматирует резервный диск в соответствии с временными шкалами, приведенными в таблице ниже. AutoReseed попытается назначить резервный том до пяти раз, с одним часом спящего режима между каждой попыткой.

5. После назначения запасного файла autoReseed выполнит операцию InPlaceSeed с помощью переключателя заполнения SafeDeleteExistingFiles. Все базы данных, которые находились на затронутом диске, повторно заполняются с помощью активной копии базы данных в качестве источника заполнения.

6. После завершения заполнения служба репликации Microsoft Exchange проверяет работоспособность только что заполненной копии.

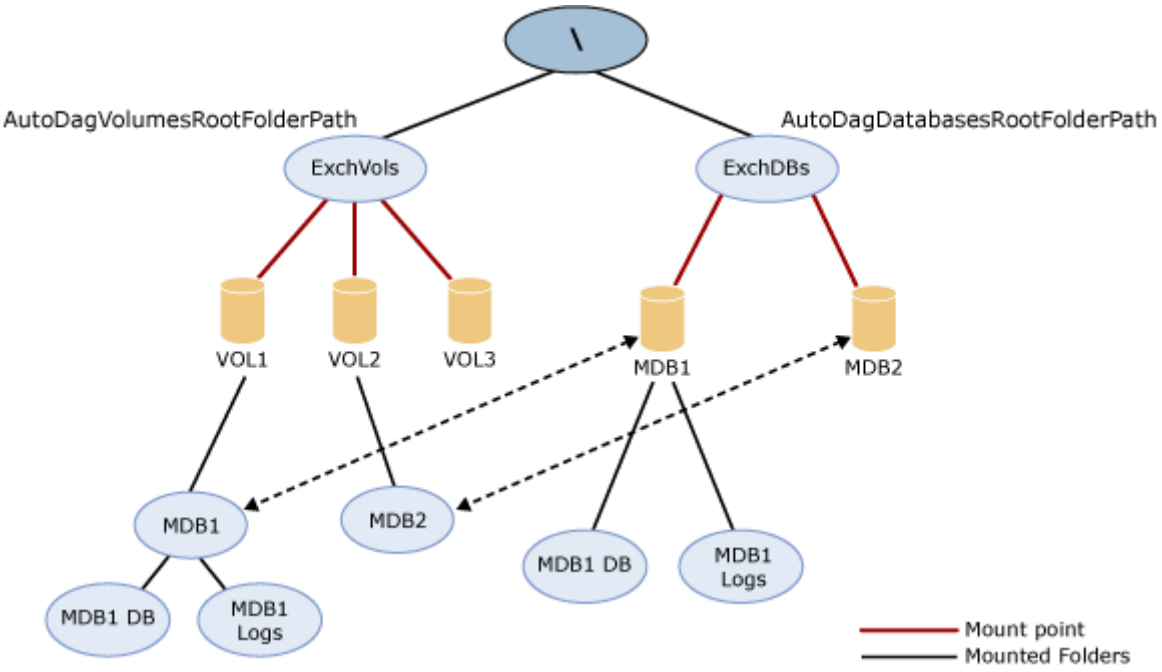
По достижении максимального числа попыток рабочий процесс останавливается. Если по истечении трех дней копия базы данных по-прежнему завершается failed andSuspended, состояние рабочего процесса сбрасывается и начинается снова с шага 1. Такое поведение сброса и возобновления является полезным (и преднамеренным), так как замена диска, контроллера и т. д. может занять несколько дней.

На этом этапе, если произошел отказ диска, потребуется вмешательство оператора или администратора, чтобы удалить и заменить отказавший диск, а затем повторно настроить заменяющий диск в качестве резервного.

AutoReseed настраивается с помощью трех свойств группы обеспечения доступности баз данных. Два из них относятся к двум используемым точкам подключения. Exchange Server используется тот факт, что Windows Server разрешает несколько точек подключения на том. Свойство *AutoDagVolumesRootFolderPath* относится к точке подключения, содержащей все доступные тома. Она включает в себя тома, на которых размещаются базы данных, и резервные тома. Свойство *AutoDagDatabasesRootFolderPath* относится к точке подключения, содержащей базы данных. Третье свойство DAG, *AutoDagDatabaseCopiesPerVolume*, используется для настройки количества копий базы данных на том.

Ниже приведен пример конфигурации AutoReseed.

Пример конфигурации AutoReseed



В этом примере используются три тома, два из которых содержат базы данных (VOL1 и VOL2), а один пустой. Он отформатированный и резервный (VOL3).

Настройка AutoReseed

1. Все три тома подключаются в единой точке подключения. В этом примере используется точка подключения C:\ExchVols. Она представляет каталог, используемый для получения хранилища для баз данных Exchange.

2. Корневой каталог базы данных почтовых ящиков подключается в качестве другой точки подключения. В этом примере используется точка подключения C:\ExchDBs. Затем структура каталога создается таким образом, чтобы база данных содержала родительский каталог с двумя подкаталогами: для файла базы данных и файлов журнала соответственно.

3. Создаются базы данных. В приведенном выше примере показана простая схема с использованием одной базы данных для каждого тома. Таким образом, том VOL1 содержит три каталога: родительский каталог и два подкаталога (для файла базы данных MDB1 и его журналов соответственно). Хотя на изображении в примере не показано, в VOL2 также будет три каталога: родительский каталог, а под этим каталогом для файла базы данных MDB2 и один для его файлов журнала.

В этой конфигурации, если произойдет сбой MDB1 или MDB2, копия базы данных, завершилась сбоем, будет автоматически повторно добавлена в VOL3.

Компонент освобождения места на диске

Компонент функции AutoReseed, который выделяет и форматирует резервные диски, называется *компонентом освобождения места на диске*. Компонент освобождения места на диске автоматически форматирует резервные диски в процессе подготовки к автоматическому повторному заполнению через различные промежутки времени в зависимости от состояния диска. Чтобы восстановление диска отформатировать диск, необходимо выполнить определенные условия:

- Компонент освобождения места на диске должен быть включен. Он включен по умолчанию, но его можно отключить с помощью Set-DatabaseAvailabilityGroup.
- Корневой путь томов должен включать точку подключения (по умолчанию это C:\ExchangeVolumes).
- Путь томов баз данных не должен включать никаких точек подключения тома (по умолчанию это C:\ExchangeDatabases).
- Если том содержит файлы, ни один из них не должен использоваться в течение суток.

Кроме выше упомянутых условий, компонент освобождения места на диске попытается отформатировать определенный том только один раз в день. В таблице ниже описано поведение форматирования компонента освобождения места на диске.

Состояние диска и копий базы данных	**Интервал форматирования**
Диск неформатирован, отформатирован, но пуст, но содержит файлы, которые не касались в течение 24 часов, а на локальном сайте Active Directory есть работоспособные активные копии базы данных, которые можно использовать в качестве источника заполнения.	1 день
Диск неформатирован, отформатирован, но пуст, но содержит файлы, которые не касались в течение 24 часов, но на локальном сайте Active Directory нет работоспособных активных копий базы данных, которые можно использовать в качестве источника заполнения.	2 дня
Диск неформатирован, отформатирован, но пуст, но содержит файлы, которые не касались в течение 24 часов, а на локальном сайте Active Directory есть работоспособные активные копии базы данных, которые можно использовать в качестве источника заполнения, но существуют неизвестные файлы за пределами файла базы данных (EDB-файл) и файлов журнала.	2 недели

Состояние диска и копий базы данных	Интервал форматирования
Диск не отформатирован, отформатирован, но пуст, но содержит файлы, которые не касались в течение 24 часов, а на локальном сайте Active Directory есть работоспособные активные копии базы данных, которые можно использовать в качестве источника заполнения, но есть один или несколько файлов базы данных (EDB-файлы) для баз данных, которые отсутствуют в Active Directory.	2 недели

Настройка MetaCacheDatabase (MCDB)

Статья • 04.04.2023

Функция MetaCacheDatabase (MCDB) включена в Exchange Server 2019 г. Это позволяет ускорить группу доступности базы данных (DAG) за счет использования твердотельных дисков (SSD). `Manage-MetaCacheDatabase.ps1` — это скрипт автоматизации, созданный для администраторов Exchange Server для настройки экземпляров MCDB и управления ими в своих daG Exchange 2019.

После установки Exchange Server 2019 можно найти `Manage-MetaCacheDatabase.ps1` здесь: ***drive*:\Program Files\Microsoft\Exchange Server\V15\Scripts**. Чтобы сделать cmDLet **Manage-MCDB** доступным в сеансе командной консоли Exchange, сделайте следующее:

PowerShell

```
cd $exscripts
. .\Manage-MetaCacheDatabase.ps1
```

Этот скрипт используется для настройки необходимых компонентов MCDB в правильно настроенном DAG, для включения или отключения MCDB, а также для настройки и восстановления MCDB на серверах.

Руководство по SSD

Все диски SSD, используемые для MCDB, должны иметь одинаковую емкость и тип. Требуется симметричная конфигурация между серверами, что означает, что на каждом сервере должно быть одинаковое количество SSD, а все диски SSD должны иметь одинаковый размер.

> ⓘ **Примечание**
>
> Командлет **Manage-MCDB** будет работать только с устройствами, предоставляемыми Windows в качестве **SSD MediaType** .

Рекомендуется ориентироваться на соотношение 1:3 между ssd и HDD-устройствами на сервер. Таким образом, разверните один SSD для каждых трех жестких дисков. Чтобы избежать уменьшения количества жестких диска на сервере, рассмотрите возможность использования накопителей-накопителей форм-фактора M.2.

Для локальных развертываний достаточно предоставить от 5% до 6% емкости SSD по сравнению с общей емкостью HDD. Например, если сервер содержит 100 ТБ емкости HDD для баз данных почтовых ящиков, достаточно выделить от 5 ДО 6 ТБ для емкости SSD.

Используемые диски SSD должны соответствовать требованиям смешанного использования и поддерживать одну запись дисков в день (DWPD) или больше с точки зрения надежности записи.

Предварительные требования

Для успешной настройки и использования MCDB требуются следующие предварительные требования:

1. DaG настроено для автоматического использования.

   Дополнительную информацию см. в следующих статьях:

   - AutoReseed
   - Настройка автоматического заполнения для группы обеспечения доступности баз данных

2. Необработанные диски SSD устанавливаются с одинаковым количеством и размером SSD для каждого сервера в DAG. Убедитесь, что все диски SSD полностью пусты, не отформатированы и не защищены от записи. Чтобы проверить это, можно использовать DiskPart или Clear-Disk.

3. Exchange Server 2019 г.

Настройка MCDB

Процесс настройки MCDB можно разбить на четыре основных этапа:

1. Задайте правильные значения для daG, которую вы хотите включить для MCDB.

2. Обновите параметры Active Directory (AD) и дождитесь распространения (путем запуска `ConfigureMCDBPrerequisite`).

3. Разрешите ускорение MCDB для каждого сервера DAG (путем запуска `ServerAllowMCDB`).

4. Создайте необходимую инфраструктуру (тома, точки подключения) для MCDB на каждом сервере (запустив `ConfigureMCDBOnServer`).

5. Разрешите базам данных выполнить отработку отказа, чтобы получить новые параметры.

После успешного выполнения всех четырех шагов начнется ускорение MCDB для каждого экземпляра базы данных с соответствующим экземпляром MCDB.

В следующих разделах описывается использование скрипта `Manage-MetaCacheDatabase.ps1` для выполнения указанных выше четырех шагов.

Шаг 1. Настройка правильных значений в DAG, для которого требуется включить MCDB

Эти параметры DAG используются для расчета правильного размера MCDB на дисках SSD:

- *AutoDagTotalNumberOfDatabases*: количество баз данных в daG (например, 50).
- *AutoDagDatabaseCopiesPerDatabase*: количество активных и пассивных копий каждой отдельной базы данных.
- *AutoDagTotalNumberOfServers*: количество серверов в daG, то есть от 2 до 16.

Например:

```
PowerShell

Set-DatabaseAvailabilityGroup testdag1 -AutoDagTotalNumberOfDatabases 20 -
AutoDagDatabaseCopiesPerDatabase 4 -AutoDagTotalNumberOfServers 8
```

Шаг 2. Запуск manage-MCDB - ConfigureMCDBPrerequisite

Этот параметр задает состояние Active Directory для объекта DAG. Для правильной работы MCDB на всех серверах требуется полная репликация состояния Active Directory.

ParameterSetIdentifier:

- *ConfigureMCDBPrerequisite*

Параметры:

Параметр	Обязательный	Описание
DagName	Верно	Имя группы доступности базы данных.
SSDSizeInBytes	Верно	Емкость в байтах каждого ssd на сервере, который будет использоваться для MCDB.
SSDCountPerServer	Верно	Количество ssd-устройств, которые будут использоваться для MCDB на каждом сервере.

Область:

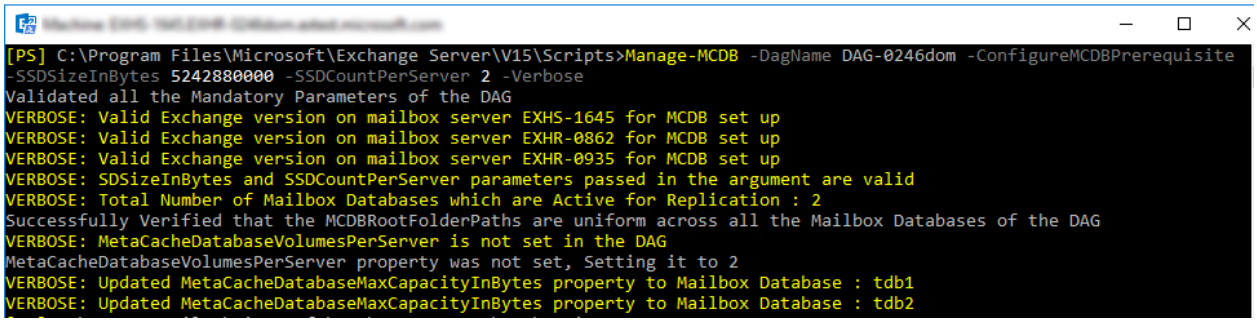
- **DAG**. *ConfigureMCDBPrerequisite* работает с объектом DAG.

> ⓘ **Примечание**
>
> MCDB будет использовать до 95 % физической емкости SSD. Оставшиеся 5 % остаются свободными для учета затрат на файловую систему и секции, а также для небольшого объема дополнительного буфера и чрезмерной подготовки.

Пример.

PowerShell

```
Manage-MCDB -DagName TestDag1 -ConfigureMCDBPrerequisite -SSDSizeInBytes
5242880000 -SSDCountPerServer 2
```



Шаг 3. Запуск manage-MCDB -ServerAllowMCDB

Эта команда задает локальное состояние для каждого члена DAG, чтобы разрешить или запретить заполнение и ускорение чтения MCDB.

ParameterSetIdentifier:

- *ServerAllowMCDB*

Параметры:

Параметр	Обязательный	Описание
DagName	Верно	Имя группы доступности базы данных.
ServerName	Верно	Указывает сервер для включения MetaCacheDatabase.
ForceFailover	Необязательный	Этот логический коммутатор можно использовать для отработки отказа всех баз данных на сервере. Это необходимо для того, чтобы все изменения конфигурации вступили в силу и начали использовать MCDB после успешного создания точек подключения и экземпляров базы данных в разделе Шаг 4. Запуск manage-MCDB -ConfigureMCDBOnServer. Он также необходим для отключения ускорения SSD.

Область:

- **Сервер**. Необходимо запустить *ServerAllowMCDB* на каждом сервере в DAG.

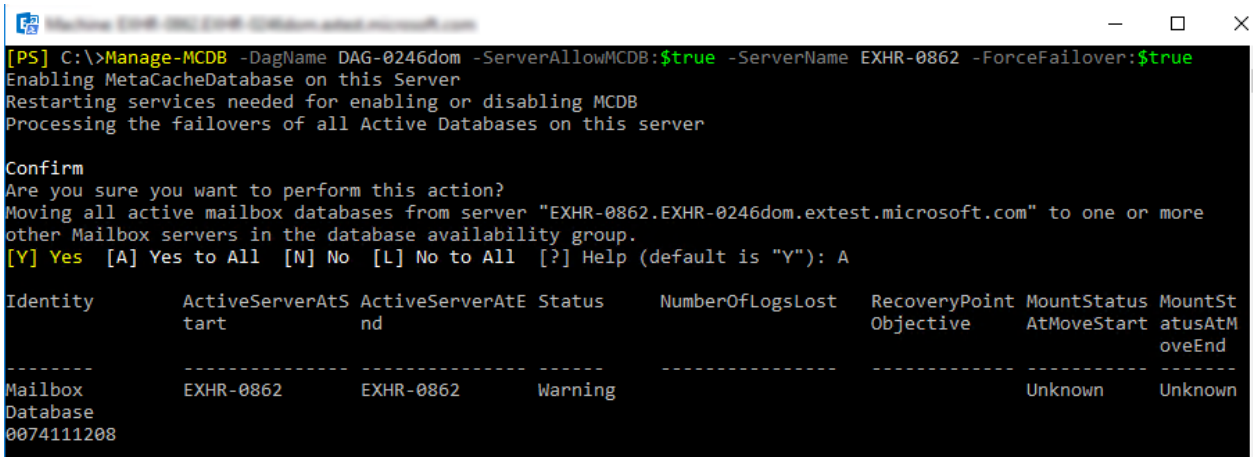
Примеры:

PowerShell

```
Manage-MCDB -DagName TestDag1 -ServerAllowMCDB:$true -ServerName "exhs-5046"
```

PowerShell

```
Manage-MCDB -DagName TestDag1 -ServerAllowMCDB:$false -ServerName "exhs-5046" -ForceFailover $true
```



Шаг 4. Запуск manage-MCDB -ConfigureMCDBOnServer

Эта команда определяет неформатированные устройства SSD и форматирует их, а также создает необходимые точки подключения на сервере для размещения

экземпляров MCDB. Этот набор параметров также можно использовать для повторного создания точек подключения на необработанном SSD, который был добавлен для замены неработающего SSD.

ParameterSetIdentifier:

- *НастройкаMCDBOnServer*

Параметры:

Параметр	Обязательный	Описание
DagName	Верно	Имя группы доступности базы данных.
ServerName	Верно	Указывает сервер для идентификации неформатированных устройств SSD и создания точек подключения.
SSDSizeInBytes	Верно	Это емкость (в байтах) каждого SSD на сервере, который будет использоваться для MCDB.

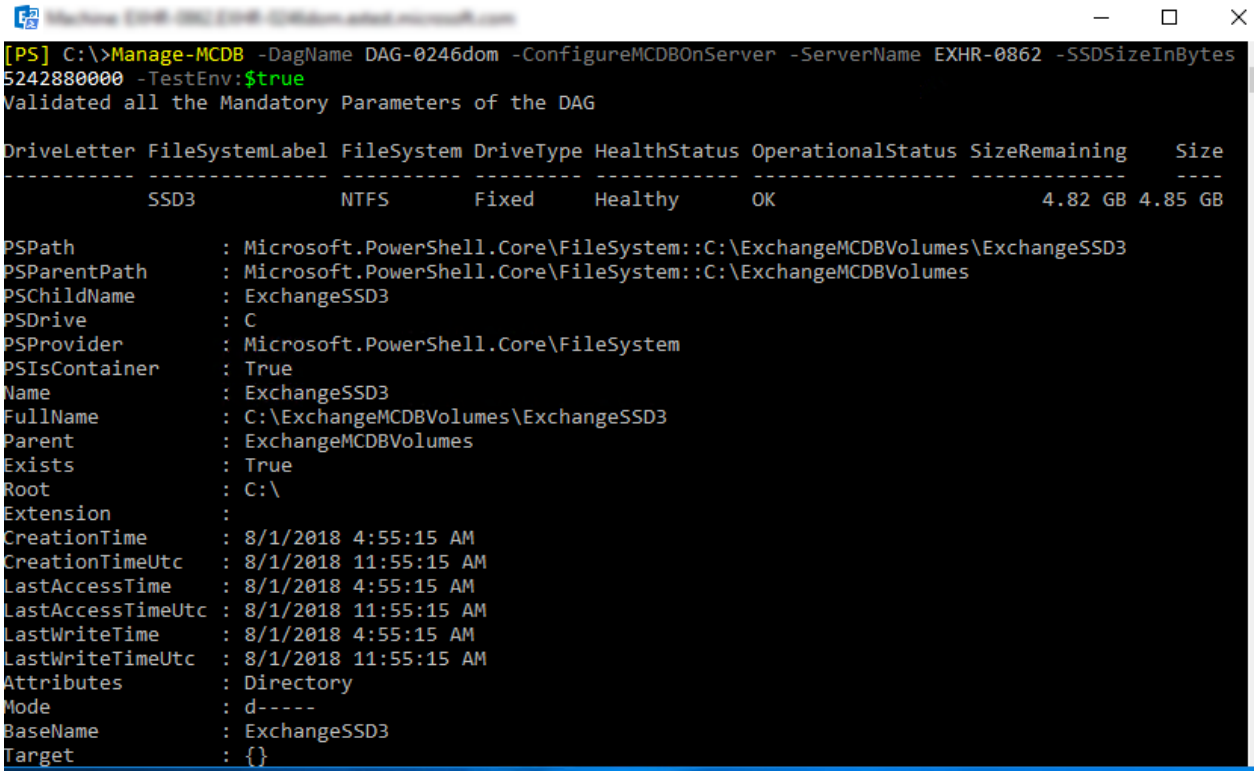
Область:

- **Сервер**. Необходимо запустить *ConfigureMCDBOnServer* на каждом сервере в DAG.

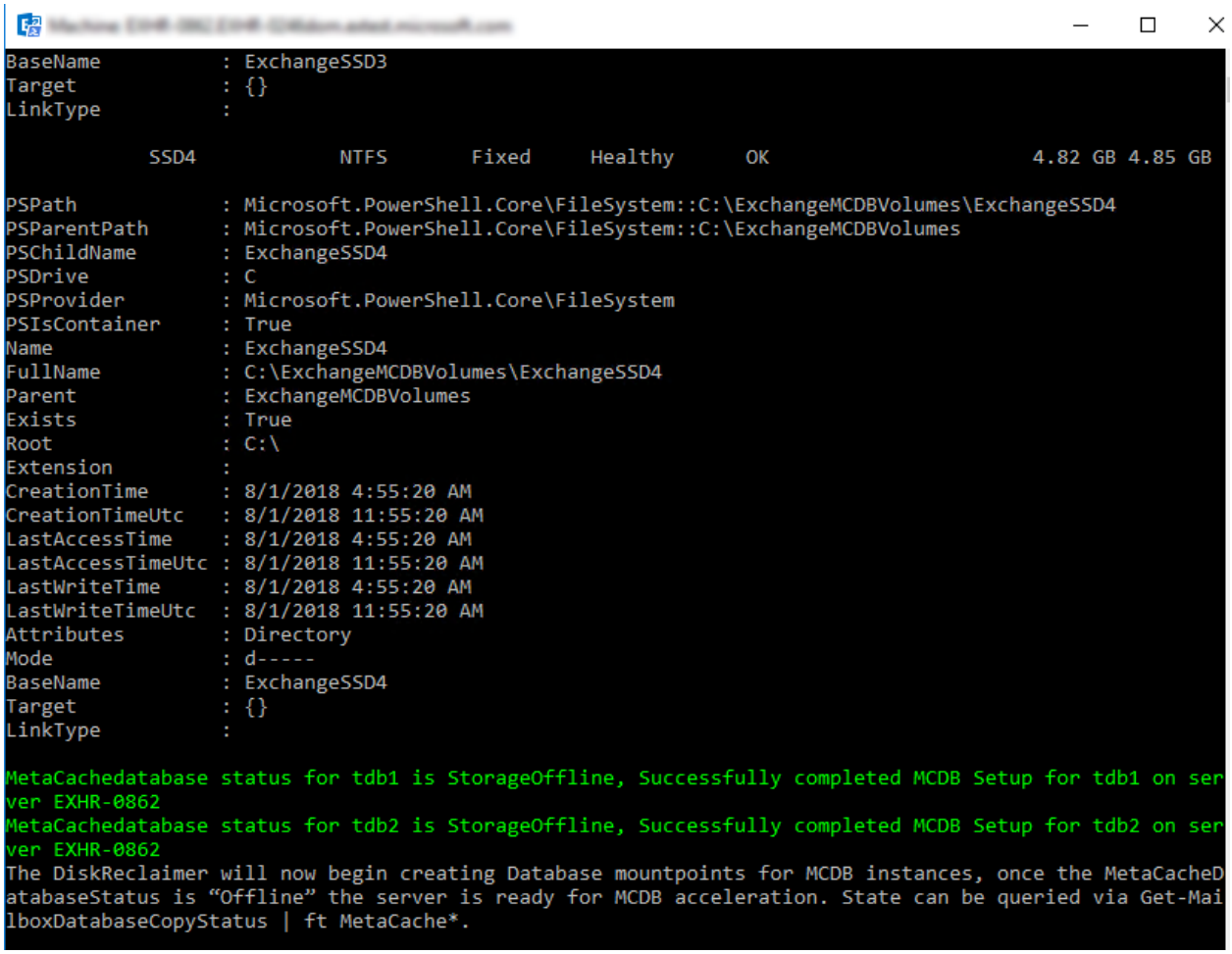
Пример.

PowerShell

```
Manage-MCDB -DagName TestDag1 -ConfigureMCDBOnServer -ServerName "exhs-4056"
-SSDSizeInBytes 5242880000
```



```
[PS] C:\>Manage-MCDB -DagName DAG-0246dom -ConfigureMCDBOnServer -ServerName EXHR-0862 -SSDSizeInBytes
5242880000 -TestEnv:$true
Validated all the Mandatory Parameters of the DAG

DriveLetter FileSystemLabel FileSystem DriveType HealthStatus OperationalStatus SizeRemaining    Size
----------- --------------- ---------- --------- ------------ ----------------- -------------    ----
            SSD3            NTFS       Fixed     Healthy      OK                      4.82 GB 4.85 GB

PSPath            : Microsoft.PowerShell.Core\FileSystem::C:\ExchangeMCDBVolumes\ExchangeSSD3
PSParentPath      : Microsoft.PowerShell.Core\FileSystem::C:\ExchangeMCDBVolumes
PSChildName       : ExchangeSSD3
PSDrive           : C
PSProvider        : Microsoft.PowerShell.Core\FileSystem
PSIsContainer     : True
Name              : ExchangeSSD3
FullName          : C:\ExchangeMCDBVolumes\ExchangeSSD3
Parent            : ExchangeMCDBVolumes
Exists            : True
Root              : C:\
Extension         :
CreationTime      : 8/1/2018 4:55:15 AM
CreationTimeUtc   : 8/1/2018 11:55:15 AM
LastAccessTime    : 8/1/2018 4:55:15 AM
LastAccessTimeUtc : 8/1/2018 11:55:15 AM
LastWriteTime     : 8/1/2018 4:55:15 AM
LastWriteTimeUtc  : 8/1/2018 11:55:15 AM
Attributes        : Directory
Mode              : d-----
BaseName          : ExchangeSSD3
Target            : {}
```



```
BaseName          : ExchangeSSD3
Target            : {}
LinkType          :

            SSD4            NTFS       Fixed     Healthy      OK                      4.82 GB 4.85 GB

PSPath            : Microsoft.PowerShell.Core\FileSystem::C:\ExchangeMCDBVolumes\ExchangeSSD4
PSParentPath      : Microsoft.PowerShell.Core\FileSystem::C:\ExchangeMCDBVolumes
PSChildName       : ExchangeSSD4
PSDrive           : C
PSProvider        : Microsoft.PowerShell.Core\FileSystem
PSIsContainer     : True
Name              : ExchangeSSD4
FullName          : C:\ExchangeMCDBVolumes\ExchangeSSD4
Parent            : ExchangeMCDBVolumes
Exists            : True
Root              : C:\
Extension         :
CreationTime      : 8/1/2018 4:55:20 AM
CreationTimeUtc   : 8/1/2018 11:55:20 AM
LastAccessTime    : 8/1/2018 4:55:20 AM
LastAccessTimeUtc : 8/1/2018 11:55:20 AM
LastWriteTime     : 8/1/2018 4:55:20 AM
LastWriteTimeUtc  : 8/1/2018 11:55:20 AM
Attributes        : Directory
Mode              : d-----
BaseName          : ExchangeSSD4
Target            : {}
LinkType          :

MetaCachedatabase status for tdb1 is StorageOffline, Successfully completed MCDB Setup for tdb1 on ser
ver EXHR-0862
MetaCachedatabase status for tdb2 is StorageOffline, Successfully completed MCDB Setup for tdb2 on ser
ver EXHR-0862
The DiskReclaimer will now begin creating Database mountpoints for MCDB instances, once the MetaCacheD
atabaseStatus is “Offline” the server is ready for MCDB acceleration. State can be queried via Get-Mai
lboxDatabaseCopyStatus | ft MetaCache*.
```

После выполнения трех предыдущих шагов (настройки *ConfigureMCDBPrerequisite*, *ServerAllowMCDBDB* и *ConfigureMCDBOnServer*) состояние MCDB будет отображаться как **Хранилище в автономном режиме**. Это означает, что среда подготовлена и готова к созданию и заполнению экземпляров MCDB. Следующая отработка отказа экземпляра базы данных приведет к созданию экземпляра MCDB и ускорению.

Экземпляры будут переходить через состояния работоспособности, показанные в состояниях работоспособности MCDB.

Можно использовать набор параметров *ServerAllowMCDB* , чтобы вызвать отработку отказа всех экземпляров базы данных, присутствующих на данном сервере. Кроме того, можно использовать командлет **Move-ActiveMailboxDatabase** для отработки отказа отдельных баз данных.

PowerShell

```
Manage-MCDB -DagName TestDag1 -ServerAllowMCDB:$true -ServerName "exhs-5046"
-ForceFailover $true
```

Состояния работоспособности MCDB

Используйте **Командлет Get-MailboxDatabaseCopyStatus** для запроса состояния экземпляров MCDB. Существует пять состояний, в которых может находиться экземпляр MCDB, как показано в следующей таблице:

Состояние	**Описание**
Отключено	MCDB отключена.
StorageOffline	Базовая инфраструктура отсутствует или недоступна, например точки подключения или пути к файлам. Это состояние, в которое находится MCDB после сбоя SSD.
Автономный режим	Ошибки на логическом уровне, например отсутствующие экземпляры MCDB.
Initializing	Временное состояние, система определяет, в каком другом состоянии она должна находиться.
Healthy	Готовы к обработке запросов.

Планирование высокого уровня доступности и устойчивости сайта

Статья • 04.04.2023

На этапе планирования специалисты по архитектуре системы, администраторы и другие заинтересованные лица должны определять бизнес-требования и требования к архитектуре для развертывания, в частности требования высокой доступности и устойчивости сайтов.

Для развертывания этих функций необходимо соблюдение некоторых общих требований, а также специальных требований к оборудованию, программному обеспечению и сети.

Общие требования

Перед развертыванием группы обеспечения доступности баз данных и созданием копий базы данных почтовых ящиков убедитесь, что выполнены следующие требования к системе.

- Служба доменных имен (DNS) запущена. В идеальном случае DNS-сервер должен принимать динамические обновления. Если DNS-сервер не принимает динамические обновления, необходимо создать запись DNS Host (A) для каждого сервера Exchange. Иначе Exchange будет работать неправильно.
- Каждый сервер почтовых ящиков в группе доступности базы данных должен являться рядовым сервером в том же домене.
- Добавление сервера почтовых ящиков Exchange, который также является сервером каталогов, в DAG не поддерживается.
- Имя, присваиваемое группе обеспечения доступности баз данных, должно быть допустимым, доступным и уникальным именем компьютера, состоящим из 15 или менее символов.

Требования к оборудованию

Как правило, для копий баз данных почтовых ящиков или групп обеспечения доступности баз данных не существует особых требований к оборудованию.

Используемые серверы должны соответствовать всем требованиям, изложенным в Exchange Server предварительных требований.

Требования к хранилищу

Как правило, к хранилищу не предъявляется никаких специальных требований для групп обеспечения доступности баз данных или копий базы данных почтовых ящиков. В группах DAG не используется управляемое кластером общее хранилище, этого не требуется. Управляемое кластером общее хранилище поддерживается для использования в DAG только в том случае, если daG настроено для использования решения, использующего API репликации сторонних производителей, встроенный в Exchange Server.

Требования к программному обеспечению

Каждый член daG должен работать под управлением одной и той же операционной системы. Exchange Server 2016 поддерживается в Windows Server 2012, Windows Server 2012 R2 и Windows Server 2016. Exchange Server 2019 поддерживается в операционной системе Windows Server 2019 и Windows Server 2022. В рамках определенного daG все члены должны работать под управлением одной поддерживаемой операционной системы.

> ⓘ **Примечание**
>
> Поддержка серверов Windows Server 2022 появилась с Exchange Server 2019 CU12 (2022H1).

Помимо выполнения предварительных требований для установки Exchange Server, необходимо выполнить требования к операционной системе. Группы доступности данных используют технологию отказоустойчивой кластеризации Windows, поэтому им требуется стандартная версия Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 или Windows Server 2022.

Требования к сети

Для каждой группы доступности базы данных и каждого ее участника также должны выполняться требования к сети. Каждое DAG должно иметь одну *сеть MAPI*, которая используется членом DAG для взаимодействия с другими серверами (например, другими серверами Exchange или серверами каталогов), а также ноль

или несколько *сетей репликации*, которые являются сетями, предназначенными для доставки и заполнения журналов.

В предыдущих версиях Exchange мы рекомендовали по крайней мере две сети (одну сеть MAPI и одну сеть репликации) для групп обеспечения доступности баз данных. В Exchange 2016 и Exchange 2019 поддерживается несколько сетей, но наша рекомендация зависит от вашей физической топологии сети. Если между участниками группы обеспечения доступности баз данных существует несколько сетей, которые полностью физически отделены друг от друга, то использование отдельной сети MAPI и сети репликации обеспечивает дополнительную избыточность. Если вы используете несколько физически разделенных сетей, но которые при этом объединены в одну физическую сеть (например, один канал глобальной сети), то рекомендуется использовать одну сеть (желательно Ethernet 10 Гбит/с) для трафика MAPI и репликации. Это позволит упростить работу с сетью.

При разработке инфраструктуры сети для группы доступности базы данных необходимо учитывать следующие факторы.

- Для каждого участника группы обеспечения доступности баз данных необходимо настроить по крайней мере один сетевой адаптер, который может устанавливать соединение со всеми остальными участниками данной группы. При использовании одного сетевого пути рекомендуется использовать по крайней мере подключение Ethernet 1 Гбит/с, но желательно — Ethernet 10 Гбит/с. Кроме того, при использовании одного сетевого адаптера для каждого участника группы доступности базы данных рекомендуется создать общее решение с учетом использования одного сетевого адаптера и пути.

- Использование двух сетевых адаптеров для каждого участника группы доступности базы данных предоставляет одну сеть MAPI и одну сеть для репликации, с избыточностью для сети репликации, а также следующие способы восстановления:

    - При возникновении сбоя в сети MAPI происходит переход сервера на другой ресурс (при наличии исправных копий базы данных почтовых ящиков, которые можно активировать).

    - В случае сбоя, затрагивающего сеть репликации, если на сеть MAPI не влияет сбой, операции доставки и заполнения журналов будут возвращаться к использованию сети MAPI, даже если для сети MAPI *задано* значение False. После того как работоспособность сети для репликации будет восстановлена и она будет готова возобновить операции доставки и заполнения журналов, необходимо переключиться на эту сеть вручную.

Чтобы переключить репликацию с сети MAPI на восстановленную сеть для репликации, можно либо приостановить и затем возобновить непрерывную репликацию с помощью командлетов **Suspend-MailboxDatabaseCopy** и **Resume-MailboxDatabaseCopy**, либо перезапустить службу репликации Microsoft Exchange. Рекомендуется использовать операции приостановки и возобновления, чтобы предотвратить краткие сбои, вызванные перезапуском службы репликации Microsoft Exchange.

- Каждый участник группы доступности базы данных должен иметь одинаковое количество сетей. Например, если для одного участника группы обеспечения доступности баз данных используется один сетевой адаптер, необходимо использовать один сетевой адаптер для каждого участника данной группы.

- Для каждой группы доступности базы данных должно быть настроено не более одной сети MAPI. Сеть MAPI должна обеспечивать подключение к другим серверам Exchange и службам, таким как Active Directory и DNS.

- При необходимости можно добавить дополнительные сети для репликации. Чтобы какой-либо сетевой адаптер не стал единственной точкой отказа, можно использовать группирование сетевых адаптеров или аналогичную технологию. Однако даже при использовании группирования сеть остается единственной точкой отказа. Более того, группирование приводит к нежелательному повышению сложности группы обеспечения доступности базы данных.

- Каждая сеть на каждом сервере участника группы доступности базы данных должна находиться в собственной подсети. Все серверы в группе доступности базы данных должны находиться в разных подсетях, но сеть MAPI и сеть для репликации должны быть маршрутизируемыми и обеспечивать подключение, при котором:

  - каждая сеть на каждом сервере участника группы доступности базы данных находится на своей подсети, отдельной от подсети, используемой другими сетями на сервере;

  - каждая сеть MAPI на сервере участника группы доступности базы данных может устанавливать связь с другими сетями MAPI участника группы доступности базы данных;

  - каждая сеть для репликации на сервере участника группы доступности базы данных может устанавливать связь с другими сетями для репликации участника группы доступности базы данных;

    - не существует прямой маршрутизации, выполняющей трафик пульса из сети для репликации на одном сервере участника DAG в сеть MAPI на другом сервере участника DAG и наоборот, или между несколькими сетями для репликации в группе доступности базы данных.

- Независимо от географического местоположения участников группы обеспечения доступности баз данных, задержка приема-передачи в сети между участниками группы не должна превышать 500 миллисекунд. Поскольку задержка приема-передачи между двумя серверами почтовых ящиков, на которых размещаются копии базы данных, увеличивается, то возрастает вероятность того, что репликация не будет обновляться. Независимо от уровня задержки в данном решении, пользователи должны убедиться, что сети между всеми участниками группы обеспечения доступности баз данных удовлетворяют целям защиты данных и доступности развертывания. Для конфигураций с более высокими уровнями задержек для достижения поставленных целей может требоваться специальная настройка группы обеспечения доступности баз данных, параметров репликации и сети, например увеличение числа баз данных или уменьшение количества почтовых ящиков на базу данных.

- Для конфигурации с несколькими центрами обработки данных требования к задержке приема-передачи могут и не быть определяющими требованиями к пропускной способности и задержке сети. Чтобы определить необходимые требования к сети для конкретной среды, следует оценить общую нагрузку сети, которая включает клиентский доступ, Active Directory, передачу данных, непрерывную репликацию и другой прикладной трафик.

- Сети группы обеспечения доступности баз данных поддерживают протокол IP версии 4 (IPv4) и IPv6. Протокол IPv6 поддерживается только при использовании IPv4; использование в среде только IPv6 невозможно. IPv6-адреса и диапазоны IP-адресов поддерживаются, только если на компьютере включены протоколы IPv6 и IPv4, а сеть поддерживает IP-адреса обеих версий. Если Exchange Server развернут в этой конфигурации, все роли сервера могут отправлять и получать данные на устройства, серверы и клиенты, использующие IPv6-адреса.

- Автоматическое назначение частных IP-адресов (APIPA) — это функция Microsoft Windows, которая автоматически назначает IP-адреса при отсутствии в сети доступных DHCP-серверов (Dynamic Host Configuration Protocol). Адреса APIPA (включая адреса, назначенные вручную из диапазона адресов APIPA) не поддерживаются для использования dag или Exchange Server.

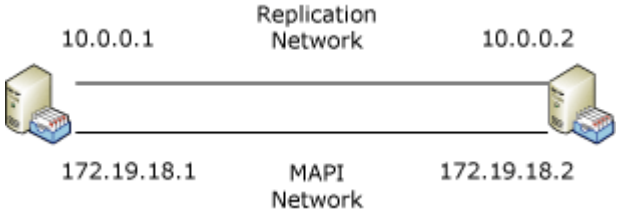
Требования к именам и IP-адресам группы обеспечения доступности баз данных

При создании каждая группа доступности базы данных получает уникальное имя, а также один или несколько статических IP-адресов или настраивается для использования протокола DHCP. Независимо от использования статических или динамически назначенных адресов любой IP-адрес, назначенный группе обеспечения доступности баз данных, должен находиться в сети MAPI.

Каждой daG, работающей в Windows Server 2012, требуется как минимум один IP-адрес в сети MAPI. При расширении сети MAPI на несколько подсетей группе доступности базы данных требуются дополнительные IP-адреса. Группы доступности базы данных, работающие на Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 или Windows Server 2022, созданные без административной точки доступа кластера, не требуют IP-адреса.

На следующем рисунке изображена группа доступности базы данных, для всех узлов которой сеть MAPI настроена в одной и той же подсети.

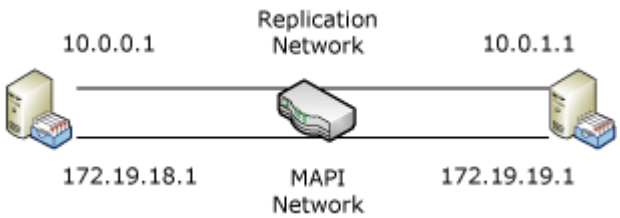
Группа обеспечения доступности баз данных с сетью MAPI в одной подсети



В этом примере сеть MAPI для каждого участника группы доступности базы данных находится в подсети 172.19.18. *x*. Поэтому группе доступности базы данных требуется один IP-адрес в этой подсети.

На следующем рисунке изображена группа обеспечения доступности баз данных, сеть MAPI которой расширяется на две подсети: 172.19.18. *x* и 172.19.19. *x*.

Группа обеспечения доступности баз данных с сетью MAPI в нескольких подсетях



В этом примере сеть MAPI для каждого участника группы доступности базы данных находится в отдельной подсети. Поэтому группе доступности базы данных

требуется два IP-адреса, по одному для каждой подсети в сети MAPI.

При каждом расширении сети MAPI группы доступности базы данных на дополнительную подсеть для группы DAG необходимо настраивать дополнительный IP-адрес для этой подсети. Каждый IP-адрес, настроенный для группы доступности базы данных, назначается и используется базовым отказоустойчивым кластером группы доступности базы данных. Имя группы доступности базы данных также используется в качестве имени для базового отказоустойчивого кластера.

В определенный момент времени кластером группы доступности базы данных используется только один из назначенных IP-адресов. Отказоустойчивый кластер Windows регистрирует этот IP-адрес в системе доменных имен при переводе IP-адреса кластера и ресурсов сетевых имен в оперативный режим работы. Кроме использования IP-адреса и сетевого имени в Active Directory также создается объект имени кластера (CNO). Имя, IP-адрес и сетевой объект кластера используются внутри системы, чтобы гарантировать безопасность группы обеспечения доступности баз данных и осуществления внутренней связи. Администраторам и конечным пользователям нет необходимости обращаться или подключаться к имени группы обеспечения доступности баз данных или IP-адресу.

> ⓘ **Примечание**
>
> Хотя IP-адрес и сетевое имя кластера используются системой внутри системы, в Exchange Server, что эти ресурсы будут доступны, нет жесткой зависимости. Даже если административная точка доступа базового кластера (например, ее IP-адрес и ресурсы сетевого имени) находится в автономном режиме, внутренняя связь по-прежнему осуществляется в daG с помощью имен рядового сервера DAG. Тем не менее, рекомендуется периодически проверять доступность этих ресурсов, чтобы убедиться, что они не находятся в автономном режиме более 30 дней. Если базовый кластер находится в автономном режиме более 30 дней, учетная запись CNO кластера становится недействительной в процессе сборки мусора в Active Directory.

Настройка сетевого адаптера для групп доступности базы данных

Каждый сетевой адаптер должен быть настроен должным образом в соответствии с его предполагаемым использованием. Настройка сетевого адаптера, используемого для сети MAPI, отличается от настройки сетевого адаптера для сети

репликации. Помимо правильной настройки каждого сетевого адаптера, необходимо также настроить порядок сетевого подключения в Windows, чтобы сеть MAPI была в верхней части порядка подключения. Подробные инструкции по изменению порядка сетевого подключения см. в разделе Изменение привязок протокола и порядка поставщика сети.

Настройка сетевого адаптера MAPI

Сетевой адаптер, предназначенный для использования сетью MAPI, необходимо настроить следующим образом.

Сетевые компоненты	**Параметры**
Клиент для сетей Microsoft	Включено
Планировщик пакетов QoS	Дополнительно включена
Служба доступа к файлам и принтерам сетей Microsoft	Включено
Протокол IP версии 6 (TCP/IP v6)	Включено
Протокол IP версии 4 (TCP/IP v4)	Включено
Драйвер в/в тополога канального уровня	Включено
Ответчик обнаружения топологии канального уровня	Включено

Свойства TCP/IP v4 для сетевого адаптера MAPI настраиваются следующим образом.

- IP-адрес для сети MAPI участника группы обеспечения доступности баз данных можно назначить вручную или настроить для использования DHCP. При использовании DHCP рекомендуется регулярно выполнять резервирование для IP-адресов сервера.
- Сетью MAPI обычно используется шлюз по умолчанию, хотя он не является обязательным.
- Необходимо настроить по крайней мере один адрес DNS-сервера. Для обеспечения избыточности рекомендуется использовать несколько DNS-серверов.
- Флажок **Зарегистрировать адреса этого подключения в DNS** должен быть установлен.

Конфигурация репликации сетевого адаптера

Сетевой адаптер, предназначенный для использования сетью для репликации, необходимо настроить следующим образом.

Сетевые компоненты	**Параметры**
Клиент для сетей Microsoft	Отключено
Планировщик пакетов QoS	Дополнительно включена
Служба доступа к файлам и принтерам сетей Microsoft	Отключено
Протокол IP версии 6 (TCP/IP v6)	Включено
Протокол IP версии 4 (TCP/IP v4)	Включено
Драйвер в/в тополога канального уровня	Включено
Ответчик обнаружения топологии канального уровня	Включено

Свойства TCP/IP v4 адаптера сети для репликации настраиваются следующим образом.

- IP-адрес для сети репликации участника группы обеспечения доступности баз данных можно назначить вручную или настроить для использования DHCP. При использовании DHCP рекомендуется регулярно выполнять резервирование для IP-адресов сервера.
- В сетях для репликации обычно отсутствует шлюз по умолчанию, но если в сети MAPI есть такой шлюз, другие сети не должны иметь шлюзов по умолчанию. Маршрутизация сетевого трафика в сети для репликации можно настроить с помощью постоянных, статичных маршрутов в соответствующую сеть других участников группы доступности базы данных посредством адресов шлюзов, обладающих возможностью направлять трафик между сетями для репликации. Весь остальной трафик, не соответствующий маршруту, будет обрабатываться шлюзом по умолчанию, который настроен на адаптере для сети MAPI.
- Адреса DNS-серверов настраивать не следует.
- Не следует устанавливать флажок **Зарегистрировать адреса этого подключения в DNS**.

Требования к следящему серверу

Следящий сервер — это сервер, который находится за пределами группы обеспечения доступности баз данных, а также используется для достижения и сохранения кворума для группы обеспечения доступности баз данных с четным количеством участников. Группы обеспечения доступности баз данных с нечетным количеством участников не используют следящий сервер. Следящий сервер должен использоваться во всех группах обеспечения доступности баз данных с четным количеством участников. Следящим сервером может быть любой компьютер, работающий под управлением Windows Server. Версия операционной системы Windows Server следящего сервера не обязательно должна совпадать с версией операционной системы, используемой участниками группы обеспечения доступности баз данных.

Кворум сохраняется на уровне кластера под группой доступности базы данных. Кворум достигается, когда большинство участников группы доступности базы данных находятся в оперативном режиме и могут связываться с другими участниками группы доступности базы данных. Это определение кворума является одним из аспектов концепции кворума отказоустойчивого кластера Windows. Также важным аспектом кворума в отказоустойчивых кластерах является *ресурс кворума*. Ресурс кворума — это внутренний ресурс отказоустойчивого кластера, предоставляющий средства арбитража, ведущие к состоянию кластера и решениям участников. Ресурс кворума также предоставляет постоянное хранилище для хранения сведений о конфигурации. Сопутствующим элементом ресурса кворума является *журнал кворума*, который представляет собой конфигурацию базы данных для кластера. В журнале форума содержатся сведения о серверах-участниках кластера, ресурсах, установленных в кластере и состоянии этих ресурсов (например, интерактивный или автономный режим).

Критически важно, чтобы каждый участник группы обеспечения доступности баз данных имел представление о конфигурации базового кластера таких групп. Кворум выступает в качестве определяющего репозитория для сведений о конфигурации кластера. Кворум также используется в качестве разрушителя связей во избежание *разделения вычислительных мощностей*. Разделение вычислительных мощностей — это состояние, когда участники группы обеспечения доступности баз данных запущены и доступны, но не могут связаться друг с другом. Возникновение синдрома "разделенности" можно предотвратить, установив требования взаимодействия большинства участников группы доступности базы данных (и, в случае с группами базы данных, с четным количеством участников и следящим сервером) для поддержки доступности группы доступности базы данных.

Планирование устойчивости сайтов

С каждым днем все больше и больше предпринимателей понимают, что доступ к надежным системам обмена сообщениями является основой делового успеха. Для многих организаций система обмена сообщениями является частью плана по обеспечению бесперебойной деятельности, а устойчивость сайтов должна обеспечиваться при развертывании службы обмена сообщениями. В своей основе многие решения по устойчивости сайтов подразумевают собой развертывание оборудования в дополнительных центрах обработки данных.

В конечном счете общая структура группы доступности базы данных, включая количество участников группы доступности базы данных и количество копий базы данных почтовых ящиков, зависит от соглашения об уровне обслуживания по восстановлению каждой организации, которое покрывает различные сценарии сбоев. На стадии планирования архитекторы и администраторы решений определяют требования для развертывания, в том числе и требования к устойчивости сайта. Они определяют используемые местоположения и необходимые цели для соглашения об уровне обслуживания по восстановлению. Соглашение об уровне обслуживания по восстановлению определяет отдельные элементы, которые будут являться основой для разработки решения, предоставляющего высокую доступность и устойчивость сайта: время восстановления и цель точки восстановления. Оба значения измеряются в минутах. Ожидаемое время восстановления — это время, затраченное на восстановление службы. Срок выполнения восстановления обозначает уровень актуальности данных после завершения операции восстановления. В соглашении об уровне обслуживания по восстановлению может быть также определено полное восстановление основного центра обработки данных после устранения в нем неполадок.

Кроме того, архитекторы и администраторы решения определяют группу пользователей, для которых требуется защита устойчивости сайта, а также конфигурацию "активный-пассивный" или "активный-активный" решения для нескольких сайтов. Как правило, в конфигурации "активный-пассивный" пользователи не размещаются в резервном центре обработки данных. В конфигурации "активный-активный" пользователи размещаются в обоих местоположениях, а некоторое количество от общего числа баз данных в решении в основном хранятся во втором центре обработки данных. Если происходит сбой обслуживания пользователей одного центра обработки данных, они автоматически активируются в другом.

Создавая соответствующие соглашения об уровне обслуживания по восстановлению часто требуется ответить на следующие вопросы.

- Какой уровень обслуживания требуется после сбоя основного центра обработки данных?
- Нужны ли пользователям их данные или достаточно только возможности обмена сообщениями?
- Насколько быстро потребуются эти данные?
- Какое количество пользователей необходимо поддерживать?
- Каким образом пользователи получат доступ к своим данным?
- Что такое соглашение об уровне обслуживания по активации резервного центра обработки данных?
- Каким образом производится переключение обслуживания обратно на основной центр обработки данных?
- Выделены ли ресурсы для обеспечения устойчивости сайтов?

Отвечая на эти вопросы, можно начать создание решения для обеспечения устойчивости сайтов системы обмена сообщениями. Краеугольным требованием к защите сайта от сбоя является создание решения для переноса данных системы обмена сообщениями в резервный центр обработки данных, где размещена резервная служба обмена сообщениями.

Планирование сертификатов

При развертывании группы доступности базы данных в одном центре данных не существует определенных требований к сертификатам. Тем не менее, при расширении группы доступности базы данных на несколько центров данных в конфигурации устойчивости сайтов существует несколько определенных требований к сертификатам. В основном структура сертификата зависит от используемого клиента, также как и требования к сертификатам других приложений, использующих сертификаты. Однако существуют определенные рекомендации, которым необходимо следовать в зависимости от типа и количества сертификатов.

Рекомендуется минимизировать число сертификатов, используемых для серверов Exchange и обратных прокси-серверов. Рекомендуется использовать один сертификат для всех конечных точек службы в каждом центре данных. В этом случае уменьшается количество используемых сертификатов, что приводит к уменьшению сложности и затрат на решение.

Для клиентов мобильного Outlook рекомендуется использовать один сертификат альтернативного имени субъекта для каждого центра данных и включить в него несколько имен узлов. Чтобы обеспечить подключение мобильного Outlook после переключения базы данных, сервера или центра данных, необходимо использовать одно имя участника сертификата для каждого сертификата, а также настроить объект конфигурации поставщика Outlook в Active Directory с тем же именем участника в форме по стандарту Microsoft (MSSTD). Например, при использовании имени участника сертификата mail.contoso.com атрибут настраивается следующим образом.

PowerShell

```
Set-OutlookProvider EXPR -CertPrincipalName "msstd:mail.contoso.com"
```

Некоторые приложения, взаимодействующие с Exchange, имеют определенные требования к сертификатам, для чего может потребоваться использование дополнительных сертификатов. Exchange Server может сосуществовать с Office Communications Server (OCS). Для OCS требуется использование сертификатов размером 1024 бита или больше с именем сервера OCS в качестве имени участника сертификата. Поскольку использование имени сервера OCS в качестве имени участника сертификата не позволяет Outlook Anywhere работать правильно, может потребоваться дополнительный отдельный сертификат для среды OCS.

Планирование сети

Кроме определенных требований к сети, которые должны соответствовать каждой группе доступности базы данных, также как и каждому серверу, являющемуся участником группы доступности базы данных, существует несколько требований и рекомендаций для конфигурации устойчивости сайтов. Для всех групп обеспечения доступности баз данных, развертываются ли ее участники на одном или нескольких сайтах, задержка приема-передачи в сети между участниками группы не должна превышать 500 миллисекунд. Кроме того, существуют определенные параметры конфигурации, рекомендуемые для групп доступности базы данных, расширенных на несколько сайтов.

- **Сети MAPI должны быть изолированы от сетей репликации**: политики сети Windows, политики брандмауэра Windows или списки управления доступом маршрутизаторов (ACL) должны использоваться для блокировки трафика между сетью MAPI и сетями репликации. Такая конфигурация необходима для предотвращения перекрестных помех сети при подтверждении соединения.

- **Клиентские записи DNS должны иметь значение Time to Live (TTL) (TTL) 5 минут**. Время простоя, которое испытывают клиенты, зависит не только от того, как быстро может произойти переключение, но и от того, как быстро выполняется репликация DNS и клиенты запрашивают обновленные сведения о DNS. Записи DNS для всех клиентских служб Exchange, включая Outlook в Интернете (прежнее название — Outlook Web App), Exchange ActiveSync, веб-службы Exchange, Outlook Anywhere, SMTP, POP3 и IMAP4 на внутреннем и внешнем DNS-серверах, должны быть настроены с сроком жизни в 5 минут.

- **Использование статических маршрутов для настройки подключения между сетями репликации**. Чтобы обеспечить сетевое подключение между каждым из сетевых адаптеров репликации, используйте постоянные статические маршруты. Это быстрая разовая настройка, выполняемая для каждого участника группы обеспечения доступности баз данных при использовании статичных IP-адресов. Если для получения IP-адресов для сетей репликации используется DHCP-сервер, его можно также использовать для назначения статичных маршрутов для репликации, что упрощает процесс настройки.

Общее планирование устойчивости сайтов

Помимо требований, перечисленных выше для обеспечения высокого уровня доступности, существуют и другие рекомендации по развертыванию Exchange Server в отказоустойчивой конфигурации сайта (например, расширение daG в нескольких центрах обработки данных). Действия, выполняемые на стадии планирования, прямо влияют на успешность решения по обеспечению устойчивости сайта. Например, неудачное планирование пространства имен может стать причиной возникновения трудностей с назначением сертификатов, а неправильная конфигурация сертификата может препятствовать доступу пользователей к службам.

Чтобы уменьшить время активации второго центра данных и позволить ему размещать конечные точки службы центров данных, в которых произошел сбой, необходимо правильно выполнить планирование. Примеры:

- Необходимо изучить и задокументировать цели соглашения об уровне обслуживания для решения по обеспечению устойчивости сайта.

- Серверы во втором центре обработки данных должны обладать достаточной вместительностью для размещения пользователей обоих центров данных.

- Во втором центре данных необходимо включить все службы, представленные в основном центре данных (если служба не входит в состав соглашения об

уровне обслуживания устойчивости сайта). К ним относятся Active Directory, сетевая инфраструктура (например, DNS или TCP/IP), службы телефонии (если используется единая система обмена сообщениями в Exchange 2016) и инфраструктура сайта (например, питание или охлаждение).

- Чтобы пользователи центров данных со сбоем могли иметь доступ к некоторым службам, необходимо настроить для них соответствующие сертификаты сервера. В некоторых службах запрещено использовать экземпляры (например, POP3 и IMAP4), а разрешено использовать только один сертификат. В таких случаях сертификат должен являться сертификатом альтернативного имени субъекта с несколькими именами, либо несколько имен должны быть достаточно схожими для использования группового сертификата (при условии, что политики безопасности организации позволяют использование группового сертификата).

- Необходимые службы должны быть определены во втором центре обработки данных. Например, если первый центр данных имеет три разных URL-адреса SMTP на разных транспортных серверах, во втором центре данных необходимо определить соответствующую конфигурацию, чтобы разрешить хотя бы одному (или всем трем) транспортному серверу размещать рабочую нагрузку.

- Для поддержки переключения центра обработки данных должна быть установлена необходимая конфигурация сети. Это может означать, что необходимо проверить конфигурацию балансировки нагрузки, настройку глобальной DNS, а также наличие подключения к Интернету с соответствующей маршрутизацией.

- Необходимо ознакомиться со стратегией включения изменений DNS, необходимых для переключения центра данных. Определенные изменения DNS, включая параметры срока жизни, необходимо определить и задокументировать для поддержки работы соглашения об уровне обслуживания.

- Стратегия проверки решения должна быть установлена и учтена в соглашении об уровне обслуживания. Периодическая проверка развертывания — это единственный метод, гарантирующий качество и устойчивость развертывания в течение долгого времени. После проверки развертывания рекомендуется задокументировать явным образом часть конфигурации, которая прямо влияет на успешность решения. Кроме того, рекомендуется усилить процесс управления изменениями в тех сегментах развертывания.

Развертывание высокого уровня доступности и устойчивости сайта в Exchange Server

Статья • 04.04.2023

Microsoft Exchange Server использует концепцию, известную как *добавочное развертывание*, для обеспечения высокого уровня доступности и устойчивости сайта. Вы просто устанавливаете два или более серверов почтовых ящиков Exchange в качестве автономных серверов, а затем при необходимости постепенно настраиваете их и базы данных почтовых ящиков для обеспечения высокой доступности и устойчивости сайта.

Обзор процесса развертывания

Хотя фактические шаги, используемые каждой организацией, могут немного отличаться, общий процесс развертывания Exchange Server в конфигурации с высоким уровнем доступности или устойчивой к сайту, как правило, одинаков. После выполнения необходимых задач планирования и разработки для построения и развертывания группы доступности базы данных (DAG) и создания копий базы данных почтовых ящиков необходимо выполнить следующие действия.

1. Создайте DAG. Дополнительные сведения см. в разделе Create a database availability group. Важно отметить, что все серверы в daG должны работать под управлением одной и той же версии Exchange. Например, нельзя смешивать серверы Exchange 2013 и Exchange 2016 в одной группе daG.

2. При необходимости подготовьте объект имени кластера (CNO). При развертывании DAG с серверами почтовых ящиков под управлением Windows Server 2012 требуется предварительная промежуточная подготовка CNO. Если вы развертываете DAG без административной точки доступа с помощью серверов почтовых ящиков, работающих Windows Server 2012 R2, вам не нужно предварительно создавать CNO. Предварительная промежуточная подготовка также требуется в средах, где создание учетной записи компьютера ограничено или учетные записи компьютера создаются в контейнере, отличном от контейнера компьютеров по умолчанию. Дополнительные сведения см. в разделе Pre-stage the cluster name object for a database availability group.

3. Добавьте два или более серверов почтовых ящиков в daG. Подробные инструкции см. в разделе Управление членством в группе доступности базы данных.

4. Настроить свойства группы DAG в соответствии с требованиями.

5. При необходимости настройте шифрование и сжатие DAG, порт репликации, IP-адреса DAG и другие свойства DAG. Подробные инструкции см. в разделе Настройка свойств группы доступности базы данных.

6. Включите режим координации активации центра обработки данных (DAC) для daG. Это защищает DAG от условий разделенного мозга на уровне базы данных во время переключения в основной центр обработки данных после переключения центра обработки данных и позволяет использовать встроенные командлеты восстановления DAG. Дополнительные сведения см. в разделе Режим координации активации центра обработки данных.

7. Добавление копий базы данных почтовых ящиков между серверами почтовых ящиков в DAG. Дополнительные сведения см. в статье Add a mailbox database copy.

Пример развертывания: группа обеспечения доступности баз данных с четырьмя участниками в двух центрах данных

В этом примере описано, как организация Contoso, Ltd. настраивает и развертывает группу DAG из четырех участников, которая будет расширена в двух физических расположениях: Бостоне и Оклахома-Сити.

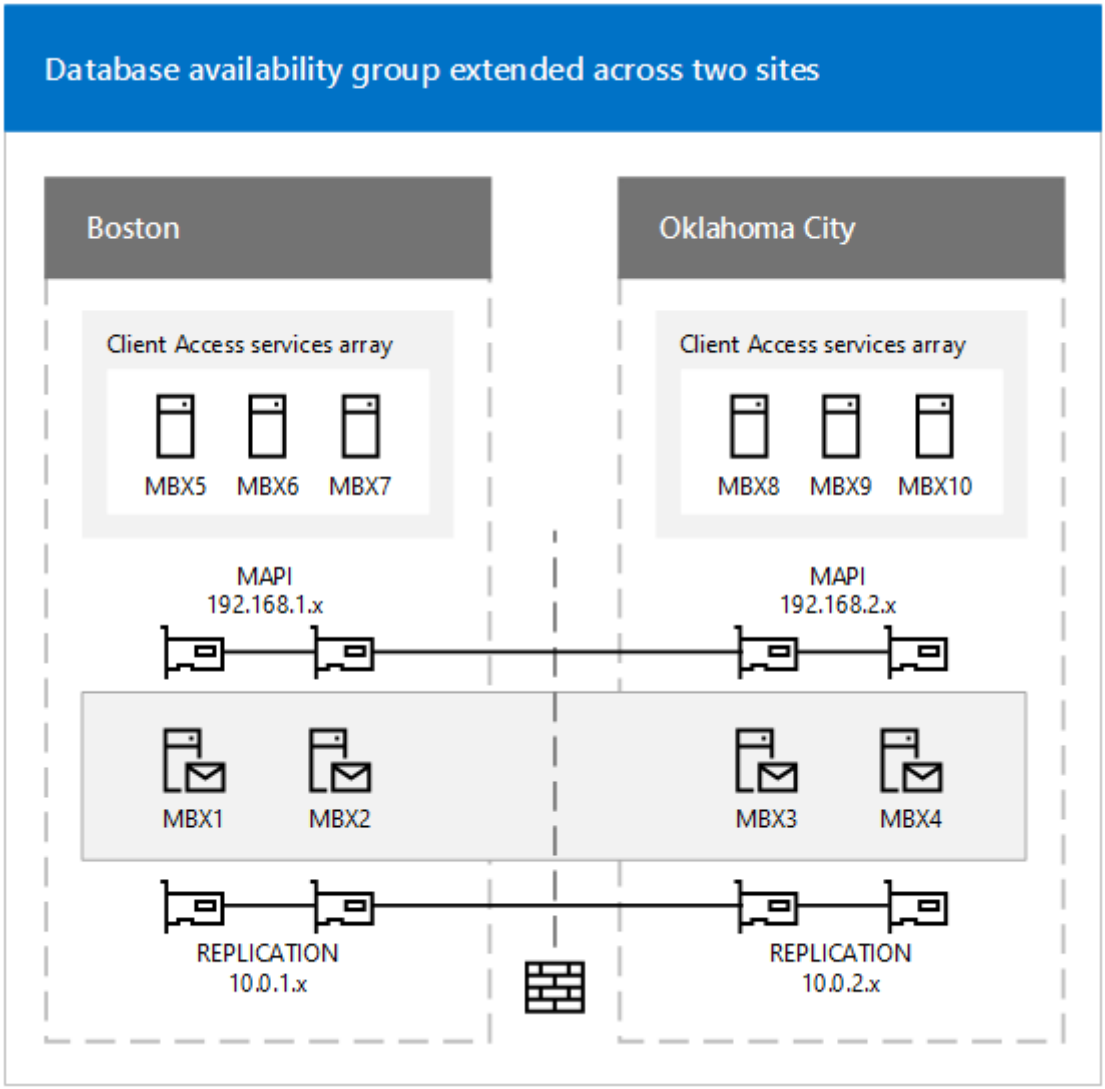
Базовая инфраструктура

Каждое расположение содержит элементы инфраструктуры, необходимые для работы инфраструктуры обмена сообщениями на основе Exchange Server, а именно:

- Службы каталогов (доменные службы Active Directory или Active Directory (AD DS)).
- Разрешение имени системы доменных имен (DNS).
- Несколько серверов Exchange, на которых запущены службы клиентского доступа

- Несколько серверов почтовых ящиков Exchange

На следующем рисунке показана конфигурация Contoso.



Конфигурация сети

Как показано на рисунке выше, решение включает в себя использование нескольких подсетей и нескольких сетей. Для каждого сервера почтовых ящиков в группе DAG предусмотрены сетевые адаптеры в различных сетях. На каждом сервере почтовых ящиков для сети MAPI (192.168) будет использоваться один сетевой адаптер. *x*. *x*) и один сетевой адаптер будет использоваться для сети репликации (10.0). *x*. *x*). Только сеть MAPI обеспечивает подключение к службам Active Directory, службам DNS, другим серверам и клиентам Exchange. Адаптер, используемый для сети репликации в каждом участнике, обеспечивает подключение только к адаптерам сети репликации в других участниках группы DAG.

В следующей таблице приведено подробное описание параметров для каждого сетевого адаптера в каждом узле.

Имя	IPv4-адрес	Маска подсети	Шлюз по умолчанию
MBX1 (MAPI)	192.168.1.4	255.255.255.0	192.168.1.1
MBX2 (MAPI)	192.168.1.5	255.255.255.0	192.168.1.1
MBX3 (MAPI)	192.168.2.4	255.255.255.0	192.168.2.1
MBX4 (MAPI)	192.168.2.5	255.255.255.0	192.168.2.1
MBX1 (репликация)	10.0.1.4	255.255.255.0	Нет
MBX2 (репликация)	10.0.1.5	255.255.255.0	Нет
MBX3 (репликация)	10.0.2.4	255.255.255.0	Нет
MBX4 (репликация)	10.0.2.5	255.255.255.0	Нет

Как показано в таблице выше, адаптеры, используемые для сетей репликации, не используют шлюзы по умолчанию. Для обеспечения сетевого соединения между всеми сетевыми адаптерами репликации в компании Contoso используются постоянные статические маршруты, которые настраиваются с помощью средства Netsh.exe.

Для настройки маршрутизации для сетевых адаптеров репликации на MBX1 и MBX2 на каждом сервере была выполнена следующая команда.

PowerShell

```
netsh interface ipv4 add route 10.0.2.0/24 <NetworkName> 10.0.1.254
```

Для настройки маршрутизации для сетевых адаптеров репликации на MBX3 и MBX4 на каждом сервере была выполнена следующая команда.

PowerShell

```
netsh interface ipv4 add route 10.0.1.0/24 <NetworkName> 10.0.2.254
```

Также были настроены следующие дополнительные параметры сети:

- Флажок **Зарегистрировать адреса этого подключения в DNS** устанавливается для каждого сетевого адаптера MAPI члена группы обеспечения доступности базы данных и снимается для каждого сетевого адаптера репликации.
- Для каждого сетевого адаптера MAPI члена группы DAG настраивается по меньшей мере один адрес DNS-сервера, а для сетевых адаптеров репликации

такие адреса не задаются. В целях избыточности в Contoso используется несколько адресов сервера DNS для их адаптеров сети MAPI.

- В Contoso брандмауэр Windows не используется, он отключен на серверах.

После настройки сетевых адаптеров в Contoso можно создать группу DAG и добавить в нее серверы почтовых ящиков.

Создание и настройка группы обеспечения доступности базы данных

Администратор принял решение создать сценарий интерфейса командной строки Windows PowerShell, который выполняет несколько задач.

- Для создания группы DAG он использует командлет New-DatabaseAvailabilityGroup. Так как boston считается основным центром обработки данных, компания Contoso решила использовать сервер-свидетель в том же центре обработки данных, а именно MBX5.
- Компания использует командлет Set-DatabaseAvailabilityGroup для предварительной настройки альтернативного следящего сервера и каталога на случай необходимости переключения ЦОД.
- Для добавления каждого из четырех серверов почтовых ящиков в группу DAG используется командлет Add-DatabaseAvailabilityGroupServer.
- Для настройки DAG для режима DAC используется командлет Set-DatabaseAvailabilityGroup . Дополнительные сведения о режиме DAC см. в разделе Режим координации активации центра обработки данных.

Ниже приведены использованные в сценарии команды.

PowerShell

```
New-DatabaseAvailabilityGroup -Name DAG1 -WitnessServer MBX5 -
WitnessDirectory C:\DAGWitness\DAG1.contoso.com -
DatabaseAvailabilityGroupIPAddresses 192.168.1.8,192.168.2.8
```

Предыдущая команда создает DAG DAG1, настраивает MBX5 в качестве следящего сервера, настраивает конкретный следящий каталог (C:\DAGWitness\DAG1.contoso.com) и настраивает два IP-адреса для DAG (по одному для каждой подсети в сети MAPI).

PowerShell

```
Set-DatabaseAvailabilityGroup -Identity DAG1 -AlternateWitnessDirectory
C:\DAGWitness\DAG1.contoso.com -AlternateWitnessServer MBX10
```

Предыдущая команда настраивает DAG1 для использования альтернативного следящего сервера MBX10 и альтернативного следящего каталога в MBX10, который использует тот же путь, который был настроен для MBX5.

> ⓘ **Примечание**
>
> Использование того же пути не требуется; в Contoso данное действие было выбрано для стандартизации их конфигурации.

PowerShell

```
Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer MBX1
Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer MBX3
Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer MBX2
Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer MBX4
```

Приведенные выше команды поочередно добавляют каждый из серверов почтовых ящиков в группу DAG. Эти команды также устанавливают компонент отказоустойчивого кластера Windows на каждый сервер почтовых ящиков (если он не был установлен ранее), создают отказоустойчивый кластер и присоединяют каждый сервер почтовых ящиков ко вновь созданному кластеру.

PowerShell

```
Set-DatabaseAvailabilityGroup -Identity DAG1 -DatacenterActivationMode
DagOnly
```

Приведенная выше команда включает режим DAC для группы DAG.

Базы данных почтовых ящиков и копии базы данных почтовых ящиков

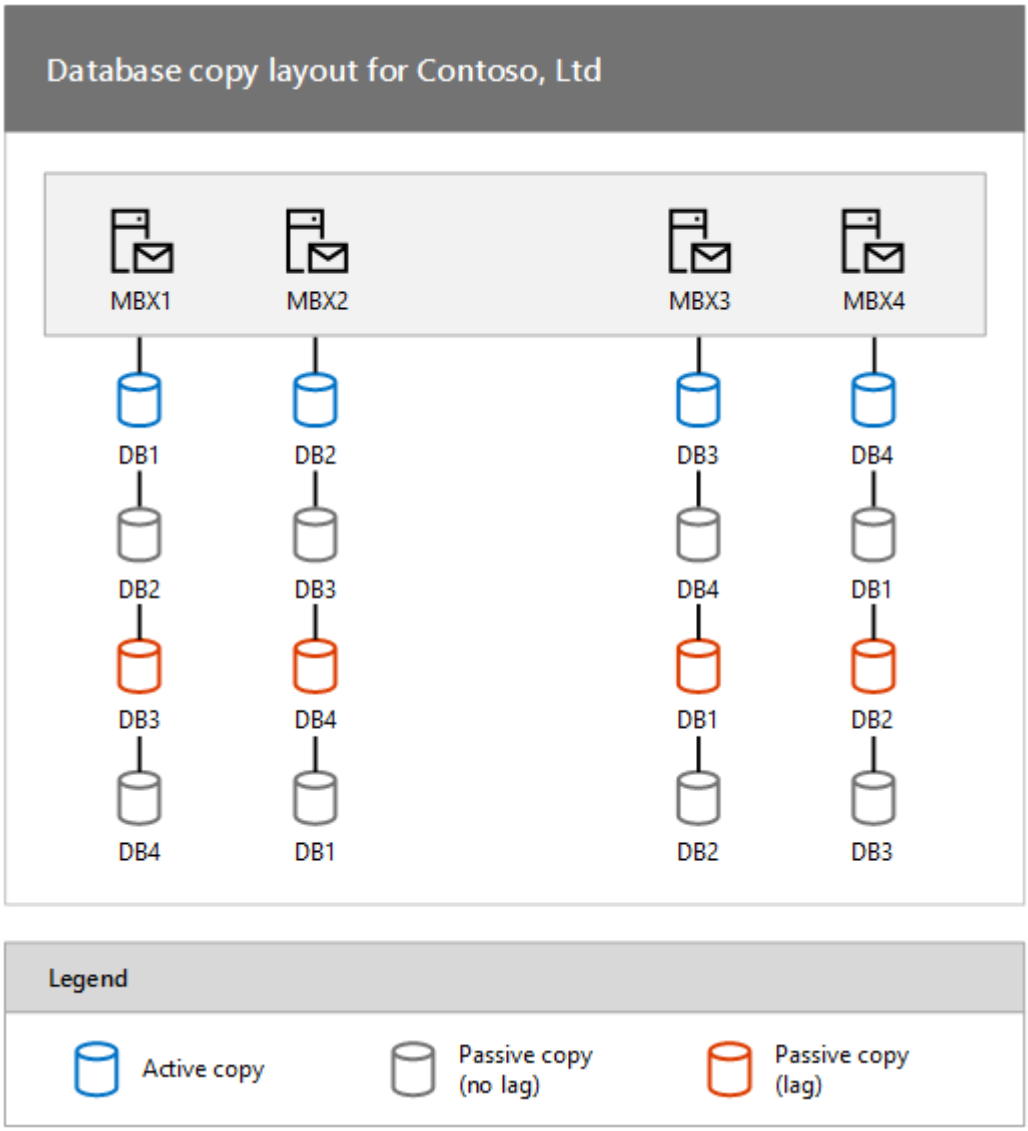
После создания группы DAG и добавления серверов почтовых ящиков в группу DAG в Contoso выполняется подготовка к созданию баз данных почтовых ящиков и их копий. Для соответствия критериям устойчивости к отказам в Contoso планируется настройка каждой базы данных почтовых ящиков с тремя неизолированными копиями базы данных и одной изолированной копией базы

данных. Для изолированной копии будет настроено значение задержки преобразования журнала, равное трем дням.

Такая конфигурация обеспечивает наличие четырех копий для каждой базы данных (одной активной, двух неизолированных пассивных и одной изолированной пассивной). В Contoso планируется наличие четырех активных баз данных для каждого сервера. Таким образом, решение Contoso содержит 16 копий базы данных.

Как показано на рисунке выше, в Contoso используется сбалансированный подход для структуры базы данных.

Структура копии базы данных для Contoso, Ltd



На каждом сервере почтовых ящиков размещаются активная копия базы данных почтовых ящиков, две неизолированных пассивных копии и одна изолированная пассивная копия. Изолированная копия каждой активной базы данных почтовых ящиков размещается на сервере почтовых ящиков на другом сайте.

Чтобы создать эту конфигурацию, администратор выполняет несколько команд.

На MBX1 выполните следующие команды.

PowerShell

```
Add-MailboxDatabaseCopy -Identity DB1 -MailboxServer MBX2
Add-MailboxDatabaseCopy -Identity DB1 -MailboxServer MBX4
Add-MailboxDatabaseCopy -Identity DB1 -MailboxServer MBX3 -ReplayLagTime
3.00:00:00 -SeedingPostponed
Suspend-MailboxDatabaseCopy -Identity DB1\MBX3 -SuspendComment "Seed from
MBX4" -Confirm:$False
Update-MailboxDatabaseCopy -Identity DB1\MBX3 -SourceServer MBX4
Suspend-MailboxDatabaseCopy -Identity DB1\MBX3 -ActivationOnly
```

На MBX2 выполните следующие команды.

PowerShell

```
Add-MailboxDatabaseCopy -Identity DB2 -MailboxServer MBX1
Add-MailboxDatabaseCopy -Identity DB2 -MailboxServer MBX3
Add-MailboxDatabaseCopy -Identity DB2 -MailboxServer MBX4 -ReplayLagTime
3.00:00:00 -SeedingPostponed
Suspend-MailboxDatabaseCopy -Identity DB2\MBX4 -SuspendComment "Seed from
MBX3" -Confirm:$False
Update-MailboxDatabaseCopy -Identity DB2\MBX4 -SourceServer MBX3
Suspend-MailboxDatabaseCopy -Identity DB2\MBX4 -ActivationOnly
```

На MBX3 выполните следующие команды.

PowerShell

```
Add-MailboxDatabaseCopy -Identity DB3 -MailboxServer MBX4
Add-MailboxDatabaseCopy -Identity DB3 -MailboxServer MBX2
Add-MailboxDatabaseCopy -Identity DB3 -MailboxServer MBX1 -ReplayLagTime
3.00:00:00 -SeedingPostponed
Suspend-MailboxDatabaseCopy -Identity DB3\MBX1 -SuspendComment "Seed from
MBX2" -Confirm:$False
Update-MailboxDatabaseCopy -Identity DB3\MBX1 -SourceServer MBX2
Suspend-MailboxDatabaseCopy -Identity DB3\MBX1 -ActivationOnly
```

На MBX4 выполните следующие команды.

PowerShell

```
Add-MailboxDatabaseCopy -Identity DB4 -MailboxServer MBX3
Add-MailboxDatabaseCopy -Identity DB4 -MailboxServer MBX1
Add-MailboxDatabaseCopy -Identity DB4 -MailboxServer MBX2 -ReplayLagTime
3.00:00:00 -SeedingPostponed
Suspend-MailboxDatabaseCopy -Identity DB4\MBX2 -SuspendComment "Seed from
MBX1" -Confirm:$False
```

```
Update-MailboxDatabaseCopy -Identity DB4\MBX2 -SourceServer MBX1
Suspend-MailboxDatabaseCopy -Identity DB4\MBX2 -ActivationOnly
```

В предыдущих примерах для командлета **Add-MailboxDatabaseCopy** параметр *ActivationPreference* не указан. В задаче автоматически увеличивается значение приоритета активации с каждой добавляемой копией. Значение приоритета исходной базы данных всегда равно 1. Для первой копии, добавляемой с помощью командлета **Add-MailboxDatabaseCopy**, автоматически назначается значение приоритета 2. Если предположить, что ни одна копия не удаляется, для следующей добавляемой копии будет автоматически назначаться значение приоритета 3 и так далее. Таким образом, в приведенных выше примерах показано, что пассивная копия, расположенная том же центре данных, что и активная копия, имеет значение приоритета активации 2, неизолированная пассивная копия в удаленном центре данных — 3, а изолированная пассивная копия в удаленном центре данных — 4.

Несмотря на наличие двух копий каждой активной базы данных в глобальной сети в другом местоположении, заполнение в глобальной сети было выполнено только один раз. Это связано с тем, что компания Contoso использует Exchange Server возможность использовать пассивную копию базы данных в качестве источника для заполнения. Использование командлета Add-MailboxDatabaseCopy с параметром *SeedingPostponed* предотвращает автоматическое заполнение создаваемой новой копии базы данных. Затем администратор может приостановить незасеянную копию, а с помощью командлета Update-MailboxDatabaseCopy с параметром *SourceServer* администратор может указать локальную копию базы данных в качестве источника операции заполнения. В результате этого заполнение второй копии базы данных, добавленной к каждому местоположению, выполняется локально, а не по глобальной сети.

> ⓘ **Примечание**
>
> В приведенном выше примере заполнение неизолированной копии базы данных выполняется по глобальной сети, а затем эта копия используется для заполнения изолированной копии базы данных, расположенной в том же центре данных, что и неизолированная копия.

В Contoso была настроена одна из пассивных копий каждой базы данных почтовых ящиков в качестве изолированной копии базы данных, что позволяет обеспечить защиту от крайне редкого, но серьезного логического повреждения базы данных. В результате администратор настраивает отстающие копии как заблокированные для активации с помощью командлета Suspend-MailboxDatabaseCopy с параметром

ActivationOnly . Это гарантирует, что изолированные копии базы данных не будут активированы в случае возникновения сбоя базы данных или сервера.

Проверка решения

После развертывания и настройки решения администратор выполняет несколько задач для проверки готовности решения перед последующим перемещением рабочих почтовых ящиков в базы данных в группе DAG. Решение необходимо проверить с помощью нескольких способов, в том числе моделирования сбоя. Для проверки решения администратор выполняет несколько задач.

Для проверки общей работоспособности группы DAG администратор выполняет командлет Test-ReplicationHealth. Этот командлет проверяет несколько аспектов репликации и состояния преобразования, чтобы предоставить сведения о каждом сервере почтовых ящиков и копии базы данных в группе DAG.

Чтобы проверить действия репликации и воспроизведения, администратор запускает командлет Get-MailboxDatabaseCopyStatus . Этот командлет может в режиме реального времени предоставлять сведения о состоянии конкретной копии базы данных почтовых ящиков или для всех копий базы данных почтовых ящиков на определенном сервере. Дополнительные сведения о мониторинге работоспособности и состояния реплицированных баз данных в DAG см. в разделе Мониторинг групп доступности баз данных.

Чтобы убедиться, что переключения срабатывают должным образом, администратор использует командлет Move-ActiveMailboxDatabase для выполнения серии переключений базы данных и сервера. После успешного выполнения этих задач администратор использует тот же командлет для перемещения активных копий базы данных обратно в исходное местоположение.

Чтобы проверить поведение системы при различных сценариях сбоя, администратор выполняет несколько задач, которые либо моделируют сбои, либо вызывают фактические сбои. Например, администратор может выполнить следующие действия:

- Отключить шнур питания на MBX1, что приводит к сбою сервера. После этого администратор проверяет активацию DB1 на другом сервере (предпочтительно на MBX2 на основе значений приоритета активации).
- Отключить сетевой кабель для сетевого адаптера MAPI на MBX2, что приводит к сбою сервера. После этого администратор проверяет активацию DB2 на другом сервере (предпочтительно на MBX1 на основе значений приоритета активации).

- Перевести диск, используемый активной копией DB3, в автономный режим, что приводит к сбою базы данных. После этого администратор проверяет активацию DB3 на другом сервере (предпочтительно на MBX4 на основе значений приоритета активации).

В зависимости от производственных потребностей могут присутствовать и другие сценарии сбоя, проверяемые организацией. После моделирования отдельного сбоя (например, отсоединения шнура питания) и проверки поведения восстановления решения администратор может вернуть исходную конфигурацию решения. В некоторых случаях решение может быть проверено на несколько одновременных сбоев. Наконец, в плане тестирования решения определяется, будет ли возвращена исходная конфигурация решения после завершения каждого моделирования сбоя.

Кроме того, администратор может принять решение разорвать сетевое подключение между двумя центрами данных, чтобы таким образом смоделировать сбой сайта. Переключение центра данных представляет собой более сложный и скоординированный процесс; однако его рекомендуется выполнять, если развертываемое решение предназначено для обеспечения устойчивости сайта для служб обмена сообщениями и данными.

Перевод в рабочую среду

Когда решение развернуто, оно может быть далее расширено с помощью добавочного развертывания. На данном этапе управление решением также перейдет к операционным процессам, в которых будут выполнены следующие задачи:

- Отслеживайте работоспособность и состояние групп доступности баз данных и копий базы данных почтовых ящиков. Дополнительные сведения см. в разделе Мониторинг групп доступности базы данных.

- При необходимости выполняйте переключение базы данных. Дополнительные сведения о переключении базы данных см. в разделе Активация копии базы данных почтовых ящиков.

Дополнительные сведения об управлении решением см. в разделе Управление высокой доступностью и устойчивостью сайтов.

Управление высоким уровнем доступности и устойчивостью сайта в Exchange Server

Статья • 04.04.2023

После сборки, проверки и развертывания решения Microsoft Exchange Server высокого уровня доступности или устойчивости сайта решение переходит от этапа развертывания к рабочему этапу общего жизненного цикла решения. Рабочая стадия состоит из нескольких задач, относящихся к группам обеспечения доступности баз данных (DAG), копиям баз данных, копиям баз данных почтовых ящиков, упреждающему мониторингу или управлению переключениями и отработками отказа.

Управление группами обеспечения доступности баз данных

Ниже приведены задачи оперативного управления, связанные с группами обеспечения доступности баз данных.

- **Создание одной или нескольких групп daG**. Создание daG обычно является однократной процедурой, выполняемой на этапе развертывания жизненного цикла решения. Пример:
    - Группа DAG настроена для режима репликации стороннего поставщика, и планируется вернуться к непрерывной репликации. Группу DAG нельзя вернуть к непрерывной репликации, необходимо создать новую группу DAG.
    - Имеются серверы в нескольких доменах. Все члены одной группы DAG должны также быть членами одного домена.
- **Управление членством DAG**. Управление членами DAG — это нечасто выполняемая задача, обычно выполняемая на этапе развертывания жизненного цикла решения. Однако благодаря гибкости добавочного развертывания членами группы DAG также можно управлять на протяжении всего жизненного цикла решения.
- **Настройка свойств DAG**. Каждая daG имеет различные свойства, которые можно настроить по мере необходимости. Эти свойства приведены ниже.

- **Следящий сервер и следящий каталог**. Следящий сервер является сервером за пределами DAG, который выступает в качестве избирателя кворума, если DAG содержит четное число членов. Следящий каталог — это каталог, созданный на следящем сервере, который используется системой для поддержания кворума.

- **IP-адреса**. Каждое DAG будет иметь один или несколько IPv4-адресов и при необходимости один или несколько IPv6-адресов. Эти IP-адреса, назначенные группе обеспечения доступности баз данных, используются базовым кластером группы DAG. Количество IPv4-адресов, назначенных группе обеспечения доступности баз данных, равно количеству подсетей, образующих сеть MAPI, используемую этой группой обеспечения доступности баз данных. Группу обеспечения доступности баз данных можно настроить так, чтобы она использовала статические IP-адреса или получала адреса автоматически с помощью протокола DHCP.

- **Режим координации активации центра обработки данных**. Режим координации активации центра обработки данных — это параметр свойства в DAG, предназначенный для предотвращения разбиения мозга на уровне базы данных в сценарии, в котором выполняется восстановление службы в основной центр обработки данных после переключения центра обработки данных. Дополнительные сведения о режиме координации активации центра обработки данных см. в разделе Режим координации активации центра обработки данных.

- **Альтернативный следящий сервер и альтернативный следящий каталог**. Альтернативный следящий сервер и альтернативный следящий каталог — это значения, которые можно предварительно настроить в процессе планирования переключения центра обработки данных. Это относится к следящему серверу и следящему каталогу, которые будут использоваться после переключения центра данных.

- **Порт репликации**. По умолчанию все группы доступности базы данных используют TCP-порт 64327 для непрерывной репликации. Вы можете изменить этот порт с помощью параметра *ReplicationPort* командлета Set-DatabaseAvailabilityGroup.

- **Сетевое обнаружение**. Вы можете принудить DAG повторно обнаруживать сети и сетевые интерфейсы. Эта операция используется при добавлении или удалении сетей, а также при введении новых подсетей. Принудительно запустить повторное обнаружение всех сетей групп обеспечения

доступности баз данных можно с помощью параметра *DiscoverNetworks* командлета Set-DatabaseAvailabilityGroup.

- **Сжатие сети**. По умолчанию группы доступности баз данных используют сжатие только между сетями DAG в разных подсетях. Вы можете включить сжатие для всех сетей DAG или только для операций заполнения; кроме того, вы можете отключить сжатие для всех сетей DAG.

- **Шифрование сети**. По умолчанию группы доступности баз данных используют шифрование только между сетями DAG в разных подсетях. Вы можете включить шифрование для всех сетей DAG или только для операций заполнения; кроме того, вы можете отключить шифрование для всех сетей DAG.

- **Завершение работы членов DAG**. Решение Exchange Server высокого уровня доступности интегрировано с процессом завершения работы Windows. Если администратор или приложение инициирует завершение работы сервера Windows в daG с подключенной базой данных, которая реплицируется на один или несколько членов DAG, система попытается активировать другую копию подключенных баз данных, прежде чем разрешить завершение работы. Однако это новое правило не гарантирует, что все базы данных на отключаемом сервере пройдут активацию без потерь. Поэтому перед завершением работы сервера, который является членом группы DAG, лучше выполнить его переключение.

Дополнительные сведения о создании группы обеспечения доступности баз данных см. в разделе Создание группы обеспечения доступности баз данных. Дополнительные сведения о настройке свойств группы DAG см. в статье Configure database availability group properties. Дополнительные сведения о каждой из предыдущих задач управления и об управлении группами доступности баз данных в целом см. в разделе Управление группами доступности баз данных.

Управление копиями баз данных почтовых ящиков

Ниже приведены задачи оперативного управления, связанные с копиями баз данных почтовых ящиков.

- **Добавление копий базы данных почтовых ящиков**. При добавлении копии базы данных почтового ящика непрерывная репликация автоматически включается между существующей базой данных и копией базы данных.

- **Настройка свойств копирования базы данных почтовых ящиков**. Вы можете настроить различные свойства, такие как политика активации базы данных, количество времени (если таковые есть) для задержки воспроизведения и задержки усечения, а также предпочтительное значение активации для копии базы данных.

- **Приостановка или возобновление копирования базы данных почтового ящика**. Копию базы данных почтового ящика можно приостановить во время подготовки к заполнения или для других форм обслуживания. Вы также можете приостановить активацию копии базы данных почтовых ящиков. Такая конфигурация предотвращает автоматическую активацию копии базы данных в результате сбоя, но позволяет обновлять эту копию за счет доставки журналов и воспроизведения.

- **Обновление копии базы данных почтового ящика**. Обновление, также известное как *засевание*, — это процесс, в котором копия базы данных почтовых ящиков добавляется на другой сервер почтовых ящиков. Она становится основной базой данных для копирования. После первоначального заполнения основной копии базы данных повторное заполнение потребуется только в исключительных обстоятельствах.

- **Активация копии базы данных почтового ящика**. Активация — это процесс назначения конкретной пассивной копии в качестве новой активной копии базы данных почтовых ящиков. Этот процесс называется *переключением*. Дополнительные сведения см. в разделе Переключения и отработки отказа далее в этом разделе.

- **Удаление копии базы данных почтового ящика**. Иногда может потребоваться удалить копию базы данных почтового ящика. Например, сервер почтовых ящиков нельзя удалить из группы DAG, пока с него не будут удалены все копии баз данных почтовых ящиков. Кроме того, чтобы изменить путь к базе данных почтовых ящиков, необходимо удалить все копии.

Подробные инструкции по добавлению копии базы данных почтовых ящиков см. в статье Add a mailbox database copy. Подробные инструкции по настройке копий базы данных почтовых ящиков см. в статье Configure mailbox database copy properties. Дополнительные сведения о каждой из предыдущих задач управления и об управлении копиями базы данных почтовых ящиков в целом см. в разделе Управление копиями баз данных почтовых ящиков. Подробные инструкции по удалению копии базы данных почтовых ящиков см. в статье Remove a mailbox database copy.

Упреждающий мониторинг

Обеспечение надежной работы серверов и работоспособности копий баз данных необходимо для непрерывного обмена сообщениями. Exchange Server включает ряд функций, которые можно использовать для выполнения различных задач мониторинга работоспособности для групп доступности баз данных и копий баз данных почтовых ящиков, в том числе:

- Get-MailboxDatabaseCopyStatus
- Test-ReplicationHealth
- Ведение журнала событий канала Crimson

Помимо наблюдения за работоспособностью и состоянием, также важно контролировать ситуации, которые могут нарушить доступность. Например, рекомендуем контролировать избыточность реплицированных баз данных. Важно избегать ситуаций, когда остается только одна копия базы данных. Этой проблеме следует назначить самый высокий приоритет и решить ее как можно скорее.

Дополнительные сведения о мониторинге работоспособности и состояния групп доступности и копий баз данных почтовых ящиков см. в разделе Мониторинг групп доступности баз данных.

Переключения и отработки отказа

Переключение — это процесс, при котором администратор вручную активирует одну или несколько копий баз данных почтовых ящиков. Переключения, которые могут происходить на уровне базы данных или на уровне сервера, обычно выполняются в рамках подготовки к обслуживанию. Управление переключениями предполагает переключение баз данных или серверов по мере необходимости. Например, чтобы выполнить обслуживание сервера почтовых ящиков в группе DAG, сначала нужно выполнить переключение сервера, чтобы на нем не было активных копий баз данных почтовых ящиков. Дополнительные сведения о переключении базы данных см. в разделе Активация копии базы данных почтовых ящиков. Переключения также можно выполнять на уровне центра данных.

Отработка отказа — это автоматическая активация системой одной или нескольких копий баз данных почтовых ящиков при сбое. Например, к переходу на другую базу данных может привести отказ диска в среде без RAID. Отказ сети MAPI или сбой питания может привести к переходу на другой сервер.

Управление группами доступности базы данных в Exchange Server

Статья • 04.04.2023

Группа доступности базы данных (DAG) — это набор из 16 серверов почтовых ящиков Exchange, которые обеспечивают автоматическое восстановление на уровне базы данных из базы данных, сервера или сети. В группах DAG используется непрерывная репликация и подмножество технологий отказоустойчивых кластеров Windows, чтобы обеспечить высокий уровень доступности и устойчивость сайта. Почтовые серверы в группе доступности базы данных отслеживают сбои в работе друг друга. При добавлении сервера почтовых ящиков в DAG этот сервер работает с другими серверами в DAG для обеспечения автоматического восстановления на уровне базы данных после сбоев базы данных.

Первоначально создается пустая группа DAG. Когда первый сервер добавляется к группе DAG, для нее автоматически создается отказоустойчивый кластер. Кроме того, инициализируется инфраструктура, которая отслеживает сбои на серверах и в сети. Механизм периодических сигналов о подтверждении соединения с отказоустойчивым кластером и база данных кластера затем используются для отслеживания и обработки информации о группе доступности, которая может быстро изменяться, например о состоянии подключения базы данных, состоянии репликации и о последнем подключении.

Создание групп обеспечения доступности баз данных

DaG можно создать с помощью мастера создания группы доступности баз данных в Центре администрирования Exchange (EAC) или с помощью командлета **New-DatabaseAvailabilityGroup** в командной консоли Exchange. При создании группы обеспечения доступности базы данных необходимо указать ее имя, а также необязательные параметры следящего сервера и следящего каталога. Кроме того, группе можно назначить один или несколько IP-адресов, используя статические IP-адреса или разрешив группе автоматически получить необходимые IP-адреса с помощью протокола DHCP. IP-адреса можно назначить группе daG вручную с помощью параметра *DatabaseAvailabilityGroupIpAddresses* . Если этот параметр не указан, группа попытается получить IP-адрес с помощью DHCP-сервера в сети.

Если вы создаете DAG, которая будет содержать серверы почтовых ящиков под управлением Windows Server 2012 R2, вы также можете создать DAG без точки

административного доступа кластера. В этом случае у кластера не будет объекта имени кластера (CNO) в Active Directory, а группа основных ресурсов кластера будет без ресурса сетевого имени или ресурса IP-адреса.

Дополнительные сведения о создании группы обеспечения доступности баз данных см. в разделе Создание группы обеспечения доступности баз данных.

При создании группы обеспечения доступности баз данных в службах Active Directory создается пустой объект, представляющий группу доступности с указанным именем, и класс объекта **msExchMDBAvailabilityGroup**.

Группы доступности баз данных используют подмножество технологий отказоустойчивой кластеризации Windows в Windows Server 2008 R2 или более поздних версий, таких как пульс кластера, сети кластера и база данных кластера (для хранения данных, которые изменяются или могут быстро изменяться, например с активного на пассивное или обратное, от подключенного к отключенному или обратному). Поэтому группы доступности базы данных можно создавать только на серверах почтовых ящиков Exchange, установленных в поддерживаемых версиях Windows, которые включают отказоустойчивую кластеризацию Windows.

> ⓘ **Примечание**
>
> Отказоустойчивый кластер, создаваемый и используемый группой DAG, должен быть выделен для этой группы. Кластер не может использоваться для другого решения для обеспечения высокого уровня доступности или в каких-либо других целях. Например, невозможно использовать отказоустойчивый кластер для кластеризации других приложений и служб. Использование базового отказоустойчивого кластера группы обеспечения доступности баз данных в других целях, кроме группы DAG, не поддерживается.

Следящий сервер и следящий каталог группы обеспечения доступности баз данных

При создании группы обеспечения доступности базы данных необходимо указать ее имя (не более 15 символов), которое является уникальным в пределах леса Active Directory. Кроме того, настраивается каждая группа доступности с помощью следящего сервера и следящего каталога. Следящий сервер и каталог на нем используются только в том случае, если в группе DAG четное число членов, и только в целях формирования кворума. Нет необходимости заранее создавать следящий каталог. Он будет автоматически создан и защищен системой Exchange

на следящем сервере. Следящий каталог не следует использовать для каких-либо целей, кроме как для сервера-свидетеля DAG.

> ⓘ **Примечание**
>
> В топологии зеркального отображения базы данных можно использовать третий сервер, который называется следящий сервер. Следящий сервер включает автоматическую отработку отказа с основного сервера на зеркальный сервер или наоборот. В отличие от основного и зеркального серверов, следящий сервер не обслуживает базу данных. Роль следящего сервера заключается в том, чтобы проверить, работает ли данный сервер-партнер. Поддержка автоматической отработки отказа является единственной функцией для следящего сервера и определяет, какой сервер содержит основную копию, а какой — зеркальную копию базы данных.

Для следящего сервера существуют следующие требования:

- Следящий сервер не должен быть членом группы DAG.
- Следящий сервер должен располагаться в том же лесу Active Directory, что и группа DAG.
- Следящий сервер должен работать под управлением Windows Server 2008 или более поздней версии.
- Один сервер может быть следящим сервером для нескольких групп DAG. Однако для каждой группы DAG требуется собственный следящий каталог.

Независимо от того, какой сервер используется в качестве следящего, если на нем включен брандмауэр Windows, необходимо включить исключение брандмауэра Windows для общего доступа к файлам и принтерам. Следящий сервер использует SMB-порт 445.

> ⓘ **Важно!**
>
> Если указанный сервер-следящий сервер не является сервером Exchange 2010 или более поздней версии, необходимо добавить универсальную группу безопасности доверенной подсистемы Exchange (USG) в локальную группу администраторов на сервере-свидетеле перед созданием DAG. Эти разрешения безопасности необходимы для создания каталога и файлового ресурса на следящем сервере в приложении Exchange.

Ни следящий сервер, ни каталог не должны быть отказоустойчивыми или использовать какую-либо форму избыточности или высокой доступности. Не требуется использовать кластеризованный файловый сервер или какую-либо другую форму устойчивости для следящего сервера. На это есть несколько причин. Чтобы возникла необходимость в следящем сервере при работе с большими группами обеспечения доступности баз данных (например, с шестью и более членами), должно произойти несколько сбоев. Так как группа DAG из шести членов может выдержать сбои двух серверов без потери кворума, то, чтобы для сохранения кворума потребовался следящий сервер, сбои должны произойти у трех членов группы. Кроме того, при наличии сбоя, который влияет на текущий следящий сервер (например, следящий сервер потерян из-за сбоя оборудования), для настройки нового следящего сервера и следящего каталога (при наличии кворума) используйте командлет Set-DatabaseAvailabilityGroup.

> **Примечание**
>
> Если следящий сервер утратил свое хранилище или кто-либо изменил следящий каталог или разрешения для общего ресурса, для настройки следящего сервера и следящего каталога в исходном расположении можно использовать командлет **Set-DatabaseAvailabilityGroup**.

Варианты размещения следящего сервера

Размещение следящего сервера группы обеспечения доступности баз данных зависит от требований компании и вариантов, доступных в организации. Exchange теперь включает поддержку новых параметров конфигурации DAG, которые не рекомендуются или недоступны в Exchange 2010. Такие параметры включают использование третьего расположения, например третьего центра обработки данных, филиала или виртуальной сети Microsoft Azure.

В следующей таблице приведены общие рекомендации по размещению следящего сервера в различных сценариях развертывания.

Сценарий развертывания	Рекомендации
Один сервер DAG, развернутый в одном центре обработки данных.	Удаленный следящий сервер в том же центре обработки данных, в котором находятся члены DAG

Сценарий развертывания	Рекомендации
Одна DAG, развернутая для двух центров обработки данных; другие расположения недоступны	Расположите следящий сервер в виртуальной сети Microsoft Azure для автоматической отработки отказа центра данных. Или Расположите следящий сервер в главном центре обработки данных
Несколько групп DAG, развернутых в одном центре обработки данных	Удаленный следящий сервер в том же центре обработки данных, в котором находятся члены DAG. Доступны следующие дополнительные параметры. • Использование одного следящего сервера для нескольких DAG • Использование члена DAG в качестве следящего сервера для другой DAG
Несколько групп DAG, развернутых для двух центров обработки данных	Расположите следящий сервер в виртуальной сети Microsoft Azure для автоматической отработки отказа центра данных. Или Расположите следящий сервер в центре обработки данных, являющемся главным для каждой DAG. Доступны следующие дополнительные параметры. • Использование одного следящего сервера для нескольких DAG • Использование члена DAG в качестве следящего сервера для другой DAG
Одна или несколько DAG, развернутых для более чем двух центров обработки данных	В данной конфигурации следящий сервер может быть расположен в центре обработки данных, в котором требуется разместить большую часть голосов кворума.

При развертывании DAG в двух центрах обработки данных теперь можно использовать третье расположение для размещения следящего сервера. Если в вашей организации есть третье расположение с сетевой инфраструктурой, изолированной от сетевых сбоев, влияющих на два центра обработки данных, в которых развернута группа доступности баз данных, можно развернуть следящий сервер DAG в этом третьем расположении, тем самым настроив daG возможность автоматической отработки отказа баз данных в другой центр обработки данных в ответ на событие сбоя на уровне центра обработки данных. Если в вашей организации два физических местоположения, вы можете использовать виртуальную сеть Microsoft Azure как третье расположение для размещения следящего сервера.

Определение следящего сервера и следящего каталога во время создания группы обеспечения доступности баз данных

При создании группы обеспечения доступности базы данных необходимо указать ее имя. Дополнительно можно указать следящий сервер и следящий каталог.

При создании группы DAG доступны следующие сочетания параметров и реакций на события:

- Можно указать только имя для DAG и оставить поля **Следящий сервер** и **каталог свидетеля** пустыми. В этом сценарии мастер выполняет поиск на локальном сайте Active Directory сервера клиентского доступа, на котором не установлен сервер почтовых ящиков, и автоматически создает каталог по умолчанию (%SystemDrive%:\DAGFileShareWitnesses\<*DAGFQDN*>) и общую папку по умолчанию (<*DAGFQDN*>) на этом сервере и использует этот сервер клиентского доступа в качестве следящего сервера. Например, рассмотрим следящий сервер CAS3, на котором установлена операционная система на диск C. DaG с именем DAG1 в домене contoso.com будет использовать каталог-свидетель по умолчанию C:\DAGFileShareWitnesses\DAG1.contoso.com, который будет использоваться как \CAS3\DAG1.contoso.com.

- Пользователь может указать имя для группы обеспечения доступности баз данных, для используемого следящего сервера, а также для каталога, созданного и открытого для совместного доступа на следящем сервере.

- Пользователь может указать имя для группы обеспечения доступности баз данных и используемого следящего сервера и оставить поле **Следящий каталог** пустым. В этом сценарии на указанном следящем сервере мастер создаст каталог по умолчанию.

- Можно указать имя группы обеспечения доступности баз данных, не заполнять поле **Следящий сервер** и указать каталог, который требуется создать и открыть для совместного доступа на следящем сервере. В этом сценарии мастер выполнит поиск сервера клиентского доступа, на котором не установлена роль сервера почтовых ящиков, автоматически создаст на сервере указанную группу обеспечения доступности баз данных, включит общий доступ для каталога и будет использовать сервер клиентского доступа в качестве следящего сервера.

После формирования группы обеспечения доступности баз данных в ней первоначально используется модель кворума "Большинство узлов". После добавления второго сервера почтовых ящиков в группу обеспечения доступности баз данных кворум автоматически меняется на модель кворума "Большинство

сайтов и общих файловых ресурсов". После этих изменений кластер группы обеспечения доступности баз данных будет использовать следящий сервер для сохранения кворума. Если следящего каталога не существует, сервер Exchange автоматически создаст его, включит для него общий доступ и предоставит для общего ресурса разрешения на полный доступ для учетной записи компьютера сетевого объекта кластера (CNO) в группе доступности баз данных.

> ⓘ **Примечание**
>
> Использование общей папки, которая является частью пространства имен распределенной файловой системы, не поддерживается.

Если брандмауэр Windows включен на следящем сервере до создания группы обеспечения доступности баз данных, он может блокировать ее создание. Сервер Exchange использует инструментарий управления Windows (WMI) для создания каталога и общего файлового ресурса на следящем сервере. Если брандмауэр Windows включен на следящем сервере и для инструментария управления Windows не настроены исключения брандмауэра, произойдет сбой командлета **New-DatabaseAvailabilityGroup**. Если указан следящий сервер, а не следящий каталог, отобразится следующее сообщение об ошибке:

```
The task was unable to create the default witness directory on server <Server Name>. Please manually specify a witness directory.
```

Если указаны следящий сервер и следящий каталог, отобразится следующее предупреждение:

```
Unable to access file shares on witness server '<ServerName>'. Until this problem is corrected, the database availability group may be more vulnerable to failures. You can use the Set-DatabaseAvailabilityGroup cmdlet to try the operation again. Error: The network path was not found.
```

Если брандмауэр Windows включен на следящем сервере после создания группы обеспечения доступности баз данных, но перед добавлением серверов, он может блокировать добавление или удаление членов группы обеспечения доступности баз данных. Если брандмауэр Windows включен на следящем сервере и для инструментария управления Windows не настроены исключения брандмауэра, командлет **Add-DatabaseAvailabilityGroupServer** вернет следующее предупреждение:

```
Failed to create file share witness directory 'C:\DAGFileShareWitnesses\DAG_FQDN' on witness server '<ServerName>'. Until this problem is corrected, the database
```

`availability group may be more vulnerable to failures. You can use the Set-DatabaseAvailabilityGroup cmdlet to try the operation again. Error: WMI exception occurred on server '<ServerName>': The RPC server is unavailable. (Exception from HRESULT: 0x800706BA)`

Чтобы устранить предыдущие сообщения об ошибках и предупреждения, выполните одно из следующих действий.

