Synology®

Synology Volume Encryption White Paper

Last Oct 20, 2023

Table of Contents

Introduction 2
What is Synology Volume Encryption? 3
Why use volume encryption? 3
Get started with volume encryption 3
How Volume Encryption Works 5
Enabling encryption upon volume creation 5
Accessing data on an encrypted volume 8
Managing access to an encrypted volume 8
Best Practices 10
Understand the scope of protection 10
Set up the Encryption Key Vault first 10
Change the keys regularly 10
Store recovery keys separately 11

Introduction

Protecting sensitive information is crucial for maintaining consumer trust and complying with regulations in today's digital landscape. With cyber threats and privacy concerns at an all-time high, encryption has become a potent defense for data security.

As an industry leader, Synology recognizes the importance of data encryption and continually strives to offer comprehensive solutions tailored to the unique security needs of organizations and individuals. For users of Synology NAS devices, volume encryption is an effective feature that can protect critical data and assure privacy. By encrypting important data stored within volumes, both organizations and individuals can mitigate the risks associated with data breaches and protect sensitive information, such as credentials, personal records, and privacy-related data.

By exploring the world of volume encryption, this white paper aims to provide insights into its benefits, functionality, implementation considerations, and best practices. With Synology's volume encryption feature, organizations and individuals can proactively protect their precious data in an evolving digital ecosystem.

What is Synology Volume Encryption?

Synology's **volume encryption** is a software-based solution designed to protect sensitive data stored on Synology NAS. This feature can be selectively deployed on a per-volume basis, ensuring that the stored data cannot be read if the underlying storage drives are misplaced, lost, stolen, or discarded at their end-of-life.

Why use volume encryption?

Some of the benefits of encrypting a volume include:

Comprehensive protection for data-at-rest

All data and metadata within an encrypted volume—including files, folders, shared folders, LUNs, and installed packages—are stored in an encrypted format.

Added security against physical threats

Encrypting a volume ensures that sensitive or critical data cannot be accessed if your storage drives fall into the wrong hands. Access to data on an encrypted volume requires the correct encryption key.

Secure and centralized key management

The Encryption Key Vault serves as a secure repository for encryption keys used to access encrypted volumes. To keep them as secure as possible, these keys are never displayed in plaintext and are only accessible to the storage system hosting the encrypted volumes.

Consistent defense for all drive types

Applying encryption at the volume level provides consistent protection, regardless of the type of drives used. This means that you can encrypt and store volume data on drives without needing to invest in additional hardware, such as self-encrypting drives (SEDs).

Get started with volume encryption

To use volume encryption, all you need is a Synology NAS that supports this feature and runs DSM 7.2 or above. Check the list of supported models for more information.

How Volume Encryption Works

You can easily create and manage encrypted volumes through the **Storage Manager** application.

Enabling encryption upon volume creation

Encryption can be conveniently enabled as part of the volume creation process. Once encryption is activated for a volume, it cannot be turned off to ensure the constant protection of your data.

Data encryption

Volumes are encrypted using the **Advanced Encryption Standard (AES)** data encryption algorithm in **xts-plain64** mode. This algorithm is widely recognized for its robust cryptographic capabilities and is considered the industry standard for safeguarding data-at-rest.

Key generation

When encryption is enabled for a volume, a unique set of encryption keys is generated for that volume. Each set of keys includes:

- A **data encryption key** that encrypts all of the data on the volume. This key is stored in an encrypted format on the drive(s) that comprises the volume.
- A **volume encryption key** that unlocks data on the volume. This key confirms the decryption of the data encryption key and grants access to the volume data in its decrypted format. All volume encryption keys are stored in the Encryption Key Vault. The Encryption Key Vault serves as both a physical location for storing the keys and a tool for facilitating centralized management.
- A **recovery key** that serves as a backup to the volume encryption key. This key is the last resort for accessing an encrypted volume in case anything happens to the volume encryption key or the key vault containing it. You are responsible for keeping each encrypted volume's recovery key in a secure location.