- Вручную создайте следящий каталог и общий ресурс на следящем сервере и назначьте для них разрешения на полный доступ для объекта CNO в группе DAG.
- Включите исключение WMI в брандмауэре Windows.
- Отключите брандмауэр Windows.

Членство в группы обеспечения доступности базы данных

После создания daG можно добавить серверы в daG или удалить их из нее с помощью мастера управления группой доступности базы данных в Центре администрирования Exchange (EAC) или командлетов **Add-DatabaseAvailabilityGroupServer** или **Remove-DatabaseAvailabilityGroupServer** в командной консоли Exchange. Подробные инструкции по управлению членством в DAG см. в разделе Управление членством в группе доступности базы данных.

> ⓘ **Примечание**
>
> Каждый сервер почтовых ящиков, являющийся членом такой группы DAG, также является узлом базового кластера, используемого группой. Таким образом, сервер почтовых ящиков одновременно может быть членом только одной группы обеспечения доступности баз данных.

Если на сервере почтовых ящиков, добавляемом в группу обеспечения доступности баз данных, не установлен компонент отказоустойчивой кластеризации, то с помощью метода, используемого для добавления сервера (например, командлета **Add-DatabaseAvailabilityGroupServer** или мастера управления группами обеспечения доступности баз данных), будет установлено средство отказоустойчивой кластеризации.

При добавлении первого сервера почтовых ящиков в группу DAG происходит следующее:

- Устанавливается компонент отказоустойчивости кластера Windows, если он еще не установлен.
- Создается отказоустойчивый кластер с помощью имени группы DAG. Отказоустойчивый кластер используется только группой DAG и должен быть выделен для этой группы. Использование кластера в других целях не поддерживается.
- Создается объект CNO в контейнере компьютеров по умолчанию.
- Регистрируется имя и IP-адрес группы обеспечения доступности баз данных в качестве записи узла (A) в службе DNS.
- Добавляется сервер к объекту DAG в Active Directory.
- Обновляется база данных кластера информацией о базах данных, установленных на добавленный сервер.

В крупных средах или средах с несколькими сайтами, особенно в которых группа DAG расширена на несколько сайтов Active Directory, необходимо дождаться завершения репликации Active Directory объекта DAG, содержащего первый член группы DAG. Если этот объект Active Directory не реплицирован во всей среде, при добавлении второго сервера может быть создан новый кластер (и новый объект CNO) для группы DAG. Это происходит потому, что объект DAG является пустым с точки зрения второго добавляемого сервера, в результате чего командлет **Add-DatabaseAvailabilityGroupServer** создает новый кластер и объект CNO для группы DAG, даже если эти объекты уже существуют. Чтобы убедиться, что объект DAG, содержащий первый сервер DAG, реплицирован, используйте командлет **Get-DatabaseAvailabilityGroup** на втором добавляемом сервере, чтобы проверить, что первый добавленный сервер включен в список членов группы обеспечения доступности баз данных.

После добавления второго и последующих серверов к группе DAG происходит следующее.

- Сервер присоединяется к отказоустойчивому кластеру Windows для группы DAG.
- Автоматически настраивается модель кворума:
    - Используется модель кворума "Большинство узлов" для групп DAG с нечетным количеством участников.

    - Используется модель кворума "Большинство узлов и общих файловых ресурсов" для групп DAG с четным количеством участников.
- При необходимости Exchange автоматически создает следящий каталог и общий ресурс.
- Добавляется сервер к объекту DAG в Active Directory.
- Обновляется база данных кластера информацией об установленных базах данных.

> ⓘ **Примечание**
>
> Автоматически меняется модель кворума. Однако если модель кворума не меняется автоматически на правильную модель, можно запустить командлет **Set-DatabaseAvailabilityGroup** только с параметром *Identity*, чтобы исправить параметры кворума для группы обеспечения доступности базы данных.

Регистрация объекта имени кластера для группы DAG

Объект имени кластера — это учетная запись компьютера, создаваемая в службе Active Directory и связываемая с ресурсом имени кластера. Ресурс имени кластера связан с объектом имени кластера, который является объектом с включенной поддержкой Kerberos, действующим как идентификатор кластера и обеспечивающим контекст безопасности кластера. Формирование базового кластера группы обеспечения доступности баз данных и объекта CNO для этого кластера выполняется при добавлении первого члена в группу DAG. После добавления первого сервера в группу DAG удаленная среда Powershell подключается к службе репликации Microsoft Exchange на добавляемом сервере почтовых ящиков. Служба репликации Microsoft Exchange устанавливает средство отказоустойчивой кластеризации (если оно не установлено) и запускает процесс создания кластера. Служба репликации Microsoft Exchange работает в контексте безопасности LOCAL SYSTEM, и создание кластера выполняется в этом контексте.

> ⊗ **Внимание!**
>
> Если члены группы обеспечения доступности баз данных используют Windows Server 2012, необходимо подготовить объект CNO до добавления первого сервера в группу DAG. Если члены группы обеспечения доступности баз данных используют Windows Server 2012 R2, и она создана без точки

административного доступа кластера, объект CNO не создается, и создавать объект CNO для группы обеспечения доступности баз данных не требуется.

В средах, в которых создание учетной записи компьютера ограничено или учетные записи компьютеров создаются в контейнере, отличном от контейнера компьютеров по умолчанию, необходимо зарегистрировать и подготовить объект CNO. Пользователь создает и отключает учетную запись компьютера для объекта CNO, а затем выполняет одно из следующих действий.

- Назначить разрешения на полный доступ к учетной записи компьютера для учетной записи компьютера, являющегося первым сервером почтовых ящиков, добавляемым в группу обеспечения доступности баз данных.
- Назначить универсальной группе безопасности доверенной подсистемы Exchange разрешения на полный доступ к учетной записи компьютера.

Назначение разрешений на полный доступ к учетной записи компьютера для учетной записи компьютера первого сервера почтовых ящиков, добавленного в группу DAG, позволяет контексту безопасности LOCAL SYSTEM управлять зарегистрированной учетной записью компьютера. Вместо этого можно назначить разрешения на полный доступ к учетной записи компьютера универсальной группе безопасности доверенной подсистемы Exchange, так как эта группа доверенной подсистемы Exchange включает в себя учетные записи компьютеров всех серверов Exchange в домене.

Дополнительные сведения о регистрации и подготовке объекта CNO для группы обеспечения доступности баз данных см. в разделе Регистрация объекта имени кластера для группы обеспечения доступности баз данных.

Удаление серверов из DAG

Серверы почтовых ящиков можно удалить из daG с помощью мастера управления группой доступности базы данных в EAC или **командлета Remove-DatabaseAvailabilityGroupServer** в командной консоли Exchange. Необходимо удалить все реплицированные базы данных почтовых ящиков с сервера почтовых ящиков, прежде чем удалить сам сервер из группы DAG. При попытке удалить сервер почтовых ящиков с реплицированными базами данных почтовых ящиков из группы DAG произойдет сбой.

Существует несколько сценариев, в которых перед выполнением определенных операций необходимо удалить сервер почтовых ящиков из группы обеспечения доступности баз данных. Это происходит в описанных ниже случаях.

- **Выполнение операции восстановления сервера**. Если сервер почтовых ящиков, который является членом DAG, потерян или иным образом завершается сбоем и не восстанавливается и требует замены, можно выполнить операцию восстановления сервера с помощью параметра **Setup /m:RecoverServer** . Однако перед выполнением операции восстановления необходимо сначала удалить сервер из DAG с помощью командлета Remove-DatabaseAvailabilityGroupServer с параметром *ConfigurationOnly* .

- **Удаление группы доступности базы данных**. Могут возникнуть ситуации, в которых необходимо удалить DAG (например, при отключении режима репликации сторонних производителей). Перед удалением группы DAG необходимо сначала удалить из нее все серверы. Попытка удаления группы DAG, содержащей члены, завершится неудачей.

Настройка свойств DAG

После добавления серверов в DAG можно использовать EAC или командную консоль Exchange для настройки свойств DAG, включая следящий сервер и каталог следящего сервера, используемый DAG, а также IP-адреса, назначенные daG.

Настраиваемые свойства включают в себя следующее:

- **Сервер-свидетель**. Имя сервера, на котором вы хотите разместить общую папку для общей папки-свидетеля. Мы рекомендуем указать сервер клиентского доступа в качестве следящего сервера. Это позволяет системе автоматически формировать, защищать и использовать общий ресурс по мере необходимости, а также позволяет администратору контролировать доступность следящего сервера.

- **Следящий каталог**. Имя каталога, который будет использоваться для хранения данных следящего файла общей папки. Этот каталог будет автоматически создан системой на указанном следящем сервере.

- **IP-адреса группы доступности базы данных. Группе доступности** необходимо назначить один или несколько IP-адресов, если только члены группы daG не работают Windows Server 2012 R2 и вы создаете группу управления базой данных без IP-адреса. В противном случае IP-адреса DAG можно настроить с помощью назначенных вручную статических IP-адресов или их можно автоматически назначить группе daG с помощью DHCP-сервера в вашей организации.

Командная консоль Exchange позволяет настроить свойства DAG, недоступные в EAC, такие как IP-адреса DAG, параметры шифрования и сжатия сети, обнаружение сети, TCP-порт, используемый для репликации, а также альтернативные параметры следящего сервера и следящего каталога, а также включить режим координации активации центра обработки данных.

Дополнительные сведения о настройке свойств группы DAG см. в разделе Настройка свойств группы обеспечения доступности баз данных.

Шифрование в сети группы обеспечения доступности баз данных

DaG поддерживают использование шифрования, используя возможности шифрования операционной системы Windows Server. Группы доступности баз данных используют проверку подлинности Kerberos между серверами Exchange. API DecryptMessage и EncryptMessage поставщика поддержки безопасности (SSP) Microsoft Kerberos отвечают за шифрование сетевого трафика группы DAG. Поставщик поддержки безопасности Microsoft Kerberos поддерживает несколько алгоритмов шифрования. (Полный список см. в разделе 3.1.5.2, "Типы шифрования" расширений протокола Kerberos). При подтверждении проверки подлинности Kerberos выбирается самый надежный поддерживаемый протокол шифрования из указанных в списке: обычно стандарт AES с 256-разрядным ключом, возможно, вместе с кодом проверки подлинности сообщения на основе хэша (HMAC) по алгоритму SHA для сохранения целостности данных. Дополнительные сведения см. в разделе HMAC.

Шифрование в сети является свойством группы DAG, а не сети DAG. Вы можете настроить шифрование сети DAG с помощью командлета **Set-DatabaseAvailabilityGroup** в командной консоли Exchange. Возможные параметры для установления связи в сети DAG показаны в следующей таблице.

Setting	**Описание**
Отключено	Шифрование сети не используется.
Включено	Шифрование в сети используется во всех сетях DAG для репликации и заполнения.
InterSubnetOnly	Шифрование в сети используется в сетях DAG при репликации в разных подсетях. Это настройка по умолчанию.
SeedOnly	Шифрование в сети используется во всех сетях DAG только для заполнения.

Сжатие в сети DAG

В группах DAG поддерживается встроенное сжатие. Если сжатие включено, при установлении связи в сети DAG используется сжатие XPRESS, которое является реализацией Microsoft для алгоритма LZ77. Это тот же тип сжатия, который используется во многих протоколах Майкрософт, в частности, в сжатии MAPI RPC между Microsoft Outlook и Exchange.

Как и шифрование в сети, сжатие в сети является свойством группы DAG, а не сети DAG. Сжатие сети DAG настраивается с помощью командлета Set-DatabaseAvailabilityGroup в командной консоли Exchange. Возможные параметры сжатия для установления связи в сети DAG показаны в следующей таблице.

Setting	Описание
Отключено	Сжатие в сети не используется.
Включен	Сжатие в сети используется во всех сетях DAG для репликации и заполнения.
InterSubnetOnly	Сжатие в сети используется в сетях DAG при репликации в разных подсетях. Это настройка по умолчанию.
SeedOnly	Сжатие в сети используется во всех сетях DAG только для заполнения.

Сети групп обеспечения доступности баз данных

Сеть DAG — это коллекция из одной или нескольких подсетей, используемых либо для трафика репликации, либо для трафика MAPI. Каждая группа DAG содержит не более одной сети MAPI и 0 или более сетей репликации. В конфигурации одного сетевого адаптера сеть используется как для трафика MAPI, так и для трафика репликации. Хотя поддерживается один сетевой адаптер и путь, рекомендуется, чтобы каждое daG было как минимум две сети DAG. В конфигурации с двумя сетями одна сеть обычно выделяется для трафика репликации, а другая сеть используется в основном для трафика MAPI. Кроме того, вы можете добавить сетевые адаптеры для каждого члена группы DAG и настроить дополнительные сети DAG как сети репликации.

> ⓘ **Примечание**
>
> При использовании нескольких сетей репликации невозможно указать приоритет использования сети. Exchange случайным образом выбирает сеть

репликации из группы сетей репликации для доставки журналов.

В Exchange 2010 во многих сценариях необходима ручная настройка сетей DAG. По умолчанию в более поздних версиях Exchange сети DAG автоматически настраиваются системой. Перед созданием или изменением сетей DAG необходимо сначала включить ручное управление сетью DAG, выполнив следующую команду:

```
PowerShell

Set-DatabaseAvailabilityGroup <DAGName> -ManualDagNetworkConfiguration $true
```

После включения настройки сети DAG вручную можно использовать командлет **New-DatabaseAvailabilityGroupNetwork** в командной консоли Exchange, чтобы создать сеть DAG. Подробные инструкции по созданию сети DAG см. в статье Создание сети группы доступности базы данных.

Для настройки свойств сети DAG можно использовать командлет **Set-DatabaseAvailabilityGroupNetwork** в командной консоли Exchange. Подробные инструкции по настройке свойств сети DAG см. в разделе Настройка сетевых свойств группы доступности базы данных. В каждой сети DAG есть необходимые и дополнительные параметры для настройки:

- **Имя сети**: уникальное имя для сети DAG из 128 символов.
- **Описание сети**: необязательное описание для сети DAG длиной до 256 символов.
- **Сетевые подсети**: одна или несколько подсетей, введенных в формате *IPAddress/Bitmask* (например, 192.168.1.0/24 для подсетей IPv4; 2001:DB8:0:C000::/64 для подсетей протокола IPv6).
- **Включить репликацию**. В EAC установите флажок, чтобы посвятить сеть DAG трафику репликации и заблокировать трафик MAPI. Снимите флажок, чтобы запретить использование сети группы DAG для репликации и включить трафик MAPI. В командной консоли Exchange используйте параметр *ReplicationEnabled* в командлете Set-DatabaseAvailabilityGroupNetwork , чтобы включить и отключить репликацию.

> ⓘ **Примечание**
>
> Отключение репликации для сети MAPI не гарантирует того, что система не будет использовать эту сеть для репликации. Когда все настроенные сети

репликации находятся в автономном режиме, неисправны или недоступны и сохраняется только сеть MAPI, для которой отключена репликация, система будет использовать эту сеть для репликации.

Начальные сети DAG (например, MapiDagNetwork и ReplicationDagNetwork01), создаваемые системой, основаны на подсетях службы кластеров. Каждый член группы DAG должен иметь идентичное количество сетевых адаптеров, а каждый сетевой адаптер должен иметь адрес IPv4 (а также, возможно, и адрес IPv6) в уникальной подсети. Несколько членов группы DAG могут иметь адреса IPv4 в одной подсети, но IP-адрес каждого сетевого адаптера определенного сервера группы DAG должен принадлежать уникальной подсети. Кроме того, шлюз по умолчанию должен использоваться только адаптером сети MAPI. Сети репликации не должны настраиваться на использование шлюза по умолчанию.

Например, рассмотрим группу DAG1 с двумя членами, каждый из которых имеет по два сетевых адаптера (один выделен для сети MAPI, а другой — для сети репликации). Примерные параметры конфигурации IP-адреса представлены в следующей таблице.

Пример настройки параметров сетевого адаптера

Адаптер "сервер-сеть"	IP-адрес/маска подсети	Шлюз по умолчанию
EX1-MAPI	192.168.1.15/24	192.168.1.1
EX1-Репликация	10.0.0.15/24	Неприменимо
EX2-MAPI	192.168.1.16	192.168.1.1
EX2-Репликация	10.0.0.16	Неприменимо

В следующей конфигурации группа DAG содержит две настроенные подсети: 192.168.1.0 и 10.0.0.0. При добавлении серверов EX1 и EX2 в группу DAG обе подсети будут пронумерованы и будет создано две сети DAG: MapiDagNetwork (192.168.1.0) и ReplicationDagNetwork01 (10.0.0.0). Эти сети будут настроены, как показано в следующей таблице.

Параметры нумерованных сетей DAG для группы DAG с одной подсетью

Имя	Подсети	Интерфейсы	Доступ MAPI включен	Репликация включена

Имя	Подсети	Интерфейсы	Доступ MAPI включен	Репликация включена
MapiDagNetwork	192.168.1.0/24	EX1 (192.168.1.15) EX2 (192.168.1.16)	Да	Да
ReplicationDagNetwork01	10.0.0.0/24	EX1 (10.0.0.15) EX2 (10.0.0.16)	Нет	Да

Чтобы завершить настройку Replicationdagnetwork01 в качестве выделенной сети репликации, отключите репликацию для MapiDagNetwork, выполнив следующую команду.

PowerShell

```
Set-DatabaseAvailabilityGroupNetwork -Identity DAG1\MapiDagNetwork -
ReplicationEnabled:$false
```

После отключения репликации для MapiDagNetwork служба репликации Microsoft Exchange использует ReplicationDagNetwork01 для непрерывной репликации. Если произойдет сбой ReplicationDagNetwork01, то служба репликации Microsoft Exchange вернется к использованию MapiDagNetwork для непрерывной репликации. Это преднамеренное действие системы для обеспечения высокого уровня доступности.

Развертывание нескольких подсетей и сетей группы обеспечения доступности баз данных

В предыдущем примере несмотря на использование в группе DAG двух различных подсетей (192.168.1.0 и 10.0.0.0) эта группа считается группой DAG с одной подсетью, потому что все члены группы используют одну подсеть для формирования сети MAPI. Когда члены группы DAG используют различные подсети для сети MAPI, такая группа называется *группой DAG с несколькими подсетями*. В группах DAG с несколькими подсетями соответствующие подсети будут автоматически назначаться каждой сети DAG.

Например, рассмотрим группу DAG2 с двумя членами, каждый из которых имеет по два сетевых адаптера (один выделен для сети MAPI, а другой — для сети репликации) и расположен на отдельном сайте Active Directory, а их сети MAPI

находятся в различных подсетях. Примерные параметры конфигурации IP-адреса представлены в следующей таблице.

Примерные параметры сетевых адаптеров для группы DAG с несколькими подсетями

Адаптер "сервер-сеть"	IP-адрес/маска подсети	Шлюз по умолчанию
EX1-MAPI	192.168.0.15/24	192.168.0.1
EX1-Репликация	10.0.0.15/24	Неприменимо
EX2-MAPI	192.168.1.15	192.168.1.1
EX2-Репликация	10.0.1.15	Неприменимо

В следующей конфигурации в DAG настроены четыре подсети: 192.168.0.0, 192.168.1.0, 10.0.0.0 и 10.0.1.0. При добавлении EX1 и EX2 в DAG будут перечислены четыре подсети, но будут созданы только две сети DAG: MapiDagNetwork (192.168.0.0, 192.168.1.0) и ReplicationDagNetwork01 (10.0.0.0, 10.0.1.0). Эти сети будут настроены, как показано в следующей таблице.

Параметры нумерованных сетей DAG для группы DAG с несколькими подсетями

Имя	Подсети	Интерфейсы	Доступ MAPI включен	Репликация включена
MapiDagNetwork	192.168.0.0/24 192.168.1.0/24	EX1 (192.168.0.15) EX2 (192.168.1.15)	Да	Да
ReplicationDagNetwork01	10.0.0.0/24 10.0.1.0/24	EX1 (10.0.0.15) EX2 (10.0.1.15)	Нет	Верно

Сети DAG и iSCSI

По умолчанию в группах DAG выполняется поиск всех сетей, обнаруженных и настроенных для использования с помощью базового кластера. При этом учитываются любые сети Internet SCSI (iSCSI), которые используются в результате применения хранилища iSCSI для одного или нескольких членов DAG. Рекомендуется использовать для хранилища iSCSI выделенные сети и сетевые адаптеры. Эти сети не должны управляться группами DAG и ее кластерами или использоваться в качестве сетей DAG (MAPI или репликация). Вместо этого для них

необходимо вручную отключить использование группой DAG и выделить их для трафика хранилища iSCSI. Для отключения обнаружения и использования сетей iSCSI в качестве сетей DAG, настройте DAG так, чтобы игнорировать любые обнаруженные сети iSCSI, с помощью командлета Set-DatabaseAvailabilityGroupNetwork, как показано в следующем примере:

PowerShell

```
Set-DatabaseAvailabilityGroupNetwork -Identity DAG2\DAGNetwork02 -
ReplicationEnabled:$false -IgnoreNetwork:$true
```

Эта команда также отключит использование сети кластером. Хотя сети iSCSI по-прежнему будут отображаться как сети DAG, они не будут использоваться для трафика репликации или MAPI после выполнения предыдущей команды.

Настройка членов DAG

Серверы почтовых ящиков, являющиеся членами группы DAG, имеют несколько свойств, относящихся к обеспечению высокого уровня доступности, которые необходимо настроить, как описано в следующих разделах.

- Автоматическое подключение базы данных
- Политика автоматической активации копии базы данных
- Maximum active databases

Автоматическое подключение базы данных

Параметр *AutoDatabaseMountDial* определяет поведение при автоматическом подключении базы данных после отработки отказа базой данных. С помощью командлета Set-MailboxServer можно настроить параметр *AutoDatabaseMountDial* с любым из следующих значений:

- `BestAvailability`: если указать это значение, база данных автоматически подключается сразу после отработки отказа, если длина очереди копирования меньше или равна 12. Длина очереди копирования — это число журналов, определяемых пассивной копией, для которых необходимо выполнить репликацию. Если значение длины очереди копирования превышает 12, база данных не будет подключаться автоматически. Если длина очереди копирования не превышает 12, Exchange попытается реплицировать оставшиеся журналы на пассивную копию и подключит базы данных.

- `GoodAvailability`: если указать это значение, база данных автоматически подключается сразу после отработки отказа, если длина очереди копирования меньше или равна шести. Длина очереди копирования — это число журналов, определяемых пассивной копией, для которых необходимо выполнить репликацию. Если значение длины очереди копирования превышает 6, база данных не будет подключаться автоматически. Если длина очереди копирования не превышает 6, Exchange попытается реплицировать оставшиеся журналы на пассивную копию и подключит базу данных.

- `Lossless`: если указать это значение, база данных не подключается автоматически, пока все журналы, созданные в активной копии, не будут скопированы в пассивную копию. При этом значении алгоритмом выбора лучшей копии диспетчера Active Manager возможные кандидаты для активации будут выбираться на основе значения приоритета активации копии базы данных, а не длины очереди копии.

Значение по умолчанию — `GoodAvailability`. Если указать или `BestAvailability` `GoodAvailability`, а все журналы из активной копии не удастся скопировать в активируемую пассивную копию, вы можете потерять некоторые данные почтового ящика. Тем не менее, функция системы безопасности (которая включена по умолчанию) обеспечивает защиту от потери данных благодаря повторной отправке сообщений в очереди системы безопасности.

Пример. Настройка автоматического подключения базы данных

В следующем примере сервер почтовых ящиков настраивается с параметром `GoodAvailability` *AutoDatabaseMountDial* .

PowerShell

```
Set-MailboxServer -Identity EX1 -AutoDatabaseMountDial GoodAvailability
```

Политика автоматической активации копии базы данных

Параметр *DatabaseCopyAutoActivationPolicy* указывает тип автоматической активации, доступной для копий базы данных почтовых ящиков на выбранных серверах почтовых ящиков. С помощью командлета Set-MailboxServer можно

настроить параметр *DatabaseCopyAutoActivationPolicy* с любым из следующих значений:

- `Blocked`: если указать это значение, базы данных не могут быть автоматически активированы на выбранных серверах почтовых ящиков.
- `IntrasiteOnly`: если указать это значение, копию базы данных можно активировать на серверах на том же сайте Active Directory. Это предотвращает отработку отказа или активацию между сайтами. Это свойство предназначено для входящих копий базы данных почтовых ящиков (например, пассивная копия становится активной). Базы данных не могут быть активированы на этом сервере почтовых ящиков для копий баз данных, которые активны на другом сайте Active Directory.
- `Unrestricted`: если указать это значение, нет особых ограничений на активацию копий баз данных почтовых ящиков на выбранных серверах почтовых ящиков.

Пример. Настройка политики автоматической активации копии базы данных

В следующем примере сервер почтовых ящиков настраивается с параметром `Blocked`*DatabaseCopyAutoActivationPolicy* .

PowerShell

```
Set-MailboxServer -Identity EX1 -DatabaseCopyAutoActivationPolicy Blocked
```

Максимальное количество активных баз данных

Параметр *MaximumActiveDatabases* (также используемый с командлетом Set-MailboxServer) указывает количество баз данных, которые можно подключить к серверу почтовых ящиков. Для соблюдения требований развертывания серверы почтовых ящиков можно настроить таким образом, чтобы не превышалась нагрузка на отдельные серверы почтовых ящиков.

Параметр *MaximumActiveDatabases* настраивается с целым числовым значением. Когда будет достигнуто максимальное количество баз данных, копии баз данных на сервере не будут активироваться при отработке отказа. Если копии уже активированы на сервере, сервер не позволит выполнить подключение баз данных.

Пример. Настройка максимального количества активных баз данных

В следующем примере показана настройка сервера почтовых ящиков для поддержки не более 20 активных баз данных.

PowerShell

```
Set-MailboxServer -Identity EX1 -MaximumActiveDatabases 20
```

Обслуживание участников DAG

Прежде чем выполнять какое-либо обслуживание программного или аппаратного обеспечения для члена группы DAG, необходимо сначала перевести этого сервера в режим обслуживания. Следующие скрипты предоставляются с Exchange Server для упрощения процедур обслуживания DAG.

- **StartDagServerMaintenance.ps1**. Помогает перемещать все активные базы данных с сервера. Он также перемещает все критически важные функции поддержки DAG, такие как роль основного активного диспетчера (PAM), и блокирует их перемещение обратно на сервер до завершения обслуживания.
- **StopDagServerMaintenance.ps1**: помогает вывести член DAG из режима обслуживания и сделать его активным целевым объектом для всех баз данных и всех критически важных функций поддержки DAG.

Оба приведенных выше скрипта принимают параметр *ServerName* (который может быть именем узла или полным доменным именем (FQDN) члена DAG) и параметр *WhatIf* . Оба сценария можно выполнять локально или удаленно. На сервере, на котором выполняются сценарии, должны быть установлены средства управления отказоустойчивым кластером Windows (RSAT-Clustering).

> ⓘ **Примечание**
>
> Скрипт **RedistributeActiveDatabases.ps1** также доступен, что помогает подключать базы данных почтовых ящиков к определенным членам DAG, как указано в предпочтительном номере активации для каждой базы данных. Однако в Exchange 2016 с накопительным пакетом обновления 2 (CU2) или более поздней версии новое свойство DAG *с именем PreferenceMoveFrequency* автоматически распределяет копии базы данных по daG. Поэтому вам потребуется использовать **RedistributeActiveDatabases.ps1** только в том случае,

если вы отключили эту функцию или хотите сбалансировать копии базы данных вручную.

Сценарий StartDagServerMaintenance.ps1 выполняет следующие задачи:

- Задает для параметра *DatabaseCopyAutoActivationPolicy* в члене `Blocked`DAG значение , что предотвращает активацию любых копий базы данных на сервере.
- Приостанавливает работу узла в кластере, что не позволяет этому узлу быть (или становиться) основным диспетчером Active Manager (PAM).
- Перемещает все активные базы данных, размещенные на сервере-члене группы DAG, на другие серверы-члены группы DAG.
- Если в данный момент член группы DAG владеет кластерной группой по умолчанию, сценарий переместит ее (и роль PAM) на другой сервер-член группы DAG.

Если при выполнении какой-либо задачи произойдет сбой, сценарий отменит все операции, кроме успешного перемещения баз данных.

Чтобы начать обслуживание члена группы DAG, включая очистку очереди транспорта и приостановку подключения клиентов, сделайте следующее:

1. Чтобы очистить очереди транспорта, выполните следующую команду:

   PowerShell

   ```
   Set-ServerComponentState <ServerName> -Component HubTransport -State
   Draining -Requester Maintenance
   ```

2. Чтобы инициировать очистку транспортных очередей, выполните следующую команду:

   PowerShell

   ```
   Restart-Service MSExchangeTransport
   ```

3. Чтобы начать процесс очистки всех вызовов единой системы обмена сообщениями (только в Exchange 2016), выполните следующую команду:

   PowerShell

```
Set-ServerComponentState <ServerName> -Component UMCallRouter -State
Draining -Requester Maintenance
```

4. Чтобы получить доступ к сценариям обслуживания DAG, выполните следующую команду:

```
PowerShell

CD $ExScripts
```

5. Чтобы запустить скрипт StartDagServerMaintenance.ps1, выполните следующую команду:

```
PowerShell

.\StartDagServerMaintenance.ps1 -ServerName <ServerName> -MoveComment
Maintenance -PauseClusterNode
```

Для значения параметра *MoveComment* можно сделать любую нотацию. В предыдущем примере используется "Обслуживание".

> ⓘ **Примечание**
>
> Выполнение этого сценария может занять некоторое время, в течение которого на экране не будут отображаться никакие действия.

6. Чтобы перенаправить сообщения, ожидающие доставки в локальных очередях, на сервер Exchange Server, указанный параметром Target, выполните команду

```
PowerShell

Redirect-Message -Server <ServerName> -Target <Server FQDN>
```

7. Чтобы поместить сервер в режим обслуживания, выполните следующую команду:

```
PowerShell

Set-ServerComponentState <ServerName> -Component ServerWideOffline -
State Inactive -Requester Maintenance
```

Чтобы убедиться в готовности сервера к обслуживанию, выполните следующие задачи.

1. Чтобы убедиться, что сервер переведен в режим обслуживания, убедитесь, что только `Monitoring` и `RecoveryActionsEnabled` находятся в активном состоянии при выполнении следующей команды:

   PowerShell

   ```
   Get-ServerComponentState <ServerName> | Format-Table Component,State -Autosize
   ```

2. Чтобы убедиться, что на сервере не размещены активные копии базы данных, выполните следующую команду:

   PowerShell

   ```
   Get-MailboxServer <ServerName> | Format-List DatabaseCopyAutoActivationPolicy
   ```

3. Чтобы убедиться, что узел кластера приостановлен, выполните следующую команду:

   PowerShell

   ```
   Get-ClusterNode <ServerName> | Format-List
   ```

4. Чтобы убедиться, что все очереди транспорта очищены, выполните следующую команду:

   PowerShell

   ```
   Get-Queue
   ```

Когда обслуживание члена группы DAG завершено и он подготовлен к возобновлению работы, его нужно перевести из режима обслуживания в рабочий режим с помощью сценария StopDagServerMaintenance.ps1. Сценарий StopDagServerMaintenance.ps1 выполняет следующие задачи:

- Возобновляет работу узла в кластере, а также восстанавливает полную функциональность кластера для члена группы DAG.
- Задает для параметра *DatabaseCopyAutoActivationPolicy* в члене `Unrestricted`DAG значение .

- Запускает командлет Resume-MailboxDatabaseCopy для каждой копии базы данных, размещенной на сервере-члене группы DAG.

Когда вы будете готовы восстановить член DAG до полного рабочего состояния, включая возобновление транспортных очередей и подключение клиента, выполните следующие задачи:

1. Чтобы настроить сервер в режиме обслуживания и быть готовым к приему клиентских подключений, выполните следующую команду:

```
PowerShell

Set-ServerComponentState <ServerName> -Component ServerWideOffline -
State Active -Requester Maintenance
```

2. Чтобы разрешить серверу принимать вызовы единой системы обмена сообщениями (только в Exchange 2016), выполните следующую команду:

```
PowerShell

Set-ServerComponentState <ServerName> -Component UMCallRouter -State
Active -Requester Maintenance
```

3. Чтобы получить доступ к сценариям обслуживания DAG, выполните следующую команду:

```
PowerShell

CD $ExScripts
```

4. Чтобы выполнить скрипт StopDagServerMaintenance.ps1, выполните следующую команду:

```
PowerShell

.\StopDagServerMaintenance.ps1 -serverName <ServerName>
```

5. Чтобы разрешить очереди транспорта возобновить прием и обработку сообщений, выполните следующую команду:

```
PowerShell

Set-ServerComponentState <ServerName> -Component HubTransport -State
Active -Requester Maintenance
```

6. Чтобы возобновить работу транспорта, выполните следующую команду:

```
PowerShell

Restart-Service MSExchangeTransport
```

Чтобы убедиться, что сервер готов к использованию в производственной среде, выполните следующие действия.

1. Чтобы проверить, не работает ли сервер в режиме обслуживания, выполните команду

```
PowerShell

Get-ServerComponentState <ServerName> | Format-Table Component,State -
Autosize
```

Если вы устанавливаете обновление Exchange и процесс обновления завершается сбоем, некоторые серверные компоненты могут остаться в неактивном состоянии, которое будет отображаться в выходных данных приведенного выше `Get-ServerComponentState` командлета. Чтобы устранить эту проблему, выполните следующие команды:

1. `Set-ServerComponentState <ServerName> -Component ServerWideOffline -State Active -Requester Functional`
2. `Set-ServerComponentState <ServerName> -Component Monitoring -State Active -Requester Functional`
3. `Set-ServerComponentState <ServerName> -Component RecoveryActionsEnabled -State Active -Requester Functional`

Завершение работы участников группы обеспечения доступности базы данных

Решение для обеспечения высокого уровня доступности Exchange интегрировано с процессом завершения работы Windows. Если администратор или приложение инициирует завершение работы сервера Windows в группе DAG, к которому подключена база данных, реплицированная на один или несколько серверов группы DAG, система попытается активировать другую копию подключенной базы данных до того, как разрешить завершение работы.

Однако это новое поведение не гарантирует активацию всех баз данных на сервере `lossless` , на которых выполняется завершение работы. Поэтому перед завершением работы сервера, который является участником группы DAG, лучше выполнить его переключение.

Установка обновлений на членах группы DAG

Установка обновлений Exchange на сервере, который является членом DAG, является относительно простым процессом. При установке накопительного пакета обновления на сервере, который является членом группы DAG, выполняется остановка нескольких служб, в том числе всех служб Exchange и службы кластеров. Общий процесс применения обновлений для участника группы DAG выглядит следующим образом.

1. С помощью шагов, указанных выше, переведите члена группы DAG в режим обслуживания.
2. Установите обновление.
3. С помощью шагов, указанных выше, выведите члена группы DAG из режима обслуживания и верните его в рабочий режим.
4. Как вариант, можно с помощью сценария RedistributeActiveDatabases.ps1 выполнить балансировку активных копий баз данных в группе DAG.

Дополнительные сведения о последних обновлениях Exchange см. в разделе Exchange Server номера сборки и даты выпуска.

Создание группы доступности базы данных в Exchange Server

Статья • 04.04.2023

Группа доступности базы данных (DAG) — это набор из 16 Microsoft Exchange Server серверов почтовых ящиков, которые обеспечивают автоматическое восстановление на уровне базы данных из базы данных, сервера или сетевого сбоя. Если почтовый сервер добавлен в группу доступности базы данных, он вместе с другими серверами в группе доступности базы данных обеспечивает автоматическое восстановление на уровне базы данных после ошибок базы данных, сервера или сети.

> ⓘ **Важно!**
>
> На всех серверах в группе обеспечения доступности баз данных должна быть установлена одна и та же версия Exchange. Вы не можете смешивать серверы Exchange 2013 и серверы Exchange в одной группе daG.

Сведения о других задачах управления, связанных с группами доступности базы данных, см. См. раздел Управление группами доступности баз данных.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 1 минута.
- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Группы доступности баз данных" в разделе Разрешения высокой доступности и устойчивости сайта .
- При создании группы обеспечения доступности баз данных с серверов почтовых ящиков, работающих под управлением Windows Server 2012, необходимо подготовить объект имени кластера (CNO) для группы доступности базы данных, прежде чем добавлять участников. Если вы создаете DAG без административной точки доступа с серверами почтовых

ящиков, работающими Windows Server 2012 R2, вам не нужно предварительно создавать CNO для daG. Подробные инструкции см. в разделе Подготовка объекта имени кластера для группы доступности базы данных.

- При создании группы доступности базы данных необходимо указать ее уникальное имя, состоящее из не более 15 символов. Помимо указания имени daG, необходимо также назначить один или несколько IP-адресов (IPv4 или IPv4 и IPv6) daG, если вы не создаете Windows Server 2012 R2 DAG без административной точки доступа и не назначаете никакие IP-адреса daG. В противном случае назначаемые IP-адреса на уровне каждой подсети должны быть предназначены для сети MAPI и быть доступны для использования. Если вы указываете один или несколько IPv4-адресов, а система настроена на использование протокола IPv6, будет предпринята попытка автоматически назначить для группы обеспечения доступности баз данных один или несколько IPv6-адресов.

- При создании DAG необходимо указать следящий сервер и следящий каталог. Рекомендуется использовать сервер Exchange Server со службами клиентского доступа. Это дает возможность администратору Exchange располагать сведениями о доступности слежения, а также обеспечить наличие всех разрешений безопасности, необходимых для использования следящего сервера.

  Доступны следующие сочетания параметров и вариантов поведения:

  - Пользователь может указать имя для группы доступности базы данных, для используемого следящего сервера, а также для каталога, созданного и открытого для совместного доступа на следящем сервере.

  - Можно указать имя для группы обеспечения доступности баз данных и используемого следящего сервера, а поле **Следящий каталог** оставить пустым. В этом сценарии система создаст на указанном следящем сервере следящий каталог по умолчанию.

    Примечание. Если указанный сервер-следящий сервер не является сервером Exchange в вашей организации, необходимо добавить универсальную группу безопасности доверенной подсистемы Exchange в локальную группу администраторов на следяном сервере. Эти разрешения безопасности необходимы для создания каталога и файлового ресурса на следящем сервере в приложении Exchange. Если эти разрешения не настроены, будет возвращена следующая ошибка.

```
Error: An error occurred during discovery of the database availability group topology. Error: An error occurred while attempting a cluster operation. Error: Cluster API "AddClusterNode() (MaxPercentage=12) failed with 0x80070005. Error: Access is denied."
```

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование Центра администрирования Exchange для создания группы обеспечения доступности баз данных

1. В EAC выберите **Серверы**>**Группы доступности базы данных**.
2. Щелкните ➕ чтобы создать DAG.
3. На странице **Создание группы обеспечения доступности баз данных** укажите приведенные ниже сведения о группе обеспечения доступности базы данных.

   - **Имя группы доступности базы данных**. Используйте это поле, чтобы ввести допустимое и уникальное имя для daG не более 15 символов. Имя эквивалентно имени компьютера, и соответствующий CNO будет создан в Active Directory с этим именем. Этим именем будет называться как группа обеспечения доступности базы данных, так и базовый кластер.

   - **Следящий сервер**. Используйте это поле, чтобы указать следящий сервер для DAG.

     Примечание. Необходимо использовать имя узла или полное доменное имя (FQDN) для следящего сервера. Использование IP-адреса или подстановочного имени не поддерживается. Кроме того, следящий сервер не может входить в группу обеспечения доступности баз данных.

   - **Каталог следящего** сервера. Используйте это поле, чтобы ввести путь к каталогу на следящее сервере, которое будет использоваться для

хранения данных следящего сервера. Если каталог не существует, он будет создан системой на следящем сервере. Если оставить это поле пустым, каталог по умолчанию (%SystemDrive%\DAGFileShareWitnesses\<DAG FQDN>) будет создан на сервере-следитее.

- **IP-адреса группы доступности базы данных**. Используйте это поле для назначения одного или нескольких статических IPv4-адресов группе daG. Введите IPv4-адрес и нажмите ➕ чтобы добавить его. Если необходимо, чтобы группа обеспечения доступности баз данных использовала протокол DHCP для получения необходимых IPv4-адресов, оставьте это поле пустым. Кроме того, введите значение 255.255.255.255, чтобы создать группу обеспечения доступности баз данных без IP-адреса или административной точки доступа кластера, которое применяется только к группам обеспечения, предназначенным для серверов почтовых ящиков под управлением Windows Server 2012 R2.

4. Нажмите кнопку **Сохранить**, чтобы создать группу обеспечения доступности баз данных.

Создание группы доступности базы данных с помощью командной консоли Exchange

В следующем примере создается daG с именем DAG1, который настроен для использования следящего сервера FILESRV1 и локального каталога C:\DAG1. DAG1 также использует протокол DHCP для IP-адресов группы.

PowerShell

```
New-DatabaseAvailabilityGroup -Name DAG1 -WitnessServer FILESRV1 -
WitnessDirectory C:\DAG1
```

В этом примере создается группа обеспечения доступности баз данных DAG3. В группе DAG3 используется следящий сервер MBX2 и локальный каталог C:\DAG3. Группе DAG3 присвоено несколько статических IP-адресов, так как участники группы обеспечения доступности баз данных используют различные подсети сети MAPI.

PowerShell

```
New-DatabaseAvailabilityGroup -Name DAG3 -WitnessServer MBX2 -
WitnessDirectory C:\DAG3 -DatabaseAvailabilityGroupIPAddresses
10.0.0.8,192.168.0.8
```

В этом примере создается группа обеспечения доступности баз данных с именем DAG5 без административной точки доступа (доступно только в группах обеспечения доступности баз данных с Windows Server 2012 R2). Кроме того, для группы обеспечения доступности баз данных в качестве следящего сервера будет использован сервер клиентского доступа MBX4; также будет создан следящий каталог по умолчанию.

PowerShell

```
New-DatabaseAvailabilityGroup -Name DAG5 -
DatabaseAvailabilityGroupIPAddresses ([System.Net.IPAddress]::None) -
WitnessServer MBX4
```

Как проверить, что все получилось?

Чтобы убедиться, что группа обеспечения доступности баз данных создана успешно, выполните одно из приведенных ниже действий.

- В EAC перейдите в раздел **Серверы**>**Группы доступности базы данных**. Отобразится новая группа обеспечения доступности баз данных.
- В командной консоли Exchange выполните следующую команду, чтобы проверить создание DAG и отобразить сведения о свойствах DAG.

  PowerShell

  ```
  Get-DatabaseAvailabilityGroup <DAGName> | Format-List
  ```

Дополнительные сведения

Группы обеспечения доступности баз данных

Настройка свойств группы обеспечения доступности баз данных

Set-DatabaseAvailabilityGroup

New-DatabaseAvailabilityGroup

New-DatabaseAvailabilityGroupNetwork

Add-DatabaseAvailabilityGroupServer

Подготовка объекта имени кластера для группы доступности базы данных в Exchange Server

Статья • 04.04.2023

В средах, где создание учетной записи компьютера ограничено или учетные записи компьютеров создаются в контейнере, отличном от контейнера компьютеров по умолчанию, можно предварительно подготовить объект имени кластера (CNO), а затем подготовить CNO, назначив ему разрешения.

Регистрация CNO также требуется для членов группы обеспечения доступности баз данных Windows Server 2012 и Windows Server 2012 R2 из-за изменений, внесенных в разрешения для объектов компьютеров в Windows. При развертывании группы доступности базы данных (DAG) с помощью серверов почтовых ящиков, работающих под управлением Windows Server 2012 или Windows Server 2012 R2, необходимо подготовить CNO, если только вы не развертываете DAG без точки доступа администрирования кластера. В группах обеспечения доступности баз данных без административных точек доступа кластера не используются объекты CNO, поэтому эти группы не нужно регистрировать.

Пользователь создает и отключает учетную запись компьютера для объекта CNO, а затем выполняет одно из указанных ниже действий.

- Назначить разрешения на полный доступ к учетной записи компьютера для учетной записи компьютера, являющегося первым сервером почтовых ящиков, добавляемым в группу обеспечения доступности баз данных.

  -Или-

- Назначить полный доступ учетной записи компьютера универсальной группе безопасности доверенной подсистемы Exchange.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 1 минута
- Необходимо использовать учетную запись, имеющую разрешения на создание объектов компьютеров в Active Directory.

- После выполнения следующих шагов дождитесь окончания репликации Active Directory. После репликации объекта можно добавить первый сервер в группу доступности баз данных.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Регистрация сетевого объекта кластера

1. Откройте пункт "Пользователи и компьютеры Active Directory".
2. Разверните узел леса.
3. Щелкните правой кнопкой мыши подразделение, в котором необходимо создать новую учетную запись, выберите команду **Создать**, а затем щелкните **Компьютер**.
4. В окне **Новый объект — Компьютер** в поле **Имя компьютера** введите имя учетной записи компьютера для сетевого объекта кластера. Это имя, которое будет использоваться для группы обеспечения доступности баз данных. Нажмите кнопку **ОК**, чтобы создать учетную запись.
5. Щелкните правой кнопкой мыши новую учетную запись компьютера и выберите команду **Отключить учетную запись**. Нажмите кнопку **Да**, чтобы подтвердить отключение, затем нажмите кнопку **ОК**.

Назначение разрешений сетевому объекту кластера

1. Откройте пункт "Пользователи и компьютеры Active Directory".
2. Если "Дополнительные параметры" отключены, включите их. Для этого откройте меню **Вид**, затем выберите пункт **Дополнительные параметры**.
3. Щелкните правой кнопкой мыши новую учетную запись компьютера и выберите **Свойства**.

4. В окне **<Имя компьютера>: свойства** на вкладке **Безопасность** нажмите кнопку **Добавить**, чтобы добавить учетную запись компьютера для первого узла, добавляемого в группу доступности баз данных, или универсальную группу безопасности доверенной подсистемы Exchange.

    - Чтобы добавить доверенную подсистему Exchange, введите Exchange Trusted Subsystem в поле **Введите имена выбираемых объектов**. Нажмите кнопку **ОК**, чтобы добавить универсальную группу безопасности. Выберите универсальную группу безопасности доверенной подсистемы Exchange и в поле **Разрешения для доверенной подсистемы Exchange**, в столбце **Разрешить**, установите флажок **Полный доступ**. Нажмите кнопку **ОК**, чтобы сохранить параметры разрешений.

    - Чтобы добавить учетную запись компьютера для первого узла, добавляемого в группу доступности баз данных, щелкните **Типы объектов**. В диалоговом окне **Типы объектов** снимите флажки **Встроенные участники безопасности**, **Группы** и **Пользователи**. Установите флажок **Компьютеры** и нажмите кнопку **ОК**. В поле **Введите имена выбираемых объектов** введите имя первого сервера почтовых ящиков, добавляемого в группу доступности баз данных, и нажмите кнопку **ОК**. Выберите учетную запись компьютера первого узла и в поле **Разрешения для <Имя_узла>**, в столбце **Разрешить**, установите флажок **Полный доступ**. Нажмите кнопку **ОК**, чтобы сохранить параметры разрешений.

Как проверить, что все получилось?

Чтобы проверить, успешно ли создан объект имени кластера (CNO):

1. Откройте пункт "Пользователи и компьютеры Active Directory".

2. Разверните узел леса.

3. Откройте подразделение, в котором создана учетная запись, и убедитесь в ее наличии в списке.

Exchange Server. Использование виртуальной машины Microsoft Azure в качестве сервера-свидетеля DAG

Статья • 04.04.2023

Для реализации этой конфигурации требуются три отдельных физических местоположения: два для размещения центров обработки данных для серверов почтовых ящиков и одно для размещения следящего сервера для группы DAG. Организации, у которых имеется только два физических местоположения, также могут воспользоваться преимуществами автоматической отработки отказа центра обработки данных благодаря использованию виртуальной машины с файловым сервером Microsoft Azure в качестве следящего сервера группы DAG. В этой статье рассматривается размещение свидетеля DAG в Microsoft Azure и предполагается, что вы знакомы с концепциями устойчивости сайта и уже имеете полностью функциональную инфраструктуру DAG, охватывающую два центра обработки данных. Если вы еще настроили инфраструктуру группы обеспечения доступности баз данных, рекомендуем сначала ознакомиться с указанными ниже статьями.

Высокая доступность и устойчивость сайтов

Группы обеспечения доступности баз данных

Планирование высокого уровня доступности и устойчивости сайта

Изменения в Microsoft Azure

Для этой конфигурации требуется VPN с несколькими сайтами. Всегда можно было подключить сеть вашей организации к Microsoft Azure с помощью VPN-подключения типа "сеть — сеть". Однако в прошлом Azure поддерживала только один VPN-подключение типа "сеть — сеть". Так как для настройки DAG и его следящего сервера в трех центрах обработки данных требовалось несколько vpn-подключений типа "сеть — сеть", размещение свидетеля DAG на виртуальной машине Azure изначально было невозможно.

В июне 2014 г. в Microsoft Azure была реализована поддержка многосайтовой сети VPN, благодаря чему организации получили возможность подключить несколько центров обработки данных к одной и той же виртуальной сети Azure. Это изменение также позволило организациям с двумя центрами обработки данных использовать Microsoft Azure в качестве третьего расположения для размещения

серверов-свидетелей DAG. Дополнительные сведения о функции VPN с несколькими сайтами в Azure см. в статье Настройка многосайтового VPN.

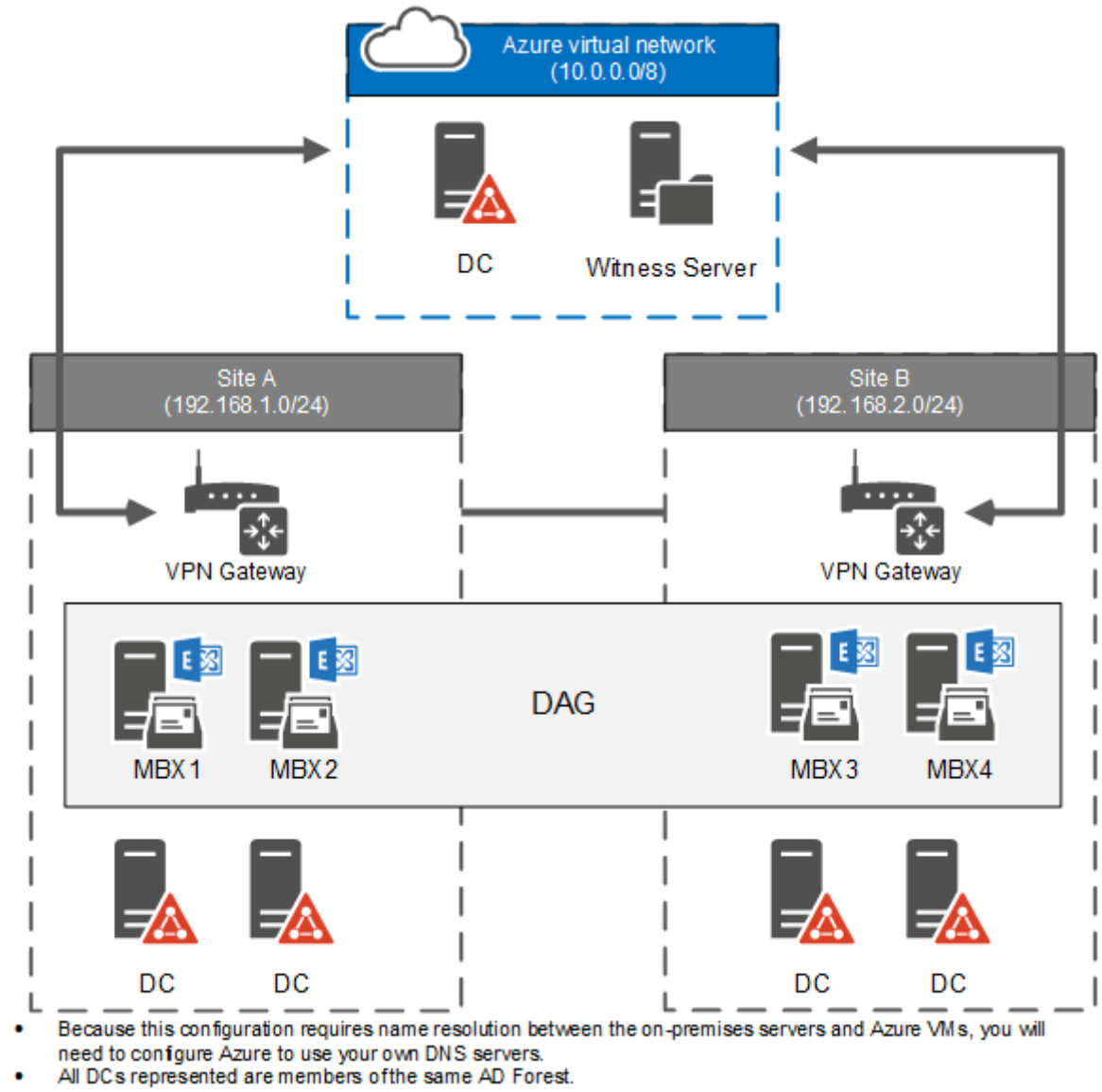
> ⓘ **Примечание**
>
> В данной конфигурации используются виртуальные машины Azure и многосайтовая сеть VPN для развертывания следящего сервера; облачный следящий сервер Azure не используется.

Следящий файловый сервер Microsoft Azure

Ниже приведен обзор использования виртуальной машины с файловым сервером Microsoft Azure в качестве следящего сервера DAG. Потребуются виртуальная сеть Azure, многосайтовая сеть VPN, объединяющая центры обработки данных с виртуальной сетью Azure, а также контроллер домена и файловый сервер, развернутые на виртуальных машинах Azure.

> ⓘ **Примечание**
>
> Существует техническая возможность использовать для этой цели лишь одну виртуальную машину Azure, а файловый ресурс-свидетель разместить на контроллере домена. Однако это приведет к ненужному повышению прав. Поэтому такая конфигурация не рекомендуется.

Следящий сервер DAG в Microsoft Azure



Первое, что нужно сделать для использования виртуальной машины Microsoft Azure для размещения следящего сервера DAG, это оформить подписку. Сведения о том, как приобрести подписку Azure, см. в статье Как приобрести Azure .

После приобретения подписки Azure необходимо выполнить указанные ниже действия.

1. Подготовьте виртуальную сеть Microsoft Azure
2. Настройте многосайтовую сеть VPN
3. Настройте виртуальные машины
4. Настройте следящий сервер DAG

> ⓘ **Примечание**
>
> Значительная часть инструкции в этой статье подразумевает использование конфигурации Microsoft Azure. Поэтому при необходимости мы будем

ссылаться на документацию Azure.

Предварительные требования

- Два центра обработки данных, которые поддерживают развертывание с высоким уровнем доступности Exchange и устойчивостью сайта. Дополнительные сведения см. в статье Планирование высокого уровня доступности и устойчивости сайта .
- Общедоступный IP-адрес, который не находится за NAT для VPN-шлюзов на каждом сайте.
- VPN-устройство на каждом сайте, совместимое с Microsoft Azure. Дополнительные сведения о совместимых устройствах см. в разделе Сведения о VPN-устройствах для виртуальная сеть.
- Знакомство с концепциями DAG и управлением.
- Знакомство с Windows PowerShell.

Этап 1. Подготовка виртуальной сети Microsoft Azure

Настройка сети Microsoft Azure является самой важной частью процесса развертывания. После завершения этого этапа у вас будет готовая полнофункциональная виртуальная сеть Azure, подключенная к двум центрам обработки данных через многосайтовую сеть VPN.

Регистрация DNS-серверов

Поскольку для данной конфигурации требуется разрешение имен между локальными серверами и виртуальными машинами Azure, необходимо настроить Azure для использования DNS-серверов. В статье Разрешение имен для ресурсов в виртуальных сетях Azure приводится обзор разрешения имен в Azure.

Выполните указанные ниже действия для регистрации DNS-серверов.

1. На портале Azure перейдите в раздел **сети**, а затем нажмите кнопку **СОЗДАТЬ**.
2. Щелкните **СЕТЕВЫЕ СЛУЖБЫ**>**ВИРТУАЛЬНАЯ СЕТЬ**>**ЗАРЕГИСТРИРОВАТЬ DNS-СЕРВЕР**.
3. Введите имя и IP-адрес DNS-сервера. Указанное здесь имя является логическим именем, используемым на портале управления и не обязательно

совпадает с фактическим именем DNS-сервера.

4. Повторите шаги 1-3 для других DNS-серверов, которые хотите добавить.

> ⓘ **Примечание**
>
> Зарегистрированные DNS-серверы не используются в режиме циклического перебора. Виртуальные машины Azure будут использовать первый DNS-сервер, указанный в списке, и будут использовать дополнительные серверы только в том случае, если первый сервер недоступен.

5. Повторите шаги 1-3, чтобы добавить IP-адрес, который будет использоваться для развертываемого в Microsoft Azure контроллера домена.

Создание объектов локальной сети в Azure

Затем следует выполнить указанные ниже действия, чтобы создать логические объекты сети, представляющие ваши центры обработки данных в Microsoft Azure.

1. На портале Azure перейдите в раздел **сети**, а затем нажмите кнопку **СОЗДАТЬ**.
2. Щелкните **СЕТЕВЫЕ СЛУЖБЫ**>**ВИРТУАЛЬНАЯ СЕТЬ**>**ДОБАВИТЬ ЛОКАЛЬНУЮ СЕТЬ**.
3. Введите имя первого сайта центра обработки данных и IP-адрес VPN-устройства на этом сайте. Этот IP-адрес должен быть статическим общим IP-адресом, который не находится за пределами NAT.
4. На следующем экране укажите IP-подсети для первого сайта.
5. Повторите шаги 1–4 для второго сайта.

Создание виртуальной сети Azure

Теперь выполните указанные ниже действия для создания виртуальной сети Azure, которая будет использоваться виртуальными машинами.

1. На портале Azure перейдите в раздел **сети**, а затем нажмите кнопку **СОЗДАТЬ**.
2. Щелкните **NETWORK SERVICES**> VIRTUAL NETWORK**CUSTOM CREATE (СОЗДАТЬ ПОЛЬЗОВАТЕЛЬСКУЮВИРТУАЛЬНУЮ СЕТЬ**> СЛУЖБ СЕТИ).

3. На странице **Сведения о виртуальной сети** укажите имя виртуальной сети и выберите географическое расположение сети.
4. На странице **DNS-серверы и подключение VPN** убедитесь, что зарегистрированные ранее DNS-серверы перечислены как DNS-серверы.
5. В разделе **ПОДКЛЮЧЕНИЕ ТИПА "СЕТЬ-СЕТЬ"** установите флажок **Настроить подключение VPN типа "сеть-сеть"**.

   > ⓘ **Важно!**
   >
   > Не устанавливайте флажок **Использование ExpressRoute**, поскольку в этом случае в конфигурацию не удастся внести изменения, необходимые для настройки многосайтовой сети VPN.

6. В разделе **ЛОКАЛЬНАЯ СЕТЬ** выберите одну из двух настроенных локальных сетей.
7. На странице **Адресное пространство виртуальной сети** укажите диапазон IP-адресов, которые вы будете использовать для виртуальной сети Azure.

Контрольная точка: проверка конфигурации сети

На этом этапе в разделе **сети** должны отобразиться виртуальная сеть, настроенная в разделе **ВИРТУАЛЬНЫЕ СЕТИ**, локальные сайты в разделе **ЛОКАЛЬНЫЕ СЕТИ** и зарегистрированные DNS-серверы в разделе **DNS-СЕРВЕРЫ**.

Этап 2. Настройка многосайтовой сети VPN

Следующим шагом является установка VPN-шлюзов для локальных сайтов. Для этого необходимо выполнить указанные ниже действия.

1. Установите VPN-шлюз для одного из сайтов с помощью портала Azure.
2. Экспортируйте параметры конфигурации виртуальной сети.
3. Измените файл конфигурации для многосайтовой сети VPN.
4. Импортируйте обновленную конфигурацию сети Azure.
5. Запишите IP-адрес шлюза Azure и предварительные ключи.
6. Настройте локальные VPN-устройства.

Дополнительные сведения о настройке многосайтовой сети VPN в Azure см. в статье Настройка многосайтовой сети VPN.

Установка VPN-шлюза для своего первого сайта

При создании виртуального шлюза обратите внимание, что вы уже указали, что он будет подключен к первому локальному сайту. При переходе в панель мониторинга виртуальной сети вы увидите, что шлюз еще не создан.

Сведения о том, как установить VPN-шлюз на стороне Azure, см. в разделе VPN-шлюз.

> **Важно!**
>
> Выполните только действия, указанные в разделе "Запустите шлюз виртуальной сети" этой статьи; сведения, содержащиеся в последующих разделах, не понадобятся.

Экспорт параметров конфигурации виртуальной сети

В настоящее время на портале управления Azure отсутствует возможность настроить многосайтовую сеть VPN. Для этой конфигурации необходимо экспортировать параметры конфигурации виртуальной сети в XML-файл, а затем изменить этот файл. Следуйте инструкциям в статье Экспорт параметров виртуальной сети в файл конфигурации сети для экспорта параметров.

Изменение параметров конфигурации сети для многосайтовой сети VPN

Откройте экспортированный файл в любом редакторе XML. Подключения шлюза к локальным сайтам перечислены в разделе "ConnectionsToLocalNetwork". Найдите этот раздел в XML-файле. Этот раздел файла конфигурации будет выглядеть следующим образом (предполагается, что локальному сайту присвоено имя "Site A"):

XML

```
<ConnectionsToLocalNetwork>
    <LocalNetworkSiteRef name="Site A">
        <Connection type="IPsec" />
</LocalNetworkSiteRef>
```

Чтобы настроить второй сайт, добавьте в раздел "ConnectionsToLocalNetwork" другой раздел "LocalNetworkSiteRef". Этот раздел в обновленном файле конфигурации будет выглядеть следующим образом (предполагается, что второму локальному сайту присвоено имя "Site B"):

XML

```
<ConnectionsToLocalNetwork>
    <LocalNetworkSiteRef name="Site A">
        <Connection type="IPsec" />
    <LocalNetworkSiteRef name="Site B">
        <Connection type="IPsec" />
</LocalNetworkSiteRef>
```

Сохраните обновленный файл параметров конфигурации.

Импорт параметров конфигурации виртуальной сети

Ссылка на второй сайт, которую вы добавили в файл конфигурации, запускает создание нового туннеля в Microsoft Azure. Импортируйте обновленный файл с помощью инструкций из раздела Создание виртуальной сети (классической) с помощью портал Azure. По завершении импорта на панели мониторинга виртуальной сети отобразятся подключения шлюза для обоих локальных сайтов.

Сохранение сведений об IP-адресе шлюза Azure и предварительных ключах

После импорта новых параметров конфигурации сети на панели мониторинга виртуальной сети отобразится IP-адрес шлюза Azure. Это IP-адрес, к которому будут подключаться VPN-устройства на обоих сайтах. Запишите этот IP-адрес для использования в будущем.

Также потребуется получить предварительные ключи IPsec/IKE для каждого созданного туннеля. Эти ключи и IP-адрес шлюза Azure потребуются для настройки локальных VPN-устройств.

Для получения предварительных ключей необходимо использовать PowerShell. Если вы не знакомы с порядком использования PowerShell для управления Azure, обратитесь к статье Справка по Azure PowerShell.

Используйте командлет Get-AzureVNetGatewayKey для извлечения предварительных ключей. Запустите этот командлет один раз для каждого туннеля. В следующем примере показаны команды, необходимые для извлечения ключей

для туннелей между виртуальной сетью "Сайт Azure" и сайтами "Сайт A" и "Сайт B". В этом примере выходные данные сохраняются в отдельных файлах. Кроме того, можно направить эти ключи в другие командлеты PowerShell или использовать их в сценарии.

PowerShell

```
Get-AzureVNETGatewayKey -VNetName "Azure Site" -LocalNetworkSiteName "Site
A" | Set-Content -Path C:\Keys\KeysForTunnelToSiteA.txt
Get-AzureVNETGatewayKey -VNetName "Azure Site" -LocalNetworkSiteName "Site
B" | Set-Content -Path C:\Keys\KeysForTunnelToSiteB.txt
```

Настройка локальных VPN-устройств

Microsoft Azure предоставляет сценарии настройки для поддерживаемых VPN-устройств. Щелкните ссылку **Загрузить скрипт VPN-устройства** на панели мониторинга виртуальной сети для загрузки соответствующего сценария для своих VPN-устройств.

Скачиваемые скрипты будут иметь параметр конфигурации для первого сайта, настроенного при настройке виртуальной сети, и его можно использовать как есть для настройки VPN-устройства для этого сайта. Например, если вы указали сайт A в качестве **локальной сети** при создании виртуальной сети, скрипт VPN-устройства можно использовать для сайта A. Однако вам потребуется изменить его, чтобы настроить VPN-устройство для сайта B. В частности, необходимо обновить общий ключ в соответствии с ключом для второго сайта.

Например, если вы используете VPN-устройство службы маршрутизации и удаленного доступа (RRAS) для своих сайтов, вам потребуется:

1. Откройте сценарий настройки в любом текстовом редакторе.
2. `#Add S2S VPN interface` Найдите раздел .
3. В этом разделе найдите команду **Add-VpnS2SInterface**. Убедитесь, что значение параметра *SharedSecret* соответствует предварительно общему ключу для сайта, для которого настраивается VPN-устройство.

Для других устройств могут потребоваться дополнительные проверки. Например, сценарии настройки для устройств Cisco устанавливают правила списка управления доступом с помощью диапазонов локальных IP-адресов. Прежде чем использовать сценарий настройки, необходимо просмотреть и проверить в нем все ссылки на локальный сайт.

Контрольная точка: проверка состояния VPN

На этом этапе оба сайта подключены к виртуальной сети Azure через VPN-шлюзы. Вы можете проверить состояние многосайтовой сети VPN, выполнив следующую команду в PowerShell.

PowerShell

```
Get-AzureVnetConnection -VNetName "Azure Site" | Format-Table
LocalNetworkSiteName, ConnectivityState
```

Если оба туннеля работают, выходные данные этой команды будут выглядеть следующим образом:

Консоль

```
LocalNetworkSiteName    ConnectivityState
--------------------    -----------------
Site A                  Connected
Site B                  Connected
```

Можно также проверить подключение, обратившись к панели мониторинга виртуальной сети на портале управления Azure. В столбце **СОСТОЯНИЕ** для обоих сайтов будет отображаться значение **Подключено**.

> **Примечание**
>
> После успешного установления подключения может потребоваться несколько минут, чтобы изменения о состоянии подключения отразились на портале управления Azure.

Этап 3. Настройка виртуальных машин

Для этого развертывания необходимо создать как минимум две виртуальные машины в Microsoft Azure: контроллер домена и файловый сервер, который будет использоваться в качестве следящего сервера DAG.

1. Создайте виртуальные машины для контроллера домена и файлового сервера в соответствии с инструкциями в статье Создание виртуальной машины под управлением Windows. При указании параметров виртуальных машин убедитесь, что выбрана виртуальная сеть, которую вы создали для параметра **РЕГИОН, ТЕРРИТОРИАЛЬНАЯ ГРУППА, ВИРТУАЛЬНАЯ СЕТЬ**.

2. С помощью Azure PowerShell укажите предпочтительные IP-адреса для контроллера домена и файлового сервера. При указании предпочтительного IP-адреса для виртуальной машины его необходимо обновить, для чего потребуется перезапустить виртуальную машину. В примере ниже задаются IP-адреса для контроллера домена Azure-DC и файлового сервера Azure FSW, 10.0.0.10 и 10.0.0.11 соответственно.

```
PowerShell

Get-AzureVM Azure-DC | Set-AzureStaticVNetIP -IPAddress 10.0.0.10 |
Update-AzureVM
```

```
PowerShell

Get-AzureVM Azure-FSW | Set-AzureStaticVNetIP -IPAddress 10.0.0.11 |
Update-AzureVM
```

> ⓘ **Примечание**
>
> Виртуальная машина с предпочтительным IP-адресом будет пытаться использовать этот адрес. Тем не менее, если этот адрес был назначен другой виртуальной машине, виртуальная машина с предпочтительным IP-адресом не запустится. Чтобы избежать подобных ситуаций, убедитесь, что используемый IP-адрес не назначен другой виртуальной машине.

3. Подготовьте контроллер домена виртуальной машины в Azure в соответствии с используемыми в вашей организации стандартами.

4. Подготовьте необходимые компоненты для следящего сервера DAG Exchange.

   a. Добавьте роль файлового сервера с помощью мастера добавления ролей и компонентов или командлета Install-WindowsFeature .

   b. Добавьте универсальную группу безопасности доверенной подсистемы Exchange в группу локальных администраторов.

Контрольная точка: просмотр состояния виртуальной машины

На этом этапе виртуальные машины должны быть настроены и работать, а также должны иметь возможность обращаться к серверам в обоих локальных центрах обработки данных.

- Убедитесь, что контроллер домена в Azure выполняет репликацию с локальных контроллеров домена.
- Убедитесь, что к файловому серверу Azure можно обратиться по имени и установить с ним подключение по протоколу SMB с серверов Exchange.
- Убедитесь, что к вашим серверам Exchange можно обратиться по имени с файлового сервера в Azure.

Этап 4. Настройка следящего сервера DAG

Наконец, необходимо настроить вашу DAG для использования нового следящего сервера. По умолчанию Exchange использует C:\DAGFileShareWitnesses как путь файловому ресурсу-свидетелю на следящем сервере. Если вы используете пользовательский путь к файлу, следует также обновить следящий каталог для конкретной общей папки.

1. Подключитесь к Командная консоль Exchange.
2. Выполните следующую команду для настройки следящего сервера для своих групп обеспечения доступности базы данных.

```
PowerShell

Set-DatabaseAvailabilityGroup -Identity DAG1 -WitnessServer Azure-FSW
```

Дополнительные сведения см. в следующих статьях:

Настройка свойств группы обеспечения доступности баз данных

Set-DatabaseAvailabilityGroup

Контрольная точка: проверка файлового ресурса свидетеля DAG

На этом этапе вы уже настроили DAG для использования файлового сервера в Azure в качестве своего следящего сервера DAG. Выполните указанные ниже действия, чтобы проверить конфигурацию.

1. Проверьте конфигурацию DAG, выполнив следующую команду:

```
PowerShell
```

```
Get-DatabaseAvailabilityGroup -Identity DAG1 -Status | Format-List
Name, WitnessServer, WitnessDirectory, WitnessShareInUse
```

Убедитесь, что для параметра *WitnessServer* задан файловый сервер в Azure, *параметру WitnessDirectory* задан правильный путь, а *параметру WitnessShareInUse* — **значение Primary**.

2. Если dag содержит четное число узлов, то файловый ресурс-свидетель будет настроен. Проверьте параметр следящего ресурса в свойствах кластера, выполнив следующую команду. Значение параметра *SharePath* должно указывать на файловый сервер и отображать правильный путь.

```
PowerShell
Get-ClusterResource -Cluster MBX1 | Get-ClusterParameter | Format-List
```

3. Затем проверьте состояние ресурса кластера "Файловый ресурс-свидетель", выполнив следующую команду. *Состояние* ресурса кластера должно отображаться **в сети**.

```
PowerShell
Get-ClusterResource -Cluster MBX1
```

4. Затем убедитесь, что общий ресурс успешно создан на файловом сервере. Для этого перейдите к папке в проводнике и к общим папкам в диспетчере серверов.

Удаление группы доступности базы данных в Microsoft Exchange

Статья • 04.04.2023

Удаление DAG является быстрой и простой задачей. Для удаления DAG можно использовать EAC или командную консоль Exchange.

Сведения о других задачах управления, связанных с группами доступности базы данных, см. См. раздел Управление группами доступности баз данных.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 1 минута.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Группы доступности баз данных" в разделе Разрешения высокой доступности и устойчивости сайта .
- Перед удалением DAG она должна быть пустой. Если daG, которую требуется удалить, содержит какие-либо серверы почтовых ящиков, сначала необходимо удалить серверы из daG. Подробные инструкции по удалению сервера почтовых ящиков из DAG см. в разделе Управление членством в группе доступности базы данных.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование центра администрирования Exchange для удаления группы обеспечения доступности баз данных

1. Перейдите в раздел **Серверы**>**Группы доступности базы данных**.
2. Выберите dag, которую нужно удалить, и щелкните **удалить**🗑
3. Нажмите кнопку **Да**, чтобы подтвердить действие и удалить группу.

Удаление группы доступности базы данных с помощью командной консоли Exchange

В этом примере показано удаление группы обеспечения доступности баз данных с именем DAG1.

PowerShell

```
Remove-DatabaseAvailabilityGroup -Identity DAG1
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно удалили группу, выполните следующие действия.

- В EAC перейдите в раздел**Группы доступности базы данныхсерверов**> и посмотрите, отображается ли daG по-прежнему.
- В командной консоли Exchange выполните следующую команду, чтобы узнать, существует ли daG:

  PowerShell

  ```
  Get-DatabaseAvailabilityGroup <DAGName>
  ```

  Если группа успешно удалена, команда выше приведет к отображению сообщения об ошибке, которое указывает, что не удается найти объект.

Настройка autoReseed для группы доступности базы данных в Exchange Server

Статья • 04.04.2023

Выполните действия, описанные в этом разделе, чтобы настроить autoReseed для группы доступности базы данных (DAG) в Exchange Server.

> ⊗ **Внимание!**
>
> Функция AutoReseed не обеспечивает автоматическое выполнение всех необходимых задач настройки. Администратор должен вручную устанавливать диски, добавлять в систему свободные диски, заменять неисправные и форматировать новые диски.

Дополнительные задачи управления, связанные с daG, см. в разделе Управление группами доступности баз данных.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 10 минут.
- Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Группы доступности баз данных" в разделе Разрешения высокой доступности и устойчивости сайта .
- Необходимо использовать один логический диск или его раздел на физический диск.
- Следует использовать определенную базу данных и структуру папок журнала, описанные в приведенных ниже шагах.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Действие 1. Настройка корневых путей для баз данных и томов

На первом этапе необходимо настроить корневые каталоги для баз данных (*AutoDagDatabasesRootFolderPath*) и томов (*AutoDagVolumesRootFolderPath*), используемых группой обеспечения доступности баз данных. Пути по умолчанию — C:\ExchangeDatabases и C:\ExchangeVolumes соответственно. Если используются пути по умолчанию, этот шаг можно пропустить.

В этом примере показано, как настроить корневой путь для баз данных.

PowerShell

```
Set-DatabaseAvailabilityGroup DAG1 -AutoDagDatabasesRootFolderPath
"C:\ExchDbs"
```

В этом примере показано, как настроить корневой путь для томов хранения.

PowerShell

```
Set-DatabaseAvailabilityGroup DAG1 -AutoDagVolumesRootFolderPath
"C:\ExchVols"
```

Как проверить, что шаг выполнен?

Чтобы проверить, успешно ли настроены корневые пути для баз данных и томов, выполните следующую команду.

PowerShell

```
Get-DatabaseAvailabilityGroup DAG1 | Format-List *auto*
```

Значения параметров *AutoDagDatabasesRootFolderPath* и *AutoDagVolumesRootFolderPath* должны соответствовать настроенным путям.

Действие 2. Настройка количества баз данных на том

Далее нужно настроить количество баз данных на том (*AutoDagDatabaseCopiesPerVolume*) для группы обеспечения доступности баз данных.

В этом примере показано, как настроить этот параметр автоматического повторного заполнения (AutoReseed) для группы обеспечения доступности баз данных, задав 4 базы данных на один том.

PowerShell

```
Set-DatabaseAvailabilityGroup DAG1 -AutoDagDatabaseCopiesPerVolume 4
```

Как проверить, что шаг выполнен?

Чтобы проверить, успешно ли настроено количество баз данных на том, выполните следующую команду.

PowerShell

```
Get-DatabaseAvailabilityGroup DAG1 | Format-List *auto*
```

Значение параметра *AutoDagDatabaseCopiesPerVolume* должно соответствовать заданному числу баз данных.

Действие 3. Создание корневых каталогов для баз данных и томов

Далее создайте каталоги, которые соответствуют корневым каталогам, настроенным в действии 1. В этом примере показано, как создать каталоги по умолчанию с помощью командной строки.

PowerShell

```
md C:\ExchangeDatabases
md C:\ExchangeVolumes
```

Как проверить, что шаг выполнен?

Чтобы проверить, успешно ли настроены корневые каталоги для баз данных и томов, выполните следующую команду.

```
PowerShell

Dir C:\
```

Созданные папки должны появиться в списке вывода.

Действие 4. Подключение томов к папкам

Для каждого тома, который будет использоваться для баз данных (включая запасные тома), используйте приложение управления дисками Windows (diskmgmt.msc), чтобы подключить каждый том в подключенной папке в папке C:\ExchangeVolumes. Например, если имеются 2 тома для размещения баз данных и 1 резервный том, подключите их к следующим папкам.

- C:\ExchangeVolumes\Volume1
- C:\ExchangeVolumes\Volume2
- C:\ExchangeVolumes\Volume3

Папкам, подключенным по пути корневого тома, можно присваивать любые имена.

Как убедиться, что все получилось?

Чтобы проверить, успешно ли подключены тома к папкам, выполните следующую команду.

```
PowerShell

Dir C:\
```

Должен быть выведен список подключенных томов.

Действие 5. Создание папок баз данных

Далее создайте каталоги баз данных в корневом пути C:\ExchangeDatabases. В этом примере показано, как создать каталоги для конфигурации хранилища с 4-мя базами данных в каждом томе.

PowerShell

```
md c:\ExchangeDatabases\db001
```

PowerShell

```
md c:\ExchangeDatabases\db002
```

PowerShell

```
md c:\ExchangeDatabases\db003
```

PowerShell

```
md c:\ExchangeDatabases\db004
```

Как проверить, что шаг выполнен?

Чтобы проверить, успешно ли подключены папки баз данных, выполните следующую команду.

PowerShell

```
Dir C:\ExchangeDatabases
```

Созданные папки должны появиться в списке вывода.

Действие 6. Создание точек подключения для баз данных

Создайте точки подключения для каждой базы данных и свяжите их с соответствующими томами. Например, подключенная папка для db001 должна находиться по пути C:\ExchangeDatabases\db001. Для этого можно воспользоваться программой diskmgmt.msc или mountvol.exe. В этом примере показано, как подключить базу данных db001 к C:\ExchangeDatabases\db001 с помощью программы mountvol.exe.

PowerShell

```
Mountvol.exe c:\ExchangeDatabases\db001 \\?\Volume (GUID)
```

Как проверить, что шаг выполнен?

Чтобы проверить, успешно ли созданы точки подключения для базы данных, выполните следующую команду.

PowerShell

```
Mountvol.exe C:\ExchangeDatabases\db001 /L
```

Подключенный том должен появиться в списке точек подключения.

Действие 7. Создание структуры каталогов баз данных

Далее создайте по два каталога в папках, созданных в действии 5, по одному для каждой базы данных и по одному для потока журнала каждой базы данных, который будет храниться на том же томе. Для вашей структуры каталогов необходимо использовать следующий формат.

C:\<*DatabaseFolderName*>\ *DatabaseName* \<*DatabaseName.db*>

C:\<*DatabaseFolderName*>\ *DatabaseName* \<*DatabaseName.log*>

В этом примере показано, как создать каталоги для 4 баз данных, которые будут храниться в томе 1.

PowerShell

```
md c:\ExchangeDatabases\db001\db001.db
```

PowerShell

```
md c:\ExchangeDatabases\db001\db001.log
```

PowerShell

```
md c:\ExchangeDatabases\db002\db002.db
```

PowerShell

```
md c:\ExchangeDatabases\db002\db002.log
```

PowerShell

```
md c:\ExchangeDatabases\db003\db003.db
```

PowerShell

```
md c:\ExchangeDatabases\db003\db003.log
```

PowerShell

```
md c:\ExchangeDatabases\db004\db004.db
```

PowerShell

```
md c:\ExchangeDatabases\db004\db004.log
```

Повторите указанные выше команды для баз данных в каждом томе.

Как проверить, что шаг выполнен?

Чтобы проверить, успешно ли создана структура каталогов баз данных, выполните следующую команду.

PowerShell

```
Dir C:\ExchangeDatabases /s
```

Созданные папки должны появиться в списке вывода.

Действие 8. Создание баз данных

Создайте базы данных с путями журналов и баз данных, для которых настроены соответствующие папки. В этом примере показано, как создать базу данных, которая будет храниться в новом каталоге и структуре точек подключения.

PowerShell

```
New-MailboxDatabase -Name db001 -Server MBX1 -LogFolderPath
C:\ExchangeDatabases\db001\db001.log -EdbFilePath
C:\ExchangeDatabases\db001\db001.db\db001.edb
```

Как проверить, что шаг выполнен?

Чтобы проверить, успешно ли созданы базы данных в соответствующей папке, выполните следующую команду.

```
PowerShell

Get-MailboxDatabase db001 | Format List *path*
```

В свойствах базы данных необходимо указать, что файл базы данных и ее файлы журнала хранятся в указанных выше папках.

Как проверить, что это работает?

Чтобы убедиться, правильно ли настроено автоматическое повторное заполнение для группы обеспечения доступности баз данных, выполните следующие действия.

1. Чтобы проверить, правильно ли настроена группа обеспечения доступности баз данных, выполните следующую команду.

   ```
   PowerShell

   Get-DatabaseAvailabilityGroup DAG1 | Format-List *auto*
   ```

2. Чтобы проверить, правильно ли настроена структура каталогов, выполните следующую команду (ниже указаны пути по умолчанию; при необходимости замените их на другие).

   ```
   PowerShell

   Dir c:\ExchangeDatabases /s
   ```

   ```
   PowerShell

   Dir c:\ExchangeVolumes /s
   ```

Настройка сетевых свойств группы доступности базы данных в Exchange Server

Статья • 04.04.2023

Настраиваемые свойства включают имя сети DAG, поле описания для сети DAG, список подсетей, используемых сетью DAG, а также возможность репликации сети DAG.

Сведения о других задачах управления, связанных с группами доступности базы данных, см. См. раздел Управление группами доступности баз данных.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 1 минута.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Группы доступности баз данных" в разделе Разрешения высокой доступности и устойчивости сайта .
- Вы можете настроить сеть DAG, только если для этой группы отключена автоматическая настройка сети. Подробные инструкции по отключению автоматической настройки сети для DAG см. в разделе Настройка свойств группы доступности базы данных.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование центра администрирования Exchange для настройки свойств сети группы

обеспечения доступности баз данных

1. В EAC выберите **Серверы**>**Группы доступности базы данных**.
2. Выберите daG, которую нужно настроить, и в области Сведения в разделе сети DAG, которую вы хотите настроить, выберите один из следующих параметров конфигурации.

   > ⓘ **Примечание**
   >
   > Эти параметры будут отображаться, только если вы выбрали **Настроить сети групп доступности базы данных вручную** на странице свойств DAG.

- **Отключить репликацию** или **Включить репликацию**. Настраивает параметры репликации для сети DAG.
- **Удалить**. Удаляет сеть DAG. Прежде чем удалять сеть DAG, необходимо сначала удалить из нее все связанные подсети.
- **Просмотр сведений**. Настраивает свойства сети DAG, такие как имя, описание и связанные подсети для сети DAG. Кроме того, вы можете просмотреть сетевые интерфейсы, связанные с этими подсетями, а также включить или отключить репликацию для сети DAG.

Настройка сетевых свойств группы доступности базы данных с помощью командной консоли Exchange

В этом примере в сеть MapiDagNetwork группы обеспечения доступности баз данных DAG1 добавляются подсеть 10.0.0.0 и маска подсети 255.0.0.0.

PowerShell

```
Set-DatabaseAvailabilityGroupNetwork -Subnets 10.0.0.0/8 -Identity
DAG1\MapiDagNetwork
```

Как проверить, что все получилось?

Чтобы проверить, успешно ли настроена сеть DAG, выполните указанные ниже действия.

- В командной консоли Exchange выполните следующую команду, чтобы отобразить параметры конфигурации сети DAG и убедиться, что сеть DAG настроена успешно.

```
PowerShell

Get-DatabaseAvailabilityGroupNetwork <DAGNetworkName> | Format-List
```

Дополнительные сведения

Set-DatabaseAvailabilityGroupNetwork

Get-DatabaseAvailabilityGroupNetwork

New-DatabaseAvailabilityGroupNetwork

Remove-DatabaseAvailabilityGroupNetwork

Создание сети группы доступности базы данных в Exchange Server

Статья • 04.04.2023

Для создания сети DAG можно использовать EAC или командную консоль Exchange.

Сведения о других задачах управления, связанных с группами доступности базы данных, см. См. раздел Управление группами доступности баз данных.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 1 минута.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Группы доступности баз данных" в разделе Разрешения высокой доступности и устойчивости сайта .
- Создать сеть DAG можно, только если отключена автоматическая настройка сети для группы DAG. Подробные инструкции по отключению автоматической настройки сети для DAG см. в разделе Настройка свойств группы доступности базы данных.
- При создании сети DAG необходимо назначить ей уникальные подсети, не используемые другими сетями DAG. При использовании подсетей, назначенных существующим сетям DAG, они удаляются из старой сети DAG и добавляются в новую.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование EAC для создания сети DAG

1. В EAC выберите **Серверы**>**Группы доступности базы данных**.
2. Выберите dag, которую нужно настроить, и нажмите кнопку
3. На странице **Новая сеть группы обеспечения доступности базы данных** введите следующую информацию:
   - **Имя сети группы доступности базы данных**. Используйте это поле, чтобы ввести имя сети, уникальной в DAG.
   - **Описание**. Используйте это поле для предоставления текстового описания сети DAG.
   - **Подсети**. Используйте это поле для связывания одной или нескольких подсетей с сетью DAG. Нажмите ➕ Чтобы добавить подсеть, щелкните , чтобы изменить подсеть, и щелкните минус (-), чтобы удалить подсеть.
4. Нажмите кнопку **Сохранить**, чтобы создать сеть DAG.

Создание сети группы доступности базы данных с помощью командной консоли Exchange

В этом примере создается сеть ReplicationDagNetwork02 с подсетью 10.0.0.0 и битовой маской 8 в группе DAG1. Для этой сети включена репликация, а также добавляется необязательное описание.

PowerShell

```
New-DatabaseAvailabilityGroupNetwork -DatabaseAvailabilityGroup DAG1 -Name
ReplicationDagNetwork02 -Description "Replication network 2" -Subnets
10.0.0.0/8 -ReplicationEnabled:$True
```

Как проверить, что все получилось?

Чтобы убедиться, что сеть DAG успешно создана, выполните одно из указанных ниже действий.

- В EAC перейдите в раздел **Серверы**>**Группы доступности базы данных**. Выберите соответствующую группу DAG, и новая сеть DAG будет отображаться в области сведений.

- В командной консоли Exchange выполните следующую команду, чтобы проверить создание сети DAG и отобразить сведения о конфигурации сети DAG.

```
PowerShell

Get-DatabaseAvailabilityGroupNetwork <DAGNetworkName> | Format-List
```

Дополнительные сведения

Set-DatabaseAvailabilityGroupNetwork

Get-DatabaseAvailabilityGroupNetwork

New-DatabaseAvailabilityGroupNetwork

Remove-DatabaseAvailabilityGroupNetwork

Управление членством в группе доступности базы данных в Exchange Server

Статья • 04.04.2023

Если сервер добавлен в группу обеспечения доступности баз данных, он вместе с другими членами этой группы обеспечивает автоматическое восстановление на уровне базы данных после ошибок базы данных, сервера или сети. При удалении сервера из группы обеспечения доступности баз данных с него снимается автоматическая защита от сбоев.

Сведения о других задачах управления, связанных с группами доступности базы данных, см. См. раздел Управление группами доступности баз данных.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут на сервер
- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Группы доступности базы данных используют технологии отказоустойчивого кластера Windows. Каждый сервер почтовых ящиков, являющийся членом такой группы обеспечения доступности баз данных, также является узлом базового кластера, используемого группой. Таким образом, сервер почтовых ящиков одновременно может быть членом только одной группы обеспечения доступности баз данных. Так как группы обеспечения доступности баз данных используют технологию WFC, на всех серверах, добавляемых в такую группу, должна быть установлена одинаковая операционная система: Windows Server 2008 R2 Enterprise или Datacenter Edition, Windows Server 2012 либо Windows Server 2012 R2 Standard или Datacenter Edition.
- Если добавляете серверы почтовых ящиков с Windows Server 2012, необходимо подготовить объект имени кластера для группы DAG. Если вы добавляете серверы почтовых ящиков под управлением Windows Server 2012 R2, а у группы доступности базы данных нет точки доступа с правами администратора, вам не нужно предварительно создавать CNO, так как группы доступности без административных точек доступа не имеют CNO.

Дополнительные сведения см. в разделе Pre-stage the cluster name object for a database availability group.

- Прежде чем добавлять участников группы обеспечения доступности баз данных, создайте ее. Дополнительные сведения см. в разделе Create a database availability group.
- Необходимо удалить все копии реплицированных баз данных с этого сервера, прежде чем удалить его из группы доступности базы данных.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Группы доступности баз данных" в разделе Разрешения высокой доступности и устойчивости сайта .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование Центра администрирования Exchange для управления членством в группе обеспечения доступности баз данных

1. В EAC выберите **Серверы**>**Группы доступности базы данных**.
2. Выберите dag, которую нужно настроить, и щелкните .
   - Чтобы добавить один или несколько серверов почтовых ящиков в DAG, щелкните ➕, выберите серверы из списка, нажмите кнопку **Добавить**, а затем нажмите **кнопку ОК**.
   - Чтобы удалить один или несколько серверов почтовых ящиков из группы обеспечения доступности баз данных, выберите серверы и щелкните значок "минус" (-).
3. Нажмите кнопку **Сохранить**, чтобы сохранить изменения.

4. После выполнения задания нажмите кнопку **Закрыть**.

Управление членством в группе доступности базы данных с помощью командной консоли Exchange

В данном примере показано добавление сервера почтовых ящиков MBX1 в группу обеспечения доступности баз данных DAG1.

PowerShell

```
Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer MBX1
```

В данном примере показано удаление сервера почтовых ящиков MBX1 из группы обеспечения доступности баз данных DAG1. Перед выполнением этой команды убедитесь, что на сервере почтовых ящиков не осталось реплицированных баз данных.

PowerShell

```
Remove-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer MBX1
```

В этом примере показано удаление параметров конфигурации сервера почтовых ящиков с именем MBX4 из группы обеспечения доступности баз данных DAG2. Сервер MBX4 продолжительное время будет находиться в автономном режиме, поэтому в течение этого времени его настройки будут удалены из группы обеспечения доступности баз данных, чтобы иметь возможность установить кворум с оставшимися в оперативном режиме членами данной группы.

PowerShell

```
Remove-DatabaseAvailabilityGroupServer -Identity DAG2 -MailboxServer MBX4 -
ConfigurationOnly
```

Как проверить, что все получилось?

Чтобы убедиться, что вы успешно распорядились членством в группе обеспечения доступности баз данных, выполните один из пунктов, перечисленных ниже.

- В EAC перейдите в раздел **Серверы**>**Группы доступности базы данных**. Нынешний состав группы обеспечения доступности баз данных отображается в столбце **Рядовые серверы**.
- В командной консоли Exchange выполните следующую команду, чтобы отобразить сведения о членстве в DAG.