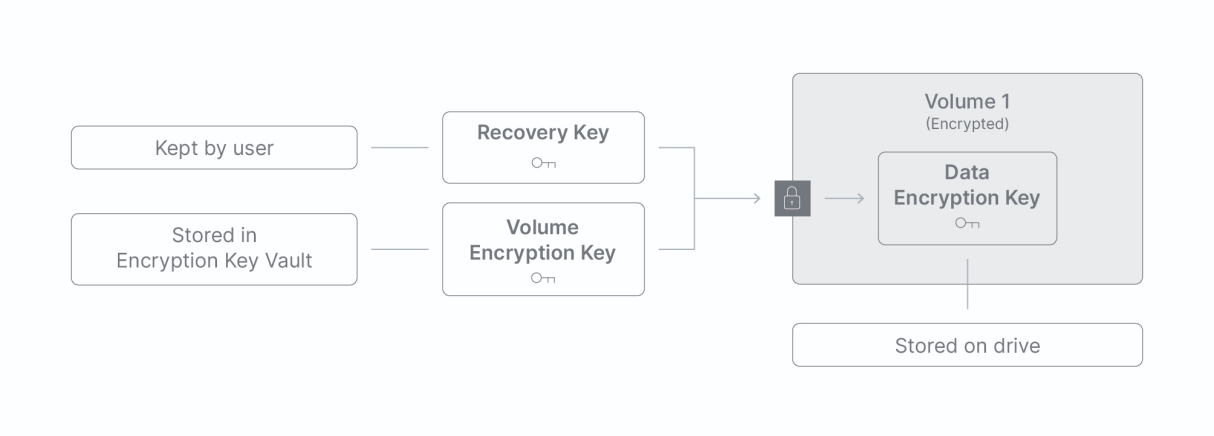

Figure 1: Keys generated when encryption is enabled for a volume

Key storage and management

The Encryption Key Vault simplifies the management of volume encryption keys by storing and managing them on your behalf. In addition to serving as a physical repository for these keys, the key vault introduces centralized management capabilities, such as:

- Enabling auto-unlocking of encrypted volumes at startup and restart by supplying keys to the storage system.
- Offering a unified interface to facilitate encryption key maintenance for you and your administrators across multiple volumes. This includes actions like resetting and replacing volume encryption keys for efficient key life-cycle management.

You can configure the key vault in one of two available storage locations:

Local key vault

The default option is to set up the Encryption Key Vault on the same Synology NAS where your encrypted volumes are stored. The **local key vault** option requires minimal configuration effort and is suitable for individuals with a single Synology NAS.

While the setup process is straightforward, the local key vault maintains stringent security standards for stored keys. It effectively safeguards against unauthorized access to encrypted volumes if the drives are stolen and misused. This security is enforced through the following methods:

Key Wrapping Using the Machine Key: The local key vault encrypts keys using the machine key native to the local NAS. Each Synology NAS has a unique machine key, so keys encrypted by a machine key can only be decrypted and used by the associated Synology NAS. Consequently, if the storage drives of an encrypted volume are stolen, the encrypted content remains inaccessible on any other NAS.

Vault Password: The local key vault requires you to set a vault password, which you will be prompted for each time you create an encrypted volume. Additionally, when the time comes to upgrade or replace your Synology NAS, this password plays a vital role in ensuring the seamless

migration of your encrypted volumes to the new device. To safeguard your data from unauthorized access, it is important to restrict access to the vault password to trusted individuals.

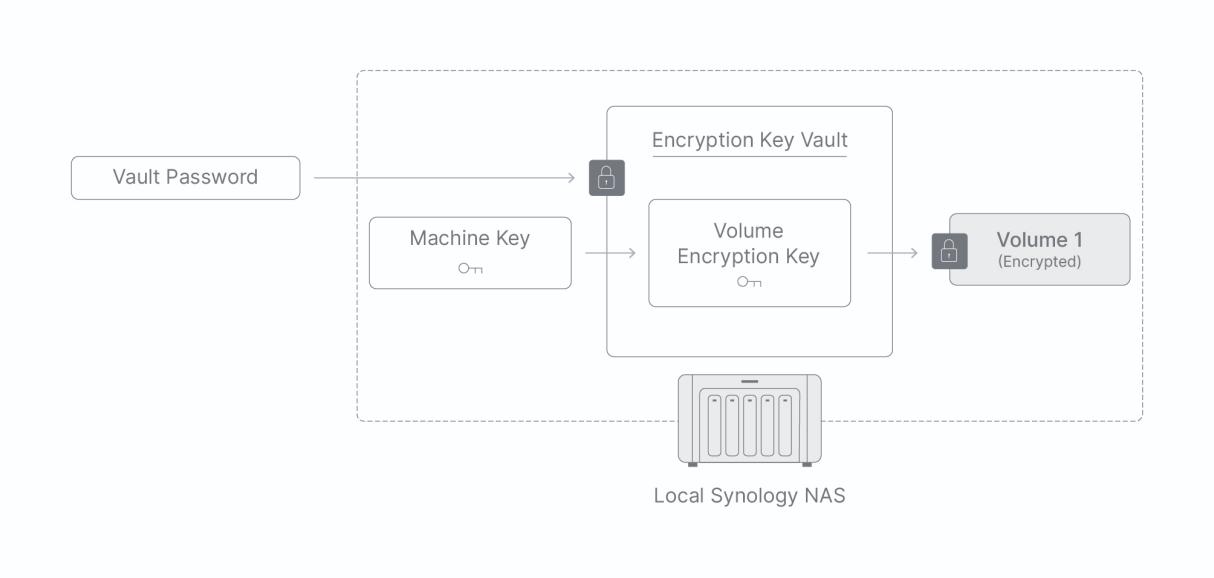

Figure 2: Storing the Encryption Key Vault on the local NAS

External key vault

Another option is to set up the Encryption Key Vault separately from your encrypted volumes and on a remote Synology NAS. Setting up an **external key vault** requires two Synology NAS devices: one acts as the "client" and stores the encrypted volumes, while the other serves as the "remote key server" responsible for key storage. While it may require some additional configurations, this method significantly enhances the security of your encrypted volumes.