```
PowerShell

Get-DatabaseAvailabilityGroup <DAGName> | Format-List Servers
```

Дополнительные сведения

Add-DatabaseAvailabilityGroupServer

Remove-DatabaseAvailabilityGroupServer

Настройка свойств группы доступности базы данных в Exchange Server

Статья • 04.04.2023

Командная консоль Exchange позволяет настроить свойства DAG, недоступные в EAC, такие как альтернативный следящий сервер и сведения о альтернативном следячем каталоге, TCP-порт, используемый для репликации, и режим координации активации центра обработки данных (DAC).

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 1 минута.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Группы доступности баз данных" в разделе Разрешения высокой доступности и устойчивости сайта .
- Значения свойств группы DAG хранятся в Active Directory и в базе данных кластера. Тем не менее некоторые свойства хранятся только в базе данных кластера. В результате базовый кластер для группы обеспечения доступности баз данных должен работать и иметь кворум, чтобы можно было задать следующие свойства:
  - ReplicationPort
  - NetworkCompression
  - NetworkEncryption
  - DiscoverNetworks
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online**

или **Exchange Online Protection** .

Использование EAC для настройки свойств группы обеспечения доступности базы данных

1. В EAC выберите **Серверы**>**Группы доступности базы данных**.
2. Выберите DAG, которую вы хотите настроить, и щелкните ✎
3. Страница **Общие** используется для просмотра членства в группе DAG и ее состояния, настройки следящего сервера и следящего каталога, а также автоматической настройки сети:
   - **Сервер-свидетель**. Имя узла или полное доменное имя (FQDN) следящего сервера для DAG. Хотя это обязательное свойство для всех групп обеспечения доступности баз данных, следящий сервер используется, когда имеется четное количество членов этой группы, а кластером применяется модель кворума "Большинство узлов и общих файловых ресурсов".
   - **Каталог следящего** сервера. Полный путь к каталогу, используемому для хранения файла witness.log на сервере-свидетеле. Хотя это обязательное свойство для всех групп обеспечения доступности баз данных, следящий каталог используется только в случае применения следящего сервера группы обеспечения доступности баз данных.
   - **Члены группы доступности базы данных**. Поле только для чтения, в котором отображается список участников DAG и их текущее рабочее состояние.
   - **Настройка сетей групп доступности базы данных вручную**. Флажок, который вы установите, когда вы хотите настроить все сети DAG вручную. Если флажок снят, система автоматически настраивает сети DAG на основе конфигурации сетевого интерфейса, а командлеты **Set-DatabaseAvailabilityGroupNetwork** и **New-DatabaseAvailabilityGroupNetwork** отключены для daG.
4. Используйте страницу **IP-адресов** , чтобы просмотреть и изменить IP-адреса, назначенные группе daG:
   - Выберите существующий IP-адрес и щелкните ✎ чтобы изменить его.

- Выберите существующий IP-адрес и нажмите кнопку со знаком минус (удаление), чтобы удалить его.
- Введите IP-адрес и нажмите ✚ чтобы добавить его в DAG.

5. Щелкните **Сохранить**, чтобы сохранить все изменения.

Настройка свойств группы доступности базы данных с помощью командной консоли Exchange

В этом примере показано, как установить следящий каталог C:\DAG1DIR для группы обеспечения доступности баз данных с именем DAG1.

PowerShell

```
Set-DatabaseAvailabilityGroup -Identity DAG1 -WitnessDirectory C:\DAG1DIR
```

В этом примере предварительно настраивается альтернативный следящий сервер MBX3 и альтернативный каталог-свидетель C:\DAGFileShareWitnesses\DAG1.contoso.com для DAG DAG1.

PowerShell

```
Set-DatabaseAvailabilityGroup -Identity DAG1 -AlternateWitnessDirectory
C:\DAGFileShareWitnesses\DAG1.contoso.com -AlternateWitnessServer MBX3
```

В этом примере показано, как настроить использование протокола DHCP для получения IP-адреса в группе обеспечения доступности баз данных с именем DAG1.

PowerShell

```
Set-DatabaseAvailabilityGroup -Identity DAG1 -
DatabaseAvailabilityGroupIPAddresses 0.0.0.0
```

В этом примере показано, как настроить использование статического IP-адреса 10.0.0.8 в группе обеспечения доступности баз данных с именем DAG1.

PowerShell

```
Set-DatabaseAvailabilityGroup -Identity DAG1 -
DatabaseAvailabilityGroupIPAddresses 10.0.0.8
```

В этом примере показано, как настроить группу обеспечения доступности баз данных DAG1 в нескольких подсетях с использованием нескольких статических IP-адресов.

PowerShell

```
Set-DatabaseAvailabilityGroup -Identity DAG1 -
DatabaseAvailabilityGroupIPAddresses 10.0.0.8,10.0.1.8
```

В этом примере показано, как настроить режим активации центра обработки данных для группы обеспечения доступности баз данных DAG1.

PowerShell

```
Set-DatabaseAvailabilityGroup -Identity DAG1 -DatacenterActivationMode
DagOnly
```

В этом примере показано, как настроить порт репликации 63132 для группы обеспечения доступности баз данных DAG1.

PowerShell

```
Set-DatabaseAvailabilityGroup -Identity DAG1 -ReplicationPort 63132
```

> ⓘ **Примечание**
>
> После изменения порта репликации по умолчанию для группы доступности базы данных необходимо вручную изменить исключения брандмауэра Windows для каждого участника группы DAG, чтобы разрешить подключение через указанный порт.

Как проверить, что все получилось?

Чтобы убедиться, что группа обеспечения доступности баз данных успешно настроена:

- В командной консоли Exchange выполните следующую команду, чтобы отобразить параметры конфигурации DAG и убедиться, что daG настроена успешно.

PowerShell

```
Get-DatabaseAvailabilityGroup <DAGName> | Format-List
```

Дополнительные сведения

Создание группы обеспечения доступности баз данных

Удаление группы обеспечения доступности баз данных

Создание сети группы доступности базы данных

Управление членством в группе обеспечения доступности баз данных

Get-DatabaseAvailabilityGroup

Set-DatabaseAvailabilityGroup

Управление копиями базы данных почтовых ящиков

Статья • 04.04.2023

В Exchange Server можно использовать консоль управления Exchange (EAC) или командную консоль Exchange, чтобы добавить копии базы данных почтовых ящиков после создания, настройки и заполнения членами сервера почтовых ящиков группы доступности базы данных (DAG).

Управление копиями базы данных

После создания нескольких копий базы данных можно использовать EAC или командную консоль Exchange для мониторинга работоспособности и состояния каждой копии, а также для выполнения других задач управления, связанных с копиями базы данных. Некоторые из задач управления, которые могут потребоваться выполнить, включают приостановку или возобновление копирования базы данных, засевание копии базы данных, мониторинг копий базы данных, настройку параметров копирования базы данных и удаление копии базы данных.

Приостановка и возобновление работы копий базы данных

По ряду причин, таких как плановое обслуживание, может потребоваться приостановить и возобновить непрерывную репликацию для копии базы данных. Кроме того, для некоторых административных задач, таких как ввод, необходимо сначала приостановить копию базы данных. Рекомендуется приостановить все действия репликации при изменении пути к базе данных или ее файлам журнала. Действие копирования базы данных можно приостановить и возобновить с помощью EAC или командлетов **Suspend-MailboxDatabaseCopy** и **Resume-MailboxDatabaseCopy** в командной консоли Exchange. Подробные инструкции по приостановке или возобновлению непрерывной репликации для копии базы данных см. в статье Приостановка или возобновление копирования базы данных почтового ящика.

Заполнение копии базы данных

Заполнение, также называемое *обновлением*, — это процесс, при котором пустая база данных или копия рабочей базы данных добавляется на другой сервер почтовых ящиков в одной с активной базой данных группе DAG. Эта база данных становится основной для копии, обслуживаемой сервером.

В зависимости от ситуации заполнение может выполняться автоматически или вручную. После добавления копия базы данных будет автоматически заполнена, если целевой сервер и его хранилище настроены правильно. Если вы хотите вручную заполнить копию базы данных и не хотите, чтобы при создании копии выполнялось автоматическое заполнение, можно использовать параметр *SeedingPostponed* при выполнении командлета Add-MailboxDatabaseCopy .

Иногда необходимо повторно заполнить копии базы данных после первоначального заполнения. Чтобы повторно заполнить копию базы данных или заполнить ее вручную, используйте мастер обновления копии базы данных в Центре администрирования Exchange или командлет Update-MailboxDatabaseCopy в командной консоли Exchange. Перед заполнением копии базы данных необходимо приостановить работу копии базы данных почтовых ящиков. Подробное описание действий по заполнению копии базы данных см. в разделе Обновление копии базы данных почтовых ящиков.

После заполнения копии базы данных вручную репликация заполненной копии базы данных почтовых ящиков будет автоматически возобновлена. Если автоматическое возобновление репликации не требуется, необходимо использовать параметр *ManualResume* при запуске командлета Update-MailboxDatabaseCopy.

Выбор объекта заполнения

Вы можете выбрать объект заполнения. По умолчанию мастер обновления копии базы данных почтовых ящиков и командлет Update-MailboxDatabaseCopy заполняют копию базы данных почтовых ящиков и копию каталога индексов содержимого. Чтобы заполнить только копию базы данных почтового ящика без заполнения каталога индексов контента, используйте параметр *DatabaseOnly* при выполнении командлета Update-MailboxDatabaseCopy . Чтобы заполнить только копию каталога индексов содержимого, используйте параметр *CatalogOnly* при запуске командлета Update-MailboxDatabaseCopy.

Выбор источника заполнения

Исправную копию базы данных можно использовать в качестве источника заполнения для дополнительной копии этой базы данных. Это может быть полезно, если группа доступности базы данных развернута в нескольких физических местоположениях. В качестве примера рассмотрим развертывание группы доступности базы данных из четырех участников, в которой два участника (MBX1 и MBX2) находятся в Москве, а другие два участника (MBX3 и MBX4) — в Санкт-Петербурге. База данных почтовых ящиков с именем DB1 активна в MBX1, а пассивные копии DB1 расположены в MBX2 и MBX3. При добавлении копии DB1 в MBX4 вы можете использовать копию в MBX3 как источник для заполнения. При этом вы избегаете заполнения по каналу глобальной сети между Москвой и Санкт-Петербургом.

Чтобы использовать определенную копию в качестве источника для заполнения при добавлении новой копии базы данных, выполните следующие действия.

- Используйте параметр *SeedingPostponed* при выполнении командлета Add-MailboxDatabaseCopy , чтобы добавить копию базы данных. Если параметр *SeedingPostponed не используется* , копия базы данных будет явно засеяна с использованием активной копии базы данных в качестве источника.
- Можно указать исходный сервер, который нужно использовать в мастере копирования базы данных почтовых ящиков в Центре администрирования Exchange, или использовать параметр *SourceServer* при выполнении командлета Update-MailboxDatabaseCopy , чтобы указать нужный исходный сервер для заполнения. В предыдущем примере сервер MBX3 указан в качестве исходного сервера. Если вы не используете параметр *SourceServer*, копия базы данных будет заполнена из активной копии базы данных.

Заполнение и сети

Помимо выбора конкретного исходного сервера для заполнения копии базы данных почтовых ящиков, можно также использовать командную консоль Exchange, чтобы указать, какие сети DAG следует использовать. Вы можете переопределить параметры сжатия и шифрования сети DAG во время начальной операции.

Вы можете указать сети, которые нужно использовать для заполнения, с помощью параметра *Network* при выполнении командлета Update-MailboxDatabaseCopy и указать сети DAG, которые вы хотите использовать. Если параметр *Network* не используется, система использует следующее поведение по умолчанию для выбора сети, используемой для операции заполнения:

- Если исходный и целевой серверы находятся в одной подсети и настроена сеть репликации, включающая в себя эту подсеть, будет использоваться сеть репликации.
- Если исходный и целевой серверы находятся в различных подсетях, даже если настроена сеть репликации, включающая в себя эти подсети, клиентская сеть (MAPI) будет использоваться для заполнения.
- Если исходный и целевой серверы находятся в различных центрах данных, будет использоваться клиентская сеть (MAPI) для заполнения.

Шифрование и сжатие данных настраивается на уровне группы DAG. По умолчанию шифрование и сжатие используются только для обмена данными в разных подсетях. Если исходный и целевой серверы находятся в разных подсетях и для группы DAG заданы значения параметров *NetworkCompression* и *NetworkEncryption* по умолчанию, вы можете переопределить эти значения, используя параметры *NetworkCompressionOverride* и *NetworkEncryptionOverride* соответственно при запуске командлета Update-MailboxDatabaseCopy.

Процесс заполнения

При запуске процесса заполнения с помощью командлета Add-MailboxDatabaseCopy или Update-MailboxDatabaseCopy выполняются следующие задачи:

1. Свойства базы данных из Active Directory считываются для проверки указанной базы данных и серверов, а также для проверки того, что исходный и целевой серверы работают Exchange Server, они оба являются членами одного daG и что указанная база данных не является базой данных восстановления. Также считываются пути к файлам базы данных.
2. Приготовления выполняются для проверки повторного заполнения из службы репликации Microsoft Exchange целевого сервера.
3. Служба репликации Microsoft Exchange на целевом сервере проверяет наличие базы данных и файлов журнала транзакций в каталогах файлов, считанных при проверке Active Directory на шаге 1.
4. Служба репликации Microsoft Exchange возвращает сведения о состоянии из целевого сервера в интерфейс администратора, в котором запущен командлет.

5. Если все предварительные проверки выполнены успешно, будет предложено подтвердить операцию перед продолжением. При подтверждении операции процесс продолжится. Если при предварительных проверках произошла ошибка, будет создан отчет об этой ошибке и произойдет сбой операции.

6. Операция заполнения начнется из службы репликации Microsoft Exchange целевого сервера.

7. Служба репликации Microsoft Exchange приостановит репликацию базы данных для активной копии базы данных.

8. Сведения о состоянии базы данных обновляются службой репликации Microsoft Exchange для отображения состояния заполнения.

9. Если на целевом сервере отсутствуют каталоги для файлов целевой базы данных и файлов журнала, они будут созданы.

10. Запрос на заполнение базы данных оправляется из службы репликации Microsoft Exchange на целевом сервере в службу репликации Microsoft Exchange на исходном сервере с помощью протокола TCP. Этот запрос и последующее подключения для заполнения базы данных выполняются в сети группы доступности базы данных, настроенной в качестве сети репликации.

11. Служба репликации Microsoft Exchange на исходном сервере запускает потоковую архивацию расширенного обработчика хранилищ (ESE) с помощью интерфейса службы банка данных Microsoft Exchange.

12. Служба банка данных Microsoft Exchange передает сведения базы данных в службу репликации Microsoft Exchange.

13. Сведения базы данных перемещаются из службы репликации Microsoft Exchange исходного сервера в службу репликации Microsoft Exchange целевого сервера.

14. Служба репликации Microsoft Exchange на целевом сервере записывает копию базы данных во временный каталог, расположенный в главном каталоге базы *данных*.

15. Операция потоковой архивации на исходном сервере заканчивается, когда достигается конец базы данных.

16. Операция записи завершается на целевом сервере, и база данных перемещается из каталога "temp-seeding" в конечное расположение. Каталог "temp-seeding" удаляется.

17. Служба репликации Microsoft Exchange на целевом сервере предоставляет запрос службе поиска Microsoft Exchange на подключение каталога индексов содержимого к копии базы данных, если она существует. Если существуют файлы каталога предыдущей копии базы данных с истекшим сроком действия, происходит сбой операции подключения, что приводит к необходимости репликации каталога с исходного сервера. Подобным образом, если каталог отсутствует в новом экземпляре копии базы данных на целевом сервере, требуется создать копию каталога. Служба репликации Microsoft Exchange указывает службе поиска Microsoft Exchange приостановить индексирование копии базы данных, пока новый каталог копируется из источника.

18. Служба репликации Microsoft Exchange на целевом сервере отправляет запрос на заполнение каталога службе репликации Microsoft Exchange на исходном сервере.

19. На исходном сервере служба репликации Microsoft Exchange запрашивает сведения о каталоге из службы поиска Microsoft Exchange и отправляет запрос на приостановку индексации.

20. Служба поиска Microsoft Exchange на исходном сервере возвращает сведения о каталоге из каталога поиска службе репликации Microsoft Exchange.

21. Служба репликации Microsoft Exchange на исходном сервере считывает файлы каталога из каталога.

22. Служба репликации Microsoft Exchange на исходном сервере перемещает данные каталога в службу репликации Microsoft Exchange на целевом сервере с помощью подключения в сети репликации. После считывания служба репликации Microsoft Exchange отправляет запрос на возобновление индексации исходной базы данных службе поиска Microsoft Exchange.

23. Если в папке на целевом сервере существуют файлы каталога, служба репликации Microsoft Exchange на целевом сервере удалит их.

24. Служба репликации Microsoft Exchange на целевом сервере записывает данные каталога во временный каталог *CiSeed.Temp* до полной передачи данных.

25. Служба репликации Microsoft Exchange перемещает все данные каталога в конечное местоположение.

26. Служба репликации Microsoft Exchange на целевом сервере возобновляет индексацию поиска в целевой базе данных.

27. Служба репликации Microsoft Exchange на целевом сервере возвращает уведомление о состоянии завершения.

28. Конечный результат операции проходит в интерфейс администратора, в котором был запущен командлет.

Настройка копий базы данных

Просмотреть информацию о конфигурации копии базы данных можно на ее странице Свойства в Центре администрирования Exchange. Вы можете просмотреть некоторые сведения о конфигурации, проверив на странице **Свойства** копию базы данных в EAC. Подробные инструкции см. в статье Настройка свойств копии базы данных почтовых ящиков.

Использование параметров задержки преобразования и задержки усечения

Копии базы данных почтовых ящиков поддерживают использование параметров *время задержки преобразования* и *время задержки усечения*, которые указываются в минутах. Установка времени задержки преобразования позволяет выполнить откат копии базы данных к определенной точке во времени. Установка времени задержки усечения позволяет использовать журналы в пассивной копии базы данных для восстановления утерянных файлов журнала активной копии базы данных. Поскольку использование обеих этих функций приводит к временному созданию файлов журнала, использование каждой из них влияет на архитектуру хранилища.

Время задержки преобразования

Интервал задержки воспроизведения — свойство копии базы данных почтовых ящиков, которое определяет интервал задержки воспроизведения журнала для копии базы данных (в минутах). Отсчет времени задержки воспроизведения начинается после репликации файла журнала в пассивную копию и успешного прохождения проверки. Задержка воспроизведения журналов в копию базы данных позволяет восстановить состояние базы данных в определенной точке времени в прошлом. Копия базы данных почтовых ящиков, для которой настроен интервал задержки воспроизведения больше 0, называется *изолированной копией базы данных почтовых ящиков*, или просто *изолированной копией*.

Стратегия, использующая копии баз данных и функции удержания для судебного разбирательства в Exchange Server, может обеспечить защиту от ряда сбоев,

которые обычно приводят к потере данных. Тем не менее, эти функции не могут обеспечить защиту от потери данных в случае логического повреждения, которое может привести к потере данных (хотя и в редких случаях). Изолированные копии разработаны для предотвращения потери данных в случае логического повреждения. Как правило, существует два типа логического повреждения

- **Логическое повреждение базы данных**. Контрольная сумма страниц базы данных совпадает, но данные на страницах логически неверны. Это происходит, когда расширенный обработчик хранилищ пытается записать страницу базы данных, и несмотря на то, что отображается сообщение об успешном завершении операции, данные либо вообще не записываются на диск, либо записываются в неправильном месте. Такая ситуация называется *утерянной очисткой*. Чтобы предотвратить потерю данных в результате утерянной очистки, расширенный обработчик хранилищ (ESE) добавляет в базу данных механизм определения утерянной очистки и функцию исправления страницы (восстановления одной страницы).

- **Логическое повреждение хранилища**. Данные добавляются, удаляются или обрабатываются таким образом, что пользователь не ожидает. Такие случаи обычно вызваны сторонними приложениями. Это повреждение является повреждением только в том смысле, что оно является таковым для пользователя. Хранилище Exchange считает транзакцию, которая привела к логическому повреждению серией правильных операций MAPI. Функция удержания для судебного разбирательства в Exchange Server обеспечивает защиту от логического повреждения хранилища (так как она предотвращает окончательное удаление содержимого пользователем или приложением). Однако возможны сценарии, когда почтовый ящик пользователя становится настолько поврежденным, что легче будет восстановить базу данных на момент до повреждения, а затем экспортировать почтовый ящик пользователя, чтобы извлечь неповрежденные данные.

Комбинация копий базы данных, политики удержания и восстановления одиночной страницы с помощью расширенного обработчика хранилищ предотвращает редкие катастрофические случаи логического повреждения хранилища. Решение о том, использовать копию базы данных с задержкой преобразования (изолированную копию), зависит от используемых сторонних приложений и от опыта исправления логических повреждений хранилища в организации.

При использовании изолированных копий необходимо учитывать следующие последствия.

- Существует настраиваемое администратором значение времени задержки преобразования, и по умолчанию оно отключено.
- Для параметра времени задержки преобразования по умолчанию установлено значение 0 дней. Максимальное значение для этого параметра — 14 дней.
- Изолированные копии не считаются высокодоступными. Они разработаны для аварийного восстановления и защиты от логического повреждения хранилища.
- Чем больше время задержки преобразования, тем дольше длится процесс восстановления базы данных. В зависимости от количества файлов журнала, которые необходимо преобразовать во время восстановления, и скорости, с которой оборудование их преобразовывает, восстановление базы данных может занять несколько часов.
- Рекомендуется определить, критично ли использование изолированных копий для общей стратегии аварийного восстановления. Если их использование является критичным, рекомендуется использовать несколько изолированных копий или использовать резервный массив независимых дисков (RAID) для защиты отдельной изолированной копии при отсутствии нескольких изолированных копий. При потере или повреждении диска отложенная во времени точка не будет потеряна.
- Отложенные копии не могут быть исправлены с помощью функции одностраничного восстановления ESE. Если при отложенной копии возникает повреждение страницы базы данных (например, ошибка -1018), копия должна быть повторно установлена. При повторном просмотре потеряется отстающий аспект копии.

Если вы хотите воспроизвести все файлы журнала и обновить копию базы данных, активировать и восстановить изолированную копию базы данных почтовых ящиков легко. Если вы хотите воспроизвести файлы журнала до определенного момента, задача становится сложнее, так как необходимо вручную управлять файлами журнала и запускать служебные программы Exchange Server (Eseutil.exe).

Подробные инструкции по активации копии базы данных отложенного почтового ящика см. в разделе Активация копии базы данных с отставленным почтовым ящиком.

Время задержки усечения

Интервал задержки усечения — свойство копии базы данных почтовых ящиков, которое определяет время задержки удаления журнала (в минутах) для копии базы данных после воспроизведения файла журнала в копию базы данных. Отсчет времени задержки усечения начинается после репликации файла журнала в пассивную копию, успешного прохождения проверки и воспроизведения в копию базы данных. Задержка усечения файлов журнала из копии базы данных позволяет выполнять восстановление после сбоев, влияющих на файлы журнала активной копии базы данных.

Копии базы данных и усечение журнала

Усечение журнала работает так же в Exchange 2016 и Exchange 2019, как и в Exchange 2010. Поведение усечения зависит от параметров времени задержки преобразования и времени задержки усечения копии.

Файл журнала копии базы данных должен соответствовать следующим критериям, если для параметров задержки установлено значение по умолчанию 0 (отключено).

- Файл журнала должен иметь архив или циклическое ведение журнала должно быть включено.
- Файл журнала должен находиться под контрольной точкой (минимальный файл журнала, необходимый для восстановления) для базы данных.
- Для всех других изолированных копий необходимо выполнить проверку файла журнала.
- Для всех других копий (неизолированных) необходимо воспроизвести файл журнала.

Для выполнения усечения необходимо соответствие копии базы данных следующим критериям.

- Файл журнала должен быть ниже контрольной точки для базы данных.
- Время, прошедшее с момента создания файла журнала, должно превышать значение ReplayLagTime + TruncationLagTime.
- Файл журнала должен быть усечен на активной копии.

В Exchange Server усечение журнала не выполняется в активной копии базы данных почтового ящика при приостановке одной или нескольких пассивных копий. Длительное плановое обслуживание может привести к накоплению значительного

количества файлов журнала. Чтобы предотвратить заполнение диска журналами транзакций, можно удалить пассивную копию базы данных, а не приостанавливать ее. После планового обслуживания можно повторно добавить эту пассивную копию базы данных.

Exchange Server теперь имеет функцию *свободного усечения*, которая отключена по умолчанию. Во время обычных операций каждая копия базы данных хранит журналы, которые должны быть отправлены в другие копии базы данных, пока все копии базы данных не подтвердят их воспроизведение (пассивные копии) или получение (отстающие копии) файлов журналов. Это поведение усечения журнала по умолчанию. Если по какой-либо причине копия базы данных переходит в автономный режим, файлы журнала начинают накапливаться на дисках, используемых другими копиями базы данных. Если затронутая копия базы данных остается в автономном режиме в течение длительного периода времени, это может привести к тому, что в других копиях базы данных не будет свободно места на диске.

Поведение усечения отличается, если включены свободное усечение и циклическое ведение журнала. Каждая копия базы данных отслеживает собственное свободное место на диске и применяет свободное усечение, если свободное место заканчивается.

- Активная копия: самая старая пассивная копия базы данных (по дате воспроизведения журналов) игнорируется, усечение начинается со следующей самой старой пассивной копии. Глобальное усечение рассчитывается в активной копии базы данных.

- Для пассивной копии, если пространство становится низким, она независимо усекает свои файлы журнала с помощью настроенных параметров, описанных далее в таблице Значения реестра. Пассивные копии будут пытаться выполнить решение об усечении, принятое для активной копии. Несмотря на значение имени MinCopiesToProtect, Exchange будет игнорировать только самый старый известный отставание на момент усечения.

При восстановлении автономной базы данных в сети в ней будут отсутствуют файлы журнала, удаленные из других работоспособных копий, а состояние копии базы данных — FailedAndSuspended. В этом случае, если настроено автоматическое использование, затронутая копия будет автоматически повторно добавлена. Если автоматическое использование не настроено, администратору потребуется вручную заполнить копию базы данных.

Если циклическое ведение журнала отключено, при свободном усечении будут учитываться резервные копии, если они были созданы, поэтому если резервные

копии журналов не были созданы, они не будут удалены путем свободного усечения.

Усечение рекомендуется использовать для предпочтительной архитектуры, в которой резервные копии не используются и включено циклическое ведение журнала.

Необходимое количество работоспособных копий, пороговое значение свободного места на диске и количество журналов для хранения — это настраиваемые параметры. По умолчанию порог свободного места на диске составляет 204800 МБ (200 ГБ), а количество журналов для хранения — 100 000 (100 ГБ) для пассивных копий и 10 000 (10 ГБ) для активных копий.

Включение свободного усечения и настройка параметров свободного усечения выполняется путем изменения реестра Windows в каждом элементе DAG. Можно настроить три значения реестра, которые хранятся в HKLM\Software\Microsoft\ExchangeServer\v15\BackupInformation. Ключ BackupInformation: следующие значения DWORD не существуют по умолчанию и должны быть созданы вручную. Значения реестра DWORD в разделе BackupInformation описаны в следующей таблице:

Значение реестра	**Описание**	**Значение по умолчанию**
LooseTruncation_MinCopiesToProtect	Этот раздел используется для включения свободного усечения. Он представляет собой количество пассивный копий, которые необходимо защитить от свободного усечения в активной копии базы данных. Если присвоить этому ключу значение 0, свободные усечения будут отключены.	0

Значение реестра	Описание	Значение по умолчанию
LooseTruncation_MinDiskFreeSpaceThresholdInMB	Пороговое значение доступного места на диске (в МБ) для запуска свободных усечений. Если количество свободного места на диске падает ниже этого значения, происходит запуск свободных усечений.	Если этот параметр реестра не настроен, при свободном усечении используется параметр по умолчанию (200 ГБ).
LooseTruncation_MinLogsToProtect	Минимальное количество файлов журналов, сохраняемых в работоспособных копиях, к которым применяется усечение. Если данный параметр реестра настроен, его значение применяется к активным и пассивным копиям.	Если данный параметр реестра не настроен, используются значения по умолчанию (100 000 для пассивных копий базы данных и 10 000 для активных копий базы данных).

При использовании значения реестра LooseTruncation_MinLogsToProtect обратите внимание, что поведение активных и пассивных копий базы данных отличается. В активной копии базы данных это количество дополнительных журналов, которые хранятся перед журналами, необходимыми для защищенных пассивных копий, и требуемый диапазон активной копии. В пассивной копии базы данных это количество журналов, храняемых из последнего доступного журнала. Одна десятая часть этого числа также используется для ведения журналов до требуемого диапазона этой пассивной копии. Эти два ограничения применяются для обеспечения того, чтобы отстающие копии базы данных не занимают слишком много места, так как требуемый диапазон обычно очень велик.

Политика активации базы данных

В некоторых случаях может потребоваться создать копию базы данных почтовых ящиков и предотвратить автоматическую активацию этой копии в случае сбоя. Ниже приведены примеры.

- При развертывании одной или нескольких копий базы данных почтовых ящиков в другом центре данных или центре данных, работающем в режиме ожидания.
- Если настроить отсроченную копию базы данных для целей восстановления.
- Если вы выполняете обслуживание или обновление сервера.

В каждом из указанных выше сценариев копии базы данных не должны автоматически активироваться системой. Чтобы предотвратить автоматическую активацию копии базы данных почтовых ящиков, можно настроить блокирование (приостановку) активации копии. Это позволяет системе обслуживать текущую базу данных с помощью доставки журнала и преобразования, но предотвращает автоматическую активацию и использование копии. Администратор должен вручную активировать заблокированные для активации копии. Политику активации базы данных можно настроить для всего сервера с помощью командлета Set-MailboxServer или отдельной копии базы данных с помощью командлета Set-MailboxDatabaseCopy , чтобы задать *параметру DatabaseCopyAutoActivationPolicy* значение Заблокировано.

Дополнительные сведения о настройке политики активации базы данных см. в разделе Настройка политики активации для копии базы данных почтовых ящиков.

Влияние перемещения почтовых ящиков на непрерывную репликацию

В интенсивно используемой базе данных почтовых ящиков с высокой скоростью создания журналов вероятность потери данных выше, если репликация в пассивные копии базы данных не успевает за созданием журналов. Скорость создания журналов возрастает при перемещении почтовых ящиков. Exchange Server включает API гарантии данных, который используется такими службами, как служба репликации почтовых ящиков Exchange (MRS), для проверки работоспособности архитектуры копирования базы данных на основе значения параметра *DataMoveReplicationConstraint*, заданного системой или администратором. В частности, API Data Guarantee может использоваться для:

- **Проверка работоспособности репликации**. Подтверждает наличие необходимого количества копий базы данных.
- **Проверка сброса репликации**. Подтверждает, что необходимые файлы журнала были воспроизведены в соответствии с необходимым числом копий базы данных.

При выполнении API-интерфейса он возвращает следующие сведения о состоянии вызывающему приложению:

- **Повторная попытка**. Указывает на наличие временных ошибок, которые препятствуют проверке условия в базе данных.
- **Удовлетворено**. Означает, что база данных соответствует требуемым условиям или база данных не реплицируется.
- **NotSatisfied**: означает, что база данных не соответствует требуемым условиям. Кроме того, вызывающему приложению предоставляется информация о причине возврата состояния **NotSatisfied**.

Значение параметра *DataMoveReplicationConstraint* для базы данных почтового ящика определяет, сколько копий базы данных следует оценить в рамках запроса. Параметр *DataMoveReplicationConstraint* имеет следующие возможные значения:

- `None`: при создании базы данных почтовых ящиков это значение задается по умолчанию. Если задано это значение, условия интерфейса Data Guarantee API игнорируются. Этот параметр следует использовать только для баз данных почтовых ящиков, которые не реплицируются.
- `SecondCopy`: это значение по умолчанию при добавлении второй копии базы данных почтовых ящиков. Если задано это значение, по крайней мере одна пассивная копия базы данных должна соответствовать условиям Data Guarantee API.
- `SecondDatacenter`: если задано это значение, по крайней мере одна пассивная копия базы данных на другом сайте Active Directory должна соответствовать условиям API гарантии данных.
- `AllDatacenters`: если задано это значение, по крайней мере одна пассивная копия базы данных на каждом сайте Active Directory должна соответствовать условиям API гарантии данных.
- `AllCopies`: если задано это значение, все копии базы данных почтовых ящиков должны соответствовать условиям API гарантии данных.

Проверка работоспособности репликации

При выполнении Data Guarantee API для оценки работоспособности инфраструктуры копий баз данных, оцениваются несколько элементов.

Во всех сценариях пассивная копия базы данных должна соответствовать следующим условиям:

- быть работоспособной;
- содержать очередь преобразования в течение 10 минут времени задержки преобразования;
- использовать очередь копирования длиной не менее 10 журналов;
- использовать среднюю очередь копирования длиной не менее 10 журналов. Средняя длина очереди копирования вычисляется на основе количества запросов состояния базы данных приложением.

Если для параметра *DataMoveReplicationConstraint* задано значение ...	**Затем для данной базы данных...**
`SecondCopy`	По крайней мере одна пассивная копия базы данных для реплицированной базы данных должна соответствовать описанным ранее условиям.
`SecondDatacenter`	По крайней мере одна пассивная копия базы данных на другом сайте Active Directory должна соответствовать описанным выше условиям.
`AllDatacenters`	Активная копия должна быть подключена, а пассивная копия на каждом сайте Active Directory должна соответствовать описанным ранее условиям.
`AllCopies`	Активная копия должна быть подключена, а все пассивные копии базы данных должны соответствовать описанным выше условиям.

Проверка очистки репликации

Data Guarantee API также можно использовать для проверки того, что требуемое число копий базы данных преобразовали необходимые журналы транзакций. Это делается за счет сравнения метки времени последнего преобразованного журнала с меткой времени вызывающей службы (в большинстве случаев это метка времени последнего файла журнала, который содержит необходимые данные), плюс дополнительные пять секунд (для учета рассогласования системного времени). Если метка времени воспроизведения больше метки времени фиксации, параметр *DataMoveReplicationConstraint* удовлетворяется. Если метка времени воспроизведения меньше метки времени фиксации, *dataMoveReplicationConstraint* не удовлетворяется.

Перед перемещением большого количества почтовых ящиков в базы данных репликации или из них в DAG рекомендуется настроить параметр

DataMoveReplicationConstraint для каждой базы данных почтовых ящиков следующим образом:

Если вы развертываете...	Задайте для dataMoveReplicationConstraint значение...
Базы данных почтовых ящиков, которые не имеют каких-либо копий базы данных	`None`
Группа DAG на одном сайте Active Directory	`SecondCopy`
Группа DAG в нескольких центрах обработки данных с использованием растянутого сайта Active Directory	`SecondCopy`
Группа DAG, в которую входят два сайта Active Directory, на каждом сайте будут копии базы данных с высокой доступностью	`SecondDatacenter`
Группа DAG, в которую входят два сайта Active Directory, на втором сайте будут только изолированные копии базы данных	`SecondCopy` Это связано с тем, что Data Guarantee API не гарантирует фиксирование данных до воспроизведения файла журнала в копии базы данных и вследствие природы изолированной копии базы данных это ограничение не позволит выполнить запрос на перемещение, если значение ReplayLagTime этой изолированной копии базы данных меньше 30 минут.
Группа DAG, в которую входят три или больше сайтов Active Directory, при этом каждый сайт будет содержать копии базы данных с высокой доступностью	`AllDatacenters`

Балансировка копий баз данных

Следствием самой структуры групп обеспечения доступности баз данных (DAG) и результатом переключений базы данных и отработок отказа в них является то, что для активных копий базы данных почтовых ящиков узлы размещения будут меняться несколько раз в течение времени жизни группы DAG. В итоге, группы DAG становятся несбалансированными с точки зрения распределения активных

копий базы данных почтовых ящиков. В следующей таблице приводится пример группы DAG, в которой имеются четыре базы данных с четырьмя копиями каждой из них (всего 16 баз данных на каждом сервере) с неравномерным распределением активных копий баз данных.

Группа DAG с несбалансированным распределением активных копий

Сервер	Количество активных баз данных	Количество пассивных баз данных	Количество подключенных баз данных	Количество отключенных баз данных	Список для подсчета приоритетов
EX1	5	11	5	0	4, 4, 3, 5
EX2	1	15	1	0	1, 8, 6, 1
EX3	12	4	12	0	13, 2, 1, 0
EX4	1	15	1	0	1, 1, 5, 9

В предыдущем примере для каждой базы данных существует четыре копии, и поэтому возможно только четыре значения для приоритета активации (1, 2, 3 или 4). В столбце **Список для подсчета приоритетов** приводится подсчет числа баз данных с каждым из этих значений. Например, на сервере EX3 имеется 13 копий баз данных с приоритетом активации 1, две копии с приоритетом 2, одна копия с приоритетом 3 и ни одной копии с приоритетом 4.

Как можно видеть, эта группа обеспечения доступности баз данных не сбалансирована с точки зрения количества активных баз данных или количества пассивных баз данных, размещаемых каждым членом такой группы, либо подсчета приоритетов активации для размещенных баз данных.

Вы можете использовать скрипт RedistributeActiveDatabases.ps1 для балансировки копий баз данных почтовых ящиков в группе обеспечения доступности баз данных. В этом сценарии базы данных перемещаются между своими копиями с целью попытки получения равных количеств подключенных баз данных на каждом сервере в группе DAG. При необходимости также выполняется попытка балансировки активных баз данных по сайтам.

В этом сценарии имеется два параметра для балансировки активных копий баз данных в группе DAG.

- **BalanceDbsByActivationPreference:** если указан этот параметр, скрипт пытается переместить базы данных в наиболее предпочтительную копию (на основе предпочтений активации) без учета сайта Active Directory.

- **BalanceDbsBySiteAndActivationPreference**: если указан этот параметр, скрипт пытается переместить активные базы данных в наиболее предпочтительную копию, а также пытается сбалансировать активные базы данных на каждом сайте Active Directory.

После запуска сценария с первым параметром предыдущая несбалансированная группа DAG становится сбалансированной, как показано в следующей таблице.

Группа DAG со сбалансированным распределением активных копий

Сервер	Количество активных баз данных	Количество пассивных баз данных	Количество подключенных баз данных	Количество отключенных баз данных	Список для подсчета приоритетов
EX1	4	12	4	0	4, 4, 4, 4
EX2	4	12	4	0	4, 4, 4, 4
EX3	4	12	4	0	4, 4, 4, 4
EX4	4	12	4	0	4, 4, 4, 4

Как показано выше, эта группа DAG теперь сбалансирована с точки зрения количества активных и пассивных баз данных на каждом сервере и приоритетов активации по серверам.

В следующей таблице перечислены параметры скрипта RedistributeActiveDatabases.ps1.

Параметры сценария RedistributeActiveDatabases.ps1

Параметр	Описание
DagName	Указывает имя группы DAG, которую необходимо сбалансировать. Если этот параметр не указан, будет использоваться та группа обеспечения доступности баз данных, членом которой является данный локальный сервер.
BalanceDbsByActivationPreference	Указывает, что согласно сценарию базы данных должны перемещаться в их наиболее предпочтительную копию безотносительно сайта Active Directory.

Параметр	Описание
BalanceDbsBySiteAndActivationPreference	При указании этого параметра в сценарии производится попытка переместить активные базы данных в их наиболее предпочтительную копию, а также сбалансировать активные базы данных в пределах каждого сайта Active Directory.
ShowFinalDatabaseDistribution	Указывает, что отчет по распределению текущей базы данных должен отображаться после перераспределения.
AllowedDeviationFromMeanPercentage	Указывает допустимую вариацию активных баз данных по сайтам, выраженную в процентах. Значение по умолчанию — 20 %. Например, если между тремя сайтами было распределено 99 баз данных, то идеальным распределением будет по 33 базы данных на каждом сайте. Если допустимое отклонение составляет 20 %, то при выполнении сценария будет производиться попытка сбалансировать базы данных таким образом, чтобы количество баз данных на каждом сайте отклонялось не более чем на 10 % в ту или другую сторону от этого значения. 10 % от 33 составляют 3,3, это значение можно округлить до 4. Следовательно, в результате выполнения сценария на каждом сайте будет от 29 до 37 баз данных.
ShowDatabaseCurrentActives	Указывает, что в сценарии необходимо создать отчет для каждой базы данных с подробными сведениями о том, как перемещалась база данных и является ли она теперь активной в своей наиболее предпочтительной копии.
ShowDatabaseDistributionByServer	Указывает, что в сценарии необходимо создать отчет для каждого сервера со сведениями о распределении базы данных на нем.
RunOnlyOnPAM	Указывает, что сценарий должен выполняться только для того члена группы DAG, который имеет роль диспетчера PAM. В сценарии в таком случае проверяется, происходит ли его запуск из диспетчера PAM. Если это условие не выполнено, то происходит выход из сценария.
События LogEvents	Указывает, что в процессе выполнения сценария необходимо внести в журнал событие 4115 (MsExchangeRepl) со сводкой по действиям.

Параметр	Описание
IncludeNonReplicatedDatabases	Указывает, что в сценарий во время определения способа перераспределения активных баз данных необходимо включить нереплицированные базы данных (базы данных без копий). Несмотря на то что нереплицированные базы данных перемещать невозможно, они могут влиять на распределение реплицированных баз данных.
Confirm	Переключатель Confirm можно использовать для отключения запросов на подтверждение, которые отображаются по умолчанию при запуске этого скрипта. Чтобы отключить запросы на подтверждение, используйте синтаксис -Confirm:$False. В синтаксисе необходимо использовать двоеточие (:).

Примеры RedistributeActiveDatabases.ps1

В этом примере показано распределение текущей базы данных для группы DAG, в том числе список для подсчета приоритетов.

PowerShell

```
RedistributeActiveDatabases.ps1 -DagName DAG1 -
ShowDatabaseDistributionByServer | Format-Table
```

Этот пример выполняет повторное распределение и балансировку активных копий базы данных почтовых ящиков в группе доступности с использованием предпочтений активации без запроса на ввода данных.

PowerShell

```
RedistributeActiveDatabases.ps1 -DagName DAG1 -
BalanceDbsByActivationPreference -Confirm:$False
```

В этом примере выполняется перераспределение и балансировка активных копий базы данных почтовых ящиков в группе DAG с учетом приоритетов активации, а также формируется сводка по процессу распределения.

PowerShell

```
RedistributeActiveDatabases.ps1 -DagName DAG1 -
BalanceDbsByActivationPreference -ShowFinalDatabaseDistribution
```

Копии базы данных мониторинга

Сведения о копии базы данных, в том числе длину очереди копирования, длину очереди воспроизведения, статус и информацию о состоянии индекса контента, можно просмотреть в Центре администрирования Exchange. Информацию о состоянии копии базы данных также можно просмотреть с помощью командлета **Get-MailboxDatabaseCopyStatus** в командной консоли Exchange.

> ⓘ **Примечание**
>
> Копия базы данных является первой защитой при сбое, влияющем на активную копию базы данных. Поэтому важно отслеживать работоспособность и состояние копий базы данных, чтобы они были доступны при необходимости.

Дополнительные сведения о мониторинге копий баз данных см. в разделе Мониторинг групп доступности баз данных.

Удаление копии базы данных

Копию базы данных можно удалить в любое время с помощью EAC или командлета **Remove-MailboxDatabaseCopy** в командной консоли Exchange. После удаления копии базы данных необходимо вручную удалить все файлы журнала базы данных и транзакций на сервере, с которого была удалена база данных. Подробные инструкции по удалению копии базы данных см. в разделе Удаление копии базы данных почтового ящика.

Переключения базы данных.

Сервер почтовых ящиков, на котором размещена активная копия базы данных, является хозяином базы данных почтовых ящиков. В процессе активации пассивной копии базы данных изменяется хозяин базы данных почтовых ящиков и пассивная копия преобразуется в новую активную копию. Этот процесс называется переключением базы данных. При переключении базы данных активная копия базы данных отключается на одном сервере почтовых ящиков, а пассивная копия этой базы данных подключается в качестве новой активной базы данных почтовых ящиков на другом сервере почтовых ящиков. При выполнении переключения можно также переопределить параметр подключения базы данных на новом хозяине базы данных почтовых ящиков.

Чтобы быстро определить, какой сервер является главным для базы данных почтовых ящиков, просмотрите правый столбец на вкладке **Копии базы данных** в Центре администрирования Exchange. Переключение можно выполнить с помощью ссылки **Активировать** в Центре администрирования Exchange или с помощью командлета **Move-ActiveMailboxDatabase** в командной консоли Exchange.

Перед активацией пассивной копии будет выполнено несколько внутренних проверок. В некоторых случаях переключение базы данных блокируется или отменяется. В других случаях с помощью командлетов можно переместить или пропустить некоторые проверки.

- Проверяется состояние копии базы данных. Если копия базы данных повреждена, переключение будет заблокировано. Это поведение можно переопределить и обойти проверку работоспособности с помощью параметра *SkipHealthChecks* командлета **Move-ActiveMailboxDatabase** . Этот параметр позволяет переместить активную копию в поврежденную копию базы данных.

- Проверяется, является ли активная копия базы данных источником заполнения каких-либо пассивных копий базы данных. Если активная копия в данный момент используется как источник для заполнения, переключение блокируется. Это поведение можно переопределить и обойти проверку исходного кода с помощью параметра *SkipActiveCopyChecks* командлета **Move-ActiveMailboxDatabase** . Этот параметр позволяет переместить активную копию, используемую как источник заполнения. При применении этого параметра заполнение будет отменено и будет считаться неудачным.

- Выполняется проверка значений длины очереди копирования и очереди преобразования копии базы данных на нахождение в пределах заданных критериев. Также выполняется проверка того, используется ли копия базы данных в качестве источника для заполнения. Если значения длины очередей не соответствуют заданным критериям или база данных является источником заполнения, переключение будет заблокировано. Это поведение можно переопределить и обойти эти проверки с помощью параметра *SkipLagChecks* командлета **Move-ActiveMailboxDatabase** . Этот параметр позволяет активировать копии, которые имеют значения очередей преобразования и копирования за пределами настроенных критериев.

- Выполняется проверка состояния каталога поиска (индексов содержимого) для копии базы данных. Если каталог поиска устарел, неисправен или поврежден, переключение будет заблокировано. Это поведение можно

переопределить и обойти проверку каталога поиска с помощью параметра *SkipClientExperienceChecks* командлета **Move-ActiveMailboxDatabase** . Этот параметр позволяет пропустить проверку работоспособности каталога поиска. Если каталог поиска для активируемой копии базы данных неисправен или нестабилен, и этот параметр используется для пропуска проверки работоспособности каталога и активации копии базы данных, необходимо повторно сканировать или заполнить каталог поиска.

When you perform a database switchover, you also have the option of overriding the mount dial settings configured for the server that hosts the passive database copy being activated. *И*спользование параметра *MountDialOverride* командлета **Move-ActiveMailboxDatabase** позволяет целевому серверу переопределить собственные параметры набора номера подключения и использовать параметры, заданные параметром *MountDialOverride* .

Дополнительные сведения о переключении копии базы данных см. в разделе Активация копии базы данных почтовых ящиков.

Добавление копии базы данных почтового ящика в Exchange Server

Статья • 04.04.2023

При добавлении копии базы данных почтовых ящиков автоматически включается непрерывная репликация между базой данных и ее копией. Копиям базы данных автоматически назначается удостоверение в формате *<DatabaseName>**<HostMailboxServerName>*. Например, копия базы данных DB1, которая размещается на сервере MBX3, будет называться DB1\MBX3.

Сведения о других задачах управления, относящихся к копиям базы данных почтовых ящиков, см. См. раздел Управление копиями базы данных почтовых ящиков.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 2 минуты, а также время на заполнение копии базы данных, которое зависит от ряда факторов, например размера базы данных, скорости, доступной полосы пропускания и задержки сети, а также скорости работы хранилища.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Копии баз данных почтовых ящиков" в разделе Разрешения высокой доступности и устойчивости сайта .
- Необходимо подключить активную копию базы данных.
- Указанный сервер почтовых ящиков не должен содержать уже существующую копию базы данных.
- Путь к копии базы данных и ее файлам журналов должен быть доступен на указанном сервере почтовых ящиков.
- Сервер, на котором размещается активная копия и сервер, на котором будет размещена пассивная копия, должны находиться в одной группе обеспечения доступности базы данных (DAG). Группа доступности базы данных также должна иметь кворум и быть работоспособной.
- Если добавляется вторая копия базы данных (например, создается первая пассивная копия базы данных), для указанной базы данных почтовых ящиков

не должно быть включено циклическое ведение журнала. Если циклическое ведение журнала включено, его необходимо отключить. После добавления копии базы данных почтовых ящиков циклическое ведение журнала можно включить. После включения циклического ведения журнала для реплицируемой базы данных почтовых ящиков вместо циклического ведения журнала JET используется циклическое ведение журнала с непрерывной репликацией (CRCL). Если добавляется третья или последующая копия базы данных, CRCL можно оставить включенным.

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование EAC для добавления копии базы данных почтовых ящиков

1. В EAC выберите **Серверы**>**Базы данных**.
2. Выберите базу данных, которую нужно скопировать, выберите **Дополнительно** (три точки справа от значка "Обновить"), а затем нажмите **Добавить копию базы данных**.
3. На странице **Добавление копии базы данных почтовых ящиков** щелкните **Обзор**, выберите сервер почтовых ящиков, на котором будет размещена копия базы данных, а затем щелкните **OK**.
4. При необходимости настройте **Приоритет активации** для копии базы данных.
5. Щелкните **Дополнительные параметры...** , чтобы назначить копию базы данных отстающей копией базы данных, настроив время задержки воспроизведения или отложив автоматическое заполнение копии базы данных.
6. Щелкните **Сохранить** для сохранения изменений конфигурации и добавления копии базы данных почтовых ящиков.
7. Нажмите кнопку **OK**, чтобы подтвердить все появляющиеся сообщения.

Добавление копии базы данных почтового ящика с помощью командной консоли Exchange

В этом примере копия базы данных почтовых ящиков DB1 добавляется на сервер почтовых ящиков MBX3. Время задержки воспроизведения и время запаздывания усечения остаются без изменений (0), а для приоритета активации устанавливается значение 2.

PowerShell

```
Add-MailboxDatabaseCopy -Identity DB1 -MailboxServer MBX3 -
ActivationPreference 2
```

В этом примере копия базы данных почтовых ящиков DB2 добавляется на сервер почтовых ящиков MBX4. Время задержки воспроизведения и время усечения задержки остаются равными нулю по умолчанию, а параметр активации настраивается со значением `5`. Кроме того, заполнение этой копии откладывается, чтобы при заполнении можно было использовать локальный исходный сервер вместо текущей активной копии базы данных, которая географически отдалена от MBX4.

PowerShell

```
Add-MailboxDatabaseCopy -Identity DB2 -MailboxServer MBX4 -
ActivationPreference 5 -SeedingPostponed
```

В этом примере копия базы данных почтовых ящиков DB3 добавляется на сервер почтовых ящиков MBX5. Время задержки воспроизведения задается в 3 дня, время усечения задержки остается по умолчанию равным нулю, а предпочтение активации настраивается со значением `4`.

PowerShell

```
Add-MailboxDatabaseCopy -Identity DB3 -MailboxServer MBX5 -ReplayLagTime
3.00:00:00 -ActivationPreference 4
```

Как проверить, все ли получилось?

Чтобы убедиться, успешно ли создана копия базы данных почтовых ящиков, выполните одно из следующих действий:

- В EAC перейдите в раздел **Серверы**>**Базы данных**. Выберите базу данных, которая была скопирована. В области "Сведения" отображается состояние копии базы данных и индекса ее содержимого, а также текущая длина очереди копирования.
- В командной консоли Exchange выполните следующую команду, чтобы убедиться, что копия базы данных почтового ящика создана и работоспособна.

  ```
  PowerShell

  Get-MailboxDatabaseCopyStatus <DatabaseCopyName>
  ```

  Состояние самой копии и индекса содержимого должно быть указано как работоспособное.

Дополнительные сведения

Копии базы данных почтовых ящиков

Управление копиями базы данных почтовых ящиков

Настройка свойств копирования базы данных почтовых ящиков в Exchange Server

Статья • 04.04.2023

Каждая копия базы данных почтового ящика имеет собственные свойства, которые можно настроить. К этим свойствам относятся время задержки воспроизведения и задержки усечения(при наличии), а также номер предпочтения активации. Дополнительные сведения о задержке воспроизведения, задержке усечения и номере предпочтения активации см. в разделе Управление копиями базы данных почтовых ящиков.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 1 минута
- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Копии баз данных почтовых ящиков" в разделе Разрешения высокой доступности и устойчивости сайта .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование Центра администрирования Exchange для настройки свойств копии базы данных почтовых ящиков

1. В EAC выберите **Серверы**>**Базы данных**.

2. Выберите базу данных, которую нужно настроить.

3. В области сведений в разделе **Копии базы данных** щелкните **Подробности** для нужной копии базы данных, а затем просмотрите или настройте следующее:

    - **База данных**. Отображает имя выбранной базы данных.

    - **Сервер почтовых ящиков**. Отображает имя сервера почтовых ящиков, на котором размещена выбранная копия базы данных.

    - **Состояние индекса контента**. Отображает текущее состояние индекса контента для выбранной копии базы данных.

    - **Состояние**. Отображает текущее состояние выбранной копии базы данных.

    - **Длина очереди копирования**. Указывает количество файлов журнала, ожидающих копирования в выбранную копию базы данных. Это поле является значимым только для пассивных копий базы данных.

    - **Длина очереди воспроизведения**. Указывает количество файлов журнала, ожидающих воспроизведения в выбранной копии базы данных. Это поле является значимым только для пассивных копий базы данных.

    - **Сообщения об ошибках**: отображаются все сообщения об ошибках для копий базы данных с состоянием `Failed` или `Failed and Suspended`.

    - **Последнее доступное время журнала**. Отображает метку даты и времени последнего созданного файла журнала в активной копии базы данных. Это поле является значимым только для пассивных копий базы данных. В активных копиях базы данных (реплицируемых и автономных) в нем будет указано никогда.

    - **Время последней проверки журнала**. Отображает метку даты и времени последнего файла журнала, проверенного LogInspector в выбранной копии базы данных. Это поле является значимым только для пассивных копий базы данных. В активных копиях базы данных (реплицируемых и автономных) в нем будет указано никогда.

    - **Время последнего копирования журнала**. Отображает метку даты и времени последнего файла журнала, скопированного logCopier в

выбранной копии базы данных. Это поле является значимым только для пассивных копий базы данных. В активных копиях базы данных (реплицируемых и автономных) в нем будет указано никогда.

- **Время последнего воспроизведения журнала**. Отображает метку даты и времени последнего файла журнала, который был воспроизведен LogReplayer в выбранной копии базы данных. Это поле является значимым только для пассивных копий базы данных. В активных копиях базы данных (реплицируемых и автономных) в нем будет указано никогда.

- **Номер предпочтения активации**. Отображает номер предпочтения активации. Он используется как часть процесса выбора оптимального копирования Active Manager и используется для балансировки daG путем перераспределения активных баз данных почтовых ящиков в daG через свойство DAG `PreferenceMoveFrequency` . Это свойство определяет частоту (измеряемую во времени), когда служба репликации Microsoft Exchange перебалансирует копии базы данных путем переключения без потерь, которое активирует копию с номером предпочтения активации 1. Значение приоритета активации — это число, равное или больше 1, где 1 означает самый высокий приоритет. Число приоритета не может быть больше числа копий базы данных почтовых ящиков.

- **Время задержки воспроизведения (в днях).** Отображает время ожидания службы хранилища сведений Microsoft Exchange перед воспроизведением файлов журналов, скопированных службой репликации Microsoft Exchange, в пассивную копию базы данных. При установке для данного параметра значения больше 0 создается изолированная копия базы данных. Значение по умолчанию для этого значения — 0 дней. Максимально допустимое значение для этого параметра — 14 дней. Минимально допустимое значение — 0 дней, а установка этого значения в 0 отключает задержку воспроизведения.

Настройка свойств копирования базы данных почтовых ящиков с помощью командной консоли Exchange

В данном примере выполняется настройка копии базы данных почтовых ящиков со значением приоритета активации 3.

PowerShell

```
Set-MailboxDatabaseCopy -Identity DB3\EX3 -ActivationPreference 3
```

В данном примере выполняется настройка копии базы данных с именем DB1, которая размещена на сервере Server1 с временем задержки преобразования со значением, равным 1 день, и значением приоритета активации — 2.

PowerShell

```
Set-MailboxDatabaseCopy -Identity DB1\Server1 -ReplayLagTime 1.0:0:0 -
TruncationLagTime 1.0:0:0 -ActivationPreference 2
```

Как проверить, что все получилось?

Чтобы убедиться, успешно ли настроена копия базы данных почтовых ящиков, выполните одно из следующих действий:

- В EAC перейдите в раздел **Серверы**>**Базы данных**. Выберите подходящую базу данных, и в области "Сведения" нажмите кнопку **Просмотр сведений**, чтобы открыть свойства копии базы данных.
- В командной консоли Exchange выполните следующую команду, чтобы отобразить сведения о конфигурации для копии базы данных.

  PowerShell

  ```
  Get-MailboxDatabaseCopyStatus <DatabaseCopyName> | Format-List
  ```

Дополнительные сведения

Set-MailboxDatabaseCopy

Get-MailboxDatabaseCopyStatus

Get-MailboxDatabase

Перемещение пути к базе данных почтового ящика для копии базы данных почтового ящика в Exchange Server

Статья • 04.04.2023

Если база данных почтовых ящиков, путь к которой изменяется, реплицируется в одну или несколько копий базы данных, необходимо выполнить описанную в этом разделе процедуру, чтобы изменить путь к базе данных. Все копии базы данных почтовых ящиков должны иметь одинаковый путь на каждом сервере, на котором размещена копия. Например, если база данных DB1 имеет путь C:\mountpoints\DB1 на сервере EX1, копии DB1 на серверах EX2, EX3 и др. также должны иметь путь C:\mountpoints\DB1.

> ⓘ **Примечание**
>
> После создания базы данных почтового ящика ее можно переместить в другой том, папку, расположение или путь с помощью EAC или командной консоли Exchange. Пошаговые инструкции по перемещению пути к базе данных для **нереплицированной** базы данных почтовых ящиков см. **в статье Управление базами данных почтовых ящиков в Exchange Server**.

Сведения о других задачах управления, относящихся к копиям базы данных почтовых ящиков, см. в статье Managing mailbox database copies.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 2 минуты, а также время на перемещение данных, которое зависит от ряда факторов, например размера базы данных, скорости, доступной полосы пропускания и задержки сети, а также скорости работы хранилища.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Копии баз данных почтовых ящиков" в разделе Разрешения высокой доступности и устойчивости сайта .

- Чтобы выполнить операцию перемещения, база данных должна быть временно отключена, что сделает ее недоступной для всех пользователей. Если база данных отключена перед операцией, она не будет подключена после выполнения операции.
- Для выполнения операции перемещения репликация базы данных должна быть отключена для всех копий. Недостаточно приостановить репликацию; Его необходимо отключить с помощью командлета Remove-MailboxDatabaseCopy , чтобы удалить копии базы данных.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Перемещение реплицированной базы данных почтовых ящиков по новому пути с помощью командной консоли Exchange

> **Примечание**
>
> Вы не можете использовать Центр администрирования Exchange (EAC) для перемещения реплицированной базы данных почтовых ящиков по новому пути.

1. Обратите внимание на любые параметры запаздывания преобразования и усечения для всех копий перемещаемой базы данных почтовых ящиков. Эти сведения можно получить с помощью командлета Get-MailboxDatabase, как показано в этом примере.

   PowerShell

   ```
   Get-MailboxDatabase DB1 | Format-List *lag*
   ```

2. Если для базы данных включено циклическое ведение журнала, его необходимо отключить перед продолжением работы. Циклическое ведение журнала можно отключить для базы данных почтовых ящиков с помощью командлета Set-MailboxDatabase, как показано в этом примере.

```
PowerShell

Set-MailboxDatabase DB1 -CircularLoggingEnabled $false
```

3. Удалите все копии базы данных почтовых ящиков для перемещаемой базы данных Дополнительные сведения см. в разделе Удаление копии базы данных почтовых ящиков. После удаления всех копий сохраните базу данных и файлы журналов транзакций с каждого сервера, с которого удаляется копия базы данных, путем их перемещения в другое местоположение. Эти файлы сохраняются, поэтому для копий базы данных не требуется повторное заполнение после повторного добавления.

4. Измените путь к базе данных почтовых ящиков. Дополнительные сведения см. в разделе Move a mailbox database path.

> ⓘ **Важно!**
>
> При выполнении операции перемещения база данных должна быть отключена. Этот процесс приведет к перерыву в обслуживании и отключению всех пользователей, имеющих почтовые ящики в перемещаемой базе данных, до завершения перемещения. После завершения операции перемещения база данных будет автоматически подключена.

5. Создайте необходимую структуру папок на каждом сервере почтовых ящиков, на котором ранее содержалась пассивная копия перемещенной базы данных почтовых ящиков. Например, если путь к базе данных был изменен на C:\mountpoints\DB1, необходимо создать такой же путь на каждом сервере почтовых ящиков, на котором будет храниться копия базы данных почтовых ящиков.

6. После создания структуры папок переместите пассивную копию базы данных почтовых ящиков, а также ее поток журнала в новое местоположение. Это файлы, которые остались и были сохранены после выполнения шага 3. Повторите этот процесс для каждой копии базы данных, удаленной на шаге 3.

7. Добавьте все копии базы данных, которые были удалены при выполнении действия 3. Дополнительные сведения см. в статье Add a mailbox database copy.

8. На каждом сервере, который содержит копию перемещаемой базы данных почтовых ящиков, выполните следующую команду, чтобы остановить и перезапустить службы индексов содержимого.

```
PowerShell

Restart-Service MSExchangeFastSearch
```

9. При необходимости включите циклическое ведение журналов с помощью командлета Set-MailboxDatabase, как показано в этом примере.

```
PowerShell

Set-MailboxDatabase DB1 -CircularLoggingEnabled $true
```

10. Повторно настройте любые ранее заданные значения времени запаздывания преобразования и времени запаздывания усечения с помощью командлета Set-MailboxDatabaseCopy, как показано в этом примере.

```
PowerShell

Set-MailboxDatabaseCopy DB1\MBX2 -ReplayLagTime 00:15:00
```

11. При добавлении каждой копии рекомендуется проверять ее работоспособность и состояние перед добавлением следующей копии. Работоспособность и состояние можно проверить следующими способами:

    a. Проверка журнала событий на наличие ошибок и событий предупреждений, связанных с базой данных или копией базы данных.

    b. Проверка работоспособности и состояния непрерывной репликации для копии базы данных с помощью командлета Get-MailboxDatabaseCopyStatus.

    c. Проверка работоспособности и состояния группы доступности базы данных и непрерывной репликации с помощью командлета Test-ReplicationHealth.

Подробные сведения о синтаксисе и параметрах см. в следующих разделах:

- Get-MailboxDatabase

- Set-MailboxDatabase
- Set-MailboxDatabaseCopy
- Get-MailboxDatabaseCopyStatus
- Test-ReplicationHealth

Как проверить, все ли получилось?

Чтобы проверить, успешно ли перемещен путь для копии базы данных почтовых ящиков, выполните одно из указанных ниже действий.

- В EAC перейдите в раздел **Серверы**>**Базы данных**. Выберите базу данных, которая была скопирована. В области "Сведения" отображается состояние копии базы данных и индекса ее содержимого, а также текущая длина очереди копирования. Убедитесь, что состояние работоспособное.
- В командной консоли Exchange выполните следующую команду, чтобы убедиться, что копия базы данных почтового ящика создана и работоспособна.

  PowerShell

  ```
  Get-MailboxDatabaseCopyStatus <DatabaseCopyName>
  ```

  Состояние самой копии и индекса содержимого должно быть указано как работоспособное.

Настройка политики активации для копии базы данных почтовых ящиков в Exchange Server

Статья • 04.04.2023

Активация — это процесс переключения пассивной копии базы данных почтовых ящиков в активную копию. Активация может происходить автоматически (системой в рамках операции отработки отказа базы данных или сервера) или выполняться вручную (администратором в рамках операции переключения базы данных или сервера). Блокировка активации базы данных позволяет предотвратить включение ее активной копии во время перехода базы данных или сервера на другой ресурс при сбое.

Сведения о других задачах управления, относящихся к копиям базы данных почтовых ящиков, см. См. раздел Управление копиями базы данных почтовых ящиков.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 1 минута
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Копии баз данных почтовых ящиков" в разделе Разрешения высокой доступности и устойчивости сайта .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование EAC для настройки политики активации для копии базы данных почтовых

ящиков

1. В EAC выберите **Серверы**>**Базы данных**.
2. Выберите базу данных, которую нужно настроить.
3. В области Сведения в разделе **Копии базы данных** найдите копию базы данных, которую требуется настроить, и нажмите кнопку **Приостановить**.
4. При необходимости добавьте комментарий и установите флажок **Эта копия может быть активирована только вручную**.
5. Щелкните **Сохранить** для сохранения изменений конфигурации копии базы данных почтовых ящиков.

Использование командной консоли Exchange для приостановки или возобновления копирования базы данных для активации

В этом примере показано, как заблокировать активацию копии базы данных DB1 на сервере MBX2.

PowerShell

```
Suspend-MailboxDatabaseCopy -Identity DB1\MBX2 -ActivationOnly
```

В этом примере показано, как возобновить активацию копии базы данных DB1 на сервере MBX2.

PowerShell

```
Resume-MailboxDatabaseCopy -Identity DB1\MBX2
```

Дополнительные сведения о синтаксисе и параметрах см. в разделах Suspend-MailboxDatabaseCopy или Resume-MailboxDatabaseCopy.

Настройка политики активации для сервера с помощью командной консоли Exchange

В данном примере выполняется настройка копий баз данных на сервере MBX2 как заблокированных для активации.

PowerShell

```
Set-MailboxServer -Identity MBX2 -DatabaseCopyAutoActivationPolicy Blocked
```

В данном примере выполняется настройка копий баз данных на сервере MBX3 как заблокированных для внесайтовой активации.

PowerShell

```
Set-MailboxServer -Identity MBX3 -DatabaseCopyAutoActivationPolicy
IntrasiteOnly
```

В данном примере выполняется настройка копий баз данных на сервере MBX4 как разблокированных для активации.

PowerShell

```
Set-MailboxServer -Identity MBX4 -DatabaseCopyAutoActivationPolicy
Unrestricted
```

Подробные сведения о синтаксисе и параметрах см. в разделе Suspend-MailboxDatabaseCopy, Resume-MailboxDatabaseCopy или Set-MailboxServer.

Как проверить, все ли получилось?

Чтобы убедиться, что политика активации успешно настроена, выполните одно из следующих действий:

- В командной консоли Exchange выполните следующую команду, чтобы проверить параметры активации для копии базы данных.

  PowerShell

  ```
  Get-MailboxDatabaseCopyStatus <DatabaseCopyName> | Format-List
  ActivationSuspended
  ```

- В командной консоли Exchange выполните следующую команду, чтобы проверить параметры активации для члена DAG.

  PowerShell

```
Get-MailboxServer <ServerName> | Format-List
DatabaseCopyAutoActivationPolicy
```

Обновление копии базы данных почтового ящика в Exchange Server

Статья • 04.04.2023

Обновление, также называемое *заполнением*, представляет собой процесс, в котором копия базы данных почтовых ящиков добавляется на другой сервер почтовых ящиков в группе обеспечения доступности баз данных (DAG). Только что добавленная копия становится базовой базой данных для пассивной копии, в которую воспроизводятся файлы журнала, скопированные из активной копии. Заполнение необходимо при следующих условиях:

- при создании новой пассивной копии базы данных. Заполнение может быть отложено для новой копии базы данных почтового ящика, но в конечном итоге каждая пассивная копия базы данных должна быть заполнена, чтобы функционировать в качестве избыточной копии базы данных.
- после перехода на другой ресурс при сбое, в ходе которого произошла потеря данных из-за возникшего расхождения и невозможности восстановления пассивной копии базы данных;
- если система обнаружила поврежденный файл журнала, который нельзя воспроизвести в пассивную копию базы данных;
- после автономной дефрагментации любой из копий базы данных;
- после сброса версии журнала для базы данных обратно на 1.

Заполнение можно выполнить, используя следующие методы.

- **Автоматическое заполнение**. Автоматическое начальное значение создает пассивную копию активной базы данных на целевом сервере почтовых ящиков. Автоматическое заполнение выполняется при создании новой базы данных.
- **Засеивание с помощью командлета Update-MailboxDatabaseCopy**. Вы можете в любое время использовать командлет Update-MailboxDatabaseCopy в командной консоли Exchange, чтобы заполнить копию базы данных.
- **Начальное значение с помощью мастера копирования базы данных почтовых ящиков**. Вы можете в любое время использовать мастер обновления копирования базы данных почтовых ящиков в Центре администрирования Exchange, чтобы заполнить копию базы данных.

- **Копирование автономной базы данных вручную**. Вы можете отключить активную копию базы данных и скопировать файл базы данных в то же расположение на другом сервере почтовых ящиков в том же daG. При использовании этого метода работа службы прерывается, так как этот процесс требует отключения базы данных.

Обновление копии базы данных может занять длительное время, особенно если копируемая база данных имеет большой объем, а также в случае высокой задержки сети или использования низкоскоростной сети. После запуска процесса заполнения не закрывайте EAC или командную консоль Exchange, пока процесс не завершится. В противном случае заполнение будет прервано.

Копия базы данных может быть заполнена, используя в качестве источника заполнения активную копию или актуальную пассивную копию. При заполнении из пассивной копии нужно учитывать, что операция заполнения будет прервана с ошибкой сетевого подключения при следующих обстоятельствах:

- если состояние копии источника заполнения меняется на Failed (сбой) или FailedAndSuspended (сбой и приостановлено);
- если база данных переходит на другую копию.

Несколько копий базы данных могут быть заполнены одновременно. Но при одновременном заполнении нескольких копий необходимо заполнять только файл базы данных, пропуская каталог индекса содержимого. Это можно сделать с помощью параметра *DatabaseOnly* с командлетом Update-MailboxDatabaseCopy .

> ⓘ **Примечание**
>
> Если не использовать параметр *DatabaseOnly* при заполнении нескольких целевых объектов из одного источника, задача завершится ошибкой `SeedInProgressException FE1C6491`.

Сведения о других задачах управления, относящихся к копиям базы данных почтовых ящиков, см. См. раздел Управление копиями базы данных почтовых ящиков.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 2 минуты, а также время на заполнение копии базы данных, которое зависит от ряда факторов, например

размера базы данных, скорости, доступной полосы пропускания и задержки сети, а также скорости работы хранилища.

- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Копии баз данных почтовых ящиков" в разделе Разрешения высокой доступности и устойчивости сайта .
- Копия базы данных почтовых ящиков должна быть приостановлена. Подробные инструкции см. в статье Приостановка или возобновление копирования базы данных почтового ящика.
- Службу удаленного реестра необходимо запустить на сервере, на котором размещена обновляемая пассивная копия базы данных.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Как обновить копию базы данных почтовых ящиков

Использование EAC для обновления копии базы данных почтовых ящиков

1. В EAC выберите **Серверы**>**Базы данных**.
2. Выберите базу данных почтовых ящиков, пассивную копию которой необходимо обновить.
3. В области сведений в разделе **Копии базы данных** щелкните элемент **Приостановить** под пассивной копией базы данных, которую необходимо

заполнить. Введите любые дополнительные комментарии и нажмите кнопку **сохранить**.

4. В области сведений в разделе **Копии базы данных** щелкните элемент **Обновить** под пассивной копией базы данных, которую необходимо заполнить.

5. По умолчанию в качестве источника заполнения базы данных используется активная копия базы данных. Если вы предпочитаете использовать пассивную копию базы данных для заполнения, нажмите кнопку **Обзор...** , чтобы выбрать сервер, содержащий пассивную копию базы данных, которую вы хотите использовать для источника.

6. Нажмите кнопку **сохранить**, чтобы обновить пассивную копию базы данных.

Обновление копии базы данных почтового ящика с помощью командной консоли Exchange

В данном примере показано, как заполнить копию базы данных с именем DB1 на сервере MBX1.

PowerShell

```
Update-MailboxDatabaseCopy -Identity DB1\MBX1
```

В данном примере показано, как заполнить копию базы данных с именем DB1 на сервере MBX1 с использованием сервера MBX2 в качестве исходного сервера почтовых ящиков для заполнения.

PowerShell

```
Update-MailboxDatabaseCopy -Identity DB1\MBX1 -SourceServer MBX2
```

В данном примере показано, как заполнить копию базы данных с именем DB1 на сервере MBX1 без заполнения каталога индекса содержимого.

PowerShell

```
Update-MailboxDatabaseCopy -Identity DB1\MBX1 -DatabaseOnly
```

В данном примере показано, как заполнить каталог индекса содержимого для копии базы данных с именем DB1 на сервере MBX1 без заполнения файла базы

данных.

```
PowerShell

Update-MailboxDatabaseCopy -Identity DB1\MBX1 -CatalogOnly
```

Копирование автономной базы данных вручную

1. Если для базы данных включено циклическое ведение журнала, его необходимо отключить перед продолжением работы. Циклическое ведение журнала можно отключить для базы данных почтовых ящиков с помощью командлета Set-MailboxDatabase, как показано в этом примере.

   ```
   PowerShell

   Set-MailboxDatabase DB1 -CircularLoggingEnabled $false
   ```

2. Отключите базу данных. Можно использовать командлет Dismount-Database, как показано в следующем примере.

   ```
   PowerShell

   Dismount-Database DB1 -Confirm $false
   ```

3. Вручную скопируйте файлы базы данных (файл самой базы и все файлы журнала) в другое расположение, например на внешний диск или в сетевую папку.

4. Подключите базу данных. Можно использовать командлет Mount-Database, как показано в следующем примере.

   ```
   PowerShell

   Mount-Database DB1
   ```

5. На сервере, где будет размещаться копия, скопируйте файлы базы данных с внешнего диска или из сетевой папки в тот же путь, что используется для активной копии базы данных. Например, если путь активной копии базы данных — D:\DB1\DB1.edb, а путь к файлам журнала — D:\DB1, то файлы базы

данных на сервере, где будет размещаться копия, следует скопировать в каталог D:\DB1.

6. Добавьте копию базы данных почтовых ящиков с помощью командлета Add-MailboxDatabaseCopy с параметром *SeedingPostponed* , как показано в этом примере.

```
PowerShell

Add-MailboxDatabaseCopy -Identity DB1 -MailboxServer MBX3 -
SeedingPostponed
```

7. Если для базы данных включено циклическое ведение журнала, включите его повторно с помощью командлета Set-MailboxDatabase, как показано в следующем примере.

```
PowerShell

Set-MailboxDatabase DB1 -CircularLoggingEnabled $true
```

Как проверить, все ли получилось?

Чтобы убедиться, успешно ли заполнена копия базы данных почтовых ящиков, выполните одно из следующих действий:

- В EAC перейдите в раздел **Серверы**>**Базы данных**. Выберите базу данных, которая была заполнена. В области "Сведения" отображается состояние копии базы данных и индекса ее содержимого, а также текущая длина очереди копирования.
- В командной консоли Exchange выполните следующую команду, чтобы убедиться, что копия базы данных почтового ящика успешно загружена и работоспособно.

```
PowerShell

Get-MailboxDatabaseCopyStatus <DatabaseCopyName>
```

Состояние самой копии и индекса содержимого должно быть указано как работоспособное.

Приостановка или возобновление копирования базы данных почтового ящика в Exchange Server

Статья • 04.04.2023

Может потребоваться приостановить или возобновить копию базы данных по ряду причин, таких как обслуживание на диске, который содержит копию базы данных. Кроме того, для аварийного восстановления может потребоваться приостановить активацию отдельной копии базы данных.

Сведения о других задачах управления, относящихся к копиям базы данных почтовых ящиков, см. См. раздел Управление копиями базы данных почтовых ящиков.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 1 минута
- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Копии баз данных почтовых ящиков" в разделе Разрешения высокой доступности и устойчивости сайта .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Приостановка копии базы данных почтового ящика

Использование EAC для приостановки копии базы данных почтовых ящиков

1. В EAC выберите **Серверы**>**Базы данных**.
2. Выберите базу данных, работу копии которой необходимо приостановить.
3. В области сведений в разделе **Копии базы данных** щелкните **Приостановить** у копии базы данных, которую требуется приостановить.
4. В поле **Комментарии** можно добавить необязательный комментарий до 512 символов, указывающий причины приостановки.
5. Чтобы приостановить автоматическую активацию копии базы данных, установите флажок **Эта копия может быть активирована только путем ручного вмешательства**.
6. Нажмите кнопку **Сохранить**, чтобы приостановить копию базы данных.

Приостановка копии базы данных почтового ящика с помощью командной консоли Exchange

В этом примере приостанавливается непрерывная репликация копии базы данных DB1, размещенной на сервере MBX1. Кроме того, было указано необязательное примечание.

PowerShell

```
Suspend-MailboxDatabaseCopy -Identity DB1\MBX1 -SuspendComment "Maintenance
on MBX1" -Confirm:$False
```

В этом примере приостанавливается непрерывная репликация копии базы данных DB2, размещенной на сервере MBX2.

PowerShell

```
Suspend-MailboxDatabaseCopy -Identity DB2\MBX2 -ActivationOnly -
Confirm:$False
```

Подробные сведения о синтаксисе и параметрах см. в разделе Suspend-MailboxDatabaseCopy.

Возобновление копирования базы данных почтового ящика

Использование EAC для удаления копии базы данных почтовых ящиков

1. В EAC выберите **Серверы**>**Базы данных**.
2. Выберите базу данных, работу копии которой необходимо возобновить.
3. В области сведений в разделе **Копии базы данных** щелкните **Возобновить** у копии базы данных, которую требуется возобновить.
4. Щелкните **Да**, чтобы возобновить копию базы данных.

Возобновление копирования базы данных почтового ящика с помощью командной консоли Exchange

В этом примере восстанавливается копия базы данных DB1 на сервере MBX1.

PowerShell

```
Resume-MailboxDatabaseCopy -Identity DB1\MBX1
```

В этом примере возобновляется работа копии базы данных DB2 на сервере MBX2 только для репликации.

PowerShell

```
Resume-MailboxDatabaseCopy -Identity DB2\MBX2 -ReplicationOnly
```

Подробные сведения о синтаксисе и параметрах см. в разделе Resume-MailboxDatabaseCopy.

Как проверить, все ли получилось?

Чтобы убедиться в том, что вы успешно приостановили или возобновили работу копии базы данных почтовых ящиков, выполните одно из следующих действий:

- В EAC перейдите в раздел **Серверы**>**Базы данных**. Выберите соответствующую базу данных и в области Сведения щелкните **Просмотреть сведения** , чтобы просмотреть свойства копии базы данных:
- В командной консоли Exchange выполните следующую команду, чтобы отобразить сведения о состоянии копии базы данных:

```
PowerShell

Get-MailboxDatabaseCopyStatus <DatabaseCopyName> | Format-List
```

Как активировать копию базы данных почтовых ящиков

Статья • 04.04.2023

Активация копии базы данных почтовых ящиков — это процесс назначения специальной пассивной копии в качестве новой активной копии базы данных почтовых ящиков. Этот процесс называется *переключением базы данных*. Переключение базы данных заключается в удалении текущей активной базы данных и назначении копии базы данных на указанном сервере в качестве новой активной копии базы данных почтовых ящиков. Копия базы данных, которая станет активной базой данных почтовых ящиков, должна быть действительной и функционирующей.

Сведения о других задачах управления, относящихся к копиям базы данных почтовых ящиков, см. См. раздел Управление копиями базы данных почтовых ящиков.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 1 минута
- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Копии баз данных почтовых ящиков" в разделе Разрешения высокой доступности и устойчивости сайта .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование Центра администрирования Exchange (EAC) для перемещения активной базы данных почтовых ящиков

1. В EAC выберите **Серверы**>**Базы данных**.
2. Выберите базу данных, копию которой необходимо активировать.
3. В области сведений в разделе **Копии базы данных** щелкните элемент **Активировать** под копией базы данных, которую необходимо активировать.
4. Нажмите кнопку **да**, чтобы активировать копию базы данных.

Перемещение активной базы данных почтового ящика с помощью командной консоли Exchange

В этом примере активируется и подключается копия базы данных DB4 на MBX3 как новая активная база данных почтовых ящиков. При использовании этой команды DB4 становится новой активной базой данных почтовых ящиков, и при этом не переопределяются настройки дозвона для подключения базы данных на MBX3.

PowerShell

```
Move-ActiveMailboxDatabase DB4 -ActivateOnServer MBX3 -
MountDialOverride:None
```

В данном примере выполняется переключение базы данных DB2 на почтовый сервер MBX1. После завершения команды на сервере MBX1 будет храниться активная копия DB2. Так как параметр *MountDialOverride* имеет значение `None`, MBX1 подключает базу данных с помощью собственных параметров автоматического подключения базы данных.

PowerShell

```
Move-ActiveMailboxDatabase DB2 -ActivateOnServer MBX1 -
MountDialOverride:None
```

В данном примере выполняется переключение базы данных DB1 на почтовый сервер MBX3. После выполнения команды на сервере MBX3 будет храниться

активная копия DB1. Так как параметр *MountDialOverride указан со значением* `Good Availability`, MBX3 подключает базу данных с помощью параметра автоматического подключения базы данных *GoodAvailability*.

PowerShell

```
Move-ActiveMailboxDatabase DB1 -ActivateOnServer MBX3 -
MountDialOverride:GoodAvailability
```

В данном примере выполняется переключение базы данных DB3 на почтовый сервер MBX4. После выполнения команды на сервере MBX4 будет храниться активная копия DB3. Так как значение параметра *MountDialOverride* не указано, сервер MBX4 подключает базу данных с помощью параметра автодозвона для подключения базы данных *Lossless*.

PowerShell

```
Move-ActiveMailboxDatabase DB3 -ActivateOnServer MBX4
```

В этом примере выполняется переключение сервера на почтовый сервер MBX1. Все активные копии базы данных почтовых ящиков на сервере MBX1 будут активированы на одном или нескольких других почтовых серверах с работоспособными копиями активных баз данных на сервере MBX1.

PowerShell

```
Move-ActiveMailboxDatabase -Server MBX1
```

В данном примере выполняется переключение базы данных DB4 на почтовый сервер MBX5. В этом примере копия базы данных на сервере MBX5 имеет значение очереди преобразования больше 6. В результате необходимо указать параметр *SkipLagChecks* , чтобы активировать копию базы данных в MBX5.

PowerShell

```
Move-ActiveMailboxDatabase DB4 MBX5 -SkipLagChecks
```

В данном примере выполняется переключение базы данных DB5 на почтовый сервер MBX6. В этом примере копия базы данных в MBX6 имеет *значение ContentIndexState* с ошибкой. В результате необходимо указать параметр *SkipClientExperienceChecks*, чтобы активировать копию базы данных на сервере MBX6.

PowerShell

```
Move-ActiveMailboxDatabase DB5 MBX6 -SkipClientExperienceChecks
```

Как проверить, все ли получилось?

Чтобы убедиться, успешно ли активирована копия базы данных почтовых ящиков, выполните одно из следующих действий:

- В EAC перейдите в раздел **Серверы**>**Базы данных**. Выберите подходящую базу данных, и в области "Сведения" нажмите кнопку **Просмотр сведений**, чтобы открыть свойства копии базы данных.
- В командной консоли Exchange выполните следующую команду, чтобы отобразить сведения о состоянии копии базы данных.

  PowerShell

  ```
  Get-MailboxDatabaseCopyStatus <DatabaseCopyName> | Format-List
  ```

Дополнительные сведения

Копии базы данных почтовых ящиков

Настройка свойств копии базы данных почтовых ящиков

Активация копии базы данных с отложенным почтовым ящиком

Статья • 04.04.2023

Изолированная копия базы данных почтовых ящиков — это копия базы данных почтовых ящиков со значением времени задержки преобразования, превышающим 0. Если требуется, чтобы база данных воспроизводила все файлы журналов и копировать базу данных в актуальном состоянии, активация и восстановление копии базы данных с отставанием — это простой процесс. Однако если вы хотите воспроизвести файлы журнала до определенного момента времени, это более сложная операция, так как вам нужно вручную управлять файлами журналов и запускать Eseutil.

Ищете другую информацию, связанную с отстаивая копиями базы данных почтовых ящиков? См. раздел Управление копиями базы данных почтовых ящиков.

> ⓘ **Примечание**
>
> Количество времени, необходимое для непосредственной активации изолированной копии базы данных почтовых ящиков, зависит от количества файлов журнала, которые необходимо преобразовать, и скорости их преобразования оборудованием. Минимальная скорость преобразования журнала составляет два журнала базы данных в секунду.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 1 минута плюс время, необходимое для дублирования изолированной копии, преобразования необходимых файлов журнала и извлечения данных или подключения базы данных для активности клиентов.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Копии баз данных почтовых ящиков" в разделе Разрешения высокой доступности и устойчивости сайта .
- Активируемая копия базы данных почтовых ящиков должна иметь значение времени задержки преобразования, превышающее 0.

- Активируемая копия базы данных почтовых ящиков должна иметь все файлы журнала на момент времени, к которому необходимо ее восстановить. Необходимо учесть, что транзакции базы данных могут охватывать несколько файлов журнала при определении момента времени,к которому необходимо выполнить восстановление.

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование командной консоли Exchange для активации копии базы данных почтового ящика на определенный момент времени

> **Примечание**
>
> Для активации изолированной копии базы данных почтовых ящиков к определенному моменту времени нельзя использовать Центр администрирования Exchange. Вместо этого вы выполняете ряд действий с помощью командной консоли Exchange и командной строки.

1. В этом примере с помощью командлета Suspend-MailboxDatabaseCopy приостанавливается репликация для активируемой изолированной копии.

   PowerShell

   ```
   Suspend-MailboxDatabaseCopy DB1\EX3 -SuspendComment "Activate lagged copy of DB1 on Server EX3" -Confirm:$false
   ```

2. При необходимости (для сохранения изолированной копии) сделайте копию копии базы данных и файлов ее журнала.

> ⓘ **Примечание**
>
> Если на этом этапе продолжить выполнение процедуры в существующем томе, это приведет к снижению производительности операции копирования при записи. В качестве альтернативы можно скопировать файлы базы данных и журналов в другой том, чтобы выполнить восстановление.

3. Определите, какие файлы журнала необходимо преобразовать в базу данных для выполнения восстановления на определенный момент времени (на основе даты и времени файла журнала, как показано в Проводнике Windows). Все журналы, созданные после этого момента, необходимо переместить в другой каталог до тех пор, пока процесс восстановления не закончится, а журналы больше не понадобятся.

4. Удалите файл контрольной точки (.chk) для базы данных.

5. В этом примере для выполнения операции восстановления используется программа Eseutil.

```
PowerShell

Eseutil.exe /r eXX /a
```

> ⓘ **Примечание**
>
> - Если восстанавливаемая база данных находится на месте, обязательно укажите файл журнала, контрольные точки и пути к базе данных в команде eseutil. Пример: `eseutil.exe /R E00 /a /l "c:\DBRecovery" /s "c:\DBRecovery" /d "c:\DBRecovery"`.
>
> - В предыдущем примере e *XX* — это префикс создания журнала для базы данных (например, E00, E01, E02 и т. д.).
>
> - Этот шаг может занять значительное время в зависимости от нескольких факторов, например от продолжительности времени задержки преобразования, количества файлов журнала, созданных в течение этого периода, и скорости, с которой оборудование может преобразовать эти журналы в восстановленную базу данных.

6. После завершения преобразования журнала база данных находится в состоянии чистого отключения и может быть скопирована и использована в целях восстановления.

7. В этом примере после завершения восстановления возобновляется репликация для базы данных, которая использовалась в процессе восстановления.

```
PowerShell

Resume-MailboxDatabaseCopy DB1\EX3
```

Дополнительные сведения о синтаксисе и параметрах см. в разделах Suspend-MailboxDatabaseCopy или Resume-MailboxDatabaseCopy.

Использование командной консоли Exchange для активации копии базы данных почтового ящика с отставанием путем воспроизведения всех незафиксированных файлов журнала

1. При необходимости (для сохранения изолированной копии) сделайте копию копии базы данных и файлов ее журнала.

2. В этом примере с помощью командлета Suspend-MailboxDatabaseCopy приостанавливается репликация для активируемой изолированной копии.

```
PowerShell

Suspend-MailboxDatabaseCopy DB1\EX3 -SuspendComment "Activate lagged
copy of DB1 on Server EX3" -Confirm:$false
```

3. При необходимости (для сохранения изолированной копии) сделайте копию копии базы данных и файлов ее журнала.

> **Примечание**
>
> Если на этом этапе продолжить выполнение процедуры в существующем томе, это приведет к снижению производительности операции копирования при записи. Если это нежелательно, можно скопировать

базу данных и файлы журнала на другой том для выполнения восстановления.

4. В этом примере активируется отставание копии базы данных почтового ящика с помощью командлета Move-ActiveMailboxDatabase с параметром *SkipLagChecks* .

```
PowerShell

Move-ActiveMailboxDatabase DB1 -ActivateOnServer EX3 -SkipLagChecks
```

Использование командной консоли Exchange для активации копии базы данных отложенного почтового ящика с помощью восстановления SafetyNet

1. При необходимости (для сохранения отстающей копии) сделайте с помощью службы теневого копирования томов (VSS) файловый (без учета Exchange) снимок томов, содержащий копию базы данных и файлы ее журналов.

2. В этом примере с помощью командлета Suspend-MailboxDatabaseCopy приостанавливается репликация для активируемой изолированной копии.

```
PowerShell

Suspend-MailboxDatabaseCopy DB1\EX3 -SuspendComment "Activate lagged
copy of DB1 on Server EX3" -Confirm:$false
```

3. При необходимости (для сохранения изолированной копии) сделайте копию копии базы данных и файлов ее журнала.

> **Примечание**
>
> Если на этом этапе продолжить выполнение процедуры в существующем томе, это приведет к снижению производительности операции копирования при записи. Если это нежелательно, можно скопировать базу данных и файлы журнала на другой том для выполнения восстановления.

4. Определите необходимые журналы для изолированной копии базы данных, выполнив поиск значения "Log Required:" в выходных данных заголовка базы данных ESEUTIL

   PowerShell

   ```
   Eseutil /mh <DBPath> | findstr /c:"Log Required"
   ```

   Запишите шестнадцатеричные числа в скобках. Первое число — это самый низкий необходимый номер версии (называемый LowGeneration), а второе число — самый высокий необходимый номер (называемый HighGeneration). Переместите все версии файлов журнала, порядковые номера которых превышают значение HighGeneration, в отдельную папку, чтобы не преобразовывать их в базу данных.

5. На сервере размещения активной копии базы данных удалите файлы журнала для изолированной копии, которая активируется с активной копии, или остановите работу службы репликации Microsoft Exchange.

6. Выполните переключение базы данных и активируйте изолированную копию. В этом примере описана процедура активации базы данных с помощью командлета Move-ActiveMailboxDatabase с несколькими параметрами.

   PowerShell

   ```
   Move-ActiveMailboxDatabase DB1 -ActivateOnServer EX3 -MountDialOverride
   BestEffort -SkipActiveCopyChecks -SkipClientExperienceChecks -
   SkipHealthChecks -SkipLagChecks
   ```

7. На данный момент база данных подключится автоматически и запросит повторную доставку отсутствующих сообщений из SafetyNet.

Как проверить, что все получилось?

Чтобы убедиться, что изолированная копия базы данных почтовых ящиков успешно активирована, выполните одно из следующих действий.

- В EAC перейдите в раздел **Серверы**>**Базы данных**. Выберите подходящую базу данных, и в области "Сведения" нажмите кнопку **Просмотр сведений**, чтобы открыть свойства копии базы данных.

- В командной консоли Exchange выполните следующую команду, чтобы отобразить сведения о состоянии копии базы данных.

PowerShell

```
Get-MailboxDatabaseCopyStatus <DatabaseCopyName> | Format-List
```

Удаление копии базы данных почтового ящика в Exchange Server

Статья • 04.04.2023

Эти процедуры можно использовать для удаления копии базы данных почтовых ящиков, но их нельзя использовать для удаления **последней** копии базы данных почтовых ящиков. Подробные сведения о том, как удалить последнюю копию базы данных почтовых ящиков, см. в разделе Удаление базы данных почтовых ящиков или статье Remove-MailboxDatabase.

Сведения о других задачах управления, относящихся к копиям базы данных почтовых ящиков, см. См. раздел Управление копиями базы данных почтовых ящиков.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 1 минута
- Копии базы данных почтовых ящиков можно удалить только из исправной группы доступности базы данных. Если группа доступности баз данных неисправна (например, из-за потери кворума неисправен основной кластер группы доступности баз данных), то удалить любую копию базы данных почтовых ящиков будет невозможно.
- При удалении последней пассивной копии базы данных нужно выключить циклическое ведение журнала непрерывной репликации (CRCL) для указанной базы данных почтовых ящиков. Если CRCL включено, его необходимо отключить. После удаления копии базы данных почтовых ящиков циклическое ведение журнала можно включить. После включения циклического ведения журнала для нереплицируемой базы данных почтовых ящиков вместо CRCL используется циклическое ведение журнала JET. Если не удаляется последняя пассивная копия базы данных, CRCL можно оставить включенным.
- После удаления копии базы данных необходимо вручную удалить все файлы журнала базы данных и транзакций на сервере, с которого была удалена база данных.
- Сведения об открытии Центра администрирования Exchange см. в разделе Центр администрирования Exchange в Exchange Server. Чтобы открыть

командную консоль Exchange, см. статью Запуск командной консоли Exchange.

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Копии баз данных почтовых ящиков" в разделе Разрешения высокой доступности и устойчивости сайта .

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование центра администрирования Exchange для удаления копии базы данных почтовых ящиков

1. В EAC выберите **Серверы**>**Базы данных**.
2. Выберите базу данных почтовых ящиков, копию которой необходимо удалить.
3. В области сведений найдите пассивную копию, которую необходимо удалить, и выберите команду **Удалить**.
4. Подтвердите удаление в диалоговом окне предупреждения, нажав кнопку **Да**.
5. Нажмите кнопку **ОК** для подтверждения удаления после рассмотрения любых сообщений.
6. Вручную удалите все файлы журнала базы данных и транзакций на сервере, с которого удалена база данных.

Удаление копии базы данных почтового ящика с помощью командной консоли Exchange

В этом примере копия базы данных почтовых ящиков DB1 удаляется с сервера почтовых ящиков MBX1.

PowerShell

```
Remove-MailboxDatabaseCopy -Identity DB1\MBX1 -Confirm:$False
```

Подробные сведения о синтаксисе и параметрах см. в разделе Remove-MailboxDatabaseCopy.

Как проверить, все ли получилось?

Чтобы убедиться, что копия базы данных почтовых ящиков успешно удалена, выполните одно из указанных ниже действий.

- В EAC перейдите в раздел **Серверы**>**Базы данных**. Выберите соответствующую базу данных, и в области Сведения удаленная пассивная копия больше не отображается.
- В командной консоли Exchange выполните следующую команду, чтобы проверить удаление копии.

  PowerShell

  ```
  Get-MailboxDatabase <DatabaseName> | Format-List DatabaseCopies
  ```

  Удаленная пассивная копия больше не отображается.

Мониторинг групп доступности баз данных

Статья • 04.04.2023

Сведения из этой статьи можно использовать для мониторинга копий баз данных почтовых ящиков в группах обеспечения доступности баз данных, сбора диагностических сведений и настройки порога мониторинга недостаточного места на диске.

Командлет Get-MailboxDatabaseCopyStatus

Используйте командлет Get-MailboxDatabaseCopyStatus для просмотра сведений о состоянии копий баз данных почтовых ящиков. Этот командлет позволяет просматривать сведения обо всех копиях конкретной базы данных, об определенной копии базы данных на определенном сервере или обо всех копиях баз данных на сервере. В следующей таблице приведены возможные значения состояния копий баз данных почтовых ящиков.

Состояние копии базы данных

Состояние копии базы данных	Описание
Не выполнено	Копия базы данных почтовых ящиков находится в состоянии Failed (Сбой), поскольку она не приостановлена, но не может копировать или преобразовывать файлы журналов. Пока копия базы данных не приостановлена и находится в состоянии сбоя, система будет периодически проверять, устранена ли проблема, которая привела к состоянию сбоя. После того как система обнаружит, что эта проблема устранена, и никакие другие проблемы не мешают, состояние копии автоматически изменяется на Healthy (Исправно).
Seeding	Выполняется заполнение или копии базы данных почтовых ящиков, или индекса контента или и того, и другого. После успешного завершения заполнения состояние копии должно измениться на Initializing (Инициализация).
SeedingSource	Копия базы данных почтовых ящиков используется как источник для заполнения копии базы данных.

Состояние копии базы данных	Описание
Suspended	Копия базы данных почтовых ящиков находится в состоянии Suspended (Приостановлено) в результате того, что администратор вручную приостановил эту копию базы данных, выполнив командлет **Suspend-MailboxDatabaseCopy**.
Healthy	Копия базы данных почтовых ящиков успешно копирует и преобразует файлы журналов, или она уже успешно скопировала и преобразовала все доступные файлы журналов.
ServiceDown	Служба репликации Microsoft Exchange недоступна или не работает на сервере, на котором находится эта копия базы данных.
Initializing	Копия базы данных почтовых ящиков будет находиться в состоянии инициализации, когда создана копия базы данных, когда служба репликации Microsoft Exchange запускается или только что запущена, а также во время перехода из состояния Suspended, ServiceDown, Failed, Seeding или SinglePageRestore в другое состояние. В этом состоянии система проверяет, находятся ли база данных и поток журнала в согласованном состоянии. В большинстве случаев копия находится в состоянии инициализации около 15 секунд, и во всех случаях она не должна находиться в этом состоянии долее 30 секунд.
Resynchronizing	Копия базы данных почтовых ящиков и ее файлы журналов сравниваются с действующей копией базы данных для поиска какого-либо отклонения этой копии. Копия остается в этом состоянии до тех пор, пока отклонение не будет обнаружено и устранено.
Mounted	Активная копия находится в оперативном режиме и принимает клиентские подключения. Только активная копия базы данных почтовых ящиков может находиться в состоянии "подключено".
Dismounted	Активная копия находится в автономном режиме и не принимает клиентские подключения. Только активная копия базы данных почтовых ящиков может находиться в состоянии "отключено".
Mounting	Активная копия переходит в оперативный режим и еще не принимает клиентские подключения. Только активная копия базы данных почтовых ящиков может находиться в состоянии "подключение".

Состояние копии базы данных	Описание
Dismounting	Активная копия переходит в автономный режим и завершает клиентские подключения. Только активная копия базы данных почтовых ящиков может находиться в состоянии "отключение".
DisconnectedAndHealthy	Копия базы данных почтовых ящиков больше не подключена к активной копии базы данных, но во время потери подключения она находилась в исправном состоянии. Это состояние представляет копию базы данных по отношению к ее исходной копии базы данных. Такое состояние может быть получено при сбоях сети группы обеспечения доступности баз денных между исходной и целевой копиями базы данных.
ОтключениеAndResynchronizing	Копия базы данных почтовых ящиков больше не подключена к активной копии базы данных, но во время потери подключения она находилась в состоянии повторной синхронизации. Это состояние представляет копию базы данных по отношению к ее исходной копии базы данных. Такое состояние может быть получено при сбоях сети группы обеспечения доступности баз денных между исходной и целевой копиями базы данных.
FailedAndSuspended	Состояния сбоя и приостановки установлены системой одновременно, поскольку был обнаружен сбой, и для устранения этого сбоя явно требуется вмешательство администратора. В качестве примера можно привести ситуацию, когда система обнаружила неустранимое отклонение активной базы данных почтовых ящиков от ее копии. В отличие от состояния сбоя, в данном состоянии система не будет периодически проверять, устранена ли проблема, и выполнять автоматическое восстановление. Здесь необходимо вмешательство администратора, который должен устранить причину сбоя, прежде чем копия база данных может быть переведена в исправное состояние.
SinglePageRestore	Это состояние указывает, что в копии базы данных почтовых ящиков происходит операция восстановления одной страницы.

Командлет **Get-MailboxDatabaseCopyStatus** также возвращает сведения о используемых сетях репликации, включая *IncomingLogCopyingNetwork*, который возвращается для пассивных копий базы данных, и *исходящие подключения*, возвращаемые для активных баз данных с несколькими копиями, а также все копии базы данных, используемые в качестве источника для операции заполнения

базы данных. Сведения об исходящих подключениях предоставляются для копий баз данных, находящихся в файловом режиме репликации. Сведения об исходящих подключениях не предоставляются для копий баз данных, находящихся в блочном режиме репликации.

Примеры использования командлета Get-MailboxDatabaseCopyStatus

В следующих примерах показано использование командлета **Get-MailboxDatabaseCopyStatus**. В каждом примере результат выполнения этого командлета передается в командлет **Format-List** для отображения результатов в виде списка.

В этом примере возвращаются сведения о состоянии всех копий базы данных с именем DB2.

```
PowerShell

Get-MailboxDatabaseCopyStatus -Identity DB2 | Format-List
```

В этом примере возвращаются сведения о состоянии всех копий базы данных на сервере почтовых ящиков с именем MBX2.

```
PowerShell

Get-MailboxDatabaseCopyStatus -Server MBX2 | Format-List
```

В этом примере возвращаются сведения о состоянии всех копий базы данных на локальном сервере почтовых ящиков.

```
PowerShell

Get-MailboxDatabaseCopyStatus -Local | Format-List
```

Дополнительные сведения об использовании командлета **Get-MailboxDatabaseCopyStatus** см. в разделе Get-MailboxDatabaseCopyStatus.

Командлет Test-ReplicationHealth

Командлет Test-ReplicationHealth можно использовать для просмотра сведений о состоянии непрерывной репликации копий баз данных почтовых ящиков. Этот

командлет можно использовать для проверки всех аспектов репликации и состояния преобразования, чтобы составить полный обзор конкретного сервера почтовых ящиков в группе обеспечения доступности баз данных.

Командлет **Test-ReplicationHealth** создан для профилактического наблюдения за непрерывной репликацией и конвейером непрерывной репликации, за доступностью службы Active Manager, а также за работоспособностью и состоянием внутренних служб кластеров, кворума и сетевых компонентов. Его можно выполнять локально или удаленно для любого сервера почтовых ящиков в группе обеспечения доступности баз данных. Командлет **Test-ReplicationHealth** выполняет тесты, приведенные в следующей таблице.

Тесты командлета Test-ReplicationHealth

Имя теста	Описание
ClusterService	Проверяет, работает ли служба кластеров и достижима ли она в указанном члене группы обеспечения доступности баз данных, а если член этой группы не указан, то достижима ли она на локальном сервере.
ReplayService	Проверяет, работает ли служба репликации Microsoft Exchange и достижима ли она в указанном члене группы обеспечения доступности баз данных, а если член этой группы не указан, то достижима ли она на локальном сервере.
ActiveManager	Проверяет, имеет ли экземпляр диспетчера Active Manager, работающий в указанном члене группы обеспечения доступности баз данных (или если этот член группы не указан, то на локальном сервере), допустимую роль (основной, дополнительный или отдельный).
TasksRpcListener	Проверяет, работает ли сервер Tasks RPC Server и достижим ли он в указанном члене группы обеспечения доступности баз данных, а если член этой группы не указан, то достижим ли он на локальном сервере.
TcpListener	Проверяет, работает ли прослушиватель копий журналов TCP и достижим ли он в указанном члене группы обеспечения доступности баз данных, а если член этой группы не указан, то достижим ли он на локальном сервере.
ServerLocatorService	Проверяет процессы клиента и сервера Active Manager в членах группы DAG и на сервере клиентского доступа, которые выполняют поиск в Active Directory и Active Manager для определения, активен ли почтовый ящик пользователя.

Имя теста	Описание
DagMembersUp	Проверяет, работают ли все члены группы обеспечения доступности баз данных, а также их доступность и достижимость.
ClusterNetwork	Проверяет, доступны ли все управляемые кластером сети в указанном члене группы обеспечения доступности баз данных (или на локальном сервере, если член этой группы не указан).
QuorumGroup	Проверяет, находится ли кластерная группа по умолчанию (группа кворума) в исправном и оперативном состоянии.
FileShareQuorum	Проверяет, настроен ли следящий сервер и файловый ресурс-свидетель таким образом, чтобы была достижима группа обеспечения доступности баз данных.
DatabaseRedundancy	Проверяет, существует ли хотя бы одна доступная работоспособная копия баз данных в указанном члене группы DAG, а если не указан ни один член группы DAG, то на локальном сервере.
DatabaseAvailability	Проверяет, достаточно ли доступны базы данных в указанном члене группы DAG, а если ни один член группы DAG не указан, то на локальном сервере.
DBCopySuspended	Проверяет, находятся ли какие-либо копии баз данных почтовых ящиков в приостановленном состоянии в указанном члене группы обеспечения доступности баз данных, а если член этой группы не указан, то на локальном сервере.
DBCopyFailed	Проверяет, находятся ли какие-либо копии баз данных почтовых ящиков в состоянии сбоя в указанном члене группы обеспечения доступности баз данных, а если член этой группы не указан, то на локальном сервере.
DBInitializing	Проверяет, находятся ли какие-либо копии баз данных почтовых ящиков в состоянии инициализации в указанном члене группы обеспечения доступности баз данных, а если член этой группы не указан, то на локальном сервере.
DBDisconnected	Проверяет, находятся ли какие-либо копии баз данных почтовых ящиков в отключенном состоянии в указанном члене группы обеспечения доступности баз данных, а если член этой группы не указан, то на локальном сервере.
DBLogCopyKeepingUp	Проверяет, выполняется ли копирование и проверка журнала пассивными копиями баз данных в указанном члене группы обеспечения доступности баз данных (или на локальном сервере, если этот член не указан) согласованно с действиями по созданию журнала в активной копии.

Имя теста	Описание
DBLogReplayKeepingUp	Проверяет, выполняются ли действия по преобразованию пассивных копий баз данных в указанном члене группы обеспечения доступности баз данных (или на локальном сервере, если этот член не указан) согласованно с действиями по копированию и проверке журнала.

Пример использования командлета Test-ReplicationHealth

В этом примере командлет **Test-ReplicationHealth** используется для тестирования исправности репликации сервера почтовых ящиков MBX1.

PowerShell

```
Test-ReplicationHealth -Identity MBX1
```

Ведение журнала событий канала Crimson

В Windows имеется две категории журналов событий: журналы Windows и журналы приложений и служб. В категорию журналов Windows входят журналы событий, доступные в предыдущих версиях Windows: журналы событий приложений, безопасности и системы. Кроме того, в эту категорию включены два новых журнала: журнал установки (Setup) и журнал пересылаемых событий (ForwardedEvents). Журналы Windows предназначены для хранения событий из устаревших приложений и событий, относящихся ко всей системе.

Журналы приложений и служб представляют собой новую категорию журналов событий. Эти журналы хранят события из одного приложения или компонента, а не события, которые имеют значение на уровне системы. Эта новая категория журналов событий называется каналом Crimson приложения.

В категорию журналов приложений и служб входят четыре подтипа: журналы администрирования, операционные, аналитические и отладки. События из журналов администрирования представляют особый интерес при использовании записей журналов событий для устранения проблем. События в журнале администрирования должны предоставлять рекомендации по реакции на эти события. События в операционном журнале также полезны, но для них может потребоваться дополнительная интерпретация. Журналы администрирования и отладки не понятны пользователям. Аналитические журналы (которые по

умолчанию скрыты и отключены) хранят события, отслеживающие проблему, и в них часто записывается большой объем событий. Журналы отладки используются разработчиками при отладке приложений.

Exchange Server регистрирует события в малиновые каналы в области журналов приложений и служб. Чтобы просмотреть эти каналы, сделайте следующее:

1. Откройте окно просмотра событий.
2. В дереве консоли перейдите к разделуЖурналы >**приложений и служб**Microsoft >**Exchange**.
3. В разделе **Exchange** выберите красный канал, например **HighAvailability** или **MailboxDatabaseFailureItems**, чтобы просмотреть события, связанные с группой обеспечения доступности баз данных и копией базы, либо **ActiveMontoring** или **ManagedAvailability**, чтобы просмотреть события, связанные с управляемой доступностью.

Канал HighAvailability содержит события, относящиеся к запуску и остановке службы репликации Microsoft Exchange и разным компонентам, работающим в службе репликации Microsoft Exchange, таким как диспетчер Active Manager, API синхронной репликации сторонних производителей, сервер Tasks RPC Server, прослушиватель TCP и модуль записи службы теневого копирования томов (VSS). Канал HighAvailability также используется диспетчером Active Manager для записи в журнал событий, относящихся к событиям отслеживания роли Active Manager и работы базы данных, таких как операция подключения базы данных и усечение журнала, а также для записи событий, относящихся к базовому кластеру группы обеспечения доступности баз данных.

Канал MailboxDatabaseFailureItems используется для ведения журнала событий, связанных с любыми сбоями, влияющими на реплицированную базу данных почтовых ящиков.

Канал ActiveMonitoring содержит определения и результирующие события зондов, мониторов и ответчиков управляемой доступности.

Канал ManagedAvailability содержит журналы и результаты действий по восстановлению и связанные события.

Монитор недостаточного дискового пространства

Exchange Server управляемой доступности каждую минуту отслеживает сотни системных метрик и компонентов, включая объем свободного места на томах, используемых ролью сервера почтовых ящиков. До выхода Exchange 2013 с пакетом обновления 1 (SP1) доступное пространство отслеживалось на всех локальных томах, в том числе на тех, которые не содержат базы данных или файлы журналов. В Exchange 2016 и Exchange 2019 отслеживаются только тома, содержащие базы данных Exchange и файлы журналов. Для монитора недостаточного дискового пространства по умолчанию установлен порог 180 ГБ. Вы можете изменить порог, добавив следующее значение DWORD (в МБ) в реестр на каждом сервере почтовых ящиков, который необходимо настроить:

Путь:
HKEY_LOCAL_MACHINE\Software\Microsoft\ExchangeServer\v15\Replay\Parameters

Значение: *SpaceMonitorLowSpaceThresholdInMB*

Например, чтобы установить для порога значение 100 ГБ, необходимо задать следующее значение реестра:

REG_DWORD 186a0 (100000)

Чтобы изменения вступили в силу, после настройки или изменения упомянутого выше значения реестра необходимо перезапустить службу управления Microsoft Exchange DAG.

Сценарий CollectOverMetrics.ps1

Exchange Server содержит скрипт с именем CollectOverMetrics.ps1, который можно найти в папке Скрипты. Сценарий CollectOverMetrics.ps1 читает журналы событий членов группы обеспечения доступности баз данных, чтобы получить информацию об операциях над базой данных (подключениях, перемещениях и отработках отказов) за определенный период времени. Для каждой операции сценарий фиксирует следующую информацию.

- Идентификатор базы данных
- Время начала и окончания операции
- Серверы, к которым была подключена база данных в моменты начала и окончания операции
- Причина для выполнения операции

- Завершилась ли операция успешно, включая сведения об ошибках в случае сбоя операции

Сценарий записывает эти сведения в CSV-файлы (одна операция на каждой строке). Для каждой группы обеспечения доступности баз данных создается отдельный CSV-файл.

Данный сценарий поддерживает параметры, позволяющие настроить его поведение и выходные данные. Например, результаты могут быть ограничены указанным подмножеством с помощью параметров *Database* или *ReportFilter* . В сводный отчет в формате HTML будут включены только операции, которые соответствуют критериям этих фильтров. Доступные параметры перечислены в следующей таблице.

Параметры скрипта CollectOverMetrics.ps1

Параметр	**Описание**
DatabaseAvailabilityGroup	Задает имя группы обеспечения доступности баз данных, из которой планируется собирать показатели. Если этот параметр не указан, будет использоваться группа обеспечения доступности баз данных, членом которой является локальный сервер. Для сбора информации и создания отчетов по нескольким группам обеспечения доступности баз данных можно использовать подстановочные символы.
Database	Предоставляет список баз данных, для которых необходимо создать отчет. Поддерживаются подстановочные знаки, например или `-Database:"DB1","DB2"` `-Database:"DB*"`.
StartTime	Задает продолжительность периода, за который создается отчет. Сценарий собирает только сведения о событиях, зарегистрированных в течение этого периода. В результате сценарий может фиксировать неполные записи об операциях (например, только конец операции в начале периода или наоборот). Если ни *StartTime* , ни *EndTime* не указаны, скрипт по умолчанию использует последние 24 часа. Если указан только один параметр, то будет задан период, равный 24 часам, который начинается или заканчивается в указанное время.

Параметр	Описание
EndTime	Задает продолжительность периода, за который создается отчет. Сценарий собирает только сведения о событиях, зарегистрированных в течение этого периода. В результате сценарий может фиксировать неполные записи об операциях (например, только конец операции в начале периода или наоборот). Если ни *StartTime* , ни *EndTime* не указаны, скрипт по умолчанию использует последние 24 часа. Если указан только один параметр, период будет равен 24 часам, начиная или заканчивающимися в указанное время.
ReportPath	Задает папку, используемую для хранения результатов обработки событий. Если этот параметр не указан, то будет использоваться папка скриптов. Если этот параметр указан, то сценарий использует список созданных им CSV-файлов в качестве исходных данных для сводного отчета в формате HTML. Этот отчет аналогичен отчету, который создается при помощи параметра -GenerateHtmlReport. Файлы могут создаваться для нескольких групп обеспечения доступности баз данных в разные моменты времени или даже в перекрывающиеся периоды; тогда сценарий объединяет все эти данные.
GenerateHtmlReport	Указывает, что сценарий собирает все записанные сведения, группирует данные по типу операции и создает файл в формате HTML, содержащий статистику для каждой группы. Отчет включает общее число операций в каждой группе, число операций, завершившихся сбоем, и статистику по продолжительности операций для каждой группы. Отчет также содержит разбивку по типам ошибок, которые привели к сбою операций.
ShowHtmlReport	Указывает, что созданный HTML-отчет следует сразу же отобразить в веб-браузере.
СуммыеCsvFiles	Указывает, что сценарий считывает данные из существующих CSV-файлов, которые были ранее созданы сценарием. Затем эти данные используются для создания сводного отчета, аналогичного отчету, созданному параметром *GenerateHtmlReport* .
ActionType	Указывает тип операций, сведения о которых должен собирать сценарий. Значения этого параметра: `Move`, `Mount`, `ismount` и `Remount`. Значение `Move` относится к любому моменту, когда база данных изменяет свой активный сервер, будь то управляемые перемещения или отработка отказа. Значения `Mount`, `Dismount` и `Remount` указывают время изменения состояния подключения базы данных без перемещения на другой компьютер.

Параметр	Описание
ActionTrigger	Указывает, сведения о каких административных операциях должен собирать сценарий. Значения этого параметра: `Admin` или `Automatic`. Автоматические действия выполняются системой автоматически (например, отработка отказа, когда сервер переходит в автономный режим). Администратор действия — это действия, выполненные администратором с помощью командной консоли Exchange или Центра администрирования Exchange.
RawOutput	Указывает, что сценарий передает результаты, которые были бы записаны в CSV-файлы, непосредственно в выходной поток, как в случае использования параметра Write-Output. Эти сведения впоследствии могут передаваться по конвейеру в другие команды.
ВключенныеExtendedEvents	Указывает, что сценарий собирает сведения о событиях, которые предоставляют диагностическую информацию по времени подключения баз данных. Этот этап может занимать много времени, если журнал событий приложений на серверах очень большой.
MergeCSVFiles	Указывает, что сценарий объединяет все CSV-файлы, содержащие данные по каждой операции, в один CSV-файл.
ReportFilter	Указывает, что к операциям необходимо применить фильтр с использованием полей в том виде, в котором они представлены в CSV-файлах. Этот параметр использует тот же формат, что `Where` и операция, при этом каждому элементу `$_` присвоено значение и возвращается логическое значение. Например, `{$_DatabaseName -notlike "Mailbox Database*"}` можно использовать для исключения баз данных по умолчанию из отчета.

Примеры использования сценария CollectOverMetrics.ps1

В этом примере выполняется сбор показателей для всех баз данных с именами, соответствующих шаблону "DB*" (с учетом подстановочного знака), в группе обеспечения доступности баз данных DAG1. После сбора показателей создается и отображается отчет в формате HTML.

PowerShell

```
CollectOverMetrics.ps1 -DatabaseAvailabilityGroup DAG1 -Database:"DB*" -
GenerateHTMLReport -ShowHTMLReport
```

В следующих примерах показаны способы фильтрации сводного отчета в HTML-формате. Первый использует параметр *Database* , который принимает список имен баз данных. Сводный отчет содержит данные только об этих базах данных. В следующих двух примерах используется параметр *ReportFilter* . В последнем примере отфильтровываются все базы данных по умолчанию.

PowerShell

```
CollectOverMetrics.ps1 -SummariseCsvFiles (dir *.csv) -Database
MailboxDatabase123,MailboxDatabase456
```

PowerShell

```
CollectOverMetrics.ps1 -SummariseCsvFiles (dir *.csv) -ReportFilter
{$_.DatabaseName -notlike "Mailbox Database*"}
```

PowerShell

```
CollectOverMetrics.ps1 -SummariseCsvFiles (dir *.csv) -ReportFilter
{($_.ActiveOnStart -like "ServerXYZ*") -and ($_.ActiveOnEnd -notlike
"ServerXYZ*")}
```

Сценарий CollectReplicationMetrics.ps1

CollectReplicationMetrics.ps1 — это еще один скрипт метрик работоспособности, включенный в Exchange Server. Этот сценарий представляет собой активную форму наблюдения, поскольку он собирает показатели в режиме реального времени в ходе выполнения. Сценарий CollectReplicationMetrics.ps1 собирает данные, полученные от счетчиков производительности, которые относятся к репликации баз данных. Этот сценарий собирает данные счетчиков с нескольких серверов почтовых ящиков, записывает данные каждого сервера в CSV-файл и создает отчеты по различным статистическим показателям для всех этих данных (например, по таким показателям, как период, в течение которого каждая копия находилась в состоянии сбоя или приостановки, средняя длина очереди копирования или преобразования или период, в течение которого для копий не выполнялись критерии отработки отказа).

Можно указать либо каждый сервер по отдельности, либо всю группу обеспечения доступности баз данных. Можно либо запустить сценарий, чтобы сначала собрать данные и затем создать отчет, либо запустить его только для сбора данных или

только для создания отчета по уже собранным данным. Можно указать частоту и общую продолжительность сбора данных.

The data collected from each server is written to a file named **CounterData.<ServerName>.<TimeStamp>.csv**. Сводный отчет будет записан в файл **с именем HaReplPerfReport.< DAGName>.< Метка> времени.csv**или **HaReplPerfReport.< Метка> времени.csv** , если вы не выполняли скрипт с параметром *DagName* .

Сценарий запускает задания Windows PowerShell для сбора данных с каждого сервера. Эти задачи выполняются в течение всего периода сбора данных. Если пользователь указывает много серверов, этот процесс может занять значительный объем памяти. Заключительный этап процесса — обработка данных для сводного отчета — может также занять много времени в случае большого объема данных. Можно выполнить этап сбора информации на одном компьютере, а затем скопировать данные на другой компьютер для обработки.

Сценарий CollectReplicationMetrics.ps1 поддерживает параметры, позволяющие настроить его поведение и выходные данные. Доступные параметры перечислены в следующей таблице.

Параметры скрипта CollectReplicationMetrics.ps1

Параметр	Описание
DagName	Задает имя группы обеспечения доступности баз данных, из которой планируется собирать показатели. Если этот параметр не указан, будет использоваться группа обеспечения доступности баз данных, членом которой является локальный сервер.
DatabaseNames	Предоставляет список баз данных, для которых необходимо создать отчет. Поддерживаются подстановочные знаки, например или `-DatabaseNames:"DB1","DB2"` `-DatabaseNames:"DB*"`.
ReportPath	Задает папку, используемую для хранения результатов обработки событий. Если этот параметр не указан, то будет использоваться папка скриптов.
Duration	Задает время, которое должен работать процесс сбора. Обычными значениями являются 1-3 часа. Большую продолжительность следует указывать только при длительных интервалах между выборками или в виде серии коротких операций, выполняемых в рамках запланированных задач.
Frequency	Указывает частоту, с которой должны собираться показатели данных. Обычными значениями являются 30 секунд, 1 минута или 5 минут. При нормальных условиях более короткие интервалы не покажут значительных отличий между выборками.

Параметр	Описание
Servers	Указывает идентификатор серверов, с которых собирается статистика. Можно указать любое значение, включая подстановочные символы или идентификаторы GUID.
Суммарные файлы	Указывает список CSV-файлов для создания сводного отчета. Эти файлы являются файлами **с именем CounterData.< CounterData>*** и создаются скриптом CollectReplicationMetrics.ps1.
Режим	Указывает этапы обработки, которые выполняет сценарий. Можно использовать следующие значения: `CollectAndReport`: это значение по умолчанию. Это значение указывает, что сценарий должен собирать данные с серверов и затем обрабатывать их для создания сводного отчета. `CollectOnly`: это значение означает, что скрипт должен просто собирать данные, а не создавать отчет. `ProcessOnly`: это значение означает, что скрипт должен импортировать данные из набора .csv файлов и обрабатывать их для создания сводного отчета. Параметр *SummariseFiles* используется для предоставления скрипту списка файлов для обработки.
MoveFilestoArchive	Указывает, что сценарий должен переместить файлы в сжатую папку после обработки.
LoadExchangeSnapin	Указывает, что скрипт должен загружать команды командной консоли Exchange. Этот параметр полезен, когда скрипт должен выполняться из-за пределов командной консоли Exchange, например в запланированной задаче.

Пример использования сценария CollectReplicationMetrics.ps1

В следующем примере показан сбор данных в течение одного часа с минутными интервалами со всех серверов в группе обеспечения доступности баз данных DAG1, а затем создание сводного отчета. Кроме того, используется параметр *ReportPath*, поэтому сценарий помещает все файлы в текущий каталог.

PowerShell

```
CollectReplicationMetrics.ps1 -DagName DAG1 -Duration "01:00:00" -Frequency
"00:01:00" -ReportPath
```

В следующем примере показано чтение данных из всех файлов, отвечающих критерию "CounterData*", и затем создание сводного отчета.

PowerShell

```
CollectReplicationMetrics.ps1 -SummariseFiles (dir CounterData*) -Mode
ProcessOnly -ReportPath
```

Переключения и отработки отказа

Статья • 04.04.2023

Переключения и отработка отказа — это две формы сбоев в Microsoft Exchange Server:

- *Переключение* — это запланированный сбой базы данных или сервера, явно инициированный командлетом или управляемой системой доступности в Exchange Server. Переключения обычно выполняются во время подготовки к обслуживанию. Переключения предполагают перемещение активной копии базы данных почтового ящика на другой сервер группы обеспечения доступности баз данных (DAG). Если при переключении не удается найти ни одной подходящей целевой базы данных, администратор получит уведомление об ошибке, а база данных почтового ящика не будет отключена.
- *Отработка отказа* подразумевает неожиданные события, которые могут приводить к недоступности служб, данных или тех и других. Отработка отказа включает в себя автоматическое восстановление системы после сбоя путем активации пассивной копии базы данных почтового ящика и ее преобразования в активную. Если при отработке отказа не удается найти ни одной подходящей целевой базы данных, база данных почтового ящика будет отключена.

Exchange Server предназначена для обработки переключений и отработок отказа.

Ищете задачи управления, связанные с высоким уровнем доступности и устойчивостью сайта? См. статью Управление высоким уровнем доступности и устойчивостью сайта.

Переключения

В Exchange Server существует три типа переключений:

- Переключения базы данных.
- Переключения сервера.
- Переключения центра данных.

Переключения базы данных

Переключение базы данных — это процесс, в ходе которого одна активная база данных переключается на другую (пассивную) копию базы данных, которая затем становится новой активной копией базы данных. Переключения базы данных могут происходить как внутри центров данных, так и между ними. Переключение базы данных можно выполнить с помощью Центра администрирования Exchange (EAC) или командной консоли Exchange. Вне зависимости от используемого интерфейса, процесс переключения выполняется следующим образом.

1. Администратор инициирует переключение базы данных, чтобы переместить текущую активную копию базы данных почтовых ящиков на другой сервер.
2. Клиент, используемый при выполнении задачи, отправляет вызов RPC в службу репликации Microsoft Exchange участника группы доступности базы данных (DAG).
3. Участник группы DAG может не выполнять обработку роли основного диспетчера Active Manager (PAM). В этом случае он переводит задачу на сервер, которому принадлежит роль PAM.
4. В рамках этой задачи выполняется вызов RPC в службу репликации Microsoft Exchange сервера, которому принадлежит роль PAM.
5. Диспетчер PAM считывает и обновляет сведения о местоположении базы данных, которые хранятся в базе данных кластера для группы доступности DAG.
6. Диспетчер PAM подключается к службе репликации Microsoft Exchange участника группы DAG, пассивная копия которой активируется в качестве новой активной копии базы данных почтовых ящиков.
7. Служба репликации Microsoft Exchange на целевом сервере отправляет запросы к службам репликации Microsoft Exchange всех участников группы DAG для определения наилучшего источника журнала копии базы данных.
8. База данных отключается от текущего сервера, и служба репликации Microsoft Exchange на целевом сервере копирует оставшиеся журналы на целевой сервер.

9. Служба репликации Microsoft Exchange на целевом сервере отправляет запросы о подключении базы данных.
10. Служба банка данных Microsoft Exchange на целевом сервере преобразует файлы журналов и подключает базу данных.
11. Коды ошибок возвращаются в службу репликации Microsoft Exchange на целевом сервере.
12. Диспетчер PAM обновляет сведения о состоянии копии базы данных в базе данных кластера для группы доступности DAG.
13. Служба репликации Microsoft Exchange на целевом сервере возвращает коды ошибок в службу репликации Microsoft Exchange диспетчера PAM.
14. Служба репликации Microsoft Exchange диспетчера PAM возвращает все ошибки на интерфейс администрирования, с которого выполнялся вызов задачи.
15. Приложение Remote PowerShell возвращает результаты операции на вызывающий интерфейс администрирования.

Дополнительные сведения о переключении базы данных см. в разделе Активация копии базы данных почтовых ящиков.

Переключения сервера

Переключение сервера — это процесс, в ходе которого все активные базы данных участника группы DAG активируются для одного или нескольких других участников этой группы. Как и при переключении баз данных, переключение сервера может происходить как в центре обработки данных, так и в разных центрах обработки данных. Его можно инициировать с помощью центра администрирования Exchange и командной консоли Exchange. Вне зависимости от используемого интерфейса, процесс переключения сервера выполняется следующим образом.

1. Администратор инициирует переключение сервера, чтобы переместить все текущие активные копии базы данных почтовых ящиков на один или несколько других серверов.
2. В рамках данной задачи для каждой активной базы данных на текущем сервере выполняются действия, описанные выше в этом разделе для переключений базы данных (шаги 2-4).
3. Диспетчер PAM считывает и обновляет сведения о местоположении базы данных, которые хранятся в базе данных кластера для группы доступности DAG.
4. Диспетчер PAM подключается к службе репликации Microsoft Exchange каждого участника группы DAG, для которого активируется пассивная копия.
5. Служба репликации Microsoft Exchange на целевых серверах отправляет запросы к службам репликации Microsoft Exchange всех других участников группы DAG для определения наилучшего источника журнала копии базы данных.
6. База данных отключается от текущего сервера, и служба репликации Microsoft Exchange на каждом целевом сервере копирует оставшиеся журналы.
7. Служба репликации Microsoft Exchange на каждом целевом сервере отправляет запросы о подключении базы данных.
8. Служба банка данных Microsoft Exchange на каждом целевом сервере преобразует файлы журналов и подключает базу данных.
9. Коды ошибок возвращаются в службу репликации Microsoft Exchange на целевом сервере.
10. Диспетчер PAM обновляет сведения о состоянии копии базы данных в базе данных кластера для группы доступности DAG.
11. Служба репликации Microsoft Exchange на целевом сервере возвращает коды ошибок в службу репликации Microsoft Exchange диспетчера PAM.
12. Служба репликации Microsoft Exchange диспетчера PAM возвращает все ошибки на интерфейс администрирования, с которого выполнялся вызов задачи.
13. Приложение Remote PowerShell возвращает результаты операции на вызывающий интерфейс администрирования.

Подробные инструкции по переключении сервера см. в разделе Выполнение переключения сервера.

Переключения центра обработки данных

В устойчивой конфигурации сайта автоматическое восстановление в ответ на сбой на уровне сайта может происходить в DAG, что позволяет системе обмена сообщениями оставаться в функциональном состоянии. Для этой конфигурации требуется по

крайней мере три расположения, так как необходимо развернуть члены DAG в двух расположениях и сервер-свидетель DAG в третьем расположении.

Если у вас нет трех расположений или даже если у вас есть три расположения, но вы хотите управлять действиями по восстановлению на уровне центра обработки данных, вы можете настроить DAG для восстановления вручную, если произойдет сбой на уровне сайта. В этом случае выполняется процесс под названием *переключение центра обработки данных*. Так же как и для многих сценариев аварийного восстановления, предварительное планирование и подготовка к переключению центра данных позволяют упростить процесс восстановления и сократить время отключения. Подробные инструкции по переключении центра обработки данных см. в разделе Переключение центра обработки данных.

Отработки отказов

Отработка отказа — это процедура автоматической активации, которая может выполняться на уровне базы данных, сервера или центра обработки данных. Отработки отказов происходят в ответ на сбой, который оказал влияние на отдельную базу данных (например, потеря данных в изолированном хранилище), на весь сервер (например, сбой материнской платы или потеря питания) или на весь сайт (например, потеря всех членов группы DAG на сайте).

Группы доступности базы данных (DAG) и копии базы данных почтовых ящиков обеспечивают полную избыточность и быстрое восстановление как данных, так и служб, обеспечивающих доступ к этим данным. В следующей таблице перечислены ожидаемые действия по восстановлению при различных сбоях. В одних случаях запустить процесс восстановления должен администратор, в других — ошибки автоматически обрабатываются системой.

Описание	**Автоматическая активация**	**Автоматическое действие по восстановлению**	**Состояние при восстановлении: активная**	**Состояние при восстановлении: пассивная**	**Действия по восстановлению**	**Comments**
«Мягкий» сбой базы данных расширенного обработчика хранилищ (ESE): диски, на которых хранится база данных, возвращают ошибки при некоторых операциях чтения (например, ошибка -1018).	Возможное кратковременное отключение. Возможная автоматическая отработка отказа.	Автоматическое исправление поврежденной страницы.	Ручное переключение, автоматическая отработка отказа или оперативное восстановление.	Сбой	Перестройка RAID, восстановление базы данных и копии базы данных, восстановление и запуск отладки, затем исправление страницы или исправление страницы на основе копии.	Могут возникать и другие "мягкие" ошибки базы данных. Сюда не включены сбои блока файловой системы NTFS. При переключении или отработке отказа выполняется обновление хост-сервера.
Сбой базы данных ESE "*semi-soft*" : диски, на которых хранится база данных, возвращают ошибки при некоторых операциях записи.	Кратковременное отключение во время автоматической отработки отказа.	Автоматическое перестроение тома/диска после возможной замены диска.	Отключено, если отсутствует возможность восстановления.	Сбой	Перестроение с помощью RAID может решить проблему. Копирование и исправление, восстановление и запуск отладки или перестроение тома/диска после возможной замены.	"Полумягкая" ошибка при операции записи обработчика ESE означает, что некоторые записи являются успешными. Сюда не включен сбой блока файловой системы NTFS.

Описание	Автоматическая активация	Автоматическое действие по восстановлению	Состояние при восстановлении: активная	Состояние при восстановлении: пассивная	Действия по восстановлению	Comments
"Полумягкий" сбой журнала обработчика ESE: диски, на которых хранятся данные журнала, возвращают невосстановимые ошибки при некоторых операциях записи и чтения.	Кратковременное отключение во время автоматической отработки отказа.	Автоматическое перестроение тома/диска после возможной замены диска.	Отключено, если отсутствует возможность восстановления.	Сбой	Перестроение с помощью RAID может решить проблему. Копирование и исправление, восстановление и запуск отладки или перестроение тома/диска после возможной замены.	"Полумягкая" ошибка чтения/записи обработчика ESE означает, что некоторые операции чтения/записи являются успешными. При сбое базы данных автоматическое восстановление запускается до начала процесса восстановления данных журнала.
Программная ошибка обработчика ESE или нехватка ресурсов: ошибка, при которой обработчик ESE завершает работу экземпляра (например, событие с идентификатором 1022, глубина контрольной точки слишком большая).	Кратковременное отключение во время автоматической отработки отказа.	Нет.	Отключено, если отсутствует возможность восстановления.	Сбой	Устранение ошибки базового ресурса.	Этот сбой может быть проявлением ошибок в других случаях.
Сбои блока NTFS: на дисках, содержащих базу данных или журналы, произошла ошибка операции чтения или записи в структуре управления NTFS.	Кратковременное отключение во время автоматической отработки отказа.	Повторное восстановление тома после возможной замены диска.	Отключено, если отсутствует возможность восстановления.	Сбой	Перестроение с помощью RAID может решить проблему. Служебные программы NTFS могут решить проблемы в блоке NTFS. Возможно, потребуется восстановление Exchange.	Эта ситуация, скорее всего, возникнет, когда RAID не используется. Если этот сценарий влияет на активный том журнала, некоторые последние файлы журнала будут потеряны. Сюда не включены ошибки, автоматически исправленные системой NTFS либо ее базовым программным или аппаратным стеком.

Описание	Автоматическая активация	Автоматическое действие по восстановлению	Состояние при восстановлении: активная	Состояние при восстановлении: пассивная	Действия по восстановлению	Comments
Сбой диска базы данных или журнала. Диск, на котором хранится база данных или журналы, завершился сбоем и недоступен.	Кратковременное отключение во время автоматической отработки отказа.	Диск переформатирован или заменен. Том полностью перестроен.	Отключено, если отсутствует возможность восстановления.	Сбой	Замена диска, возможно, с последующим перестроением RAID. Замена диска с последующим полным перестроением тома. Полное перестроение тома.	Неприменимо.
Сбой базы данных или тома журнала: произошел сбой тома из-за проблем в системе NTFS или на нижнем уровне тома.	Кратковременное отключение во время автоматической отработки отказа.	Диск переформатирован или заменен.	Отключено, если отсутствует возможность восстановления.	Сбой	Замена диска, возможно, с последующим перестроением RAID. Замена диска с последующим полным перестроением тома. Полное перестроение тома.	Неприменимо.
Недостаточно места в базе данных или в томе журнала: недостаточно места в файловой системе NTFS, в которой находится база данных или файлы журнала.	Автоматическая обработка отказа, если другая копия находится в ином состоянии.	Нет.	Отключено.	Сбой	Запуск полной или добавочной архивации, удаление журнала вручную, ожидание завершения операции, возобновление копирования базы данных или восстановление поврежденной копии базы данных.	Неприменимо.
Администратор отключает неправильную базу данных.	Если автоматическая отработка отказа не заблокирована администратором, отключение будет кратковременным. Если автоматическая отработка отказа запрещена, отключение будет продолжаться до тех пор, пока не будет подключена база данных.	Нет.	Отключено.	Неприменимо	Ошибку исправляет администратор.	Неприменимо.

Описание	Автоматическая активация	Автоматическое действие по восстановлению	Состояние при восстановлении: активная	Состояние при восстановлении: пассивная	Действия по восстановлению	Comments
Администратор приостанавливает неправильную копию базы данных.	В зависимости от конфигурации и задействованной копии автоматическое восстановление может быть запрещено.	Нет.	Неприменимо.	Приостановка	Ошибку исправляет администратор.	Неприменимо.
Администратор отключает обслуживание базы данных хранилища, NTFS или тома.	Если автоматическая отработка отказа не заблокирована администратором, отключение будет кратковременным. Если автоматическая отработка отказа заблокирована, отключение будет продолжаться до тех пор, пока администратор не завершит задачу.	Нет.	Отключено.	Неприменимо	Задачу завершает администратор.	Неприменимо.
Администратор приостанавливает обслуживание копии базы данных хранилища, NTFS или тома.	В зависимости от конфигурации и задействованной копии автоматическое восстановление может быть запрещено.	Нет.	Неприменимо.	Приостановка	Действия завершает администратор.	Неприменимо.
Администратор отключает базу данных для обслуживания в автономном режиме.	Отключение до тех пор, пока не будет выполнено восстановление.	Нет.	Отключено.	Приостановка	Действия завершает администратор.	Активная и пассивная копии базы данных не совпадают. Администратору необходимо приостановить копии.
Сбой сети хранения данных (SAN), диска или контроллера хранилища.	Кратковременное отключение во время автоматической отработки отказа.	Нет.	Отключено.	Любое	Восстановление оборудования.	Пассивная копия базы данных будет находиться в состоянии, которое существовало во время сбоя системы.
Обслуживание оборудования сервера.	Кратковременное отключение во время автоматической отработки отказа (если не заблокировано администратором).	Нет.	Отключено.	Любое	Завершение действий.	Пассивная копия базы данных будет находиться в состоянии, которое существовало во время завершения работы системы.

Описание	Автоматическая активация	Автоматическое действие по восстановлению	Состояние при восстановлении: активная	Состояние при восстановлении: пассивная	Действия по восстановлению	Comments
Обслуживание программного обеспечения сервера.	Кратковременное отключение во время автоматической отработки отказа (если не заблокировано администратором).	Нет.	Отключено.	Любое	Завершение действий.	Пассивная копия базы данных будет находиться в состоянии, которое существовало во время завершения работы системы.
Служба банка данных Microsoft Exchange остановлена или приостановлена администратором.	Кратковременное отключение во время автоматической отработки отказа.	Нет.	Отключено.	Любое	Перезапустите службу банка данных Microsoft Exchange.	Неприменимо.
Сбой службы банка данных Microsoft Exchange. Операционная система по-прежнему работает.	Кратковременное отключение во время автоматической отработки отказа.	Диспетчер служб перезапускает службу банка данных Microsoft Exchange.	Отключено.	Любое	Перезапуск службы банка данных Microsoft Exchange вручную или автоматически.	Пассивная копия базы данных будет находиться в состоянии, которое существовало во время сбоя службы банка данных Microsoft Exchange.
Частичный отказ службы банка данных Microsoft Exchange. Часть хранилища Exchange прекращает функционировать, но это не считается полным отказом.	Возможное кратковременное отключение во время автоматической отработки отказа.	Нет.	Подключено и частично функционирует.	Любое, но, возможно, частично функционирующее	Перезагрузка сервера, перезапуск операционной системы или службы банка данных Microsoft Exchange.	Неприменимо.
Сбой сервера. Сбой сервера по одной из следующих причин: Полный отказ питания Невосстановимая поломка микросхемы процессора, материнской платы или объединительной платы Ошибка остановки операционной системы Операционная система не отвечает на запросы Полный сбой связи	Кратковременное отключение во время автоматической отработки отказа.	Перезагрузка компьютера.	Отключено.	Любое	Восстановление питания, изменение параметров операционной системы, изменение параметров оборудования, замена оборудования, перезапуск операционной системы, обслуживание операционной системы, обслуживание оборудования или устранение проблем связи.	Неприменимо.

Описание	Автоматическая активация	Автоматическое действие по восстановлению	Состояние при восстановлении: активная	Состояние при восстановлении: пассивная	Действия по восстановлению	Comments
Сбой кворума в группе доступности базы данных.	Отключение до тех пор, пока не будет выполнено восстановление.	Нет.	Отключено.	Любое	Восстановление неисправного кворума, назначение нового кворума или восстановление сети, ставшей причиной неисправности кворума.	Пассивная копия базы данных будет находиться в состоянии, которое существовало во время сбоя системы.
Сбой связи в сети MAPI: сервер больше не доступен в сети MAPI.	Кратковременное отключение во время автоматической отработки отказа. Потерь данных быть не должно.	Нет. Попытки установки связи продолжают выполняться.	Отключено.	Любое	Устранение неполадки в оборудовании или программном обеспечении для решения проблемы связи.	Неприменимо.
Сбой связи в сети репликации: серверу не удается получить сигналы подтверждения, копии журнала или заполнение через поврежденную сеть репликации.	Возможно кратковременное отключение копирования или заполнения во время переключения нагрузки на другую сеть.	Нет. Попытки установки связи продолжают выполняться.	Нет.	Любое	Устранение неполадки в оборудовании или программном обеспечении для решения проблемы связи.	Сбой оказал влияние на устойчивость.
Множественные ошибки сетевой связи: серверу не удается получить сигналы подтверждения, копии журнала или заполнение через несколько сетей.	Кратковременное отключение во время автоматической отработки отказа. Потерь данных быть не должно.	Нет. Попытки установки связи продолжают выполняться.	Отключено.	Любое	Устранение неполадки в оборудовании или программном обеспечении для решения проблемы связи.	По-прежнему работает по крайней мере дна сеть.
Частичный сбой одной или нескольких сетей: в сетях возникают ошибки с высокой скоростью.	Ошибка не обнаружена; никаких действий.	Нет.	Подключено, но возможны проблемы с производительностью.	Любое	Устранение неполадки в оборудовании или программном обеспечении для решения проблемы связи.	Скорости возникновения ошибок в сетях превышают обычные.
Невыявленное зависание операционной системы: операционная система перестает отвечать на запросы, но это не выявлено системой мониторинга или кластеризации.	Нет.	Нет.	Любое.	Любое	Перезапуск или отключение неотвечающих ресурсов.	Зависание не выявлено, поэтому никакие действия не предпринимаются. Возможно, некоторые функциональные возможности являются действующими.
Сбой диска с операционной системой.	Кратковременное отключение во время автоматической отработки отказа.	Нет.	Отключено.	Любое	Замена диска и перестроение сервера или перестроение тома с помощью RAID.	Неприменимо.

Описание	Автоматическая активация	Автоматическое действие по восстановлению	Состояние при восстановлении: активная	Состояние при восстановлении: пассивная	Действия по восстановлению	Comments
Недостаточно места на диске с операционной системой.	Кратковременное отключение во время автоматической отработки отказа.	Нет.	Отключено.	Любое	Освобождение места в томе вручную.	Неприменимо.
На диске с двоичными файлами Exchange возникает сбой тома или диска.	Кратковременное отключение во время автоматической отработки отказа.	Нет.	Отключено.	Любое	Замена диска и переустановка приложения или перестроение тома с помощью RAID.	Неприменимо.
Недостаточно места на диске с двоичными файлами Exchange.	Кратковременное отключение во время автоматической отработки отказа.	Нет.	Отключено.	Любое	Освобождение места в томе вручную.	Неприменимо.
Обнаружен недопустимый новый журнал: последовательность журнала прерывается существующим файлом.	Кратковременное отключение во время автоматической отработки отказа; возможно, с другими копиями не возникло такой проблемы.	Нет.	Отключено.	Сбой	Удаление аварийных журналов после определения источника.	Не следует реплицировать аварийные журналы.
При непрерывной репликации обнаружен недопустимый журнал: при преобразовании обнаружен несоответствующий журнал во время операции копирования или преобразования.	Неприменимо.	Удаление журнала.	Неприменимо.	Сбой	Удаление недопустимого журнала; перемещение потока журналов, оказывающих негативное воздействие.	Неприменимо.

Отработки отказов в базах данных

Отработка отказа в базах данных происходит, когда активная копия базы данных больше не может оставаться активной. Следующие вхождения являются частью отработки отказа базы данных:

1. Служба банка данных Microsoft Exchange обнаруживает сбой в базе данных.
2. Служба банка данных Microsoft Exchange записывает сбои в журнал событий канала crimson.
3. Диспетчер Active Manager на сервере, на котором находится неисправная база данных, обнаруживает события сбоя.
4. Диспетчер Active Manager запрашивает сведения о состоянии копии базы данных у других серверов, на которых хранится копия базы данных.
5. Другие серверы возвращают диспетчеру Active Manager запрошенные сведения о состоянии копии базы данных.
6. PAM инициирует перемещение активной базы данных на другой сервер в группе DAG с использованием процесса выбора лучших копий.
7. Диспетчер PAM обновляет местоположение подключения базы данных в базе данных кластера для обращения к выбранному серверу.
8. Диспетчер PAM отправляет запрос диспетчеру Active Manager на выбранном сервере о его назначении главным сервером для этой базы данных.

9. Диспетчер Active Manager на выбранном сервере отправляет запрос в службу репликации Microsoft Exchange на создание копии последних журналов с предыдущего сервера и устанавливает флажок подключения для этой базы данных.
10. Служба репликации Microsoft Exchange копирует журналы с сервера, на котором ранее находилась активная копия базы данных.
11. Диспетчер Active Manager считывает номер последней версии журнала из базы данных кластера.
12. Служба банка данных Microsoft Exchange подключает новую активную копию базы данных.

Отработки отказов на серверах

Отработка отказа на сервере происходит, если участник группы DAG больше не может обслуживать сеть MAPI или служба кластеров участника группы DAG больше не может поддерживать связь с оставшимися участниками этой группы. Следующие вхождения являются частью отработки отказа сервера:

1. Служба кластеров диспетчера PAM отправляет уведомление этому диспетчеру в одном из двух случаев:
2. **Узел вниз**: сервер доступен, но не может участвовать в операциях DAG.
3. **Сеть MAPI отключена**. С сервером нельзя связаться по сети MAPI и, следовательно, не может участвовать в операциях DAG.
4. Если сервер доступен, диспетчер PAM подключается к диспетчеру Active Manager на поврежденном сервере и запрашивает немедленное отключение всех баз данных.
5. Для каждой поврежденной копии базы данных выполняется следующее:
6. Диспетчер PAM запрашивает сведения о состоянии копии базы данных у всех серверов в группе DAG.
7. Диспетчер PAM получает ответ от всех доступных и активных участников группы DAG.
8. Диспетчер PAM пытается определить наилучший источник журнала на всех отвечающих серверах, запрашивая у каждого номер последней версии журнала.
9. Каждый сервер сообщает в ответ номер версии журнала.
10. Диспетчер PAM извлекает текущее состояние каталога индекса поиска из базы данных кластера.
11. На основе номера версии журнала и работоспособности каталога каждой копии базы данных диспетчер PAM выбирает лучшие копии для активации.
12. Диспетчер PAM обновляет подключенное местоположение базы данных в базе данных кластера.
13. Диспетчер PAM инициирует отработку отказа в базе данных, связываясь с диспетчером Active Manager на одном или нескольких серверах.
14. Диспетчер Active Manager на выбранных серверах запрашивает службу репликации Microsoft Exchange на копирование последних журналов с предыдущего сервера и установку флажка подключения.
15. Если база данных является подключаемой, диспетчер Active Manager на серверах подключает базы данных.

Дополнительные сведения о процессе выбора лучших копий диспетчером Active Manager см. в разделе Активный диспетчер.

Отработки отказа в центрах обработки данных

После Exchange 2010 были внесены значительные изменения в конфигурацию устойчивости сайта. Благодаря упрощению пространства имен, консолидации ролей сервера, разделению служб клиентского доступа и восстановлению DAG (в Exchange Server пространство имен не требуется перемещаться вместе с DAG), а также изменениями в отношении балансировки нагрузки Exchange Server предоставляет варианты устойчивости сайта, такие как возможность использовать одно глобальное пространство имен. Если у вас есть более двух расположений для развертывания компонентов службы обмена сообщениями, Exchange Server также включает настройку службы обмена сообщениями для автоматической отработки отказа в ответ на сбои, которые требовали вмешательства вручную в предыдущих версиях.

Exchange использует отказоустойчивость, встроенную в пространство имен, с помощью нескольких IP-адресов, балансировки нагрузки и, при необходимости, возможности принимать серверы в эксплуатацию и не работать. Exchange Server позволяет использовать возможность клиентов кэшировать несколько IP-адресов, возвращенных с DNS-сервера в ответ на запрос

разрешения имен. Клиенты с возможностью кэширования нескольких IP-адресов (включая почти все клиенты на основе HTTP в Exchange Server, такие как Outlook, Outlook Anywhere, EAS, EWS, Outlook в Интернете, EAC, RPS и т. д.), могут использовать эти несколько IP-адресов, что обеспечивает отработку отказа на стороне клиента. Вы можете настроить DNS для передачи нескольких IP-адресов клиенту в процессе разрешения имен. Клиент запрашивает mail.contoso.com и получает, например, 2 или 4 IP-адреса. Клиент будет использовать несколько полученных IP-адресов. Это упрощает работу клиента, поскольку если один из IP-адресов не работает, клиент имеет несколько других вариантов подключения. Если клиент пробует один адрес и тот не работает, клиент ждет 20 секунд, а затем пробует следующий адрес в списке. Таким образом, если вы потеряете подключение к основному массиву служб клиентского доступа (CAS) и у вас есть второй опубликованный IP-адрес для второго массива CAS, восстановление для клиентов происходит автоматически (и примерно через 21 секунду).

Современные HTTP-клиенты (операционные системы и веб-браузеры, которым не более десяти лет) работают с этой избыточностью автоматически. Стек HTTP может принимать несколько IP-адресов для полного доменного имени, и если первый IP-адрес, который он пытается выполнить сбой (например, не удается подключиться), он попытается использовать следующий IP-адрес в списке. При обратимом сбое (подключение потеряно после установки сеанса из-за периодических сбоев в службе, когда, например, устройство удаляет пакеты и должно быть удалено из службы), пользователю может потребоваться обновить браузер.

При правильной конфигурации отработка отказа может происходить на уровне клиента, и клиенты будут автоматически перенаправляться во второй центр обработки данных, где запущены службы клиентского доступа, а серверы, на которых выполняются службы клиентского доступа, будут прокси-сервером обмена данными обратно с сервером почтовых ящиков пользователя, который остается не затронутым сбоем (так как переключение не выполняется). Вместо того, чтобы восстанавливать службу, служба восстанавливается сама, и вы можете сосредоточиться на устранении основной проблемы (например, замене подсистемы балансировки нагрузки, которая завершилась сбоем).

Благодаря быстрой отработке отказа пространства имен между центрами обработки данных все, что требуется для отработки отказа центра обработки данных, — механизм отработки отказа роли сервера почтовых ящиков в центрах обработки данных. Для автоматической отработки отказа для группы DAG необходимо просто разработать решение, при котором группа равномерно распределяется между двумя центрами обработки данных, а затем разместить следящий сервер в третьем расположении для его арбитража членами группы DAG в каждом центре обработки данных (вне зависимости от состояния сети между центрами обработки данных с членами этой группы). Очень важно то, что третье расположение изолированно от сетевых сбоев, влияющих на расположения с членами группы DAG.

Если у вас всего два центра обработки данных и вы хотите настроить автоматический отработку отказа, можно использовать Microsoft Azure в качестве третьего расположения. Вам потребуется создать виртуальную сеть Azure и подключить ее к двум центрам обработки данных с помощью виртуальной частной сети из нескольких точек. Затем вы сможете разместить следящий сервер на виртуальной машине Microsoft Azure. Дополнительные сведения см. в статье Using a Microsoft Azure VM as a DAG witness server.

Переключения центра данных.

Статья • 04.04.2023

В устойчивой конфигурации сайта автоматическое восстановление в ответ на сбой на уровне сайта может происходить в DAG, что позволяет системе обмена сообщениями оставаться в функциональном состоянии. Для этой конфигурации требуется по крайней мере три расположения, так как необходимо развернуть члены DAG в двух расположениях и сервер-свидетель DAG в третьем расположении.

Если у вас нет трех расположений или даже если у вас есть три расположения, но вы хотите управлять действиями по восстановлению на уровне центра обработки данных, вы можете настроить DAG для восстановления вручную в случае сбоя на уровне сайта. В этом случае выполняется процесс под названием *переключение центра обработки данных*. Как и для многих сценариев аварийного восстановления, предварительное планирование и подготовка к переключению центра обработки данных позволяют упростить процесс восстановления и сократить время отключения.

Существует четыре основных шага, которые необходимо выполнить для переключения центра данных после принятия первоначального решения активировать второй центр данных.

1. **Завершение частично работающего центра обработки данных**. Этот шаг включает прекращение работы служб Exchange в основном центре обработки данных, если какие-либо службы по-прежнему запущены. Этот шаг имеет большое значение для роли сервера почтовых ящиков, так как для нее используется активная/пассивная модель высокого уровня доступности. Если службы в частично неисправном центре данных не остановлены, этот центр данных может вызвать неполадки, которые негативно повлияют на службы во время переключения на основной центр данных.

   > **ⓘ Важно!**
   >
   > Если надежность сети или инфраструктуры Active Directory снизилась из-за сбоя основного центра данных, рекомендуется отключить все службы обмена сообщениями, пока эти зависимости не будут восстановлены до состояния работоспособности службы.

2. **Проверка и подтверждение предварительных требований для второго центра обработки данных**. Этот шаг можно выполнить параллельно с шагом 1, так как проверка работоспособности инфраструктуры во втором центре обработки данных в значительной степени не зависит от первого центра обработки данных. Каждой организации обычно требуется собственный метод выполнения этого шага. Например, при его выполнении можно просмотреть сведения о работоспособности, собранные и отфильтрованные с помощью приложения отслеживания инфраструктуры, или использовать уникальное для инфраструктуры организации средство. Это критически важный шаг, так как вы не хотите активировать второй центр обработки данных, когда его инфраструктура неработоспособна и нестабильна.

3. **Активация серверов почтовых ящиков**. На этом шаге начинается процесс активации второго центра обработки данных. Этот шаг можно выполнить параллельно с шагом 4, так как службы Microsoft Exchange могут обрабатывать сбои базы данных и восстанавливаться. Активация серверов почтовых ящиков включает в себя процессы пометки неисправных серверов из основного центра данных как недоступных и последующей активации серверов во втором центре данных. Процесс активации серверов почтовых ящиков зависит от того, находится ли группа обеспечения доступности баз данных в режиме координации активации баз данных. Дополнительные сведения см. в разделе Режим координации активации центра обработки данных .

   Если группа обеспечения доступности баз данных находится в режиме координации активации баз данных, для завершения работы частично неисправного центра данных (при необходимости) и активации серверов почтовых ящиков можно использовать командлеты для устойчивости сайта Exchange. Например, в режиме координации активации баз данных этот шаг выполняется с помощью командлета Stop-DatabaseAvailabilityGroup. В некоторых случаях необходимо дважды пометить серверы как недоступные (по одному разу в каждом центре данных). Затем выполняется запуск командлета Restore-DatabaseAvailabilityGroup для восстановления оставшихся членов группы обеспечения доступности баз данных во втором центре данных и сокращения членов группы обеспечения доступности баз данных до действующих, для чего повторно устанавливается кворум. Если группа обеспечения доступности баз данных не находится в режиме координации активации баз данных, для активации серверов почтовых ящиков необходимо использовать средства для отказоустойчивого кластера Windows. После завершения любой из описанных процедур можно активировать и

подключить копии баз данных, которые были пассивными во втором центре данных. На этом этапе восстановление сервера почтовых ящиков завершено.

4. **Активация служб клиентского доступа**. Это включает использование сведений о сопоставлении URL-адресов и методологии изменения системы доменных имен (DNS) для выполнения всех необходимых обновлений DNS. Сведения о сопоставлении включают в себя данные об изменениях службы DNS, которые необходимо выполнить. Время, необходимое для завершения обновления, зависит от используемой методологии и параметров времени жизни (TTL) записи DNS (а также от того, учитывает ли инфраструктура развертывания TTL).

Пользователям может потребоваться доступ к службам обмена сообщениями после выполнения шагов 3 и 4. Шаги 3 и 4 описаны подробнее далее в этом разделе.

Завершение работы частично неисправного центра данных

Если какие-либо члены группы обеспечения доступности баз данных в неисправном центре данных все еще работают, необходимо завершить их работу.

Если exchange DAG находится в режиме приложения уровня данных, серверы в сбое центра обработки данных можно отключить с помощью одной команды. Это позволит подключить базы данных в другом центре обработки данных, даже если daG не имеет кворума (более половины членов DAG доступно).

Если группа обеспечения доступности баз данных находится в режиме координации активации баз данных, для завершения работы членов группы обеспечения доступности баз данных в основном центре данных необходимо выполнить следующие действия.

1. Члены DAG в основном центре обработки данных должны быть помечены как остановлены в основном центре обработки данных. *Остановлено* — это состояние Active Manager, которое предотвращает подключение баз данных, и Active Manager на каждом сервере в сбое центра обработки данных помещается в это состояние с помощью командлета Stop-DatabaseAvailabilityGroup . Параметр *ActiveDirectorySite* этого командлета можно использовать, чтобы пометить все серверы в основном центре обработки данных как остановленные одной командой. Этот шаг может оказаться невозможным в зависимости от сбоя. Этот шаг следует выполнить, если это разрешено состоянием центра обработки данных. Командлет **Stop-**

DatabaseAvailabilityGroup должен выполняться на всех серверах в основном центре обработки данных. Если сервер почтовых ящиков недоступен, но Active Directory работает в основном центре обработки данных, команда **Stop-DatabaseAvailabilityGroup** с параметром *ConfigurationOnly* должна быть запущена на всех серверах в этом состоянии в основном центре обработки данных или сервер почтовых ящиков должен быть отключен. Если не отключить серверы почтовых ящиков в неисправном центре обработки данных или выполнить команду **Stop-DatabaseAvailabilityGroup** на серверах, это может привести к возникновению синдрома разделения мозга в двух центрах обработки данных. Для удовлетворения этого требования может потребоваться по отдельности отключить компьютеры с помощью устройств управления питанием.

2. На этом шаге необходимо обновить второй центр данных, чтобы получить сведения о том, какие серверы основного центра данных остановлены. Для этого выполните ту же команду **Stop-DatabaseAvailabilityGroup** с параметром *ConfigurationOnly* , используя тот же параметр *ActiveDirectorySite* и указав имя сайта Active Directory в первичном центре обработки данных, в котором произошел сбой. Целью этого шага является отправка на серверы во втором центре данных сведений о том, какие серверы почтовых ящиков можно использовать при восстановлении службы.

Если группа обеспечения доступности баз данных не находится в режиме координации активации баз данных, для завершения работы членов группы обеспечения доступности баз данных в основном центре данных необходимо выполнить следующие действия.

1. Чтобы принудительно исключить членов группы обеспечения доступности баз данных в основном центре данных из базового кластера группы обеспечения доступности баз данных, необходимо выполнить на каждом члене группы следующую команду:

```
PowerShell
```

```
net stop clussvc
```

```
PowerShell
```

```
cluster <DAGName> node <DAGMemberName> /forcecleanup
```

2. Затем необходимо перезапустить члены группы обеспечения доступности баз данных во втором центре данных, чтобы завершить процесс исключения из

второго центра данных. Остановите службу кластера на каждом члене группы обеспечения доступности баз данных во втором центре данных посредством запуска следующей команды на каждом члене:

```
PowerShell

net stop clussvc
```

3. На члене группы обеспечения доступности баз данных во втором центре данных запустите принудительное формирование кворума службы кластера с помощью следующей команды:

```
PowerShell

net start clussvc /forcequorum
```

4. Откройте средство управления отказоустойчивости кластеров и подключитесь к базовому кластеру DAG. Разверните кластер, а затем узел **Узлы**. Щелкните правой кнопкой мыши каждый узел в основном центре обработки данных, выберите **Дополнительные действия**, а затем выберите **Вытеснить**. Завершив вытеснение членов DAG в основном центре обработки данных, закройте средство управления отказоустойчивости кластеров.

Если в сбое центра обработки данных используются какие-либо службы единой системы обмена сообщениями, они должны быть отключены, чтобы предотвратить маршрутизацию вызовов в сбойный центр обработки данных. Вы можете отключить службы единой системы обмена сообщениями с помощью командлета Disable-UMService (например, `Disable-UMService EX1`). Кроме того, если вы используете шлюз VoIP, вы также можете удалить записи сервера из шлюза VoIP или изменить записи DNS для серверов, завершившихся сбоем, чтобы они указывали на IP-адрес серверов во втором центре обработки данных, если шлюз VoIP настроен для маршрутизации вызовов с помощью DNS.

> ⓘ **Примечание**
>
> Единая система обмена сообщениями недоступна в Exchange 2019

Активация серверов почтовых ящиков

Эти шаги, необходимые для активации серверов почтовых ящиков во время переключения центра данных, также зависят от того, находится ли группа

обеспечения доступности баз данных в режиме координации активации баз данных. Перед активацией членов группы обеспечения доступности баз данных во втором центре данных рекомендуется проверить готовность служб инфраструктуры во втором центре данных к активации службы обмена сообщениями.

Если группа обеспечения доступности баз данных находится в режиме координации активации баз данных, для активации серверов почтовых ящиков во втором центре данных выполните следующие действия.

1. Необходимо остановить службу кластеров для каждого участника группы доступности базы данных во втором центре данных. Вы можете использовать командлет **Stop-Service** , чтобы остановить службу (например, `Stop-Service ClusSvc`), или использовать `net stop clussvc` из командной строки с повышенными привилегиями.

2. Затем необходимо активировать серверы почтовых ящиков в резервном центре данных с помощью командлета Restore-DatabaseAvailabilityGroup. Сайт Active Directory резервного центра данных передается в командлет **Restore-DatabaseAvailabilityGroup** для определения того, какие серверы будут использоваться для восстановления службы и настройки группы доступности баз данных на использование другого сервера свидетеля. Если альтернативный следящий сервер ранее не был настроен, его можно настроить с помощью параметров *AlternateWitnessServer* и *AlternateWitnessDirectory* командлета Restore-DatabaseAvailabilityGroup . При успешном выполнении этой команды критерии кворума сужаются до серверов в резервном центре данных. Если количество серверов в этом центре данных является четным, группа доступности базы данных будет использовать дополнительный следящий сервер, определенный с помощью параметра объекта группы доступности базы данных.

3. Теперь можно активировать базы данных. В зависимости от определенной конфигурации, используемой в организации, активация может выполняться автоматически или вручную. При установке для серверов в резервном центре данных параметра блокировки активации система не будет выполнять автоматический переход из основного центра данных в резервный центр данных любой базы данных. Если в резервном центре данных отсутствуют ограничения для перехода на другой ресурс при сбое для всех копий базы данных, система автоматически активирует копии во втором центре данных, рассматривая их работоспособными. Если для баз данных установлен параметр блокировки активации, требующий явного выполнения активации вручную, активацию можно выполнить двумя способами.

4. Снимите флажок с параметра, который блокирует активацию. Система возвращается к поведению по умолчанию, при котором выполняется активация любой доступной копии.

5. Чтобы активировать базу данных во втором центре данных, не снимайте флажок с этого параметра и используйте командлет Move-ActiveMailboxDatabase. Если параметр блокировки активации включен, для выполнения этого шага с помощью командлета **Move-ActiveMailboxDatabase** необходимо явным образом определить цель перемещения.

6. Последний шаг — просмотреть все сообщения об ошибках и предупреждения для задач. Необходимо просмотреть и исправить все указанные предупреждения. Модель разработки задач для этих команд не будет правильной, только если не будут достигнуты основные цели для этой разработки. Например, выполнение командлета **Restore-DatabaseAvailabilityGroup** не будет успешным, если не удалось сузить кворум группы доступности базы данных, чтобы разрешить перезапуск сервера во втором центре данных для обслуживания без отключения кворума. Тем не менее, все выходные данные задач используются для определения проблем, требующих административной поддержки. Рекомендуется сохранять все выходные данные задач и просматривать их на наличие действий, требующих административной поддержки.

Если группа обеспечения доступности баз данных находится в режиме координации активации баз данных, для завершения активации серверов почтовых ящиков во втором центре данных выполните следующие действия.

1. На основании числа членов группы обеспечения доступности баз данных во втором центре данных измените кворум.

2. Если число членов группы обеспечения доступности баз данных является нечетным, измените модель кворума с большинства общих файловых ресурсов и сайтов на набор большинства сайтов с помощью следующей команды:

   PowerShell

   ```
   cluster <DAGName> /quorum /nodemajority
   ```

3. Если число членов группы обеспечения доступности баз данных является четным, перенастройте следящий сервер и каталог, запустив в командной консоли Exchange следующую команду:

```
PowerShell

Set-DatabaseAvailabilityGroup <DAGName> -WitnessServer <ServerName>
```

4. Запустите службу кластера на всех оставшихся членах группы обеспечения доступности баз данных во втором центре данных с помощью следующей команды:

```
PowerShell

net start clussvc
```

5. Выполните переключение сервера, чтобы активировать базы данных почтовых ящиков в группе обеспечения доступности баз данных, запустив на каждом члене группы обеспечения доступности баз данных следующую команду:

```
PowerShell

Move-ActiveMailboxDatabase -Server <DAGMemberinPrimarySite> -
ActivateOnServer <DAGMemberinSecondSite>
```

6. Подключите базы данных почтовых ящиков на каждом члене группы обеспечения доступности баз данных на втором сайте с помощью следующей команды:

```
PowerShell

Get-MailboxDatabase <DAGMemberinSecondSite> | Mount-Database
```

Активация служб клиентского доступа

Клиенты подключаются к конечным точкам службы (например, Outlook в Интернете, автообнаружение, Exchange ActiveSync, Любой Outlook, POP3, IMAP4 и массиву служб клиентского доступа RPC) для доступа к службам и данным Exchange. Таким образом, активация служб клиентского доступа включает изменение сопоставления записей DNS для этих конечных точек службы с IP-адресов в основном центре обработки данных с IP-адресами во втором центре обработки данных, настроенными в качестве новых конечных точек службы. В зависимости от конфигурации DNS изменяемые записи DNS могут быть в той же зоне DNS или в различных зонах.

Активация служб клиентского доступа

Клиенты будут автоматически подключены к новым конечным точкам служб одним из двух способов.

- Клиенты продолжат попытки подключения и будут автоматически подключены по истечении срока жизни исходной записи DNS и записи в кэше службы DNS клиента. Пользователи также могут выполнить `ipconfig /flushdns` команду из командной строки, чтобы вручную очистить свой кэш DNS.

- Клиенты, запускающие или перезапуска, будут выполнять поиск DNS при запуске и получат новый IP-адрес для конечной точки службы, которая будет являться сервером Exchange Server, на котором запущены службы клиентского доступа, или массив служб клиентского доступа во втором центре обработки данных.

При условии, что все соответствующие изменения конфигурации были завершены для определения и настройки служб во втором центре обработки данных для работы в том же виде, в который они находились в основном центре обработки данных, и при условии, что установленная конфигурация DNS является правильной, никаких дополнительных изменений для активации служб клиентского доступа не потребуется.

Активация служб транспорта

Клиенты и другие серверы, которые отправляют сообщения, обычно определяют эти серверы с помощью службы DNS. Процесс активации транспортных служб во втором центре обработки данных включает в себя изменение записей DNS для указания IP-адресов серверов почтовых ящиков во втором центре обработки данных. Клиенты и серверы отправки будут автоматически подключены к серверам во втором центре обработки данных одним из двух способов.

- Клиенты продолжат попытки подключения и будут автоматически подключены по истечении срока жизни исходной записи DNS и записи в кэше службы DNS клиента. Пользователи также могут выполнить `ipconfig /flushdns` команду из командной строки, чтобы вручную очистить свой кэш DNS.

- С помощью запуска или перезапуска клиентов можно выполнить поиск DNS при запуске и получить новый IP-адрес для конечной точки SMTP, которая станет сервером почтовых ящиков во втором центре обработки данных.

Если все соответствующие изменения конфигурации выполнены для определения и настройки работоспособности служб во втором центре обработки данных, идентичной их работоспособности в основном центре обработки данных, а также если установленная конфигурация DNS правильная, не требуется выполнять другие изменения для активации транспортных служб.

Активация служб единой системы обмена сообщениями в Exchange 2016

> ⓘ **Примечание**
>
> Единая система обмена сообщениями не доступна в Exchange 2019.

Службы единой системы обмена сообщениями (UM) в Exchange 2016 подключаются к системе УАТС и телефонным линиям организации. Логическое подключение между системой УАТС и службой единой системы обмена сообщениями выполняется с помощью шлюза IP. Шлюзы IP включают в себя функцию высокого уровня доступности и позволяют переключаться между несколькими службами единой системы обмена сообщениями при обнаружении сбоя.

Если во втором центре обработки данных есть службы единой системы обмена сообщениями, которые находятся в отключенном состоянии, так как они предназначены для решения для обеспечения устойчивости сайта, их можно включить с помощью командлета Enable-UMService (например, `Enable-UMService EX4`).

Если шлюзы IP связаны со службами единой системы обмена сообщениями с помощью серверов DNS, процесс активации служб единой системы обмена сообщениями будет также включать в себя изменение записей DNS для указания новых IP-адресов, которые будут настроены для службы единой системы обмена сообщениями во втором центре обработки данных. Если все соответствующие изменения конфигурации выполнены для определения и настройки работоспособности служб во втором центре обработки данных, идентичной их работоспособности в основном центре обработки данных, а также если установленная конфигурация DNS является правильной, не требуется выполнять другие изменения для активации служб единой системы обмена сообщениями.

Если используемый шлюз IP не поддерживает имена DNS для разрешения служб единой системы обмена сообщениями, потребуется выполнить дополнительные

шаги конфигурации, чтобы вручную указать для IP-шлюза IP-адреса служб единой системы обмена сообщениями во втором центре обработки данных.

Активация пограничных транспортных серверов

Эти шаги необходимы для активации роли пограничного транспортного сервера и зависят от определенной конфигурации. Для пограничных транспортных серверов в двух центрах данных можно настроить активную/пассивную или активную/активную конфигурацию. В активной/пассивной конфигурации пограничный транспортный сервер во втором центре данных не используется, пока второй центр данных не будет активирован. В активной/активной конфигурации пограничные транспортные серверы в обоих центрах данных выполняют непрерывную доставку почты.

В активной/активной конфигурации не требуется выполнять шаги для активации пограничных транспортных серверов второго центра данных, так как они уже запущены. В активной/пассивной конфигурации необходимо обновить запись ресурса DNS MX для каждого домена SMTP при переключении с основного центра данных на резервный центр данных. Активная/активная конфигурация обеспечивает простое решение переключения центра данных, но она имеет недостаток, требующий тщательного отслеживания нагрузки, чтобы убедиться, что после переключения центра данных пограничные транспортные серверы во втором центре данных могут обеспечить достаточную емкость для поддержки повышенной нагрузки, проходящей через нее, так как пограничные транспортные серверы в основном центре данных будут недоступны.

Даже при использовании активной/активной конфигурации может потребоваться обновление записей ресурсов MX для пограничных транспортных серверов во время переключения центра данных. Если запись ресурса MX для неисправного центра данных будет указывать на неисправный центр данных, при запуске восстановления центра данных могут выполняться попытки подключения к пограничным транспортным серверам неисправного центра данных. Это может произойти, когда службы пограничного транспортного сервера находятся в нестабильном состоянии (например, из-за того, что зависимые службы в центре данных восстанавливаются).

Если записи DNS находятся под управлением организации, процесс активации пограничных транспортных серверов включает в себя обновление записи ресурса MX для каждого домена SMTP, размещенного на сервере.

> ⓘ **Примечание**

Если запись ресурса MX, используемая организацией, не размещена на сервере DNS, которым управляет организация, можно указать ссылку на запись CNAME в записи ресурса MX и использовать запись CNAME под управлением организации. Запись CNAME затем можно обновить.

Обновления DNS включают входящий трафик, а исходящий трафик обрабатывается при активации баз данных почтовых ящиков на сайте, на котором работают пограничные транспортные серверы.

- Если входящие подключения SMTP инициируются с помощью обновленных сведений о разрешении имен, клиенты SMTP будут подключаться к пограничным транспортным серверам во втором центре данных. Маршрутизация трафика будет выполняться соответствующим образом с помощью пограничного транспортного сервера и дальнейшие изменения не потребуются.

- Если исходящие подключения SMTP инициированы, будет выполнена попытка подключения к локальному доступному пограничному транспортному серверу, а такие сообщения будут отправлены в очередь или отправлены немедленно в зависимости от состояния принимающего сервера.

Восстановление службы для основного центра данных

Обычно, ошибки центра данных являются временным или постоянными. При наличии постоянной ошибки, например события, которое приведет к разрушению основного центра данных, будет невозможно активировать основной центр данных. Тем не менее, при наличии временной ошибки (например, длительной потери питания или обширного, но восстанавливаемого повреждения), будет невозможно полностью восстановить основной центр данных.

Процесс восстановления службы для неисправного центра данных называется *обратным переключением*. Шаги, используемые для обратного переключения центра данных, аналогичны шагам, используемым для переключения центра данных. Важным отличием является то, что обратное переключение центра данных является запланированным и продолжительность отключения обычно намного короче.

Обратите внимание, что обратное переключение можно выполнить только после повторной активации зависимостей инфраструктуры для Exchange, перехода их в стабильное рабочее состояние и проверки этих зависимостей. Если эти

зависимости недоступны и неработоспособны, процесс обратного переключения может привести к более длительному отключению, чем ожидалось, а также может произойти сбой выполнения процесса.

Обратное переключение роли сервера почтовых ящиков

Обратное переключение в основной центр данных необходимо выполнить в первую очередь для роли сервера почтовых ящиков. В следующих шагах подробно описан процесс обратного переключения роли сервера почтовых ящиков.

1. Во время процесса переключения центра данных был выполнен перевод серверов почтовых ящиков в основном центре данных в остановленное состояние. Если среда (например, основной центр данных, зависимости Exchange и подключение к глобальной сети) готова, первым шагом является перевод серверов почтовых ящиков в восстановленном основном центре данных в начальное состояние и добавление их в группу доступности базы данных. Используемый способ зависит от того, находится ли группа обеспечения доступности баз данных в режиме координации активации баз данных.

    a. Если группа обеспечения доступности баз данных находится в режиме координации активации баз данных, можно повторно добавить члены группы обеспечения доступности баз данных в основной сайт с помощью командлета Start-DatabaseAvailabilityGroup. После этого выполните командлет Set-DatabaseAvailabilityGroup для группы доступности базы данных, чтобы убедиться, что группа использует правильную модель кворума.

    b. Если группа обеспечения доступности баз данных не находится в режиме координации активации баз данных, можно повторно добавить члены группы обеспечения доступности баз данных в основной сайт с помощью командлета Add-DatabaseAvailabilityGroupServer.

2. После добавления серверов почтовых ящиков в основном центре данных в группу доступности базы данных потребуется некоторое время для синхронизации копий баз данных. В зависимости от причин сбоя, длительности отключения и действий, выполняемых администратором во время отключения, может потребоваться повторное заполнение копий базы данных. Например, если во время отключения выполняется удаление копий базы данных из неисправного основного центра данных, чтобы разрешить усечение файла журнала для исправных активных копий во втором центре

данных, потребуется повторное заполнение. С этого момента можно обрабатывать каждую отдельную базу данных. После восстановления работоспособности реплицированной копии базы данных в основном центре данных можно перейти к следующему шагу.

> ⓘ **Примечание**
>
> При выполнении этого процесса не требуется одновременное перемещение всех баз данных. Рекомендуется одновременно перемещать большую часть баз данных организации, но некоторые базы данных сильно задерживаются во втором центре данных при наличии проблем, связанных с копиями баз данных в основном центре данных.

3. После восстановления работоспособности большей части баз данных в основном центре данных можно запланировать отключение обратного переключения. В запланированное время необходимо выполнить следующие шаги.

   a. Во время процесса переключения центра данных группа доступности базы данных была настроена для использования дополнительного следящего сервера. Необходимо повторно настроить группу доступности базы данных для использования следящего сервера в основном центре данных. Если вы используете тот же следящий сервер и следящий каталог, которые использовались до сбоя основного центра обработки данных, можно выполнить `Set-DatabaseAvailabilityGroup -Identity DAGName` команду . Если планируется использовать сервер или каталог свидетеля, отличные от исходного сервера и каталога свидетеля, используйте команду Set-DatabaseAvailabilityGroup для требуемой настройки параметров сервера и каталога свидетеля.

   b. Базы данных, повторно активированные в основном центре данных, необходимо отключить во втором центре данных. Чтобы отключить базы данных, используйте командлет Dismount-Database.

   c. После отключения баз данных URL-адреса серверов, на которых выполняются службы клиентского доступа, должны быть перемещены из второго центра обработки данных в основной центр обработки данных. Это достигается путем изменения записи DNS для URL-адресов, чтобы она указывала на сервер служб клиентского доступа или массив в основном центре обработки данных. Это приведет к тому, что система будет работать

как при выполнении перехода на другой ресурс при сбое для каждой перемещаемой базы данных.

> **Важно!**
>
> Не переходите к следующему шагу до тех пор, пока не будут перемещены URL-адреса серверов, на которых выполняются службы клиентского доступа, а срок жизни DNS и записей кэша истек. Активация баз данных в основном центре обработки данных перед перемещением URL-адресов в основной центр обработки данных приведет к недопустимой конфигурации (например, подключенной базе данных, которая не имеет служб клиентского доступа, запущенных на сайте Active Directory).

4. Так как каждая база данных в основном центре данных находится в работоспособном состоянии, ее можно активировать в основном центре данных с помощью переключения баз данных. Для этого используйте командлет Move-ActiveMailboxDatabase для каждой базы данных, которую необходимо активировать.

5. После перемещения всех баз данных в основной центр данных его можно подключить с помощью командлета Mount-Database.

После активации и подключения одной или нескольких баз данных в основном центре данных можно выполнять процедуры обратного переключения для других ролей сервера.

Переключение служб клиентского доступа

В рамках процесса переключения внутренние и внешние записи DNS, используемые клиентами, другими серверами и IP-шлюзами для разрешения конечных точек службы для служб клиентского доступа, служб транспорта и единой системы обмена сообщениями, а также пограничных транспортных серверов, были изменены таким образом, чтобы они указывали на соответствующие конечные точки во втором центре обработки данных. Процесс обратного переключения для других ролей сервера включает в себя изменение этих записей для указания на конечные точки восстановленной службы в основном центре данных.

Кроме того, как и с изменениями DNS, внесенными во время переключения на второй центр данных, клиенты, серверы и шлюзы IP будут выполнять попытки

подключения и будут автоматически подключены после истечения срока жизни исходной записи DNS и записи в кэше DNS.

Повторная установка устойчивости сайтов

После успешного переключения на основной центр обработки данных можно восстановить устойчивость сайта для основного центра обработки данных, проверив работоспособность и состояние каждой копии базы данных почтового ящика во втором центре обработки данных. Кроме того, если какие-либо копии базы данных во втором центре обработки данных изначально были заблокированы для активации, вы можете перенастроить эти параметры в настоящее время.

Выполнение переключения сервера

Статья • 04.04.2023

Переключение сервера является частью процесса подготовки к запланированному отключению текущего сервера почтовых ящиков.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 30 секунд на базу данных
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Группы доступности баз данных" в разделе Разрешения высокой доступности и устойчивости сайта .

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Переключение сервера с помощью Центра администрирования Exchange

Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Копии баз данных почтовых ящиков" в разделе Разрешения высокой доступности и устойчивости сайта .

1. В EAC перейдите в раздел **Серверы**>.
2. Выберите сервер почтовых ящиков, на который требуется переключиться.
3. В области сведений выберите команду **Переключить сервер**.
4. На странице **Переключение сервера** выполните одно из указанных ниже действий.
5. Не изменяйте параметр по умолчанию **Автоматически выбрать конечный сервер** (в этом случае система автоматически выберет наиболее подходящий

сервер почтовых ящиков для каждой переключаемой базы данных) и нажмите кнопку **сохранить**.

6. Выберите пункт **Использовать указанный сервер как цель для переключения**, нажмите кнопку **Обзор**, чтобы выбрать сервер почтовых ящиков, а затем нажмите кнопку **сохранить**.

7. После завершения переключения нажмите кнопку **закрыть**, чтобы выйти со страницы **Переключение сервера**.

Использование командной консоли Exchange для переключения сервера

В этом примере выполняется переключение сервера MBX1. Система автоматически выбирает наиболее подходящий сервер почтовых ящиков для каждой активной базы данных сервера MBX1.

PowerShell

```
Move-ActiveMailboxDatabase -Server MBX1
```

В этом примере выполняется переключение сервера почтовых ящиков MBX4. После завершения выполнения команды сервер MBX5 размещает активную копию баз данных, которые были ранее активны на сервере MBX4.

PowerShell

```
Move-ActiveMailboxDatabase -Server MBX4 -ActivateOnServer MBX5
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе Move-ActiveMailboxDatabase.

Резервное копирование, восстановление и аварийное восстановление в Exchange Server

Статья • 04.04.2023

Планирование защиты данных — это сложный процесс, основанный на многочисленных решениях, принимаемых на этапе планирования развертывания. В рамках планирования важно понимать способы защиты данных, а также определять, какой метод лучше всего соответствует потребностям вашей организации.

Традиционно резервные копии использовались в таких сценариях:

- **Аварийное восстановление**. В случае сбоя оборудования или программного обеспечения несколько копий базы данных в DAG обеспечивают высокий уровень доступности с быстрой отработкой отказа и практически без потери данных. Это позволяет избежать простоя и результирующей потери производительности, что приводит к значительным затратам на восстановление после резервного копирования на прошлый момент времени на диск или ленту. DaG можно расширить на несколько сайтов и обеспечить устойчивость к сбоям диска, сервера, сети и центра обработки данных.

- **Восстановление случайно удаленных элементов**. Исторически сложилось так, что в ситуации, когда пользователь удалял элементы, которые позже требовалось восстановить, он включал поиск резервного носителя, на котором хранились данные, которые необходимо восстановить, а затем каким-то образом получить нужные элементы и предоставить их пользователю. С помощью папки "Элементы с возможностью восстановления" в Exchange 2016 и Exchange 2019 и политики удержания, которая может быть применена к ней, можно хранить все удаленные и измененные данные в течение указанного периода времени, поэтому восстановление этих элементов будет проще и быстрее. Это снижает нагрузку на администраторов Exchange и службу технической поддержки, позволяя конечным пользователям самостоятельно восстанавливать случайно удаленные элементы, тем самым уменьшая сложность и административные расходы, связанные с восстановлением отдельных элементов. Дополнительные сведения см. в разделах Политика обмена сообщениями и соответствие требованиям в Exchange Server и Защита от потери данных в Exchange Server.

- **Долгосрочное хранение данных**. Резервные копии также используются в качестве архива, и обычно лента используется для хранения моментальных снимков данных на определенный момент времени в течение длительных периодов времени в соответствии с требованиями соответствия. Новые функции архивации, поиска по нескольким почтовым ящикам и хранения сообщений в Exchange Server обеспечивают механизм эффективного хранения данных в режиме, доступном конечным пользователям в течение длительных периодов времени. Это позволяет экономить на дорогостоящем восстановлении с ленты и повысить производительность. Дополнительные сведения см. в разделах Архивация на месте в Exchange Server, Обнаружение электронных данных на месте в Exchange Server и Удержание на месте и удержание для судебного разбирательства в Exchange Server.

- **Моментальный снимок базы данных на определенный момент времени**. Если для вашей организации требуется прошедшую копию данных почтового ящика, Exchange предоставляет возможность создать копию базы данных с отстающей базой данных в среде DAG. Это может быть полезно в редких случаях логического повреждения хранилища, реплицируемого на несколько копий баз данных в группе обеспечения доступности баз данных, когда требуется вернуться к определенному моменту времени в прошлом. Также можно использовать эту функцию при случайном удалении администратором почтового ящика или данных пользователя. Восстановление из изолированной копии может выполняться быстрее восстановления из архива, так как изолированные копии не требуют длительного копирования с резервного сервера на сервер Exchange. Это может значительно снизить общую стоимость владения за счет сокращения времени простоя.

Так как существуют собственные функции Exchange Server, которые отвечают каждому из этих сценариев эффективным и экономичным образом, вы можете сократить или исключить использование традиционных резервных копий в вашей среде.

Собственная система защиты данных Exchange

В предпочтительной архитектуре Корпорации Майкрософт для Exchange Server 2016 и Exchange Server 2019 года используется концепция, известная как защита собственных данных Exchange. Собственная система защиты данных Exchange основана на встроенных функциях Exchange для защиты данных почтового ящика без использования резервных копий (хотя эти функции можно использовать и для

создания резервных копий). Exchange 2016 и Exchange 2019 включают в себя несколько функций, которые при правильном развертывании и настройке могут обеспечить встроенную защиту данных, что избавляет от необходимости создавать традиционные резервные копии данных. Использование функций высокого уровня доступности, встроенных в Exchange Server, чтобы свести к минимуму время простоя и потерю данных в случае аварии, также может снизить общую стоимость владения системой обмена сообщениями. В сочетании с другими встроенными функциями, такими как удержание по юридическим причинам, эти функции могут помочь вам уменьшить или исключить использование традиционного резервного копирования на определенный момент времени, а также сэкономить на сопутствующих расходах.

Помимо определения того, позволяет ли Exchange Server отойти от традиционных резервных копий на определенный момент времени, рекомендуется оценить стоимость текущей инфраструктуры резервного копирования. Рассчитайте затраты, связанные с простоями и потерями данных для конечных пользователей при попытке восстановления после сбоя с помощью такой инфраструктуры. Следует также учитывать расходы на оборудование, установку и покупку лицензии, а также расходы на управление, связанные с восстановлением данных и обслуживанием архивов. В зависимости от требований вашей организации вполне вероятно, что чистая среда Exchange 2016 или Exchange 2019 с по крайней мере тремя копиями базы данных почтовых ящиков обеспечит более низкую общую стоимость владения, чем одна с резервными копиями.

Перед использованием функций, встроенных в Exchange Server в качестве замены традиционных резервных копий, следует учесть несколько проблем. Кроме того, возможны соображения, уникальные для вашей организации. Рассмотрите следующие вопросы и обратите внимание, что этот список не является исчерпывающим.

- Следует определить, сколько копий базы данных необходимо развернуть. Настоятельно рекомендуется развернуть не менее трех неизолированных копий базы данных почтовых ящиков перед переходом с традиционных форм защиты базы данных, таких как RAID или традиционные архивы на основе VSS.
- Необходимо четко определить требования к ожидаемому времени и точке восстановления, а также убедиться, что использование объединенного набора встроенных функций архивации вместо традиционных позволит выполнить эти требования.
- Необходимо определить, сколько копий каждой базы данных потребуется создать, чтобы выдержать различные сценарии сбоев, от которых требуется

защитить систему.

- Следует определить, позволит ли удаление группы обеспечения доступности баз данных или некоторых ее участников выделить необходимые ресурсы для поддержки традиционного решения архивации. Если да, позволит ли это решение улучшить соглашения об уровне обслуживания относительно ожидаемого времени или точки восстановления.

- Следует определить, можете ли вы позволить себе потерять моментальную копию, если для участника группы обеспечения доступности баз данных, на котором размещена данная копия, произойдет сбой, влияющий на копию или ее целостность.

- Exchange Server позволяет развертывать гораздо большие почтовые ящики с рекомендуемым максимальным размером базы данных почтовых ящиков в 2 ТБ (при использовании двух или более высокодоступных копий баз данных почтовых ящиков). Основываясь на больших почтовых ящиках, которые, скорее всего, будут развернуты большинством организаций, следует определить целевую точку восстановления, если при активации копии базы данных или отстающей копии базы данных необходимо воспроизвести большое количество файлов журналов.

- Определите, каким образом будет выполняться обнаружение и предотвращение репликации логического повреждения в активной копии базы данных на пассивные копии этой базы данных. Это включает определение плана восстановления для данной ситуации, а также частоты повторения этого сценария в прошлом. При частых логических повреждениях в организации рекомендуется учитывать этот сценарий при разработке и создать одну или несколько изолированных копий, а также использовать достаточное окно задержки преобразования, позволяющее определить и исправить логическое повреждение до его репликации на другие копии базы данных.

При успешном завершении полной или добавочной архивации осуществляется усечение файлов журнала транзакций, которые больше не требуются для восстановления базы данных. Если резервные копии не создаются, усечение журнала не выполняется. Чтобы предотвратить создание большого количества файлов журнала, необходимо включить циклическое ведение журнала для реплицированных баз данных. Использование циклического ведения журнала с непрерывной репликацией является новым типом циклического ведения журнала, который называется циклическим ведением журнала непрерывной репликации (CRCL) и отличается от циклического ведения журнала расширенного обработчика

хранилищ. В то время как циклическое ведение журнала расширенного обработчика хранилищ выполняется и управляется службой банка данных Microsoft Exchange, циклическое ведение журнала непрерывной репликации выполняется и управляется службой репликации Microsoft Exchange. При включенном циклическом ведении журнала расширенного обработчика хранилищ дополнительные файлы журнала не создаются; вместо этого при необходимости перезаписывается текущий файл журнала. Однако в среде с непрерывной репликацией файлы журнала необходимы для доставки и преобразования журналов. В результате при включении циклического ведения журнала непрерывной репликации текущий файл журнала не перезаписывается, а для процесса доставки и преобразования журналов создаются закрытые файлы журнала.

В частности, служба репликации Microsoft Exchange управляет процессом циклического ведения журнала непрерывной репликации таким образом, что обеспечивается непрерывность журналов, а журналы не удаляются, пока они необходимы для репликации. Служба репликации Microsoft Exchange и служба банка данных Microsoft Exchange взаимодействуют с помощью удаленного вызова процедур (RPC), касающихся того, какие файлы журнала могут быть удалены.

Чтобы усечение использовалось только на высокодоступных (неизолированных) копиях базы данных почтовых ящиков, следующие вопросы должны иметь положительный ответ.

- Архивировался ли файл журнала или включено CRCL.
- Файл журнала находится ниже контрольной точки.
- Согласны ли другие неотсроченные копии базы данных с удалением.
- Изучался ли файл журнала всеми отсроченными копиями базы данных.

Чтобы усечение использовалось только на изолированных копиях базы данных, следующие вопросы должны иметь положительный ответ.

- Файл журнала находится ниже контрольной точки.
- Время, прошедшее с момента создания файла журнала, превышает значение ReplayLagTime + TruncationLagTime.
- Удаляется ли файл журнала в активной копии базы данных.

Поддерживаемые технологии резервного копирования

Exchange Server поддерживает только резервные копии на основе VSS с поддержкой Exchange. Exchange Server включает подключаемый модуль для резервного копирования Windows Server, который позволяет создавать и восстанавливать резервные копии данных Exchange на основе VSS. Для резервного копирования и восстановления Exchange Server необходимо использовать приложение с поддержкой Exchange, которое поддерживает модуль записи VSS для Exchange Server, например Windows Server Backup (с подключаемым модулем VSS), Microsoft System Center 2012 — Data Protection Manager или стороннее приложение на основе VSS, поддерживающее Exchange.

Дополнительные сведения об архивации и восстановлении данных Exchange с помощью системы архивации данных Windows Server см. в разделе Резервное копирование и восстановление данных Exchange с помощью системы архивации данных Windows Server.

модуль записи VSS Exchange Server

Более ранние версии Exchange включали два средства записи VSS: один внутри службы хранилища сведений Microsoft Exchange (store.exe), а другой — в службе репликации Microsoft Exchange (msexchangerepl.exe). Еще в Exchange 2013 функция записи VSS, ранее обнаруженная в службе Хранилища сведений Microsoft Exchange, была перемещена в службу репликации Microsoft Exchange. Эта архитектура остается неизменной в Exchange 2016 и Exchange 2019. Этот модуль записи с именем Microsoft Exchange Writer используется приложениями на основе VSS с поддержкой Exchange для резервного копирования активных и пассивных копий базы данных, а также для восстановления резервных копий базы данных. Хотя модуль записи выполняется в службе репликации Microsoft Exchange, для объявления записи требуется служба хранилища сведений Microsoft Exchange. В результате для архивации или восстановления баз данных Exchange требуются обе службы.

Восстановление Exchange Server

Почти все параметры конфигурации для серверов почтовых ящиков и служб клиентского доступа хранятся в Active Directory. Как и в предыдущих версиях Exchange, Exchange 2016 и Exchange 2019 включает параметр установки для восстановления потерянных серверов. Этот параметр , */m:RecoverServer*,

используется для перестроения и повторного создания потерянного сервера с помощью параметров и сведений о конфигурации, хранящихся в Active Directory. Однако обратите внимание, что некоторые параметры не сохраняются, например локальный файл web.config и другие файлы конфигурации. Кроме того, не сохраняются пользовательские записи реестра. Для отслеживания и воссоздания таких изменений мы рекомендуем использовать надежный процесс управления изменениями.

Подробные инструкции по восстановлению сервера с потерянным сервером Exchange см. в разделе Восстановление Exchange Server. Подробные инструкции по восстановлению потерянного сервера, который входит в группу доступности базы данных (DAG), см. в разделе Восстановление сервера-члена группы доступности базы данных.

Восстановление единого хранилища контактов

Если Microsoft Lync Server 2013 или Skype для бизнеса Server 2015 используется в среде Exchange 2016 или Exchange 2019, контактные данные lync/Skype для бизнеса пользователя хранятся в специальной папке контактов в почтовом ящике пользователя. Это называется единым хранилищем контактов (UCS). При восстановлении почтового ящика, перенесенного в UCS, может быть затронут список контактов службы обмена мгновенными сообщениями для конечного пользователя. Если пользователь был перенесен после последней архивации, восстановление почтового ящика приведет к полной потере списка контактов пользователя. В менее значительных случаях изменения списка контактов, внесенные пользователем после последней архивации, будут утеряны. Для устранения риска возможной потери данных убедитесь, что пользователь перенесен на сервер мгновенных сообщений перед восстановлением почтового ящика.

База данных восстановления

База данных восстановления представляет собой специальный тип базы данных почтовых ящиков, который позволяет подключать восстановленную базу данных почтовых ящиков и извлекать данные из восстановленной базы данных в рамках операции восстановления. Для восстановления данных из базы данных восстановления можно использовать командлет New-MailboxRestoreRequest. После извлечения данных их можно экспортировать в папку или добавить в существующий почтовый ящик. Базы данных восстановления позволяют выполнять

восстановление данных из архива или копии базы данных без воздействия на пользовательский доступ к текущим данным.

Использование базы данных восстановления для базы данных почтовых ящиков из предыдущих версий Exchange не поддерживается. Кроме того, целевой почтовый ящик, используемый для слияния и извлечения данных, должен находиться в том же лесу Active Directory, что и база данных, подключенная в базе данных восстановления.

Дополнительные сведения см. в разделе Базы данных восстановления. Подробные инструкции по созданию базы данных восстановления см. в разделе Создание базы данных восстановления. Подробные инструкции по использованию базы данных восстановления см. в разделе Восстановление данных с помощью базы данных восстановления.

Переносимость баз данных

Переносимость базы данных — это функция, которая позволяет перемещать базу данных почтовых ящиков Exchange на любой другой сервер почтовых ящиков Exchange в той же организации и подключать ее к ней. Использование переносимости баз данных повышает надежность благодаря устранению шагов, выполняемых вручную, когда высока вероятность возникновения ошибки, из процедур аварийного восстановления. Переносимость баз данных также позволяет сократить общее время восстановления для различных сценариев сбоя.

Подробные инструкции по использованию переносимости базы данных см. в разделе Перемещение базы данных почтовых ящиков с помощью переносимости базы данных.

Переносимость аварийного восстановления

Переносимость аварийного восстановления — это функция, обеспечивающая решение для ограниченной поддержки непрерывной работы электронной почты в случае ошибок, влияющих на базу данных почтовых ящиков, сервер или весь сайт. Переносимость аварийного восстановления предоставляет пользователю временный почтовый ящик для отправки и получения электронной почты на время восстановления или исправления его исходного почтового ящика. Временный почтовый ящик может находиться на том же сервере почтовых ящиков Exchange или на любом другом сервере почтовых ящиков Exchange в вашей организации. Это позволяет разместить на альтернативном сервере почтовые ящики пользователей, находившиеся на сервере, который стал недоступен.

Клиенты, поддерживающие функцию автообнаружения, например Microsoft Outlook, автоматически перенаправляются на новый сервер без необходимости вручную обновлять профиль настольной системы пользователя. После восстановления данных исходного почтового ящика пользователя администратор может объединить восстановленный и аварийный почтовые ящики пользователя в один обновленный почтовый ящик.

Процесс использования переносимости аварийного восстановления называется *аварийным восстановлением*. Аварийное восстановление включает в себя создание на сервере почтовых ящиков пустой базы данных вместо неисправной. Эта пустая база данных, которая называется *аварийной базой данных*, позволяет пользователям отправлять и получать электронную почту, пока неисправная база данных восстанавливается. После восстановления неисправной базы данных аварийная и восстановленная базы данных переключаются, а данные аварийной базы данных добавляются в восстановленную базу данных.

Дополнительные сведения см. в разделе Переносимость звонка. Подробные инструкции по восстановлению абонентского сигнала см. в разделе Восстановление абонентского сигнала.

Exchange Server: резервное копирование и восстановление данных Exchange с помощью резервного копирования Windows Server

Статья • 04.04.2023

В предпочтительной архитектуре Корпорации Майкрософт для Exchange Server используется концепция, известная как защита собственных данных Exchange. Защиту собственных данных Exchange обеспечивают нативные функции Exchange, которые служат для защиты данных почтового ящика и заменяют традиционные функции резервного копирования. Чтобы создать резервные копии, можно воспользоваться подключаемым модулем Exchange для системы архивации данных Windows Server (WSB). Этот модуль позволяет создавать резервные копии данных Exchange с помощью службы теневого копирования томов (VSS), но требует установки WSB.

Подключаемый модуль WSBExchange.exe запускается в качестве службы, которую можно определить как серверное расширение Microsoft Exchange для системы архивации данных Windows Server. (Краткое название службы — WSBExchange.) Эта служба автоматически устанавливается и настраивается на ручной запуск на всех серверах почтовых ящиков. Этот модуль позволяет системе архивации данных Windows Server создавать резервные копии Exchange с помощью службы теневого копирования томов.

Прежде чем приступить к резервному копированию данных Exchange с помощью системы архивации данных Windows Server, рекомендуется ознакомиться с приведенной ниже информацией о функциях и параметрах этого подключаемого модуля.

- Резервные копии, создаваемые с помощью WSB, выполняются на уровне тома, и единственный способ выполнить резервное копирование или восстановление на уровне приложения — выбрать весь том. Чтобы создать резервную копию базы данных и ее потока журналов, необходимо создать резервную копию всего тома, содержащего базу данных и журналы, а не только отдельные папки. Вы не можете создать резервную копию данных без резервного копирования всего тома, содержащего эти данные.

- Резервное копирование должно выполняться локально на сервере, для которого создается резервная копия, и вы не можете использовать подключаемый модуль для создания удаленных резервных копий VSS. Отсутствует удаленное администрирование WSB или подключаемого модуля. Однако для удаленного управления резервными копиями можно использовать службы удаленных рабочих столов или службы терминалов.

- Архив можно создать на локальном диске или в удаленном общем сетевом ресурсе.

- Можно создавать только полные резервные копии. Усечение журналов выполняется только после успешного создания с помощью VSS полного архива тома или папок, содержащих базу данных Exchange.

- При восстановлении данных можно восстанавливать только данные Exchange. Данные можно восстанавливать как в исходное местоположение, так и в другое место. При восстановлении данных в исходное расположение система архивации данных Windows Server и подключаемый модуль автоматически выполняют процесс восстановления, в том числе отключают существующую базу данных и воспроизводят журналы в восстановленной базе данных.

- Базы данных восстановления Exchange (RDB) не подлежат восстановлению. Чтобы воспользоваться RDB, необходимо восстановить данные в другое расположение, а затем вручную скопировать или переместить восстановленные данные из этого расположения в структуру папки RDB.

- При восстановлении данных Exchange все резервные копии баз данных должны быть восстановлены вместе. Невозможно восстановить отдельную базы данных.

- Восстановление без операционной системы поддерживается при использовании WSB. Однако рекомендуемый подход к восстановлению для серверов Exchange — восстановить сервер Exchange Server, а затем восстановить данные. Если вы используете стороннее приложение резервного копирования (например, не майкрософт), то поддержка восстановления Exchange без операционной системы может быть доступна у вашего поставщика приложений резервного копирования.

В следующей таблице описана поддержка параметров резервного копирования и восстановления, доступных для Exchange Server с WSB.

Если вы...	**Тогда...**

Если вы...	Тогда...
Создайте резервную копию полного сервера...	Резервное копирование с помощью службы VSS будет выполнено без усечения журналов транзакций для баз данных на сервере.
Выполните настраиваемое резервное копирование и выберите один или несколько томов для резервного копирования...	Резервное копирование с помощью службы VSS будет выполнено с усечением журналов транзакций для баз данных в выбранных томах после завершения процесса.
Выполните настраиваемое резервное копирование и выберите одну или несколько папок для резервного копирования...	Резервное копирование с помощью службы VSS будет выполнено с усечением журналов транзакций для баз данных. Однако восстановление резервных копий сведется к восстановлению отдельных файлов, так как параметр восстановления на уровне приложения будет недоступен.

Дополнительные сведения о резервном копировании данных Exchange с помощью системы архивации данных Windows Server см. в разделе Использование системы архивации данных Windows Server для резервного копирования в Exchange.

Дополнительные сведения о восстановлении данных из резервной копии, созданной с помощью системы архивации данных Windows Server, см. в разделе Восстановление резервной копии данных Exchange с помощью системы архивации данных Windows Server.

Резервное копирование Exchange Server

Статья • 04.04.2023

Вы можете с помощью системы архивации данных Windows Server создавать резервные копии баз данных Exchange и их восстанавливать. Exchange содержит подключаемый модуль системы архивации данных Windows Server, который позволяет выполнять резервное копирование данных Exchange с использованием службы теневого копирования томов (VSS).

Что нужно знать перед началом работы

- Осталось времени до завершения: 1 минута, плюс время, необходимое для резервного копирования данных
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Восстановление почтового ящика" в разделе Разрешения получателей .
- Система архивации данных Windows Server должна быть установлена на локальном компьютере.
- При выполнении архивации запускается проверка согласованности файлов данных Exchange, во время которой проверяется состояние файлов и возможность их использования для восстановления. В случае успешного выполнения проверки согласованности данные Exchange можно будет восстановить из этой резервной копии. Если проверка согласованности завершена неуспешно, данные Exchange будут недоступны для восстановления. Программа резервного копирования Windows Server выполняет проверку согласованности данных в моментальном снимке резервной копии. Таким образом, пользователь получает уведомление о результатах проверки согласованности до копирования файлов из снимка на носитель резервной копии.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование системы архивации данных Windows Server для резервного копирования в Exchange

1. Запустите систему архивации данных Windows Server.
2. Выберите пункт **Локальная архивация**.
3. В области Действия щелкните **Резервное копирование один раз...** , чтобы запустить мастер резервного копирования один раз.
4. На странице **Параметры архивации** выберите пункт **Другие параметры** и нажмите кнопку **Далее**.
5. На странице **Конфигурация архивации** выберите пункт **Настраиваемая** и нажмите кнопку **Далее**.
6. На странице **Объекты для архивации** нажмите кнопку **Добавить элементы**, чтобы выбрать тома, которые нужно заархивировать, и нажмите кнопку **OK**.

   > ⓘ **Примечание**
   >
   > Выберите тома, а не отдельные папки. Единственный способ выполнить архивирование или восстановление на уровне приложений — выбрать весь том.

7. Выберите пункт **Дополнительные параметры**. На вкладке **Исключения** нажмите кнопку **Добавить исключение**, чтобы добавить файлы или их типы, которые необходимо исключить при архивировании.

   > ⓘ **Примечание**
   >
   > По умолчанию в резервную копию включаются тома с компонентами операционной системы и приложениями; исключить их нельзя.

8. На вкладке **Параметры VSS** выберите элемент **Полная архивация VSS**, нажмите кнопку **OK**, а затем — **Далее**.
9. На странице **Тип места назначения** выберите расположение, в котором необходимо сохранить резервную копию, и нажмите кнопку **Далее**.

- Если выбран пункт **Локальные диски**, откроется страница **Место назначения архивации**. Выберите параметр из раскрывающегося списка **Место назначения архива** и нажмите кнопку **Далее**.

- Если выбран пункт **Удаленная общая папка**, откроется страница **Выбор удаленной папки**. Укажите UNC-путь для файлов резервной копии и настройте параметры управления доступом. Выберите пункт **Не наследовать**, если хотите, чтобы резервная копия была доступна только при использовании определенной учетной записи. Укажите имя пользователя и пароль для учетной записи с разрешениями на запись на компьютере, на котором размещена удаленная папка, а затем нажмите кнопку **ОК**. Или же выберите пункт **Наследовать**, если хотите, чтобы к резервной копии имели доступ все, у кого есть доступ к удаленной папке. Нажмите кнопку **Далее**.

10. На странице **Подтверждение** проверьте параметры архивации и нажмите кнопку **Архивация**.

11. На странице **Ход архивации** можно наблюдать за состоянием и ходом операции создания резервной копии.

12. Нажмите кнопку **Закрыть**, чтобы в любой момент закрыть страницу **Ход архивации**. Резервное копирование продолжится в фоновом режиме.

Как проверить, что все получилось?

Чтобы убедиться, что вы успешно завершили резервное копирование данных:

- На сервере, на котором выполнялось резервное копирование Windows Server, будет отображаться состояние последней резервной копии, которое должно иметь значение Успешно. Вы также можете убедиться, что резервное копирование выполнено успешно, просмотрев журналы резервного копирования Windows Server.

- Откройте средство просмотра событий и убедитесь, что в журнале событий приложения зарегистрировано событие завершения резервного копирования.

- Чтобы убедиться, что резервная копия каждой базы данных на выбранных томах создана успешно, выполните такую команду в командной консоли Exchange:

```
PowerShell
```

```
Get-MailboxDatabase -Server <ServerName> -Status | Format-List
Name,*FullBackup
```

Свойства *SnapshotLastFullBackup* и *LastFullBackup* базы данных указывают, когда была создана последняя успешная резервная копия и была ли она полной резервной копией VSS.

Использование системы архивации данных Windows Server для восстановления резервной копии Exchange

Статья • 04.04.2023

Вы можете с помощью системы архивации данных Windows Server создавать резервные копии баз данных Exchange и их восстанавливать. Exchange включает подключаемый модуль для резервного копирования Windows Server, который позволяет создавать и восстанавливать резервные копии данных Exchange на основе службы теневого копирования томов (VSS). Дополнительные сведения см. в разделе Using Windows Server Backup to back up and restore Exchange data.

Что нужно знать перед началом работы

- Осталось времени до завершения: 1 минута плюс время, необходимое для восстановления данных
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Восстановление почтового ящика" в разделе Разрешения получателей .
- Систему архивации данных Windows Server необходимо установить на локальном компьютере.
- При восстановлении базы данных в исходное местоположение она может оставаться в состоянии "грязного" отключения и подключаться системой. Во время восстановления базы данных в альтернативное расположение (например, в процессе подготовки к использованию базы данных восстановления) ее необходимо вручную перевести в состояние "чистого" отключения с помощью служебных программ базы данных сервера Exchange (Eseutil.exe).

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование системы архивации данных Windows Server для восстановления резервной копии Exchange

1. Запустите систему архивации данных Windows Server.
2. Выберите пункт **Локальная архивация**.
3. В области Действия нажмите кнопку **Восстановить...** , чтобы запустить мастер восстановления.
4. На странице **Приступая к работе** выполните одно из указанных ниже действий:
    - Если восстанавливаемая резервная копия данных создана на локальном сервере, выберите пункт **Этот сервер (имя_сервера)** и нажмите кнопку **Далее**.
    - Если восстанавливаемые данные хранятся на другом сервере или восстанавливаемая резервная копия находится на другом компьютере, выберите пункт **Другой сервер**, а затем нажмите кнопку **Далее**. На странице **Укажите тип размещения** выберите пункт **Локальные диски** или **Удаленная общая папка** и нажмите кнопку **Далее**. Если выбран пункт **Локальные диски**, на странице **Выберите расположение резервной копии** укажите диск с резервной копией и нажмите кнопку **Далее**. Если выбран пункт **Удаленная общая папка**, на странице **Укажите удаленную папку** введите UNC-путь к резервной копии и нажмите кнопку **Далее**.
5. На странице **Выбор даты архивации** выберите дату и время резервной копии, которую требуется восстановить, и нажмите кнопку **Далее**.
6. На странице **Тип восстановления** выберите пункт **Приложения**, а затем нажмите кнопку **Далее**.

    > ⓘ **Примечание**
    >
    > Если пункт **Приложения** отсутствует в этом разделе, значит, для последующего восстановления была выбрана резервная копия на уровне папки, а не тома. Резервное копирование данных Exchange с помощью системы архивации данных Windows Server требует создания резервных копий на уровне тома.

7. Убедитесь, что на странице **Выбор приложения** в поле **Приложения** выбран сервер Exchange. Чтобы просмотреть компоненты приложения резервной копии, нажмите кнопку **Просмотреть сведения**. Если восстанавливается самая последняя резервная копия, будет отображен флажок **Не выполнять восстановление базы данных приложений с повтором всех завершенных транзакций**. Чтобы система архивации данных Windows Server не выполняла восстановление базы данных с повтором всех завершенных транзакций согласно списку незавершенных действий в журнале транзакций, установите этот флажок. Нажмите кнопку **Далее**.

8. На странице **Параметры восстановления** выберите расположение для восстановления данных и нажмите кнопку **Далее**.

    - Выберите **Восстановить в исходное расположение** , если вы хотите восстановить данные Exchange непосредственно в исходное расположение. Если вы используете этот параметр, вы не сможете выбрать, какие базы данных будут восстановлены. все базы данных с резервной копией на томе будут восстановлены в исходных расположениях.

    - Чтобы восстановить отдельные базы данных и файлы в указанное местоположение, выберите пункт **Восстановить в другое расположение**. Чтобы указать другое местоположение, нажмите кнопку **Обзор**. Этот параметр позволит выбрать базы данных, которые необходимо восстановить. После восстановления файлы данных можно переместить в базу данных восстановления, вручную вернуться в исходное расположение или подключить к другому месту в организации Exchange с помощью переносимости базы данных. При восстановлении в другое расположение восстановленная база данных будет находиться в состоянии неправильного отключения. По завершении восстановления необходимо вручную перевести ее в состояние правильного отключения с помощью Eseutil.exe.

9. На странице **Подтверждение** проверьте параметры восстановления и нажмите кнопку **Восстановить**.

10. На странице **Ход восстановления** можно наблюдать за состоянием и ходом операции восстановления.

11. После завершения операции восстановления нажмите кнопку **Закрыть**.

Как проверить, что все получилось?

На странице **Ход восстановления** будет указано, что восстановление прошло успешно (либо не было выполнено). Чтобы убедиться, что данные успешно восстановлены:

- Изучите конечный каталог резервной копии и проверьте, существуют ли восстановленные данные.
- Убедитесь, что работа успешно выполнена, просмотрев журналы архивации на сервере, на котором была запущена система архивации данных Windows Server.
- Откройте окно просмотра событий и убедитесь, что завершение восстановления зафиксировано в журнале событий приложений.

Восстановление серверов Exchange

Статья • 04.04.2023

Вы можете восстановить потерянный сервер Exchange Server с помощью параметра */Mode:RecoverServer* в автоматическом режиме (из командной строки) программы установки Exchange. Так как большинство параметров сервера Exchange хранятся в Active Directory, `Setup.exe /Mode:RecoverServer` команда использует эти сведения во время установки Exchange на новом сервере с тем же именем.

Восстановление утерянного сервера Exchange часто выполняется с помощью нового оборудования. Однако можно также использовать существующий сервер, на котором еще не установлен Exchange.

В этом разделе показано, как восстановить потерянный сервер Exchange Server, который не является членом группы доступности базы данных (DAG). Подробные инструкции по восстановлению сервера, который входил в DAG, см. в разделе Восстановление рядового сервера группы доступности базы данных.

Ищете другие задачи управления, связанные с резервным копированием и восстановлением данных? Ознакомьтесь с статьей Резервное копирование, восстановление и аварийное восстановление.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 20 минут
- Для учетной записи, которую вы будете использовать для восстановления сервера, требуются следующие разрешения:
  - Членство администраторов домена в группах безопасности.
  - Членство в группе роли "Управление организацией Exchange".
- Если Exchange установлен в расположении, отличном от расположения по умолчанию %ProgramFiles%\Microsoft\Exchange Server\V15, необходимо включить в `Setup.exe /Mode:RecoverServer` команду параметр */TargetDir:<Path>*, чтобы указать расположение файлов программы Exchange (двоичные). Если параметр */TargetDir* не используется, файлы Exchange будут установлены в расположении по умолчанию при восстановлении сервера Exchange.

Чтобы найти расположение установки Exchange на потерянном сервере Exchange, выполните следующие действия.

1. Откройте файл ADSIEDIT.MSC или LDP.EXE.
2. Перейдите в **раздел CN=ExServerName,CN=Servers,CN=First Administrative Group,CN=Administrative Groups,CN=ExOrg Name,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=DomainName,CN=Com**
3. Щелкните объект сервера Exchange правой кнопкой мыши и выберите пункт **Свойства**.
4. Найдите атрибут **msExchInstallPath** . Этот атрибут содержит текущий путь установки.

- Если у вас нет установочного носителя для версии накопительного обновления (CU), установленной на сервере для восстановления, можно восстановить сервер с помощью последнего доступного накопительного обновления. Для скачивания доступны только последние два CU. Дополнительные сведения см. в разделе Обновления для Exchange Server. После успешного обновления adminDisplayVersion в EMS или атрибуте msExchVersion на восстановленном сервере будет отображаться старый номер сборки, и это косметический характер. Можно запустить программу установки /m:upgrade /IAcceptEchangeServerLicenseTerms или дождаться следующего выпуска накопительного обновления и выполнить обновление, которое исправит это.
- Целевой сервер должен использовать ту же версию Windows Server, что и потерянный сервер. Например, невозможно восстановить потерянный сервер Exchange 2016 под управлением Windows 2012 R2 на новом сервере под управлением Windows 2016 или наоборот.
- Те же буквы дисков, которые использовались для подключенных баз данных на потерянном сервере, также должны существовать на целевом сервере.
- Целевой сервер должен иметь те же общие характеристики производительности и конфигурацию оборудования, что и потерянный сервер.
- Параметр */Mode:RecoverServer* назначает самозаверяющий сертификат всем службам Exchange, для которых требуется ПРОТОКОЛ SSL/TLS. Если сервер ранее использовал SSL/TLS-сертификат, выданный другим центром сертификации, потребуется повторно импортировать сертификат и настроить

службы для использования сертификата. В противном случае пользователи получат запрос на сертификат при попытке подключиться (например, в Outlook).

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по **адресу Exchange Server**.

Восстановление утерянного сервера Exchange

1. Сбросьте учетную запись компьютера для утерянного сервера. Подробные инструкции см. в разделе Сброс учетной записи компьютера.
2. Установите подходящую операционную систему и укажите для нового сервера имя утерянного сервера. Восстановление не будет выполнено, если целевой сервер Windows не имеет того же имени, что и потерянный сервер Exchange Server.
3. Присоедините сервер к тому же домену, что и утерянный сервер.
4. Установите необходимые компоненты и компоненты операционной системы на целевом сервере. Дополнительные сведения см. Exchange Server требования к системе.
5. На целевом сервере откройте проводник, щелкните правой кнопкой мыши скачанный файл ISO-образа Exchange и выберите **Подключить**. Обратите внимание на назначенную букву виртуального DVD-диска.
6. Откройте окно командной строки Windows. Например:
   - Нажмите клавиши Windows + R, чтобы открыть диалоговое окно **Выполнить**, введите cmd.exe и нажмите кнопку **ОК**.
   - Нажмите кнопку **Пуск**. В поле **Поиск** введите **командная строка**, а затем в списке результатов выберите **Командная строка**.
7. В окне командной строки введите следующую команду:

> **Примечание**

- Предыдущий параметр */IAcceptExchangeServerLicenseTerms* не будет работать, начиная с Exchange Server 2016 и Exchange Server 2019 за сентябрь 2021 Обновления г. Теперь необходимо использовать */IAcceptExchangeServerLicenseTerms_DiagnosticDataON* или */IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF* для автоматической установки и установки по сценариям.

- В примерах ниже используется переключатель */IAcceptExchangeServerLicenseTerms_DiagnosticDataON*. Вы можете изменить переключатель на */IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF*.

Консоль

```
<Virtual DVD drive letter>:\Setup.exe
/IAcceptExchangeServerLicenseTerms_DiagnosticDataON /Mode:RecoverServer
[/TargetDir:<Path>] [/DomainController:<ServerNameOrFQDN>]
[/DoNotStartTransport] [/EnableErrorReporting]
```

В этом примере файлы установки Exchange на диске E: используются для установки Exchange в расположении по умолчанию (%ProgramFiles%\Microsoft\Exchange Server\V15) и восстановления сервера Exchange Server.

PowerShell

```
E:\Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON
/Mode:RecoverServer
```

Это тот же пример, но для сопоставления расположения на потерянном сервере требуется пользовательское расположение для файлов программы Exchange.

PowerShell

```
E:\Setup.exe /IAcceptExchangeServerLicenseTerms_DiagnosticDataON
/Mode:RecoverServer /TargetDir:"D:\Program Files\Exchange"
```

Дополнительные сведения о необязательных параметрах см. в статье Использование автоматического режима в программе установки Exchange.

8. После завершения установки, но перед переводом восстановленного сервера в рабочую среду перенастройте все пользовательские параметры, которые ранее присутствовали на сервере, а затем перезапустите сервер.

Как проверить, все ли получилось?

Успешное завершение установки — первый показатель успешного восстановления. Чтобы проверить, успешно ли вы восстановили потерянный сервер, откройте средство служб Windows (services.msc) и убедитесь, что службы Microsoft Exchange установлены и запущены.

Возможные проблемы с агентом скриптов

Если вы ранее включили агент скриптов в организации Exchange, процесс восстановления может завершиться ошибкой. Ошибка будет выглядеть следующим образом:

Консоль

```
"Initialization failed: '"Scripting Agent initialization failed: "File is
not found: 'C:\Program Files\Microsoft\Exchange
Server\V15\Bin\CmdletExtensionAgents\ScriptingAgentConfig.xml'.""' --->
Microsoft.Exchange.Provisioning.ProvisioningException: "Scripting Agent
initialization failed: "File is not found: 'C:\Program
Files\Microsoft\Exchange
Server\V15\Bin\CmdletExtensionAgents\ScriptingAgentConfig.xml'."" --->
System.IO.FileNotFoundException: "File is not found: 'C:\Program
Files\Microsoft\Exchange
Server\V15\Bin\CmdletExtensionAgents\ScriptingAgentConfig.xml'."
```

Если в вашей организации есть другие серверы Exchange, вам потребуется:

1. Отключите агент скриптов в командной консоли Exchange на существующем сервере:

   PowerShell

   ```
   Disable-CmdletExtensionAgent -Identity "Scripting Agent"
   ```

2. Запустите программу установки Exchange в режиме восстановления, как описано выше в этом разделе.

3. Включите агент сценариев в командной консоли Exchange после завершения восстановления сервера Exchange:

PowerShell

```
Enable-CmdletExtensionAgent -Identity "Scripting Agent"
```

Если восстановленный сервер Exchange Server является единственным сервером Exchange в вашей организации, вам потребуется:

1. Переименуйте файл %ExchangeInstallPath%Bin\CmdletExtensionAgents\ScriptingAgentConfig. **xml.sample** to %ExchangeInstallPath%Bin\CmdletExtensionAgents\ScriptingAgentConfig. **xml**.

   Значением по умолчанию %ExchangeInstallationPath% является %ProgramFiles%\Microsoft\Exchange Server\V15, но фактическим значением является место установки Exchange на сервере.

2. Повторно запустите программу установки Exchange в режиме восстановления, как описано выше в этом разделе.

Восстановление рядового сервера группы доступности базы данных в Exchange Server

Статья • 04.04.2023

Если сервер почтовых ящиков, который входит в группу доступности базы данных (DAG), потерян или завершается сбоем и не восстанавливается и нуждается в замене, можно выполнить операцию восстановления сервера.

Microsoft Exchange Server программа установки включает параметр */m:RecoverServer*, который можно использовать для выполнения операции восстановления сервера. При запуске программы установки с параметром */m:RecoverServer* программа установки считывает сведения о конфигурации сервера из Active Directory для сервера с тем же именем, что и сервер, с которого выполняется программа установки.

После извлечения сведений о конфигурации сервера из Active Directory на сервере устанавливаются исходные файлы и службы Exchange, а также к серверу применяются роли и параметры, хранившиеся в Active Directory.

Сведения о других задачах управления, связанных с группами доступности базы данных, см. См. раздел Управление группами доступности баз данных.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 30 минут.
- Прежде чем выполнять эту процедуру или процедуры, необходимо назначить вам разрешения. Сведения о необходимых разрешениях см. в записи "Копии баз данных почтовых ящиков" в разделе Разрешения высокой доступности и устойчивости сайта .
- Если Exchange установлен в расположении, отличном от расположения по умолчанию, необходимо использовать параметр установки */TargetDir* , чтобы указать расположение программных файлов Exchange. Если параметр */TargetDir* не используется, файлы программы Exchange будут установлены в расположении по умолчанию (%programfiles%\Microsoft\Exchange Server\V15).

  Чтобы определить расположение для установки, выполните указанные ниже действия.

1. Откройте файл ADSIEDIT.MSC или LDP.EXE.
2. Перейдите в следующее расположение:
   CN=ExServerName,CN=Servers,CN=First Administrative Group,CN=Administrative Groups,CN=ExOrg Name,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=DomainName,CN=Com
3. Щелкните объект сервера Exchange правой кнопкой мыши и выберите пункт **Свойства**.
4. Найдите атрибут **msExchInstallPath**. Этот атрибут содержит текущий путь установки.

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Восстановление сервера с помощью команды Setup /m:RecoverServer

1. Извлеките все параметры задержки преобразования и задержки усечения для всех копий баз данных почтовых ящиков, существовавших на восстанавливаемом сервере, с помощью командлета Get-MailboxDatabase.

```
PowerShell

Get-MailboxDatabase DB1 | Format-List *lag*
```

2. Удалите все копии баз данных почтовых ящиков, существовавшие на восстанавливаемом сервере, с помощью командлета Remove-MailboxDatabaseCopy.

```
PowerShell

Remove-MailboxDatabaseCopy DB1\MBX1
```

3. Удалите конфигурацию отказавшего сервера из группы обеспечения доступности баз данных с помощью командлета Remove-DatabaseAvailabilityGroupServer.

```
PowerShell

Remove-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer
MBX1
```

> **Примечание**
>
> Если удаленный член DAG находится в автономном режиме и не может быть подключен к сети, необходимо добавить `-ConfigurationOnly` параметр в предыдущую команду. Если вы используете `-ConfigurationOnly` параметр, необходимо также вручную исключить узел из кластера.

4. Сбросьте учетную запись компьютера сервера в Active Directory. Подробные инструкции см. в разделе Сброс учетной записи компьютера.

5. Откройте окно командной строки. С помощью исходного установочного носителя выполните такую команду:

```
PowerShell

Setup /m:RecoverServer
```

6. После завершения процесса восстановления программы установки добавьте восстановленный сервер в группу обеспечения доступности баз данных с помощью командлета Add-DatabaseAvailabilityGroupServer.

```
PowerShell

Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer MBX1
```

7. После того как сервер будет снова добавлен в группу обеспечения доступности баз данных, можно заново выполнить конфигурацию копий баз данных почтовых ящиков с помощью командлета Add-MailboxDatabaseCopy. Если для любой из добавляемых ранее копий базы данных была задержка воспроизведения или задержка усечения больше 0, можно использовать

параметры *ReplayLagTime* и *TruncationLagTime* командлета Add-MailboxDatabaseCopy , чтобы перенастроить эти параметры:

```
PowerShell

Add-MailboxDatabaseCopy -Identity DB1 -MailboxServer MBX1
Add-MailboxDatabaseCopy -Identity DB2 -MailboxServer MBX1 -
ReplayLagTime 3.00:00:00
Add-MailboxDatabaseCopy -Identity DB3 -MailboxServer MBX1 -
ReplayLagTime 3.00:00:00 -TruncationLagTime 3.00:00:00
```

ⓘ Примечание

Вам потребуется перенастроить виртуальные каталоги на восстановленном сервере и повторно создать все внесенные настройки. Вам также может потребоваться выполнить дополнительные действия по восстановлению в зависимости от конфигурации. См. **статью Развертывание учетных данных ASA на другом сервере Exchange Server, на котором выполняются службы клиентского доступа**.

Необходимо импортировать сертификат подписи AD FS. См. **раздел Шаг 1. Проверка требований к сертификатам для AD FS**.

Как узнать, что это исправление сработает?

Чтобы убедиться, что член DAG успешно восстановлен, используйте следующий метод:

- В командной консоли Exchange выполните следующую команду, чтобы проверить работоспособность и состояние восстановленного члена DAG.

```
PowerShell

Test-ReplicationHealth <ServerName>
```

```
PowerShell

Get-MailboxDatabaseCopyStatus -Server <ServerName>
```

Все тесты работоспособности репликации должны пройти успешно, и состояние баз данных и их индексы содержания должны быть работоспособны.

Базы данных восстановления в Exchange Server

Статья • 04.04.2023

База данных восстановления (RDB) — это специальная база данных почтовых ящиков, которая позволяет подключать восстановленную базу данных почтовых ящиков и извлекать из нее данные. Для извлечения данных из базы данных восстановления можно использовать командлет New-MailboxRestoreRequest. После извлечения данные можно экспортировать в папку или добавить в существующий почтовый ящик. Базы данных восстановления позволяют восстанавливать данные из архива или копии базы данных, не нарушая доступ пользователей к текущим данным.

Microsoft Exchange Server поддерживает возможность восстановления данных непосредственно в базе данных восстановления. Подключение восстановленных данных в качестве базы данных восстановления позволяет администратору восстановить отдельные почтовые ящики или отдельные элементы в почтовом ящике. Восстановить данные в базу данных восстановления можно двумя способами.

- Если база данных восстановления уже существует, приложение может отключить ее, восстановить данные в эту базу и в файлы журналов, а затем снова подключить базу данных.
- Базу данных и файлы журналов можно восстановить в любую папку на диске. Exchange анализирует восстановленные данные и воспроизводит журналы транзакций, чтобы привести базы данных в актуальное состояние, после чего базу данных восстановления можно настроить так, чтобы она указывала на уже восстановленные файлы базы данных.

Различие между базой данных почтовых ящиков и базой данных восстановления

Базы данных восстановления отличаются от стандартных баз данных почтовых ящиков в нескольких аспектах, приведенных ниже.

- База данных восстановления создается с помощью командной консоли Exchange.

- Базы данных восстановления не поддерживают отправку и получение почты. Доступ к базе данных восстановления по всем клиентским протоколам (включая SMTP, POP3 и IMAP4) блокируется. Это сделано для того, чтобы базу данных восстановления нельзя было использовать для вставки и удаления почты в системе обмена сообщениями.

- Доступ клиента MAPI с помощью Microsoft Outlook или Outlook в Интернете заблокирован. Базы данных восстановления поддерживают доступ MAPI, но только для средств восстановления и приложений. При использовании MAPI для входа в почтовый ящик в базе данных восстановления необходимо указывать идентификаторы GUID почтового ящика и базы данных.

- Почтовые ящики в базе данных восстановления не могут быть подключены к учетным записям пользователей. Чтобы разрешить пользователю доступ к данным почтового ящика в базе данных восстановления, необходимо добавить этот почтовый ящик в существующий почтовый ящик или экспортировать его в папку.

- Политики управления системой и почтовыми ящиками не применяются. Это сделано для того, чтобы из базы данных восстановления невозможно было удалять элементы во время восстановления.

- Оперативное обслуживание для баз данных восстановления не выполняется.

- Для баз данных восстановления невозможно включить циклическое ведение журналов.

- В любой момент к серверу почтовых ящиков может быть подключена только одна база данных восстановления. Использование базы данных восстановления не учитывается в ограничении, установленном для сервера почтовых ящиков.

- В базе данных почтовых ящиков нельзя создавать копии базы данных восстановления.

- Базу данных восстановления можно использовать в качестве целевой для операций восстановления, но не для операций резервного копирования.

- Восстанавливаемая база данных, подключенная как RDB, никак не связана с исходным почтовым ящиком.

Использование базы данных восстановления

Чтобы можно было использовать базу данных восстановления, должны выполняться определенные условия. RDB можно использовать только для баз данных почтовых ящиков Exchange 2016 и более поздних версий. Базы данных почтовых ящиков из предыдущих версий Exchange не поддерживаются. Кроме того, почтовый ящик, используемый для слияния и извлечения данных, должен находиться в том же лесу Active Directory, что и база данных, подключенная в RDB.

Базу данных восстановления можно использовать для восстановления данных в следующих случаях:

- **Восстановление номера номера одного и того же сервера**. Восстановление из RDB можно выполнить после восстановления исходной базы данных из резервной копии в рамках операции восстановления абонентского сигнала.
- **Восстановление номера номера альтернативного сервера**. Вы можете использовать альтернативный сервер для размещения базы данных абонентского номера, а затем восстановить данные из RDB после восстановления исходной базы данных из резервной копии.
- **Восстановление почтового ящика**. Отдельный почтовый ящик можно восстановить из резервной копии по истечении срока хранения удаленного почтового ящика. Затем вы можете извлечь данные из восстановленного почтового ящика и скопировать их в папку или добавить в другой почтовый ящик.
- **Восстановление определенных элементов**. Восстановление можно из данных резервной копии, которые были удалены или удалены из почтового ящика.

> ⓘ **Примечание**
>
> При восстановлении контента в активном почтовом ящике списки управления доступом (ACL) к папкам не сохраняются. Так как в процессе восстановления данные почтовых ящиков обычно восстанавливаются и добавляются в исходную базу данных, восстановление или копирование списков ACL не требуется.

База данных восстановления предназначена для восстановления базы данных почтовых ящиков в следующих условиях и сценариях:

- Логические сведения об исходной базе данных и ее почтовых ящиках остались без изменений и не были повреждены в Active Directory.

- Необходимо восстановить отдельный почтовый ящик или одну базу данных. Сценарии восстановления:
    - восстановление или ремонт базы данных во время использования аварийной базы данных в целях слияния этих двух баз данных;
    - Восстановление базы данных на сервере, отличном от исходного сервера для этой базы данных. При необходимости можно объединить восстановленные данные обратно с исходным сервером.
    - восстановление элементов, ранее удаленных пользователями из своих почтовых ящиков, после истечения периода хранения удаленных элементов.

Базы данных восстановления не предназначены для восстановления целых серверов, несколько баз данных, а также изменения или восстановления топологии Active Directory.

Подробные инструкции по созданию RDB см. в статье Создание базы данных восстановления. Подробные инструкции по использованию RDB см. в статье Восстановление данных с помощью базы данных восстановления.

Создание базы данных восстановления в Exchange Server

Статья • 04.04.2023

С помощью командной консоли Exchange можно создать базу данных восстановления — специальную базу данных почтовых ящиков, которая используется для подключения и извлечения данных из восстановленной базы данных. Создав базу данных восстановления, вы можете переместить в нее восстановленную базу данных почтовых ящиков, а затем извлечь из последней данные с помощью командлета New-MailboxRestoreRequest. После извлечения данные можно экспортировать в папку или добавить в существующий почтовый ящик. С помощью баз данных восстановления можно восстановить данные, используя резервную или другую копию базы данных и не лишая при этом пользователей доступа к текущим данным.

Ищете другие задачи управления, связанные с базами данных восстановления? Ознакомьтесь с статьей Базы данных восстановления.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 1 минута
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Восстановление почтового ящика" в разделе Разрешения получателей.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование командной консоли Exchange для создания базы данных

восстановления

В этом примере показано, как создать базу данных восстановления RDB1 на сервере почтовых ящиков MBX2.

```
PowerShell

New-MailboxDatabase -Recovery -Name RDB1 -Server MBX2
```

В этом примере показано, как создать базу данных восстановления RDB2 на сервере почтовых ящиков MBX1 с помощью пользовательского пути к файлу базы данных и папке журнала.

```
PowerShell

New-MailboxDatabase -Recovery -Name RDB2 -Server MBX1 -EdbFilePath
"C:\Recovery\RDB2\RDB2.EDB" -LogFolderPath "C:\Recovery\RDB2"
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе New-MailboxDatabase.

Как проверить, все ли получилось?

Чтобы убедиться, что база данных восстановления успешно создана, сделайте следующее:

- Чтобы просмотреть сведения о конфигурации базы данных восстановления, выполните в командной консоли Exchange следующую команду:

  ```
  PowerShell

  Get-MailboxDatabase <RecoveryDatabaseName> | Format-List
  ```

Другие задачи

После создания базы данных восстановления можно также выполнить восстановление данных с помощью базы данных восстановления. Подробные инструкции см. в статье Восстановление данных с помощью базы данных восстановления.

Восстановление данных с помощью базы данных восстановления в Exchange Server

Статья • 04.04.2023

База данных восстановления представляет собой специальный тип базы данных почтовых ящиков, который позволяет подключать восстановленную базу данных почтовых ящиков и извлекать данные из восстановленной базы данных в рамках операции восстановления. Базы данных восстановления позволяют выполнять аварийное восстановление данных из архива или копии базы данных без воздействия на пользовательский доступ к текущим данным.

После создания базы данных восстановления вы можете восстановить в нее базу данных почтовых ящиков, используя приложение резервного копирования или скопировав базу данных и ее файлы журналов в структуру папок базы данных восстановления. После этого можно воспользоваться командлетом New-MailboxRestoreRequest для извлечения данных из восстановленной базы данных. После извлечения данные можно экспортировать в папку или объединить с существующими данными почтового ящика.

Дополнительные сведения о задачах управления, связанных с базами данных восстановления (RDB), см. в статье Базы данных восстановления.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 1 минута плюс время на приведение базы данных в состояние чистого отключения и извлечение данных.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Восстановление почтового ящика" в разделе Разрешения получателей .
- Некоторые приложения резервного копирования позволяют восстановить данные Exchange непосредственно в базу данных восстановления. Система архивации данных Windows Server может восстанавливать в базу данных восстановления только резервные копии на уровне файлов. Она не может использоваться для восстановления резервных копий на уровне приложения в базу данных восстановления.

- Базу данных и файлы журнала, содержащие восстановленные данные, необходимо восстановить или скопировать в структуру папок базы данных восстановления.
- База данных должна находиться в состоянии чистого отключения. Поскольку база данных восстановления представляет собой альтернативное расположение восстановления для всех баз данных, все восстановленные базы данных будут находиться в состоянии неправильного отключения. Для переключения восстановленных баз данных в состояние чистого отключения следует использовать команду **Eseutil /R**.

Использование командной консоли Exchange для восстановления данных с помощью базы данных восстановления

1. Скопируйте восстановленную базу данных и ее файлы журнала или восстановите их в расположение, которое будет использоваться для базы данных восстановления.
2. С помощью программы Eseutil переведите эту базу данных в состояние чистого отключения. В следующем примере EXX — это префикс создания журнала для базы данных (например, E00, E01, E02 и т. д.).

   PowerShell

   ```
   Eseutil /R EXX /l <RDBLogFilePath> /d <RDBEdbFolder>
   ```

   В следующем примере показан префикс создания журнала E01 и путь базы данных восстановления и файла журнала E:\Databases\RDB1:

   PowerShell

   ```
   Eseutil /R E01 /l E:\Databases\RDB1 /d E:\Databases\RDB1
   ```

3. Создайте базу данных восстановления. Присвойте базе данных восстановления уникальное имя, но используйте имя и путь к файлу базы данных для параметра EdbFilePath, а также расположение восстановленных файлов журнала для параметра LogFolderPath.

   PowerShell

```
New-MailboxDatabase -Recovery -Name <RDBName> -Server <ServerName> -
EdbFilePath <RDBPathandFileName> -LogFolderPath <LogFilePath>
```

В следующем примере показано создание базы данных восстановления, которая будет использоваться для восстановления базы данных DB1.edb и ее файлов журнала, расположенных в папке E:\Databases\RDB1.

PowerShell

```
New-MailboxDatabase -Recovery -Name <RDBName> -Server <ServerName> -
EdbFilePath "E:\Databases\RDB1\DB1.EDB" -LogFolderPath
"E:\Databases\RDB1"
```

4. Перезапустите службу банка данных Microsoft Exchange:

PowerShell

```
Restart-Service MSExchangeIS
```

5. Подключите базу данных:

PowerShell

```
Mount-database <RDBName>
```

6. Убедитесь, что подключенная база данных содержит почтовые ящики, которые вы хотите восстановить:

PowerShell

```
Get-MailboxStatistics -Database <RDBName> | Format-Table
DisplayName,MailboxGUID -AutoSize
```

7. С помощью командлета New-MailboxRestoreRequest восстановите почтовый ящик или элементы из базы данных восстановления в производственный почтовый ящик.

   В следующем примере показано восстановление исходного почтового ящика с идентификатором MailboxGUID 1d20855f-fd54-4681-98e6-e249f7326ddd из базы данных DB1 в целевом почтовом ящике с псевдонимом Morris.

PowerShell

```
New-MailboxRestoreRequest -SourceDatabase DB1 -SourceStoreMailbox
1d20855f-fd54-4681-98e6-e249f7326ddd -TargetMailbox Morris
```

В следующем примере содержимое исходного почтового ящика с отображаемым именем Morris Cornejo в базе данных почтовых ящиков DB1 восстанавливается в архивный почтовый ящик для Morris@contoso.com.

PowerShell

```
New-MaiboxRestoreRequest -SourceDatabase DB1 -SourceStoreMailbox
"Morris Cornejo" -TargetMailbox Morris@contoso.com -TargetIsArchive
```

8. Периодически проверяйте состояние запроса восстановления почтового ящика с помощью командлета Get-MailboxRestoreRequest.

   Когда состояние восстановления изменится на "Завершено", уделите запрос, используя командлет Remove-MailboxRestoreRequest. Например:

PowerShell

```
Get-MailboxRestoreRequest -Status Completed | Remove-
MailboxRestoreRequest
```

Как проверить, что все получилось?

Чтобы убедиться, что вы успешно восстановили данные почтового ящика, откройте целевой почтовый ящик с помощью приложения Outlook или Outlook Web App и проверьте наличие восстановленных данных.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Перемещение базы данных почтовых ящиков с помощью переносимости базы данных в Exchange Server

Статья • 04.04.2023

Переносимость баз данных поможет сократить общее время восстановления в случае некоторых сценариев сбоя. Использование переносимости баз данных повышает надежность благодаря устранению шагов, выполняемых вручную, когда высока вероятность возникновения ошибки, из процедур аварийного восстановления. Обратите внимание, что базы данных почтовых ящиков из предыдущих версий Exchange нельзя переместить на сервер почтовых ящиков под управлением Exchange 2016 или Exchange 2019.

> **Примечание**
>
> Если используется функция переносимости баз данных для восстановления базы данных почтовых ящиков, версии операционной системы и Exchange Server на исходном и целевом серверах Exchange Server должны быть одинаковыми. Например, если база данных почтовых ящиков Exchange 2016 была ранее установлена на сервере с Windows Server 2016, функция переносимости баз данных будет работать только после переноса этой базы данных на сервер с Windows Server 2016 и Exchange 2016.

Что нужно знать перед началом работы

- Предполагаемое время выполнения: 5 минут, а также время, необходимое для восстановления данных, перемещения файлов базы данных и ожидания завершения репликации Active Directory.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Восстановление почтового ящика" в разделе Разрешения получателей .
- Центр администрирования Exchange нельзя использовать для перемещения почтовых ящиков пользователей в восстановленную или аварийную базу данных с помощью функции переноса баз данных.

> **Совет**

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование командной консоли Exchange для перемещения почтовых ящиков пользователей в восстановленную базу данных или с помощью переносимости базы данных

1. Убедитесь, что работа базы данных, которую необходимо переместить, завершена нормально. Если работа база данных не завершена должным образом, выполните "мягкое" восстановление.

   > **Примечание**
   >
   > При выполнении "мягкого" восстановления все незафиксированные файлы журналов фиксируются в базе данных. При отсутствии некоторых необходимых файлов журналов невозможно выполнить "мягкое" восстановление. Перейдите к шагу 2.

   Чтобы зафиксировать все незафиксированные файлы журналов в базе данных, в командной строке запустите следующую команду.

   PowerShell

   ```
   ESEUTIL /R <Enn>
   ```

   > **Примечание**
   >
   > <E *nn*> указывает префикс файла журнала для базы данных, в которой планируется воспроизвести файлы журнала. Префикс файла журнала, заданный <E *nn*> , является обязательным параметром для Eseutil /r.

2. Создайте базу данных на сервере, используя следующий синтаксис:

   PowerShell

```
New-MailboxDatabase -Name <DatabaseName> -Server <ServerName> -
EdbFilePath <DatabaseFileNameandPath> -LogFolderPath <LogFilesPath>
```

3. Укажите атрибут *This database can be over written by restore* с помощью следующей синтаксической конструкции.

```
PowerShell

Set-MailboxDatabase <DatabaseName> -AllowFileRestore $true
```

4. Переместите файлы базы данных (EDB-файл, файлы журналов и каталог поиска Exchange) в папку базы данных, указанную при создании новой базы данных.

5. Подключите базу данных с помощью следующей синтаксической конструкции:

```
PowerShell

Mount-Database <DatabaseName>
```

6. После подключения базы данных измените параметры учетной записи пользователя с помощью командлета Set-Mailbox, чтобы учетная запись указывала на почтовый ящик на новом сервере почтовых ящиков. Чтобы переместить всех пользователей из старой базы данных в новую, введите команду в следующем формате.

```
PowerShell

Get-Mailbox -Database <SourceDatabase> |where {$_.ObjectClass -NotMatch
'(SystemAttendantMailbox|ExOleDbSystemMailbox)'}| Set-Mailbox -Database
<TargetDatabase>
```

7. Инициировать доставку любых сообщений, оставшихся в очередях, можно с помощью следующей команды.

```
PowerShell

Get-Queue <QueueName> | Retry-Queue -Resubmit $true
```

После завершения репликации Active Directory все пользователи смогут получить доступ к своим почтовым ящикам на новом сервере Exchange Server. Большинство

клиентов перенаправляются через службу автообнаружения. Outlook в Интернете пользователи также перенаправляются автоматически.

Как проверить, все ли получилось?

Чтобы убедиться, что почтовый ящик успешно перемещен, выполните следующие действия.

- Откройте почтовый ящик с помощью Outlook в Интернете.
- Откройте почтовый ящик с помощью Microsoft Outlook.

Переносимость звонка в Exchange Server

Статья • 04.04.2023

Перенос звонка — это функция Exchange Server 2016 и Exchange Server 2019 годах, которая предоставляет ограниченное решение для непрерывности бизнес-процессов при сбоях, влияющих на базу данных почтовых ящиков, сервер или весь сайт. Временный почтовый ящик поддерживает возможность отправки электронной почты пользователями, и этот почтовый ящик может находиться на том же сервере почтовых ящиков Exchange или на любом другом сервере почтовых ящиков Exchange в вашей организации при условии, что они содержат базы данных с той же версией схемы базы данных. Это позволяет на альтернативном сервере размещать почтовые ящики пользователей, которые ранее находились на сервере, который больше недоступен. Клиенты, поддерживающие автообнаружения, автоматически перенаправляются на новый сервер без необходимости вручную обновлять профиль рабочего стола пользователя. После восстановления данных исходного почтового ящика пользователя администратор может объединить восстановленный и аварийный почтовые ящики пользователя в один обновленный почтовый ящик.

Процесс использования переносимости аварийного восстановления называется *аварийным восстановлением*. Аварийное восстановление включает в себя создание на сервере почтовых ящиков пустой базы данных вместо неисправной. Эта пустая база данных, которая называется *аварийной базой данных*, позволяет пользователям отправлять и получать сообщения электронной почты, пока неисправная база данных восстанавливается.

Существуют три варианта выполнения аварийного восстановления.

- **Восстановление звонка на сервере с неработоспособной базой данных**. Если сервер, на котором размещена сбойная база данных, по-прежнему работает, рекомендуется выполнить восстановление звонка на этом сервере. Это уменьшает время простоя, так как не требуется перемещать файлы базы данных между серверами. Кроме того, не понадобится изменять конфигурации профилей системы обмена сообщениями для клиентов, не поддерживающих автообнаружение.

- **Восстановление абонентского сигнала с помощью альтернативного сервера для базы данных абонентского номера**. Если сервер завершается сбоем и его необходимо перестроить, наиболее эффективный способ предоставить

пользователям базовые функции электронной почты — создать базу данных абонентского номера на другом сервере и использовать перенос базы данных для перемещения конфигурации почтового ящика пользователей на этот новый сервер. Так как этот процесс включает возвращение аварийной базы данных на первоначальный (восстановленный) сервер, этот вариант увеличивает время полного восстановления. Кроме того, этот процесс сложнее, чем выполнение аварийного восстановления на первоначальном сервере. Чтобы выполнить этот процесс, сервер, на котором размещается аварийная база данных, должен иметь необходимые для обслуживания дополнительных пользователей ресурсы. Кроме того, если клиент пользователя не поддерживает функцию автообнаружения, необходимо настроить профиль системы обмена сообщениями, чтобы он указывал на аварийный сервер.

- **Восстановление абонентского сигнала с помощью и пребывания на альтернативном сервере для базы данных абонентского сигнала**. Этот вариант аналогичен предыдущему параметру, за исключением того, что вы не возвращаетесь к исходному серверу. Этот вариант рекомендуется для случаев, когда восстанавливать неисправный сервер невозможно или нецелесообразно. В этом сценарии после выполнения операции восстановления пользователи обычно остаются на альтернативном. Чтобы выполнить этот процесс, сервер, на котором размещается аварийная база данных, должен иметь необходимые для обслуживания дополнительных пользователей ресурсы. Кроме того, если клиент пользователя не поддерживает функцию автообнаружения, необходимо настроить профиль системы обмена сообщениями, чтобы он указывал на аварийный сервер.

Все три варианта состоят из одинаковых основных шагов, приведенных ниже.

1. **Создание пустой аварийной базы данных для замены неисправной.**

   Эта новая база данных разрешит пользователям, почтовые ящики которых находились в неисправной базе данных, отправлять и получать новые сообщения. Переносимость аварийного восстановления позволяет перенаправить пользователя в другую базу данных без перемещения почтового ящика. Если аварийная база данных создается на сервере, отличном от сервера, на котором размещалась неисправная база данных, потребуется переместить конфигурацию почтового ящика на новый сервер.

2. **Восстановление старой базы данных.**

   Воспользуйтесь стандартно используемым программным обеспечением для резервного копирования и восстановления, чтобы восстановить неисправную

базу данных. Если отсутствует резервная копия неисправной базы данных, по возможности восстановите неисправную базу данных другими средствами. При использовании для аварийного восстановления того же сервера, на котором размещена неисправная база данных, понадобится восстановить базу данных в базу данных восстановления.

3. **Замена аварийной базы данных на восстановленную.**

   После восстановления неисправной базы данных замените ее на аварийную. Это позволит пользователям отправлять и получать электронную почту, а также получать доступ ко всем данным в восстановленной базе данных. Если пользователи перемещены в аварийную базу данных на другом сервере, понадобится переместить конфигурацию почтовых ящиков обратно на исходный сервер.

4. **Слияние баз данных.**

   Чтобы перенести данные из аварийной базы данных в восстановленную базу данных, данные объединяются с помощью командлета New-MailboxRestoreRequest.

Шаги аварийного восстановления подробно описаны в статье Выполнение аварийного восстановления.

Восстановление звонка в Exchange Server

Статья • 04.04.2023

Процесс использования переносимости абонентского номера называется восстановлением абонентского номера, который включает в себя создание пустой базы данных на сервере почтовых ящиков для замены базы данных, которая завершила сбой. Дополнительные сведения см. в разделе Переносимость абонентского сигнала.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут плюс время, необходимое для восстановления данных.
- Для создания базы данных абонентского номера должно быть развернуто меньше максимального количества баз данных (не более пяти баз данных на сервер для Exchange Standard Edition, не более 100 баз данных на сервер для Exchange выпуск Enterprise).
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Восстановление почтового ящика" в разделе Разрешения получателей .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование командной консоли Exchange для восстановления звонка на одном сервере

> **Примечание**
>
> Невозможно использовать Центр администрирования Exchange для выполнения аварийного восстановления на одном сервере.

1. Убедитесь, что все существующие файлы восстанавливаемой базы данных сохраняются на случай необходимости восстановления в дальнейшем.

2. Используйте командлет New-MailboxDatabase для создания аварийной базы данных, как показано в следующем примере.

   PowerShell

   ```
   New-MailboxDatabase -Name DTDB1 -EdbFilePath D:\DialTone\DTDB1.EDB
   ```

3. Используйте командлет Set-Mailbox для перемещения почтовых ящиков пользователей, сохраненных в восстанавливаемой базе данных, как показано в следующем примере.

   PowerShell

   ```
   Get-Mailbox -Database DB1 | Set-Mailbox -Database DTDB1
   ```

4. Используйте командлет Mount-Database для подключения базы данных, чтобы разрешить клиентским компьютерам получать к ней доступ, а также отправлять и получать сообщения, как показано в следующем примере.

   PowerShell

   ```
   Mount-Database -Identity DTDB1
   ```

5. Создайте базу данных восстановления (RDB) и восстановите или скопируйте файлы базы данных и журналов, содержащие данные, которые нужно восстановить, в RDB. Подробные инструкции см. в разделе Создание базы данных восстановления.

6. После копирования данных в базу данных восстановления, но перед подключением восстановленной базы данных, необходимо скопировать все файлы журнала из неисправной базы данных в папку журналов базы данных восстановления, чтобы их можно было просматривать в восстановленной базе данных.

7. Подключите базу данных восстановления, а затем используйте командлет Dismount-Database, чтобы отключить ее, как показано в следующем примере.

```
PowerShell

Mount-Database -Identity RDB1
Dismount-Database -Identity RDB1
```

8. После отключения базы данных восстановления переместите текущую базу данных и файлы журнала из папки базы данных восстановления в безопасное местоположение. Это необходимо для подготовки к переключению с базы данных восстановления на аварийную базу данных.

9. Отключите аварийную базу данных, как показано в следующем примере. Обратите внимание, что во время отключения базы данных прерывается обслуживание конечных пользователей.

```
PowerShell

Dismount-Database -Identity DTDB1
```

10. Переместите базу данных и файлы журнала из папки аварийной базы данных в папку базы данных восстановления.

11. Переместите базу данных и файлы журнала из безопасного местоположения, содержащего восстановленную базу данных, в папку аварийной базы данных, а затем подключите базу данных, как показано в следующем примере.

```
PowerShell

Mount-Database -Identity DTDB1
```

    Это возобновит обслуживание конечных пользователей. Пользователи смогут получить доступ к исходной рабочей базе данных, а также отправлять и получать сообщения.

12. Подключите базу данных восстановления, как показано в следующем примере.

```
PowerShell

Mount-Database -Identity RDB1
```

13. Используйте командлеты Get-Mailbox и New-MailboxRestoreRequest для экспорта данных из базы данных восстановления и их импорта в восстановленную базу, как показано в следующем примере. Все сообщения, отправленные и полученные с помощью аварийной базы данных, будут импортированы в рабочую базу данных.

    PowerShell

    ```
    $mailboxes = Get-Mailbox -Database DTDB1
    ```

    PowerShell

    ```
    $mailboxes | %{ New-MailboxRestoreRequest -SourceStoreMailbox
    $_.ExchangeGuid -SourceDatabase RDB1 -TargetMailbox $_ }
    ```

14. После завершения операции восстановления можно отключить и удалить базу данных восстановления, как показано в следующем примере.

    PowerShell

    ```
    Dismount-Database -Identity RDB1
    Remove-MailboxDatabase -Identity RDB1
    ```

Дополнительные сведения о синтаксисе и параметрах см. в следующих разделах:

- New-MailboxDatabase
- Get-Mailbox
- Set-Mailbox
- Mount-Database
- Dismount-Database
- Remove-MailboxDatabase

Как проверить, все ли получилось?

Чтобы убедиться, что почтовый ящик успешно перемещен, выполните следующие действия.

- Откройте почтовый ящик с помощью Outlook в Интернете.

- Откройте почтовый ящик с помощью Microsoft Outlook.

Управляемая доступность

Статья • 04.04.2023

Удобство работы пользователей с электронной почтой всегда было основной целью администраторов систем обмена сообщениями. В организации Exchange Server необходимо активно отслеживать все аспекты системы и быстро устранять все обнаруженные проблемы. Это позволяет сделать компонент *управляемой доступности* благодаря встроенным возможностям мониторинга и действиям по восстановлению, чтобы улучшить впечатления от использования.

Управляемая доступность

Управляемая доступность, также известная как *активный мониторинг* или *локальный активный мониторинг*, представляет собой интеграцию встроенных действий мониторинга и восстановления с платформой высокого уровня доступности Exchange. Она создана для обнаружения проблем и восстановления после них сразу после их возникновения и обнаружения системой. В отличие от предыдущих решений и методов мониторинга для Exchange функция управляемой доступности не пытается определить основную причину проблемы или уведомить о ней пользователей. Она сконцентрирована на восстановлении, а именно на трех ключевых аспектах работы пользователей:

- **Доступность**. Могут ли пользователи получить доступ к службе?
- **Задержка**. Как это происходит для пользователей?
- **Ошибки**. Могут ли пользователи выполнить то, что они хотят?

Управляемая доступность предлагает решение по наблюдению за работоспособностью и аварийному восстановлению. Она отходит от наблюдения за отдельными срезами системы, выполняя сквозное наблюдение за работой пользователей и защищая работу конечных пользователей путем ориентированных на восстановление вычислений.

Управляемая доступность — это внутренний процесс, который выполняется на каждом сервере Exchange Server. Он каждую секунду опрашивает и анализирует сотни метрик работоспособности. Если что-то не так, то в большинстве случаев проблема будет исправлена автоматически. Но всегда будут неполадки, которые функция управляемой доступности не сможет устранить самостоятельно. В таких случаях управляемая доступность будет передавать проблему администратору с ведением журнала событий.

Управляемая доступность реализуется в форме две службы:

- **Служба диспетчера работоспособности Exchange (MSExchangeHMHost.exe)**: это процесс контроллера, используемый для управления рабочими процессами. Он используется для создания, выполнения, запуска и остановки рабочих процессов по мере необходимости. Он также используется для восстановления рабочих процессов при сбоях, чтобы рабочие процессы не становились едиными точками отказа.
- **Рабочий процесс Диспетчера работоспособности Exchange (MSExchangeHMWorker.exe)**: это рабочий процесс, отвечающий за выполнение задач во время выполнения в управляемой платформе доступности.

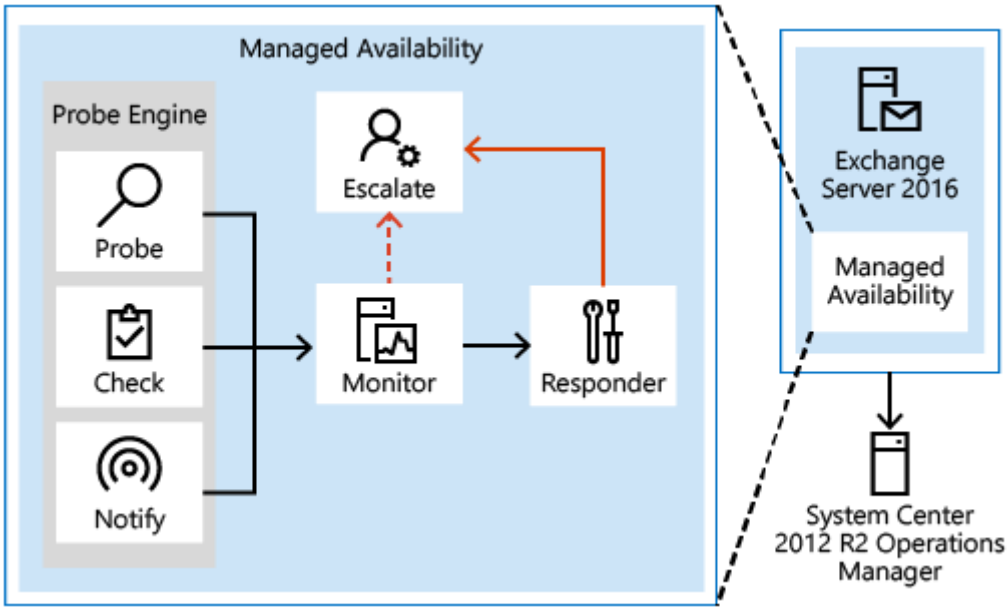
Управляемая доступность использует постоянное хранилище для выполнения своих функций:

- XML-файлы в папке \bin\Monitoring\config используются для хранения параметров конфигурации некоторых рабочих элементов зондов и мониторов.
- Active Directory используется для хранения глобальных переопределений.
- Реестр Windows используется для хранения данных времени выполнения, например закладок, и локальных переопределений (для определенного сервера).
- Инфраструктура журнала событий красного канала Windows используется для хранения результатов рабочих элементов.
- Почтовые ящики работоспособности используются для операций зондов. Для каждой базы данных почтовых ящиков на сервере создается несколько почтовых ящиков работоспособности.

Компоненты управляемой доступности

Как показано на следующем рисунке, управляемая доступность содержит три главных асинхронных компонента, которые непрерывно выполняют работу.

Компоненты управляемой доступности



Зонды

Первый компонент называется *зондом*. Зонды отвечают за измерения на сервере и сбор данных.

Существует три основных категории зондов: повторяющиеся зонды, уведомления и проверки. Повторяющиеся зонды — это выполняемые системой искусственные транзакции по тестированию работы пользователей. Проверки — это инфраструктура, которая выполняет сбор данных о производительности, включая трафик пользователя. Кроме того, они проверяют собранные данные на соответствие порогам, установленным для определения пиков среди ошибок пользователей, что позволяет инфраструктуре проверок узнавать о возникновении ошибок у пользователей. Наконец, логика уведомлений позволяет системе в случае критического события незамедлительно принять меры и не ждать результатов данных, собранных зондом. Это типичные исключения или условия, которые могут быть обнаружены и распознаны без большого набора образцов.

Периодично запускаемые зонды каждые несколько минут оценивают некоторые аспекты работоспособности службы. Они могут передавать электронные сообщения через службу Exchange ActiveSync в почтовый ящик мониторинга, подключаться к конечной точке RPC или проверять возможность подключения для клиентского доступа к почтовому ящику.

Все зонды определяются при запуске службы диспетчера работоспособности в красном канале Microsoft.Exchange.ActiveMonitoring\ProbeDefinition. Каждое определение пробы имеет множество свойств, но наиболее релевантные свойства:

- **Имя** Имя пробы, начинающееся с *sampleMask* монитора пробы.
- **TypeName**. Код типа объекта зонда, который содержит его логику.

- **ServiceName**. Имя настроек работоспособности, в которые входит этот зонд.
- **TargetResource** Объект, проверяемый пробой. При выполнении он добавляется к имени зонда для получения результата зонда, *ResultName*.
- **RecurrenceIntervalSeconds**. Частота выполнения зонда.
- **TimeoutSeconds**. Время ожидания зонда до появления ошибки.

Существуют сотни повторяющихся зондов. Большинство из них создаются для отдельных баз данных, поэтому их количество растет с числом баз данных. Большинство зондов определяются в коде, поэтому их невозможно обнаружить напрямую.

В основе повторяющихся зондов лежит запуск через равные промежутки времени (*RecurrenceIntervalSeconds*) и проверка (или зондирование) некоторых аспектов работоспособности. Если компонент работоспособен, зонд записывает информационное событие в канал Microsoft.Exchange.ActiveMonitoring\ProbeResult с параметром *ResultType*, имеющим значение 3. Если происходит ошибка проверки или истекает время ожидания, зонд выдает ошибку и записывает сообщение об ошибке в тот же канал. *Тип результата* 4 означает, что проверка завершилась сбоем, а *resultType* 1 означает, что истекло время ожидания. Если истекает время ожидания, многие пробы будут выполняться повторно до значения свойства *MaxRetryAttempts*.

> ⓘ **Примечание**
>
> Индивидуальный канал ProbeResult может быть занят сотнями зондов, которые выполняются каждые несколько минут и записывают события в журнал. Это может существенно повлиять на производительность сервера Exchange при создании ресурсоемких запросов для журналов событий в производственной среде.

Уведомления — это зонды, которые выполняет не инфраструктура диспетчера работоспособности, а некоторые другие службы на сервере. Эти службы проводят собственный мониторинг, а затем передают их данные в инфраструктуру управляемой доступности, напрямую записывая результаты зондов. Эти зонды не отображаются в канале ProbeDefinition, поскольку в нем описываются только зонды, выполняемые инфраструктурой управляемой доступности. Например, монитор ServerOneCopyMonitor активируют результаты зонда, записанные службой MSExchangeDAGMgmt. Эта служба выполняет собственный мониторинг, определяет наличие проблемы и записывает в журнал результаты зонда.

Большинство зондов-уведомлений могут записывать в журнал как красные события (указывают на неработоспособный монитор), так и зеленые (возобновление работоспособности монитора).

Проверки — это зонды, которые записывают в журнал события, только когда счетчик производительности становится больше или меньше порогового значения. На самом деле они представляют особый случай зондов-уведомлений, так существует служба, которая отслеживает счетчики производительности на сервере и записывает события в журнал канала ProbeResult, если достигнуто заданное пороговое значение.

С помощью монитора для этой проверки можно определить счетчик и пороговое значение, которые считаются неработоспособными. Мониторы типа *Microsoft.Office.Datacenter.ActiveMonitoring.OverallConsecutiveSampleValueAboveThresholdMonitor* или *Microsoft.Office.Datacenter.ActiveMonitoring.OverallConsecutiveSampleValueBelowThresholdMonitor* означают, что зонд, который они отслеживают, является пробой проверки.

Мониторинг

Результаты собранных зондами измерений поступают во второй компонент — *монитор*. Монитор содержит всю используемую системой бизнес-логику, основанную на собранных данных. Подобно подсистеме распознавания шаблонов, монитор ищет различные шаблоны среди всех собранных измерений, а затем принимает решение, можно ли считать компонент работоспособным.

Мониторы отправляют запросы данным, чтобы определить, требуются ли действия на основании предварительно определенного набора правил. В зависимости от правила или природы ошибки монитор может инициировать отвечающее устройство или передать ошибку на обработку человеку, выполнив запись в журнале событий. Кроме того, мониторы определяют, сколько времени после сбоя выполняется ответчик, и рабочий процесс действия восстановления. Мониторы имеют различные состояния. С точки зрения состояния системы мониторы имеют два состояния:

- **Работоспособность**. Монитор работает правильно, и все собранные метрики находятся в пределах нормальных рабочих параметров.
- **Неработоспособно**. Монитор не работоспособен и инициировал восстановление через ответчика или уведомил администратора путем эскалации.

С точки зрения администрирования мониторы имеют дополнительные состояния, которые отображаются в командной консоли Exchange:

- **Пониженная производительность**. Если монитор находится в неработоспособном состоянии от 0 до 60 секунд, он считается неработоспособным. Если монитор пребывает в неработоспособном состоянии дольше 60 секунд, он считается неработоспособным.

- **Отключено**: монитор был явно отключен администратором.

- **Недоступно**: служба работоспособности Exchange периодически запрашивает состояние каждого монитора. Если служба не получает ответ на запрос, состояние монитора изменяется на "Недоступный".

- **Исправление**. Администратор задает состояние восстановления, чтобы указать системе, что корректирующее действие выполняется человеком, что позволяет системе и людям различать другие сбои, которые могут произойти в то же время, когда выполняется корректирующее действие (например, операция повторного копирования базы данных).

Каждый монитор имеет свойство *SampleMask* в своем определении. При выполнении монитора он ищет события в канале ProbeResult, имеющие *имя результата* , соответствующее *образцуMask* монитора. Эти события могут происходить из повторяющихся зондов, уведомлений или проверок. Если достигнуто пороговое значение монитора, он становится неработоспособным. С точки зрения монитора все три типа зондов одинаковые, ведь каждый из них создает записи в журнале канала ProbeResult.

Стоит отметить, что сбой одной пробы не обязательно указывает на то, что что-то не так с сервером. Это дизайн мониторов, чтобы правильно определить, когда есть реальная проблема, которая требуется устранить. Вот почему многие мониторы имеют пороговые значения нескольких сбоев пробы, прежде чем стать неработоспособными. Даже в этом случае многие из этих проблем могут быть автоматически устранены ответчиками, поэтому лучше всего искать проблемы, требующие вмешательства вручную, — в канале Microsoft.Exchange.ManagedAvailability\Monitoring crimson. Это будет включать последнюю ошибку пробы.

Ответчики

Наконец, *ответчики* предпринимают действия по восстановлению и эскалации. Как следует из их названия, ответчики реализуют определенный ответ на оповещение от монитора. Если что-то не работает, первое действие — попытка

восстановления соответствующего компонента. Это могут быть действия по многоуровневому восстановлению, например сначала последовательно перезапускаются пул приложений, служба и сервер, а в самом конце сервер переводится в автономный режим и не может принимать трафик. Если действия по восстановлению не помогают, система через журнал уведомляет о проблеме оператора-человека.

Ответчики выполняют различные действия по восстановлению, такие как сброс пула рабочих ролей приложений или перезапуск сервера. Существует несколько видов ответчиков:

- **Ответчик перезапуска** — завершает и перезапускает службу.
- **Ответчик сброса пула приложений** — останавливает и перезапускает пул приложений в службах IIS.
- **Ответчик отработки отказа** — инициирует отработку отказа базы данных или сервера.
- **Ответчик критической ошибки** — инициирует критическую ошибку сервера, приводящую к его перезагрузке.
- **Автономный ответчик** — отключает протокол на сервере (отклоняет запросы клиентов).
- **Оперативный ответчик** — активирует протокол на сервере (принимает запросы клиентов).
- **Ответчик эскалации** — передает проблему администратору с помощью журнала событий.

Помимо указанных ответчиков у некоторых компонентов также есть специализированные уникальные ответчики.

Все средства реагирования включают в себя поведение регулирования, которое предоставляет встроенный механизм виртуализации для управления действиями ответчика. Регулирование позволяет добиться того, что система не будет скомпрометирована или не выйдет из строя в результате операций восстановления ответчика. Все ответчики регулируются одинаково. При регулировании действие восстановления ответчика может быть пропущено или отложено в зависимости от действия. Например, когда ответчик регулируется ответчик критической ошибки, его действие пропускается, а не задерживается.

Настройки работоспособности

С точки зрения отчетности управляемая доступность реализует два представления работоспособности: внутреннее и внешнее.

Во внутреннем представлении используются *наборы работоспособности*. Каждый компонент в Exchange Server (например, Outlook в Интернете, Exchange ActiveSync, служба хранилища сведений, индексирование контента, транспортные службы и т. д.) отслеживается управляемой доступностью с помощью проб, мониторов и ответчиков. Группа проб, мониторов и ответчиков для данного компонента называется *набором работоспособности*. Набор работоспособности — это группа проб, мониторов и средств реагирования, которые определяют работоспособность этого компонента. Текущее состояние набора работоспособности (например, является ли он работоспособным или неработоспособным) определяется с помощью мониторов набора работоспособности. Если все мониторы набора работоспособности работоспособны, то набор работоспособности находится в работоспособном состоянии. Если какой-либо монитор не находится в работоспособном состоянии, состояние набора работоспособности будет определяться его наименее работоспособным монитором.

Подробные инструкции для просмотра работоспособности сервера или состояния набора оценки работоспособности см. в статье Manage health sets and server health.

Группы работоспособности

Внешнее представление управляемой доступности состоит из *групп работоспособности*. Группы работоспособности доступны для System Center Operations Manager 2012 R2.

Существует четыре основных группы работоспособности:

- **Точки соприкосновения с пользователями.** Компоненты, которые влияют на взаимодействие с пользователями в реальном времени, например протоколы или банк данных.
- **Компоненты служб.** Компоненты без прямого взаимодействия с пользователями в реальном времени, например служба репликации почтовых ящиков Microsoft Exchange или процесс создания автономной адресной книги (OABGen).
- **Серверные компоненты** Физические ресурсы сервера, такие как место на диске, память и сеть.
- **Доступность зависимостей** Возможность доступа сервера к необходимым зависимостям, таким как Active Directory, DNS и т. д.

Если установлен пакет управления Exchange, System Center Operations Manager (SCOM) служит порталом работоспособности для просмотра сведений, связанных со средой Exchange. Панель мониторинга SCOM содержит три представления работоспособности сервера Exchange:

- **Активные оповещения** Средства реагирования на эскалацию записывают события в журнал событий Windows, которые используются монитором в SCOM. Они отображаются в виде оповещений в представлении активных оповещений.

- **Работоспособности организации** В этом представлении отображается сводная сводка по общему состоянию работоспособности организации Exchange. Эти накопительные пакеты включают отображение работоспособности для отдельных групп доступности баз данных и работоспособности на определенных сайтах Active Directory.

- **Работоспособность сервера.** Связанные настройки работоспособности объединяются в группы работоспособности, сводная информация о которых отображается в этом представлении.

Переопределения

Переопределения позволяют администратору настраивать некоторые аспекты зондов, мониторов и ответчиков управляемой доступности. Переопределения можно использовать для точной настройки некоторых пороговых значений, используемых компонентом управляемой доступности. С их помощью также можно включить экстренные действия для непредвиденных событий, для которых могут потребоваться параметры конфигурации, отличных от настроек по умолчанию.

Переопределения можно создать и применять для одного сервера (это называют *переопределением сервера*) или для группы серверов (*глобальное переопределение*). Данные конфигурации переопределения сервера хранятся в реестре Windows на сервере, к которому применяется переопределение. Данные конфигурации глобального переопределения хранятся в Active Directory.

Переопределения можно настраивать без срока действия или с заданным сроком действия. Кроме того, глобальные переопределения можно настроить для всех серверов или только серверов с определенной версией Exchange.

При настройке переопределения оно не вступит в силу немедленно. Служба диспетчера работоспособности Microsoft Exchange проверяет наличие

обновленных данных конфигурации каждые 10 минут. Кроме того, глобальные переопределения зависят от задержки репликации Active Directory.

Подробные инструкции по просмотру или настройке серверных или глобальных переопределений см. в разделе Настройка управляемых переопределений доступности.

Задачи управления и командлеты

Существует три основных операционных задачи, которые администраторы обычно выполняют в отношении управляемой доступности:

- извлечение или просмотр состояния системы;
- просмотр настроек работоспособности и сведений о зондах, мониторах и ответчиках;
- управление переопределениями.

Двумя основными средствами управления для управляемой доступности являются журнал событий Windows и командная консоль Exchange. Компонент управляемой доступности записывает много информации в красные каналы ActiveMonitoring и ManagedAvailability журналов событий Exchange, например:

- определения зондов, мониторов и ответчиков, которые записываются в соответствующие журналы событий *Definition;
- результаты зондов, мониторов и ответчиков, которые записываются в соответствующие журналы событий *Results;
- Сведения о действиях восстановления ответчика, в том числе о запуске действия восстановления, и оно считается завершенным (успешно или нет), которые регистрируются в журнале событий RecoveryActionResults.

Существует 12 командлетов для управляемой доступности, которые описаны в следующей таблице.

Командлет	Описание

Командлет	Описание
Get-ServerHealth	Используется для получения необработанной информации о работоспособности сервера, например настройки работоспособности и их текущее состояние (исправно или нет), мониторы настроек работоспособности, серверные компоненты, целевые ресурсы для зондов и временные метки, связанные с временем запуска или остановки зонда или монитора, а также время перехода в то или иное состояние.
Get-HealthReport	Используется для получения сводного представления работоспособности, которое включает в себя настройки работоспособности и их текущее состояние.
Get-MonitoringItemIdentity	Используется для просмотра зондов, мониторов и ответчиков, связанных с определенными настройками работоспособности.
Get-MonitoringItemHelp	Используется для просмотра описания некоторых свойств зондов, мониторов и ответчиков.
Add-ServerMonitoringOverride	Используется для создания локального, предназначенного для конкретного сервера переопределения зонда, монитора или ответчика.
Get-ServerMonitoringOverride	Используется для просмотра списка локальных переопределений на указанном сервере.
Remove-ServerMonitoringOverride	Используется для удаления локального переопределения на указанном сервере.
Add-GlobalMonitoringOverride	Используется для создания глобального переопределения для группы серверов.
Get-GlobalMonitoringOverride	Используется для просмотра списка глобальных переопределяет, настроенных в организации.
Remove-GlobalMonitoringOverride	Используется для удаления глобального переопределения.
Set-ServerComponentState	Используется для настройки состояния одного или нескольких серверных компонентов.
Get-ServerComponentState	Используется для просмотра состояния одного или нескольких серверных компонентов.

Управление наборами работоспособности и работоспособностью сервера в Exchange Server

Статья • 04.04.2023

Вы можете использовать встроенные командлеты отчетов о работоспособности для выполнения различных задач, связанных с управляемой доступностью, например:

- просмотр работоспособности сервера или группы серверов;
- просмотр списка настроек работоспособности;
- просмотр списка зондов, мониторов и ответчиков, связанных с определенными настройками работоспособности;
- просмотр списка мониторов и их текущего состояния.

Дополнительные сведения об отчетах о работоспособности и управляемой доступности см. в разделе Управляемая доступность.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 2 минуты
- Для процедур, описанных в этом разделе, требуется командная консоль Exchange. Дополнительные сведения см. в разделе Открытие командной консоли Exchange.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Просмотр работоспособности сервера с помощью командной консоли Exchange

Чтобы получить сводку о работоспособности сервера Exchange, можно использовать командную консоль Exchange.

Выполните следующую команду, чтобы просмотреть наборы работоспособности и сведения о работоспособности на сервере Exchange Server:

PowerShell

```
Get-HealthReport -Identity <ServerName>
```

PowerShell

```
Get-ServerHealth -Identity <ServerName> | Format-Table
Server,CurrentHealthSetState,Name,HealthSetName,AlertValue,HealthGroupName -
Auto
```

Выполните любую из следующих команд, чтобы просмотреть наборы работоспособности на сервере Exchange server или группе доступности базы данных:

PowerShell

```
Get-ExchangeServer | Get-HealthReport -RollupGroup
```

PowerShell

```
Get-ExchangeServer | Get-HealthReport -RollupGroup -HealthSetName
<HealthSet>
```

PowerShell

```
(Get-DatabaseAvailabilityGroup <DAGName>).Servers | Get-HealthReport -
RollupGroup
```

Подробные сведения о синтаксисе и параметрах см. в разделе Get-HealthReport.

Просмотр списка наборов работоспособности с помощью командной

консоли Exchange

Набор работоспособности — это группа мониторов, проб и средств реагирования для компонента, которые определяют, является ли компонент работоспособным или неработоспособным.

Выполните следующую команду, чтобы просмотреть наборы работоспособности на сервере Exchange Server:

```
PowerShell

Get-HealthReport -Server <ServerName>
```

Подробные сведения о синтаксисе и параметрах см. в разделе Get-HealthReport.

Использование командной консоли Exchange для просмотра проб, мониторов и ответов для набора работоспособности

С помощью командной консоли Exchange можно просмотреть список проб, мониторов и ответчиков, связанных с набором работоспособности на сервере Exchange Server.

Выполните следующую команду, чтобы просмотреть пробы, мониторы и ответчики, связанные с набором работоспособности на сервере Exchange Server:

```
PowerShell

Get-MonitoringItemIdentity -Server <ServerName> -Identity <HealthSetName> |
Format-Table Identity,ItemType,Name -Auto
```

Подробные сведения о синтаксисе и параметрах см. в разделе Get-MonitoringItemIdentity.

Использование командной консоли Exchange для просмотра списка мониторов и их текущей работоспособности

Состояние мониторов определяется на основе состояния «худших» мониторов в настройках работоспособности. Вы можете просмотреть сведения о настройках

работоспособности, чтобы узнать, какие мониторы исправны, а какие нет.

Выполните следующую команду, чтобы просмотреть список мониторов и их текущую работоспособность на сервере Exchange Server:

PowerShell

```
Get-ServerHealth -HealthSet <HealthSetName> -Server <ServerName> | Format-Table Name, AlertValue -Auto
```

Подробные сведения о синтаксисе и параметрах см. в разделе Get-ServerHealth.

Настройка переопределений управляемой доступности в Exchange Server

Статья • 04.04.2023

Управляемая доступность выполняет непрерывное проверка для обнаружения возможных проблем с компонентами Exchange или их зависимостями, а также выполняет действия по восстановлению, чтобы убедиться, что взаимодействие с конечным пользователем не влияет из-за проблем с любым из этих компонентов. Однако могут быть сценарии, в которых встроенные параметры могут не подходить для вашей среды. Управляемые пробы доступности, мониторы и ответчики можно настроить путем создания переопределения.

Существует два типа переопределений: локальные и глобальные. Как следует из их названия, локальные переопределения доступны только на сервере, на котором они созданы, а глобальные переопределения используются на нескольких серверах. Оба типа переопределения можно создать либо на определенный период времени, либо для заданной версии Exchange.

> ⓘ **Примечание**
>
> При создании переопределения оно вступит в силу не сразу. Служба управления работоспособностью Microsoft Exchange проверяет наличие изменений конфигурации каждые 10 минут и загружает все обнаруженные изменения. Если вы не хотите ждать, вы можете перезапустить службу.

Дополнительные сведения об управляемой доступности см. в статье Управляемое доступность. Дополнительные задачи управления, связанные с управляемой доступностью, см. в разделе Управление наборами работоспособности и работоспособностью сервера.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут
- Для процедур, описанных в этом разделе, требуется командная консоль Exchange. Чтобы открыть командную консоль Exchange, см. статью Запуск командной консоли Exchange.

- Для выполнения этой процедуры можно использовать только PowerShell. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование Командная консоль Exchange для создания локальных переопределений

Чтобы создать локальное переопределение на определенный период времени, используйте следующий синтаксис:

PowerShell

```
Add-ServerMonitoringOverride -Server <ServerName> -Identity <HealthSetName>\
<MonitoringItemName>[\<TargetResource>] -ItemType <Probe | Monitor |
Responder | Maintenance> -PropertyName <PropertyName> -PropertyValue <Value>
-Duration <dd.hh:mm:ss>
```

Чтобы создать локальное переопределение для определенной версии Exchange, используйте следующий синтаксис.

PowerShell

```
Add-ServerMonitoringOverride -Server <ServerName> -Identity <HealthSetName>\
<MonitoringItemName>[\<TargetResource>] -ItemType <Probe | Monitor |
Responder | Maintenance> -PropertyName <PropertyName> -PropertyValue <Value>
-Version <15.01.xxxx.xxx>
```

> **Примечание**
>
> При создании переопределения значения, используемые в параметре *Identity* , будут учитывать регистр.

В этом примере добавляется локальное переопределение, которое отключает ответчик `ActiveDirectoryConnectivityConfigDCServerReboot` на сервере с именем EXCH03 на 20 дней.

PowerShell

```
Add-ServerMonitoringOverride -Server EXCH03 -Identity
"AD\ActiveDirectoryConnectivityConfigDCServerReboot" -ItemType Responder -
PropertyName Enabled -PropertyValue 0 -Duration 20.00:00:00
```

Как проверить, все ли получилось?

Чтобы проверить, создано ли локальное переопределение, просмотрите список локальных переопределений с помощью командлета **Get-ServerMonitoringOverride**:

PowerShell

```
Get-ServerMonitoringOverride  -Server <ServerIdentity> | Format-List
```

Переопределение должно появиться в списке.

Использование Командная консоль Exchange для удаления локальных переопределений

Чтобы удалить локальное переопределение, используйте следующий синтаксис.

PowerShell

```
Remove-ServerMonitoringOverride -Server <ServerName> -Identity
<HealthSetName>\<MonitoringItemName>[\<TargetResource>] -ItemType
<ExistingItemTypeValue> -PropertyName <PropertytoRemove>
```

В этом примере удаляется существующее локальное переопределение ответчика `ActiveDirectoryConnectivityConfigDCServerReboot` в наборе работоспособности Exchange с сервера EXCH01.

PowerShell

```
Remove-ServerMonitoringOverride -Server EXCH01 -Identity
Exchange\ActiveDirectoryConnectivityConfigDCServerReboot -ItemType Responder
-PropertyName Enabled
```

Как проверить, все ли получилось?

Чтобы проверить, удалено ли локальное переопределение, просмотрите список локальных переопределений с помощью командлета **Get-ServerMonitoringOverride**:

```
PowerShell

Get-ServerMonitoringOverride  -Server <ServerIdentity> | Format-List
```

Переопределения не должно быть в списке.

Использование Командная консоль Exchange для создания глобальных переопределений

Чтобы создать глобальное переопределение на определенный срок, используйте следующий синтаксис.

```
PowerShell

Add-GlobalMonitoringOverride -Identity <HealthSetName>\<MonitoringItemName>
[\<TargetResource>] -ItemType <Probe | Monitor | Responder | Maintenance> -
PropertyName <PropertytoOverride> -PropertyValue <NewPropertyValue> -
Duration <dd.hh:mm:ss>
```

Чтобы создать глобальное переопределение для определенной версии Exchange, используйте следующий синтаксис.

```
PowerShell

Add-GlobalMonitoringOverride -Identity <HealthSetName>\<MonitoringItemName>
[\<TargetResource>] -ItemType <Probe | Monitor | Responder | Maintenance> -
PropertyName <PropertytoOverride> -PropertyValue <NewPropertyValue> -
ApplyVersion <15.01.xxxx.xxx>
```

> ⓘ **Примечание**
>
> При создании переопределения значения, используемые в параметре *Identity* , будут учитывать регистр.

В этом примере добавляется глобальное переопределение, которое отключает пробу на `OnPremisesInboundProxy` 30 дней.

PowerShell

```
Add-GlobalMonitoringOverride -Identity
"FrontendTransport\OnPremisesInboundProxy" -ItemType Probe -PropertyName
Enabled -PropertyValue 0 -Duration 30.00:00:00
```

В этом примере добавляется глобальное переопределение, которое отключает `StorageLogicalDriveSpaceEscalate` ответчик для всех серверов с Exchange версии 15.01.0225.042.

PowerShell

```
Add-GlobalMonitoringOverride -Identity
"MailboxSpace\StorageLogicalDriveSpaceEscalate" -PropertyName Enabled -
PropertyValue 0 -ItemType Responder -ApplyVersion "15.01.0225.042"
```

Как проверить, все ли получилось?

Чтобы проверить, было ли глобальное переопределение успешно создано, выполните командлет **Get-GlobalMonitoringOverride** для просмотра списка глобальных переопределений:

PowerShell

```
Get-GlobalMonitoringOverride
```

Переопределение должно появиться в списке.

Использование Командная консоль Exchange для удаления глобальных переопределений

Чтобы удалить глобальное переопределение, используйте следующий синтаксис.

PowerShell

```
Remove-GlobalMonitoringOverride -Identity <HealthSetName>\
<MonitoringItemName>[\<TargetResource>] -ItemType <ExistingItemTypeValue> -
PropertyName <OverriddenProperty>
```

В этом примере удаляется существующее глобальное переопределение `ExtensionAttributes` свойства пробы `OnPremisesInboundProxy` в наборе `FrontEndTransport` работоспособности.

PowerShell

```
Remove-GlobalMonitoringOverride -Identity
FrontEndTransport\OnPremisesInboundProxy -ItemType Probe -PropertyName
ExtensionAttributes
```

Как проверить, все ли получилось?

Чтобы проверить, было ли глобальное переопределение успешно удалено, выполните командлет **Get-GlobalMonitoringOverride** для просмотра списка глобальных переопределений:

PowerShell

```
Get-GlobalMonitoringOverride
```

Переопределения не должно быть в списке.

Работоспособность и производительность сервера в Exchange Server

Статья • 04.04.2023

Для проектирования и поддержки производительной инфраструктуры обмена сообщениями важно иметь представление о работоспособности и производительности серверов. Exchange 2016 и Exchange 2019 продолжают использовать функции, представленные в Exchange 2013, чтобы управлять работоспособностью и производительностью сервера.

Управляемая доступность

Управляемая доступность предоставляет встроенные действия мониторинга и восстановления, которые сохраняют взаимодействие с конечными пользователями. Управляемая доступность состоит из двух процессов: службы диспетчера работоспособности Exchange (MSExchangeHMHost.exe) и рабочего процесса диспетчера работоспособности Exchange (MSExchangeHMWorker.exe) и следующих компонентов:

- **Модуль пробы**. Модуль *пробы* выполняет измерения на сервере.
- **Подсистема проб мониторинга**. Подсистема *проб мониторинга* хранит бизнес-логику о том, что представляет собой работоспособное состояние. Он работает как система распознавания шаблонов, которая ищет шаблоны и измерения, отличающиеся от работоспособного состояния, и делает вывод о неработоспособности компонентов или функций.
- **Подсистема ответчика**. Когда *обработчик ответчика* оповещается о неработоспособном компоненте, он сначала пытается восстановить этот компонент. Управляемая доступность обеспечивает многоуровневость действий по восстановлению. Первой попыткой может быть перезапуск пула приложений, второй — перезапуск соответствующей службы, а третьей — перезагрузка сервера. Заключительной попыткой может быть перевод сервера в автономный режим, чтобы он больше не принимал трафик. Если по итогам всех этих действий проблема не устраняется, в службу поддержки отправляется предупреждение.

Дополнительные сведения об управляемой доступности см. в статье Управляемое доступность.

Управление рабочими нагрузками

Служба управления рабочими нагрузками состоит из следующих компонентов:

- *Управление рабочей нагрузкой пользователей* — это новое имя функций регулирования пользователей, появившихся в Exchange 2010. Эти параметры можно настраивать в соответствии с потребностями среды.
- *Управление системной рабочей нагрузкой* автоматически регулирует определенные рабочие нагрузки Exchange, отслеживая работоспособность основных ресурсов сервера. Эти параметры следует настраивать только по руководством Служба поддержки пользователей Майкрософт.

Дополнительные сведения об управлении рабочими нагрузками пользователей см. в разделе Управление рабочими нагрузками пользователей в Exchange Server.

Управление рабочей нагрузкой пользователей в Exchange Server

Статья • 04.04.2023

С помощью управления рабочими нагрузками пользователей вы можете контролировать использование системных ресурсов Exchange пользователями. Эта функция была доступна в Exchange 2010 (известной как *регулирование пользователей*) и была расширена до текущего уровня в Exchange 2013.

Рабочая нагрузка — это компонент, протокол или служба, которые явно определены для управления системными ресурсами на серверах Exchange. Каждая рабочая нагрузка потребляет системные ресурсы на сервере Exchange Server (например, ЦП, память, сеть и диск). К примерам рабочих нагрузок относятся Outlook в Интернете (предыдущее название — Outlook Web App), Exchange ActiveSync, перенос почтовых ящиков и помощники по обслуживанию почтовых ящиков.

Управление потреблением системных ресурсов Exchange пользователями

По умолчанию параметры рабочих нагрузок позволяют пользователям кратковременно увеличивать объем используемых ими ресурсов без снижения пропускной способности. Так как вы можете ограничить доступ пользователей к ресурсам, число экземпляров крупных потребителей ресурсов блокируется. Вы можете дополнительно бюджетировать потребление ресурсов пользователем, задав для пользователей ставку пополнения. В приведенном ниже списке представлены важные понятия, связанные с управлением рабочими нагрузками пользователей.

- **Квоты на ускорение**. Позволяет пользователям выполнять короткие периоды повышенного потребления ресурсов без какого-либо регулирования.
- **Ставка пополнения**. Использует бюджетную систему для управления потреблением ресурсов пользователем и указывает скорость начисления бюджета пользователя (насколько бюджет увеличивается) в течение бюджетного времени. Например, если время квоты составляет один час, то скорость зарядки 600 000 мс означает, что квота ресурсов для пользователей перезаряжается на десять минут использования в час.

- **Формирование трафика (микрослои).** Работает путем задержки пользователя на короткие периоды времени, когда его использование ресурсов достигает заданного предела за определенный интервал времени. Эта задержка возникает в течение очень коротких периодов времени (пользователи обычно не замечают задержку) и задолго до того, как потребление ресурсов значительно повлияет на производительность Exchange Server. Формирование трафика сохраняет доступность сервера Exchange Server, не блокируя производительность пользователей, оказывает меньшее влияние на пользователей, чем блокировка пользователей, и значительно снижает вероятность блокировки пользователя.

- **Максимальное использование**. Временно блокирует пользователя, достигшего максимального порогового значения ресурсов пользователя (пользователь потребляет необычно большое количество ресурсов в течение короткого интервала времени). Блокировка снимается, как только того позволит квота использования ресурсов для пользователя (после перезарядки квоты).

В командной консоли Exchange для управления пользовательской рабочей нагрузкой используются следующие командлеты:

- **Просмотр, создание, удаление и изменение параметров рабочей нагрузки пользователя**: Get-ThrottlingPolicy, New-ThrottlingPolicy, Remove-ThrottlingPolicy и Set-ThrottlingPolicy.

- **Назначение параметров рабочей нагрузки пользователей пользователям или компьютерам**: Get-ThrottlingPolicyAssociation и Set-ThrottlingPolicyAssociation

Области в параметрах рабочих нагрузок пользователей

По умолчанию существует одна политика регулирования с именем `GlobalThrottlingPolicy`. Для этой политики задана область "Глобальная", то есть она применяется ко всем пользователям в организации. Как правило, параметры стандартной политики регулирования подходят для пользователей в большинстве организаций Exchange. Вместо того чтобы настраивать стандартную политику регулирования, вы можете создавать собственные политики с другими параметрами. В пользовательских политиках регулирования доступны следующие области:

- **Организация**. Параметры регулирования применяются ко *всем* пользователям в организации.
- **Обычный**. Параметры регулирования, которые применяются только к *определенным* пользователям в организации.

Ниже описывается порядок применения политик регулирования.

1. Политики регулирования с областью "Обычная" применяются к пользователям раньше, чем политики для организации и стандартная политика регулирования.
2. Политики регулирования с областью "Организация" применяются к пользователям раньше, чем стандартная политика регулирования.
3. Стандартная политика регулирования применяется последней или только к тем пользователям, которым не назначены политики с областью "Обычная" или "Организация".

Если вы создаете пользовательские политики регулирования, их параметры должны быть не такими, как у стандартной политики. Следует учесть разницу в параметрах между политиками с областями "Обычная" и "Организация" и стандартной политикой (например, от менее строгих к более строгим или наоборот).

> ⓘ **Примечание**
>
> Настоятельно рекомендуем не менять стандартную политику регулирования, так как изменения стандартной политики могут быть переписаны при установке будущих обновлений Exchange. Вместо этого следует создавать пользовательские политики регулирования с персонализированными параметрами.

Регулирование пользователей в средах сосуществования Exchange 2010

Пользователи с почтовыми ящиками на серверах Exchange 2016 регулируются с помощью функций Exchange 2016, даже если среда Exchange 2016 установлена в организации Exchange 2010. В приведенном ниже списке представлены важные замечания касательно регулирования в средах с сосуществованием.

- Почтовые ящики Exchange 2010 регулируются с помощью функций Exchange 2010, даже если пользователи получают доступ к своим почтовым ящикам через серверы клиентского доступа Exchange 2010.
- При установке Exchange 2016 в организации Exchange 2010 программа установки Exchange 2016 может попробовать перенести некоторые параметры регулирования Exchange 2010. Однако функции регулирования так сильно отличаются, что старые параметры, скорее всего, не повлияют на регулирование в Exchange 2016.

Диагностические данные, собранные для Exchange Server

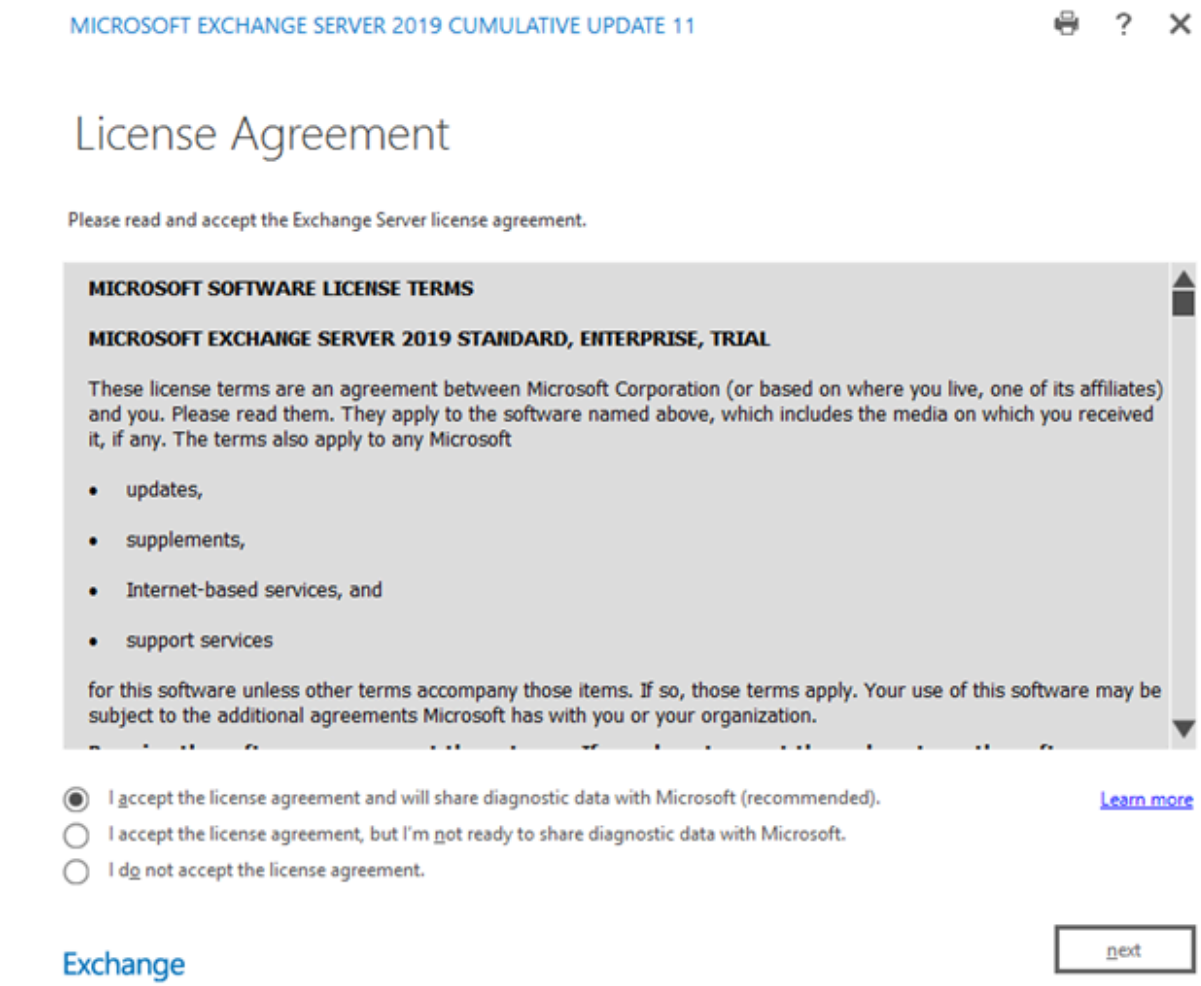
Статья • 11.02.2025

Корпорация Майкрософт собирает диагностические данные, чтобы поддерживать безопасность и актуальность Exchange Server, находить и устранять проблемы, а также выявлять и устранять угрозы. Когда накопительное обновление за сентябрь 2021 г. (или более поздняя версия) устанавливается на сервере почтовых ящиков, Exchange Server 2016 или Exchange Server 2019 может отправлять диагностические данные с каждого сервера Exchange в службу конфигурации Office (OCS) в облаке Майкрософт. В процессе принятия лицензионного соглашения изменено, чтобы вы могли выбрать, следует ли предоставлять доступ к диагностическим данным корпорации Майкрософт.

Изменение в процессе принятия срока лицензии

При использовании версии графического пользовательского интерфейса (GUI) программы установки Exchange появится новый экран лицензионного соглашения, как показано ниже.

Вместо двух вариантов теперь существует три варианта.



Выберите один из указанных ниже вариантов.

Развернуть таблицу

Выделение	Описание
Я принимаю условия лицензионного соглашения и буду передавать диагностические данные в Майкрософт	Это параметр по умолчанию, который принимает лицензионное соглашение и позволяет отправлять данные в корпорацию Майкрософт.
Я принимаю лицензионное соглашение, но не готов делиться диагностическими данными с корпорацией Майкрософт	Этот параметр принимает лицензионное соглашение, но запрещает отправку данных в корпорацию Майкрософт.
Я не принимаю условия лицензионного соглашения	Если вы не принимаете лицензионное соглашение, вы не сможете установить накопительный пакет обновления.

Автоматическая установка Exchange Server

Параметры принятия также доступны при автоматической установке из командной строки с использованием новых переключателей установки:

Развернуть таблицу

Выделение	Описание
/IAcceptExchangeServerLicenseTerms_DiagnosticDataON	Используйте этот переключатель, чтобы принять условия лицензии и отправлять необязательные данные в корпорацию Майкрософт, когда служба EM запрашивает меры по устранению рисков.
/IAcceptExchangeServerLicenseTerms_DiagnosticDataOFF	Используйте этот новый переключатель установки, чтобы принять условия лицензии и отключить отправку необязательных данных в корпорацию Майкрософт.

> **ⓘ Важно!**
>
> Параметр **/IAcceptExchangeServerLicenseTerms** был удален из программы установки Exchange Server из командной строки и заменен двумя новыми переключателями установки, показанными выше.

Собранные диагностические данные

Если сбор диагностических данных включен, ваш сервер Exchange ежечасно отправляет в службу конфигурации Office следующую информацию:

Развернуть таблицу

Data	Описание
ExchangeVersion	Версия сервера (сведения о сборке CU и SU)
ServiceState	Сведения о состоянии службы по устранению последствий чрезвычайных ситуаций (`enabled` или `disabled`)
ImmutableDeviceId	Уникальный идентификатор сервера
ImmutableOrgId	Уникальный идентификатор для организации Exchange

Data	Описание
КонфигурацииПриложения	Список всех примененных мер по устранению рисков
ConfigurationsBlocked	Список всех заблокированных мер по устранению рисков
MiscConfigurations	Сведения о следующем Exchange Server состоянии компонента: • `SerializationSigningEnabled` • `MSIPCEnabled` • `EncryptionAlgorithmCBCEnabled`

Начиная с Exchange Server 2019 CU15 (2025H1), Exchange Server собирает следующие дополнительные данные телеметрии:

Развернуть таблицу

Data	Описание
PrimaryKey	Уникальный идентификатор сервера, который выступает в качестве первичного ключа: `{OrganizationId}.{DeviceId}`
OrganizationId	Уникальный идентификатор для организации Exchange
DeviceId	Уникальный `MachineId` идентификатор сервера
RemoteMailboxCount	Общее число почтовых ящиков, где `RecipientTypeDetails` — `RemoteUserMailbox`
ServerVersion	Номер сборки Exchange Server сборки, выполняемой на сервере
ServerRole	Роль Exchange Server, запущенная на сервере
IsPPE	Указывает, является ли это предварительной установкой Exchange Server (по умолчанию — `false`).
MailBoxDataValue	Общее число почтовых ящиков в организации и на базе сервера Exchange Server
AuthServerDataList	Сведения о настроенном `Auth Server` в организации: • `Name` • `AuthMetaDataURL` • `IsDefaultAuthorizationEndpoint` • `TokenIssuingEndpoint` • `ApplicationIdentifier`
AcceptedDomainsList	Сведения о настроенном `Accepted Domains` в организации: • `DomainName`

Data	Описание
	• `IsTenantDomain` • `IsDefault`
AmsiDataValue	Сведения о конфигурации `AMSI` : • `EnabledAll` • `EnabledApi` • `EnabledAutoD` • `EnabledEas` • `EnabledEcp` • `EnabledEws` • `EnabledMapi` • `EnabledOab` • `EnabledOwa` • `EnabledPowerShell` • `EnabledOthers`
BinaryFormatterDataValue	Сведения о конфигурации `Binary Formatter` : • `EnableSecureDeserializerLocation` • `EnableFirstFallbackDeserializerLocation` • `EnableSecondFallbackDeserializerLocation`
FlightingDataValue	Сведения о рейсах, настроенных с помощью `Feature Flighting`: • `FeaturesAwaitingAdminApproval` • `FeaturesBlocked` • `FeaturesEnabled` • `RingLevel`

Настройка параметра диагностических данных после завершения установки

После завершения установки можно включить или отключить отправку диагностических данных в OCS на любом сервере Exchange Server с помощью командлета **Set-ExchangeServer**.

Чтобы отключить отправку необязательных данных в корпорацию Майкрософт:

```
Powershell
```

```
Set-ExchangeServer -Identity <ServerName> -DataCollectionEnabled:$false
```

Чтобы включить отправку необязательных данных в корпорацию Майкрософт:

Powershell

```
Set-ExchangeServer -Identity <ServerName> -DataCollectionEnabled:$true
```

Защита от нежелательной почты и вредоносных программ в Exchange Server

Статья • 29.05.2024

Антиспам и защита от вредоносных программ включены в Exchange Server 2016 и Exchange Server 2019.

- Защита от нежелательной меры обеспечивается теми же встроенными агентами транспорта, что и в Exchange Server 2010. Эти агенты включены по умолчанию на пограничных транспортных серверах, и многие из них можно включить на серверах почтовых ящиков Exchange.
- Защиту от вредоносных программ обеспечивает соответствующий агент, который впервые появился в Exchange Server 2013. Агент вредоносных программ доступен и включен по умолчанию на серверах почтовых ящиков Exchange.

В приведенной ниже таблице представлены ссылки на статьи, содержащие общие сведения и указания по настройке параметров встроенных функций фильтрации нежелательной почты и вредоносных программ в организации.

Развернуть таблицу

Статья	Описание
Защита от нежелательной нежелательной записи в Exchange Server	Описывает встроенные функции защиты от нежелательной отспамов в Exchange Server и настройку параметров защиты от нежелательной отспамов.
Запуск антивирусного программного обеспечения Windows на серверах Exchange	Описывает рекомендации по запуску антивирусных программ Windows на серверах Exchange.

Сведения о функциях защиты от спама в Microsoft 365 см. в статье Защита от нежелательной почты в EOP.

Защита от нежелательной отспамов в Exchange Server

Статья • 04.04.2023

Спаммеры или вредоносные отправители используют различные методы для отправки нежелательной электронной почты в вашу организацию. Не существует единого средства или процесса, с помощью которого можно устранить весь спам. Тем не менее в Microsoft Exchange реализован многоуровневый и многогранный подход к сокращению количества таких сообщений. Exchange использует агенты транспорта для защиты от нежелательной информации, а встроенные агенты, доступные в Exchange Server 2016 и Exchange Server 2019 годах, относительно не изменились по сравнению с Exchange Server 2010 г. В Exchange 2016 и Exchange 2019 настройка этих агентов и управление ими доступны только в командной консоли Exchange.

Для получения дополнительных функций защиты от нежелательной почты и упрощения управления можно приобрести Exchange Online Protection (EOP), которая входит в состав Microsoft 365 и Office 365. Дополнительные сведения о microsoft 365 или Office 365 защиты от спама см. в статье Защита от нежелательной почты в EOP.

Агенты защиты от нежелательной почты на серверах почтовых ящиков

Как правило, агенты защиты от нежелательной почты включаются на серверах почтовых ящиков, если в организации нет пограничного транспортного сервера или не выполняется дополнительная фильтрация входящих сообщений. Дополнительные сведения см. в разделе Включение функций защиты от нежелательной почты на серверах почтовых ящиков.

Как и всем агентам транспорта, каждому агенту защиты от нежелательной почты назначается значение приоритета. Чем ниже значение, тем выше приоритет, поэтому агент с приоритетом 1 обычно применяется к сообщению раньше агента с приоритетом 9. Тем не менее событие SMTP транспортного конвейера, в котором зарегистрирован агент, также очень важно для определения порядка, в котором агент защиты от нежелательной почты обрабатывает сообщения. Агент с низким приоритетом, зарегистрированный на более раннем этапе транспортного конвейера, выполняется перед агентом с высоким приоритетом, который был зарегистрирован в транспортном конвейере позже.

С учетом значения приоритета агента по умолчанию и события SMTP, в котором он зарегистрирован, агенты защиты от нежелательной почты применяются к сообщениям на серверах почтовых ящиков в следующем порядке:

1. **Агент фильтрации отправителей**. Фильтрация отправителей сравнивает отправляющий сервер со списком отправителей или доменов отправителей, которым запрещено отправлять сообщения в организацию. Дополнительные сведения см. в разделе Фильтрация отправителей.

2. **Агент идентификатора отправителя**. Идентификатор отправителя зависит от IP-адреса отправляющего сервера и предполагаемого ответственного адреса (PRA) отправителя, чтобы определить, является ли адрес электронной почты отправки поддельным. Дополнительные сведения см. в разделе Sender ID.

3. **Агент фильтра содержимого**. Агент фильтрации содержимого назначает каждому сообщению уровень достоверности нежелательной почты (SCL) на основе данных из допустимых и нежелательных сообщений. Дополнительные сведения см. в разделе Фильтрация содержимого.

   Карантин спама — это компонент агента фильтра содержимого, снижающий риск потери подлинных сообщений, ошибочно определенных как спам. Он представляет собой временное место хранения для подозрительных сообщений, где их может проверить администратор. Дополнительные сведения см. в разделе Карантин спама в Exchange Server.

   При фильтрации содержимого также используется функция объединения списков надежных отправителей. Объединение списков надежных отправителей собирает данные списков надежных отправителей, которые пользователи настраивают в Microsoft, Outlook и Outlook в Интернете, и делает эту сведений доступных для агента фильтра содержимого. Дополнительные сведения см. в разделе Объединение списков надежных отправителей.

4. **Агент анализа протоколов (репутация отправителя):** агент анализа протоколов — это агент, обеспечивающий репутацию отправителя. Он выполняет ряд проверок, чтобы вычислить уровень репутации отправителя (SRL) для входящих сообщений, по которому затем определяется действие, выполняемое с этими сообщениями. Дополнительные сведения см. в разделе Sender reputation and the Protocol Analysis agent.

Агенты защиты от нежелательной почты на пограничных транспортных серверах

Если в сети периметра организации установлен пограничный транспортный сервер, на нем устанавливаются и по умолчанию включаются все агенты защиты от нежелательной почты, доступные серверу почтовых ящиков. Однако следующие агенты доступны только на пограничных транспортных серверах:

- **Агент фильтрации подключений**. Фильтрация подключений использует список заблокированных IP-адресов, список разрешенных IP-адресов, поставщики списков блокировок IP-адресов и поставщики списка разрешенных IP-адресов для определения того, должно ли быть заблокировано или разрешено подключение. Дополнительные сведения см. в разделе Фильтрация подключений на пограничных транспортных серверах.

- **Агент фильтра получателей**. Фильтрация получателей использует список блокировок получателей для идентификации сообщений, которым запрещено входить в организацию. Фильтр получателей также использует локальный каталог получателей для отклонения сообщений, отправленных недопустимым получателям. Дополнительные сведения см. в статье Фильтрация получателей на пограничных транспортных серверах.

  > ⓘ **Примечание**
  >
  > Хотя агент фильтра получателей доступен на серверах почтовых ящиков, его не следует настраивать. Если при фильтрации получателей на сервере почтовых ящиков в сообщении обнаруживается по крайней мере один недопустимый или заблокированный получатель, сообщение отклоняется. Агент фильтра получателей активируется, когда вы устанавливаете агенты защиты от спама на сервере почтовых ящиков, но не блокирует получателей.

- **Агент фильтрации вложений**. Фильтрация вложений блокирует сообщения или вложения на основе имени файла вложения, расширения или типа контента MIME. Дополнительные сведения см. в разделе Фильтрация вложений на пограничных транспортных серверах.

С учетом заданного по умолчанию значения приоритета агента и события SMTP транспортного конвейера, в котором зарегистрирован этот агент, агенты защиты от нежелательной почты применяются к сообщениям на пограничном транспортном сервере в следующем порядке:

1. Агент фильтрации подключений

2. Агент фильтра отправителей

3. Агент фильтра получателей
4. Агент идентификации отправителей
5. Агент фильтра содержимого
6. Агент анализа протокола (репутация отправителя)
7. Агент фильтрации вложений

Метки нежелательной почты

Метки нежелательной почты применяются к сообщениям и используются агентами защиты от нежелательной почты. Вы можете просматривать метки нежелательной почты, чтобы выявлять проблемы, связанные со спамом. Дополнительные сведения см. в разделе Метки защиты от нежелательной почты.

Стратегия защиты от нежелательной почты

Защита от нежелательной почты — это баланс между блокированием нежелательных сообщений и разрешением подлинных. Если настроить слишком много функций строгой защиты от нежелательной почты, высока вероятность блокировки множества подлинных сообщений (ложных срабатываний). Если же сделать защиту слишком свободной, в организацию будет проникать много спама.

Ниже приводятся некоторые рекомендации, которые следует учитывать при настройке встроенных функций защиты от нежелательной почты в Exchange.

- Отклоняйте сообщения, определяемые агентом фильтрации подключений, агентом фильтра получателей и агентом фильтра отправителей, а не карантином сообщений или применением меток защиты от спама. Этот подход рекомендуется по следующим причинам:
    - Как правило, сообщения, обнаруженные при использовании параметров по умолчанию для фильтрации подключений, получателей и отправителей, можно считать нежелательными без дальнейших проверок. Например, если для фильтрации отправителей настроена блокировка определенных отправителей, нет необходимости продолжать обработку сообщений от этих отправителей. (Если вы не хотите, чтобы сообщения отклонялись, вы бы не поместили их в список заблокированных отправителей).
    - Настройка более агрессивного уровня для агентов защиты от спама, которые сталкиваются с сообщениями на ранних этапах транспортного

конвейера, позволяет сэкономить ресурсы обработки, пропускной способности и дисков. Чем дальше сообщение проходит по транспортному конвейеру, тем больше переменных приходится учитывать оставшимся компонентам защиты от нежелательной почты, чтобы успешно определить сообщение как спам. Отклоняйте очевидный спам как можно раньше, чтобы оставить время для подозрительных сообщений.

- Необходимо отслеживать эффективность функций защиты от нежелательной почты на их текущих уровнях конфигурации. Мониторинг позволяет реагировать на тенденции, а также повышать и понижать интенсивность защиты. Для начала следует использовать параметры по умолчанию, чтобы свести к минимуму число ложных срабатываний. По мере отслеживания количества спама и ложных срабатываний вы можете повышать интенсивность защиты в зависимости от типов спама и атак, наблюдаемых в организации.

См. также

Защита от нежелательной почты в EOP

Включение функции защиты от спама на серверах почтовых ящиков

Статья • 04.04.2023

Следующие агенты защиты от нежелательной почты доступны в транспортной службе на серверах почтовых ящиков Exchange 2016 и Exchange 2019, но они не устанавливаются по умолчанию:

- Агент фильтрации содержимого
- Агент фильтра отправителей
- Агент идентификации отправителей
- Агент анализа протокола для репутации отправителя

Вы можете установить эти агенты защиты от спама на сервере почтовых ящиков с помощью сценария командной консоли Exchange, что важно, если эти агенты — ваша единственная защита от спама. Как правило, вам не нужно устанавливать агенты защиты от спама на сервере почтовых ящиков, если в вашей организации используются другие фильтры спама для входящей почты.

> ⓘ **Примечание**
>
> Хотя агент фильтра получателей доступен на серверах почтовых ящиков, его не следует настраивать. Если при фильтрации получателей на сервере почтовых ящиков в сообщении обнаруживается по крайней мере один недопустимый или заблокированный получатель, сообщение отклоняется. Агент фильтра получателей активируется, когда вы устанавливаете агенты защиты от спама на сервере почтовых ящиков, но не блокирует получателей.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 15 минут
- Для выполнения этой процедуры можно использовать только PowerShell. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

- Агент фильтра подключений и агент фильтра вложений недоступны на серверах почтовых ящиков. Они доступны только на пограничных транспортных серверах, где они установлены и включены по умолчанию. Однако агент защиты от вредоносных программ устанавливается и включается по умолчанию на сервере почтовых ящиков. Дополнительные сведения см. в разделе Защита от вредоносных программ в Exchange Server.

- Если вы используете другие агенты защиты от спама Exchange для обработки сообщений перед их попаданием на сервер почтовых ящиков (например, пограничный транспортный сервер в сети периметра), агенты защиты от спама на сервере почтовых ящиков распознают X-заголовки защиты от спама в сообщениях, и такие сообщения не подвергаются повторной проверке.

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Конфигурация транспорта" в разделе Разрешения потока обработки почты .

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Шаг 1. Запустите сценарий PowerShell Install-AntispamAgents.ps1

Выполните следующую команду в командной консоли Exchange на сервере почтовых ящиков:

PowerShell

```
& $env:ExchangeInstallPath\Scripts\Install-AntiSpamAgents.ps1
```

Как убедиться, что все получилось?

Все сработало, если сценарий выполнен без ошибок и требуется перезапустить службу транспорта Microsoft Exchange. Результат выглядит следующим образом:

Выходные данные

```
WARNING: Please exit Windows PowerShell to complete the installation.
WARNING: The following service restart is required for the change(s) to take
effect : MSExchangeTransport
WARNING: The following service restart is required for the change(s) to take
effect : MSExchangeTransport
Identity                                          Enabled         Priority
--------                                          -------         --------
Content Filter Agent                              True            8
WARNING: Please exit Windows PowerShell to complete the installation.
WARNING: The following service restart is required for the change(s) to take
effect : MSExchangeTransport
WARNING: The following service restart is required for the change(s) to take
effect : MSExchangeTransport
Sender Id Agent                                   True            9
WARNING: Please exit Windows PowerShell to complete the installation.
WARNING: The following service restart is required for the change(s) to take
effect : MSExchangeTransport
WARNING: The following service restart is required for the change(s) to take
effect : MSExchangeTransport
Sender Filter Agent                               True            10
WARNING: Please exit Windows PowerShell to complete the installation.
WARNING: The following service restart is required for the change(s) to take
effect : MSExchangeTransport
WARNING: The following service restart is required for the change(s) to take
effect : MSExchangeTransport
Recipient Filter Agent                            True            11
WARNING: Please exit Windows PowerShell to complete the installation.
WARNING: The following service restart is required for the change(s) to take
effect : MSExchangeTransport
WARNING: The following service restart is required for the change(s) to take
effect : MSExchangeTransport
Protocol Analysis Agent                           True            12
WARNING: The agents listed above have been installed. Please restart the
Microsoft Exchange Transport service for
changes to take effect.
```

Шаг 2. Перезапустите службу транспорта Microsoft Exchange

Выполните следующую команду в командной консоли Exchange на сервере почтовых ящиков:

PowerShell

```
Restart-Service MSExchangeTransport
```

Как убедиться, что все получилось?

Это сработало, если перезапуск службы транспорта Microsoft Exchange прошел без ошибок. Результат выглядит следующим образом:

Выходные данные

```
WARNING: Waiting for service 'Microsoft Exchange Transport
(MSExchangeTransport)' to start...
WARNING: Waiting for service 'Microsoft Exchange Transport
(MSExchangeTransport)' to start...
WARNING: Waiting for service 'Microsoft Exchange Transport
(MSExchangeTransport)' to start...
WARNING: Waiting for service 'Microsoft Exchange Transport
(MSExchangeTransport)' to start...
WARNING: Waiting for service 'Microsoft Exchange Transport
(MSExchangeTransport)' to start...
WARNING: Waiting for service 'Microsoft Exchange Transport
(MSExchangeTransport)' to start...
```

Шаг 3. Укажите внутренние SMTP-серверы вашей организации

Необходимо указать IP-адреса всех внутренних SMTP-серверов, которые должен игнорировать агент Sender ID. Достаточно указать IP-адрес по крайней мере одного внутреннего SMTP-сервера. Если сервер почтовых ящиков, на котором работают агенты защиты от спама, является единственным SMTP-сервером в организации, введите IP-адрес этого компьютера.

Чтобы добавить IP-адреса внутренних SMTP-серверов, не изменяя существующие значения, выполните следующую команду в командной консоли Exchange на сервере почтовых ящиков:

PowerShell

```
Set-TransportConfig -InternalSMTPServers @{Add="<ip address1>","<ip
address2>"...}
```

В этом примере показано, как добавить адреса внутренних SMTP-серверов 10.0.1.10 и 10.0.1.11 в конфигурацию транспорта организации.

PowerShell

```
Set-TransportConfig -InternalSMTPServers @{Add="10.0.1.10","10.0.1.11"}
```

Как убедиться, что все получилось?

Чтобы убедиться, что вы успешно указали IP-адрес по крайней мере одного внутреннего SMTP-сервера, выполните следующую команду в командной консоли Exchange на сервере почтовых ящиков и убедитесь, что IP-адрес отображается.

PowerShell

```
Get-TransportConfig | Format-List InternalSMTPServers
```

Шаг 4. Дальнейшие действия

- Теперь на сервере почтовых ящиков должны быть установлены и запущены агент фильтра содержимого, агент Sender ID, агент фильтра отправителей и агент анализа протокола (репутации отправителей). Чтобы убедиться в этом, выполните следующую команду в командной консоли Exchange на сервере почтовых ящиков:

  PowerShell

  ```
  Get-TransportAgent
  ```

  PowerShell

  ```
  Get-ContentFilterConfig | Format-Table Name,Enabled; Get-
  SenderFilterConfig | Format-Table Name,Enabled; Get-SenderIDConfig |
  Format-Table Name,Enabled; Get-SenderReputationConfig | Format-Table
  Name,Enabled
  ```

- Чтобы просмотреть подробные сведения о конфигурации каждого агента, выполните следующие команды:

  PowerShell

  ```
  Get-ContentFilterConfig | Format-List
  *Enabled,RejectionResponse,*Postmark*,Bypassed*,Quarantine*;
  ```

  PowerShell

  ```
  Get-SenderFilterConfig | Format-List *Enabled,*Block*
  ```

  PowerShell

```
Get-SenderIDConfig | Format-List *Enabled*,*Action,Bypassed*
```

PowerShell

```
Get-SenderReputationConfig | Format-List
*Enabled*,*Proxy*,*Block*,*Ports*
```

- Сведения о настройке каждого агента см. в следующих статьях:
  - Процедуры фильтрации содержимого
  - Процедуры объединения списков надежных отправителей
  - Configure Content Filtering to Use Safe Domain Data
  - Пороговые значения уровня достоверности нежелательной почты Exchange (SCL)
  - Процедуры фильтрации отправителей
  - Процедуры кода отправителя
  - Процедуры репутации отправителя
- По умолчанию агент фильтра содержимого, агент фильтра отправителей и агент Sender ID записывают свои действия в журнале агентов защиты от спама на сервере почтовых ящиков. Если сведения записываются в журнал, эти агенты защиты от спама работают. Чтобы просмотреть расположение и конфигурацию журнала, выполните следующую команду в командной консоли Exchange на сервере почтовых ящиков:

PowerShell

```
Get-TransportService | Format-List AgentLog*
```

Инструкции по настройке журнала см. в статье Configure antispam Agent Logging.

Метки нежелательной почты

Статья • 04.04.2023

Метки защиты от спама в Exchange Server применяют диагностические метаданные или метки, такие как сведения об отправителе, результаты проверки головоломки и результаты фильтрации содержимого, к сообщениям при передаче через функции защиты от спама, которые фильтруют входящие сообщения из Интернета. С помощью таких меток можно просмотреть результаты фильтрации сообщения для защиты от нежелательной почты, а также диагностировать неполадок, связанных со спамом. Функции защиты от нежелательной почты и метки, по сути, ничем не отличаются от тех, которые используются в Exchange Server 2010. Существует четыре основных метки защиты от нежелательной почты Exchange:

- метка уровня вероятности фишинга (PCL);
- метка кода отправителя;
- метка уровня вероятности нежелательной почты (SCL);
- метка отчета о защите от нежелательной почты.

Метки для защиты от нежелательной почты добавляются в сообщения в виде полей X-заголовка в заголовке сообщения. Вы можете просматривать метки защиты от нежелательной почты в сообщении с помощью Outlook. Дополнительные сведения см. в статье View antispam stamps in Outlook.

Метка уровня вероятности фишинга

Метка PCL указывает на вероятность того, что сообщение является фишинговым (на основе его содержимого). Метка PCL применяется при обработке сообщения агентом фильтрации содержимого. Дополнительные сведения о фильтрации содержимого см. в разделе Фильтрация содержимого.

Значения PCL описаны в таблице ниже.

Значение PCL	Verdict	Описание
1-3	`Neutral`	Маловероятно, что содержимое этого сообщения связано с фишингом.
4-8	`Suspicious`	Вероятно, что содержимое этого сообщения связано с фишингом.

Значение PCL отображается в заголовке **X-MS-Exchange-Organization-PCL:** X-, а вердикт PCL отображается в метке отчета о антиспаме как `PCL:PhishingLevel <Verdict>`. В Outlook метка PCL используется для блокирования содержимого подозрительных сообщений.

Метка кода отправителя

Метка кода отправителя присваивается инфраструктурой политики отправителей (SPF), которая определяет использование доменов в сообщениях электронной почты. Агент код отправителя определяет статус кода отправителя для сообщения. Значения этого статуса описаны в таблице ниже.

Состояние	Описание
`Pass`	IP-адрес и предполагаемый адрес (PRA) прошли проверку идентификации отправителей.
`Neutral`	Опубликованные данные кода отправителя являются явно неокончательными.
`SoftFail`	IP-адрес для PRA может находиться в неразрешенном наборе.
`Fail`	IP-адрес запрещен. Во входящей почте не найдена функция PRA или домен отправки не существует.
`None`	В DNS отправителя отсутствуют опубликованные данные SPF.
`TempError`	Временный сбой DNS, например, недоступный сервер DNS.
`PermError`	Недействительная запись DNS, например ошибка в формате записи.

Метка идентификатора отправителя отображается в заголовке **X-MS-Exchange-Organization-SenderIdResult:** X-header, а также в метке отчета antispam как `SenderIDStatus <Status>`. Результат SPF отображается в заголовке **Received-SPF**.

Дополнительные сведения приведены в следующих разделах:

- Код отправителя
- Инфраструктура политики отправителей: синтаксис записи SPF

Метка уровня вероятности нежелательной почты

> ⓘ **Примечание**

В ноябре 2016 г. корпорация Майкрософт прекратила выпуск обновлений определений спама для фильтров SmartScreen в Exchange и Outlook. Существующие определения спама SmartScreen остались на месте, но их эффективность, скорее всего, со временем снизится. Дополнительные сведения см. в статье **Прекращение поддержки SmartScreen в Outlook и Exchange**.

Метка PCL показывает оценку сообщения на основании его содержимого. Для оценки содержимого сообщения и назначения каждому сообщению рейтинга уровня вероятности нежелательной почты агент фильтра содержимого использует технологию Майкрософт SmartScreen. Значения SCL описаны в таблице ниже.

Значение SCL	**Описание**
0–9	0 означает очень низкий уровень вероятности того, что сообщение является спамом. 9 означает очень высокий уровень вероятности того, что сообщение является спамом.
-1	Сообщение пропущено во время сканирования для защиты от нежелательной почты (например, сообщение было от внутреннего отправителя).

Значение SCL отображается в X-заголовке **X-MS-Exchange-Organization-SCL:**.

Действия, выполняемые Exchange и Outlook на основе значения SCL, зависят от параметров порогового значения SCL. Дополнительные сведения см. в статье Пороговые значения уровня достоверности нежелательной почты Exchange (SCL).

Метка отчета о защите от нежелательной почты

Метка отчета о защите от нежелательной почты представляет собой итоговый отчет по результатам применения фильтра нежелательной почты к сообщению. Агент фильтрации содержимого применяет эту метку к сообщению в X-заголовке **X-MS-Exchange-Organization-Antispam-Report:**. В отчете о защите от нежелательной почты используется следующий синтаксис:

```
X-MS-Exchange-Organization-Antispam-Report: DV:
<DATVersion>;CW:CustomList;PCL:PhishingVerdict
```

```
<verdict>;P100:PhishingBlock;PP:Presolve;SID:SenderIDStatus <status>;TIME:
<SendReceiveDelta>;MIME:MimeCompliance;OrigIP:<SourceIPAddress>
```

В таблице ниже представлена информация фильтра нежелательной почты, которая может отображаться в метке отчета о защите от нежелательной почте. Обратите внимание, что в метке отчета о защите от нежелательной почты представлены только результаты и выводы фильтров нежелательной почты, примененных к нему. Поэтому в этой метке обычно отсутствуют все возможные метки и значения.

Метка	**Описание**
DV	Марка версии DAT (DV) показывает версию файла описания нежелательной почты, использованного при проверке сообщения.
SA	Марка действий по отношению к подписи (SA) показывает, что сообщение было либо восстановлено, либо удалено на основании подписи, присутствующей в сообщении.
SV	Марка версии подписи DAT (SV) показывает версию файла подписи, использованного при проверке сообщения.
CW	Метка пользовательского веса (CW) показывает, что сообщение содержит неразрешенное слово или фразу, а также что значение SCL, или "вес", этого неразрешенного слова или фразы использовано при вычислении итоговой оценки SCL. • Неразрешенные, или блокированные, фразы имеют максимальный вес и меняют оценку SCL на 9. • Утвержденные, или разрешенные, слова и фразы имеют минимальный вес и меняют значение SCL на 0. Дополнительные сведения о добавлении утвержденных и неутвержденных слов или фраз в агент фильтрации содержимого см. в разделе Процедуры фильтрации содержимого.

Метка	Описание
PP	Метка предварительно решенной задачи (PP) показывает, что если сообщение отправителя содержит правильную, разрешенную компьютерную почтовую марку (основанную на функциях проверки почтовых марок Outlook), отправитель вряд ли является злоумышленником. В этом случае агент фильтра содержимого снижает оценку SCL. Агент фильтрации содержимого не изменяет уровень SCL, если включена функция проверки почтовых марок и при этом выполняются следующие условия. • Входящее сообщение не содержит компьютерной почтовой марки. • Компьютерная почтовая марка недействительна. Дополнительные сведения о функции проверки почтовых марок см. в статье Фильтрация содержимого.
TIME:TimeBasedFeatures	Показывает, что с момента отправки сообщения и до момента его доставки прошло значительное количество времени. Метка TIME используется для определения конечной оценки SCL для сообщения.
OrigIP	Указывает IP-адрес исходного сервера обмена сообщениями.
MIME:MIMECompliance	Показывает, что сообщение электронной почты не соответствует стандарту MIME.
P100:PhishingBlock	Показывает, что сообщение содержит URL-адрес, указанный в файле определения фишинга.
IPOnAllowList	Показывает, что IP-адрес отправителя не включен в список разрешенных IP-адресов. Дополнительные сведения о списке разрешенных IP-адресов см. в разделе Список разрешенных IP-адресов.
MessageSecurityAntispamBypass	Показывает, что содержимое сообщения не проходило через фильтры и что отправитель получил разрешение не проходить фильтры нежелательной почты.
SenderBypassed	Показывает, что агент фильтрации содержимого не выполняет фильтрацию содержимого сообщений, получаемых от этого отправителя. Дополнительные сведения см. в разделе Процедуры фильтрации содержимого.

Метка	Описание
AllRecipientsBypassed	Показывает, что одно из следующих условий выполняется для всех получателей, указанных в сообщении: • Параметр *AntispamBypassedEnabled* в почтовом ящике получателя имеет значение `$true`. Дополнительные сведения см. в статье Использование командной консоли Exchange для настройки почтового ящика на обход фильтрации для защиты от нежелательной почты. • Отправитель сообщения включен в список надежных отправителей у получателя. Дополнительные сведения о списке надежных отправителей см. в разделе Использование командной консоли Exchange для настройки коллекции списков надежных отправителей почтового ящика. • Агент фильтрации содержимого не выполняет фильтрацию содержимого сообщений, отправляемых этому получателю. Дополнительные сведения об исключениях для получателей см. в статье Использование командной консоли Exchange для настройки исключений для получателей и отправителей для функции фильтрации содержимого.

Просмотр меток нежелательной почты в Outlook

Статья • 04.04.2023

Встроенные агенты защиты от спама в Exchange Server применять диагностические метаданные или метки в качестве X-заголовков к сообщениям по мере их поступления в организацию. Дополнительные сведения об этих метках см. в статье Antispam stamps. Вы можете использовать Microsoft Outlook для просмотра полей X-заголовков антиспамов в сообщениях, которые помогут вам диагностировать проблемы, связанные со спамом.

Что нужно знать перед началом работы

- Предполагаемое время выполнения процедуры: менее 5 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Доступ к почтовому ящику" в разделе Разрешения потока обработки почты .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование Outlook 2010 или более поздней версии для просмотра меток защиты от нежелательной почты

1. Откройте Outlook на клиентском компьютере и в представлении **Почта** дважды щелкните сообщение, чтобы открыть его.
2. В разделе **Теги** на ленте щелкните значок **Параметры сообщений**, чтобы отобразить диалоговое окно **Свойства** для сообщений.

3. В диалоговом окне **Свойства** в разделе **Заголовки Интернета** воспользуйтесь полосой прокрутки, чтобы просмотреть X-заголовки для защиты от нежелательной почты. Необходимые поля заголовка:

    - **X-MS-Exchange-Organization-SenderIdResult:**
    - **X-MS-Exchange-Organization-SCL:**
    - **X-MS-Exchange-Organization-PCL:**
    - **X-MS-Exchange-Organization-Antispam-Report:**

Чтобы упростить поиск нужных значений, выберите весь текст в поле **Заголовки Интернета** (нажмите клавиши CTRL + A), скопируйте текст (нажмите клавиши CTRL + C или щелкните текст правой кнопкой мыши и выберите команду **Копировать**), а затем вставьте его в Блокнот.

Вот пример значений, которые можно найти в подозрительных сообщениях:

```
X-MS-Exchange-Organization-SenderIdResult:Fail
X-MS-Exchange-Organization-SCL:6
X-MS-Exchange-Organization-PCL:7X-MS-Exchange-Organization-Antispam-Report:
DV:3.3.15608.880;SID:SenderIDStatus Fail;PCL:PhishingLevel
SUSPICIOUS;CW:CustomList;PP:Presolved;TIME:TimeBasedFeatures;OrigIP:10.1.1.1
```

Настройка параметров Exchange для защиты от нежелательной почты в почтовых ящиках

Статья • 04.04.2023

В Exchange Server можно настроить определенные параметры защиты от нежелательной почты для отдельных почтовых ящиков, которые отличаются от параметров защиты от нежелательной почты, применяемых к остальным почтовым ящикам в вашей организации. Доступные возможности защиты почтовых ящиков от спама практически такие же, как и в Exchange 2010.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Функции защиты от нежелательной почты" в разделе Разрешения для защиты от вредоносных программ и "Антиспам" в разделе Разрешения получателей .
- По умолчанию в службе транспорта на сервере почтовых ящиков не включены функции защиты от нежелательной почты. Как правило, их следует включать, только если организация Exchange не выполняет никакую предварительную фильтрацию нежелательной почты до приема входящих сообщений. Дополнительные сведения см. в разделе Включение функций защиты от нежелательной почты на серверах почтовых ящиков.
- Для выполнения этой процедуры можно использовать только PowerShell. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование Командная консоль Exchange для включения или отключения правила нежелательной почты в почтовом ящике

По умолчанию в каждом почтовом ящике включено правило нежелательной почты (скрытое правило папки "Входящие", которое называется "Правило нежелательной почты"). Это правило определяет указанные ниже функции Exchange для защиты от нежелательной почты:

- **Доставка сообщений в папку Нежелательной Email на основе порогового значения папки нежелательной Email SCL**. Если exchange присваивает сообщению значение уровня достоверности нежелательной почты (SCL), а значение SCL больше порогового значения нежелательной Email папки SCL, настроенного для организации Exchange (значение по умолчанию — 4) или непосредственно в почтовом ящике (значение по умолчанию не настроено). Правило фильтра нежелательной почты перемещает сообщение в папку Нежелательная Email.

- **Доставка сообщений в папку Нежелательная Email на основе коллекции списков безопасности в почтовом ящике**. Записи в списке Надежные отправители, Список надежных получателей и Список заблокированных отправителей, настроенные в почтовом ящике, определяют, доставляет ли правило нежелательной почты сообщение в папку "Входящие" или "Нежелательная Email". Пользователи могут настроить коллекцию списков безопасности для собственного почтового ящика в Microsoft Outlook или Outlook в Интернете. Администраторы же для настройки таких коллекций могут воспользоваться командлетом **Set-MailboxJunkEmailConfiguration**.

Когда в почтовом ящике включено правило нежелательной почты, Exchange может доставлять сообщения в папку нежелательной почты (на основе списка заблокированных отправителей или порогового значения вероятности нежелательной почты) и предотвращать доставку сообщений в эту папку (на основе списка надежных отправителей). В Outlook в Интернете этому значению соответствует параметр **Автоматически фильтровать нежелательную почту**.

Если же в почтовом ящике отключено правило нежелательной почты, Exchange не будет отправлять сообщения в папку нежелательной почты на основе порогового значения вероятности нежелательной почты и списка заблокированных отправителей, настроенных для почтового ящика. В Outlook в Интернете этому значению соответствует параметр **Не перемещать сообщения в папку "Нежелательная почта"**.

Чтобы включить или отключить правило нежелательной почты для почтового ящика, используйте следующий синтаксис:

PowerShell

```
Set-MailboxJunkEmailConfiguration <MailboxIdentity> -Enabled <$true |
$false>
```

Пример отключения правила нежелательной почты для почтового ящика пользователя Ori Epstein.

PowerShell

```
Set-MailboxJunkEmailConfiguration "Ori Epstein" -Enabled $false
```

Пример отключения правила нежелательной почты для всех почтовых ящиков пользователей отдела North America в домене consoto.com.

PowerShell

```
Get-Mailbox -RecipientTypeDetails UserMailbox -OrganizationalUnit
"contoso.com/North America" | Set-MailboxJunkEmailConfiguration -Enabled
$false
```

Пример отключения правила нежелательной почты для всех почтовых ящиков пользователей, которые есть в базе данных почтовых ящиков MDB 01.

PowerShell

```
Get-Mailbox -RecipientTypeDetails UserMailbox -Database "MDB 01" | Set-
MailboxJunkEmailConfiguration -Enabled $false
```

Пример отключения правила нежелательной почты для всех почтовых ящиков пользователей организации.

PowerShell

```
$All = Get-Mailbox -RecipientTypeDetails UserMailbox -ResultSize Unlimited;
$All | foreach {Set-MailboxJunkEmailConfiguration $_.Name -Enabled $false}
```

Дополнительные сведения см. в статье Set-MailboxJunkEmailConfiguration.

Примечания.

- С помощью **командлета Set-MailboxJunkEmailConfiguration** можно отключить правило нежелательной почты в почтовом ящике, открытом в Outlook (в режиме кэширования Exchange) или Outlook в Интернете. Если почтовый ящик не был открыт, вы получите сообщение об ошибке: `The Junk Email configuration couldn't be set. The user needs to sign in to Outlook Web App before they can modify their Safe Senders and Recipients or Blocked Senders lists.` Если вы хотите подавить эту ошибку для массовых операций, можно добавить `-ErrorAction SlientlyContinue` в команду **Set-MailboxJunkEmailConfiguration** .

- Отключение правила нежелательной почты для почтового ящика приведет к тому, что правило не будет перемещать соответствующие сообщения в папку нежелательной почты. Однако фильтр нежелательной Email Outlook также может определить, является ли сообщение спамом, и может использовать коллекцию безопасных списков для перемещения сообщений в папку "Входящие" или папку "Нежелательная Email". Дополнительные сведения см. в разделе Сведения о параметрах нежелательной почты в Outlook данной статьи.

Как проверить, что все получилось?

Чтобы убедиться в том, что правило нежелательной почты для почтового ящика успешно включено или отключено, воспользуйтесь любой из приведенных ниже процедур.

- Замените <*MailboxIdentity*> идентификатором почтового ящика и выполните следующую команду, чтобы проверить значение свойства **Enabled** :

```
PowerShell

Get-MailboxJunkEmailConfiguration <MailboxIdentity> | Format-List
Enabled
```

- Для массовых операций используйте тот же фильтр, который идентифицировал почтовые ящики, и **замените команду Set-MailboxJunkEmailConfiguration** на `Get-MailboxJunkEmailConfiguration | Format-Table -Auto Identity,Enabled`. Например:

```
PowerShell

Get-Mailbox -RecipientTypeDetails UserMailbox -OrganizationalUnit
"contoso.com/North America" | Get-MailboxJunkEmailConfiguration |
```

```
Format-Table -Auto Identity,Enabled
```

- Замените <*MailboxIdentity*> идентификатором почтового ящика и выполните следующую команду, чтобы проверить значение свойства **Enabled** правила нежелательной почты.

```
PowerShell

Get-InboxRule "Junk E-mail Rule" -Mailbox <MailboxIdentity> -
IncludeHidden
```

Использование Командная консоль Exchange для настройки коллекции списков надежных отправителей почтового ящика

В коллекцию списков надежных отправителей для почтового ящика входят списки надежных отправителей, надежных получателей и заблокированных отправителей. По умолчанию пользователи могут настроить коллекцию списков безопасности в своем почтовом ящике в Outlook или Outlook в Интернете. Администраторы же для настройки таких коллекций для почтовых ящиков пользователей могут воспользоваться командлетом **Set-MailboxJunkEmailConfiguration**. Соответствующие параметры описаны в таблице ниже.

Параметр в Set-MailboxJunkEmailConfiguration	**Параметр Outlook Web App**
BlockedSendersAndDomains	**Перемещать электронную почту от этих отправителей и доменов в папку "Нежелательная почта"**
КонтактыНадежный	**Доверять сообщениям электронной почты от моих контактов**
TrustedListsOnly	**Не доверять электронной почте, если отправитель не входит в список надежных отправителей и получателей**
TrustedSendersAndDomains *TrustedRecipientsAndDomains*	**Не перемещать электронную почту от этих отправителей и доменов в папку "Нежелательная почта"**

Для настройки коллекции списков надежных отправителей для почтового ящика следует использовать следующий синтаксис:

```
PowerShell
```

```
Set-MailboxJunkEmailConfiguration <MailboxIdentity> -
BlockedSendersAndDomains <EmailAddressesOrDomains | $null> -ContactsTrusted
<$true | $false> -TrustedListsOnly <$true | $false> -
TrustedSendersAndDomains  <EmailAddressesOrDomains | $null>
```

Чтобы ввести несколько значений и перезаписать все существующие записи для параметров *BlockedSendersAndDomains* и *TrustedSendersAndDomains* , используйте следующий синтаксис: `"<EmailAddressOrDomain1>","<EmailAddressOrDomain2>"...`. Чтобы добавить или удалить одно или несколько значений, не затрагивая другие существующие записи, используйте следующий синтаксис: `@{Add="<EmailAddressOrDomain1>","<EmailAddressOrDomain2>"... ; Remove="<EmailAddressOrDomain3>","<EmailAddressOrDomain4>...}`

В примере ниже выполняется настройка следующих параметров для коллекции списков надежных отправителей в почтовом ящике пользователя Ori Epstein:

- Добавляет значение shopping@fabrikam.com в список Заблокированные отправители.
- Удаляет значение chris@fourthcoffee.com из списка надежных отправителей и списка Надежные получатели.
- настройка контактов в папке контактов как надежных отправителей.

PowerShell

```
Set-MailboxJunkEmailConfiguration "Ori Epstein" -BlockedSendersAndDomains
@{Add="shopping@fabrikam.com"} -TrustedSendersAndDomains
@{Remove="chris@fourthcoffee.com"} -ContactsTrusted $true
```

Пример очистки списка заблокированных отправителей для всех почтовых ящиков пользователей отдела North America в домене consoto.com.

PowerShell

```
Get-Mailbox -RecipientTypeDetails UserMailbox -OrganizationalUnit
"contoso.com/North America" | Set-MailboxJunkEmailConfiguration -
BlockedSendersAndDomains $null
```

В этом примере добавляется michelle@tailspintoys.com в список Надежные отправители и Надежные получатели во всех почтовых ящиках пользователей в базе данных почтовых ящиков С именем MDB 01.

PowerShell

```
Get-Mailbox -RecipientTypeDetails UserMailbox -Database "MDB 01" | Set-
MailboxJunkEmailConfiguration -TrustedSendersAndDomains
@{Add="michelle@tailspintoys.com"}
```

Пример удаления домена contoso.com из списка заблокированных отправителей для всех почтовых ящиков пользователей организации.

PowerShell

```
$All = Get-Mailbox -RecipientTypeDetails UserMailbox -ResultSize Unlimited;
$All | foreach {Set-MailboxJunkEmailConfiguration $_.Name -
BlockedSendersAndDomains @{Remove="contoso.com"}}
```

Дополнительные сведения см. в статье Set-MailboxJunkEmailConfiguration.

Примечания.

- Командлет **Set-MailboxJunkEmailConfiguration** можно использовать только для настройки коллекции списков безопасности в почтовом ящике, открытом в Outlook (в режиме кэширования Exchange) или Outlook в Интернете. Если почтовый ящик не был открыт, вы получите сообщение об ошибке: `The Junk Email configuration couldn't be set. The user needs to sign in to Outlook Web App before they can modify their Safe Senders and Recipients or Blocked Senders lists.` Если вы хотите подавить эту ошибку для массовых операций, можно добавить `-ErrorAction SlientlyContinue` в команду **Set-MailboxJunkEmailConfiguration** .

- Отключение правила нежелательной почты для почтового ящика приведет к тому, что правило не будет перемещать соответствующие сообщения в папку нежелательной почты или из нее на основе коллекции списков надежных отправителей. Однако даже если правило нежелательной почты отключено, вы по-прежнему можете настроить коллекцию списков безопасности, а фильтр нежелательной Email Outlook может использовать коллекцию списков безопасности для перемещения сообщений в папку "Входящие" или "Нежелательная Email". Дополнительные сведения см. в разделе Сведения о параметрах нежелательной почты в Outlook данной статьи.

- Функция агрегирования списка безопасности агента фильтра содержимого может совместно использовать коллекцию списков безопасности почтовых ящиков со встроенными агентами защиты от нежелательной почты Exchange. Дополнительные сведения см. в разделе Объединение списков надежных отправителей.

- С помощью командлета **Set-MailboxJunkEmailConfiguration** невозможно внести изменения непосредственно в список надежных отправителей. Сначала нужно внести изменения в список надежных отправителей, и они синхронизируются со списком надежных получателей.

- Фильтр нежелательной Email Outlook имеет дополнительные параметры сбора списков безопасности (например, **автоматическое добавление пользователей, которые я отправляю по электронной почте, в список надежных отправителей** и отдельная конфигурация списка надежных отправителей и списка надежных получателей). Дополнительные сведения см. в статье Использование фильтров нежелательной Email для управления видимых сообщений.

Как проверить, все ли получилось?

Чтобы убедиться в том, что коллекция списков надежных отправителей для почтового ящика успешно настроена, воспользуйтесь любой из приведенных ниже процедур.

- Замените <*MailboxIdentity*> идентификатором почтового ящика и выполните следующую команду, чтобы проверить значения свойств:

  PowerShell

  ```
  Get-MailboxJunkEmailConfiguration <MailboxIdentity> | Format-List
  trusted*,contacts*,blocked*
  ```

  Если список адресов электронной почты слишком длинный, используйте следующий синтаксис:

  PowerShell

  ```
  (Get-MailboxJunkEmailConfiguration
  <MailboxIdentity>).BlockedSendersAndDomains
  ```

- Для массовых операций укажите фильтр, используемый для настройки коллекции списков безопасности, и **замените команду Set-MailboxJunkEmailConfiguration** на `Get-MailboxJunkEmailConfiguration | Format-List Identity,trusted*,contacts*,blocked*`. Например:

  PowerShell

```
Get-Mailbox -RecipientTypeDetails UserMailbox -OrganizationalUnit
"contoso.com/North America" | Get-MailboxJunkEmailConfiguration |
Format-List Identity,trusted*,contacts*,blocked*
```

Использование Командная консоль Exchange для управления возможностью настройки параметров нежелательной почты в Outlook в Интернете

Администраторы могут разрешить или запретить пользователям включать или отключать правило нежелательной почты, а ограничить для них возможность настройки коллекции списков надежных отправителей для их собственных почтовых ящиков в Outlook в Интернете. Такая настройка не приводит к включению или отключению правила нежелательной почты для почтового ящика; это лишь способ управления возможностью настройки соответствующих параметров почтового ящика в Outlook в Интернете.

Чтобы использовать политики почтовых ящиков Outlook в Интернете для управления возможностью пользователей настраивать параметры нежелательной почты для их собственных почтовых ящиков, воспользуйтесь следующим синтаксисом:

PowerShell

```
Set-OwaMailboxPolicy <OWAMailboxPolicyIdentity> -JunkEmailEnabled <$true |
$false>
```

Пример запрета возможности настраивать параметры нежелательной почты в Outlook в Интернете для всех почтовых ящиков, которые указаны в политике почтовых ящиков Outlook в Интернете, которая называется "Default".

PowerShell

```
Set-OwaMailboxPolicy Default -JunkEmailEnabled $false
```

Дополнительные сведения см. в статье Set-OwaMailboxPolicy.

Чтобы использовать виртуальные каталоги Outlook в Интернете для управления возможностью пользователей настраивать параметры нежелательной почты для их

собственных почтовых ящиков в Outlook в Интернете, воспользуйтесь следующим синтаксисом:

```
PowerShell

Set-OwaVirtualDirectory <OWAVirtualDirectoryIdentity> -JunkEmailEnabled
<$true | $false>
```

Пример запрета возможности настраивать параметры нежелательной почты для всех пользователей, подключающихся к виртуальному каталогу Outlook в Интернете, который называется "owa (Default Web Site)", на сервере Mailbox01.

```
PowerShell

Set-OwaVirtualDirectory "Mailbox01\owa (Default Web Site)" -JunkEmailEnabled
$false
```

Примечание. Чтобы применить изменения к виртуальным каталогам Outlook в Интернете, необходимо перезапустить службы IIS, выполнив команды `Stop-Service WAS -Force` и `Start-Service W3SVC`.

Дополнительные сведения см. в статье Set-OwaVirtualDirectory.

Как проверить, все ли получилось?

Чтобы убедиться в том, что возможность настройки параметров нежелательной почты в Outlook в Интернете успешно настроена, воспользуйтесь любой из приведенных ниже процедур.

- В случае с политиками почтовых ящиков Outlook в Интернете выполните следующую команду, чтобы проверить значение свойства **JunkEmailEnabled**:

  ```
  PowerShell

  Get-OwaMailboxPolicy | Format-Table -Auto Name,JunkEmailEnabled
  ```

- В случае с виртуальными каталогами Outlook в Интернете выполните следующую команду, чтобы проверить значение свойства **JunkEmailEnabled**:

  ```
  PowerShell

  Get-OwaVirtualDirectory | Format-Table -Auto Name,JunkEmailEnabled
  ```

Использование Командная консоль Exchange для настройки пороговых значений вероятности нежелательной почты для почтового ящика

Пороговые значения вероятности нежелательной почты — это функция агента фильтрации содержимого, с помощью которой можно эскалировать действия, выполняемые с сообщениями на основе присвоенного им значения вероятности нежелательной почты. Дополнительные сведения см. в статье Пороговые значения уровня достоверности нежелательной почты Exchange (SCL).

Если для почтового ящика настроено пороговое значение вероятности нежелательной почты (отличное от нуля), то этот параметр переопределяет соответствующее пороговое значение для агента фильтрации содержимого или организации Exchange. В таблице ниже приведены пороговые значения вероятности нежелательной почты, доступные для почтового ящика.

Пороговое значение SCL**	**Оператор сравнения значения вероятности нежелательной почты**	**Действие**	**Параметр доступен в агенте фильтрации содержимого?**	**Comments**
Удалить	Больше или равно	Автоматическое удаление сообщения (без отчета о недоставке).	Да	Если включен этот порог, значение вероятности нежелательной почты должно быть больше всех остальных.

Пороговое значение SCL**	**Оператор сравнения значения вероятности нежелательной почты**	**Действие**	**Параметр доступен в агенте фильтрации содержимого?**	**Comments**
Отклонение	Больше или равно	Отклонение сообщения с отправкой отчета о недоставке.	Да	Значение вероятности нежелательной почты должно быть меньше значения порога удаления, но больше значений порога перемещения в карантин или папку нежелательной почты. По умолчанию этот порог включен в агенте фильтрации содержимого. Также по умолчанию ему присвоено значение 7.

Пороговое значение SCL**	Оператор сравнения значения вероятности нежелательной почты	Действие	Параметр доступен в агенте фильтрации содержимого?	Comments
Карантин	Больше или равно	Отклонение и помещение сообщения в почтовый ящик карантина нежелательной почты. Дополнительные сведения о настройке почтового ящика карантина спама см. в разделе Настройка почтового ящика карантина нежелательной почты.	Да	Если включен этот порог, значение вероятности нежелательной почты должно быть меньше значений порога удаления или отклонения, но больше значения порога перемещения в папку нежелательной почты.

Пороговое значение SCL**	Оператор сравнения значения вероятности нежелательной почты	Действие	Параметр доступен в агенте фильтрации содержимого?	Comments
Папка нежелательной почты	Больше	Доставка сообщения в папку нежелательной почты в почтовом ящике. Выполнение этого действия управляется правилом нежелательной почты, которое по умолчанию включено в каждом почтовом ящике. Дополнительные сведения см. в разделе Использование командной консоли Exchange для включения или отключения правила нежелательной почты в почтовом ящике данной статьи.	Нет Пороговое значение вероятности нежелательной почты настраивается для почтового ящика. Настройка порогового значения вероятности нежелательной почты выполняется для организации Exchange или почтового ящика.	Значение вероятности нежелательной почты должно быть меньше, чем остальные. По умолчанию это пороговое значение включено в организации Exchange и имеет значение по умолчанию 4. Так как правило нежелательной почты по умолчанию включено во всех почтовых ящиках, сообщения, поступающие в почтовый ящик со значением SCL 5 или выше, перемещаются в папку Нежелательная Email.

Чтобы настроить параметры порога вероятности нежелательной почты для почтового ящика, используйте следующий синтаксис:

PowerShell

```
Set-Mailbox <MailboxIdentity> -SCLDeleteEnabled <$true | $false | $null> -
SCLDeleteThreshold <0-9 | $null> -SCLRejectEnabled <$true | $false | $null>
-SCLRejectThreshold <0-9 | $null> -SCLQuarantineEnabled <$true | $false |
```

```
$null> -SCLQuarantineThreshold <0-9 | $null> -SCLJunkEnabled <$true | $false
| $null> -SCLJunkThreshold <0-9 | $null>
```

Пример отключения порога вероятности нежелательной почты для почтового ящика пользователя Jeff Phillips.

PowerShell

```
Set-Mailbox "Jeff Phillips" -SCLJunkEnabled $false
```

Пример отключения порога вероятности нежелательной почты для всех почтовых ящиков пользователей отдела North America в домене consoto.com.

PowerShell

```
Get-Mailbox -RecipientTypeDetails UserMailbox -OrganizationalUnit
"contoso.com/North America" | Set-Mailbox -SCLJunkEnabled $false
```

Пример отключения порога вероятности нежелательной почты для всех почтовых ящиков пользователей, которые имеются в базе данных почтовых ящиков MDB 01.

PowerShell

```
Get-Mailbox -RecipientTypeDetails UserMailbox -Database "MDB 01" | Set-
Mailbox -SCLJunkEnabled $false
```

Пример отключения порога вероятности нежелательной почты для всех почтовых ящиков пользователей организации.

PowerShell

```
$All = Get-Mailbox -RecipientTypeDetails UserMailbox -ResultSize Unlimited;
$All | foreach {Set-Mailbox $_.Name -SCLJunkEnabled $false}
```

Примечания.

- Чтобы удалить определенные пороговые значения SCL в почтовом ящике, чтобы пороговое значение SCL контролировался агентом фильтра содержимого (удаление, отклонение или карантин) или организацией Exchange (папка нежелательной Email), используйте значение `$null`.
- Если отключить пороговое значение нежелательной почты Email папки *SCL (SCLJunkEnabled* — `$false`), но правило нежелательной почты по-прежнему включено в почтовом ящике, Exchange по-прежнему может доставлять

сообщения в папку "Нежелательная Email" на основе списка Заблокированные отправители почтового ящика. Кроме того, даже если отключить правило нежелательной почты для почтового ящика, Outlook (в режиме кэширования Exchange) по-прежнему будет перемещать сообщения в папку нежелательной почты, самостоятельно принимая решение о том, является ли сообщение спамом, или на основе записей в списке заблокированных отправителей.

Как проверить, все ли получилось?

Чтобы убедиться в том, что пороги вероятности нежелательной почты для почтового ящика успешно настроены, воспользуйтесь любой из приведенных ниже процедур.

- Для одного почтового ящика *замените*< *MailboxIdentity*> идентификатором почтового ящика и выполните следующую команду, чтобы проверить значения свойств:

```
PowerShell

Get-Mailbox <MailboxIdentity> | Format-List SCL*
```

- Для массовых операций укажите фильтр, который использовался для настройки пороговых значений SCL, и замените команду **Set-Mailbox** на `Format-List Name,SCL*`. Например:

```
PowerShell

Get-Mailbox -RecipientTypeDetails UserMailbox -OrganizationalUnit
"contoso.com/North America" | Format-List Name.SCL*
```

Использование Командная консоль Exchange для настройки порогового значения вероятности нежелательной почты для папки "Нежелательная почта" для всех почтовых ящиков в организации

Если используется пороговое значение вероятности нежелательной почты для папки "Нежелательная почта", настроенное для организации Exchange, то при

соблюдении всех указанных ниже условий правило нежелательной почты доставляет сообщения в папку нежелательной почты почтового ящика.

- Службой Exchange сообщению присвоено значение вероятности нежелательной почты (обычно оно присваивается агентом фильтрации содержимого).
- В почтовом ящике включено правило нежелательной почты. Оно включено по умолчанию, однако для того, чтобы оно заработало в полной мере, почтовый ящик необходимо открыть в Outlook (в режиме кэширования Exchange) или в Outlook в Интернете.
- Для почтового ящика не настроен порог вероятности нежелательной почты (по умолчанию порог не настроен).
- Значение SCL сообщения больше порогового значения нежелательной Email папки SCL, настроенного для организации Exchange. Значение по умолчанию — 4. Это означает, что сообщения со значением SCL 5 или выше перемещаются в папку "Нежелательная Email" правилом нежелательной почты.

Для настройки порогового значения вероятности нежелательной почты для всех почтовых ящиков в организации используйте следующий синтаксис:

PowerShell

```
Set-OrganizationConfig -SCLJunkThreshold <0-9>
```

Пример задания для вероятности нежелательной почты значения 5 (все сообщения, значения вероятности нежелательной почты которых больше или равны 6, перемещаются правилом нежелательной почты в папку "Нежелательная почта").

PowerShell

```
Set-OrganizationConfig -SCLJunkThreshold 5
```

Примечания.

- Чтобы переопределить пороговое значение вероятности нежелательной почты почтового ящика, можно настроить соответствующий порог в почтовом ящике. Дополнительные сведения см. в разделе Использование командной консоли Exchange для настройки пороговых значений вероятности нежелательной почты для почтового ящика данной статьи.

- Если отключить правило нежелательной почты в почтовом ящике, значение порогового значения папки нежелательной Email SCL для организации Exchange (или в почтовом ящике) будет бессмысленным, так как правило нежелательной почты требуется exchange для доставки сообщений в папку "Нежелательная Email". Дополнительные сведения см. в разделе Использование командной консоли Exchange для включения или отключения правила нежелательной почты в почтовом ящике данной статьи.

Как проверить, все ли получилось?

Чтобы проверить, успешно ли настроено пороговое значение вероятности нежелательной почты для всех почтовых ящиков организации, выполните следующую команду, чтобы проверить значение свойства **SCLJunkThreshold**:

PowerShell

```
Get-OrganizationConfig | Format-List SCLJunkThreshold
```

Использование Командная консоль Exchange для настройки почтового ящика на обход фильтрации Exchange для защиты от нежелательной почты

Почтовый ящик можно настроить таким образом, чтобы сообщения обходили все фильтры Exchange для защиты от нежелательной почты. Такую настройку можно применить в случае, если в организации используются фильтры Exchange для защиты от нежелательной почты, однако требуется, чтобы сообщения, отправляемые на определенные почтовые ящики, обходили такие фильтры. Такой подход к фильтрации нежелательной почты можно применить в отношении почтовых ящиков, для которых критичны любые ложные срабатывания (например, для почтовых ящиков отдела продаж или службы поддержки, когда существует риск заблокировать сообщения от вполне надежных источников).

Для настройки почтового ящика на обход фильтров нежелательной почты используйте следующий синтаксис:

PowerShell

```
Set-Mailbox <MailboxIdentity> -AntispamBypassEnabled <$true | $false>
```

Пример исключения сообщений, отправленных на почтовый ящик "Customer Support", из фильтров Exchange для защиты от нежелательной почты.

```
PowerShell

Set-Mailbox "Customer Support" -AntispamBypassEnabled $true
```

Как проверить, все ли получилось?

Чтобы убедиться в том, что почтовый ящик успешно настроен на обход фильтров нежелательной почты, воспользуйтесь любой из приведенных ниже процедур.

- Замените <MailboxIdentity> удостоверением почтового ящика, а затем выполните следующую команду, чтобы проверить значение свойства **AntispamBypassEnabled**:

  ```
  PowerShell

  Get-Mailbox <MailboxIdentity> | Format-List AntispamBypassEnabled
  ```

- Чтобы найти все почтовые ящики в организации, которые настроены на обход фильтров нежелательной почты, выполните следующую команду:

  ```
  PowerShell

  Get-Mailbox -ResultSize Unlimited | where {$_.AntispamBypassEnabled -eq $true} | Format-Table Name,AntispamBypassEnabled
  ```

Сведения о параметрах нежелательной почты в Outlook

Чтобы включить, отключить и настроить параметры фильтра нежелательной Email на стороне клиента, доступные в Outlook, используйте групповая политика. Дополнительные сведения см. в разделах Файлы административных шаблонов (ADMX/ADML) и Центр развертывания Office для Приложения Microsoft 365 для предприятий, Office 2019 и Office 2016 и Развертывание параметров нежелательной почты, таких как список надежных отправителей, с помощью групповая политика.

Если для фильтра нежелательной Email Outlook задано значение **Нет автоматической фильтрации** в**параметрах**>**нежелательной**>**почты**, Outlook не

пытается классифицировать сообщения как спам, но по-прежнему использует коллекцию безопасных списков (список надежных отправителей, список надежных получателей и список заблокированных отправителей) для перемещения сообщений в папку "Нежелательная Email".

Если для фильтра нежелательной почты Outlook выбран параметр **Низкий** или **Высокий**, то фильтр нежелательной почты Outlook использует собственную технологию фильтрации SmartScreen для определения и перемещения спама в папку "Нежелательная почта". Такая классификация спама выполняется отдельно от порога вероятности нежелательной почты, настроенного для организации Exchange или почтового ящика. Фактически Outlook игнорирует значение вероятности нежелательной почты, присвоенное сообщению программой Exchange (это касается всех значений вероятности нежелательной почты, отличных от -1), и руководствуется собственными критериями определения того, является ли сообщение спамом (хотя выводы о том, что сообщение является нежелательным, сделанные Exchange и Outlook, могут совпадать).

> ⓘ **Примечание**
>
> В ноябре 2016 г. корпорация Майкрософт прекратила выпуск обновлений определений спама для фильтров SmartScreen в Exchange и Outlook. Существующие определения спама SmartScreen остались на месте, но их эффективность, скорее всего, со временем снизится. Дополнительные сведения см. в статье **Прекращение поддержки SmartScreen в Outlook и Exchange**.

Итак, для перемещения сообщений в папку "Нежелательная почта" фильтр нежелательной почты Outlook может использовать как коллекции списков надежных отправителей почтового ящика, так и собственную классификацию спама, даже если в почтовом ящике отключены правило нежелательной почты и/или порог вероятности нежелательной почты. Разница заключается в том, на основании чего сообщение перемещается в папку "Нежелательная почта", — согласно правилу нежелательной почты на сервере или в соответствии с настройками фильтра нежелательной почты в клиенте Outlook.

Outlook и Outlook в Интернете поддерживают коллекцию безопасных списков. Коллекция списков безопасности сохраняется в почтовом ящике Exchange, поэтому изменения в коллекции списков безопасности в Outlook отображаются в Outlook в Интернете и наоборот. Функция агрегирования списка безопасного списка агента фильтра содержимого предоставляет доступ к этим спискам со встроенными

агентами защиты от нежелательной информации Exchange. Дополнительные сведения см. в разделе Объединение списков надежных отправителей.

Фильтрация содержимого

Статья • 04.04.2023

> **Примечание**
>
> В ноябре 2016 г. корпорация Майкрософт прекратила выпуск обновлений определений спама для фильтров SmartScreen в Exchange и Outlook. Существующие определения спама SmartScreen остались на месте, но их эффективность, скорее всего, со временем снизится. Дополнительные сведения см. в статье **Прекращение поддержки SmartScreen в Outlook и Exchange**.

Функция фильтрации содержимого оценивает входящие сообщения, определяя вероятность нежелательной почты. В отличие от других технологий фильтрации, фильтрация содержимого основана на характеристиках из статистически значимой выборки обыкновенных и нежелательных сообщений. Фильтрация содержимого в Exchange Server предоставляется агентом фильтра содержимого и практически не изменяется с Exchange Server 2010 г. Обновления для агента фильтрации содержимого периодически появляются в Центре обновления Майкрософт.

По умолчанию агент фильтрации содержимого включен на пограничных транспортных серверах, но его также можно включить на серверах почтовых ящиков. Дополнительные сведения см. в разделе Включение функций защиты от нежелательной почты на серверах почтовых ящиков.

Дополнительные сведения о настройке агента фильтра содержимого см. в разделе Процедуры фильтрации содержимого.

Использование агента фильтра содержимого

Агент фильтрации содержимого определяет вероятность нежелательной почты (SCL), присваивая каждому сообщению оценку от 0 до 9. Чем выше оценка, тем вероятнее, что сообщение нежелательное. В зависимости от этой оценки агент может выполнять следующие действия:

- **Удалить**. Сообщение автоматически удаляется без отчета о недоставке (также известного как отчет о недоставке, уведомление о состоянии доставки, DSN или *сообщение о отказе*).
- **Отклонить**: сообщение отклоняется с помощью NDR.

- **Карантин**. Сообщение отправляется в почтовый ящик карантина нежелательной почты. Дополнительные сведения о почтовом ящике карантина нежелательной почты см. в статье Карантин нежелательной почты в Exchange Server.

Например, можно указать, что сообщения с оценкой вероятности нежелательной почты 7 и выше следует удалять, с оценкой 6 — отклонять, с оценкой 5 — помещать на карантин.

Вы можете настроить пороги SCL, назначив каждому из этих действий разные оценки SCL. Дополнительные сведения о том, как настроить пороговое значение SCL в соответствии с требованиями организации, см. в разделе Пороговые значения уровня достоверности спама Exchange (SCL).

> ⓘ **Примечание**
>
> Сообщения больше 11 МБ не проверяются интеллектуальным фильтром сообщений. Они проходят через агент фильтрации содержимого без проверки.

Разрешающие и блокирующие выражения

Вы можете настроить, как агент фильтра содержимого присваивает значения SCL, настроив пользовательские слова или фразы, которые агент будет использовать для применения обработки фильтра. Утвержденные слова или фразы настраиваются с помощью разрешенных фраз, а неутвержденные слова или фразы — с блок-фразами. Когда агент фильтра содержимого обнаруживает фразу Allow во входящего сообщения, агент автоматически присваивает сообщению значение SCL, равное 0. Кроме того, когда агент фильтра содержимого обнаруживает фразу Block во входящего сообщения, агент присваивает рейтинг SCL 9. Можно создать до 800 пользовательских слов или фраз в любом сочетании прописных и строчных букв. Однако этот случай игнорируется агентом фильтра содержимого.

Проверка штемпеля электронной почты Outlook

Агент фильтрации содержимого также включает проверку штемпеля электронной почты Outlook. Эта проверка применяется к исходящим сообщениям, чтобы помочь системам обмена сообщениями различать обыкновенную и нежелательную почту, а также уменьшить количество ложных срабатываний. *Ложное срабатывание* имеет место, когда фильтр нежелательной почты

неправильно определяет обыкновенное сообщение как нежелательное. Если функция проверки штемпеля электронной почты Outlook включена, агент фильтрации содержимого анализирует входящие сообщения по заголовкам вычислительных штемпелей. Наличие действительного, разрешенного вычислительного заголовка штемпеля в сообщении указывает, что клиентский компьютер, на котором создано сообщение, разрешил вычислительный штемпель, поэтому агент фильтрации содержимого, вероятно, понизит оценку SCL для этого сообщения.

Несмотря на то что для вычисления отдельных штемпелей компьютеру не требуется много времени, обработка штемпелей для миллионов нежелательных сообщений может стать препятствием для злонамеренного отправителя. Если сообщение отправителя содержит действительный, разрешенный вычислительный штемпель, вряд ли оно вредоносное, поэтому агент фильтрации содержимого снижает оценку SCL. Если функция проверки штемпелей включена, а входящее сообщение не содержит вычислительного заголовка со штемпелем или вычислительный заголовок со штемпелем недействителен, агент фильтрации содержимого не изменяет оценку вероятности нежелательной почты.

Обход получателя, отправителя и домена отправителя

В некоторых организациях все сообщения на определенные псевдонимы необходимо принимать, что может привести к проблемам, если ваша организация управляет большим объемом нежелательной почты. Вы можете настроить исключения для фильтрации содержимого от определенных получателей, отправителей и доменов.

Например, у компании Woodgrove Bank есть псевдоним customerloans@woodgrovebank.com , который предоставляет поддержку по электронной почте внешним кредитным клиентам, поэтому администраторы Exchange настраивают блок-фразы для фильтрации сообщений, которые обычно используются в спаме, отправляемые недобросовестными кредитными агентствами. Чтобы предотвратить отклонение потенциально допустимых сообщений, администраторы устанавливают исключения для фильтрации содержимого, вводя список адресов электронной почты получателей в конфигурации агента фильтра содержимого.

Объединение списка надежных отправителей

Агрегирование списков безопасности — это набор функций защиты от нежелательнойam, которые совместно используются в Outlook и Exchange. Как

следует из названия, он собирает данные из списков защиты от нежелательной сети, которые настраивают пользователи Outlook, и делает эти данные доступными для агентов антиспам на сервере Exchange Server. Агент фильтра содержимого использует списки надежных отправителей Outlook, списки надежных получателей и доверенные контакты для оптимизации фильтрации нежелательной почты. Email сообщения от этих контактов определяются агентом фильтра содержимого как безопасные. Фильтрация отправителей и агент фильтра отправителей использует список заблокированных отправителей Outlook для фильтрации отправителей для каждого получателя. Дополнительные сведения см. в разделе Объединение списков надежных отправителей.

Настройка агента фильтра содержимого

Агент фильтра содержимого настраивается с помощью командной консоли Exchange. Дополнительные сведения см. в разделе Процедуры фильтрации содержимого.

Чтобы определить, является ли сообщение нежелательным, агенту фильтрации содержимого требуются обновления. В них содержится информация о поддельных веб-сайтах, эвристические данные для фильтра SmartScreen (Майкрософт) и другие обновления интеллектуального фильтра сообщений. Размер этих обновлений обычно около 6 МБ, и они остаются полезными дольше, чем другие обновления для защиты от спама.

Обновления для фильтра содержимого доступны в Центре обновления Майкрософт. Обновленные данные обновления фильтра содержимого можно загружать каждые две недели.

Использование значения SCL в правилах потока обработки почты на пограничных транспортных серверах

На пограничных транспортных серверах агент правил edge действует с сообщениями, прежде чем значение SCL будет добавлено агентом фильтра содержимого. Если вы хотите использовать правило потока обработки почты *SCLOver* (также известное как правило транспорта), необходимо настроить агент фильтра содержимого для запуска перед агентом правил Edge, изменив приоритеты агента транспорта. Дополнительные сведения см. в статье Создание значений SCL сообщений для правил потока обработки почты на пограничных транспортных серверах.

Примечания.

- Хотя агент фильтра содержимого работает на других событиях SMTP, значение SCL отмечено в сообщении экземпляром агента фильтра содержимого, зарегистрированным в событии `OnEndOfData` SMTP.

- Если настроить агент фильтра содержимого для работы с сообщениями перед агентом пограничных правил на пограничном транспортном сервере, сервер может нести дополнительные расходы на обработку, так как сообщения, которые обычно отклоняются другими правилами потока обработки почты, получаются и оцениваются агентом фильтра содержимого до их отклонения агентом правил Edge. Кроме того, вы не сможете настроить правило потока обработки почты для пометки сообщения со значением `-1`SCL , которое сообщает агенту фильтра содержимого игнорировать сообщение.

Дополнительные сведения об агентах транспорта и приоритете агента транспорта см. в разделе Транспортные агенты в Exchange Server.

Процедуры фильтрации содержимого

Статья • 04.04.2023

Функция фильтрации содержимого оценивает входящие сообщения, чтобы определить, являются ли они обыкновенными или нежелательными. Дополнительные сведения о фильтрации содержимого и агенте фильтра содержимого см. в разделе Фильтрация содержимого.

Ряд аспектов фильтрации содержимого можно настроить. Например:

- Включить или отключить фильтрацию содержимого для сообщений из внутренних (прошедших проверку подлинности) и внешних (не прошедших проверку подлинности) источников (по умолчанию она включена для входящих сообщений из внешних источников).
- Настроить исключения для фильтрации содержимого от определенных отправителей, получателей и исходных доменов.
- Настроить разрешенные и заблокированные выражения, которые требуется искать в сообщениях.
- Настроить пороговые значения вероятности нежелательной почты (SCL), которые определяют, какие действия необходимо предпринимать в отношении сообщений (удалять, отклонять или помещать на карантин).

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: менее 5 минут
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Антиспам" раздела Разрешения для защиты от вредоносных программ и защиты от вредоносных программ .
- Для выполнения этой процедуры можно использовать только PowerShell. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- По умолчанию в службе транспорта на сервере почтовых ящиков не включены функции защиты от нежелательной почты. Как правило, их следует включать, только если организация Exchange не выполняет никакую предварительную фильтрацию нежелательной почты до приема входящих

сообщений. Дополнительные сведения см. в разделе Включение функций защиты от нежелательной почты на серверах почтовых ящиков.

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Включение или отключение фильтрации содержимого с помощью командной консоли Exchange

Чтобы отключить фильтрацию контента, выполните следующую команду:

```
Set-ContentFilterConfig -Enabled $false
```

Чтобы включить фильтрацию содержимого, выполните следующую команду:

```
Set-ContentFilterConfig -Enabled $true
```

> **Примечание**
>
> При отключении фильтрации контента, соответствующий агент фильтрации все еще включен. Чтобы отключить агент фильтра содержимого, выполните команду : `Disable-TransportAgent "Content Filter Agent"`.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно включили или отключили фильтрацию содержимого, выполните следующую команду, чтобы проверить значение свойства **Enabled**:

```
Get-ContentFilterConfig | Format-List Enabled
```

Использование командной консоли Exchange для включения или отключения фильтрации содержимого для внешних сообщений

По умолчанию фильтрация содержимого включена для внешних сообщений.

Чтобы отключить фильтрацию контента для внешних сообщений, выполните следующую команду:

```
Set-ContentFilterConfig -ExternalMailEnabled $false
```

Чтобы включить фильтрацию контента для внешних сообщений, выполните следующую команду:

```
Set-ContentFilterConfig -ExternalMailEnabled $true
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно включили или отключили фильтрацию содержимого для внешних сообщений, выполните следующую команду, чтобы проверить значение свойства **ExternalMailEnabled**:

```
Get-ContentFilterConfig | Format-List ExternalMailEnabled
```

Включение или отключение фильтрации содержимого для внутренних сообщений с

помощью командной консоли Exchange

Не рекомендуем применять фильтры защиты от спама к сообщениям от надежных партнеров или внутренним сообщениям. В этом случае всегда существует вероятность ложного срабатывания фильтра. Чтобы снизить эту вероятность, настройте запуск агентов защиты от спама только для сообщений из непроверенных и неизвестных источников.

Чтобы включить фильтрацию контента для внутренних сообщений, выполните следующую команду:

```
Set-ContentFilterConfig -InternalMailEnabled $true
```

Чтобы выключить фильтрацию контента для внутренних сообщений, выполните следующую команду:

```
Set-ContentFilterConfig -InternalMailEnabled $false
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно включили или отключили фильтрацию содержимого для внутренних сообщений, выполните следующую команду, чтобы проверить значение свойства **InternalMailEnabled**:

```
Get-ContentFilterConfig | Format-List InternalMailEnabled
```

Использование командной консоли Exchange для настройки исключений получателей и отправителей для фильтрации содержимого

Вы можете указать исключения получателей и отправителей, которые заменят существующие значения, либо добавить или удалить определенные исключения

получателей и отправителей, не изменяя другие существующие значения.

Чтобы заменить существующие значения, используйте следующий синтаксис:

```
Set-ContentFilterConfig -BypassedRecipients <recipient1,recipient2...> -
BypassedSenders <sender1,sender2...> -BypassedSenderDomains
<domain1,domain2...>
```

В этом примере настраиваются следующие исключения в фильтрации контента:

- Получатели laura@contoso.com и julia@contoso.com не проверяются с помощью фильтрации содержимого.
- Отправители steve@fabrikam.com и cindy@fabrikam.com не проверяются с помощью фильтрации содержимого.
- Все отправители из домена nwtraders.com и дочерних доменов не проверяются при фильтрации контента.

```
Set-ContentFilterConfig -BypassedRecipients
laura@contoso.com,julia@contoso.com -BypassedSenders
steve@fabrikam.com,cindy@fabrikam.com -BypassedSenderDomains *.nwtraders.com
```

Чтобы добавить или удалить записи, не изменяя другие существующие значения, используйте следующий синтаксис:

```
Set-ContentFilterConfig -BypassedRecipients @{Add="<recipient1>","
<recipient2>"...; Remove="<recipient1>","<recipient2>"...} -BypassedSenders
@{Add="<sender1>","<sender2>"...; Remove="<sender1>","<sender2>"...} -
BypassedSenderDomains @{Add="<domain1>","<domain2>"...; Remove="<domain1>","
<domain2>"...}
```

В этом примере настраиваются следующие исключения в фильтрации контента:

- Добавьте tiffany@contoso.com и chris@contoso.com в список существующих получателей, которые не проверяются фильтрацией содержимого.
- Добавьте joe@fabrikam.com и michelle@fabrikam.com в список существующих отправителей, которые не проверяются фильтрацией содержимого.

- Добавить blueyonderairlines.com в список текущих доменов, отправители из которых не проверяются при фильтрации контента.
- Удалить домен woodgrovebank.com и все его дочерние домены из списка текущих доменов, отправители из которых не проверяются при фильтрации контента.

```
Set-ContentFilterConfig -BypassedRecipients
@{Add="tiffany@contoso.com","chris@contoso.com"} -BypassedSenders
@{Add="joe@fabrikam.com","michelle@fabrikam.com"} -BypassedSenderDomains
@{Add="blueyonderairlines.com"; Remove="*.woodgrovebank.com"}
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно настроили исключения получателей и отправителей, выполните следующую команду, чтобы проверить значения свойств:

```
Get-ContentFilterConfig | Format-List Bypassed*
```

Использование командной консоли Exchange для настройки разрешенных и заблокированных фраз для фильтрации содержимого

Чтобы добавить разрешенные и заблокированные слова и выражения, используйте следующий синтаксис:

```
Add-ContentFilterPhrase -Influence GoodWord -Phrase <Phrase> -Influence
BadWord -Phrase <Phrase>
```

Этот пример разрешает все сообщения, которые содержат фразу "отзыв клиента".

```
Add-ContentFilterPhrase -Influence GoodWord -Phrase "customer feedback"
```

В этом примере блокирует все сообщения, которые содержат фразу "подсказка по акциям".

```
Add-ContentFilterPhrase -Influence BadWord -Phrase "stock tip"
```

Чтобы удалить разрешенные или заблокированные выражения, выполните следующую команду:

```
Remove-ContentFilterPhrase -Phrase <Phrase>
```

В этом примере удаляется фраза "подсказка по акциям":

```
Remove-ContentFilterPhrase -Phrase "stock tip"
```

Как проверить, что все получилось?

Чтобы убедиться, что вы успешно настроили разрешенные и заблокированные выражения, выполните следующую команду, чтобы проверить значения свойств:

```
Get-ContentFilterPhrase | Format-Table -Auto Influence,Phrase
```

Настройка пороговых значений SCL для фильтрации содержимого с помощью командной консоли Exchange

Чтобы настроить пороговые значения вероятности нежелательной почты и предпринимаемые действия, используйте следующий синтаксис:

```
Set-ContentFilterConfig -SCLDeleteEnabled <$true | $false> -
SCLDeleteThreshold <Value> -SCLRejectEnabled <$true | $false> -
```

```
SCLRejectThreshold <Value> -SCLQuarantineEnabled <$true | $false> -
SCLQuarantineThreshold <Value>
```

Примечания.

- Действие "Удалить" имеет более высокий приоритет по сравнению с действием "Отклонить", а действие "Отклонить" — более высокий приоритет по сравнению с действием "Поместить на карантин". Таким образом, пороговое значение вероятности нежелательной почты для действия "Удалить" должно превышать пороговое значение вероятности нежелательной почты действия "Отклонить", которое, в свою очередь, должно превышать пороговое значение вероятности нежелательной почты действия "Поместить на карантин". Только действие "Отклонить" включено по умолчанию, его пороговое значение SCL по умолчанию равно 7.

- Для действия "Поместить на карантин" требуется почтовый ящик карантина нежелательной почты. Дополнительные сведения см. в разделе Настройка почтового ящика карантина нежелательной почты.

В этом примере настраиваются следующие пороговые значения вероятности нежелательной почты:

- Действие **Удалить** включено, соответствующее пороговое значение SCL равно 9.

- Действие **Отклонить** включено, соответствующее пороговое значение SCL равно 8.

- Действие **Поместить на карантин** включено, соответствующее пороговое значение SCL равно 7.

```

Set-ContentFilterConfig -SCLDeleteEnabled $true -SCLDeleteThreshold 9 -
SCLRejectEnabled $true -SCLRejectThreshold 8 -SCLQuarantineEnabled $true -
SCLQuarantineThreshold 7
```

Как проверить, что все получилось?

Чтобы убедиться, что вы успешно настроили пороговые значения SCL, выполните следующую команду, чтобы проверить значения свойств:

```

```

```
Get-ContentFilterConfig | Format-List SCL*
```

Настройка ответа на отклонение для фильтрации содержимого с помощью командной консоли Exchange

Если действие "Отклонить" включено, вы можете настроить ответ при отклонении, который передается отправителю сообщения. Ответ не должен превышать 240 символов.

Чтобы настроить сообщение об отклонении, используйте следующий синтаксис:

```
Set-ContentFilterConfig -RejectionResponse "<Custom Text>"
```

В этом примере для агента фильтрации контента настраивается отправка настроенного ответа об отклонении.

```
Set-ContentFilterConfig -RejectionResponse "Your message was rejected
because it appears to be SPAM."
```

Как проверить, что все получилось?

Чтобы убедиться, что вы успешно настроили сообщение об отклонении, выполните следующую команду, чтобы проверить значения свойств:

```
Get-ContentFilterConfig | Format-List *Reject*
```

Использование командной консоли Exchange для включения или отключения Email postmarking в Outlook

Проверка outlook *Email postmarking* — это вычислительное доказательство того, что Microsoft Outlook применяется к исходящим сообщениям, чтобы помочь системам обмена сообщениями отличать допустимые сообщения электронной почты от нежелательной почты (уменьшить количество ложных срабатываний). Postmarking впервые появилась в Outlook 2007 и включена в Outlook по умолчанию.

Чтобы отключить проверку почтового штемпеля Outlook, выполните следующую команду:

```
Set-ContentFilterConfig -OutlookEmailPostmarkValidationEnabled $false
```

Чтобы включить проверку почтового штемпеля Outlook, выполните следующую команду:

```
Set-ContentFilterConfig -OutlookEmailPostmarkValidationEnabled $true
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно настроили добавление штемпелей электронной почты Outlook, выполните следующую команду, чтобы проверить значение свойства **OutlookEmailPostmarkValidationEnabled**:

```
Get-ContentFilterConfig | Format-List OutlookEmailPostmarkValidationEnabled
```

Объединение списка надежных отправителей

Статья • 04.04.2023

В Exchange Server *агрегирование списка безопасности* относится к адресам электронной почты отправителей и получателей, которые собираются из параметров нежелательной Email всех пользователей в Microsoft Outlook, Outlook в Интернете или **командлете Set-MailboxJunkEmailConfiguration** и совместно используются встроенными агентами защиты от спама Exchange. Агрегат safelist практически не изменился с Exchange Server 2010 года.

При включении и настройке агрегирования списков безопасности Exchange может выполнить следующие действия на основе статистических данных списка безопасности:

- Доставка входящих сообщений от отправителей, которые считаются надежными, без дополнительной обработки для защиты от нежелательной почты (в результате чего сообщения могут быть идентифицированы как спам).
- Блокирование входящих сообщений от отправителей, которые определены как вредоносные.

Порядок настройки объединения списков надежных отправителей см. в статье Safelist aggregation procedures.

В контексте фильтрации нежелательной почты сообщение с *ошибочно положительным результатом* представляет собой допустимое сообщение, определенное как спам. В организациях, где фильтруются многие тысячи сообщений ежедневно, наличие даже небольшой доли ошибочно положительных оценок означает, что пользователи не получат множество допустимых сообщений. Объединение списков надежных отправителей, вероятно, является наиболее эффективным способом уменьшения числа ошибочно положительных оценок.

Сведения, содержащиеся в коллекции списков надежных отправителей пользователя

Коллекция списков надежных отправителей — это объединенные данные из пользовательского списка надежных отправителей, списка надежных получателей,

списка заблокированных отправителей и внешних контактов (дополнительно). Эти данные хранятся в почтовом ящике Exchange иOutlook. Дополнительные сведения о добавлении записей в коллекцию списков надежных отправителей пользователя и удалении их из него см. в разделе Использование командной консоли Exchange для настройки коллекции списков надежных отправителей почтового ящика.

В пользовательской коллекции списков надежных отправителей хранятся следующие сведения:

- **Надежные отправители**: SMTP-адрес электронной почты в поле **От:**
- **Безопасные получатели**: SMTP-адрес электронной почты в поле **Кому:** .
- **Заблокированные отправители**. Как и безопасные отправители, пользователи могут блокировать нежелательных отправителей, добавляя их в список заблокированных отправителей.
- **Безопасный домен**. Это часть списка надежных отправителей, но вместо SMTP-адреса электронной почты (masato@contoso.com) указывается домен отправителя (lcontoso.com).

  Примечание. По умолчанию Exchange не включает безопасные домены во время агрегирования списка безопасности. Однако вы можете настроить объединение списка надежных отправителей так, чтобы включить в него данные надежного домена. Дополнительные сведения см. в статье Configure Content Filtering to Use Safe Domain Data.
- **Внешние контакты**. В коллекцию безопасных списков можно включить два типа внешних контактных данных:
  - **Получатели, которым пользователь отправил почту**: эти адреса электронной почты добавляются в список Надежных отправителей, если пользователь выбирает **Автоматически добавлять пользователей, которым я отправляю сообщение, в список надежных отправителей в параметрах** Нежелательной Email в Outlook.
  - **Контакты в папке контактов пользователя**. Эти адреса электронной почты добавляются в список Надежных отправителей, если пользователь выбирает **также доверять электронной почте из моих контактов** в параметрах Нежелательная Email в Outlook, Outlook в Интернете или командлете **Set-MailboxJunkEmailConfiguration**.

How Exchange uses the safelist collection

Коллекция списков надежных отправителей хранится на сервере почтовых ящиков пользователя. Пользователь может поддерживать в коллекции списков надежных отправителей до 1024 уникальных элементов. В Exchange есть помощник по почтовым ящикам, который называется помощником по параметрам почтового ящика нежелательной Email, который отслеживает изменения в коллекции списков безопасности для почтовых ящиков на сервере. Затем он проводит репликацию этих изменений в Active Directory, где коллекция списков надежных отправителей хранится в каждом объекте пользователя. Коллекция списков надежных отправителей оптимизирована для уменьшения объема хранения и репликации. Если в сети периметра имеется выписанный пограничный транспортный сервер, служба Microsoft Exchange EdgeSync обеспечивает репликацию коллекции списков надежных отправителей в экземпляр служб Active Directory облегченного доступа к каталогам (AD LDS) на пограничном транспортном сервере.

Следующие антиспам-агенты Exchange используют коллекцию safelist:

- Агент фильтрации содержимого использует данные из списка надежных отправителей для доставки сообщений от этих отправителей без дополнительной (ненужной) обработки.
- Агент фильтра отправителей использует данные из списка заблокированных отправителей для отклонения или удаления сообщений от таких отправителей. Дополнительные сведения см. в статье Sender filtering procedures.

Примечание. Хотя список надежных получателей можно включить в агрегирование списка безопасности, агент фильтра содержимого не действует с данными надежных получателей.

Хеширование записей коллекции списков надежных отправителей

Записи коллекции safelist хэшируются (SHA-256) в одну сторону, прежде чем они будут сохранены в виде наборов массивов в трех атрибутах объектов пользователя, **msExchSafeSenderHash**, **msExchSafeRecipientHash** и **msExchBlockedSendersHash** в виде двоичного большого объекта. При хэширования данных создаются выходные данные фиксированной длины, и выходные данные, скорее всего, будут уникальными. Для хэширования записей коллекции safelist создается 4-байтовый хэш. При получении сообщения из Интернета Exchange хэширует адрес электронной почты отправителя и сравнивает его с хэшами, хранящимися от имени почтового ящика назначения. Если отправитель

соответствует хэшу надежных отправителей, сообщение обходит фильтрацию содержимого. Если отправитель соответствует хэшу заблокированных отправителей, сообщение блокируется.

Одностороннее хеширование записей коллекции списков надежных отправителей выполняет следующие важные функции:

- **Сокращает объем хранилища и репликации**. В большинстве случаев хэширование уменьшает размер данных. Поэтому сохранение и передача хэшированной версии записи коллекции списков надежных отправителей экономит место при хранении и время при репликации. Например, пользователь, имеющий 200 записей в коллекции списка безопасности, создаст около 800 байт хэшированных данных, хранящихся и реплицируемых в Active Directory.
- **Делает коллекции списков безопасности пользователей непригодными для использования злоумышленниками**. Так как односторонние хэш-значения невозможно перепроектировать в исходный SMTP-адрес или домен, коллекции списков безопасности не предоставляют пригодные для использования адреса электронной почты злоумышленникам, которые могут скомпрометировать сервер Exchange.

Включение объединения списка надежных отправителей

Объединение списков надежных отправителей включено по умолчанию. Данные сбора списка безопасности записываются в Active Directory помощником по почтовым ящикам "Параметры нежелательной Email". В отличие от предыдущих версий Exchange, вам не нужно вручную запускать командлет **Update-SafeList** для хэширования и записи данных сбора списка безопасности в Active Directory.

Объединение списков надежных отправителей можно запустить вручную с помощью командлета **Update-Safelist**. Однако нужно помнить о трафике репликации, который может возникнуть автоматически при выполнении этой команды. Запуск командлета **Update-Safelist** на нескольких почтовых ящиках, в которых активно используются списки надежных отправителей, может привести к появлению значительного объема сетевого трафика. Для нескольких почтовых ящиков эту команду рекомендуется запускать в нерабочие часы, когда загрузка минимальна.

Командлет **Update-SafeList** считывает коллекцию списков надежных отправителей из почтового ящика пользователя, хэширует каждую запись, сортирует записи для

быстрого поиска, а затем преобразует хэш в двоичный атрибут. Наконец, командлет **Update-SafeList** сравнивает созданный двоичный атрибут с каждым значением, хранящимся в атрибуте. Если два значения совпадают, командлет **Update-SafeList** не обновляет значение пользовательского атрибута за счет применения данных объединения списка надежных отправителей. Если значения отличаются, командлет **Update-SafeList** обновляет значение объединения списка надежных отправителей.

Дополнительные сведения об использовании **Update-SafeList** см. в статье Safelist aggregation procedures.

Процедуры объединения списков надежных отправителей

Статья • 04.04.2023

В Exchange Server *агрегирование списка безопасности* относится к данным отправителя и получателя, которые собираются из параметров нежелательной Email всех пользователей в Microsoft Outlook, Outlook в Интернете или **командлете Set-MailboxJunkEmailConfiguration** и совместно используемые встроенными агентами защиты от спама Exchange. Дополнительные сведения см. в разделе Объединение списков надежных отправителей.

Процедуры, описанные в этом разделе, можно использовать для следующего:

- Настройка ограничений на число надежных отправителей и заблокированных отправителей, которые хранятся для определенных почтовых ящиков.
- Объединение списков надежных отправителей вручную.
- Проверка правильности работы объединения списков надежных отправителей.

Дополнительные сведения о добавлении записей в коллекцию списков надежных отправителей пользователя и удалении их из него см. в разделе Использование командной консоли Exchange для настройки коллекции списков надежных отправителей почтового ящика.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в разделе "Разрешения подготовки получателей" раздела Разрешения получателей и в разделе "Функции защиты от нежелательной почты" раздела Разрешения для защиты от вредоносных программ .
- Для выполнения этой процедуры можно использовать только PowerShell. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

- По умолчанию в службе транспорта на сервере почтовых ящиков не включены функции защиты от нежелательной почты. Как правило, их следует включать, только если организация Exchange не выполняет никакую предварительную фильтрацию нежелательной почты до приема входящих сообщений. Дополнительные сведения см. в разделе Включение функций защиты от нежелательной почты на серверах почтовых ящиков.

- Следует помнить о трафике репликации, который может возникнуть автоматически при запуске командлета **Update-SafeList**. Выполнение этой команды на нескольких почтовых ящиках, в которых активно используются списки надежных отправителей, может привести к появлению значительного объема сетевого трафика. Для нескольких почтовых ящиков эту команду рекомендуется запускать в нерабочие часы, когда загрузка минимальна.

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование Командная консоль Exchange для настройки ограничений коллекции списков надежных отправителей почтового ящика

Можно настроить максимальное число надежных отправителей и список заблокированных отправителей, задаваемых пользователем. По умолчанию пользователи могут настроить до 5000 надежных отправителей и 500 заблокированных отправителей.

Чтобы настроить максимальное количество надежных отправителей и заблокированных отправителей, используйте следующий синтаксис:

PowerShell

```
Set-Mailbox <MailboxIdentity> -MaxSafeSenders <Integer> -MaxBlockedSenders
<Integer>
```

В этом примере в почтовом ящике john@contoso.com настраивается не более 2000 надежных отправителей и 200 заблокированных отправителей.

PowerShell

```
Set-Mailbox john@contoso.com -MaxSafeSenders 2000 -MaxBlockedSenders 200
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно настроили ограничения коллекции списка безопасных почтовых ящиков, замените *<MailboxIdentity>* идентификатором почтового ящика и выполните следующую команду, чтобы проверить значения свойств почтового ящика.

PowerShell

```
Get-Mailbox <MailboxIdentity> | Format-List Name,Max*Senders
```

Использование Командная консоль Exchange для объединения списков надежных отправителей вручную

Объединение выполняется автоматически, поэтому вам не требуется самостоятельно запускать командлет **Update-Safelist**. Однако вы можете запустить этот командлет для проверки объединения списков надежных отправителей.

Чтобы вручную запустить объединение списков надежных отправителей, используйте следующий синтаксис:

PowerShell

```
Update-Safelist <MailboxIdentity> [-Type <SafeSenders | SafeRecipients | Both>] [-IncludeDomains]
```

В этом примере список надежных отправителей для почтового ящика john@contoso.com записывается в Active Directory.

PowerShell

```
Update-Safelist john@contoso.com
```

Дополнительные сведения о синтаксисе и параметрах см. в разделе Update-SafeList.

Примечания.

- Вам не нужно использовать параметр *Type* , так как:
  - Значение по умолчанию — `SafeSenders`.
  - Агент фильтра содержимого не использует данные списка надежных получателей, поэтому `SafeRecipients` значения или `Both` не нужны.
- По умолчанию при объединении списков надежных отправителей не включатся записи доменов из списка надежных отправителей (только адреса электронной почты), однако вы можете настроить объединение таким образом, чтобы учитывались и записи доменов из коллекции списков надежных отправителей. Дополнительные сведения см. в статье Configure Content Filtering to Use Safe Domain Data.

Как проверить, все ли получилось?

Чтобы убедиться, что объединение успешно настроено, выполните следующие действия:

Действие 1. Использование Командная консоль Exchange для проверки включения агента фильтрации содержимого на сервере Exchange

Выполните следующую команду:

PowerShell

```
Get-ContentFilterConfig | Format-List Enabled
```

Если в выходных данных свойство **Enabled** имеет значение `True`, фильтрация содержимого включена. Если это не так, выполните следующую команду для включения фильтрации содержимого и агента фильтра содержимого на сервере Exchange:

PowerShell

```
Set-ContentFilterConfig -Enabled $true
```

Действие 2. (Необязательно) Используйте редактор ADSI, чтобы проверить репликацию данных объединения списка надежных отправителей на пограничные транспортные серверы

Этот шаг необходимо выполнять, только если вы используете агент фильтрации содержимого на компьютере с установленной ролью подписанного пограничного транспортного сервера в сети периметра.

Можно просмотреть объекты пользователя в экземпляре Службы Active Directory облегченного доступа к каталогам (AD LDS) на пограничном транспортном сервере, чтобы:

- убедиться, что в коллекции списков надежных отправителей указаны актуальные сведения об объектах пользователя;
- убедиться, что служба Microsoft Exchange EdgeSync реплицировала данные в экземпляр служб Active Directory облегченного доступа к каталогам.

Существует три атрибута коллекции списков надежных отправителей для каждого объекта пользователя.

- **msExchSafeRecipientsHash**: сохраняет хэш коллекции списка надежных получателей для пользователя.
- **msExchSafeSendersHash**: сохраняет хэш коллекции списка надежных отправителей для пользователя.
- **msExchBlockedSendersHash**: сохраняет хэш коллекции заблокированных отправителей для пользователя.

Если в атрибуте присутствует шестнадцатеричная строка, например `0xac 0xbd 0x03 0xca`, объект user был обновлен. Если атрибут имеет значение `<Not Set>`, атрибут не был обновлен.

Для поиска и просмотра атрибутов можно использовать редактор ADSI на пограничном транспортном сервере (запустить надстройку ADSIEdit.msc).

Действие 3. Отправьте тестовое сообщение, чтобы убедиться, что объединение списков надежных отправителей работает

Чтобы проверить работу функции объединения списков безопасных отправителей, необходимо отправить сообщение от безопасного отправителя, который в противном случае был бы заблокирован при фильтрации содержимого (например, в сообщении содержится заблокированная фраза). Если объединение списков надежных отправителей работает, сообщение должно быть доставлено в папку "Входящие".

1. Откройте почтовый ящик Exchange в Outlook и добавьте внешний адрес электронной почты (связанный с учетной записью, к которому можно получить доступ) в список надежных отправителей. Дополнительные сведения см. в разделе Добавление имен в списки фильтра нежелательной Email.

2. Воспользуйтесь командлетом **Update-SafeList**, чтобы вручную реплицировать коллекцию списков надежных отправителей из своего почтового ящика в Active Directory:

   ```
   PowerShell

   Update-Safelist <YourMailboxIdentity>
   ```

3. Необязательно. Если агент фильтра содержимого запущен на подписанном пограничном транспортном сервере в сети периметра, выполните командлет **Start-EdgeSynchronization** , чтобы принудительно выполнить репликацию EdgeSync.

4. Добавьте определенное слово в качестве заблокированной фразы в конфигурацию фильтра содержимого. Например:

   ```
   PowerShell

   Add-ContentFilterPhrase -Influence BadWord -Phrase "SafeList
   aggregation test"
   ```

   Дополнительные сведения см. в разделе Использование командной консоли Exchange для настройки разрешенных и заблокированных фраз для фильтра содержимого.

5. Из внешней учетной записи электронной почты, выбранной в действии 1, отправьте в почтовый ящик Exchange сообщение, содержащее заблокированную фразу, заданную в действии 4.

   Если сообщение успешно доставляется в папку "Входящие", объединение списка надежных отправителей функционирует правильно.

Карантин спама в Exchange Server

Статья • 04.04.2023

Многие организации связаны законодательными или нормативными требованиями, предъявляемыми к защите и доставке надежных сообщений электронной почты. В Exchange Server карантин нежелательной почты — это функция агента фильтра содержимого, которая снижает риск потери допустимых входящих сообщений электронной почты, предоставляя временное хранилище для сообщений, которые идентифицируются как спам. Карантин спама практически не изменился с Exchange Server 2010 года.

Сообщения, которые агент фильтра содержимого считает спамом, доставляются в почтовый ящик карантина нежелательной почты в организации в отчете о недоставке. Администраторы могут использовать Microsoft Outlook для просмотра сообщений в почтовом ящике карантина нежелательной почты и принятия соответствующих мер. Например, вы можете удалять сообщения или отправлять обыкновенные сообщения их получателям. Кроме того, для почтового ящика карантина нежелательной почты можно настроить автоматическое удаление сообщений по истечении определенного периода времени.

Чтобы использовать карантин нежелательной почты, сделайте следующее:

1. Убедитесь в том, что включена фильтрация содержимого.
2. Создайте выделенный почтовый ящик для карантина нежелательной почты.
3. указать почтовый ящик для карантина нежелательной почты;
4. установить порог вероятности нежелательной почты для карантина;
5. осуществлять управление почтовым ящиком для карантина нежелательной почты;
6. отрегулировать, если необходимо, порог вероятности нежелательной почты для карантина.

Подробные инструкции см. в разделе Настройка почтового ящика карантина нежелательной почты.

Дополнительные сведения

Агент фильтра содержимого оценивает входящие сообщения и назначает каждому из них вероятность нежелательной почты (SCL). SCL — это число от 0 до 9, где 0

означает очень низкую вероятность спама, а 9 — очень высокую. Для более высоких значений SCL можно настроить более серьезные действия. Например:

- **SCL имеет значение 8 или выше**: автоматически удалите сообщение.
- **SCL имеет значение 7**: отклонить сообщение с помощью недоставки.
- **SCL имеет значение 6**. На карантине сообщение.
- **SCL — 5**. Доставьте сообщение в папку "Нежелательная Email" пользователя.
- **SCL имеет значение 4 или ниже**. Доставьте сообщение в папку "Входящие" пользователя.

Дополнительные сведения см. в статье Пороговые значения уровня достоверности нежелательной почты Exchange (SCL).

В почтовом ящике карантина нежелательной почты можно просмотреть результаты фильтрации, проверив метки нежелательной почты (X-заголовки), добавленные к сообщениям. Дополнительные сведения см. в статье View antispam stamps in Outlook. Затем вы можете настроить пороговые значения вероятности нежелательной почты для более точной фильтрации спама, поступающего в организацию. Например:

- В почтовый ящик карантина нежелательной почты поступает слишком много обыкновенных сообщений (слишком много ложных срабатываний).
- В почтовый ящик карантина поступает слишком много очевидного спама (недостаточно спама отклоняется или удаляется).

Сведения о том, как отправить сообщение из карантина нежелательной почты получателю, см. в следующих статьях:

- Настройка Outlook для отображения исходного отправителя в почтовом ящике карантина нежелательной почты
- Освобождение сообщений из почтового ящика карантина нежелательной почты

Настройка почтового ящика карантина нежелательной почты в Exchange Server

Статья • 04.04.2023

Сообщения, которые агент фильтра содержимого считает нежелательной почтой, можно направлять в почтовый ящик карантина нежелательной почты. Если включен порог карантина вероятности нежелательной почты, все сообщения, помещенные на карантин, преобразуются в отчеты о недоставке (которые также называются NDR, уведомлениями о доставке, DSN или сообщениями о недоставке) и отправляются в указанный почтовый ящик карантина нежелательной почты. Администраторы могут просматривать сообщения, помещенные в карантин, и выпускать их предполагаемым получателям с помощью Microsoft Outlook.

Что нужно знать перед началом работы

- Предполагаемое время выполнения задачи: 30 минут.
- По умолчанию в службе транспорта на сервере почтовых ящиков не включены функции защиты от нежелательной почты. Как правило, их следует включать, только если организация Exchange не выполняет никакую предварительную фильтрацию нежелательной почты до приема входящих сообщений. Дополнительные сведения см. в разделе Включение функций защиты от нежелательной почты на серверах почтовых ящиков.
- Пользователь, отвечающий за почтовый ящик карантина нежелательной почты, может просматривать потенциально личные и конфиденциальные сообщения, а затем отправлять почту от имени любого пользователя в организации Exchange.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Действие 1. Убедитесь, что включена фильтрация содержимого

Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Функции защиты от вредоносных программ" в разделе Разрешения для защиты от вредоносных программ и защиты от вредоносных программ .

1. Выполните следующую команду, чтобы убедиться, что агент фильтра содержимого установлен и включен на сервере Exchange:

   PowerShell

   ```
   Get-TransportAgent "Content Filter Agent"
   ```

2. Выполните следующую команду, чтобы убедиться, что фильтрация содержимого включена.

   PowerShell

   ```
   Get-ContentFilterConfig | Format-List Enabled
   ```

Дополнительные сведения см. в разделе Процедуры фильтрации содержимого.

Действие 2. Создание выделенного почтового ящика для карантина нежелательной почты

Чтобы создать почтовый ящик карантина, выполните указанные ниже действия.

- **Создание выделенной базы данных Exchange**. Рекомендуется создать выделенную базу данных для почтового ящика карантина нежелательной почты. Почтовый ящик для карантина нежелательной почты должен иметь базу данных большого размера, поскольку при достижении квоты хранилища последующие сообщения будут потеряны. Дополнительные сведения см. в статье Управление базами данных почтовых ящиков в Exchange Server.

- **Создание выделенного почтового ящика и учетной записи пользователя**. Рекомендуется создать выделенный почтовый ящик и учетную запись пользователя для почтового ящика карантина нежелательной почты.

Дополнительные сведения см. в разделе Создание почтовых ящиков пользователей в Exchange Server.

Можно применять различные политики получателей, например, управление записями обмена сообщениями, квоты почтового ящика и права делегирования в зависимости от потребностей организации и корпоративных политик соответствия требованиям. Дополнительные сведения см. в статье Управление записями сообщений в Exchange Server.

> ⓘ **Примечание**
>
> Если сообщение в карантине отклонено из-за квоты хранилища, сообщение будет потеряно. Exchange не будет создавать отчеты о недоставке для сообщений, помещенных в карантин, так как сообщения, отправленные на карантин, заключаются в отчеты о недоставке.

- **Настройка Outlook**. Необходимо настроить разрешения делегирования доступа Outlook в соответствии с потребностями вашей организации. Кроме того, вы можете настроить профиль Outlook для отображения исходного значения отправителя, получателя и SCL сообщения. Дополнительные сведения см . в разделе Настройка Outlook для отображения исходного отправителя в почтовом ящике карантина нежелательной почты.

Действие 3. Указание почтового ящика для карантина нежелательной почты

Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Функции защиты от вредоносных программ" в разделе Разрешения для защиты от вредоносных программ и защиты от вредоносных программ .

Используйте следующий синтаксис.

PowerShell

```
Set-ContentFilterConfig -QuarantineMailbox <SmtpAddress>
```

В этом примере все сообщения, превышающие пороговое значение карантина нежелательной почты, отправляются в spamQ@contoso.com.

PowerShell

```
Set-ContentFilterConfig -QuarantineMailbox spamQ@contoso.com
```

Как убедиться, что все получилось?

Чтобы убедиться, что вы успешно указали почтовый ящик карантина нежелательной почты, выполните следующую команду для проверки значения свойства **QuarantineMailbox**:

PowerShell

```
Get-ContentFilterConfig | Format-List QuarantineMailbox
```

Действие 4. Установка порогового значения вероятности нежелательной почты для перемещения в папку карантина

Порог вероятности нежелательной почты для карантина — это значение для перенаправления сообщения в почтовый ящик карантина нежелательной почты. Значение порога вероятности нежелательной почты для карантина задается в диапазоне от 0 до 9, где 0 указывает на крайне малую вероятность того, что сообщение будет спамом, а 9 указывает, что сообщение с большой долей вероятности является спамом.

Дополнительные сведения о настройке порогов вероятности нежелательной почты в соответствии с потребностями организации и об установке порогов вероятности нежелательной почты для каждого почтового ящика см. в разделах Использование командной консоли Exchange для настройки пороговых значений вероятности нежелательной почты для функции фильтрации содержимого и Использование командной консоли Exchange для настройки пороговых значений вероятности нежелательной почты для почтового ящика.

Действие 5. Управление почтовым ящиком карантина нежелательной почты

При управлении почтовым ящиком для карантина нежелательной почты необходимо следовать следующим рекомендациям.

- Повторно **отправьте это сообщение** в Outlook, чтобы освободить сообщения, помещенные в карантин, для предполагаемых получателей. Подробнее см. в разделе Освобождение сообщений из почтового ящика карантина нежелательной почты.

- Необходимо отслеживать размер почтового ящика карантина нежелательной почты. Объем сообщений электронной почты может изменяться из-за большого набора сотрудников, естественной тенденции увеличения размеров сообщений или порогового значения вероятности нежелательной почты для действия помещения в карантин.

- Необходимо отслеживать почтовый ящик для карантина нежелательной почты на случай ложных срабатываний. Если почтовый ящик карантина нежелательной почты содержит много сообщений в результате ложных срабатываний, увеличьте пороговое значение вероятности нежелательной почты для карантина. Дополнительные сведения об определении причины доставки сообщений в почтовый ящик для карантина нежелательной почты из-за ложных срабатываний см. в статье View antispam stamps in Outlook.

- Используйте один и тот же профиль Outlook для просмотра и освобождения сообщений, помещенных в карантин, из почтового ящика карантина нежелательной почты. Применение разрешений к другому профилю Outlook для выпуска сообщений не поддерживается.

> ⓘ **Важно!**
>
> Отчеты о недоставке для помещенных в карантин сообщений не доставляются в почтовый ящик карантина нежелательной почти. Отчеты о недоставке, определенные как спам, удаляются, даже если их оценка вероятности нежелательной почты указывает, что их следует поместить на карантин. Для отслеживания таких сообщений необходимо использовать журнал агента или журнал отслеживания сообщений. Дополнительные сведения см. в разделе **Ведение журналов агента антиспамов**.

Действие 6. Регулировка порога вероятности нежелательной почты для карантина

После установки порога вероятности нежелательной почты для карантина необходимо периодически проверять настройки и регулировать их в зависимости от потребностей организации. Например, если в почтовый ящик для карантина

нежелательной почты доставляется слишком много сообщений в результате ложных срабатываний, следует увеличить значение порога вероятности нежелательной почты для карантина. Дополнительные сведения о настройке порога вероятности нежелательной почты для карантина см. в статье Использование командной консоли Exchange для настройки пороговых значений вероятности нежелательной почты для функции фильтрации содержимого.

Настройка Outlook для отображения исходного отправителя в почтовом ящике карантина нежелательной почты

Статья • 04.04.2023

Карантин нежелательной почты — функция агента фильтрации содержимого, снижающая риск потери сообщений из надежных источников. Карантин нежелательной почты обеспечивает временное хранение сообщений, определенных как спам, которые не следует доставлять в почтовый ящик пользователя в организации. Дополнительные сведения см. в разделе Карантин спама в Exchange Server.

Когда сообщение соответствует заданному порогу карантина для нежелательной почты, оно включается в отчет о недоставке (который также называется NDR, уведомление о доставке, DSN или сообщение о недоставке) и доставляется на почтовый ящик карантина нежелательной почты. Поскольку сообщения, помещенные на карантин, хранятся как отчеты о недоставке, адрес администратора почты в организации будет указываться в поле адреса **From:** для всех сообщений. Тем не менее, наличие исходного адреса отправителя, исходного адреса получателя, а также исходной вероятности нежелательной почты в списке полей упрощает поиск сообщения, которое нужно восстановить.

По умолчанию эти поля нельзя добавить в представление сообщений в Microsoft Outlook. Необходимо создать форму Outlook, которая добавляет исходного отправителя, исходного получателя и исходную вероятность нежелательной почты как поля, которые можно выбрать. Создав эту настраиваемую форму, можно настроить Outlook таким образом, чтобы эти поля отображались при просмотре сообщения.

Что нужно знать перед началом работы

- Предполагаемое время выполнения процедуры: 15 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Доступ к почтовому ящику" в разделе Разрешения потока обработки почты .

- Для выполнения этой процедуры необходимо настроить почтовый ящик карантина. Дополнительные сведения см. в разделе Настройка почтового ящика карантина нежелательной почты.

- Необходимо настроить профиль Outlook, который используется для доступа к почтовому ящику карантина нежелательной почты. Дополнительные сведения о настройке и использовании нескольких профилей Outlook см. в статье Обзор профилей электронной почты Outlook.

  Для поиска свойств MAPI помещенного в карантин сообщения, в котором содержатся сведения об исходном отправителе, получателе и значения вероятности нежелательной почты, можно использовать служебные программы MAPI (такие как , OutlookSpy или MFCMAPI). Если вы считаете, что другие свойства MAPI обеспечивают лучшие результаты, чем те, которые указаны в этой статье, их можно использовать в настраиваемой форме Outlook.

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Шаг 1. Создание настраиваемой формы Outlook с помощью Блокнота

1. Откройте Блокнот и скопируйте следующий код в документ.

```text
[Description]
MessageClass=IPM.Note
CLSID={00020D31-0000-0000-C000-000000000046}
DisplayName=Quarantine Extension Form
Category=Standard
Subcategory=Form
Comment=This form allows the Original Sender
(ReceivedRepresentingEmailAddress), Original Recipient (To), and
Original SCL (OriginalScl) values to be viewed as columns.
LargeIcon=IPML.ico
SmallIcon=IPMS.ico
```

```
Version=3.0
Locale=enu
Hidden=1
Owner=Microsoft Corporation
Contact=Your Name
[Platforms]
Platform1=Win16
Platform2=NTx86
Platform9=Win95
[Platform.Win16]
CPU=ix86
OSVersion=Win3.1
[Platform.NTx86]
CPU=ix86
OSVersion=WinNT3.5
[Platform.Win95]
CPU=ix86
OSVersion=Win95
[Properties]
Property01=ReceivedRepresentingEmailAddress
Property02=DisplayTo
Property03=OriginalScl
[Property.ReceivedRepresentingEmailAddress]
Type=31
NmidInteger=0x0078
DisplayName=ReceivedRepresentingEmailAddress
[Property.DisplayTo]
Type=31
NmidInteger=0x0E04
DisplayName=DisplayTo
[Property.OriginalScl]
Type=3
NmidPropset={41F28F13-83F4-4114-A584-EEDB5A6B0BFF}
NmidString=OriginalScl
DisplayName=OriginalScl
[Verbs]
Verb1=1
[Verb.1]
DisplayName=&Open
Code=0
Flags=0
Attribs=2
[Extensions]
Extensions1=1
[Extension.1]
Type=31
NmidPropset={00020D0C-0000-0000-C000-000000000046}
NmidInteger=1
Value=1000000000000000
```

2. Сохраните файл в папке форм Office, используя следующие значения:

   - **Путь**: `<OfficeInstallPath>\<OfficeVersion>\Forms\<LCID>`

- **<OfficeInstallPath>**:
  - Для 32-разрядных версий Office в 32-разрядных версиях Microsoft Windows или 64-разрядных версий Office в 64-разрядных версиях Windows путь по умолчанию — `C:\Program Files\Microsoft Office\root`.
  - Для 32-разрядных версий Office в 64-разрядных версиях Windows путь по умолчанию — `C:\Program Files (x86)\Microsoft Office\root`.
- **<OfficeVersion>**
  - **Outlook 2010**: `Office14`
  - **Outlook 2013**: `Office15`
  - **Outlook 2016**:`Office16`
- **<LCID>**. Это значение идентификатора языкового стандарта (LCID). Например, LCID для английского языка — 1033. Дополнительные сведения см. в разделах Идентификаторы языка и Значения идентификаторов OptionState в Office.
- **Имя**. Для остальной части этой процедуры предполагается, что файл имеет имя `QTNE.cfg`. Имя файла не важно, но обязательно сохраните файл как QTNE.cfg, а не QTNE.cfg.txt.

Например, в случае с 32-разрядной английской версией Outlook 2016, установленной в 64-разрядной версии Windows, сохраните файл как:

```
"C:\Program Files (x86)\Microsoft Office\root\Office16\Forms\1033\QTNE.cfg"
```

> ⓘ **Примечание**
>
> Если система управления доступом пользователей Windows (UAC) не позволяет сохранить файл в нужное место, сначала сохраните его во временной папке, а затем и скопируйте.

Шаг 2. Настройка Outlook 2010 или более поздней версии для использования настраиваемой формы Outlook

1. Откройте почтовый ящик карантина нежелательной почты в Outlook на клиентском компьютере и нажмите кнопку**Параметры**>**файлов**>**Дополнительно**.

2. В разделе **Разработка** нажмите **Настраиваемые формы**.

3. В появившемся диалоговом окне **Параметры** нажмите кнопку **Управление формами**.

4. В появившемся диалоговом окне **Диспетчер форм** нажмите кнопку **Установить**. Перейдите к расположению `QTNE.cfg` файла, выберите его и нажмите кнопку **Открыть**. Просмотрите сведения в диалоговом окне **Свойства формы** и нажмите кнопку **ОК**, чтобы установить форму расширения карантина в библиотеке личных форм.

5. Вернитесь к диалоговому окну **Диспетчер форм**, нажмите кнопку **Закрыть**. Щелкните **ОК** дважды, чтобы закрыть остальные диалоговые окна, и вернитесь в основное окно Outlook.

6. В представлении **Почта** в папке "Входящие" щелкните **Вид**>**Добавить столбцы**.

7. В появившемся диалоговом окне **Показать столбцы** в раскрывающемся списке **Выбрать столбцы из** прокрутите до конца списка и выберите **Формы**.

8. В открывшемся диалоговом окне **Выбор форм для папки** в поле **Выбранные формы** выберите **Сообщение** и щелкните **Удалить**. В поле **Личные формы** выберите **Форма расширения карантина**, а затем нажмите **Добавить**. Когда закончите, нажмите кнопку **Закрыть**.

9. Вернитесь к диалоговому окну **Показать столбцы** в разделе **Доступные столбцы** выберите одно или несколько из следующих полей и щелкните **Добавить** после каждого выбранного поля.

    - **ReceivedRepresentingEmailAddress**: Исходный отправитель
    - **DisplayTo**: исходный получатель (обратите внимание, что после его добавления он отображается как **"К** ")
    - **OriginalScl**: Original SCL

    Используйте кнопки **Вверх** и **Вниз** для расположения столбцов в представлении. Для достижения наилучших результатов поместите новые поля после поля **Вложение** и до поля **От**. По завершении дважды нажмите кнопку **ОК** , чтобы вернуться к основному интерфейсу Outlook.

Как проверить, все ли получилось?

Вы узнаете, сработала ли эта процедура, если для сообщений в почтовом ящике карантина нежелательной почты при просмотре через Outlook отображаются сведения об исходном отправителе, исходном получателе, а также значения вероятности нежелательной почты.

Освобождение сообщений, помещенных в карантин, из почтового ящика карантина нежелательной почты в Exchange Server

Статья • 04.04.2023

После настройки почтового ящика карантина нежелательной почты в Exchange Server вы можете повторно **отправить это сообщение** в Microsoft Outlook, чтобы освободить сообщения в карантине для предполагаемых получателей. Сведения о настройке почтового ящика карантина нежелательной почты см. в статье Настройка почтового ящика карантина нежелательной почты.

Что нужно знать перед началом работы

- Предполагаемое время выполнения процедуры: менее 5 минут.
- **Повторно отправить это сообщение** недоступно в Outlook в Интернете. Необходимо настроить профиль Outlook, который используется для доступа к почтовому ящику карантина нежелательной почты. Дополнительные сведения о настройке и использовании нескольких профилей Outlook см. в статье Обзор профилей электронной почты Outlook.
- Чтобы упростить поиск сообщения, которое требуется восстановить, можно создать настраиваемую форму Outlook для отображения исходных отправителей и получателей в представлении сообщения. Подробные инструкции см . в разделе Настройка Outlook для отображения исходного отправителя в почтовом ящике карантина нежелательной почты.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Доступ к почтовому ящику" в разделе Разрешения потока обработки почты .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Освобождение сообщения из почтового ящика карантина нежелательной почты с помощью Outlook 2010 или более поздней версии

1. Откройте почтовый ящик карантина нежелательной почты с помощью Outlook на клиентском компьютере.
2. В представлении **Почта** найдите сообщение, которое нужно восстановить, в папке **Входящие**, а затем дважды щелкните его, чтобы открыть.
3. В разделе **Перемещение** ленты щелкните **Действия**>**Повторно отправить это сообщение**.
4. При открытии сообщения щелкните **Отправить**, чтобы повторно отправить сообщение получателю.

Примечание. **Повторно отправить это сообщение** не работает с несколькими сообщениями. Их потребуется отправить по отдельности.

Как проверить, что все получилось?

Чтобы убедиться, что вы успешно извлекли сообщение из почтового ящика карантина нежелательной почты, обратитесь к получателю и проверьте, получил ли он сообщение.

Пороговые значения уровня достоверности нежелательной почты Exchange (SCL)

Статья • 04.04.2023

> **Примечание**
>
> В ноябре 2016 г. корпорация Майкрософт прекратила выпуск обновлений определений спама для фильтров SmartScreen в Exchange и Outlook. Существующие определения спама SmartScreen остались на месте, но их эффективность, скорее всего, со временем снизится. Дополнительные сведения см. в статье **Прекращение поддержки SmartScreen в Outlook и Exchange**.

В Exchange Server можно определить конкретные действия для сообщений в соответствии с порогами уровня достоверности спама (SCL). Например, на сервере Exchange, на котором запущен агент фильтра содержимого, можно определить разные пороговые значения для отклонения, удаления и помещения сообщений на карантин. Эти значения и действия практически не изменились по сравнению с Exchange Server 2010

Агент фильтра содержимого присваивает сообщениям оценку вероятности нежелательной почты после того, как другие агенты защиты от спама обработали входящие сообщения. Многие агенты защиты от спама, которые обрабатывают входящие сообщения до агента фильтра содержимого, выполняют с сообщением конкретный набор действий. Например, агент фильтра подключений на пограничном транспортном сервере отклоняет сообщения с IP-адресов на основе списка блокировок реального времени. Агент фильтра отправителей блокирует сообщения на основе списка заблокированных отправителей, а агент фильтра получателей — на основе списка заблокированных получателей. В процессе обработки сообщений другие агенты защиты от спама значительно уменьшают количество сообщений (в большинстве случаев совершенно нежелательных сообщений), которые должен обработать агент фильтра содержимого. Дополнительные сведения о порядке обработки сообщений агентами антиспамов см. в разделе Защита от спама в Exchange Server.

Так как фильтрация содержимого — не точная наука, очень важно иметь возможность настроить действия агента с учетом различных значений вероятности

нежелательной почты. Тщательно отслеживая и настраивая пороговые значения вероятности нежелательной почты, вы можете уменьшить:

- размер почтового ящика карантина нежелательной почты и количество сообщений в нем;
- количество сообщений электронной почты, которые по ошибке помещаются на карантин или в папку нежелательной почты пользователя (ложные срабатывания);
- количество нежелательных сообщений оскорбительного характера, которые попадают в почтовый ящик пользователя (сообщений, которые не должны были попасть даже в папку нежелательной почты);
- количество нежелательных сообщений, которые попадают в папку "Входящие" пользователя.

Пороговые значения вероятности нежелательной почты в агенте фильтра содержимого и пороговое значение для доставки в папку нежелательной почты для почтового ящика пользователя позволяют реализовать более комплексную и точную стратегию защиты от спама и снизить общую стоимость развертывания и обслуживания решения для защиты от спама в организации Exchange.

Действия для пороговых значений вероятности нежелательной почты

Настраивая действия для пороговых значений вероятности нежелательной почты, вы можете ужесточить фильтрацию содержимого для сообщений, которые с большей вероятностью являются спамом. Для работы с этой функцией полезно понимать различные действия для пороговых значений вероятности нежелательной почты и то, как они реализуются.

- **Пороговое значение удаления SCL**. Если значение SCL сообщения больше или равно пороговой величине удаления SCL, агент фильтра содержимого автоматически удаляет сообщение. Данные об удалении сообщения не передаются на уровне протокола на исходный сервер обмена сообщениями или отправителю. Если значение вероятности нежелательной почты сообщения меньше порогового значения вероятности нежелательной почты для удаления, агент фильтра содержимого сравнивает значение вероятности нежелательной почты и пороговое значение вероятности нежелательной почты для отклонения.

- **Пороговое значение отклонения SCL**. Если значение SCL сообщения больше или равно пороговой величине отклонения SCL, но меньше порогового значения удаления SCL, агент фильтра содержимого отклоняет сообщение и отправляет ответ на отклонение в отправляющий систему. Ответ об отклонении можно настраивать. В некоторых случаях исходному отправителю сообщения отправляется отчет о недоставке. Если значение вероятности нежелательной почты сообщения меньше порогового значения вероятности нежелательной почты для отклонения, агент фильтра содержимого сравнивает его и пороговое значение для помещения на карантин.

- **Пороговое значение карантина SCL**. Если значение SCL сообщения больше или равно пороговой отметке карантина SCL, но меньше порогового значения отклонения SCL, агент фильтра содержимого отправляет сообщение в почтовый ящик карантина нежелательной почты. Дополнительные сведения о настройке почтового ящика карантина спама см. в разделе Настройка почтового ящика карантина нежелательной почты.

  Администраторы должны периодически проверять, не слишком ли много очевидного спама помещено на карантин без необходимости (слишком высокое пороговое значение вероятности нежелательной почты для помещения на карантин) и не слишком ли много обычных сообщений помещено на карантин (слишком низкое пороговое значение вероятности нежелательной почты для помещения на карантин). Сведения о том, как просмотреть результаты проверок сообщений, помещенных на карантин, на спам, см. в статье View antispam stamps in Outlook.

  Если значение вероятности нежелательной почты сообщения меньше порогового значения вероятности нежелательной почты для помещения на карантин, сообщение доставляется на соответствующий сервер почтовых ящиков, где оценивается пороговое значение вероятности нежелательной почты для доставки в папку нежелательной почты организации или почтового ящика.

- **Пороговое значение папки нежелательной Email SCL**. Если значение SCL сообщения превышает пороговое значение нежелательной Email папки SCL, настроенное для организации или почтового ящика, сообщение доставляется в папку "Нежелательная Email". Если значение вероятности нежелательной почты сообщения равно или меньше порогового значения для доставки в папку нежелательной почты, сообщение доставляется в папку "Входящие".

  В отличие от других пороговых значений вероятности нежелательной почты, которые контролируются агентом фильтра содержимого, пороговое значение

вероятности нежелательной почты для доставки в папку нежелательной почты, контролируется правилом нежелательной почты (скрытое правило папки "Входящие"), включенным по умолчанию в каждом почтовом ящике. Агент фильтра содержимого присваивает значение вероятности нежелательной почты сообщению, но за доставку сообщения в папку нежелательной почты отвечает правило нежелательной почты. Дополнительные сведения см. в разделе, посвященном включению и отключению правила нежелательной почты в почтовом ящике с помощью командной консоли Exchange.

Агент фильтра содержимого и папка нежелательной почты обрабатывают значение порога вероятности нежелательной почты по-разному. Агент фильтра содержимого использует значение больше или равно для порогового значения SCL, а папка "Нежелательная Email" использует больше. Например, если настроить агент фильтра содержимого с пороговым значением удаления SCL 8, все сообщения с SCL 8 или выше удаляются автоматически. Однако при настройке папки "Нежелательная Email" с пороговым значением SCL 4 все сообщения с SCL 5 или выше перемещаются в папку "Нежелательная Email", а сообщения с SCL 4 или ниже доставляются в папку "Входящие".

Область действия пороговых значений вероятности нежелательной почты

Вы можете настроить пороговые значения вероятности нежелательной почты в следующих расположениях:

- **Конфигурация сервера**. Пороговые значения SCL для удаления, отклонения и карантина в агенте фильтра содержимого.
- **Конфигурация организации**: нежелательной почты SCL Email пороговое значение папки в организации Exchange.
- **Конфигурация почтового ящика**. Пороговые значения SCL для определенных почтовых ящиков.

Пороговые значения вероятности нежелательной почты для агента фильтра содержимого

Пороговые значения вероятности нежелательной почты для удаления, отклонения и помещения на карантин на пограничном транспортном сервере или сервере почтовых ящиков, на котором запущен агент фильтра содержимого, настраиваются

с помощью командлета **Set-ContentFilterConfig**. Со временем, проанализировав функции спама и показатели журналов и отчетов, вы сможете дополнительно настроить эти пороговые значения вероятности нежелательной почты.

Параметры пороговых значений вероятности нежелательной почты, доступные для командлета **Set-ContentFilterConfig**, приведены в таблице ниже.

Параметр	**Описание**
SCLDeleteEnabled	Включает и отключает пороговое значение удаления SCL. Допустимые значения: `$true` или `$false`. Значение по умолчанию — `$false`, что означает, что пороговое значение удаления SCL не включено по умолчанию. Пороговое значение удаления SCL задается с помощью параметра *SCLDeleteThreshold* .
SCLDeleteThreshold	Пороговое значение вероятности нежелательной почты для удаления. Сообщение, значение вероятности нежелательной почты которого больше или равно этому значению, автоматически удаляется. Максимальное значение равно 9, это также значение по умолчанию. Пороговое значение вероятности нежелательной почты для удаления должно быть больше всех других пороговых значений вероятности нежелательной почты.
SCLRejectEnabled	Включает и отключает пороговое значение отклонения SCL. Допустимые значения: `$true` или `$false`. Значение по умолчанию — `$true`, что означает, что пороговое значение отклонения SCL включено по умолчанию. Пороговое значение отклонения SCL задается с помощью параметра *SCLRejectThreshold* .
SCLRejectThreshold	Пороговое значение вероятности нежелательной почты для отклонения. Сообщение, значение вероятности нежелательной почты которого больше или равно этому значению, отклоняется, а отправителю отсылается отчет о недоставке. Максимальное значение равно 9, а значение по умолчанию равно 7. Пороговое значение вероятности нежелательной почты для отклонения должно быть меньше порогового значения вероятности нежелательной почты для удаления, но больше пороговых значений для помещения на карантин или доставки в папку нежелательной почты.

Параметр	Описание
SCLQuarantineEnabled	Включает и отключает пороговое значение карантина SCL. Допустимые значения: `$true` или `$false`. Значение по умолчанию — `$false`, что означает, что пороговое значение карантина SCL не включено по умолчанию. Пороговое значение карантина SCL задается с помощью параметра *SCLQuarantineThreshold* . Дополнительные сведения о настройке почтового ящика карантина нежелательной почты, необходимого для помещения сообщений на карантин, см. в статье Настройка почтового ящика карантина нежелательной почты.
SCLQuarantineThreshold	Пороговое значение вероятности нежелательной почты для помещения на карантин. Сообщение, значение вероятности нежелательной почты которого больше или равно этому значению, перенаправляется в почтовый ящик карантина нежелательной почты. Максимальное значение равно 9, это также значение по умолчанию. Пороговое значения вероятности нежелательной почты для помещения на карантин должно быть меньше порогового значения вероятности нежелательной почты для отклонения, но больше порогового значения вероятности нежелательной почты для доставки в папку нежелательной почты (параметр *SCLJunkThreshold* командлета **Set-OrganizationConfig** или **Set-Mailbox**).

Примеры настройки пороговых значений вероятности нежелательной почты для агента фильтра содержимого см. в разделе, посвященном настройке пороговых значений вероятности нежелательной почты для фильтра содержимого с помощью командной консоли Exchange.

Пороговые значения вероятности нежелательной почты для организации

Пороговое значение вероятности нежелательной почты для доставки в папку нежелательной почты для всех почтовых ящиков в организации устанавливается с помощью параметра *SCLJunkThreshold* командлета **Set-OrganizationConfig**. Это единственное пороговое значение вероятности нежелательной почты, которое можно настроить на уровне организации. Значение вероятности нежелательной почты обычно присваивается сообщениям агентом фильтра содержимого.

Параметр *SCLJunkThreshold* командлета **Set-OrganizationConfig** описан в таблице ниже.

Параметр	Описание
SCLJunkThreshold	Значение вероятности нежелательной почты, которое используется, когда правило нежелательной почты включено в почтовом ящике, а пороговое значение вероятности нежелательной почты для доставки в папку нежелательной почты не настроено. Сообщение со значением SCL, превышающим это значение, перемещается в папку "Нежелательная Email" правилом нежелательной почты. Максимальное значение — 9, а значение по умолчанию — 4. Это означает, что сообщения со значением SCL 5 или выше перемещаются в папку "Нежелательная Email", а сообщения со значением SCL 4 или ниже доставляются в папку "Входящие".

Примечания.

- Пороговое значение для доставки в папку нежелательной почты включено по умолчанию, так как правило нежелательной почты включено по умолчанию во всех почтовых ящиках. Если правило нежелательной почты отключено в почтовом ящике, пороговое значение вероятности нежелательной почты для доставки в папку нежелательной почты (для организации или почтового ящика) отключено для почтового ящика.

- Вы можете отключить правило нежелательной почты в почтовом ящике с помощью параметра *Enabled***командлета Set-MailboxJunkEmailConfiguration**, но только после открытия почтового ящика в Outlook (в режиме кэширования Exchange) или Outlook в Интернете.

- Вы можете контролировать доступность параметров нежелательной почты в Outlook в Интернете, чтобы пользователи не могли включать или отключать правила нежелательной почты в своих почтовых ящиках.

Дополнительные сведения см. в статье Configure Exchange antispam settings on mailboxes.

Пороговые значения вероятности нежелательной почты для почтового ящика

Вы можете настроить все пороговые значения SCL для почтового ящика с помощью командлета **Set-Mailbox**. Параметры вероятности нежелательной почты, доступные для командлета **Set-ContentFilterConfig**, также доступны для командлета **Set-Mailbox**:

- *SCLDeleteEnabled*

- *SCLDeleteThreshold*
- *SCLRejectEnabled*
- *SCLRejectThreshold*
- *SCLQuarantineEnabled*
- *SCLQuarantineThreshold*

В отличие от пороговых параметров SCL в **Set-ContentFilterConfig**, параметры командлета **Set-Mailbox** также принимают значение `$null` (значение пусто), которое является значением по умолчанию для всех пороговых значений SCL в почтовом ящике. Это пустое значение по умолчанию указывает, что для почтового ящика не настроены пороговые значения вероятности нежелательной почты, поэтому агент фильтра содержимого использует свои параметры порогового значения вероятности нежелательной почты для сообщений, отправляемых в почтовый ящик.

Если для почтового ящика настроить пороговое значение вероятности нежелательной почты, параметр переопределит соответствующее пороговое значение вероятности нежелательной почты агента фильтра содержимого для сообщений, отправляемых в почтовый ящик. Пороговые значения вероятности нежелательной почты, настроенные для почтового ящика, хранятся в Active Directory и реплицируются на подписанные пограничные транспортные серверы службой Microsoft Exchange EdgeSync.

Результаты аналогичны для параметра *SCLJunkThreshold*, доступного в **Set-OrganizationConfig** и **Set-Mailbox**: значение порога нежелательной Email папки SCL, настроенное в почтовом ящике (значение не пустое), переопределяет значение SCL в организации для сообщений, отправляемых в почтовый ящик.

> ⓘ **Примечание**
>
> Пороговые значения вероятности нежелательной почты для почтового ящика не применяются для сообщений от групп рассылки.

Параметр порогового значения вероятности нежелательной почты, уникальной для почтового ящика, позволяет включить или отключить пороговое значение вероятности нежелательной почты для доставки в папку нежелательной почты. Параметр *SCLJunkEnabled* доступен только для командлета **Set-Mailbox** и описан в таблице ниже.

Параметр	Описание
SCLJunkEnabled	Включает и отключает пороговое значение папки нежелательной Email SCL в почтовом ящике. Допустимые значения: `$true`, `$false` или `$null` (пустая). Значение по умолчанию пустое (`$null`), что означает, что пороговое значение нежелательной Email папки SCL не настроено в почтовом ящике и управляется тем, включено или отключено правило нежелательной почты в почтовом ящике. Пороговое значение нежелательной Email папки SCL по умолчанию устанавливается параметром *SCLJunkThreshold* командлета **Set-OrganizationConfig**. Это значение для почтового ящика можно переопределить с помощью параметра *SCLJunkThreshold* в командлете **Set-Mailbox** .

Примечания.

- Вы можете отключить пороговое значение вероятности нежелательной почты для доставки в папку нежелательной почты для почтового ящика, отключив правило нежелательной почты в почтовом ящике. Однако в этом случае правило также не сможет использовать список надежных отправителей, список надежных получателей и список заблокированных отправителей для перемещения сообщений в папку нежелательной почты или папку "Входящие".

- Даже если правило нежелательной почты и пороговое значение вероятности нежелательной почты для доставки в папку нежелательной папки для почтового ящика отключены, фильтр нежелательной почты Outlook на стороне клиента по-прежнему может перемещать сообщения в папку нежелательной почты.

Дополнительные сведения см. в статье Configure Exchange antispam settings on mailboxes.

Мониторинг пороговых значений вероятности нежелательной почты

Для сбора результирующих данных фильтрации можно использовать несколько встроенных скриптов, расположенных в `%ExchangeInstallPath%Scripts` папке, например **Get-AntispamSCLHistogram.ps1**. Если данные показывают, что необходимы немедленные изменения, отрегулируйте пороговые значения вероятности нежелательной почты. Или соберите данные и проанализируйте отчеты о спаме, чтобы определить, нужны ли изменения.

Фильтрация отправителей в Exchange Server

Статья • 04.04.2023

Функция фильтрации отправителей сравнивает список заблокированных отправителей, который ведет администратор Exchange, со значением команды **MAIL FROM** в подключениях SMTP, чтобы определить, что следует делать с входящими сообщениями от этих отправителей. Фильтрация отправителей в Exchange Server предоставляется агентом фильтра отправителей и практически не изменяется с Exchange Server 2010 г.

Агент фильтра отправителей может блокировать отдельных отправителей (например, kim@contoso.com), целые домены (contoso.com) или домены и все поддомены (*.contoso.com). Вы можете указать, сообщения из каких источников должен проверять агент — внутренних, внешних или обоих. Вы также можете настроить действие для сообщений от заблокированных отправителей:

- **Отклонить**. Агент фильтра отправителей отклоняет SMTP-запрос с ошибкой сеанса `554 5.1.0 Sender Denied` SMTP и закрывает подключение.

- **Состояние метки**. Агент фильтра отправителей принимает сообщение и обновляет сообщение, указывая, что оно поступило от заблокированного отправителя. Эта информация используется агентом фильтрации содержимого при вычислении вероятности нежелательной почты (SCL) для сообщения. Дополнительные сведения о фильтрации содержимого и агенте фильтра содержимого см. в разделе Фильтрация содержимого.

По умолчанию агент фильтрации отправителей включен на пограничных транспортных серверах, но его также можно включить на серверах почтовых ящиков. Дополнительные сведения см. в разделе Включение функций защиты от нежелательной почты на серверах почтовых ящиков.

Дополнительные сведения о настройке агента фильтра отправителей см. в разделе Процедуры фильтрации отправителей.

> ⓘ **Важно!**
>
> SMTP-заголовки **MAIL FROM:** можно подделать, поэтому агент фильтрации отправителей следует использовать вместе с агентом Sender ID. Агент Sender ID использует исходный IP-адрес сервера отправителя, чтобы убедиться, что домен, указанный в SMTP-заголовке MAIL FROM:, соответствует

зарегистрированному домену. Дополнительные сведения об агенте Sender ID см. Дополнительные сведения об агенте идентификатора отправителя см. в разделе **Идентификатор отправителя**.

Использование агента фильтра отправителей для блокировки сообщений

По умолчанию агент фильтрации отправителей проверяет только сообщения из внешних источников. *Внешние источники* — это источники, не прошедшие проверку подлинности. Вы можете настроить агент фильтрации отправителей так, чтобы он проверял сообщения из внутренних (прошедших проверку подлинности) источников. Однако обычно не рекомендуется применять фильтры защиты от спама к сообщениям от надежных партнеров или внутренним сообщениям.

Вы также можете настроить агент фильтрации отправителей так, чтобы он блокировал входящие сообщения, в которых в SMTP-команде **MAIL FROM** не указан отправитель и имя домена. Этот параметр помогает предотвратить атаки NDR на сервер Exchange. Большинство обыкновенных SMTP-сообщений приходит с SMTP-серверов, которые предоставляют сведения об отправителе и домене в команде SMTP **MAIL FROM**.

Определение действия для сообщений от заблокированных отправителей

После того как вы настроили заблокированных отправителей и источники, отслеживаемые агентом фильтрации отправителей, необходимо указать, что следует делать с сообщениями от этих отправителей — отклонять или принимать и помечать. Рекомендуем отклонять сообщения, так как вероятность ложных срабатываний на основе указанного списка заблокированных отправителей гораздо ниже, чем на основе других вычисляемых свойств сообщения.

Обыкновенное сообщение может быть отклонено агентом фильтрации отправителей только в двух сценариях:

- Вы неправильно указали заблокированного отправителя.
- Домен в вашем списке заблокированных отправителей позднее повторно зарегистрирован как надежная компания.

Процедуры фильтрации отправителей

Статья • 04.04.2023

Функция фильтрации отправителей обрабатывает входящие сообщения, сравнивая список заблокированных отправителей со значением команды **MAIL FROM** в SMTP-подключениях. Дополнительные сведения о фильтрации отправителей и агенте фильтра отправителей см. в разделе Фильтрация отправителей.

Ряд аспектов фильтрации отправителей можно настроить. Например:

- Включить или отключить фильтрацию отправителей для сообщений из внутренних (прошедших проверку подлинности) и внешних (не прошедших проверку подлинности) источников (по умолчанию она включена для сообщений из внешних источников).
- Настроить заблокированных отправителей и заблокированные домены.
- Указать, следует ли блокировать сообщения с пустым полем отправителя.
- Настроить действия для сообщений, содержащих заблокированных отправителей или домены.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Функции защиты от вредоносных программ" в разделе Разрешения для защиты от вредоносных программ и защиты от вредоносных программ .
- Для выполнения этой процедуры можно использовать только PowerShell. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- По умолчанию в службе транспорта на сервере почтовых ящиков не включены функции защиты от нежелательной почты. Как правило, их следует включать, только если организация Exchange не выполняет никакую предварительную фильтрацию нежелательной почты до приема входящих сообщений. Дополнительные сведения см. в разделе Включение функций защиты от нежелательной почты на серверах почтовых ящиков.

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Включение или отключение фильтрации отправителей с помощью командной консоли Exchange

Чтобы отключить фильтрацию отправителей, выполните следующую команду:

PowerShell

```
Set-SenderFilterConfig -Enabled $false
```

Чтобы включить фильтрацию отправителей, выполните следующую команду:

PowerShell

```
Set-SenderFilterConfig -Enabled $true
```

> **Примечание**
>
> Когда фильтрация отправителей отключена, базовый агент фильтрации отправителей остается включенным. Чтобы отключить агент фильтра отправителей, выполните команду : `Disable-TransportAgent "Sender Filter Agent"`.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно включили или отключили фильтрацию отправителей, выполните следующую команду, чтобы проверить значение свойства **Enabled**:

```
```

PowerShell

```
Get-SenderFilterConfig | Format-List Enabled
```

Включение или отключение фильтрации отправителей для внешних подключений с помощью командной консоли Exchange

По умолчанию фильтрация отправителей включена для внешних (без проверки подлинности) SMTP-подключений.

Чтобы отключить фильтрацию отправителей для внешних подключений, выполните следующую команду:

PowerShell

```
Set-SenderFilterConfig -ExternalMailEnabled $false
```

Чтобы включить фильтрацию отправителей для внешних подключений, выполните следующую команду:

PowerShell

```
Set-SenderFilterConfig -ExternalMailEnabled $true
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно включили или отключили фильтрацию отправителей для внешних SMTP-подключений, выполните следующую команду, чтобы проверить значение свойства **ExternalMailEnabled**:

PowerShell

```
Get-SenderFilterConfig | Format-List ExternalMailEnabled
```

Включение или отключение фильтрации отправителей для внутренних подключений с помощью командной консоли Exchange

Не рекомендуем применять фильтры защиты от спама к сообщениям от надежных партнеров или внутренним сообщениям. Чтобы избежать неправильной обработки обыкновенных сообщений, настройте запуск агентов защиты от спама только для сообщений из внешних источников.

Чтобы включить фильтрацию отправителей для внутренних (прошедших проверку подлинности) SMTP-подключений, выполните следующую команду:

PowerShell

```
Set-SenderFilterConfig -InternalMailEnabled $true
```

Чтобы отключить фильтрацию отправителей для внутренних подключений, выполните следующую команду:

PowerShell

```
Set-SenderFilterConfig -InternalMailEnabled $false
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно включили или отключили фильтрацию отправителей для внутренних SMTP-подключений, выполните следующую команду, чтобы проверить значение свойства **InternalMailEnabled**:

PowerShell

```
Get-SenderFilterConfig | Format-List InternalMailEnabled
```

Использование командной консоли Exchange для настройки заблокированных отправителей и доменов для фильтрации отправителей

Вы можете указать заблокированных отправителей и домены, которые заменят существующие значения, либо добавить или удалить заблокированных отправителей и домены, не изменяя другие существующие значения.

Чтобы заменить существующие значения, используйте следующий синтаксис:

```
```

PowerShell

```
Set-SenderFilterConfig -BlockedSenders <sender1,sender2...> -BlockedDomains
<domain1,domain2...> -BlockedDomainsAndSubdomains <domain1,domain2...>
```

В этом примере агент фильтра отправителей настраивает для блокировки сообщений из kim@contoso.com и john@contoso.com, сообщений из домена fabrikam.com и сообщений из northwindtraders.com и всех его поддоменов.

PowerShell

```
Set-SenderFilterConfig -BlockedSenders kim@contoso.com,john@contoso.com -
BlockedDomains fabrikam.com -BlockedDomainsAndSubdomains
northwindtraders.com
```

Чтобы добавить или удалить записи, не изменяя другие существующие значения, используйте следующий синтаксис:

PowerShell

```
Set-SenderFilterConfig -BlockedSenders @{Add="<sender1>","<sender2>"...;
Remove="<sender1>","<sender2>"...} -BlockedDomains @{Add="<domain1>","
<domain2>"...; Remove="<domain1>","<domain2>"...} -
BlockedDomainsAndSubdomains @{Add="<domain1>","<domain2>"...; Remove="
<domain1>","<domain2>"...}
```

В данном примере представлена настройка агента фильтрации отправителей, при которой указываются следующие сведения.

- Добавьте chris@contoso.com и michelle@contoso.com в список существующих отправителей, которые заблокированы.
- Удалите tailspintoys.com из списка существующих заблокированных доменов отправителей.
- Добавьте blueyonderairlines.com в список существующих заблокированных доменов и поддоменов отправителей.

PowerShell

```
Set-SenderFilterConfig -BlockedSenders
@{Add="chris@contoso.com","michelle@contoso.com"} -BlockedDomains
@{Remove="tailspintoys.com"} -BlockedDomainsAndSubdomains
@{Add="blueyonderairlines.com"}
```

Как проверить, что все получилось?

Чтобы убедиться, что вы успешно настроили заблокированных отправителей, выполните следующую команду, чтобы проверить значения свойств:

```
PowerShell

Get-SenderFilterConfig | Format-List Blocked*
```

Использование командной консоли Exchange для настройки фильтрации отправителей для блокировки сообщений с пустыми отправителями

Чтобы включить или отключить блокировку сообщений, в которых не указан отправитель, используйте следующий синтаксис:

```
PowerShell

Set-SenderFilterConfig -BlankSenderBlockingenabled <$true | $false>
```

В этом примере агент фильтрации отправителей настраивается на блокировку сообщений, в которых не указан отправитель в SMTP-команде **MAIL FROM:**:

```
PowerShell

Set-SenderFilterConfig -BlankSenderBlockingEnabled $true
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно включили или отключили блокирующие сообщения с пустыми отправителями, выполните следующую команду, чтобы проверить значение свойства:

```
PowerShell

Get-SenderFilterConfig | Format-List BlankSenderBlockingEnabled
```

Настройка действия фильтрации отправителей с помощью командной консоли Exchange

Обычно сообщения от заблокированных отправителей или доменов отклоняют; это действие по умолчанию. Однако функция фильтрации отправителей может пропускать эти сообщения в вашу организацию для дальнейшего анализа другими агентами защиты от спама.

Чтобы настроить действие для сообщений от заблокированных отправителей или доменов, используйте следующий синтаксис:

PowerShell

```
Set-SenderFilterConfig -Action <Reject | StampStatus>
```

В этом примере агент фильтрации отправителей настраивается на получение сообщений от заблокированных отправителей или доменов. Агент фильтрации отправителей обновляет сообщение, чтобы указать, что оно пришло от заблокированного отправителя. Эти данные используются при вычислении вероятности нежелательной почты (SCL) для сообщения.

PowerShell

```
Set-SenderFilterConfig -Action StampStatus
```

В этом примере агент фильтрации отправителей настраивается на отклонение сообщений от заблокированных отправителей или доменов. Агент фильтра отправителей отклоняет SMTP-запрос с ошибкой сеанса `554 5.1.0 Sender Denied` SMTP и закрывает подключение.

PowerShell

```
Set-SenderFilterConfig -Action Reject
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно настроили действие для фильтрации отправителей, выполните следующую команду, чтобы проверить значение свойства **Action**:

PowerShell

```
Get-SenderFilterConfig | Format-List Action
```

Использование командной консоли Exchange для настройки действия фильтрации отправителей для заблокированных отправителей из агрегирования SafeList

Агрегат SafeList добавляет заблокированных отправителей, определенных пользователями в Microsoft Outlook или Outlook в Интернете, в список Заблокированные отправители, используемый агентом фильтра отправителей. Дополнительные сведения см. в разделе Объединение списков надежных отправителей.

Чтобы настроить действие, выполняемое фильтрацией отправителей для сообщений, содержащих заблокированных отправителей, определенных агрегатом SafeList, используйте следующий синтаксис:

PowerShell

```
Set-SenderFilterConfig -RecipientBlockedSenderAction <Delete | Reject>
```

В этом примере агент фильтра отправителей настраивает автоматическое удаление сообщений, содержащих заблокированных отправителей, определенных агрегатом SafeList.

PowerShell

```
Set-SenderFilterConfig -RecipientBlockedSenderAction Delete
```

В этом примере агент фильтра отправителей настраивает на отклонение сообщений, содержащих заблокированных отправителей, определенных агрегатом SafeList с отчетом о недоставке (также известное как недоставка, уведомление о состоянии доставки, DSN или сообщение о отказе).

PowerShell

```
Set-SenderFilterConfig -RecipientBlockedSenderAction Reject
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно настроили действие для фильтрации заблокированных отправителей из объединения списков надежных отправителей, выполните следующую команду, чтобы проверить значение свойства **RecipientBlockedSenderAction**:

PowerShell

```
Get-SenderFilterConfig | Format-List RecipientBlockedSenderAction
```

Идентификатор отправителя в Exchange Server

Статья • 04.04.2023

Для обнаружения *спуфинга* используется технология Sender ID. Спуфинг — это подделка адреса отправителя сообщения. Раньше было довольно просто отправлять поддельные электронные сообщения, так как адрес отправителя в заголовке сообщения не проверялся. Технология Sender ID определяет, не подделан ли адрес отправителя, используя заголовок SMTP **RECEIVED** и запрос записей DNS для домена отправителя. Идентификатор отправителя в Exchange Server предоставляется агентом идентификатора отправителя и практически не изменяется с Exchange Server 2010 года.

По умолчанию агент Sender ID включен на пограничных транспортных серверах, но его также можно включить на серверах почтовых ящиков. Дополнительные сведения см. в разделе Включение функций защиты от нежелательной почты на серверах почтовых ящиков.

Дополнительные сведения о настройке агента идентификатора отправителя см. в разделе Процедуры идентификатора отправителя.

Использование кода отправителя для противодействия спуфингу

Когда сервер Exchange получает входящее сообщение, агент Sender ID проверяет IP-адрес отправителя, запрашивая записи DNS для домена отправителя. Такая проверка подтверждает, что сообщение получено с IP-адреса, авторизованного для этого домена отправителя. IP-адрес авторизованного сервера-отправителя известен как *адрес PRA*.

Администраторы публикуют записи инфраструктуры политики отправителей (SPF) в системе DNS, которые определяют авторизованные серверы исходящих сообщений для домена. Если запись SPF доступна в системе DNS для домена отправителя, агент Sender ID анализирует эту запись, чтобы определить, разрешено ли отправлять электронную почту с исходного IP-адреса для домена, указанного в адресе электронной почты отправителя. Дополнительные сведения о том, что содержит запись SPF и как создать запись SPF, см. в разделе Платформа политики отправителей: синтаксис записи SPF.

Значения состояния кода отправителя

Агент Sender ID генерирует состояние Sender ID для сообщения. Состояние Sender ID может иметь следующие значения:

- **Пройти**. IP-адрес и PRA прошли проверку проверки идентификатора отправителя.
- **Нейтральный**. Опубликованные данные идентификатора отправителя явно неубедительна.
- **Обратимый сбой**. IP-адрес для PRA может находиться в недопустимом наборе.
- **Сбой**: IP-адрес запрещен. Адрес PRA не найден во входящем сообщении или домен отправителя не существует.
- **Нет**. В DNS для домена отправителя не существует опубликованных данных SPF.
- **TempError**: произошел временный сбой DNS, например недоступный DNS-сервер.
- **PermError**: недопустимая запись DNS, например ошибка в формате записи.

Примечание. Если исходный IP-адрес отсутствует, невозможно задать состояние идентификатора отправителя. Exchange продолжает обрабатывать сообщение без учета состояния идентификатора отправителя, и сообщение не возвращается или отклоняется. В этом случае состояние Sender ID не определяется, а событие регистрируется в журнале приложения.

Состояние Sender ID добавляется к метаданным сообщения, а затем преобразуется в свойство MAPI. Фильтр нежелательной почты в Outlook использует свойство MAPI во время вычисления вероятности нежелательной почты (SCL).

Outlook не отображает состояние Sender ID и не помечает сообщение как нежелательное на основе лишь значения Sender ID. Вместо этого Outlook использует значение состояния Sender ID только при вычислении вероятности нежелательной почты для сообщения.

Дополнительные сведения о том, как состояние идентификатора отправителя отображается в сообщениях, см. в разделе Метки защиты от спама.

Параметры кода отправителя для обработки поддельной почты и недостижимых серверов DNS

Вы можете настроить действия, которые будут выполняться, когда агент идентификатора отправителя идентифицирует сообщения, содержащие поддельные отправителя (состояние идентификатора отправителя — `Fail`), и когда dns-сервер не может быть достигнут (состояние идентификатора отправителя — `TempError`):

- **Состояние метки**. Агент идентификатора отправителя метит состояние идентификатора отправителя в метаданных сообщения и позволяет продолжить доставку сообщения. Этот параметр установлен по умолчанию.
- **Отклонить**. Агент идентификатора отправителя отклоняет сообщение с сообщением об ошибке SMTP уровня 5 *XX* , который включает текст, соответствующий состоянию идентификатора отправителя.
- **Удалить**. Агент идентификатора отправителя автоматически удаляет сообщение без ответа об ошибке SMTP. Exchange Server отправляет фиктивную команду **SMTP OK** на исходный сервер, а затем удаляет сообщение. Так как исходный сервер считает, что сообщение отправлено, он не повторяет отправку сообщения в том же сеансе.

Дополнительные сведения о том, как настроить действие, выполняемое для поддельной почты и недоступных DNS-серверов, см. в статье Процедуры идентификатора отправителя.

Обновление службы DNS, подключенной к Интернету, для поддержки технологии Sender ID в организации

Эффективность технологии Sender ID зависит от конкретных данных службы DNS. Чем больше организаций настраивают записи SPF для своих доменов, тем эффективнее технология Sender ID может распознавать поддельные сообщения.

Чтобы поддержать инфраструктуру Sender ID, необходимо создать записи SPF для доменов, из которых отправляются сообщения в вашей организации. Дополнительные сведения о создании и развертывании записей SPF см. в разделе Платформа политики отправителей: синтаксис записей SPF.

Указание доменов получателей и отправителей для исключения из фильтрации кодов отправителей

Вы можете исключить определенных получателей и домены отправителей из фильтрации идентификаторов отправителей с помощью **командлета Set-SenderIdConfig** в командной консоли Exchange. Дополнительные сведения см. в разделе Процедуры идентификатора отправителя.

Процедуры Sender ID

Статья • 04.04.2023

Технология Sender ID определяет поддельные электронные сообщения, сравнивая исходный IP-адрес с доменом в электронном адресе отправителя с помощью записи SPF в DNS. Дополнительные сведения об идентификаторе отправителя и агенте идентификатора отправителя см. в разделе Фильтрация отправителей.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Функции защиты от вредоносных программ" в разделе Разрешения для защиты от вредоносных программ и защиты от вредоносных программ .
- Для выполнения этой процедуры можно использовать только PowerShell. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- По умолчанию в службе транспорта на сервере почтовых ящиков не включены функции защиты от нежелательной почты. Как правило, их следует включать, только если организация Exchange не выполняет никакую предварительную фильтрацию нежелательной почты до приема входящих сообщений. Дополнительные сведения см. в разделе Включение функций защиты от нежелательной почты на серверах почтовых ящиков.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Включение или отключение идентификатора отправителя с помощью командной консоли

Exchange

Чтобы отключить идентификацию отправителей, выполните следующую команду:

PowerShell

```
Set-SenderIDConfig -Enabled $false
```

Чтобы включить идентификацию отправителей, выполните следующую команду:

PowerShell

```
Set-SenderIDConfig -Enabled $true
```

> ⓘ **Примечание**
>
> При отключении идентификации отправителей, соответствующий агент идентификации все еще включен. Чтобы отключить агент идентификатора отправителя, выполните команду : `Disable-TransportAgent "Sender ID Agent"`.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно включили или отключили технологию Sender ID, выполните следующую команду, чтобы проверить значение свойства **Enabled**:

PowerShell

```
Get-SenderIDConfig | Format-List Enabled
```

Включение или отключение идентификатора отправителя для внешних подключений с помощью командной консоли Exchange

По умолчанию технология Sender ID включена для внешних (не прошедших проверку подлинности) SMTP-подключений.

Чтобы отключить фильтрацию отправителей для внешних подключений, выполните следующую команду:

```
```

PowerShell

```
Set-SenderIDConfig -ExternalMailEnabled $false
```

Чтобы включить идентификацию отправителей для внешних подключений, выполните следующую команду:

PowerShell

```
Set-SenderIDConfig -ExternalMailEnabled $true
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно включили или отключили технологию Sender ID для внешних SMTP-подключений, выполните следующую команду, чтобы проверить значение свойства **ExternalMailEnabled**:

PowerShell

```
Get-SenderFilterConfig | Format-List ExternalMailEnabled
```

Включение или отключение идентификатора отправителя для внутренних подключений с помощью командной консоли Exchange

Не рекомендуем применять фильтры защиты от спама к сообщениям от надежных партнеров или внутренним сообщениям. Чтобы избежать неправильной обработки обыкновенных сообщений, следует настроить запуск агентов защиты от спама только для сообщений из внешних источников.

Чтобы включить идентификацию отправителей для внутренних (прошедших проверку подлинности) SMTP-подключений, выполните следующую команду:

PowerShell

```
Set-SenderIDConfig -InternalMailEnabled $true
```

Чтобы отключить идентификацию отправителей для внешних подключений, выполните следующую команду:

```
```

PowerShell

```
Set-SenderIDConfig -InternalMailEnabled $false
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно включили или отключили технологию Sender ID для внутренних SMTP-подключений, выполните следующую команду, чтобы проверить значение свойства **InternalMailEnabled**:

PowerShell

```
Get-SenderIDConfig | Format-List InternalMailEnabled
```

Использование командной консоли Exchange для настройки действия идентификатора отправителя для поддельных сообщений

Чтобы настроить действие Sender ID для поддельных сообщений, используйте следующий синтаксис:

PowerShell

```
Set-SenderIDConfig -SpoofedDomainAction <StampStatus | Reject | Delete>
```

В этом примере агент идентификатора отправителя настраивает на отклонение любых сообщений с ответом об ошибке 5 *xx* SMTP, если домен отправителя имеет запись SPF, а IP-адрес исходного сервера не указан в качестве доверенного сервера для домена (состояние идентификатора отправителя — `Fail`).

PowerShell

```
Set-SenderIDConfig -SpoofedDomainAction Reject
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно настроили действие Sender ID для поддельных сообщений, выполните следующую команду, чтобы проверить значения свойства

SpoofedDomainAction:

```
PowerShell

Get-SenderIDConfig | Format-List SpoofedDomainAction
```

Использование командной консоли Exchange для настройки действия идентификатора отправителя для временных ошибок

Чтобы настроить действие Sender ID для временных ошибок, используйте следующий синтаксис:

```
PowerShell

Set-SenderIDConfig -TempErrorAction <StampStatus | Reject | Delete>
```

В этом примере агент идентификатора отправителя настраивает для пометки сообщений, если не удается определить состояние идентификатора отправителя из-за временной ошибки DNS-сервера (состояние идентификатора отправителя — `TempError`). Сообщение будет обработано другими агентами защиты от спама, а агент фильтрации содержимого использует метку при определении значения вероятности нежелательной почты для сообщения.

```
PowerShell

Set-SenderIDConfig -TempErrorAction StampStatus
```

Обратите внимание, что `StampStatus` является значением по умолчанию для параметра *TempErrorAction* .

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно настроили действие Sender ID для временных ошибок, выполните следующую команду, чтобы проверить значения свойства **TempErrorAction**:

```
PowerShell
```

```
Get-SenderIDConfig | Format-List TempErrorAction
```

Настройка исключений домена получателя и отправителя с помощью командной консоли Exchange

Чтобы заменить существующие значения, выполните следующую команду:

PowerShell

```
Set-SenderIDConfig -BypassedRecipients <recipient1,recipient2...> -
BypassedSenderDomains <domain1,domain2...>
```

В этом примере агент идентификатора отправителя настраивает обход проверки идентификатора отправителя для сообщений, отправленных kim@contoso.com в и john@contoso.com, а также для обхода проверки идентификатора отправителя для сообщений, отправленных из домена fabrikam.com.

PowerShell

```
Set-SenderIDConfig -BypassedRecipients kim@contoso.com,john@contoso.com -
BypassedSenderDomains fabrikam.com
```

Чтобы добавить или удалить записи, не изменяя другие существующие значения, используйте следующий синтаксис:

PowerShell

```
Set-SenderIDConfig -BypassedRecipients @{Add="<recipient1>","
<recipient2>"...; Remove="<recipient1>","<recipient2>"...} -
BypassedSenderDomains @{Add="<domain1>","<domain2>"...; Remove="<domain1>","
<domain2>"...}
```

В этом примере настраивается агент Sender ID со следующими параметрами:

- Добавьте chris@contoso.com и michelle@contoso.com в список существующих получателей, которые обходят проверку идентификатора отправителя.
- Удалить tailspintoys.com из списка существующих доменов, обходящих проверку кода отправителя.

PowerShell

```
Set-SenderIDConfig -BypassedRecipients
@{Add="chris@contoso.com","michelle@contoso.com"} -BypassedSenderDomains
@{Remove="tailspintoys.com"}
```

Как проверить, что все получилось?

Чтобы убедиться, что вы успешно настроили исключения доменов получателей и отправителей, выполните следующую команду, чтобы проверить значения свойств:

PowerShell

```
Get-SenderIDConfig | Format-List BypassedRecipients,BypassedSenderDomains
```

Репутация отправителя и агент анализа протоколов в Exchange Server

Статья • 04.04.2023

Функция защиты от спама на основе репутации отправителя в Exchange блокирует сообщения в зависимости от характеристик отправителя. Чтобы определить, какое действие следует предпринять в отношении входящего сообщения, она использует сохраненные сведения об отправителе. Эта функция основана на использовании агента анализа протокола.

Дополнительные сведения о настройке репутации отправителя и агента анализа протоколов см. в разделе Процедуры репутации отправителя.

По умолчанию агент анализа протокола включен на пограничных транспортных серверах, но его также можно включить на серверах почтовых ящиков. Дополнительные сведения см. в разделе Включение функций защиты от нежелательной почты на серверах почтовых ящиков.

Вычисление уровня репутации отправителя (SRL)

Уровень репутации отправителя (SRL) рассчитывается исходя из следующей статистики:

- **Анализ HELO/EHLO**. Команды HELO и EHLO SMTP предназначены для предоставления доменного имени, например Contoso.com, или IP-адреса отправляющего SMTP-сервера принимающему SMTP-серверу. Злонамеренные пользователи, или *спамеры*, часто разными способами подделывают оператор HELO/EHLO. Например, вводят IP-адрес, не соответствующий IP-адресу, с которого произошло подключение. Кроме того, в попытке представить, будто домены находятся в организации, в оператор HELO спамеры подставляют домены, о которых известно, что они локально поддерживаются на принимающем сервере. В других случаях злоумышленники, рассылающие нежелательную почту, изменяют домен, передаваемый в операторе HELO. Как правило, обычный пользователь использует в операторах HELO разный, но относительно постоянный набор доменов.

Поэтому на основании анализа оператора HELO/EHLO для каждого отправителя можно сделать вывод, что он, возможно, рассылает нежелательную почту. Например, отправитель, который в определенный период времени передает много разных уникальных операторов HELO/EHLO, вероятно, рассылает нежелательную почту. Отправители, последовательно предоставляющие в операторах HELO IP-адрес, не совпадающий с настоящим IP-адресом, определенным агентом фильтрации подключений, вероятно, также рассылают нежелательную почту. Удаленные отправители, постоянно предоставляющие имя локального домена в операторе HELO в той же организации, на которой расположен сервер Exchange, вероятно, также рассылают нежелательную почту.

- **Обратный поиск DNS**. Репутация отправителя также проверяет, соответствует ли исходный IP-адрес, с которого отправитель передал сообщение, зарегистрированным доменным именем, которое отправитель отправляет в команде SMTP HELO или EHLO.

  Функция "репутация отправителя" выполняет обратный запрос DNS, отправляя в DNS исходящий IP-адрес. Результат, возвращаемый службой DNS, — имя домена, зарегистрированное центром доменных имен для данного IP-адреса. Функция репутации отправителя сравнивает имя домена, возвращенное службой DNS, с именем домена, переданным отправителем в SMTP-команде HELO/EHLO. Если имена доменов не совпадают, то отправитель, вероятно, является пользователем, рассылающим нежелательную почту, и общий уровень репутации отправителя для него должен быть увеличен.

  Агент идентификатора отправителя выполняет аналогичную задачу, но успех агента идентификатора отправителя зависит от законных отправителей, чтобы обновить инфраструктуру DNS для идентификации всех SMTP-серверов отправки электронной почты в своей организации. Выполняя обратный поиск DNS, вы можете помочь определить потенциальных спамеров.

- **Анализ оценок SCL сообщений от определенного отправителя**. Когда агент фильтра содержимого обрабатывает сообщение, он присваивает сообщению оценку уровня достоверности нежелательной почты (SCL). Оценка вероятности нежелательной почты — это число от 0 до 9. Более высокая оценка вероятности нежелательной почты означает, что сообщение с большой вероятностью будет нежелательным. Данные о каждом отправителе и оценках SCL их сообщений сохраняются для анализа при помощи функции «Репутация отправителя». Функция «Репутация отправителя» вычисляет статистику для отправителя, определяя соотношение между всеми

сообщениями от данного отправителя, которые имели в прошлом низкую оценку SCL, и всеми сообщениями от этого же отправителя, которые имели высокую оценку SCL. Кроме того, количество сообщений с высокой оценкой SCL, пришедших от отправителя за предыдущий день, применяется к общему значению SRL.

- **Проверка открытого прокси-сервера отправителя**. *Открытый прокси-сервер* — это прокси-сервер, который принимает запросы на подключение от любого пользователя в любом месте и пересылает трафик так, как если бы он поступил с локальных узлов. Прокси-серверы ретранслируют TCP-трафик через брандмауэр, обеспечивая пользовательским приложениям прозрачный доступ через брандмауэр. Поскольку протоколы прокси-серверов — облегченные и независимые от протоколов пользовательского приложения, то прокси-серверы могут использоваться многими различными службами. Прокси-серверы могут также применяться для общего использования одного подключения к Интернету несколькими компьютерами. Прокси-серверы обычно настраиваются так, чтобы пересекать прокси-серверы можно было только с известных брандмауэру доверенных компьютеров. Разрешенный отправитель может быть открытым прокси-сервером из-за непреднамеренной неправильной настройки или вредоносной программы.

  Открытые прокси-серверы предоставляют для пользователей-злоумышленников идеальный способ скрыть свои истинные учетные данные, чтобы реализовать атаку типа «отказ в обслуживании» (DoS) или разослать нежелательную почту. Так как все больше прокси-серверов настраивается как открытые по умолчанию, открытые прокси-серверы становятся обычным явлением. Кроме того, чтобы скрыть истинный IP-адрес отправителя, злоумышленник может использовать цепочку из нескольких открытых прокси-серверов.

  Когда функция репутации отправителя выполняет тест открытого прокси-сервера, она форматирует SMTP-запрос, чтобы подключиться к серверу Exchange с открытого прокси-сервера. Если SMTP-запрос от прокси-сервера получен, функция репутации отправителя убеждается, что сервер является открытым, и обновляет статистику проверки для этого отправителя.

Репутация отправителя взвешивает каждую из этих статистических данных и вычисляет SRL для каждого отправителя. Уровень репутации отправителя — это число от 0 до 9, отражающее вероятность того, что пользователь рассылает нежелательную почту или выполняет другие вредоносные действия. Значение 0 указывает, что отправитель, скорее всего, не будет спамом; значение 9 указывает, что отправитель, скорее всего, будет спамом.

Вы можете установить пороговое значение для блокировки от 0 до 9, при котором функция репутации отправителя отправляет запрос агенту фильтрации отправителей и тем самым запрещает отправителю отправлять сообщения в организацию. Когда отправитель заблокирован, он на заданный период времени добавляется в список заблокированных отправителей. Способ обработки заблокированных сообщений зависит от настройки агента фильтрации отправителей. Заблокированные сообщения можно:

- **Отклонение**: сообщения возвращаются в отчете о недоставке (также известном как недоставка, уведомление о состоянии доставки, DSN или сообщение о отказе).
- **Удалить**. Сообщения автоматически удаляются без недоставки.
- **Принять**: сообщения принимаются и помечаются как поступающие от заблокированного отправителя

Дополнительные сведения об агенте фильтрации отправителей см. в статье Фильтрация отправителей.

Если отправитель добавлен в список заблокированных IP-адресов или службу репутации IP-адресов (Майкрософт), функция репутации отправителя немедленно отправляет запрос агенту фильтрации отправителей, чтобы его заблокировать. Чтобы воспользоваться этой функцией, необходимо включить и настроить службу обновления средства защиты от спама Microsoft Exchange.

По умолчанию для отправителей, которые не были проанализированы, функция репутации отправителя устанавливает оценку 0. После того как от отправителя приходит 20 или более сообщений, она рассчитывает значение уровня репутации отправителя, которое основывается на статистике, описанной ранее в этой статье.

Когда следует использовать SRL

Функция репутации отправителя обрабатывает сообщения на двух этапах SMTP-сеанса:

- **В команде MAIL FROM: SMTP** репутация отправителя действует на сообщение только в том случае, если сообщение было заблокировано или иным образом действовало агентом фильтрации подключений, агентом фильтра отправителей, агентом фильтра получателей или агентом идентификатора отправителя. В этом случае репутация отправителя получает текущую оценку SRL отправителя из профиля отправителя, сохраненного для этого отправителя на сервере Exchange Server. После получения и оценки этой

оценки конфигурация сервера Exchange определяет поведение, которое происходит при конкретном подключении в соответствии с пороговым значением блока.

- **После команды SMTP "конец данных"**: команда SMTP конца передачи данных (**EOD**) выполняется при отправке всех фактических данных сообщения. На этой стадии SMTP-сеанса многие агенты защиты от спама уже обработали сообщение. В результате выполнения этих процедур статистика, используемая функцией репутации отправителя, обновляется. Таким образом, эта функция получает обновленные данные для последующего расчета или пересчета значения SRL для отправителя.

Настройка обнаружения открытых прокси-серверов

Когда агент репутации отправителя вычисляет уровень репутации отправителя, он пытается подключиться к исходному IP-адресу отправителя с помощью распространенных протоколов прокси-серверов, таких как SOCKS4, SOCKS5, HTTP, Telnet, Cisco и Wingate. Чтобы подключиться к серверу Exchange с открытого прокси-сервера с помощью SMTP-запроса, агент репутации отправителя форматирует запрос в соответствии с протоколом. Если SMTP-запрос получен от прокси-сервера, агент репутации отправителя убеждается, что прокси-сервер является открытым, и корректирует оценку уровня репутации отправителя согласно этому результату. По умолчанию для агента репутации отправителя включено обнаружение открытых прокси-серверов.

Дополнительные сведения о настройке обнаружения открытых прокси-серверов см. в разделе Процедуры репутации отправителя.

Установка порогового значения для блокировки по уровню репутации отправителя

Уровень репутации отправителя — это число от 0 до 9, отражающее вероятность того, что пользователь рассылает нежелательную почту или выполняет другие вредоносные действия. Вам необходимо настроить пороговое значение для блокировки по уровню репутации отправителя, чтобы указать значение уровня репутации, при котором отправитель будет заблокирован. По умолчанию пороговое значение для блокировки равно 7, что означает, что отправители с

уровнями репутации 7, 8 или 9 будут заблокированы. Рекомендуется отслеживать эффективность функции репутации отправителей и агента анализа протокола на уровне по умолчанию.

На пограничном транспортном сервере, если пороговое значение блока SRL достигнуто или превышено конкретным отправителем, репутация отправителя добавляет отправителя в список заблокированных IP-адресов в агенте фильтрации подключений. Иногда спамеры отправляют пакеты спама от одного отправителя. В этом сценарии, если репутация отправителя вычисляет значение SRL, превышающее пороговое значение блока SRL, отправитель добавляется в список заблокированных отправителей в течение настраиваемого времени. По умолчанию продолжительность блокировки равняется 24 часам. Через 24 часа отправитель удаляется из списка заблокированных отправителей и может отправлять сообщения снова.

При добавлении отправителя в список блокировок IP-адресов агент репутации отправителя удаляет профиль отправителя. Агент репутации отправителя удаляет этот профиль, поскольку в существующем профиле заблокированного отправителя указано, что уровень репутации отправителя превышает пороговое значение для блокировки по уровню репутации отправителя. В противном случае заблокированный отправитель был бы вновь добавлен в список блокировок IP-адресов по окончании периода блокировки отправителя.

Дополнительные сведения о настройке блокировки отправителей см. в статье Процедуры репутации отправителя.

Процедуры репутации отправителя

Статья • 04.04.2023

Репутация отправителя и агент анализа протокола блокируют нежелательные сообщения в соответствии с различными характеристиками отправителя. Репутация отправителя основана на имеющихся сведениях об отправителе и определяет, какое действие будет предпринято (если это требуется) в отношении входящего сообщения. Дополнительные сведения см. в разделах Репутация отправителя и агент анализа протоколов.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Функции защиты от вредоносных программ" в разделе Разрешения для защиты от вредоносных программ и защиты от вредоносных программ .
- Для выполнения этой процедуры можно использовать только PowerShell. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- По умолчанию в службе транспорта на сервере почтовых ящиков не включены функции защиты от нежелательной почты. Как правило, их следует включать, только если организация Exchange не выполняет никакую предварительную фильтрацию нежелательной почты до приема входящих сообщений. Дополнительные сведения см. в разделе Включение функций защиты от нежелательной почты на серверах почтовых ящиков.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Включение или отключение репутации отправителя с помощью командной консоли Exchange

Чтобы отключить репутацию отправителя, выполните следующую команду:

```
PowerShell
Set-SenderReputationConfig -Enabled $false
```

Чтобы включить репутацию отправителя, выполните следующую команду:

```
PowerShell
Set-SenderReputationConfig -Enabled $true
```

> ⓘ **Примечание**
>
> Функция репутации отправителя основана на использовании агента анализа протокола. При отключении функции репутации отправителя агент анализа протокола все еще включен. Чтобы отключить агент анализа протоколов, выполните команду : `Disable-TransportAgent "Protocol Analysis Agent"`.

Как проверить, все ли получилось?

Чтобы убедиться, что репутация отправителя успешно включена или отключена, выполните следующую команду и проверьте значение свойства **Enabled**:

```
PowerShell
Get-SenderReputationConfig | Format-List Enabled
```

Использование командной консоли Exchange для включения или отключения репутации отправителя для внешних сообщений

По умолчанию репутация отправителя включена для внешних сообщений (сообщений из внешних источников).

Чтобы отключить репутацию отправителя, выполните следующую команду:

PowerShell

```
Set-SenderReputationConfig -ExternalMailEnabled $false
```

Чтобы включить репутацию отправителя, выполните следующую команду:

PowerShell

```
Set-SenderReputationConfig -ExternalMailEnabled $true
```

Как проверить, все ли получилось?

Чтобы убедиться, что репутация отправителя успешно включена или отключена для внешних сообщений, выполните следующую команду и проверьте значение свойства **ExternalMailEnabled**:

PowerShell

```
Get-SenderReputationConfig | Format-List ExternalMailEnabled
```

Использование командной консоли Exchange для включения или отключения репутации отправителя для внутренних сообщений

Не рекомендуем применять фильтры защиты от спама к сообщениям от надежных партнеров или внутренним сообщениям. В этом случае всегда существует вероятность ложного срабатывания фильтра. Чтобы снизить эту вероятность, настройте запуск агентов фильтрации защиты от спама только для сообщений из непроверенных и неизвестных источников.

Чтобы включить репутацию отправителя для внутренних сообщений, выполните следующую команду:

PowerShell

```
Set-SenderReputationConfig -InternalMailEnabled $true
```

Чтобы отключить репутацию отправителя для внутренних сообщений, выполните следующую команду:

PowerShell

```
Set-SenderReputationConfig -InternalMailEnabled $false
```

Как проверить, все ли получилось?

Чтобы убедиться, что репутация отправителя успешно включена ли отключена для внутренних сообщений, выполните следующую команду и проверьте значение свойства **InternalMailEnabled**:

PowerShell

```
Get-SenderReputationConfig | Format-List InternalMailEnabled
```

Настройка блокировки отправителей в репутации отправителя с помощью командной консоли Exchange

Вычисленный уровень репутации отправителя (SRL) и указанное пороговое значение SRL используются для временной блокировки отправителя. Чтобы настроить блокировку отправителей на основе репутации, используйте следующий синтаксис:

PowerShell

```
Set-SenderReputationConfig -SenderBlockingEnabled <$true | $false> -
SrlBlockThreshold <0 - 9> [-SenderBlockingPeriod <0 - 48>]
```

В этом примере пороговое значение SRL для блокировки снижается до 6 (то есть блокируются отправители с уровнями 6, 7, 8 и 9), а нарушители блокируются на 36 часов:

PowerShell

```
Set-SenderReputationConfig -SrlBlockThreshold 6 -SenderBlockingPeriod 36
```

В этом примере отключается блокировка отправителей.

PowerShell

```
Set-SenderReputationConfig -SenderBlockingEnabled $false
```

Примечания.

- Значение по умолчанию параметра *SenderBlockingEnabled* — `$true`.
- Значение параметра *SenderBlockingPeriod* по умолчанию: 24.
- Значение параметра *SrlBlockThreshold* по умолчанию: 7.
- Невозможно одновременно отключить блокировку отправителей и обнаружение открытых прокси-серверов. По крайней мере одна из этих функций должна быть включена.

Как проверить, что все получилось?

Чтобы убедиться, что блокировку отправителей успешно настроено, выполните следующую команду и проверьте значения свойств:

PowerShell

```
Get-SenderReputationConfig | Format-List *block*
```

Настройка обнаружения открытого прокси-сервера в репутации отправителя с помощью командной консоли Exchange

По умолчанию обнаружение открытых прокси-серверов используется как одно из условий для вычисления уровня репутации исходного сервера. При обнаружении открытого прокси-сервера exchange server пытается отправить тестовое сообщение с исходного сервера обмена сообщениями. Если тестовое сообщение успешно доставлено обратно на сервер Exchange Server, это означает, что исходный сервер настроен как открытый прокси-сервер (намеренно или непреднамеренно).

Для обнаружения открытых прокси-серверов используются протоколы и TCP-порты, описанные в следующей таблице, поэтому эти порты должны быть открыты в брандмауэре:

Протоколы	Порты
SOCKS4, SOCKS5	1081, 1080
Wingate, Telnet, Cisco	23
HTTP CONNECT, HTTP POST	6588, 3128, 80

Кроме того, если для контроля исходящего интернет-трафика в организации используется прокси-сервер, то доступ к Интернету для функции репутации отправителей необходимо настроить через него. В частности, определите необходимые имя и тип прокси-сервера, а также TCP-порт.

Чтобы настроить обнаружение открытых прокси-серверов, используйте следующий синтаксис:

PowerShell

```
Set-SenderReputationConfig -OpenProxyDetectionEnabled <$true | $false> [-
ProxyServerName <String> -ProxyServerPort <Port> -ProxyServerType <None |
Socks4 | Socks5 | HttpConnect | HttpPost | Telnet | Cisco | Wingate>]
```

В этом примере настраивается подключение к Интернету через прокси-сервер SERVER01, который использует протокол HTTP CONNECT через порт 80.

PowerShell

```
Set-SenderReputationConfig -ProxyServerName SERVER01 -ProxyServerPort 80 -
ProxyServerType HttpConnect
```

В этом примере отключается обнаружение открытых прокси-серверов.

PowerShell

```
Set-SenderReputationConfig -OpenProxyDetectionEnabled $false
```

Примечания.

- Значение по умолчанию параметра *OpenProxyDetectionEnabled* — `$true`.
- Значение по умолчанию параметра *ProxyServerName* пусто (`$null`).
- Значение параметра *ProxyServerPort* по умолчанию: 0.
- Значение по умолчанию параметра *ProxyServerType* — `None`.

- Невозможно одновременно отключить обнаружение открытых прокси-серверов и блокировку отправителей. По крайней мере одна из этих функций должна быть включена.

Как проверить, что все получилось?

Чтобы убедиться, что обнаружение открытых прокси-серверов успешно настроено, выполните следующую команду и проверьте значения свойств:

PowerShell

```
Get-SenderReputationConfig | Format-List *proxy*
```

См. также

Get-SenderReputationConfig

Set-SenderReputationConfig

Использование фильтрации вложений на пограничных транспортных серверах в Exchange Server

Статья • 04.04.2023

В Exchange Server можно использовать фильтрацию вложений на пограничных транспортных серверах для управления вложениями, получаемыми пользователями в сообщениях электронной почты. Она выполняется агентом фильтрации вложений, который доступен только на пограничных транспортных серверах, и по сути не отличается от Exchange Server 2010.

Сведения о настройке параметров фильтрации вложений см. в статье Процедуры фильтрации вложений на пограничных транспортных серверах.

Типы фильтрации вложений

Для контроля вложений, поступающих в организацию или исходящих из нее через пограничный транспортный сервер, можно использовать следующие типы фильтрации вложений.

- **Фильтрация на основе имени файла или расширения имени файла**. Вы указываете точное имя файла или расширение имени файла, которое требуется отфильтровать. Например, `BadFileName.exe` или `*.exe`.

- **Фильтрация на основе типа контента MIME файла**. Вы указываете значение типа контента MIME, которое требуется отфильтровать. Значение типа контента MIME указывает, что такое вложение: например, изображение JPEG, исполняемый файл или файл Microsoft Excel. Типы контента выражаются как*подтип*> *типа*</ ><. Например, файл изображения JPEG выражается как `image/jpeg`.

  Чтобы просмотреть полный список расширений имен файлов и типов содержимого, которые может обнаружить фильтрация вложений, выполните в командной консоли Exchange на пограничном транспортном сервере следующую команду:

  PowerShell

```
Get-AttachmentFilterEntry | Format-Table -Auto Type,Name
```

После определения файлов для поиска вы можете настроить действие, применяемое к сообщениями, которые содержатся в этих вложениях. Нельзя указывать разные действия для разных типов вложений. Необходимо настроить одно из следующих действий для всех сообщений, которые соответствуют одному из фильтров вложений.

- **Отклонить (заблокировать) сообщение**: сообщение заблокировано. Отправитель получает отчет о недоставке, в котором указывается, что сообщение не доставлено, так как содержит недопустимое вложение. Вы можете изменить текст отчета о недоставке. Текст по умолчанию: `Message rejected due to unacceptable attachments`.

- **Удалите вложение, но разрешите сообщение.** Вложение удаляется из сообщения. Однако само сообщение и любые другие вложения, которые не соответствуют условиям фильтра, пропускаются. Если вложение удалено, оно заменяется текстовым файлом, в котором объясняется, почему данное вложение было удалено. Это действие выполняется по умолчанию.

- **Автоматическое удаление сообщения**: сообщение удаляется. Ни отправитель, ни получатель не получают уведомления.

Примечания.

- Невозможно извлечь сообщения или вложения, которые были заблокированы или удалены. При настройке фильтров вложений тщательно проверьте совпадения по именам файлов и убедитесь, что этот фильтр не затронет допустимые вложения.

- Если вы удалите вложения из сообщений с цифровой подписью, зашифрованных или защищенных сообщений, вы аннулируете цифровую подпись, и сообщения невозможно будет прочитать. Поэтому рекомендуем подписывать и шифровать исходящие сообщения после обработки агентом фильтрации вложений.

Дополнительные сведения см. в статье Процедуры фильтрации вложений на пограничных транспортных серверах.

Вложения по умолчанию в фильтрации вложений

Вложения по умолчанию, которые определены в фильтрации вложений, описаны в приведенной ниже таблице.

Тип	Имя
`ContentType`	`application/hta`
`ContentType`	`application/javascript`
`ContentType`	`application/msaccess`
`ContentType`	`application/prg`
`ContentType`	`application/x-javascript`
`ContentType`	`application/x-msdownload`
`ContentType`	`message/partial`
`ContentType`	`text/javascript`
`ContentType`	`text/scriptlet`
`ContentType`	`x-internet-signup`
`FileName`	`*.ade`
`FileName`	`*.adp`
`FileName`	`*.app`
`FileName`	`*.asx`
`FileName`	`*.bas`
`FileName`	`*.bat`
`FileName`	`*.chm`
`FileName`	`*.cmd`
`FileName`	`*.com`
`FileName`	`*.cpl`
`FileName`	`*.crt`
`FileName`	`*.csh`
`FileName`	`*.exe`
`FileName`	`*.fxp`

Тип	Имя
`FileName`	`*.hlp`
`FileName`	`*.hta`
`FileName`	`*.inf`
`FileName`	`*.ins`
`FileName`	`*.isp`
`FileName`	`*.js`
`FileName`	`*.jse`
`FileName`	`*.ksh`
`FileName`	`*.lnk`
`FileName`	`*.mda`
`FileName`	`*.mdb`
`FileName`	`*.mde`
`FileName`	`*.mdt`
`FileName`	`*.mdw`
`FileName`	`*.mdz`
`FileName`	`*.msc`
`FileName`	`*.msi`
`FileName`	`*.msp`
`FileName`	`*.mst`
`FileName`	`*.ops`
`FileName`	`*.pcd`
`FileName`	`*.pif`
`FileName`	`*.prf`
`FileName`	`*.prg`
`FileName`	`*.ps1`

Тип	Имя
`FileName`	`*.ps1xml`
`FileName`	`*.ps11`
`FileName`	`*.ps11xml`
`FileName`	`*.ps2`
`FileName`	`*.ps2xml`
`FileName`	`*.psc1`
`FileName`	`*.psc2`
`FileName`	`*.reg`
`FileName`	`*.scf`
`FileName`	`*.scr`
`FileName`	`*.sct`
`FileName`	`*.shb`
`FileName`	`*.shs`
`FileName`	`*.url`
`FileName`	`*.vb`
`FileName`	`*.vbe`
`FileName`	`*.vbs`
`FileName`	`*.wsc`
`FileName`	`*.wsf`
`FileName`	`*.wsh`
`FileName`	`*.xnk`

Процедуры фильтрации вложений на пограничных транспортных серверах

Статья • 04.04.2023

Фильтрация вложений в Exchange Server предоставляется агентом фильтра вложений, доступным только на пограничных транспортных серверах. Фильтрация вложений предотвращает попадание в организацию файлов, вложенных в сообщения электронной почты. Можно настроить одну или несколько записей фильтрации вложений так, чтобы фильтровать вложения по типу содержимого или по имени файла.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Функции защиты от нежелательной почты" в разделе Разрешения для защиты от вредоносных программ и "Транспортные агенты" в разделе Разрешения потока обработки почты .
- Изменения параметров настройки фильтрации вложений на пограничном транспортном сервере действуют только на локальном компьютере. Если в сети периметра имеется несколько пограничных транспортных серверов, фильтрацию вложений необходимо настроить отдельно на каждом из этих серверов.
- Для выполнения этой процедуры можно использовать только PowerShell. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

Совет

Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Включение или отключение фильтрации вложений с помощью командной консоли Exchange

При включении или отключении агента фильтрации вложений изменение вступает в силу после перезапуска службы транспорта Microsoft Exchange. При перезапуске службы транспорта Microsoft Exchange на пограничном транспортном сервере поток обработки почты на сервере временно прерывается.

Чтобы отключить фильтрацию вложений, выполните приведенную ниже команду.

```
PowerShell

Disable-TransportAgent "Attachment Filtering Agent"
```

Чтобы включить фильтрацию вложений, выполните приведенную ниже команду.

```
PowerShell

Enable-TransportAgent "Attachment Filtering Agent"
```

После включения или отключения фильтрации вложений перезапустите службу транспорта Microsoft Exchange, выполнив указанную ниже команду.

```
PowerShell

Restart-Service MSExchangeTransport
```

Как проверить, все ли получилось?

Для проверки успешности включения или выключения фильтрации вложений выполните следующую команду, чтобы проверить значение свойства **Enabled**:

```
PowerShell

Get-TransportAgent "Attachment Filtering Agent"
```

Использование командной консоли Exchange для просмотра и поиска записей

фильтрации вложений

Записи фильтрации вложений определяют вложения в сообщения, которые не должны попадать в организацию. Чтобы просмотреть записи фильтрации вложений, используемые агентом фильтрации вложений, выполните приведенную ниже команду.

PowerShell

```
Get-AttachmentFilterEntry | Format-Table -Auto Type,Name
```

Чтобы просмотреть определенную запись типа контента MIME, используйте следующий синтаксис:

PowerShell

```
Get-AttachmentFilterEntry ContentType:<MIMEContentType>
```

Например, чтобы просмотреть, имеется ли запись типа контента MIME для изображений в формате JPEG, выполните следующую команду:

PowerShell

```
Get-AttachmentFilterEntry ContentType:image/jpeg
```

Если появляется сообщение об ошибке , `Couldn't find the specified identity.` тип контента MIME не определен в записях фильтрации вложений.

Чтобы просмотреть определенную запись имени или расширения файла, используйте приведенный ниже синтаксис.

PowerShell

```
Get-AttachmentFilterEntry FileName:<FileName or FileNameExtension>
```

Например, чтобы просмотреть, имеется ли запись расширения имени файла для вложений в формате JPEG, выполните следующую команду:

PowerShell

```
Get-AttachmentFilterEntry FileName:*.jpg
```

Если появляется сообщение об ошибке , `Couldn't find the specified identity.` имя файла или расширение имени файла не определены в записях фильтрации вложений.

Дополнительные сведения см. в статье Get-AttachmentFilterEntry.

Добавление записей фильтрации вложений с помощью командной консоли Exchange

Чтобы добавить запись фильтрации вложений, которая фильтрует вложения по типу контента MIME, используйте приведенный ниже синтаксис.

PowerShell

```
Add-AttachmentFilterEntry -Name <MIMEContentType> -Type ContentType
```

В примере ниже добавляется запись типа контента MIME, которая фильтрует изображения в формате JPEG.

PowerShell

```
Add-AttachmentFilterEntry -Name image/jpeg -Type ContentType
```

Чтобы добавить запись фильтрации вложений, которая фильтрует вложения по имени или расширению файла, используйте приведенный ниже синтаксис.

PowerShell

```
Add-AttachmentFilterEntry -Name <FileName or FileNameExtension> -Type
FileName
```

В примере ниже выполняется фильтрация вложений с расширением имени JPG-файла.

PowerShell

```
Add-AttachmentFilterEntry -Name *.jpg -Type FileName
```

Дополнительные сведения см. в статье Add-AttachmentFilterEntry.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно добавили запись фильтрации вложений, отправьте тестовое сообщение с вложением запрещенного типа с внешнего почтового ящика внутреннему получателю и убедитесь, что сообщение и вложение обрабатываются должным образом.

Удаление записей фильтрации вложений с помощью командной консоли Exchange

Чтобы удалить запись фильтрации вложений, которая фильтрует вложения по типу контента MIME, используйте приведенный ниже синтаксис.

PowerShell

```
Remove-AttachmentFilterEntry ContentType:<ContentType>
```

В примере ниже удаляется запись типа контента MIME для изображений в формате JPEG.

PowerShell

```
Remove-AttachmentFilterEntry ContentType:image/jpeg
```

Чтобы удалить запись фильтрации вложений, которая фильтрует вложения по имени или расширению файла, используйте приведенный ниже синтаксис.

PowerShell

```
Remove-AttachmentFilterEntry FileName:<FileName or FileNameExtension>
```

В примере ниже удаляется запись имени файла для расширения имени JPG-файла.

PowerShell

```
Remove-AttachmentFilterEntry FileName:*.jpg
```

Дополнительные сведения см. в статье Remove-AttachmentFilterEntry.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно удалили запись фильтрации вложений, отправьте тестовое сообщение с вложением разрешенного типа с внешнего почтового ящика

внутреннему получателю и убедитесь, что сообщение успешно доставлено вместе с вложением.

Использование командной консоли Exchange для просмотра действия фильтрации вложений

Чтобы просмотреть действие фильтрации вложений, выполняемое в случае обнаружения в сообщении запрещенного вложения, выполните приведенную ниже команду.

PowerShell

```
Get-AttachmentFilterListConfig | Format-List
Action,AdminMessage,RejectResponse,ExceptionConnectors
```

Настройка действия фильтрации вложений с помощью командной консоли Exchange

Чтобы настроить действие фильтрации вложений, выполняемое в случае обнаружения в сообщении вложения запрещенного типа, используйте следующий синтаксис:

PowerShell

```
Set-AttachmentFilterListConfig [-Action <Reject | Strip | SilentDelete>] [-
RejectResponse "<Message text>"] [-AdminMessage "<Replacement file text>"]
[-ExceptionConnectors <ConnectorGUID>]
```

В этом примере в конфигурацию фильтрации вложений вносятся приведенные ниже изменения.

- Сообщения с запрещенными вложениями отклоняются (блокируются). Обратите внимание, что указать разные действия для разных типов вложений невозможно.
- Для отклоненных сообщений используется настраиваемый ответ.

PowerShell

```
Set-AttachmentFilterListConfig -Action Reject -RejectResponse "This message
contains a prohibited attachment. Your message can't be delivered. Please
resend the message without the attachment."
```

Дополнительные сведения см. в статье Set-AttachmentFilterListConfig.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно настроили действие фильтрации вложений, отправьте тестовое сообщения с вложением запрещенного типа из внешнего почтового ящика внутреннему получателю и убедитесь, что сообщение и вложение обрабатываются должным образом.

Фильтрация подключений на пограничных транспортных серверах в Exchange Server

Статья • 04.04.2023

Фильтрация подключений — это функция защиты от нежелательной почты в Exchange Server, которая разрешает или блокирует электронную почту на основе источника сообщения. Фильтрация подключений выполняется агентом фильтрации подключений, доступным только на пограничных транспортных серверах, и практически не изменяется с Exchange Server 2010 года. Чтобы определить действие для входящего сообщения (если оно необходимо), агент фильтра подключений использует IP-адрес почтового сервера.

По умолчанию агент фильтрации подключений первым оценивает входящее сообщение на пограничном транспортном сервере. Исходный IP-адрес SMTP-подключения сравнивается с разрешенными и заблокированными IP-адресами. Если исходный IP-адрес разрешен, сообщение отправляется получателям в вашей организации без последующей обработки остальными агентами защиты от спама. Если исходный IP-адрес заблокирован, SMTP-подключение отклоняется. Если исходный IP-адрес не разрешен, и не заблокирован, сообщение переходит к другим агентам защиты от спама на пограничном транспортном сервере.

Фильтрация подключений сравнивает IP-адрес исходного почтового сервера со значениями в списке разрешенных IP-адресов, списке блокировок IP-адресов, поставщиках списков разрешенных IP-адресов и поставщиках списков блокировок IP-адресов. Чтобы фильтрация подключений работала, необходимо настроить по крайней мере один из этих хранилищ данных IP-адресов. Если данные IP-адресов не указаны, агент фильтрации подключений следует отключить. Дополнительные сведения см. в статье Процедуры фильтрации подключений на пограничных транспортных серверах.

Запрещенный список IP-адресов

Список блокировок IP-адресов содержит IP-адреса почтовых серверов, которые необходимо заблокировать. Ip-адреса вручную сохраняются в списке блокировок IP-адресов. При этом можно добавить отдельные адреса или диапазоны адресов. Вы можете указать срок действия, определяющий период блокировки IP-адреса

или диапазона. Когда срок действия истек, запись IP-адреса в списке блокировок IP-адресов отключается.

Если агент фильтрации подключений находит исходный IP-адрес в списке блокировок IP-адресов, smtp-подключение будет удалено после обработки всех заголовков **RCPT TO** (получателей конвертов) в сообщении.

IP-адреса также могут автоматически добавляться в список блокировок IP-адресов с помощью функции репутации отправителя агента анализа протоколов. Дополнительные сведения см. в разделе Sender reputation and the Protocol Analysis agent.

Утвержденный список IP-адресов

Список разрешенных IP-адресов содержит IP-адреса почтовых серверов, которые вы хотите назначить надежными источниками электронной почты. Email почтовых серверов, указанных в списке разрешенных IP-адресов, не могут обрабатываться другими агентами exchange antispam.

Вы вручную сохраняете IP-адреса в списке разрешенных IP-адресов. При этом можно добавить отдельные адреса или диапазоны адресов. Вы можете указать срок действия, определяющий период, в течение которого IP-адрес или диапазон будет считаться разрешенным. По достижении срока действия запись в списке разрешенных IP-адресов отключается.

Поставщики списков блокировок IP-адресов

Поставщики списков блокировок *IP-адресов часто называются списками блокировок в режиме реального времени или списками больших двоичных* данных. Поставщики списков блокировок IP-адресов компилируют списки IP-адресов почтовых серверов, которые отправляют спам. Многие поставщики списков блокировок IP-адресов также компилируют списки IP-адресов почтовых серверов, которые могут использоваться для нежелательной почты. В качестве примера можно привести почтовые серверы, настроенные для открытой ретрансляции, поставщики услуг Интернета (ISP), которые назначают динамические IP-адреса, и ISP, которые разрешают SMTP-трафик почтовых серверов от учетных записей удаленного доступа.

При настройке фильтрации подключений для использования поставщика списка блокировок IP-адресов агент фильтрации подключений сравнивает IP-адрес подключающегося почтового сервера со списком IP-адресов поставщика списка

блокировок IP-адресов. Если найдено совпадение, сообщение не будет передано в организацию. Вы можете настроить фильтрацию подключений для использования нескольких поставщиков списков блокировок IP-адресов и назначать разные значения приоритета каждому поставщику.

Агент фильтрации подключений проверяет исходный IP-адрес в списке разрешенных IP-адресов и списке блокировок IP-адресов. Если IP-адрес отсутствует в любом списке, агент фильтрации подключений запрашивает поставщик списка блокировок IP-адресов в соответствии с назначенным приоритетом. Если IP-адрес определен поставщиком списка блокировок IP-адресов, пограничный транспортный сервер ожидает и обрабатывает заголовок **RCPT TO** , отвечает на отправляющий почтовый сервер с ошибкой `SMTP 550` и закрывает подключение. Подключение не удаляется сразу, поэтому попытка подключения может быть зарегистрирована, а также потому, что вы можете указать получателей, для которых сообщения не заблокированы любыми поставщиками списков блокировок IP-адресов.

Если IP-адрес не определен ни в одном из поставщиков списка блокировок IP-адресов, агент фильтрации содержимого передает сообщение следующему агенту транспорта на пограничном транспортном сервере.

Для каждого поставщика списка блокировок IP-адресов можно настроить ошибку `SMTP 550` , которая возвращается отправителю при блокировке сообщения. Следует определить поставщика списка блокировок IP-адресов, который определил источник сообщения как спам. Если допустимый исходный почтовый сервер ошибочно идентифицируется как источник нежелательной почты, администратор может обратиться к поставщику списка заблокированных IP-адресов и предпринять необходимые действия, чтобы удалить почтовый сервер из поставщика списка блокировок IP-адресов.

Поставщики списков блокировок IP-адресов могут возвращать различные коды, чтобы определить, почему IP-адрес определен в их списках. Большинство поставщиков списка блокировок IP-адресов возвращают типы данных битовой маски или абсолютного значения. В этих типах данных поставщик списка блокировок IP-адресов может использовать несколько значений для классификации IP-адреса по типу угроз.

При использовании поставщиков списков блокировок IP-адресов следует учитывать следующие проблемы:

- Сбои или задержки в службе поставщика списка блокировок IP-адресов могут привести к задержкам при обработке сообщений на пограничном

транспортном сервере. Всегда следует выбирать надежных поставщиков списков блокировок IP-адресов.

- Заслуживающие доверия исходные серверы могут быть случайно определены как источники нежелательной почты. Например, почтовый сервер непреднамеренно может быть настроен для открытой ретрансляции. Всегда следует выбирать поставщиков списков блокировок IP-адресов, которые предоставляют четкие процедуры для оценки и удаления из своих служб.

Примеры битовой маски и абсолютных значений

В этом разделе показан пример кодов состояния, возвращаемых большинством поставщиков списков блокировок. Коды состояния, возвращаемые поставщиком, см. в документации для конкретного поставщика.

Для типов данных битовой маски служба поставщика списка блокировок IP-адресов возвращает код состояния 127.0.0. *x*, где целое число *x* — это одно из значений, перечисленных в следующей таблице.

Значения и коды состояния для типов данных «битовая маска»

Значение	Код состояния
1	IP-адрес находится в списке блокировок IP-адресов.
2	SMTP-сервер настроен в качестве открытого ретранслятора.
4	Данный IP-адрес поддерживает IP-адрес для коммутируемого доступа.

Для абсолютных типов значений поставщик списка блокировок IP-адресов возвращает явные ответы, определяющие, почему IP-адрес определен в списке блокировок. В следующей таблице приводятся некоторые примеры абсолютных значений и откликов в явном виде.

Значения и коды состояния для типов данных «абсолютное значение»

Значение	Отклик
127.0.0.2	Данный IP-адрес является непосредственным источником нежелательной почты.
127.0.0.4	Данный IP-адрес является источником массовой рассылки.
127.0.0.5	Удаленный сервер, отправляющий данное сообщение, поддерживает многокаскадные открытые ретрансляции.

Поставщики списка разрешенных IP-адресов

Поставщики списка разрешенных IP-адресов также называются *безопасными списками*. Поставщики списка разрешенных IP-адресов настраиваются так же, как поставщики списков блокировок IP-адресов, но результаты противоположны: они определяют IP-адреса почтовых серверов, которые определенно не связаны со спамом. Если IP-адрес подключающегося почтового сервера определен поставщиком разрешенных IP-адресов, сообщение освобождается от обработки другими агентами exchange antispam. По этой причине поставщики списков блокировок IP-адресов используются гораздо чаще, чем поставщики разрешенных IP-адресов. Тщательно выбирайте поставщиков разрешенных IP-адресов.

Проверка поставщиков списков блокировок IP-адресов и поставщиков разрешенных IP-адресов

После настройки фильтрации подключений для использования поставщика списка блокировок IP-адресов или поставщика списка разрешенных IP-адресов можно выполнить тесты, чтобы убедиться, что поставщики работают правильно. Большинство поставщиков предоставляют тестовые IP-адреса, которые можно использовать для проверки служб. При тестировании поставщика агент фильтрации подключений отправляет запрос DNS, который должен привести к определенному ответу от поставщика. Дополнительные сведения о том, как проверить IP-адреса в службе поставщика списка блокировок IP-адресов или службы поставщика разрешенных IP-адресов, см. в разделе Процедуры фильтрации подключений на пограничных транспортных серверах.

Настройка фильтрации подключений на пограничных транспортных серверах, не подключенных напрямую к Интернету

Фильтрацию подключений можно использовать на пограничных транспортных серверах, которые не получают электронную почту напрямую из Интернета. В этом случае пограничный транспортный сервер находится за другим почтовым сервером, получающим и обрабатывающим сообщения, поступающие непосредственно из Интернета. Например, ваша организация может отправлять трафик электронной почты через антиспам-сервер, службу или устройство, прежде чем сообщения доходят до пограничного транспортного сервера. При этом агент

фильтра подключений должен извлекать из сообщения правильный исходный IP-адрес. Для этого агенту фильтрации подключений требуется проанализировать значения поля заголовка **Received** и сравнить их с известными IP-адресами почтового сервера, расположенным между пограничным транспортным сервером и Интернетом.

Каждый почтовый сервер, который принимает и ретранслирует SMTP-сообщение на пути доставки, добавляет собственное поле **Received** в заголовок сообщения. Обычно заголовок **Received** содержит доменное имя и IP-адрес почтового сервера, который обработал сообщение.

Если пограничный транспортный сервер не принимает сообщения непосредственно из Интернета, необходимо использовать параметр *InternalSMTPServers* в **командлете Set-TransportConfig** на сервере почтовых ящиков Exchange, чтобы определить IP-адрес почтового сервера, который находится между пограничным транспортным сервером и Интернетом. Данные об IP-адресах реплицируются на пограничные транспортные серверы с помощью EdgeSync. При получении сообщений пограничным транспортным сервером агент фильтрации подключений предполагает, что IP-адрес в поле **Заголовка Получено** , который не соответствует значению, указанному параметром *InternalSMTPServers* , является исходным IP-адресом, который необходимо проверить. Поэтому для корректной работы фильтрации подключений необходимо указать все внутренние SMTP-серверы.

Процедуры фильтрации подключений на пограничных транспортных серверах

Статья • 04.04.2023

Фильтрация подключений — это функция антиспамов, предоставляемая агентом фильтрации подключений, которая доступна только на пограничных транспортных серверах в Exchange Server. Фильтрация подключений включает следующие функции:

- Запрещенный список IP-адресов
- Поставщики списков блокировок IP-адресов
- Утвержденный список IP-адресов
- Поставщики списка разрешенных IP-адресов

Каждый из этих компонентов можно включать и отключать независимо.

Дополнительные сведения о фильтрации подключений см. в статье Фильтрация подключений на пограничных транспортных серверах.

Что нужно знать перед началом работы

- Предполагаемое время для завершения каждой процедуры: 5 минут.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Функции защиты от вредоносных программ" в разделе Антиспам и разрешения для защиты от вредоносных программ .
- Для выполнения этой процедуры можно использовать только PowerShell. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online**

или **Exchange Online Protection** .

Включение или отключение фильтрации подключений с помощью командной консоли Exchange

Чтобы полностью включить или отключить фильтрацию подключений, необходимо включить либо отключить агент фильтрации подключений. Изменения вступят в силу после перезапуска службы транспорта Microsoft Exchange. При перезапуске службы Microsoft Exchange на пограничном транспортном сервере поток обработки почты на сервере временно прерывается.

Чтобы отключить фильтрацию подключений, выполните следующую команду:

PowerShell

```
Disable-TransportAgent "Connection Filtering Agent"
```

Чтобы включить фильтрацию подключений, выполните следующую команду:

PowerShell

```
Enable-TransportAgent "Connection Filtering Agent"
```

Чтобы изменение вступило в силу, перезапустите службу транспорта Microsoft Exchange, выполнив следующую команду.

PowerShell

```
Restart-Service MSExchangeTransport
```

Как проверить, все ли получилось?

Чтобы убедиться, что фильтрация подключений включена или отключена, выполните следующую команду, чтобы проверить значение свойства **Enabled** .

PowerShell

```
Get-TransportAgent "Connection Filtering Agent" | Format-List Enabled
```

Процедуры списка блокировок IP-адресов

Эти процедуры применяются к списку блокировок IP-адресов, который настраиваются вручную. Они не применяются к поставщикам списков блокировок IP-адресов.

Используйте командлеты **IPBlockListConfig** , чтобы просмотреть и настроить, как фильтрация подключений использует список блокировок IP-адресов. Используйте командлеты **IPBlockListEntry** для просмотра и настройки IP-адресов в списке блокировок IP-адресов.

Просмотр конфигурации списка блокировок IP-адресов с помощью командной консоли Exchange

Чтобы просмотреть конфигурацию списка блокировок IP-адресов, выполните следующую команду:

```
PowerShell

Get-IPBlockListConfig | Format-List *Enabled,*Response
```

Включение или отключение списка блокировок IP-адресов с помощью командной консоли Exchange

Чтобы отключить список блокировок IP-адресов, выполните следующую команду:

```
PowerShell

Set-IPBlockListConfig -Enabled $false
```

Чтобы включить список блокировок IP-адресов, выполните следующую команду:

```
PowerShell

Set-IPBlockListConfig -Enabled $true
```

Дополнительные сведения см. в разделе Set-IPBlockListConfig.

Как проверить, все ли получилось?

Чтобы убедиться, что список заблокированных IP-адресов успешно включен или отключен, выполните следующую команду, чтобы проверить значение свойства **Enabled** .

PowerShell

```
Get-IPBlockListConfig | Format-List Enabled
```

Настройка списка блокировок IP-адресов с помощью командной консоли Exchange

Чтобы настроить список блокировок IP-адресов, используйте следующий синтаксис:

PowerShell

```
Set-IPBlockListConfig [-ExternalMailEnabled <$true | $false>] [-
InternalMailEnabled <$true | $false> -MachineEntryRejectionResponse "<Custom
response text>"] [-StaticEntryRejectionResponse "<Custom response text>"]
```

В этом примере список блокировок IP-адресов настраивается со следующими параметрами:

- Список блокировок IP-адресов фильтрует входящие подключения с внутреннего и внешнего почтовых серверов. По умолчанию подключения фильтруются только с внешних почтовых серверов (*для ExternalMailEnabled* задано значение `$true`, а *для InternalMailEnabled* — значение `$false`). Подключения от внешних партнеров с проверкой подлинности и без нее считаются внешними.

- Настраиваемый текст ответа для подключений, отфильтрованных по IP-адресам, которые были автоматически добавлены в список блокировок IP-адресов функцией репутации отправителя агента анализа протоколов, имеет значение "Подключение с IP-адреса {0} было отклонено репутацией отправителя".

- Настраиваемый текст ответа для подключений, которые были отфильтрованы по IP-адресам, которые были добавлены в список блокировок IP-адресов, имеет значение "Подключение с IP-адреса {0} было отклонено фильтрацией подключений".

PowerShell

```
Set-IPBlockListConfig -InternalMailEnabled $true -
MachineEntryRejectionResponse "Connection from IP address {0} was rejected
by sender reputation." -StaticEntryRejectionResponse "Connection from IP
address {0} was rejected by connection filtering."
```

Дополнительные сведения см. в разделе Set-IPBlockListConfig.

Как проверить, все ли получилось?

Чтобы убедиться, что список блокировок IP-адресов успешно настроен, выполните следующую команду, чтобы проверить значения свойств.

PowerShell

```
Get-IPBlockListConfig | Format-List *MailEnabled,*Response
```

Просмотр записей списка блокировок IP-адресов с помощью командной консоли Exchange

Чтобы просмотреть все записи списка блокировок IP-адресов, выполните следующую команду:

PowerShell

```
Get-IPBlockListEntry
```

Обратите внимание, что каждая запись списка блокировок IP-адресов определяется целым числом. Целое число удостоверения назначается в порядке возрастания при добавлении записей в список блокировок IP-адресов и список разрешенных IP-адресов.

Чтобы просмотреть определенную запись списка блокировок IP-адресов, используйте следующий синтаксис:

PowerShell

```
Get-IPBlockListEntry <-Identity IdentityInteger | -IPAddress IPAddress>
```

Например, чтобы просмотреть запись списка блокировок IP-адресов, содержащую IP-адрес 192.168.1.13, выполните следующую команду:

PowerShell

```
Get-IPBlockListEntry -IPAddress 192.168.1.13
```

Дополнительные сведения см. в разделе Get-IPBlockListEntry.

> **Примечание**
>
> При использовании параметра *IPAddress* результирующая запись списка блокировок IP-адресов может быть отдельным IP-адресом, диапазоном IP-адресов или IP-адресом междоменной маршрутизации (CIDR). Чтобы использовать параметр *Identity* , укажите целочисленное значение, присвоенное записи списка блокировок IP-адресов.

Добавление записей списка блокировок IP-адресов с помощью командной консоли Exchange

Чтобы добавить записи списка блокировок IP-адресов, используйте следующий синтаксис:

PowerShell

```
Add-IPBlockListEntry <-IPAddress IPAddress | -IPRange IP range or CIDR IP>
[-ExpirationTime <DateTime>] [-Comment "<Descriptive Comment>"]
```

В этом примере добавляется запись списка блокировок IP-адресов для диапазона IP-адресов от 192.168.1.10 до 192.168.1.15 и настраивается срок действия записи списка блокировок IP-адресов 4 июля 2018 г. в 15:00.

PowerShell

```
Add-IPBlockListEntry -IPRange 192.168.1.10-192.168.1.15 -ExpirationTime
"7/4/2018 15:00"
```

Дополнительные сведения см. в разделе Add-IPBlockListEntry.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно добавили запись списка блокировок IP-адресов, выполните следующую команду и убедитесь, что отображается новая запись списка блокировок IP-адресов.

```
```

PowerShell

```
Get-IPBlockListEntry
```

Удаление записей списка блокировок IP-адресов с помощью командной консоли Exchange

Чтобы удалить записи списка блокировок IP-адресов, используйте следующий синтаксис:

PowerShell

```
Remove-IPBlockListEntry <IdentityInteger>
```

В этом примере удаляется запись списка блокировок IP-адресов со значением *Identity* 3.

PowerShell

```
Remove-IPBlockListEntry 3
```

В этом примере удаляется запись списка блокировок IP-адресов, содержащая IP-адрес 192.168.1.12, без использования целочисленного значения *Identity* . Обратите внимание, что запись списка блокировок IP-адресов может быть отдельным IP-адресом или диапазоном IP-адресов.

PowerShell

```
Get-IPBlockListEntry -IPAddress 192.168.1.12 | Remove-IPBlockListEntry
```

Дополнительные сведения см. в разделе Remove-IPBlockListEntry.

Как проверить, все ли получилось?

Чтобы убедиться, что запись списка блокировок IP-адресов успешно удалена, выполните следующую команду и убедитесь, что удаленная запись списка блокировок IP-адресов удалена.

PowerShell

```
Get-IPBlockListEntry
```

Процедуры поставщика списка блокировок IP-адресов

Эти процедуры применяются к поставщикам списков блокировок IP-адресов. Они не применяются к списку блокировок IP-адресов.

Используйте командлеты **IPBlockListProvidersConfig** , чтобы просмотреть и настроить, как фильтрация подключений использует все поставщики списков блокировок IP-адресов. Используйте командлеты **IPBlockListProvider** для просмотра, настройки и тестирования поставщиков списков блокировок IP-адресов.

Использование командной консоли Exchange для просмотра конфигурации всех поставщиков списков блокировок IP-адресов

Чтобы просмотреть, как фильтрация подключений использует все поставщики списков блокировок IP-адресов, выполните следующую команду:

PowerShell

```
Get-IPBlockListProvidersConfig | Format-List *Enabled,Bypassed*
```

Дополнительные сведения см. в разделе Get-IPBlockListProvidersConfig.

Включение или отключение всех поставщиков списков блокировок IP-адресов с помощью командной консоли Exchange

Чтобы отключить все поставщики списков блокировок IP-адресов, выполните следующую команду:

PowerShell

```
Set-IPBlockListProvidersConfig -Enabled $false
```

Чтобы включить все поставщики списков блокировок IP-адресов, выполните следующую команду:

PowerShell

```
Set-IPBlockListProvidersConfig -Enabled $true
```

Дополнительные сведения см. в разделе Set-IPBlockListProvidersConfig.

Как проверить, все ли получилось?

Чтобы убедиться, что вы включили или отключили все поставщики списков блокировок IP-адресов, выполните следующую команду, чтобы проверить значение свойства **Enabled** :

PowerShell

```
Get-IPBlockListProvidersConfig | Format-List Enabled
```

Настройка всех поставщиков списков блокировок IP-адресов с помощью командной консоли Exchange

Чтобы настроить, как фильтрация подключений использует все поставщики списков блокировок IP-адресов, используйте следующий синтаксис:

PowerShell

```
Set-IPBlockListProvidersConfig [-BypassedRecipients
<recipient1,recipient2...>] [-ExternalMailEnabled <$true | $false>] [-
InternalMailEnabled <$true | $false>]
```

В этом примере настраивается для всех поставщиков списков блокировок IP-адресов со следующими параметрами:

- Поставщики списка блокировок IP-адресов фильтруют входящие подключения с внутреннего и внешнего почтовых серверов. По умолчанию подключения фильтруются только с внешних почтовых серверов (*для ExternalMailEnabled* задано значение `$true`, а *для InternalMailEnabled* — значение `$false`). Подключения от внешних партнеров с проверкой подлинности и без нее считаются внешними.

- Сообщения, отправляемые внутренним получателям и michelle@fabrikam.com исключенные chris@fabrikam.com из фильтрации поставщиками списков блокировок IP-адресов. Обратите внимание, что если вы хотите добавить получателей в список, не затрагивая существующих получателей, используйте синтаксис `@{Add="<recipient1>","<recipient2>"...}`.

PowerShell

```
Set-IPBlockListProvidersConfig -BypassedRecipients
chris@fabrikam.com,michelle@fabrikam.com -InternalMailEnabled $true
```

Дополнительные сведения см. в разделе Set-IPBlockListProvidersConfig.

Как проверить, все ли получилось?

Чтобы убедиться, что все поставщики списков блокировок IP-адресов успешно настроены, выполните следующую команду, чтобы проверить значения свойств:

PowerShell

```
Get-IPBlockListProvidersConfig | Format-List *MailEnabled,Bypassed*
```

Просмотр поставщиков списков блокировок IP-адресов с помощью командной консоли Exchange

Чтобы просмотреть сводный список всех поставщиков списка блокировок IP-адресов, выполните следующую команду:

PowerShell

```
Get-IPBlockListProvider
```

Чтобы просмотреть сведения об определенном поставщике, используйте следующий синтаксис.

PowerShell

```
Get-IPBlockListProvider <IPBlockListProviderIdentity>
```

В этом примере показаны сведения о поставщике списка блокировок IP-адресов Contoso.

PowerShell

```
Get-IPBlockListProvider "Contoso IP blocklist Provider" | Format-List
Name,Enabled,Priority,LookupDomain,*Match,*Response
```

Дополнительные сведения см. в разделе Get-IPBlockListProvider.

Добавление поставщика списка блокировок IP-адресов с помощью командной консоли Exchange

Чтобы добавить поставщик списка блокировок IP-адресов, используйте следующий синтаксис:

PowerShell

```
Add-IPBlockListProvider -Name "<Descriptive Name>" -LookupDomain <FQDN> [-
Priority <Integer>] [-Enabled <$true | $false>] [-AnyMatch <$true | $false>]
[-BitmaskMatch <IPAddress>] [-IPAddressesMatch
<IPAddressStatusCode1,IPAddressStatusCode2...>] [-RejectionResponse "<Custom
Text>"]
```

В этом примере создается поставщик списка блокировок IP-адресов с именем Contoso IP-поставщик списка блокировок со следующими параметрами:

- **Полное доменное имя для использования поставщика**: rbl.contoso.com
- **Код битовой маски для использования от поставщика**: 127.0.0.1

PowerShell

```
Add-IPBlockListProvider -Name "Contoso IP blocklist Provider" -LookupDomain
rbl.contoso.com -BitmaskMatch 127.0.0.1
```

> ⓘ **Примечание**
>
> При добавлении нового поставщика списка блокировок IP-адресов он включается по умолчанию (значение *Включено* равно `$true`), а значение приоритета увеличивается (первая запись имеет значение *Priority* 1).

Дополнительные сведения см. в разделе Add-IPBlockListProvider.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно добавили поставщик списка блокировок IP-адресов, выполните следующую команду и убедитесь, что отображается новый поставщик списка блокировок IP-адресов.

PowerShell

```
Get-IPBlockListProvider
```

Включение или отключение поставщика списка блокировок IP-адресов с помощью командной консоли Exchange

Чтобы включить или отключить определенный поставщик списка блокировок IP-адресов, используйте следующий синтаксис:

```
PowerShell

Set-IPBlockListProvider <IPBlockListProviderIdentity> -Enabled <$true | $false>
```

В этом примере отключается поставщик с именем Contoso IP-списка блокировки.

```
PowerShell

Set-IPBlockListProvider "Contoso IP blocklist Provider" -Enabled $false
```

В этом примере включается поставщик списка блокировок IP-адресов Contoso.

```
PowerShell

Set-IPBlockListProvider "Contoso IP blocklist Provider" -Enabled $true
```

Дополнительные сведения см. в разделе Set-IPBlockListProvider.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно включили или отключили поставщик списка блокировок IP-адресов, выполните следующую команду, чтобы проверить значение свойства **Enabled** :

```
PowerShell

Get-IPBlockListProvider | Format-Table -Auto Name,LookupDomain,Priority,Enabled
```

Настройка поставщика списка блокировок IP-адресов с помощью командной консоли Exchange

Параметры конфигурации, доступные в командлете **Set-IPBlockListProvider** , идентичны параметрам командлета **Add-IPBlockListProvider** .

Чтобы настроить существующий поставщик списка блокировок IP-адресов, используйте следующий синтаксис:

PowerShell

```
Set-IPBlockListProvider <IPBlockListProviderIdentity> -Name "<Descriptive
Name>" -LookupDomain <FQDN> [-Priority <Integer>] [-AnyMatch <$true |
$false>] [-BitmaskMatch <IPAddress>] [-IPAddressesMatch
<IPAddressStatusCode1,IPAddressStatusCode2...>] [-RejectionResponse "<Custom
Text>"]
```

Например, чтобы добавить код состояния IP-адреса 127.0.0.1 в список существующих кодов состояния для поставщика с именем Поставщик списка блокировок IP-адресов Contoso, выполните следующую команду:

PowerShell

```
Set-IPBlockListProvider "Contoso IP blocklist Provider" -IPAddressesMatch
@{Add="127.0.0.1"}
```

Дополнительные сведения см. в разделе Set-IPBlockListProvider.

Как проверить, все ли получилось?

Чтобы убедиться, что поставщик списка блокировок IP-адресов успешно настроен, выполните следующую команду, чтобы проверить значения свойств. Обязательно замените *<IPBlockListProviderIdentity>* именем поставщика списка блокировок IP-адресов.

PowerShell

```
Get-IPBlockListProvider <IPBlockListProviderIdentity> | Format-List
```

Использование командной консоли Exchange для тестирования поставщика списка блокировок IP-адресов

Чтобы протестировать поставщик списка блокировок IP-адресов, используйте следующий синтаксис:

PowerShell

```
Test-IPBlockListProvider <IPBlockListProviderIdentity> -IPAddress
<IPAddressToTest>
```

В этом примере проверяется поставщик списка ip-адресов Contoso, найдите IP-адрес 192.168.1.1.

PowerShell

```
Test-IPBlockListProvider "Contoso IP blocklist Provider" -IPAddress
192.168.1.1
```

Дополнительные сведения см. в разделе Test-IPBlockListProvider.

Удаление поставщика списка блокировок IP-адресов с помощью командной консоли Exchange

Чтобы удалить поставщик списка блокировок IP-адресов, используйте следующий синтаксис:

PowerShell

```
Remove-IPBlockListProvider <IPBlockListProviderIdentity>
```

В этом примере удаляется поставщик списка блокировок IP-адресов Contoso.

PowerShell

```
Remove-IPBlockListProvider "Contoso IP blocklist Provider"
```

Дополнительные сведения см. в разделе Remove-IPBlockListProvider.

Как проверить, все ли получилось?

Чтобы убедиться, что поставщик списка блокировок IP-адресов успешно удален, выполните следующую команду и убедитесь, что удаленный поставщик списка блокировок IP-адресов удален.

PowerShell

```
Get-IPBlockListProvider
```

Процедуры списка разрешенных IP-адресов

Эти процедуры применяются к списку разрешенных IP-адресов, который настраиваются вручную. Они не применяются к поставщикам списка разрешенных IP-адресов.

Используйте командлеты **IPAllowListConfig** , чтобы просмотреть и настроить, как фильтрация подключений использует список разрешенных IP-адресов. Используйте командлеты **IPAllowListEntry** для просмотра и настройки IP-адресов в списке разрешенных IP-адресов.

Просмотр конфигурации списка разрешенных IP-адресов с помощью командной консоли Exchange

Чтобы просмотреть конфигурацию списка разрешенных IP-адресов, выполните следующую команду.

PowerShell

```
Get-IPAllowListConfig | Format-List *Enabled
```

Дополнительные сведения см. в разделе Get-IPAllowListConfig.

Включение или отключение списка разрешенных IP-адресов с помощью командной консоли Exchange

Чтобы отключить список разрешенных IP-адресов, выполните следующую команду:

PowerShell

```
Set-IPAllowListConfig -Enabled $false
```

Чтобы включить список разрешенных IP-адресов, выполните следующую команду:

PowerShell

```
Set-IPAllowListConfig -Enabled $true
```

Как проверить, все ли получилось?

Чтобы убедиться, что список разрешенных IP-адресов успешно включен или отключен, выполните следующую команду, чтобы проверить значение свойства **Enabled** :

```
PowerShell

Get-IPAllowListConfig | Format-List Enabled
```

Настройка списка разрешенных IP-адресов с помощью командной консоли Exchange

Чтобы настроить список разрешенных IP-адресов, используйте следующий синтаксис:

```
PowerShell

Set-IPAllowListConfig [-ExternalMailEnabled <$true | $false>] [-
InternalMailEnabled <$true | $false>
```

В этом примере настраивается список разрешенных IP-адресов для фильтрации входящих подключений с внутреннего и внешнего почтовых серверов. По умолчанию подключения фильтруются только с внешних почтовых серверов (*для ExternalMailEnabled* задано значение `$true`, а *для InternalMailEnabled* — значение `$false`). Подключения от внешних партнеров с проверкой подлинности и без нее считаются внешними.

```
PowerShell

Set-IPAllowListConfig -InternalMailEnabled $true
```

Дополнительные сведения см. в разделе Set-IPAllowListConfig.

Как проверить, все ли получилось?

Чтобы убедиться, что список разрешенных IP-адресов успешно настроен, выполните следующую команду, чтобы проверить значения свойств:

```
PowerShell

Get-IPAllowListConfig | Format-List *MailEnabled
```

Просмотр записей списка разрешенных IP-адресов с помощью командной консоли Exchange

Чтобы просмотреть все записи списка разрешенных IP-адресов, выполните следующую команду:

```
PowerShell

Get-IPAllowListEntry
```

Обратите внимание, что каждая запись списка разрешенных IP-адресов определяется целым числом. Целое число удостоверения назначается в порядке возрастания при добавлении записей в список блокировок IP-адресов и список разрешенных IP-адресов.

Чтобы просмотреть определенную запись списка разрешенных IP-адресов, используйте следующий синтаксис:

```
PowerShell

Get-IPAllowListEntry <-Identity IdentityInteger | -IPAddress IPAddress>
```

Например, чтобы просмотреть запись списка разрешенных IP-адресов, содержащую IP-адрес 192.168.1.13, выполните следующую команду:

```
PowerShell

Get-IPAllowListEntry -IPAddress 192.168.1.13
```

Дополнительные сведения см. в разделе Get-IPAllowListEntry.

> ⓘ **Примечание**
>
> При использовании параметра *IPAddress* результирующая запись списка разрешенных IP-адресов может быть отдельным IP-адресом, диапазоном IP-адресов или IP-адресом междоменной маршрутизации (CIDR). Чтобы использовать параметр *Identity* , укажите целочисленное значение, присвоенное записи списка разрешенных IP-адресов.

Добавление записей списка разрешенных IP-адресов с помощью командной консоли Exchange

Чтобы добавить записи списка разрешенных IP-адресов, используйте следующий синтаксис:

```
PowerShell

Add-IPAllowListEntry <-IPAddress IPAddress | -IPRange IP range or CIDR IP>
[-ExpirationTime <DateTime>] [-Comment "<Descriptive Comment>"]
```

В этом примере добавляется запись списка разрешенных IP-адресов для диапазона IP-адресов от 192.168.1.10 до 192.168.1.15 и настраивается срок действия записи списка разрешенных IP-адресов 4 июля 2018 г. в 15:00.

```
PowerShell

Add-IPAllowListEntry -IPRange 192.168.1.10-192.168.1.15 -ExpirationTime
"7/4/2018 15:00"
```

Дополнительные сведения см. в разделе Add-IPAllowListEntry.

Как проверить, все ли получилось?

Чтобы убедиться, что запись списка разрешенных IP-адресов успешно добавлена, выполните следующую команду и убедитесь, что отображается новая запись списка разрешенных IP-адресов.

```
PowerShell

Get-IPAllowListEntry
```

Удаление записей списка разрешенных IP-адресов с помощью командной консоли Exchange

Чтобы удалить записи списка разрешенных IP-адресов, используйте следующий синтаксис:

```
PowerShell

Remove-IPAllowListEntry <IdentityInteger>
```

В этом примере удаляется запись списка разрешенных IP-адресов со значением *Identity* 3.

```
```

PowerShell

```
Remove-IPAllowListEntry 3
```

В этом примере удаляется запись списка разрешенных IP-адресов, содержащая IP-адрес 192.168.1.12, без использования целочисленного значения *Identity* . Обратите внимание, что запись списка разрешенных IP-адресов может быть отдельным IP-адресом или диапазоном IP-адресов.

PowerShell

```
Get-IPAllowListEntry -IPAddress 192.168.1.12 | Remove-IPAllowListEntry
```

Дополнительные сведения см. в разделе Remove-IPAllowListEntry.

Как проверить, все ли получилось?

Чтобы убедиться, что запись списка разрешенных IP-адресов успешно удалена, выполните следующую команду и убедитесь, что удаленная запись списка ip-адресов удалена.

PowerShell

```
Get-IPAllowListEntry
```

Процедуры поставщика списка разрешенных IP-адресов

Эти процедуры применяются к поставщикам списка разрешенных IP-адресов. Они не применяются к списку разрешенных IP-адресов.

Используйте командлеты **IPAllowListProvidersConfig** , чтобы просмотреть и настроить, как фильтрация подключений использует все поставщики списка разрешенных IP-адресов. Используйте командлеты **IPAllowListProvider** для просмотра, настройки и тестирования поставщиков списка разрешенных IP-адресов.

Использование командной консоли Exchange для просмотра конфигурации всех поставщиков списка разрешенных IP-адресов

Чтобы просмотреть, как фильтрация подключений использует все поставщики списка разрешенных IP-адресов, выполните следующую команду:

```
PowerShell

Get-IPAllowListProvidersConfig | Format-List *Enabled
```

Дополнительные сведения см. в разделе Get-IPAllowListProvidersConfig.

Включение или отключение всех поставщиков списка разрешенных IP-адресов с помощью командной консоли Exchange

Чтобы отключить все поставщики списка разрешенных IP-адресов, выполните следующую команду:

```
PowerShell

Set-IPAllowListProvidersConfig -Enabled $false
```

Чтобы включить все поставщики списка разрешенных IP-адресов, выполните следующую команду:

```
PowerShell

Set-IPAllowListProvidersConfig -Enabled $true
```

Дополнительные сведения см. в разделе Set-IPAllowListProvidersConfig.

Как проверить, все ли получилось?

Чтобы убедиться, что вы включили или отключили все поставщики списка разрешенных IP-адресов, выполните следующую команду, чтобы проверить значение свойства **Enabled** :

```
PowerShell

Get-IPAllowListProvidersConfig | Format-List Enabled
```

Настройка всех поставщиков списка разрешенных IP-адресов с помощью командной консоли Exchange

Чтобы настроить, как фильтрация подключений использует все поставщики списка разрешенных IP-адресов, используйте следующий синтаксис:

```
PowerShell

Set-IPAllowListProvidersConfig [-ExternalMailEnabled <$true | $false>] [-
InternalMailEnabled <$true | $false>]
```

В этом примере все поставщики списка разрешенных IP-адресов настраивают фильтрацию входящих подключений с внутреннего и внешнего почтовых серверов. По умолчанию подключения фильтруются только с внешних почтовых серверов (*для ExternalMailEnabled* задано значение `$true`, а *для InternalMailEnabled* — значение `$false`). Подключения от внешних партнеров с проверкой подлинности и без нее считаются внешними.

```
PowerShell

Set-IPAllowListProvidersConfig -InternalMailEnabled $true
```

Дополнительные сведения см. в разделе Set-IPAllowListProvidersConfig.

Как проверить, все ли получилось?

Чтобы убедиться, что все поставщики списка разрешенных IP-адресов настроены успешно, выполните следующую команду, чтобы проверить значения свойств:

```
PowerShell

Get-IPAllowListProvidersConfig | Format-List *MailEnabled
```

Использование командной консоли Exchange для просмотра поставщиков списка разрешенных IP-адресов

Чтобы просмотреть сводный список всех поставщиков списка разрешенных IP-адресов, выполните следующую команду.

```
PowerShell

Get-IPAllowListProvider
```

Чтобы просмотреть сведения об определенном поставщике, используйте следующий синтаксис.

PowerShell

```
Get-IPAllowListProvider <IPAllowListProviderIdentity>
```

В этом примере показаны сведения о поставщике с именем Contoso IP-список разрешенных поставщиков.

PowerShell

```
Get-IPAllowListProvider "Contoso IP allowlist Provider" | Format-List
Name,Enabled,Priority,LookupDomain,*Match
```

Дополнительные сведения см. в разделе Get-IPAllowListProvider.

Добавление поставщика списка разрешенных IP-адресов с помощью командной консоли Exchange

Чтобы добавить поставщик списка разрешенных IP-адресов, используйте следующий синтаксис:

PowerShell

```
Add-IPAllowListProvider -Name "<Descriptive Name>" -LookupDomain <FQDN> [-
Priority <Integer>] [-Enabled <$true | $false>] [-AnyMatch <$true | $false>]
[-BitmaskMatch <IPAddress>] [-IPAddressesMatch
<IPAddressStatusCode1,IPAddressStatusCode2...>]
```

В этом примере создается поставщик списка разрешенных IP-адресов с именем "Поставщик списка разрешенных IP-адресов Contoso" со следующими параметрами:

- **Полное доменное имя для использования поставщика**: allow.contoso.com
- **Код битовой маски для использования от поставщика**: 127.0.0.1

PowerShell

```
Add-IPAllowListProvider -Name "Contoso IP allowlist Provider" -LookupDomain
allow.contoso.com -BitmaskMatch 127.0.0.1
```

> ⓘ **Примечание**
>
> При добавлении нового поставщика списка разрешенных IP-адресов он включается по умолчанию (значение *Включено* равно `$true`), а значение приоритета увеличивается (первая запись имеет значение *Priority* 1).

Дополнительные сведения см. в разделе Add-IPAllowListProvider.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно добавили поставщик списка разрешенных IP-адресов, выполните следующую команду и убедитесь, что отображается новый поставщик списка разрешенных IP-адресов.

PowerShell

```
Get-IPAllowListProvider
```

Включение или отключение поставщика списка разрешенных IP-адресов с помощью командной консоли Exchange

Чтобы включить или отключить определенный поставщик списка разрешенных IP-адресов, используйте следующий синтаксис:

PowerShell

```
Set-IPAllowListProvider <IPAllowListProviderIdentity> -Enabled <$true |
$false>
```

В этом примере отключается поставщик списка разрешенных IP-адресов Contoso.

PowerShell

```
Set-IPAllowListProvider "Contoso IP allowlist Provider" -Enabled $false
```

В этом примере включается поставщик с именем Contoso IP-список разрешенных поставщиков.

PowerShell

```
Set-IPAllowListProvider "Contoso IP allowlist Provider" -Enabled $true
```

Дополнительные сведения см. в разделе Set-IPAllowListProvider.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно включили или отключили поставщик списка разрешенных IP-адресов, выполните следующую команду, чтобы проверить значение свойства **Enabled** :

PowerShell

```
Get-IPAllowListProvider | Format-Table -Auto
Name,LookupDomain,Priority,Enabled
```

Настройка поставщика списка разрешенных IP-адресов с помощью командной консоли Exchange

Параметры конфигурации, доступные в командлете **Set-IPAllowListProvider** , идентичны параметрам командлета **Add-IPAllowListProvider** .

Чтобы настроить существующий поставщик списка разрешенных IP-адресов, используйте следующий синтаксис:

PowerShell

```
Set-IPAllowListProvider <IPAllowListProviderIdentity> -Name "<Descriptive
Name>" -LookupDomain <FQDN> [-Priority <Integer>] [-AnyMatch <$true |
$false>] [-BitmaskMatch <IPAddress>] [-IPAddressesMatch
<IPAddressStatusCode1,IPAddressStatusCode2...>]
```

Например, чтобы добавить код состояния IP-адреса 127.0.0.1 в список существующих кодов состояния для поставщика с именем Поставщик списка разрешенных IP-адресов Contoso, выполните следующую команду:

PowerShell

```
Set-IPAllowListProvider "Contoso IP allowlist Provider" -IPAddressesMatch
@{Add="127.0.0.1"}
```

Дополнительные сведения см. в разделе Set-IPAllowListProvider.

Как проверить, все ли получилось?

Чтобы убедиться, что поставщик списка разрешенных IP-адресов успешно настроен, выполните следующую команду. Обязательно замените *<IPAllowListProviderIdentity>* именем поставщика списка разрешенных IP-адресов.

```
PowerShell

Get-IPAllowListProvider <IPAllowListProviderIdentity> | Format-List
```

Использование командной консоли Exchange для тестирования поставщика списка разрешенных IP-адресов

Чтобы протестировать поставщик списка разрешенных IP-адресов, используйте следующий синтаксис:

```
PowerShell

Test-IPAllowListProvider <IPAllowListProviderIdentity> -IPAddress
<IPAddressToTest>
```

В этом примере проверяется поставщик списка разрешенных IP-адресов Contoso путем поиска IP-адреса 192.168.1.1.

```
PowerShell

Test-IPAllowListProvider "Contoso IP allowlist Provider" -IPAddress
192.168.1.1
```

Дополнительные сведения см. в разделе Test-IPAllowListProvider.

Удаление поставщика списка разрешенных IP-адресов с помощью командной консоли Exchange

Чтобы удалить поставщик списка разрешенных IP-адресов, используйте следующий синтаксис:

```
PowerShell

Remove-IPAllowListProvider <IPAllowListProviderIdentity>
```

В этом примере удаляется поставщик списка разрешенных IP-адресов с именем Contoso IP allowlist Provider.

PowerShell

```
Remove-IPAllowListProvider "Contoso IP allowlist Provider"
```

Дополнительные сведения см. в разделе Remove-IPAllowListProvider.

Как проверить, все ли получилось?

Чтобы убедиться, что поставщик списка разрешенных IP-адресов успешно удален, выполните следующую команду и убедитесь, что удаленный поставщик списка IP-адресов удален.

PowerShell

```
Get-IPAllowListProvider
```

Фильтрация получателей на пограничных транспортных серверах в Exchange Server

Статья • 04.04.2023

Фильтрация получателей — это функция защиты от нежелательной почты в Exchange Server, которая использует заголовок **RCPT TO** SMTP для определения того, какие действия (если таковые имеются) выполнять с входящим сообщением. Фильтрация получателей выполняется агентом фильтра получателей и практически не изменяется с Exchange Server 2010 года.

Агент фильтра получателей блокирует сообщения в соответствии с характеристиками получателя в организации. Агент фильтра получателей может предотвратить доставку сообщений в следующих сценариях.

- **Несуществующие получатели**. Вы можете запретить доставку получателям, которых нет в адресной книге организации. Например, может потребоваться остановить доставку в часто используемые имена учетных записей, например administrator@contoso.com или support@contoso.com.

- **Группы рассылки с ограниченным доступом**. Вы можете запретить доставку электронной почты в группы рассылки, которые должны использоваться только внутренними пользователями.

- **Почтовые ящики, которые никогда не должны получать сообщения из Интернета**. Вы можете запретить доставку почты Из Интернета в определенный почтовый ящик или псевдоним, который обычно используется в организации, например служба технической поддержки.

Агент фильтрации получателей обрабатывает получателей из одного или обоих следующих источников данных:

- **Список заблокированных получателей**. Определяемый администратором список получателей, которые никогда не должны получать сообщения из Интернета.

- **Подстановка получателей**: запрашивает Active Directory, чтобы убедиться, что получатель существует в организации. На пограничном транспортном сервере для поиска получателей требуется доступ к сведениям Active Directory, предоставляемым EdgeSync локальному экземпляру служб Active

Directory облегченного доступа к каталогу (AD LDS). Дополнительную информацию см. в статье Edge Subscriptions.

При включении агента фильтрации получателей над входящими сообщениями в зависимости от характеристик получателей выполняется одно из следующих действий. Эти получатели указываются заголовком **RCPT TO** .

- Если входящее сообщение содержит получателя, находящегося в списке "Заблокированный получатель", сервер Exchange server отправляет `550 5.1.1 User unknown` на отправляющий сервер ошибку сеанса SMTP.
- Если входящее сообщение содержит получателя, который не совпадает ни с какими получателями в поиске получателей, сервер Exchange server отправляет `550 5.1.1 User unknown` на отправляющий сервер ошибку сеанса SMTP.
- Если получатель отсутствует в списке "Блокировка получателей", а получатель найден в поиске получателей, сервер Exchange server отправляет SMTP-ответ на отправляющий сервер, а следующий агент защиты от нежелательной почты `250 2.1.5 Recipient OK` в цепочке обрабатывает сообщение.

> ⓘ **Примечание**
>
> Хотя агент фильтра получателей доступен на серверах почтовых ящиков, его не следует настраивать. Если при фильтрации получателей на сервере почтовых ящиков в сообщении обнаруживается по крайней мере один недопустимый или заблокированный получатель, сообщение отклоняется. Агент фильтра получателей активируется, когда вы устанавливаете агенты защиты от спама на сервере почтовых ящиков, но не блокирует получателей. Дополнительные сведения см. в разделе **Включение функций защиты от нежелательной почты на серверах почтовых ящиков**.

Настройка поиска получателей

Один из самых эффективных способов уменьшить объем спама — проверять получателей до приема входящих сообщений из Интернета. Вы включаете блокировку сообщений, отправляемых получателям, которые не существуют в организации Exchange, и блокировку определенных получателей с помощью командлета **Set-RecipientFilterConfig** в командной консоли Exchange.

Возможность замедления отклика

Функция поиска получателей позволяет серверу-отправителю определять, действителен ли адрес электронной почты. Как упоминалось ранее, если получатель входящего сообщения является известным получателем, сервер Exchange отправляет `250 2.1.5 Recipient OK` обратно SMTP-ответ на отправляющий сервер. Эта функция обеспечивает идеальную среду для *атаки на сбор данных каталога*, когда спамер использует автоматизированную программу для сбора адресов электронной почты, возвращающих `250 2.1.5 Recipient OK` SMTP-ответ.

Для борьбы с атаками на сбор данных каталогов Exchange включает функции tarpitting. Эта функция увеличивает расходы пользователя на отправку спама.

Если тарпитирование не настроено, сервер Exchange Server немедленно возвращает отправителю ошибку `550 5.1.1 User unknown` сеанса SMTP, если получатель не находится в поиске получателей. Кроме того, если тарпитирование настроено, сервер Exchange ожидает указанное количество секунд, прежде чем вернет ошибку `550 5.1.1 User unknown` . Такая пауза в SMTP-сеансе затрудняет автоматизацию атаки для сбора сведений каталога и делает ее менее выгодной для злонамеренного пользователя. По умолчанию для соединителей получения настроенная задержка равна 5 секундам.

Чтобы настроить задержку до того, как SMTP возвращает ошибку `550 5.1.1 User unknown` , необходимо задать интервал тарпитирования с помощью параметра *TarpitInterval* в **командлете Set-ReceiveConnector** . Дополнительную информацию см. в разделе Регулирование количества сообщений на соединителях получения.

Несколько пространств имен

Агент фильтрации получателей выполняет поиск получателей только для обслуживаемых доменов. Если организация принимает и пересылает сообщения от имени другого домена, который настроен в качестве домена внешней ретрансляции или внутренней ретрансляции, то агент фильтрации получателей не выполняет поиск получателя среди получателей в этих доменах. Однако если получатель указан в черном списке получателей, то он также блокируется агентом фильтрации получателей.

Обратите внимание, что также можно настроить обслуживаемые домены на пограничном транспортном сервере. Если домен настроен как домен внутренней ретрансляции или внешней ретрансляции, то агент фильтрации получателей на

пограничных транспортных серверах также выполняет поиск среди получателей в этих доменах.

Защита от вредоносных программ в Exchange Server

Статья • 04.04.2023

Защита от вредоносных программ в Exchange Server 2016 г. помогает бороться с вирусами и шпионским ПО в среде обмена сообщениями электронной почты. *Вирусы* заражают другие программы и данные, а также распространяются по компьютеру в поисках программ, которые можно заразить. *Программы-шпионы* собирают персональные данные (например, данные для входа) и отправляют их своему автору.

Защита от вредоносных программ в Exchange Server была введена в Exchange 2013 и предоставляется агентом транспорта с именем Вредоносный агент. Агент сканирует сообщения, когда они проходят через транспортную службу на сервере почтовых ящиков. Фильтрация вредоносных программ настраивается с помощью:

- **Политики защиты от вредоносных программ**. Укажите входящие и исходящие параметры сканирования и уведомлений для фильтрации вредоносных программ. Существует политика по умолчанию, которая применяется ко всем получателям в организации Exchange, и вы можете создать дополнительные политики, которые применяются в определенном порядке.

- **Параметры сервера защиты от вредоносных программ**. Укажите ошибки и действия повтора, а также параметры обновления обработчика и определения для фильтрации вредоносных программ. Агент защиты от вредоносных программ каждый час получает доступ к Интернету через TCP-порт 80 (HTTP), чтобы проверить наличие обновлений подсистемы и определений.

- **Сценарии защиты от вредоносных программ**. Включите или отключите фильтрацию вредоносных программ на сервере, а также вручную скачивание обновлений подсистемы и определений.

Процедуры, связанные с фильтрацией вредоносных программ, см. в разделе Процедуры защиты от вредоносных программ в Exchange Server. Дополнительные сведения о функциях защиты от нежелательной Exchange Server см. в разделе Защита от нежелательной Exchange Server.

Политики защиты от вредоносных программ

Политики защиты от вредоносных программ управляют параметрами действий и уведомлений при обнаружении вредоносных программ. Ниже перечислены важные параметры политик защиты от вредоносных программ.

- **Действие**. Указывает, что следует делать, если сообщение содержит вредоносные программы. Доступны следующие варианты:
  - Удалите сообщение (это значение по умолчанию).
  - Замените все вложения текстовым файлом, содержащим этот текст по умолчанию:

    > "В одном или нескольких вложениях этого сообщения электронной почты обнаружены вредоносные программы. Все вложения удалены".

  - Заменить все вложения на текстовый файл с указанным вами текстом.
- **Уведомления**. Если политика защиты от вредоносных программ настроена для удаления сообщений, вы можете выбрать, следует ли отправлять уведомление отправителю. Отправка уведомлений может зависеть от того, является ли отправитель внутренним или внешним. По умолчанию сообщение с уведомлением обладает следующими свойствами:
  - **С**: Postmaster postmaster@ <*defaultdomain.com*>
  - **Тема**: невозможно доставить сообщение
  - **Текст сообщения**: Это сообщение автоматически создано программой доставки почты. Ваше электронное сообщение не было доставлено получателям, так как в нем обнаружены вредоносные программы".

  Вы можете настраивать свойства сообщений для внутренних и внешних уведомлений. Вы также можете указывать дополнительных получателей (администраторов), которые будут получать уведомления о недоставленных сообщениях от внутренних или внешних отправителей.
- **Фильтры получателей**. Для пользовательских политик защиты от вредоносных программ можно указать условия и исключения получателей, которые определяют, к кому применяется политика. Для условий и исключений можно использовать следующие свойства:
  - по получателю;
  - по обслуживаемому домену;

- по членству в группе.

  Условие или исключение можно использовать только один раз, но оно может содержать несколько значений. Указать несколько значений в одном условии или исключении можно с помощью оператора OR (например, <*получатель1*> or <*получатель2*>). Между разными условиями и исключениями используется оператор AND (например, <*получатель1*> and <*участник группы 1*>).

- **Приоритет**. При создании нескольких настраиваемых политик защиты от вредоносных программ можно указать порядок их применения.

Сравнение политик защиты от вредоносных программ в Центре администрирования Exchange и командной консоли Exchange

Ниже перечислены основные элементы политики защиты от вредоносных программ.

- **Политика фильтрации вредоносных программ**. Указывает параметры действий и уведомлений для фильтрации вредоносных программ.

- **Правило фильтрации вредоносных программ**: указывает приоритет и фильтры получателей (к которым применяется политика) для политики фильтрации вредоносных программ.

Разница между этими двумя элементами не так заметна, если вы управляете политиками защиты от вредоносных программ с помощью Центра администрирования Exchange:

- Создавая политику защиты от вредоносных программ в Центре администрирования Exchange, на самом деле вы одновременно создаете правило фильтрации для защиты от вредоносных программ и связанную с ним политику с одинаковыми именами.

- При изменении политики защиты от вредоносных программ в EAC параметры, связанные с именем, приоритетом, включенным или отключенным фильтром и фильтрами получателей, изменяют правило фильтрации вредоносных программ. Другие настройки (параметры действий и уведомлений) меняют соответствующую политику фильтрации для защиты от вредоносных программ.

- При удалении политики защиты от вредоносных программ с помощью Центра администрирования Exchange удаляются правило и соответствующая политика фильтрации для защиты от вредоносных программ.

В командной консоли Exchange разница между политиками и правилами фильтрации для защиты от вредоносных программ очевидна. Вы управляете политиками фильтрации вредоносных программ с помощью командлетов ***-MalwareFilterPolicy** , а правила фильтрации вредоносных программ — с помощью командлетов ***-MalwareFilterRule** .

- В командной консоли Exchange сначала создается политика, а затем — правило фильтрации для защиты от вредоносных программ, указывающее политику, к которой оно применяется.

- В командной консоли Exchange параметры политики и правила фильтрации для защиты от вредоносных программ настраиваются отдельно.

- При удалении политики фильтрации для защиты от вредоносных программ с помощью командной консоли Exchange соответствующее правило не удаляется автоматически, и наоборот.

Стандартная политика защиты от вредоносных программ

На каждом сервере почтовых ящиков есть встроенная политика защиты от вредоносных программ под названием "По умолчанию" с указанными ниже свойствами.

- Политика фильтрации для защиты от вредоносных программ с именем "По умолчанию" применяется ко всем получателям в организации Exchange, даже если с ней не связано ни одного правила фильтрации для защиты от вредоносных программ (фильтрации получателей).

- Для политики с именем "По умолчанию" задано специальное значение приоритета Самый низкий, которое невозможно изменить (эта политика всегда применяется последней). Все настраиваемые политики защиты от вредоносных программ, которые вы создаете, всегда имеют более высокий приоритет, чем политика с именем Default.

- Политика с именем "По умолчанию" является стандартной (для свойства **IsDefault** задано значение `True`), и удалить стандартную политику невозможно.

Параметры сервера защиты от вредоносных программ

С помощью командлетов **Get-MalwareFilteringServer** и **Set-MalwareFilteringServer** в командной консоли Exchange можно просматривать и настраивать параметры обновления, времени ожидания и скачивания для агента защиты от вредоносных программ на сервере почтовых ящиков. Процедуры с использованием этих командлетов представлены в статьях Обход фильтрации вредоносных программ на серверах почтовых ящиков с помощью командной консоли Exchange и Настройка фильтрации вредоносных программ для сканирования сообщений, уже отсканированных службой EOP, с помощью командной консоли Exchange.

Скрипты для защиты от вредоносных программ

Exchange включает два скрипта Командная консоль Exchange, с помощью которых можно управлять фильтрацией для защиты от вредоносных программ.

- Скрипт `Disable-Antimalwarescanning.ps1` отключает агента защиты от вредоносных программ, а также обновление определений и модуля защиты от вредоносных программ на сервере почтовых ящиков.
- Скрипт `Enable-Antimalwarescanning.ps1` включает агента защиты от вредоносных программ, обновление определений и модуля защиты от вредоносных программ, а также запускает обновление модуля и определений на сервере почтовых ящиков.
- `Update-MalwareFilteringServer.ps1` вручную запускает модуль вредоносных программ и обновления определений на сервере почтовых ящиков.

Дополнительные сведения об использовании этих скриптов см . в статьях Включение или отключение фильтрации вредоносных программ на серверах почтовых ящиков с помощью командной консоли Exchange и скачивание обновлений антивредоносного ПО и определений.

Параметры защиты от вредоносных программ в Exchange Server

В приведенном ниже списке перечислены варианты защиты от вредоносных программ для Exchange.

- **Встроенная защита от вредоносных программ**. Вы можете использовать встроенную защиту от вредоносных программ в Exchange для борьбы с вредоносными программами. Ее можно использовать как саму по себе, так и в сочетании с другими решениями защиты от вредоносных программ, чтобы обеспечить многоуровневую защиту от вредоносных программ.

- **Exchange Online Protection (EOP):** вы можете заплатить за подписку на EOP, которая является решением для защиты от вредоносных программ, которое используется в Microsoft 365 и Office 365. Служба EOP использует несколько модулей для защиты от вредоносных программ, обеспечивая эффективную, экономную и многоуровневую защиту от вредоносных программ. Ниже перечислены преимущества сочетания встроенного средства защиты от вредоносных программ со службой EOP.

  - EOP использует несколько модулей защиты от вредоносных программ, в то время как встроенная защита от вредоносных программ использует один механизм.

  - Служба EOP включает возможности создания отчетов, в том числе статистики по вредоносным программам.

  - Служба EOP включает функцию трассировки сообщений для самостоятельного устранения проблем с потоком обработки почты, в том числе обнаружения вредоносных программ.

    Дополнительные сведения о EOP см. в разделе Защита от вредоносных программ в EOP.

- **Защита от вредоносных программ сторонних производителей**. Вы можете приобрести стороннюю антивредоносную программу.

Защита Exchange от вредоносных программ: вопросы и ответы

В этом разделе представлены ответы на часто задаваемые вопросы о встроенных функциях фильтрации и сканирования в Exchange для защиты от вредоносных программ.

Почему вредоносные программы, обнаруженные другими антивредоносными службами, прошли фильтрацию антивредоносных программ Exchange?

Это могло произойти по одной из двух причин.

- Наиболее вероятным сценарием является вложение сообщения, которое на самом деле не содержит активного вредоносного кода. Некоторые модули защиты от вредоносных программ более агрессивны, чем другие, и эти подсистемы могут останавливать сообщения просто потому, что они содержат усеченные полезные данные вредоносных программ, которые на самом деле ничего не делают.
- Вы получили новый вариант вредоносной программы, для которой наш модуль для защиты от вредоносных программ еще не выпустил файл шаблона.

Мне пришло сообщение с незнакомым вложением. Это вредоносная программа или вложение можно проигнорировать?

Настоятельно рекомендуем не открывать вложения, назначение которых вам неясно. Если вы хотите, чтобы мы изучили вложение, отправьте его нам, как описано в следующем разделе.

Разделы справки отправлять в корпорацию Майкрософт известные вредоносные программы, подозрительные файлы или ложные срабатывания?

Сохраните копию сообщения и отправьте сообщение на веб-сайт портал для обнаружения угроз (Microsoft), чтобы мы могли изучить его.

Если образец содержит вредоносную программу, мы примем меры, чтобы вирус не мог обойти защиту. Если же образец не опасен, мы примем соответствующие меры, чтобы этот файл больше не определялся как вредоносный.

Где можно просмотреть сообщения, удаленные фильтром защиты от вредоносных программ?

Это невозможно. Сообщения, в которых обнаружен активный вредоносный код, удаляются.

Можно ли обходить фильтрацию для защиты от вредоносных программ с помощью правил потока

обработки почты?

Нет, нельзя использовать правила потока обработки почты (также известные как правила транспорта) для обхода агента вредоносных программ. Вместо этого отправьте вложение в защищенном паролем .zip файле (защищенный паролем файл .zip файлы обходятся с помощью фильтрации вредоносных программ).

Процедуры защиты от вредоносных программ в Exchange Server

Статья • 04.04.2023

Exchange Server включает агент вредоносных программ, установленный на серверах почтовых ящиков. Дополнительные сведения о фильтрации вредоносных программ в Exchange см. в статье Защита от вредоносных программ в Exchange Server.

В этом разделе описаны следующие процедуры для управления фильтрацией вредоносных программ в Exchange:

- Отключение или включение фильтрации вредоносных программ на сервере почтовых ящиков
- Обход фильтрации вредоносных программ на сервере почтовых ящиков
- Создание политик защиты от вредоносных программ
- Просмотр политик защиты от вредоносных программ
- Изменение политик защиты от вредоносных программ
- Включение и отключение политик защиты от вредоносных программ
- Установка приоритета политик защиты от вредоносных программ
- Удаление политик защиты от вредоносных программ
- Настройте фильтрацию вредоносных программ для сканирования сообщений, которые уже были проверены Exchange Online Protection (EOP).
- Настройка обхода фильтрации вредоносных программ для получателя или группы получателей.

Что нужно знать перед началом работы

- Рекомендуем вручную скачать модуль защиты от вредоносных программ и обновления определений на сервер Exchange Server до его размещения в рабочей среде. Дополнительные сведения см. в разделе Скачивание обновлений антивредоносного ПО и определений.

- Политика защиты от вредоносных программ состоит из политики фильтрации вредоносных программ и правила фильтрации вредоносных программ. Каждый элемент управляет разными параметрами, которые не перекрываются. Разница между этими элементами не видна в EAC, но она очевидна в командной консоли Exchange, так как для управления параметрами используются различные командлеты (***-MalwareFilterPolicy** и ***-MalwareFilterRule**). В этом разделе описываются политики защиты от

вредоносных программ для процедур в EAC, политики фильтрации вредоносных программ и правила фильтрации вредоносных программ для процедур в командной консоли Exchange. Дополнительные сведения см. в разделе Защита от вредоносных программ в Exchange Server.

- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Антивредоносное ПО" в разделе Разрешения для защиты от вредоносных программ и защиты от вредоносных программ .

- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Включение или отключение фильтрации вредоносных программ на серверах почтовых ящиков с помощью командной консоли Exchange

При отключении фильтрации вредоносных программ на сервере почтовых ящиков отключается агент защиты от вредоносных программ, а также обновление определений и модуля.

1. Чтобы отключить фильтрацию вредоносных программ на локальном сервере почтовых ящиков, выполните следующую команду в командной консоли Exchange:

   ```
   PowerShell

   & $env:ExchangeInstallPath\Scripts\Disable-AntimalwareScanning.ps1
   ```

   Чтобы включить фильтрацию вредоносных программ на локальном сервере почтовых ящиков, выполните следующую команду в командной консоли Exchange:

```
PowerShell

& $env:ExchangeInstallPath\Scripts\Enable-AntimalwareScanning.ps1
```

Если команда выполнена успешно, вы увидите следующее сообщение:

`Anti-malware scanning is successfully <enabled or disabled>. Please restart MSExchangeTransport for the changes to take effect.`

Примечание. Скрипт включения также применяет обновления модуля и определений вредоносных программ по мере необходимости.

2. Перезапустите службу транспорта Exchange, выполнив следующую команду, которая временно прервет поток обработки почты на сервере:

```
PowerShell

Restart-Service MSExchangeTransport
```

Чтобы изменения вступили в силу, может потребоваться до 10 минут.

Как проверить, все ли получилось?

Чтобы убедиться, что вы успешно включили или отключили фильтрацию вредоносных программ на сервере почтовых ящиков, выполните следующую команду в командной консоли Exchange и проверьте значение свойства **Enabled** :

```
PowerShell

Get-TransportAgent "Malware Agent"
```

Использование командной консоли Exchange для обхода фильтрации вредоносных программ на серверах почтовых ящиков

Обход фильтрации вредоносных программ позволяет временно отключить фильтрацию вредоносных программ на сервере без нарушения потока обработки почты (перезапуск службы транспорта Exchange не требуется).

Примечание. При устранении проблемы следует *обходить* фильтрацию вредоносных программ на сервере почтовых ящиков. По завершении следует снова включить фильтрацию вредоносных программ.

Чтобы обойти или повторно включить фильтрацию вредоносных программ на сервере почтовых ящиков, используйте следующий синтаксис:

```
PowerShell

Set-MalwareFilteringServer -Identity <ServerIdentity> -BypassFiltering
<$true | $false>
```

В этом примере показано, как обойти фильтрацию вредоносных программ на сервере Mailbox01.

```
PowerShell

Set-MalwareFilteringServer -Identity Mailbox01 -BypassFiltering $true
```

В этом примере на том же сервере повторно включается фильтрация вредоносных программ.

```
PowerShell

Set-MalwareFilteringServer -Identity Mailbox01 -BypassFiltering $false
```

Чтобы изменения вступили в силу, может потребоваться до 10 минут.

Подробные сведения о синтаксисе и параметрах см. в статье Set-MalwareFilteringServer.

Как проверить, все ли получилось?

Чтобы убедиться, что вы временно обошли или повторно выполнили фильтрацию вредоносных программ на сервере почтовых ящиков, выполните следующую команду в командной консоли Exchange и проверьте значение свойства **BypassFiltering** :

```
PowerShell

Get-MalwareFilteringServer | Format-List Name,BypassFiltering
```

Создание политик защиты от вредоносных программ

Создание политик защиты от вредоносных программ с помощью Центра администрирования Exchange

При создании политики защиты от вредоносных программ в Центре администрирования Exchange одновременно создаются правило фильтрации вредоносных программ и связанная с ним одноименная политика.

1. В EAC перейдите в раздел **Фильтр защиты**>**от вредоносных программ** и нажмите кнопку **Создать**➕ .

2. На открывающейся странице **Новая политика защиты от вредоносных программ** настройте следующие параметры:

   - **Имя**. Укажите уникальное, описательное имя политики.
   - **Описание**. По желанию введите описание политики.
   - **Ответ на обнаружение вредоносных программ**. Выберите один из следующих вариантов:
     - **Удалить все сообщение**. Запрещает доставку всего сообщения предполагаемым получателям. Это значение используется по умолчанию.
     - **Удаление всех вложений и использование текста оповещений по умолчанию**. Заменяет все вложения сообщений (а не только обнаруженные) текстовым файлом, содержащим этот текст по умолчанию:

       > "В одном или нескольких вложениях этого сообщения электронной почты обнаружены вредоносные программы. Все вложения удалены".

     - **Удаление всех вложений и использование пользовательского текста оповещений**. Заменяет все вложения сообщений (а не только обнаруженные) текстовым файлом, содержащим настраиваемый текст, указанный в поле **Текст пользовательского оповещения** .

     ⓘ **Примечание**

При обнаружении вредоносной программы в **тексте входящего** или исходящего сообщения все сообщение удаляется независимо от параметра, настроенного для **ответа на обнаружение вредоносных программ**.

- **Уведомление**. Параметры в этом разделе управляют уведомлениями, когда фильтрация вредоносных программ удаляет сообщение. Параметры не применяются к сообщениям, в которых все вложения заменяются текстом оповещения по умолчанию или пользовательским текстом оповещений.

  - **Уведомления отправителя**. Выберите один или оба из этих параметров:

    - **Уведомление внутренних отправителей**. Внутренний отправитель находится в организации Exchange.

    - **Уведомление внешних отправителей**. Внешний отправитель находится за пределами организации Exchange.

  - **Уведомления администратора**. Выберите один или оба из этих параметров:

    - **Уведомление администратора о недоставленных сообщениях от внутренних отправителей**. Если выбран этот параметр, введите адрес электронной почты для уведомлений в поле **Адрес электронной почты администратора** .

    - **Уведомление администратора о недоставленных сообщениях от внешних отправителей**. Если выбран этот параметр, введите адрес электронной почты для уведомлений в поле **Адрес электронной почты администратора** .

  - **Настройка уведомлений**. Эти параметры заменяют текст уведомления по умолчанию, используемый для отправителей или администраторов. Дополнительные сведения о значениях по умолчанию см. в разделе Политики защиты от вредоносных программ.

    - **Использовать настраиваемый текст уведомления**. Если вы выбрали этот параметр, необходимо использовать поля **От имени** и **От адреса** , чтобы указать имя отправителя и адрес электронной почты, которые используются в настраиваемом уведомлении.

- **Сообщения от внутренних отправителей**. Если вы решили уведомлять отправителей или администраторов о недоставленных сообщениях от внутренних отправителей, необходимо использовать поля **Тема** и **Сообщение** , чтобы указать тему и текст сообщения пользовательского уведомления.

- **Сообщения от внешних отправителей**. Если вы решили уведомлять отправителей или администраторов о недоставленных сообщениях от внешних отправителей, необходимо использовать поля **Тема** и **Сообщение** , чтобы указать тему и текст сообщения пользовательского уведомления.

- **Применено к**: параметры в этом разделе определяют внутренних получателей, к которым применяется политика.

  - **Если**: щелкните раскрывающийся список **Выбрать один** и выберите условия для правила:

    - **Получатель:** указывает один или несколько почтовых ящиков, почтовых пользователей или почтовых контактов в организации Exchange. В появившемся диалоговом окне **Выбор участников** выберите одного или нескольких получателей из списка и нажмите кнопку **Добавить .>**. В поле **Проверка имен** можно использовать подстановочные знаки для нескольких адресов электронной почты (например, *@fabrikam.com). После этого нажмите кнопку **ОК**.

    - **Домен получателя:** указывает получателей в одном или нескольких настроенных обслуживаемых доменах в организации Exchange. В появившемся диалоговом окне выберите один или несколько доменов и нажмите кнопку **добавить ->**. После этого нажмите кнопку **ОК**.

    - **Получатель является членом**: указывает одну или несколько групп в организации Exchange. В появившемся диалоговом окне **Выбор участников** выберите одну или несколько групп из списка и нажмите кнопку **Добавить .>**. После этого нажмите кнопку **ОК**.

  Это условие можно использовать только один раз, но вы можете указать для него несколько значений. Чтобы добавить условие, нажмите **Добавить условие** и выберите один из оставшихся вариантов.
  - **За исключением случая, если**: Чтобы добавить исключения для правила, нажмите кнопку **Добавить исключение**, щелкните

раскрывающийся список **Выбрать одно** и настройте исключение для правила. Параметры и поведение полностью идентичны условиям.

3. По завершении нажмите кнопку **Сохранить**.

Создание политик защиты от вредоносных программ с помощью командной консоли Exchange

Создание политики защиты от вредоносных программ в командной консоли Exchange состоит из двух этапов:

1. Создание политики фильтрации вредоносных программ.
2. Создание правила фильтрации вредоносных программ, указывающего политику, к которой оно применяется.

Примечания.

- Вы можете создать новое правило фильтрации вредоносных программ и назначить ему существующую, не связанную с ним политику фильтрации вредоносных программ. Правило фильтрации вредоносных программ не может быть связано с несколькими политиками фильтрации вредоносных программ.
- Существует два параметра, которые можно настроить для новых политик защиты от вредоносных программ в командной консоли Exchange, которые недоступны в EAC до создания политики:
  - Создайте новую политику как отключенную (*включено*`$false` в **командлете New-MalwareFilterPolicy**).
  - Задайте приоритет политики во время создания (*номер*> *приоритета*<) в командлете **New-MalwareFilterRule**.
- Политики фильтрации вредоносных программ, создаваемые в командной консоли Exchange, не отображаются в EAC, пока вы не назначите политику фильтрации вредоносных программ правилу фильтрации вредоносных программ.
- Параметр, доступный в командной консоли Exchange, который недоступен в EAC, — это возможность включать или отключать фильтрацию вредоносных программ для входящих или исходящих сообщений с помощью параметров *BypassInboundMessages* или *BypassOutboundMessages* в командлете **New-MalwareFilterPolicy** .

Шаг 1. Создание политики фильтрации вредоносных программ с помощью командной консоли Exchange

Чтобы создать политику фильтрации вредоносных программ, используйте следующий синтаксис:

PowerShell

```
New-MalwareFilterPolicy -Name "<PolicyName>" [-Action <DeleteMessage | DeleteAttachmentAndUseDefaultAlert | DeleteAttachmentAndUseCustomAlert>] [-AdminDisplayName "<OptionalComments>"] [-BypassInboundMessages <$true | $false>] [-BypassOutboundMessages <$true | $false>] [-CustomNotifications <$true | $false>] [<Inbound notification options>] [<Outbound notification options>]
```

В этом примере создается политика фильтрации вредоносных программ с именем Contoso Malware Filter Policy и следующими параметрами:

- Блокировать сообщения, содержащие вредоносные программы (мы не используем параметр *Action* , а значение по умолчанию — `DeleteMessage`).
- Не уведомляйте отправителя сообщения об обнаружении в сообщении вредоносных программ (мы не используем параметры *EnableExternalSenderNotifications* или *EnableInternalSenderNotifications* , а значение по умолчанию для обоих — `$false`).
- Уведомляйте администратора admin@contoso.com об обнаружении вредоносных программ в сообщении от внутреннего отправителя.

PowerShell

```
New-MalwareFilterPolicy -Name "Contoso Malware Filter Policy" -EnableInternalSenderAdminNotifications $true -InternalSenderAdminAddress admin@contoso.com
```

Подробные сведения о синтаксисе и параметрах см. в статье New-MalwareFilterPolicy.

Шаг 2. Создание правила фильтрации вредоносных программ с помощью командной консоли Exchange

Чтобы создать правило фильтрации вредоносных программ, используйте следующий синтаксис:

PowerShell

```
New-MalwareFilterRule -Name "<RuleName>" -MalwareFilterPolicy "<PolicyName>"
<Recipient filters> [<Recipient filter exceptions>] [-Comments "
<OptionalComments>"]
```

В этом примере создается новое правило фильтрации вредоносных программ с именем Contoso Recipients и следующими параметрами:

- с правилом связана политика фильтрации вредоносных программ под названием Contoso Malware Filter Policy;
- правило применяется к получателям в домене contoso.com.

PowerShell

```
New-MalwareFilterRule -Name "Contoso Recipients" -MalwareFilterPolicy
"Contoso Malware Filter Policy" -RecipientDomainIs contoso.com
```

Подробные сведения о синтаксисе и параметрах см. в статье New-MalwareFilterRule.

Как проверить, все ли получилось?

Чтобы убедиться, что политика защиты от вредоносных программ успешно создана, выполните одно из указанных ниже действий.

- В EAC перейдите в раздел **Фильтр защиты**>**от вредоносных программ**. Убедитесь, что созданное правило присутствует в списке. Нажмите ✎ чтобы проверить параметры правила.
- В командной консоли Exchange замените <*PolicyName*> именем политики фильтрации вредоносных программ и выполните следующую команду, чтобы проверить значения свойств:

PowerShell

```
Get-MalwareFilterPolicy -Identity "<PolicyName>" | Format-List
```

- В командной консоли Exchange замените <*RuleName*> именем правила фильтрации вредоносных программ и выполните следующую команду, чтобы проверить значения свойств:

  PowerShell

  ```
  Get-MalwareFilterRule -Identity "<RuleName>" | Format-List
  ```

- Используйте тестовый файл EICAR, чтобы убедиться, что фильтр вредоносных программ работает надлежащим образом.

1. Откройте Блокнот и вставьте следующий текст (и только его) в пустой файл:

   ```
   PowerShell
   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
   ```

   Сохраните файл под именем EICAR.txt в расположении, которое вам будет легко найти и которое исключено из сканирования антивирусной программой на компьютере. Размер файла будет составлять 68 байтов.

2. Создайте сообщения электронной почты, вложите в сообщение файл EICAR.txt и отправьте сообщение получателю в организации Exchange, на который должна повлиять политика вредоносных программ.

3. Проверьте почтовый ящик получателя, чтобы убедиться, что фильтрация вредоносных программ сработала с сообщением, то есть сообщение было удалено или доставлено с замещающим текстовым файлом оповещения для вложения, а сообщения уведомлений были доставлены отправителю и/или администраторам.

4. По завершении удалите файл EICAR.TXT, чтобы не беспокоить других пользователей.

Просмотр политик защиты от вредоносных программ

Просмотр политик защиты от вредоносных программ с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел **Фильтр защиты**>**от вредоносных программ**.

2. При выборе политики сведения о ней отображаются в области сведений. Чтобы просмотреть дополнительные сведения о политике, нажмите кнопку **Изменить**.

   - Значения свойств **Enabled** и **Priority**, а также параметры со вкладки **Применяется к** входят в состав правила фильтрации вредоносных программ.

- Параметры на вкладках **Общие** и **Параметры** входят в состав политики фильтрации вредоносных программ.

Использование командной консоли Exchange для просмотра политик фильтрации вредоносных программ

Чтобы получить сводный список всех политик фильтрации вредоносных программ, выполните следующую команду:

```
PowerShell

Get-MalwareFilterPolicy
```

Чтобы получить подробные сведения об определенной политике фильтрации вредоносных программ, используйте следующий синтаксис:

```
PowerShell

Get-MalwareFilterPolicy -Identity "<PolicyName>" | Format-List [<Specific properties to view>]
```

В этом примере возвращаются значения всех свойств политики фильтрации вредоносных программ с именем Executives.

```
PowerShell

Get-MalwareFilterPolicy -Identity "Executives" | Format-List
```

В этом примере возвращаются только указанные свойства той же политики.

```
PowerShell

Get-MalwareFilterPolicy -Identity "Executives" | Format-List Action,AdminDisplayName,CustomNotifications,Enable*Notifications
```

Подробные сведения о синтаксисе и параметрах см. в статье Get-MalwareFilterPolicy.

Использование командной консоли Exchange для просмотра правил фильтрации вредоносных

программ

Чтобы получить сводный список всех правил фильтрации вредоносных программ, выполните следующую команду:

```
PowerShell

Get-MalwareFilterRule
```

Чтобы получить подробные сведения об определенном правиле фильтрации вредоносных программ, используйте следующий синтаксис:

```
PowerShell

Get-MalwareFilterRule -Identity "<RuleName>" | Format-List [<Specific
properties to view>]
```

В этом примере возвращаются значения всех свойств правила фильтрации вредоносных программ с именем Executives.

```
PowerShell

Get-MalwareFilterRule -Identity "Executives" | Format-List
```

В этом примере возвращаются только указанные свойства правила.

```
PowerShell

Get-MalwareFilterRule -Identity "Executives" | Format-List
Name,Priority,State,MalwareFilterPolicy,*Is,*SentTo,*MemberOf
```

Подробные сведения о синтаксисе и параметрах см. в статье Get-MalwareFilterRule.

Изменение политик защиты от вредоносных программ

Дополнительные параметры не доступны при изменении политики вредоносных программ в EAC или командной консоли Exchange. Доступны те же параметры, что и при создании политики.

Изменение политики защиты от вредоносных программ с помощью Центра администрирования Exchange

1. В EAC перейдите в раздел **Фильтр защиты**>**от вредоносных программ**.
2. Выберите политику и нажмите кнопку **Изменить**. Дополнительные сведения о параметрах см. в разделе Использование EAC для создания политик защиты от вредоносных программ этой статьи.

   Примечания.

   - Параметры не отображаются на одной странице, а разделены на вкладки **Общие**, **Параметры** и **Применяется к**. Вкладка **Применяется к** недоступна в стандартной политике с именем Default.
   - Переименовать политику по умолчанию невозможно.

Изменение политики фильтрации вредоносных программ с помощью командной консоли Exchange

Чтобы изменить политику фильтрации вредоносных программ, используйте следующий синтаксис:

```
PowerShell

Set-MalwareFilterPolicy -Identity "<PolicyName>" <Settings>
```

Подробные сведения о синтаксисе и параметрах см. в статье Set-MalwareFilterPolicy.

Изменение правила фильтрации вредоносных программ с помощью командной консоли Exchange

При изменении правила фильтрации вредоносных программ в командной консоли Exchange его нельзя отключить или включить (в **командлете Set-MalwareFilterRule** нет параметра *Enabled*). Вместо этого используйте **командлеты Disable-MalwareFilterRule** и **Enable-MalwareFilterRule** , как описано далее в этом разделе.

Чтобы изменить правило фильтрации вредоносных программ, используйте следующий синтаксис:

```
PowerShell
```

```
Set-MalwareFilterRule -Identity "<RuleName>" <Settings>
```

Подробные сведения о синтаксисе и параметрах см. в статье Set-MalwareFilterRule.

Включение и отключение политик защиты от вредоносных программ

По умолчанию политики защиты от вредоносных программ включены при их создании в EAC или командной консоли Exchange, но вы можете использовать командную консоль Exchange для создания правила фильтрации отключенных вредоносных программ (используйте командлет **New-MalwareFilterRule** и параметр *Enabled* со значением `$false`).

Включение и отключение политики защиты от вредоносных программ в Центре администрирования Exchange

1. В EAC перейдите в раздел **Фильтр защиты**>**от вредоносных программ**.
2. Выберите политику в списке, а затем настройте один из следующих параметров:
   - **Отключить политику**. Снимите флажок в столбце **Включено** .
   - **Включить политику**. Установите флажок в столбце **Включено** .

Использование командной консоли Exchange для включения или отключения правил фильтрации вредоносных программ

Чтобы включить или отключить правило фильтрации вредоносных программ в командной консоли Exchange, используйте следующий синтаксис:

PowerShell

```
<Enable-MalwareFilterRule | Disable-MalwareFilterRule> -Identity "
<RuleName>"
```

В этом примере отключается правило фильтрации вредоносных программ с именем Marketing Department.

PowerShell

```
Disable-MalwareFilterRule -Identity "Marketing Department"
```

В этом примере включается то же правило.

PowerShell

```
Enable-MalwareFilterRule -Identity "Marketing"
```

Дополнительные сведения о синтаксисе и параметрах см. в статьях Enable-MalwareFilterRule и Disable-MalwareFilterRule.

Как проверить, все ли получилось?

Чтобы убедиться, что политика защиты от вредоносных программ успешно включена или отключена, используйте любую из описанных ниже процедур.

- В EAC перейдите в раздел **Фильтр защиты**> от**вредоносных программ** и в списке политик защиты от вредоносных программ проверьте состояние флажка в столбце **Включено**.
- В командной консоли Exchange выполните следующую команду, чтобы просмотреть список правил и их значения свойств **State** :

  PowerShell

  ```
  Get-MalwareFilterRule
  ```

Установка приоритета настраиваемых политик защиты от вредоносных программ

По умолчанию политикам защиты от вредоносных программ назначается приоритет, основанный на том, в каком порядке они были созданы (приоритет новых политик ниже, чем у старых). Чем ниже значение, тем выше приоритет политики, а порядок обработки политик зависит от их приоритетов (политики с высоким приоритетом обрабатываются раньше, чем политики с низким приоритетом). У двух политик не может быть одинаковый приоритет.

Примечания.

- В Центре администрирования Exchange изменить приоритет политики защиты от вредоносных программ можно только после ее создания. В командной консоли Exchange можно переопределить приоритет по умолчанию при создании правила фильтрации вредоносных программ (что может повлиять на приоритет существующих правил).

- Для стандартной политики защиты от вредоносных программ с именем Default задано значение приоритета "Самый низкий". Его невозможно изменить.

Использование EAC для задания приоритета настраиваемых политик защиты от вредоносных программ

В Центре администрирования Exchange политики защиты от вредоносных программ обрабатываются в том же порядке, в котором они отображаются (для первой политики в свойстве **Приоритет** задано значение 0). Чтобы изменить приоритет политики, переместите ее вверх или вниз в списке (в Центре администрирования Exchange невозможно напрямую изменить значение свойства **Приоритет**).

1. В EAC перейдите в раздел **Фильтр защиты**>**от вредоносных программ**.

2. Выберите политику, а затем щелкните **Переместить вверх** (🡅) или **Переместить вниз** (🡇), чтобы переместить правило вверх или вниз в списке.

Использование командной консоли Exchange для задания приоритета настраиваемых правил фильтрации вредоносных программ

Максимальный приоритет, который можно задать для правила, — 0. Минимальное значение зависит от количества правил. Например, если у вас есть пять правил, вы можете использовать значения 0–4. Изменение приоритета существующего правила оказывает каскадное влияние на другие правила. Например, если вы измените приоритет правила на 2, когда у вас есть пять правил (с приоритетами от 0 до 4), то для существующего правила с приоритетом 2 будет задан приоритет 3, а для правила с приоритетом 3 будет задан приоритет 4.

Чтобы задать приоритет правила фильтрации вредоносных программ в командной консоли Exchange, используйте следующий синтаксис:

```
```

PowerShell

```
Set-MalwareFilterRule -Identity "<RuleName>" -Priority <Number>
```

В этом примере для правила Marketing Department задается приоритет 2. Все правила с приоритетом не больше 2 понижаются на один ранг (значения приоритета увеличиваются на 1).

PowerShell

```
Set-MalwareFilterRule -Identity "Marketing Department" -Priority 2
```

Примечание. Чтобы задать приоритет нового правила при его создании, используйте параметр *Priority* командлета **New-MalwareFilterRule**.

Как проверить, все ли получилось?

Чтобы убедиться, что приоритет политики защиты от вредоносных программ успешно изменен, используйте любую из описанных ниже процедур.

- В EAC перейдите в раздел **Фильтр защиты**>**от вредоносных программ** и проверьте значение **Приоритет** политик защиты от вредоносных программ в списке.
- В командной консоли Exchange выполните следующую команду, чтобы просмотреть список правил и их значения свойств **Priority** :

  PowerShell

  ```
  Get-MalwareFilterRule
  ```

Удаление политик защиты от вредоносных программ

Примечание. Стандартную политику защиты от вредоносных программ удалить невозможно.

Удаление политик защиты от вредоносных программ с помощью Центра администрирования Exchange

При удалении политики защиты от вредоносных программ в Центре администрирования Exchange удаляется как правило фильтрации вредоносных программ, так и соответствующая политика.

1. В EAC перейдите в раздел **Фильтр защиты**>**от вредоносных программ**.
2. Выберите политику защиты от вредоносных программ, которую нужно удалить, из списка, и нажмите кнопку **Удалить** (🗑

Удаление политик фильтрации вредоносных программ с помощью командной консоли Exchange

При использовании командной консоли Exchange для удаления политики фильтрации вредоносных программ соответствующее правило фильтра вредоносных программ не удаляется.

Чтобы удалить политику фильтрации вредоносных программ в командной консоли Exchange, используйте следующий синтаксис:

```
PowerShell

Remove-MalwareFilterPolicy -Identity "<PolicyName>"
```

В этом примере удаляется политика фильтрации вредоносных программ с именем Marketing Department.

```
PowerShell

Remove-MalwareFilterPolicy -Identity "Marketing Department"
```

Подробные сведения о синтаксисе и параметрах см. в статье Remove-MalwareFilterPolicy.

Удаление правил фильтрации вредоносных программ с помощью командной консоли Exchange

При использовании командной консоли Exchange для удаления правила фильтрации вредоносных программ связанная политика фильтрации вредоносных программ не удаляется.

Чтобы удалить правило фильтра вредоносных программ в командной консоли Exchange, используйте следующий синтаксис:

PowerShell

```
Remove-MalwareFilterRule -Identity "<RuleName>"
```

В этом примере удаляется правило фильтрации вредоносных программ с именем Marketing Department.

PowerShell

```
Remove-MalwareFilterRule -Identity "Marketing Department"
```

Подробные сведения о синтаксисе и параметрах см. в статье Remove-MalwareFilterRule.

Как проверить, все ли получилось?

Чтобы убедиться, что политика защиты от вредоносных программ успешно удалена, используйте любую из описанных ниже процедур.

- В EAC перейдите в раздел **Фильтр**>**защиты от вредоносных программ** и убедитесь, что удаленная политика больше не находится в списке.
- В командной консоли Exchange выполните следующую команду, чтобы убедиться, что удаленная политика фильтрации вредоносных программ больше не указана:

  PowerShell

  ```
  Get-MalwareFilterPolicy
  ```

- В командной консоли Exchange выполните следующую команду, чтобы убедиться, что удаляемое правило фильтрации вредоносных программ больше не указано:

  PowerShell

  ```
  Get-MalwareFilterRule
  ```

Использование командной консоли Exchange для настройки фильтрации

вредоносных программ для повторного сканирования сообщений, уже проверенных EOP

По умолчанию передаваемые сообщения, проверенные Exchange Online Protection (EOP), не проверяются агентом вредоносных программ в Exchange. Однако повторное сканирование этих сообщений может добавить еще один уровень защиты от вредоносных программ.

Чтобы включить или отключить проверку на наличие вредоносных программ в сообщениях, которые уже были проверены EOP, используйте следующий синтаксис в командной консоли Exchange:

PowerShell

```
Set-MalwareFilteringServer -Identity <ServerIdentity> -ForceRescan <$true | $false>
```

В этом примере включается сканирование на наличие вредоносных программ в сообщениях, уже отсканированных службой EOP, на сервере почтовых ящиков с именем Mailbox01.

PowerShell

```
Set-MalwareFilteringServer -Identity Mailbox01 -ForceRescan $true
```

В этом примере отключается сканирование на наличие вредоносных программ в сообщениях, уже отсканированных службой EOP, на том же сервере.

PowerShell

```
Set-MalwareFilteringServer -Identity Mailbox01 -ForceRescan $false
```

Как проверить, все ли получилось?

Чтобы убедиться, что вы настроили фильтрацию вредоносных программ для повторного сканирования сообщений, которые уже были проверены EOP, выполните следующую команду в командной консоли Exchange и проверьте значение свойства **ForceRescan** :

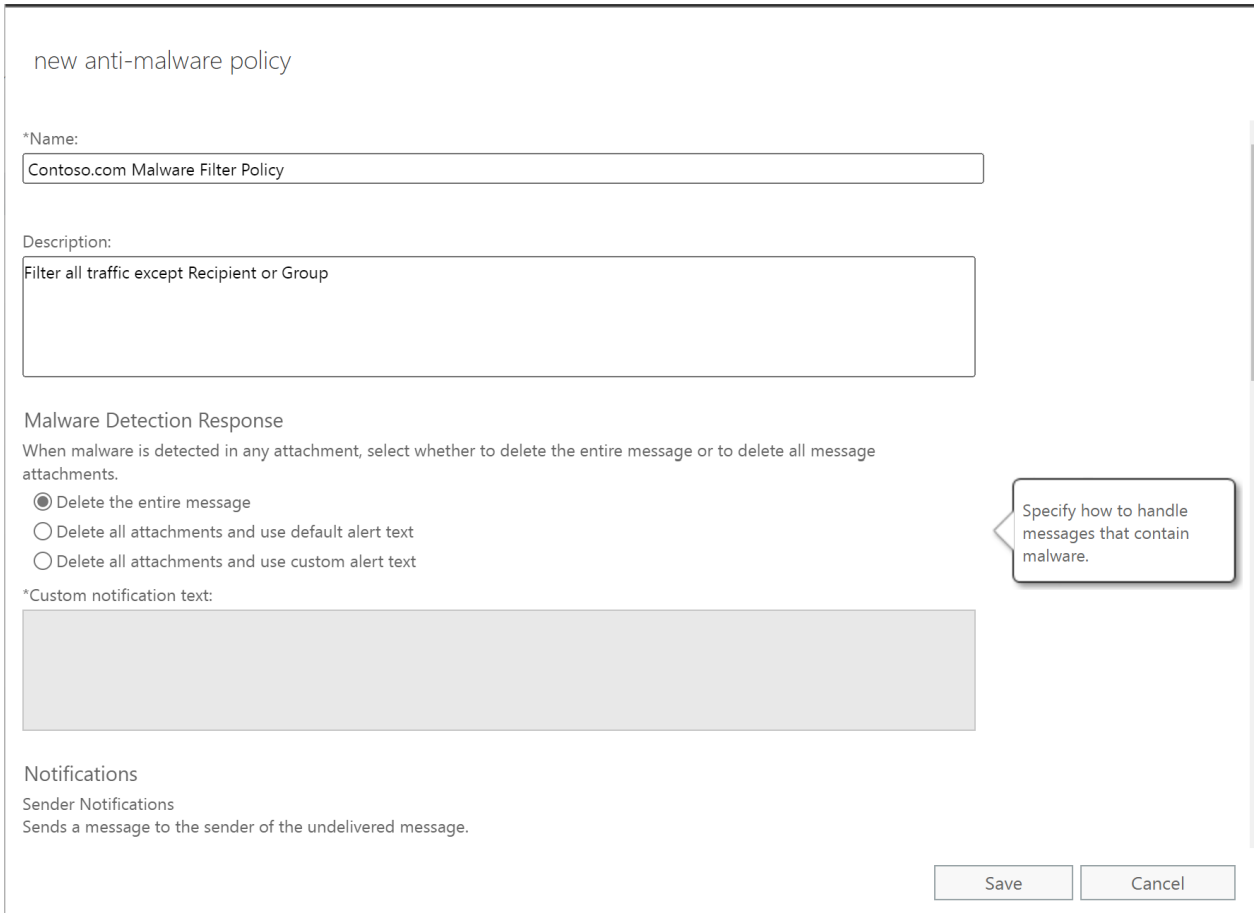
PowerShell

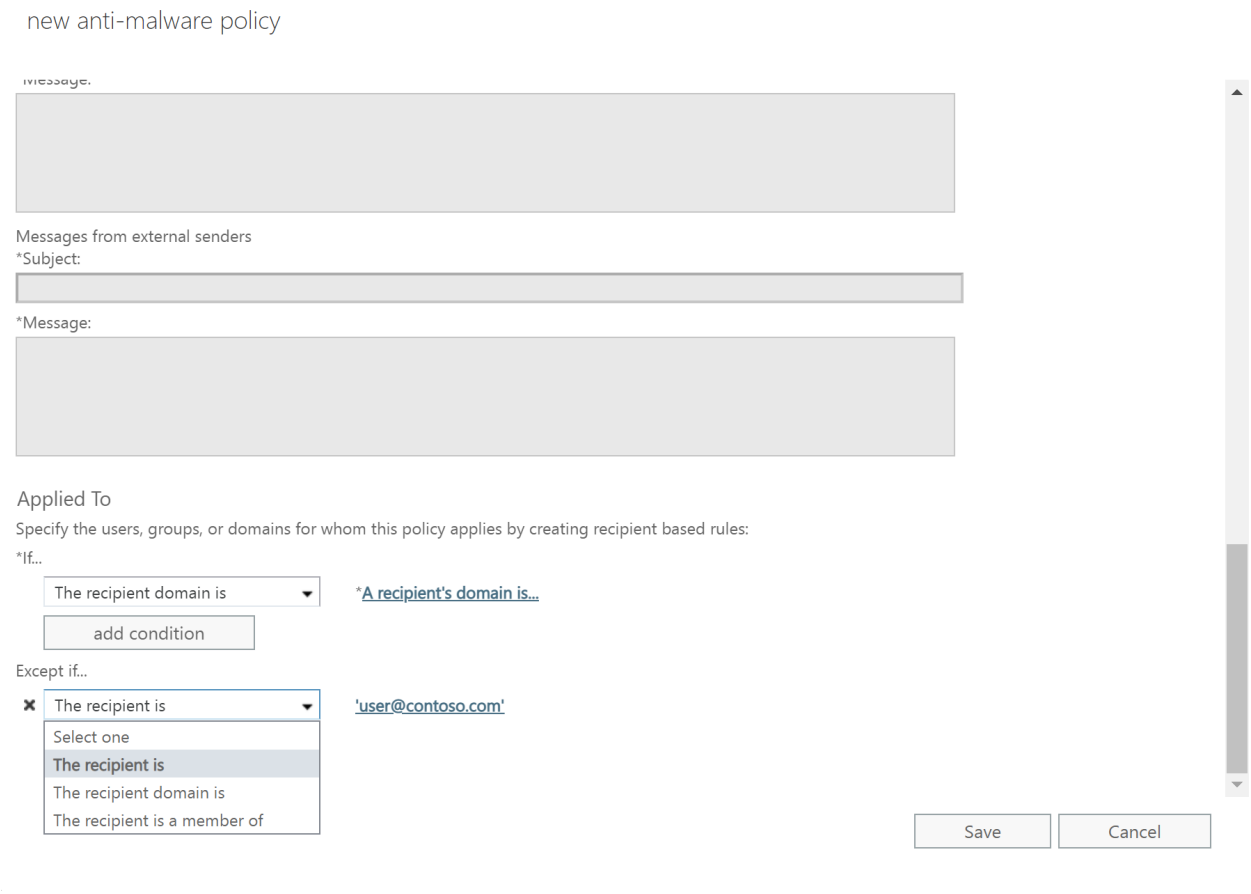
```
Get-MalwareFilteringServer | Format-List Name, ForceRescan
```

Настройка обхода фильтрации вредоносных программ для получателя или группы получателей

Чтобы разрешить конкретному получателю или группе получателей получать сообщения электронной почты с вложениями, которые в противном случае были бы обнаружены и удалены политикой защиты от вредоносных программ по умолчанию, необходимо создать новую политику защиты от вредоносных программ с помощью EAC или PowerShell. Эта политика должна быть настроена для сканирования сообщений электронной почты для всех получателей, и в этой политике должно быть задано условие исключения для получателя или группы, которые предназначены для получения такого содержимого.

Использование EAC для создания новой политики защиты от вредоносных программ:





При этом будет создана политика вредоносных программ, которая будет сканировать весь трафик электронной почты, кроме сообщений, отправляемых пользователю или группе, освобожденным.

Использование командной консоли Exchange для создания политики защиты от вредоносных программ:

Используйте командную консоль Exchange, чтобы изменить правило фильтрации вредоносных программ.

После создания политики защиты от вредоносных программ и установки соответствующего исключения необходимо создать новую политику защиты от вредоносных программ, чтобы незасканированные сообщения обошли политику защиты от вредоносных программ по умолчанию, которая всегда имеет самый низкий приоритет. Это изменение можно сделать с помощью командной консоли Exchange, чтобы задать для параметра **-BypassInboundMessages** этого правила фильтрации от вредоносных программ значение True. Подробные сведения о синтаксисе и параметрах см. в статье Set-MalwareFilterPolicy.

PowerShell

```
Set-MalwareFilterPolicy -Identity "<PolicyName>" -BypassInboundMessages
$true
```

Этот метод не требует перезапуска службы и может позволить администраторам Exchange и группам безопасности временно или навсегда обходить обнаружение вредоносных программ для конкретного получателя или группы, что в противном случае не доставляет сообщения в эту конкретную подгруппу без ущерба для безопасности всей организации Exchange и в конечном итоге сохраняет безопасность в своих системах и для своих клиентов.

Как проверить, все ли получилось?

PowerShell

```
Get-MalwareFilterPolicy "<PolicyName>" | fl BypassInboundMessages
```

Скачивание модуля защиты от вредоносных программ и обновлений определений

Статья • 04.04.2023

Администраторы могут вручную скачивать обновления модуля защиты от вредоносных программ и определений (сигнатур). Мы настоятельно рекомендуем скачать обновления подсистемы и определений, прежде чем переводить сервер Exchange Server в рабочую среду.

Что нужно знать перед началом работы

- Предполагаемое время для завершения: 5 минут.
- Для выполнения этой процедуры можно использовать только PowerShell.

  Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.
- Для скачивания обновлений компьютер должен быть способен подключаться к Интернету и устанавливать соединения через TCP-порт 80 (HTTP). Если ваша организация использует прокси-сервер для доступа к Интернету, см. следующий раздел этой статьи.
- Для выполнения этой процедуры (процедур) необходимы соответствующие разрешения. Сведения о необходимых разрешениях см. в записи "Защита от вредоносных программ" в разделе Разрешения для защиты от вредоносных программ и защиты от вредоносных программ .
- Сочетания клавиш для процедур, описанных в этой статье, приведены в статье Сочетания клавиш в Центре администрирования Exchange.

> **Совет**
>
> Возникли проблемы? Обратитесь за помощью к участникам форумов Exchange. Посетите форумы по адресу: **Exchange Server**, **Exchange Online** или **Exchange Online Protection**.

Использование Командная консоль Exchange для ручного скачивания обновления ядра и определений

Чтобы скачать обновления ядра и определений, запустите эту команду:

```PowerShell
& $env:ExchangeInstallPath\Scripts\Update-MalwareFilteringServer.ps1 -Identity <FQDN of server>
```

В этом примере вручную скачиваются обновления ядра и определений на сервере Exchange с именем mailbox01.contoso.com:

```PowerShell
& $env:ExchangeInstallPath\Scripts\Update-MalwareFilteringServer.ps1 -Identity mailbox01.contoso.com
```

При необходимости можно использовать параметр *EngineUpdatePath* для скачивания обновлений из расположения, отличного от расположения по умолчанию. Этот параметр позволяет указать альтернативный адрес HTTP или путь в формате UNC. Если указать путь в формате UNC, он должен быть доступен для сетевой службы.

В этом примере вручную скачиваются обновления обработчика и определений на сервер Exchange с именем mailbox01.contoso.com из пути UNC `\\FileServer01\Data\MalwareUpdates`:

```PowerShell
& $env:ExchangeInstallPath\Scripts\Update-MalwareFilteringServer.ps1 -Identity mailbox01.contoso.com -EngineUpdatePath \\FileServer01\Data\MalwareUpdates
```

Как проверить, все ли получилось?

Чтобы убедиться, что обновления успешно загружены, необходимые открыть окно просмотра событий и просмотреть журнал событий. Рекомендуется использовать фильтрацию событий FIPFS, как описано в следующей процедуре.

1. В меню **Пуск** выберите **Все программы**>**Администрирование**>**Просмотр событий**.
2. В Просмотр событий разверните папку **Журналы Windows** и выберите **Приложение**.
3. В меню **Действия** выберите **Фильтр текущего журнала**.
4. В диалоговом окне **Фильтр текущего журнала** в раскрывающемся **списке Источники событий** установите флажок **FIPFS** и нажмите **кнопку OK**.

Если обновления ядра были загружены успешно, вы увидите событие с идентификатором 6033, которое будет выглядеть следующим образом:

```
MS Filtering Engine Update process performed a successful scan engine update.

Scan Engine: Microsoft

Update Path: http://forefrontdl.microsoft.com/server/scanengineupdate

Last Update time: 2012-08-16T13:22:17.000Z

Engine Version: 1.1.8601.0

Signature Version: 1.131.2169.0
```

Использование Командная консоль Exchange для настройки параметров прокси-сервера для обновления ядра защиты от вредоносных программ

Если ваша организация использует прокси-сервер для управления доступом к Интернету, необходимо определить прокси-сервер, чтобы скачать обновления ядра защиты от вредоносных программ и определений. Параметры прокси-сервера, доступные с помощью **средстваNetsh.exe** , параметров подключения к Internet Explorer и параметра *InternetWebProxy* в командлете **Set-ExchangeServer** , не влияют на скачивание обновлений защиты от вредоносных программ.

Вот как настроить прокси-сервер для обновления ядра защиты от вредоносных программ:

1. Выполните следующую команду:

```
```

```
PowerShell

Add-PsSnapin Microsoft.Forefront.Filtering.Management.Powershell
```

2. Использование командлетов **Get-ProxySettings** и **Set-ProxySettings** для просмотра и выбора параметров прокси-сервера, используемых для скачивания обновлений ядра защиты от вредоносных программ. Командлет **Set-ProxySettings** использует такой синтаксис:

   ```
   PowerShell

   Set-ProxySettings -Enabled <$true | $false> -Server <Name or IP address
   of proxy server> -Port <TCP port of proxy server>
   ```

   Например, для обновления ядра защиты от вредоносных программ через прокси-сервер с адресом 172.17.17.10 на TCP-порте 80 выполните следующую команду.

   ```
   PowerShell

   Set-ProxySettings -Enabled $true -Server 172.17.17.10 -Port 80
   ```

Чтобы проверить параметры прокси-сервера, запустите командлет **Get-ProxySettings**.

Дополнительные сведения

- Процедуры защиты от вредоносных программ в Exchange Server
- Обновление модулей сканирования вручную в Microsoft Exchange Server

интеграция Exchange Server AMSI

Статья • 13.11.2024

Обзор

Интерфейс проверки антивредоносных программ Windows (AMSI) — это универсальный стандарт интерфейса, который позволяет приложениям и службам интегрироваться с любым продуктом защиты от вредоносных программ, присутствующих на Windows Server. AMSI не зависит от поставщика и позволяет интегрировать в приложения наиболее распространенные методы сканирования и защиты вредоносных программ, предоставляемые современными продуктами. Он был введен с Windows Server 2016.

AMSI поддерживает структуру вызовов, позволяющую сканировать файлы и память или поток, проверять URL-адрес источника содержимого и ip-репутацию и другие методы. Он также поддерживает понятие сеанса, чтобы поставщики средств защиты от вредоносных программ могли сопоставлять различные запросы на сканирование. Например, различные фрагменты вредоносных полезных данных могут быть связаны для принятия более обоснованного решения. Это было бы труднее достичь, просто взглянув на эти фрагменты в изоляции.

Интеграция AMSI в Exchange Server позволяет антивирусной и антивредоносной программе с поддержкой AMSI сканировать содержимое в HTTP-запросах, отправляемых в Exchange Server, и блокировать вредоносный запрос, прежде чем он будет обработан Exchange Server. Проверка выполняется в режиме реального времени любым решением антивирусной программы и защиты от вредоносных программ с поддержкой AMSI, которое запускается на сервере Exchange Server, когда сервер начинает обрабатывать запрос. Эта функция обеспечивает автоматическое устранение рисков и защиту, которая дополняет существующую защиту от вредоносных программ в Exchange Server, чтобы сделать серверы Exchange более безопасными.

Начиная с обновления системы безопасности Exchange Server ноября 2024 г., интеграция AMSI перенимается на следующий уровень, так как она предоставляет новые возможности для сканирования `HTTP message body`. Эта функция отключена по умолчанию и может быть включена, выполнив действия, описанные в разделе Включение Exchange Server проверки тела AMSI.

Предварительные условия

Чтобы воспользоваться преимуществами интеграции AMSI в Exchange Server, необходимо выполнить следующие предварительные требования:

- Windows Server 2016 или выше
- Частичная функциональность (без проверки текста AMSI):
  - Exchange Server 2016 CU21 / Exchange Server 2019 CU10
- Полная функциональность (с проверкой текста AMSI):
  - Exchange Server 2016 CU23 / Exchange Server 2019 CU13/CU14 + Exchange Server обновление для системы безопасности (SU) за ноябрь 2024 г. или более поздней версии
- Microsoft Defender с версией обработчика AV версии 1.1.18300.4 или с совместимым сторонним поставщиком AV с поддержкой AMSI проверка с вашим поставщиком.

Обязательно устанавливайте последнее обновление Exchange Server, чтобы воспользоваться исправлениями ошибок и последними улучшениями.

Проверка интеграции Exchange Server AMSI

В этом разделе мы предоставляем сведения, которые помогут вам проверка, правильно ли настроена интеграция EXCHANGE SERVER AMSI. Exchange Server интеграция AMSI включена по умолчанию, за исключением функции сканирования тела AMSI Exchange Server.

Поиск установленного поставщика AMSI

Чтобы убедиться, что на Exchange Server установлен поставщик AMSI, выполните следующие команды Windows PowerShell и проверьте выходные данные:

PowerShell

```
$AMSI = Get-ChildItem -Path "HKLM:\SOFTWARE\Microsoft\AMSI\Providers" -
Recurse
$AMSI -match "[0-9A-Fa-f\-]{36}"
$Matches.Values | ForEach-Object { Get-ChildItem -Path
"HKLM:\SOFTWARE\Classes\CLSID\{$_}" | Format-Table -AutoSize }
```

Выходные данные отображаются примерно так, как в этом примере, в зависимости от установленного антивирусного продукта.

PowerShell

```
Name                    Property
----                    --------
Hosts                   (default) : Scanned Hosting Applications
Implemented Categories
InprocServer32          (default) : "C:\ProgramData\Microsoft\Windows
Defender\Platform\4.18.2106.6-0\MpOav.dll"
                        ThreadingModel : Both
```

Результаты показывают, что единственный установленный поставщик находится по адресу `C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2106.6-0\MpOav.dll`, который соответствует `Microsoft Windows Defender`. Windows Server 2016 или более поздней версии операционные системы распознают установку поставщика AMSI, что подтверждается этой информацией.

Проверка конфигурации AMSI IIS

Одним из основных компонентов интеграции Exchange Server AMSI является `HttpRequestFilteringModule`. Этот модуль настраивается в `web.config` файле для большинства служб, которые находятся в `FrontEnd` каталогах и `ClientAccess` . Если вы регулярно заменяете или изменяете `web.config` файлы, убедитесь, что этот модуль включен. В противном случае интеграция AMSI работает неправильно. Строка конфигурации выглядит следующим образом:

XML

```
<add name="HttpRequestFilteringModule"
type="Microsoft.Exchange.HttpRequestFiltering.HttpRequestFilteringModule,
Microsoft.Exchange.HttpRequestFiltering, Version=15.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35" />
```

Проверка версии Защитника Windows

Чтобы проверить подписи с помощью Microsoft Windows Defender, откройте командную строку и используйте `MpCmdRun` средство, которое проверяет наличие последних определений и отображает текущую версию обработчика.

- Запуск от `cmd.exe` имени администратора
- Перейдите на сайт `%programdata%\Microsoft\Windows Defender\Platform\<antimalware platform version>`
- Запустите `mpcmdrun.exe -SignatureUpdate`

Выходные данные должны выглядеть примерно так:

command

```
Microsoft Windows Command Prompt
Copyright (C) Microsoft Corporation. All rights reserved.

C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2105.5-
0>MpCmdRun.exe -SignatureUpdate

Signature update started . . .
Service Version: 4.18.2106.6
Engine Version: 1.1.18300.4
AntiSpyware Signature Version: 1.343.1364.0
AntiVirus Signature Version: 1.343.1364.0
Signature update finished. No updates needed
```

Убедитесь, что интеграция AMSI работает

Если модуль AMSI обнаруживает вредоносный запрос, он регистрируется в папке `%ExchangeInstallPath%\Logging\HttpRequestFiltering` со значением `ScanResult` `Detected`. Модуль не регистрирует безопасные вызовы; Таким образом, наличие журнала указывает на то, что был обнаружен вредоносный вызов. Если запрос заблокирован, служба IIS возвращает `400 (Bad Request)` запрашивающий код состояния.

Ниже приведен пример файла журнала, который содержит запросы `HTTP POST` , которые помогли заблокировать AMSI:

text

```
DateTime,MajorVersion,MinorVersion,BuildVersion,RevisionVersion,ServerHostNa
me,SharedCacheLatency,TotalLatency,HttpMethod,UrlHost,UrlStem,UrlQuery,Serve
rIP,Protocol,HeaderNames,CookieNames,ScanResult,GenericInfo,GenericErrors
#Software: Microsoft Exchange Server
#Version: 15.01.build
#Log-type: Http Request Filtering Logs
#Date: 2021-06-30T10:03:57.573Z
#Fields:
DateTime,MajorVersion,MinorVersion,BuildVersion,RevisionVersion,ServerHostNa
me,SharedCacheLatency,TotalLatency,HttpMethod,UrlHost,UrlStem,UrlQuery,Serve
rIP,Protocol,HeaderNames,CookieNames,ScanResult,GenericInfo,GenericErrors
6/30/2021 10:03:57
AM,15,1,2334,0,SERVER01,,,POST,localhost,/ecp/x.js,,::1,FrontEnd.Ecp,Content
-Length;Cookie;Host,X-BEResource,Detected,,
6/30/2021 10:09:41
AM,15,1,2334,0,SERVER01,,,POST,SERVER01.contoso.com,/ecp/x.js,,192.168.10.52
,FrontEnd.Ecp,Content-Length;Cookie;Host,X-BEResource,Detected,,
6/30/2021 10:09:43
```

```
AM,15,1,2334,0,SERVER01,,,POST,SERVER01.contoso.com,/ecp/x.js,,192.168.10.52
,FrontEnd.Ecp,Content-Length;Cookie;Host,X-BEResource,Detected,,
```

Вы можете использовать скрипт Test-AMSI , чтобы проверить, работает ли интеграция AMSI должным образом. Скрипт отправляет созданный HTTP-запрос для активации средства проверки защиты от вредоносных программ, и вы можете проверка файлы журнала на Exchange Server для `Detected` записей после выполнения. Кроме того, скрипт можно использовать для проверка поставщиков AMSI в системе, а также для включения или отключения интеграции AMSI.

Если Exchange Server включено сканирование тела AMSI, в командной консоли Exchange (EMS) можно выполнить следующую команду:

PowerShell

```
 Get-Mailbox -Anr "amsiscantest:x5opap4pzx54p7cc7$eicar-standard-antivirus-
test-fileh+h*"
```

Команда не должна выполняться, и если вы открываете Microsoft Defender или запускаете `Get-MpThreat` с помощью PowerShell, вы увидите, что угроза `Exploit:Script/ExchangeEicar.A` заблокирована.

Включение Exchange Server проверки текста AMSI

Функция проверки текста EXCHANGE AMSI, которая появилась в Exchange Server обновлении для системы безопасности (SU) за ноябрь 2024 г., по умолчанию отключена. Его можно включить и настроить, создав переопределение параметра с помощью командлета New-SettingOverride . Эту функцию можно включить для каждого протокола или для всех протоколов. Команды `New-SettingOverride` в этом разделе создают `Global` переопределение, которое настраивает функцию на всех серверах Exchange в организации. Его можно включить только на подмножестве серверов. Для этого добавьте `-Server` параметр, как описано в документации New-SettingOverride .

> **ⓘ Важно!**
>
> Рекомендуется сначала включить эту функцию для подмножества служб, так как это может привести к проблемам с производительностью. Кроме того, мы просим вас связаться с нами, если у вас возникли какие-либо проблемы после включения Exchange Server проверки тела AMSI. Вы можете связаться с нами,

отправив электронное письмо на адрес ExchOnPremFeedback[at]microsoft.com.

Чтобы включить функцию проверки тела AMSI для определенного протокола, можно выбрать из предопределенного набора протоколов. Exchange Server сканирование тела AMSI поддерживает все протоколы, кроме `RPC over HTTP`:

- EnabledAll
- EnabledApi
- EnabledAutoD
- EnabledEcp
- EnabledEws
- EnabledMapi
- EnabledEas
- EnabledOab
- EnabledOwa
- EnabledPowerShell
- EnabledOthers

Следующим шагом является создание переопределения для протоколов, которые требуется включить. Можно создать одно переопределение, содержащее все протоколы, для которых должно быть включено сканирование тела AMSI. Обязательно выполните все команды из командной консоли Exchange с повышенными привилегиями (EMS):

PowerShell

```
New-SettingOverride -Name "EnableAMSIBodyScanForEcpEwsOwa" -Component Cafe -
Section AmsiRequestBodyScanning -Parameters
@("EnabledEcp=True","EnabledEws=True","EnabledOwa=True") -Reason "Enabling
AMSI body Scan for ECP, EWS and OWA"
Get-ExchangeDiagnosticInfo -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh
Restart-Service -Name W3SVC, WAS -Force
```

Можно создать несколько переопределений, например по одному для каждого протокола:

PowerShell

```
New-SettingOverride -Name "EnableAMSIBodyScanForEcp" -Component Cafe -
Section AmsiRequestBodyScanning -Parameters ("EnabledEcp=True") -Reason
"Enabling AMSI body Scan for ECP"
New-SettingOverride -Name "EnableAMSIBodyScanForEws" -Component Cafe -
```

```
Section AmsiRequestBodyScanning -Parameters ("EnabledEws=True") -Reason
"Enabling AMSI body Scan for EWS"
New-SettingOverride -Name "EnableAMSIBodyScanForOwa" -Component Cafe -
Section AmsiRequestBodyScanning -Parameters ("EnabledOwa=True") -Reason
"Enabling AMSI body Scan for OWA"
Get-ExchangeDiagnosticInfo -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh
Restart-Service -Name W3SVC, WAS -Force
```

Чтобы включить проверку текста AMSI для всех протоколов на всех серверах Exchange в вашей среде, выполните следующие действия.

PowerShell

```
New-SettingOverride -Name "EnableAMSIBodyScanAllProtocols" -Component Cafe -
Section AmsiRequestBodyScanning -Parameters ("EnabledAll=True") -Reason
"Enabling AMSI body Scan for all protocols"
Get-ExchangeDiagnosticInfo -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh
Restart-Service -Name W3SVC, WAS -Force
```

По умолчанию функция передает первую `4096 bytes` часть текста в средство проверки защиты от вредоносных программ. Можно настроить количество байтов, которые должны быть проверены. Максимально возможное значение — `1048576 bytes (1 MB)`. Мы рекомендуем начать с конфигурации по умолчанию и изменить размер, если возникают проблемы с производительностью. Этот параметр можно настроить, выполнив следующие команды. Обязательно замените `BodyScanSizeInBytes=8192` новым размером байтов, который должен быть обработан:

PowerShell

```
New-SettingOverride -Name "ConfigureCustomAMSIBodyScanSize" -Component Cafe
-Section AmsiRequestBodyScanning -Parameters ("BodyScanSizeInBytes=8192") -
Reason "Adjusting AMSI body Scan size to 8192 bytes"
Get-ExchangeDiagnosticInfo -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh
Restart-Service -Name W3SVC, WAS -Force
```

⚠ **Предупреждение**

Конфигурация, упомянутая в следующем разделе, не должна быть включена, если корпорация Майкрософт явно не посоветуется.

Можно заблокировать любой запрос, размер которого `HTTP message body` превышает максимальный размер, доступный `1048576 bytes (1 MB)` для сканирования. Эту функцию можно включить для подмножества протоколов (например, OWA, ECP, EWS) или для всех протоколов. Поддерживаемые протоколы перечислены в предыдущем разделе. В следующем примере блокируются запросы, в которых размер текста превышает максимальный размер сканируемых для протокола Outlook в Интернете (OWA):

PowerShell

```
New-SettingOverride -Name "BlockRequestBodyGreaterThanMaxScanSizeOWA" -
Component Cafe -Section BlockRequestBodyGreaterThanMaxScanSize -Parameters
("EnabledOwa=True") -Reason "Block requests with body size greater than 1 MB
for OWA"
Get-ExchangeDiagnosticInfo -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh
Restart-Service -Name W3SVC, WAS -Force
```

Отключение интеграции Exchange Server AMSI

Если вы столкнулись с проблемами с интеграцией Exchange Server AMSI или хотите временно отключить ее для исследования или устранения неполадок, можно создать переопределение, чтобы отключить интеграцию. Следующие команды должны выполняться из командной консоли Exchange с повышенными привилегиями (EMS).

Чтобы отключить интеграцию AMSI на определенном Exchange Server, выполните следующие команды. Замените `<ServerName>` именем Exchange Server:

PowerShell

```
New-SettingOverride -Name "DisablingAMSIScan" -Server <ServerName> -
Component Cafe -Section HttpRequestFiltering -Parameters ("Enabled=False") -
Reason "Troubleshooting AMSI"
Get-ExchangeDiagnosticInfo -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh
Restart-Service -Name W3SVC, WAS -Force
```

Чтобы отключить интеграцию AMSI на всех серверах Exchange Server в организации, можно выполнить следующие команды:

PowerShell

```
New-SettingOverride -Name "DisablingAMSIScan" -Component Cafe -Section
HttpRequestFiltering -Parameters ("Enabled=False") -Reason "Troubleshooting
AMSI"
Get-ExchangeDiagnosticInfo -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh
Restart-Service -Name W3SVC, WAS -Force
```

Чтобы включить интеграцию AMSI обратно, можно выполнить следующие команды, чтобы удалить переопределение:

PowerShell

```
Get-SettingOverride | Where-Object {($_.SectionName -eq
"HttpRequestFiltering") -and ($_.Parameters -eq "Enabled=False")} | Remove-
SettingOverride
Get-ExchangeDiagnosticInfo -Process
Microsoft.Exchange.Directory.TopologyService -Component VariantConfiguration
-Argument Refresh
Restart-Service -Name W3SVC, WAS -Force
```

Запуск антивирусного программного обеспечения Windows на серверах Exchange

Статья • 04.04.2023

При запуске антивирусных программ Windows на серверах Microsoft Exchange вы можете повысить безопасность и работоспособность организации Exchange. Однако если они настроены неправильно, антивирусные программы Windows могут вызвать проблемы в Exchange Server.

Любая антивирусная программа для Windows включает два основных компонента:

- *Сканирование памяти* или *защита в реальном времени* отслеживает все файлы и процессы, загруженные и выполняемые в активной памяти компьютера.
- *Сканирование на уровне файлов* — это регулярная проверка файлов на жестком диске на вирусы вручную. Некоторые антивирусные программы автоматически запускают такое сканирование после обновления сигнатур вирусов, чтобы гарантировать, что все файлы отсканированы с использованием последних сигнатур.

Самая значительная из потенциальных проблем заключается в том, что антивирусная программа для Windows может заблокировать или поместить в карантин открытый файл журнала или базы данных, который Exchange должен изменить. Это может привести к серьезным сбоям в Exchange Server, а также может привести к ошибкам журнала событий 1018. По этой причине очень важно исключить такие файлы из числа файлов, сканируемых антивирусной программой для Windows.

Другая проблема заключается в том, что антивирусные программы Windows не могут заменить решения для защиты от спама и вредоносных программ на основе электронной почты, так как антивирусные программы Windows, выполняемые на серверах Windows, не могут обнаруживать вирусы, вредоносные программы и спам, распространяемые только по электронной почте.

Рекомендуемые исключения для антивирусных программ Windows на серверах Exchange

При развертывании антивирусной программы Windows на сервере Exchange Server убедитесь, что исключения папок, исключения процессов и исключения расширений имен файлов, описанные в этих разделах, настроены для сканирования как на уровне памяти, так и на уровне файлов.

Примечание. Значение **%ExchangeInstallPath%** обычно `C:\Program Files\Microsoft\Exchange Server\V15\` имеет значение (включает в себя конечный "\"), значение **%SystemRoot%** — обычно `C:\Windows` (не содержит конечный "\"), а % **SystemDrive%** — обычно `C:` (не содержит конечного "\").

Расположение многих из этих папок Exchange можно настроить в командной консоли Exchange. Сведения о том, как открыть командную консоль Exchange в локальной организации Exchange, см. в статье Open the Exchange Management Shell.

Исключения папок

Исключите следующие папки из проверки на уровне файлов и проверки памяти на серверах Exchange.

> ⓘ **Примечание**
>
> Единая система обмена сообщениями не доступна в Exchange 2019.

Folder	Категория	Описание	Серверы
`%SystemRoot%\Cluster`	Группы обеспечения доступности баз данных	База данных кворума кластера и другие файлы для групп обеспечения доступности баз данных (DAG).	Серверы почтовых ящиков

Folder	Категория	Описание	Серверы
`%SystemDrive%\DAGFileShareWitnesses\<DAGFQDN>`	Группы обеспечения доступности баз данных	Следящий каталог на следящем сервере, настроенном для группы DAG. Следящий сервер может быть практически любым сервером Microsoft Windows в локальном лесу Active Directory, который еще не является членом daG. Чтобы просмотреть фактическое расположение, выполните следующую команду: `Get-DatabaseAvailabilityGroup <DAGName> | Format-List *Witness*`	Любой
`%ExchangeInstallPath%ClientAccess\OAB`	Автономные адресные книги	Файлы автономных адресных книг.	Серверы почтовых ящиков
`%ExchangeInstallPath%FIP-FS`	Антивредоносные программы и защита от потери данных	Сканирование содержимого, используемое агентом защиты от вредоносных программ и функцией защиты от потери данных (DLP).	Серверы почтовых ящиков
`%ExchangeInstallPath%GroupMetrics`	Подсказки	Файлы показателей групп, используемые при вычислении значений для подсказок "Большая аудитория" и "Внешние получатели".	Серверы почтовых ящиков

`%ExchangeInstallPath%Logging`	Журналы процессов Exchange	Во вложенных папках этой папки хранятся журналы Exchange различных типов. Например:
		• Журналы помощника по восстановлению календаря
		• Журналы помощника для управляемых папок
		• Журналы протокола IMAP4
		• Журналы протокола POP3
		
		Чтобы увидеть фактические расположения, выполните следующие команды:
		
		`Get-MailboxServer -Identity <ServerName> | Format-List *LogPath*`
		
		`Get-PopSettings <ServerName> | Format-List LogFileLocation`
		
		`Get-ImapSettings <ServerName> | Format-List LogFileLocation`
			Серверы почтовых ящиков

`%ExchangeInstallPath%Mailbox`	Базы данных почтовых ящиков	Базы данных Exchange, файлы контрольных точек и файлы журналов. По умолчанию эти файлы располагаются во вложенных папках по именам баз данных. Чтобы просмотреть фактические расположения, выполните следующую команду: `Get-MailboxDatabase -Server \ServerName> | Format-List EdbFilePath,LogFolderPath` По умолчанию файлы индекса для контекста базы данных находятся в той же папке, что и файлы базы данных, во вложенной папке, именем которой является GUID базы данных.	Серверы почтовых ящиков
`%ExchangeInstallPath%TransportRoles\Data\Adam`	Edgesync	Файлы служб Active Directory облегченного доступа к каталогам (AD LDS) и файлы журналов.	Пограничные транспортные серверы
`%ExchangeInstallPath%TransportRoles\Data\IpFilter`	Фильтрация подключения	Файлы базы данных IP-фильтров, контрольных точек и журналов.	Пограничные транспортные серверы
`%ExchangeInstallPath%TransportRoles\Data\Queue`	Очереди	Файлы базы данных очередей, контрольных точек и журналов.	Серверы почтовых ящиков Пограничные транспортные серверы

Folder	Категория	Описание	Серверы
`%ExchangeInstallPath%TransportRoles\Data\SenderReputation`	Репутация отправителя	Файлы базы данных репутации отправителя, контрольных точек и журналов.	Пограничные транспортные серверы Серверы почтовых ящиков
`%ExchangeInstallPath%TransportRoles\Data\Temp`	Преобразование содержимого	Преобразование содержимого, выполняемое в транспортном конвейере.	Серверы почтовых ящиков Пограничные транспортные серверы

`%ExchangeInstallPath%TransportRoles\Logs`	Журналы транспорта	Журналы потока обработки почты и транспортного конвейера находятся во вложенных папках, например:
		• Ведение журнала агентов
		• Ведение журнала подключений
		• Отслеживание сообщений
		• Трассировка конвейера
		• Ведение журнала протокола для соединителей отправки и получения
		
		Чтобы увидеть фактические расположения, выполните следующие команды:
		
		`Get-TransportService <ServerName> | Format-List *LogPath,*TracingPath`
		
		`Get-FrontEndTransportService <ServerName> | Format-List *LogPath`
		
		`Get-MailboxTransportService <ServerName> | Format-List *LogPath,*TracingPath`
			Серверы почтовых ящиков
			Пограничные транспортные серверы (только для службы транспорта)

`%ExchangeInstallPath%TransportRoles\Pickup`	Каталог раскладки	Администраторы используют каталог раскладки, чтобы тестировать поток обработки почты, а приложения — для создания и отправки собственных файлов сообщений. Чтобы просмотреть фактическое расположение, выполните следующую команду: `Get-TransportService <ServerName> | Format-List PickupDirectoryPath`	Серверы почтовых ящиков Пограничные транспортные серверы
`%ExchangeInstallPath%TransportRoles\Replay`	Каталог преобразования	Каталог преобразования получает сообщения с серверов внешних шлюзов и может использоваться для передачи сообщений, экспортированных администраторами из очередей серверов Exchange. Чтобы просмотреть фактическое расположение, выполните следующую команду: `Get-TransportService <ServerName> | Format-List ReplayDirectoryPath`	Серверы почтовых ящиков Пограничные транспортные серверы
`%ExchangeInstallPath%UnifiedMessaging\Grammars`	Единая система обмена сообщениями.	Файлы грамматики для разных языковых стандартов, например en-EN или es-ES.	Серверы почтовых ящиков Exchange 2016
`%ExchangeInstallPath%UnifiedMessaging\Prompts`	Единая система обмена сообщениями	Файлы голосовых приглашений, приветствий и информационных сообщений.	Серверы почтовых ящиков Exchange 2016
`%ExchangeInstallPath%UnifiedMessaging\Temp`	Единая система обмена сообщениями	Временные файлы, создаваемые единой системой обмена сообщениями.	Серверы почтовых ящиков Exchange 2016

Folder	Категория	Описание	Серверы
`%ExchangeInstallPath%UnifiedMessaging\Voicemail`	Единая система обмена сообщениями	Временные файлы голосовой почты.	Серверы почтовых ящиков Exchange 2016
`%ExchangeInstallPath%Working\OleConverter`	Преобразование содержимого	Преобразования из формата TNEF, также известного как RTF, в формат MIME/HTML.	Серверы почтовых ящиков Пограничные транспортные серверы
`%SystemDrive%\inetpub\temp\IIS Temporary Compressed Files`	Веб-компоненты	Папка сжатия служб IIS, используемая с Outlook в Интернете.	Серверы почтовых ящиков
`%SystemRoot%\Temp\OICE_<GUID>`	Служба поиска Exchange	Временные файлы, используемые службой поиска Exchange и пакетом фильтров Microsoft Filter Pack для преобразования файлов в изолированной среде.	Серверы почтовых ящиков

Исключения для процессов

Многие антивирусные программы поддерживают сканирование процессов, которое может негативно повлиять на Microsoft Exchange, если сканируются неправильные процессы. Таким образом, следует исключить указанные ниже процессы Exchange и связанные с ними процессы из сканирования.

Процесс	Path	Comments	Серверы
ComplianceAuditService.exe	`%ExchangeInstallPath%Bin`	Служба аудита соответствия требованиям Microsoft Exchange (MSComplianceAudit)	Серверы почтовых ящиков
Dsamain.exe	`%SystemRoot%\System32`	Служба ADAM Microsoft Exchange (ADAM_MSExchange) (Службы Active Directory облегченного доступа к каталогам на подписанных пограничных транспортных серверах)	Пограничные транспортные серверы
EdgeTransport.exe	`%ExchangeInstallPath%Bin`	Рабочий процесс службы транспорта Microsoft Exchange	Серверы почтовых ящиков Пограничные транспортные серверы
fms.exe	`%ExchangeInstallPath%FIP-FS\Bin`	Компонент сканирования контента, используемый агентом вредоносных программ и DLP.	Серверы почтовых ящиков
hostcontrollerservice.exe	`%ExchangeInstallPath%Bin\Search\Ceres\HostController`	Служба контроллера узла поиска Microsoft Exchange (HostControllerService)	Серверы почтовых ящиков
inetinfo.exe	`%SystemRoot%\System32\inetsrv`	Службы IIS (IIS)	Серверы почтовых ящиков
Microsoft.Exchange.AntispamUpdateSvc.exe	`%ExchangeInstallPath%Bin`	Служба обновления средства защиты от нежелательной почты Microsoft Exchange (MSExchangeAntispamUpdate)	Серверы почтовых ящиков Пограничные транспортные серверы

Процесс	Path	Comments	Серверы
Microsoft.Exchange.ContentFilter.Wrapper.exe	`%ExchangeInstallPath%TransportRoles\agents\Hygiene`	Агент фильтра содержимого	Серверы почтовых ящиков Пограничные транспортные серверы
Microsoft.Exchange.Diagnostics.Service.exe	`%ExchangeInstallPath%Bin`	Служба диагностики Microsoft Exchange (MSExchangeDiagnostics)	Серверы почтовых ящиков Пограничные транспортные серверы
Microsoft.Exchange.Directory.TopologyService.exe	`%ExchangeInstallPath%Bin`	Служба топологии Active Directory Microsoft Exchange (MSExchangeADTopology)	Серверы почтовых ящиков
Microsoft.Exchange.EdgeCredentialSvc.exe	`%ExchangeInstallPath%Bin`	Служба учетных данных Microsoft Exchange (MSExchangeEdgeCredential)	Пограничные транспортные серверы
Microsoft.Exchange.EdgeSyncSvc.exe	`%ExchangeInstallPath%Bin`	Служба Microsoft Exchange EdgeSync (MSExchangeEdgeSync)	Серверы почтовых ящиков
Microsoft.Exchange.Imap4.exe	`%ExchangeInstallPath%FrontEnd\PopImap`	Служба IMAP4 Microsoft Exchange (MSExchangeImap4)	Серверы почтовых ящиков
Microsoft.Exchange.Imap4service.exe	`%ExchangeInstallPath%ClientAccess\PopImap`	Внутренняя служба IMAP4 Microsoft Exchange (MSExchangeIMAP4BE)	Серверы почтовых ящиков
Microsoft.Exchange.Notifications.Broker.exe	`%ExchangeInstallPath%Bin`	Служба брокера уведомлений Microsoft Exchange (MSExchangeNotificationsBroker)	Серверы почтовых ящиков
Microsoft.Exchange.Pop3.exe	`%ExchangeInstallPath%FrontEnd\PopImap`	Служба POP3 Microsoft Exchange (MSExchangePop3)	Серверы почтовых ящиков
Microsoft.Exchange.Pop3service.exe	`%ExchangeInstallPath%ClientAccess\PopImap`	Внутренняя служба POP3 Microsoft Exchange (MSExchangePOP3BE)	Серверы почтовых ящиков
Microsoft.Exchange.ProtectedServiceHost.exe	`%ExchangeInstallPath%Bin`	Служба узла Microsoft Exchange (MSExchangeServiceHost)	Серверы почтовых ящиков Пограничные транспортные серверы
Microsoft.Exchange.RPCClientAccess.Service.exe	`%ExchangeInstallPath%Bin`	Служба клиентского доступа RPC Microsoft Exchange (MSExchangeRPC)	Серверы почтовых ящиков
Microsoft.Exchange.Search.Service.exe	`%ExchangeInstallPath%Bin`	Служба поиска Microsoft Exchange (MSExchangeFastSearch)	Серверы почтовых ящиков
Microsoft.Exchange.Servicehost.exe	`%ExchangeInstallPath%Bin`	Служба узла Microsoft Exchange (MSExchangeServiceHost)	Серверы почтовых ящиков Пограничные транспортные серверы
Microsoft.Exchange.Store.Service.exe	`%ExchangeInstallPath%Bin`	Служба банка данных Microsoft Exchange (MSExchangeIS)	Серверы почтовых ящиков

Процесс	Path	Comments	Серверы
Microsoft.Exchange.Store.Worker.exe	`%ExchangeInstallPath%Bin`	Рабочий процесс службы банка данных Microsoft Exchange	Серверы почтовых ящиков
Microsoft.Exchange.UM.CallRouter.exe	`%ExchangeInstallPath%FrontEnd\CallRouter`	Служба маршрутизатора вызовов единой системы обмена сообщениями Microsoft Exchange (MSExchangeUMCR)	Серверы почтовых ящиков Exchange 2016
MSExchangeCompliance.exe	`%ExchangeInstallPath%Bin`	Служба соответствия Microsoft Exchange (MSExchangeCompliance)	Серверы почтовых ящиков
MSExchangeDagMgmt.exe	`%ExchangeInstallPath%Bin`	Служба управления группами обеспечения доступности баз данных Microsoft Exchange (MSExchangeDagMgmt)	Серверы почтовых ящиков
MSExchangeDelivery.exe	`%ExchangeInstallPath%Bin`	Служба транспортной доставки почтовых ящиков Microsoft Exchange (MSExchangeDelivery)	Серверы почтовых ящиков
MSExchangeFrontendTransport.exe	`%ExchangeInstallPath%Bin`	Интерфейсная служба транспорта Microsoft Exchange (MSExchangeFrontEndTransport)	Серверы почтовых ящиков
MSExchangeHMHost.exe	`%ExchangeInstallPath%Bin`	Служба диспетчера работоспособности Microsoft Exchange (MSExchangeHM)	Серверы почтовых ящиков Пограничные транспортные серверы
MSExchangeHMWorker.exe	`%ExchangeInstallPath%Bin`	Рабочий процесс службы диспетчера работоспособности Microsoft Exchange	Серверы почтовых ящиков Пограничные транспортные серверы
MSExchangeMailboxAssistants.exe	`%ExchangeInstallPath%Bin`	Служба помощников по обслуживанию почтовых ящиков Microsoft Exchange (MSExchangeMailboxAssistants)	Серверы почтовых ящиков
MSExchangeMailboxReplication.exe	`%ExchangeInstallPath%Bin`	Служба репликации почтовых ящиков Microsoft Exchange (MSExchangeMailboxReplication)	Серверы почтовых ящиков
MSExchangeRepl.exe	`%ExchangeInstallPath%Bin`	Служба репликации Microsoft Exchange (MSExchangeRepl)	Серверы почтовых ящиков
MSExchangeSubmission.exe	`%ExchangeInstallPath%Bin`	Служба отправки транспорта почтовых ящиков Microsoft Exchange (MSExchangeSubmission)	Серверы почтовых ящиков
MSExchangeTransport.exe	`%ExchangeInstallPath%Bin`	Служба транспорта Microsoft Exchange (MSExchangeTransport)	Серверы почтовых ящиков Пограничные транспортные серверы
MSExchangeTransportLogSearch.exe	`%ExchangeInstallPath%Bin`	Служба поиска журналов транспорта Microsoft Exchange (MSExchangeTransportLogSearch)	Серверы почтовых ящиков Пограничные транспортные серверы

Процесс	Path	Comments	Серверы
MSExchangeThrottling.exe	`%ExchangeInstallPath%Bin`	Служба регулирования Microsoft Exchange (MSExchangeThrottling)	Серверы почтовых ящиков
Noderunner.exe	`%ExchangeInstallPath%Bin\Search\Ceres\Runtime\1.0`	Служба поиска Microsoft Exchange (MSExchangeFastSearch)	Серверы почтовых ящиков
OleConverter.exe	`%ExchangeInstallPath%Bin`	Преобразует сообщения в формате RTF в MIME/HTML для внешних получателей.	Серверы почтовых ящиков
ParserServer.exe	`%ExchangeInstallPath%Bin\Search\Ceres\ParserServer`	Служба поиска Microsoft Exchange (MSExchangeFastSearch)	Серверы почтовых ящиков
ScanEngineTest.exe	`%ExchangeInstallPath%FIP-FS\Bin`	Компонент сканирования содержимого, используемый агентом защиты от вредоносных программ и DLP	Серверы почтовых ящиков
ScanningProcess.exe	`%ExchangeInstallPath%FIP-FS\Bin`	Компонент сканирования содержимого, используемый агентом защиты от вредоносных программ и DLP	Серверы почтовых ящиков
UmService.exe	`%ExchangeInstallPath%Bin`	Служба единой системы обмена сообщениями Microsoft Exchange (MSExchangeUM)	Серверы почтовых ящиков Exchange 2016
UmWorkerProcess.exe	`%ExchangeInstallPath%Bin`	Рабочий процесс службы единой системы обмена сообщениями Microsoft Exchange	Серверы почтовых ящиков Exchange 2016
UpdateService.exe	`%ExchangeInstallPath%FIP-FS\Bin`	Компонент сканирования содержимого, используемый агентом защиты от вредоносных программ и DLP	Серверы почтовых ящиков
wsbexchange.exe	`%ExchangeInstallPath%Bin`	Серверное расширение Microsoft Exchange для программы архивации данных (wsbexchange)	Серверы почтовых ящиков

Исключения для расширений имен файлов

Помимо определенных папок и процессов, из проверки необходимо исключить перечисленные ниже расширения имен файлов, характерные для Exchange, на тот случай, если произойдет сбой исключений папок или файлы будут перемещены из расположений по умолчанию.

Расширения	Описание	Серверы
.config	Расширения, связанные с приложениями	Серверы почтовых ящиков Пограничные транспортные серверы
.Chk .Edb JFM-файл .Jrs .Журнала .Que	Расширения, связанные с базами данных	Серверы почтовых ящиков Пограничные транспортные серверы
.Dsc .txt	Расширения, связанные с показателями групп	Серверы почтовых ящиков
.Cfg .Grxml	Расширения, связанные с единой системой обмена сообщениями	Серверы почтовых ящиков Exchange 2016

Расширения	Описание	Серверы
.Lzx	Расширения, связанные с автономной адресной книгой	Серверы почтовых ящиков

Сведения о документации по Обмену

Статья • 04.04.2023

Это коллекция инструкций и тематических разделов, организованных по темам или технологиям Microsoft Exchange. К каждому разделу можно обратиться непосредственно из оглавления в левой части экрана, по ссылке из другого раздела справки, из результатов поиска или из собственного списка избранных разделов.

Другие сведения, относящиеся к документации Exchange, см. в разделе Уведомления об авторских правах сторонних разработчиков.

Где найти документацию Exchange

Документация по Exchange — это основной шлюз для получения подробных технических сведений о Microsoft Exchange.

В блоге группы разработчиков Exchange можно найти технические статьи, написанные командой разработчиков Exchange, а также объявления о выходе продукта и обновления для него. Этот блог — отличный способ общения с командой разработчиков Exchange. Мы читаем ваши отзывы и комментарии и отвечаем на них.

Если вы являетесь администратором гибридного или Exchange Online развертывания Exchange, вас также может заинтересовать управление Microsoft 365 и Office 365.

Дополнительные ресурсы

Ищете больше, чем просто документацию? Ознакомьтесь с другими ресурсами Exchange:

- форумы Exchange Server. Форум предоставляет место для обсуждения Exchange с пользователями и участниками команды Exchange.
- Разработка exchange и Exchange Online. Документация разработчика по Exchange приведена здесь.
- Поддержка для бизнеса. Выберите **Серверы**>**Exchange Server** ресурсы поддержки для нескольких версий Exchange.

- Специальные возможности для людей с ограниченными возможностями. В этой статье содержатся важные сведения о функциях, продуктах и службах, которые помогают сделать Microsoft Exchange более доступным для людей с ограниченными возможностями.

Специальные возможности для людей с ограниченными возможностями

Статья • 04.04.2023

Корпорация Майкрософт стремится к тому, чтобы сделать использование своих продуктов и служб простым и удобным для каждого. В приведенных ниже разделах содержатся сведения о возможностях, продуктах и службах, облегчающих инвалидам работу с Microsoft Exchange.

- Accessibility features of Exchange
- Accessibility features of Exchange Help
- Accessibility products and services from Microsoft

Специальные возможности Exchange

Следующие функции в системе Microsoft Exchange делают ее более доступной людям с ограниченными возможностями.

- Сочетания клавиш в Центре администрирования Exchange
- Сочетания клавиш в Outlook в Интернете

Кроме того, некоторые специальные возможности и служебные программы Windows могут помочь пользователям Exchange с ограниченными возможностями. Кроме того, Windows PowerShell изменения размера и цвета предоставляют параметры специальных возможностей при использовании командной консоли Exchange. Дополнительные сведения о параметрах специальных возможностей Windows PowerShell см. в статье Специальные возможности в Windows PowerShell ISE.

Специальные возможности справки Exchange

Все рисунки в справке к Microsoft Exchange, включая снимки экрана, диаграммы и графики, имеют соответствующий замещающий текст. Пользователи, которым сложно просматривать рисунки, могут задержать указатель мыши на рисунке и

прочитать замещающий текст. Замещающий текст описывает, что показано на рисунке.

Продукты и службы корпорации Майкрософт, поддерживающие специальные возможности

В приведенных ниже разделах содержатся сведения о возможностях, продуктах и службах, облегчающих инвалидам работу с ОС Microsoft Windows.

> **Примечание**
>
> Сведения, приведенные в данном разделе, распространяются только на пользователей лицензированных продуктов корпорации Майкрософт на территории США. Если вы приобрели данный продукт не на территории США, посетите веб-сайт **Microsoft Accessibility (Специальные возможности продуктов корпорации Майкрософт)**, чтобы найти телефонные номера и адреса служб технической поддержки корпорации Майкрософт. Для получения сведений о доступности в вашем регионе продуктов и служб, описанных в данном разделе, вы можете связаться с представителем дочернего подразделения. Узнать больше о специальных возможностях, реализованных в продуктах корпорации Майкрософт, можно на веб-сайте специальных возможностей в продуктах корпорации Майкрософт.

Специальные возможности Windows

Операционная система Windows имеет множество встроенных функций специальных возможностей, которые полезны для людей, которые испытывают трудности при вводе текста или использовании мыши, слепые или слабовидящие, глухие или слабослышащие. Эти компоненты устанавливаются с помощью программы установки ОС. Дополнительные сведения об этих функциях см. в статье Справка в Windows и Специальные возможности Майкрософт.

- **Бесплатные пошаговые руководства**. Корпорация Майкрософт предлагает серию пошаговых руководств, в которые приводятся подробные процедуры по настройке параметров специальных возможностей и параметров на компьютере. Данные сведения представлены параллельном формате, что позволяет изучить использование мыши, клавиатуры или их комбинации.

Чтобы найти пошаговые учебники по продуктам корпорации Майкрософт, посетите веб-сайт Microsoft Accessibility (Специальные возможности продуктов корпорации Майкрософт) .

- **Специальные технологические продукты для Windows**. Доступны широкие возможности специальных возможностей, которые упрощают использование компьютеров для людей с ограниченными возможностями. Имеется возможность поиска по каталогу продуктов с поддержкой специальных возможностей для Windows на сайте "Специальные возможности продуктов корпорации Microsoft".

  Перед обновлением программного обеспечения или оборудования с использованием продукта с поддержкой специальных возможностей свяжитесь с поставщиком данного продукта, чтобы получить сведения о возможных проблемах с совместимостью.

Документация в альтернативных форматах

При наличии трудностей с чтением или обращением с печатными материалами можно получить документацию по большому количество продуктов корпорации Майкрософт в более доступных форматах. Чтобы получить перечень доступной документации по продуктам, посетите веб-сайт Microsoft Accessibility (Специальные возможности продуктов корпорации Майкрософт) .

Кроме того, дополнительные публикации о продуктах корпорации Майкрософт можно приобрести в компании Learning Ally. Learning Ally распространяет данные документы среди зарегистрированных членов своей службы рассылки. Чтобы получить сведения о наличии документации по продуктам корпорации Microsoft и книг издательства Microsoft Press, свяжитесь с компанией Learning Ally.

> Learning Ally
> 20 Roszel Road
> Princeton, NJ 08540
> Телефонный номер для жителей США: (800) 221-4792
> Веб-сайт: Learning Ally

Служба технической поддержки для людей с нарушениями слуха

Пользователи, страдающие глухотой или нарушениями слуха, могут обращаться в службы поддержки по продуктам Майкрософт и службы поддержки клиентов по

текстовому телефону (TTY/TDD):

- По вопросам поддержки клиентов обращайтесь в Центр информационной поддержки продаж Майкрософт по телефону (800) 892-5234 с 6:30 до 17:30 (по тихоокеанскому времени), с понедельника по пятницу, кроме праздников.
- Для получения помощи по техническим вопросам в США обращайтесь в службы поддержки по продуктам Майкрософт по телефону (800) 892-5234 с 6:00 до 18:00 (по тихоокеанскому времени), с понедельника по пятницу, кроме праздников. В Канаде звоните по телефону (905) 568-9641 с 8:00 до 20:00 (по восточному времени) с понедельника по пятницу, кроме праздников.

При использовании службы поддержки корпорации Майкрософт действуют цены и условия, актуальные на момент использования службы. Дополнительные сведения см. в разделе служба поддержки Майкрософт.

Дополнительные сведения

Дополнительные сведения о том, как поддержка специальных возможностей для компьютеров помогает улучшить жизнь инвалидов, см. на веб-сайте Microsoft Accessibility (Специальные возможности продуктов корпорации Майкрософт).

Exchange Server: уведомления об авторских правах сторонних производителей

Статья • 04.04.2023

Outside In HTML Export © 1991, 2011 Oracle

Поддерживаемые платформы - Outside In HTML Export:

Windows (32-разрядная):

Windows 2000

Windows Server 2003

Windows Vista

Windows Server 2008

Windows XP

Windows 7

Windows Itanium (64-разрядная):

Windows .NET Server 2003 Enterprise Edition для платформы Itanium

Windows (64-разрядная):

Windows 2003 x 64 Datacenter

Windows 2003 x 64 Enterprise

Windows 2003 x 64 Standard Windows Server

Windows Server 2008

Windows Server 2008 R2

Windows 7

Сочетания клавиш в Центре администрирования Exchange

Статья • 04.04.2023

Майкрософт стремится к тому, чтобы сделать использование своих продуктов и служб простым и удобным для каждого. В этом разделе содержатся сведения о сочетаниях клавиш, которые делают Exchange Server и другие продукты и службы Майкрософт более доступными для людей с ограниченными возможностями.

Сочетания клавиш в Центре администрирования Exchange в Exchange Server

С помощью сочетаний клавиш в Центре администрирования Exchange (EAC) можно быстро выполнить распространенные задачи, описанные в следующей таблице. Дополнительные сведения о EAC см. в разделе Центр администрирования Exchange в Exchange Server.

Действие	Сочетание клавиш
Перемещение между областями или элементами управления в Центре администрирования Exchange	TAB SHIFT-TAB
Перемещение между элементами раскрывающихся меню в Центре администрирования Exchange	Клавиша СТРЕЛКА ВВЕРХ Клавиша СТРЕЛКА ВНИЗ Обратите внимание, что вы не можете использовать tab или Shift-Tab для перемещения между элементами в раскрывающихся меню.

Действие	Сочетание клавиш
Перемещение между элементами списков	Клавиша СТРЕЛКА ВВЕРХ Клавиша СТРЕЛКА ВНИЗ PgUp (СТРАНИЦА ВВЕРХ) PgDn (СТРАНИЦА ВНИЗ) HOME Конец Обратите внимание, что вы также можете использовать клавиши СТРЕЛКА ВВЕРХ, СТРЕЛКА ВНИЗ, СТРЕЛКА ВЛЕВО и СТРЕЛКА ВПРАВО, чтобы: • перемещаться между переключателями; • перемещаться в пределах группы связанных флажков.
Перемещение между элементами страниц основных свойств	Клавиша СТРЕЛКА ВВЕРХ Клавиша СТРЕЛКА ВНИЗ PgUp (СТРАНИЦА ВВЕРХ) PgDn (СТРАНИЦА ВНИЗ) HOME Конец TAB SHIFT-TAB Можно использовать клавишу ВВОД или ПРОБЕЛ, чтобы активировать ваш выбор.
Перемещение между элементами страниц вторичных свойств	Клавиша СТРЕЛКА ВВЕРХ Клавиша СТРЕЛКА ВНИЗ PgUp (СТРАНИЦА ВВЕРХ) PgDn (СТРАНИЦА ВНИЗ) HOME Конец TAB SHIFT-TAB Можно использовать клавишу ВВОД или ПРОБЕЛ, чтобы активировать ваш выбор.

Сочетания клавиш в других продуктах и службах Майкрософт

Чтобы узнать о специальных возможностях в Microsoft 365 или Office 365, включая сочетания клавиш, посетите веб-сайт Специальных возможностей Майкрософт.

Заявление о конфиденциальности для Exchange Server

Статья • 04.04.2023

Корпорация Майкрософт принимает все меры для соблюдения вашей конфиденциальности, предоставляя программное обеспечение, которое гарантирует производительность, эффективность и удобство использования, отвечающие ожиданиям пользователей. Настоящее заявление о конфиденциальности относится к Microsoft Exchange Server 2016 и Exchange Server 2019. Этот раздел посвящен функциям, использующим подключение к Интернету. Он не относится к другим веб-сайтам, продуктам и службам Майкрософт (как в Интернете, так и вне его).

Exchange 2016 и Exchange 2019 позволяют использовать на ПК, мобильных телефонах и в веб-браузерах функции электронной почты, календарей, контактов и другие возможности совместной работы в Интернете.

Данное заявление о конфиденциальности касается развертывания и использования Exchange 2016 и Exchange 2019 в сетевой среде предприятия. Если вы используете технологии Exchange Server как службу, которой управляет корпорация Майкрософт или третье лицо, ознакомьтесь с политикой конфиденциальности и безопасности этой службы, предоставленной корпорацией Майкрософт или сторонним поставщиком услуг.

ИТ-администраторы Exchange 2016 и Exchange 2019 могут включать и отключать определенные функции в Exchange, использующие подключение к Интернету, или развертывать другие технологии, которые затрагивают конфиденциальность, на основе юридических рекомендаций и рекомендаций по соответствию требованиям либо внутренних политик. Запросы относительно конфиденциальности, которые связаны с политикой организации, предоставляющей доступ к Exchange 2016 или Exchange 2019, следует подавать в эту же организацию. Корпорация Майкрософт не несет ответственности за методы обеспечения конфиденциальности своих клиентов и других третьих лиц.

Сбор и использование ваших сведений

Корпорация Майкрософт, управляемые ею дочерние подразделения и аффилированные лица будут использовать полученные от вас сведения для поддержки используемых вами возможностей, предоставления услуг и выполнения

транзакций, запрошенных или авторизованных вами. Эти сведения также могут использоваться для анализа и улучшения продуктов и услуг Майкрософт.

Мы можем отправлять определенные стандартные сообщения, связанные с обслуживанием, такие как приветственные письма, напоминания об оплате счетов, информацию о технических проблемах со службами и объявления о безопасности. Некоторые службы Майкрософт могут отправлять периодические письма, которые считаются частью предоставления услуг. Иногда мы можем спросить ваше мнение, пригласить вас для участия в опросе или отправить вам рекламные сообщения о других продуктах или службах корпорации Майкрософт и ее аффилированных лиц.

Чтобы сделать вашу работу с Майкрософт более согласованной и персонализированной, сведения, собранные одной из служб Майкрософт, могут быть объединены со сведениями, полученными другими службами Майкрософт. Мы также можем дополнить полученную информацию сведениями от других компаний. Например, мы можем использовать службы других компаний, позволяющие нам определять общий географический регион на основе вашего IP-адреса, чтобы настроить определенные службы в соответствии с вашим географическим регионом.

За исключением случаев, упомянутых в данном заявлении, предоставленные вами личные данные не будут переданы третьей стороне без вашего согласия.

Иногда мы нанимаем другие компании для предоставления ограниченных услуг от нашего имени, таких как ответы на вопросы клиентов о продуктах или услугах или выполнение статистического анализа наших услуг. Мы предоставим этим компаниям только личную информацию, необходимую им для предоставления услуги, и им запрещено использовать эти сведения для каких-либо других целей.

Корпорация Майкрософт может использовать или раскрывать сведения о вас, в том числе текст ваших сообщений, для (a) соблюдения требований закона, предоставления ответа на судебный запрос или выполнения требования судебных органов; (b) защиты прав или собственности корпорации Майкрософт либо ее клиентов, включая обеспечение выполнения соглашений Майкрософт или политик, регламентирующих использование служб; или (c) если есть основания полагать, что такой доступ или раскрытие требуется для личной защиты сотрудников и клиентов Майкрософт, а также общественности.

Сведения, собранные или отправленные в корпорацию Майкрософт через Exchange 2016 и Exchange 2019, могут храниться и обрабатываться в США или любой другой стране либо регионе, где есть центры Майкрософт, ее аффилированных лиц, дочерних подразделений или поставщиков услуг. Корпорация Майкрософт придерживается соглашения Safe Harbor, как это

рекомендовано Министерством торговли США в отношении сбора, использования и хранения данных из Европейского союза, Европейской экономической зоны и Швейцарии.

Сбор и использование сведений о вашем компьютере

При использовании программного обеспечения с функциями, использующими подключение к Интернету, сведения о вашем компьютере ("стандартные сведения о компьютере") отправляются на посещаемые вами веб-сайты и в веб-службы, которые вы используете. Корпорация Майкрософт использует стандартные сведения о компьютере для предоставления служб, использующих подключение к Интернету, улучшения своих продуктов и услуг, а также для статистического анализа. К стандартным сведениям о компьютере обычно относятся такие данные, как IP-адрес, версия операционной системы, версия браузера, а также параметры языка и региональных стандартов. В некоторых случаях к стандартным сведениям о компьютере могут также относиться код оборудования, обозначающий производителя устройства, имя и версию устройства. Если определенная функция или служба отправляет сведения в корпорацию Майкрософт, отправляются и стандартные сведения о компьютере.

Сведения о конфиденциальности для других функций, программ или служб Exchange 2016 или Exchange 2019, указанные в этом заявлении о конфиденциальности, содержат описание собираемых дополнительных сведений и способа их использования.

Защита сведений о пользователе

Корпорация Майкрософт обеспечивает защиту личных данных пользователя. Для защиты личных данных от несанкционированного доступа, использования и разглашения применяются различные технологии и процедуры. Например, предоставленные пользователем сведения хранятся в компьютерных системах с ограниченным доступом, расположенных в охраняемых помещениях.

Специальная функция. Отчеты об ошибках Microsoft

Описание функции. Служба ведения отчетов об ошибках Microsoft позволяет сообщать о возникших ошибках в корпорацию Майкрософт и получать сведения, которые могут помочь в избежании и устранении таких проблем.

Собираемые, обрабатываемые и передаваемые сведения. Информацию о сведениях, собираемых, обрабатываемых и передаваемых функцией "Отчеты об

ошибках (Майкрософт)", см. в заявлении о конфиденциальности для этой функции.

Использование сведений. Отправленные данные отчетов об ошибках могут использоваться для решения проблем клиентов и улучшения программного обеспечения и служб Майкрософт.

Выбор и управление. Вам будет предложено принять участие в создании отчетов об ошибках Майкрософт при первом обнаружении ошибки. Если вы решите включить его, microsoft Error Reporting автоматически сообщит о проблемах, с которыми вы столкнулись, в корпорацию Майкрософт. Кроме того, ИТ-администратор может включить или отключить отчеты об ошибках Майкрософт во время настройки Exchange Server для всех пользователей.

В редких случаях (например, когда проблему очень сложно решить), корпорация Майкрософт может подать запрос на дополнительные данные, в том числе разделы памяти (которые могут включать общую память для одного или всех приложений, запущенных во время возникновения ошибки), некоторые параметры реестра и один или несколько файлов с компьютера пользователя. Также могут быть запрошены текущие документы. При запросе дополнительных данных вы сможете просмотреть сведения, содержащиеся в отчете об ошибке, до принятия решения об отправке отчета в корпорацию Майкрософт.

Важные сведения. Корпоративные клиенты могут использовать групповую политику для настройки службы ведения отчетов об ошибках (Майкрософт) на своих компьютерах. При настройке можно отключить ведение отчетов об ошибках (Майкрософт). Если вы администратор и вам нужно настроить групповую политику для ведения отчетов об ошибках (Майкрософт), технические сведения доступны в справочнике по параметрам групповой политики для Windows и Windows Server.

Специальная функция. Онлайн-отзывы

Описание функции. Онлайн-отзывы позволяют отправить отзыв о продуктах и услугах непосредственно в корпорацию Майкрософт.

Собираемые, обрабатываемые и передаваемые сведения. Если вы используете онлайн-отзывы, в корпорацию Майкрософт передаются содержимое сообщения и стандартные сведения о компьютере.

Использование сведений. Отправляемая информация может использоваться для улучшения сайтов, продуктов или служб Майкрософт. Информация, которую мы

собираем из этой функции, также может использоваться для запроса дополнительных сведений об отзыве, предоставленном о продукте или услуге.

Выбор и управление. Использование функции онлайн-отзывов является необязательным.

Специальная функция. Интерактивная справка

Описание функции. При выборе справки происходит подключение к материалам поддержки в Интернете, которые содержат наиболее актуальные сведения.

Собираемая, обработанная или передаваемая информация. При использовании справки запрос отправляется в корпорацию Майкрософт, а также любые оценки или отзывы, предоставленные по темам справки. Любая личная информация, введенная в поля поиска или обратной связи, будет отправлена в корпорацию Майкрософт, но не будет использоваться для идентификации или связи с вами.

Использование сведений. Справка использует сведения поиска для возврата наиболее подходящих результатов, разработки нового и улучшения имеющегося содержимого.

Выбор и управление. Не используйте справку, если не хотите подключаться к материалам поддержки в Интернете.

Специальная функция. Программа улучшения качества программного обеспечения

Что делает эта функция. Если вы решили принять участие, программа улучшения качества программного обеспечения (CEIP) собирает основные сведения о конфигурации оборудования и о том, как вы используете программное обеспечение и службы Майкрософт для выявления тенденций и шаблонов использования. CeIP также собирает тип и количество возникающих ошибок, производительность программного и аппаратного обеспечения и скорость служб. Корпорация Майкрософт не собирает ваше имя, адрес или другую контактную информацию.

Собранные, обработанные или передаваемые данные: информация ceIP автоматически отправляется в корпорацию Майкрософт, когда эта функция

включена. Дополнительные сведения о собираемой, обрабатываемой или передаваемой ceIP информации см. в заявлении о конфиденциальности для программы улучшения качества программного обеспечения Майкрософт.

Использование сведений. Корпорация Майкрософт использует эти сведения для улучшения качества, надежности и производительности программного обеспечения и служб Майкрософт.

Выбор и управление: ceIP отключена по умолчанию, если только ИТ-администратор не решил включить его за вас. Вам будет предложено зарегистрироваться в установщике Exchange. Если администратор не ограничил ваши возможности, вы можете изменить параметры CEIP в любое время.

Специальная функция. Расширение "Карты Bing"

Работа функции. Расширение "Карты Bing" отображается в Outlook и Outlook в Интернете (прежнее название — Outlook Web App), когда служба Exchange 2016 или Exchange 2019 обнаруживает в тексте сообщения электронной почты адрес. Это расширение позволяет подать запрос на карту местности в Карты Bing.

Собранные, обработанные или передаваемые данные. При щелчке расширения Карты Bing в пользовательском интерфейсе сведения, которые Exchange определяет как адрес, будут переданы Карты Bing службе, которая выполнит запрос на основе адреса и вернет для него карту. Дополнительные сведения о политике конфиденциальности Bing см. в разделе Bing в Заявлении о конфиденциальности Майкрософт.

Использование сведений. Сведения об адресе используются, чтобы отобразить для него карту.

Выбор и управление. Эту функцию может отключить ИТ-администратор или пользователь.

Специальная функция. Автономный режим

Описание функции. В Outlook Web App функции автономного режима сохраняют на компьютере пользователя контакты, календарь и сведения электронной почты, чтобы пользователь имел к ним доступ без сетевого подключения.

Собираемые, обработанные или передаваемые данные: собираемые и сохраненные сведения включают контакты, календарь и электронную почту из

почтового ящика пользователя на Exchange Server. Эта функция не передает информацию в корпорацию Майкрософт.

Использование сведений. Данные хранятся локально на компьютере пользователя для обеспечения доступа в автономном режиме.

Выбор и управление. В Outlook в Интернете эта функция отключена по умолчанию, и пользователь должен включить автономный режим. Кроме того, ИТ-администраторы могут отключить параметр для этой функции, чтобы пользователи не могли его включить.

Специальная функция. Фотография отправителя

Описание функции. В Outlook в Интернете функция "Фотография отправителя" позволяет получателю увидеть фотографию отправителя сообщения электронной почты, если получатель и отправитель принадлежат к одной организации.

Собранные, обработанные или передаваемые данные. Если Outlook в Интернете считает, что фотография отправителя может быть доступна, адрес электронной почты отправителя отправляется на сервер Exchange Server. Передача может быть отправлена частично в незашифрованной форме. Эта функция не передает информацию в корпорацию Майкрософт.

Использование сведений. Адрес электронной почты отправителя используется для поиска его фотографии на конечном сервере Exchange.

Выбор и управление. ИТ-администраторы могут отключить эту функцию.

Специальная функция. Карточка контакта

Что делает эта функция: при просмотре сообщений электронной почты в Outlook в Интернете пользователь может щелкнуть имя отправителя или одного из получателей в сообщении, чтобы получить карточку контакта для конкретного лица. На карточке контакта отображаются сведения об этом человеке.

Собранные, обработанные или передаваемые данные. Когда пользователь запрашивает данные карточки контакта для кого-либо, щелкнув имя пользователя из сообщения электронной почты, адрес электронной почты или аналогичный идентификатор пользователя, информация которого запрашивается, отправляется на сервер Exchange Server. Передача может быть отправлена частично в

незашифрованной форме. Эта функция не передает информацию в корпорацию Майкрософт.

Использование сведений. Адрес электронной почты пользователя, чья карточка контакта запрашивается, используется для поиска его данных карточки контакта на конечном сервере Exchange.

Выбор и управление. Не щелкайте имя пользователя для получения его карточки контакта, если не хотите передавать сведения, идентифицирующие его, на сервер Exchange.

Изменения в данном заявлении о конфиденциальности

Корпорация Майкрософт обеспечивает защиту личных данных пользователя. Для защиты личных данных от несанкционированного доступа, использования и разглашения применяются различные технологии и процедуры. Например, предоставленные пользователем сведения хранятся в компьютерных системах с ограниченным доступом, расположенных в охраняемых помещениях.

Дополнительные сведения

Корпорация Майкрософт приветствует замечания к этому заявлению о конфиденциальности и его дополнениям. Если у вас возникли вопросы или вы считаете, что мы не выполняем требования этих документов, заполните веб-форму или напишите нам по адресу:

Политика конфиденциальности корпорации Майкрософт

Корпорация Майкрософт

One Microsoft Way

Redmond, Washington 98052 USA (США)

(425) 882-80-80

Чтобы найти дочернее подразделение Майкрософт в своей стране или регионе, воспользуйтесь этой страницей.