Key Management Interoperability Protocol (KMIP): The communication between the two NAS devices (the client and the remote key server) uses KMIP, which is a standardized protocol governed by the Organization for the Advancement of Structured Information Standards (OASIS). KMIP enables the client to securely store and retrieve keys from the key vault on the remote key server, while also allowing the remote key server to provide keys to the connected client.

Secure SSL Connection: To reinforce security, KMIP incorporates support for SSL, ensuring a secure connection between the client and the remote key server. SSL encrypts the connection to prevent data tampering and ensure confidentiality, authenticity, and integrity during transmission.

The use of an external key vault broadens the protective scope of volume encryption. It not only guards against the theft or misplacement of storage drives but also covers the loss of an entire NAS system. Access to the external key vault is severed when the NAS hosting the encrypted volumes moves outside the local area network or when you manually terminate the connection.

The external key vault proves ideal if:

- You possess two or more Synology NAS.
- You require an encryption key management system based on the OASIS KMIP standard.
- You prefer to maintain separation between volume encryption keys and encrypted data.

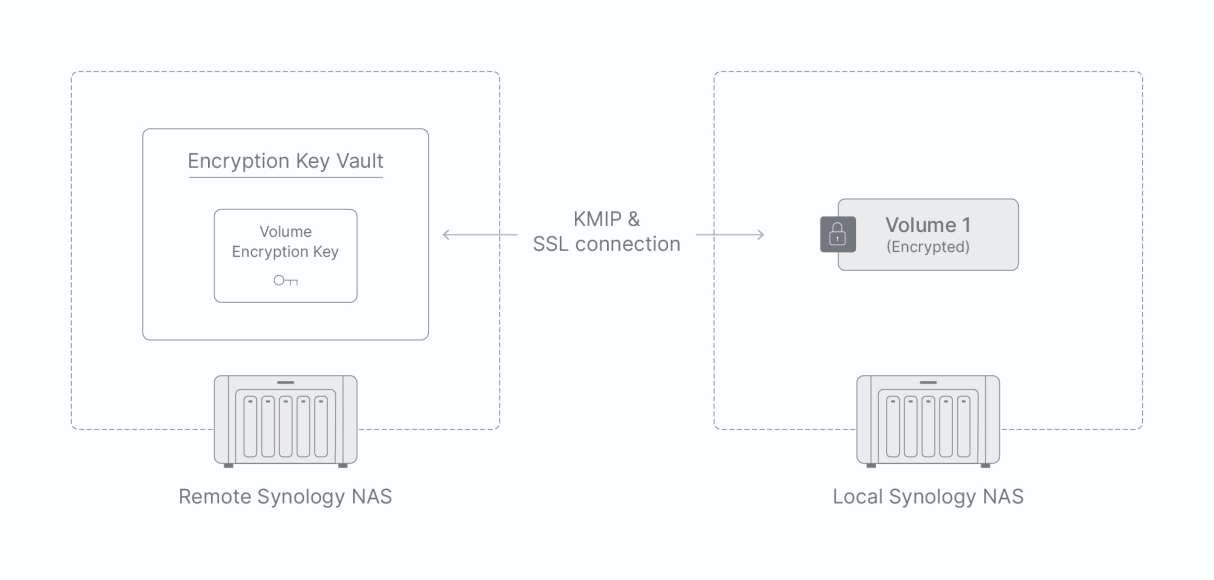

Figure 3: Storing the Encryption Key Vault on a remote NAS via KMIP

Accessing data on an encrypted volume

Enabling volume encryption does not compromise ease of use. You can store and access data in the same way as you normally would while ensuring stored data is protected.

Synology's volume encryption relies on two core technologies: **Linux Unified Key Setup (LUKS)** and **device mapper crypt (dm-crypt)**. LUKS defines the overall framework for volume encryption, while dm-crypt offers transparent encryption capabilities. The latter is particularly important because it ensures that encryption/decryption processes happen seamlessly and automatically in the background.

Managing access to an encrypted volume

Once encryption is enabled for a volume, it will always be in one of two states: locked and inaccessible, or unlocked and accessible.

Unlocked

All encrypted volumes are **auto-unlocked** at system startup or restart, provided that the Encryption Key Vault and the corresponding volume encryption keys are available. When an encrypted volume is in an unlocked state, all of its parts become accessible.

To ensure successful data access and minimal disruption to associated services, it is imperative to have the Encryption Key Vault readily available to the storage system during startup and restart.

Locked

During system startup, if the Encryption Key Vault is disconnected or otherwise unavailable, auto-unlocking cannot take place. As a result, all encrypted volumes will remain in a locked and inaccessible state, causing any services or packages associated with them to be suspended or denied access.

The only way to regain access to the locked volumes is by using their corresponding recovery key. In the case of multiple locked encrypted volumes, each one must be **manually unlocked** with its respective recovery key.

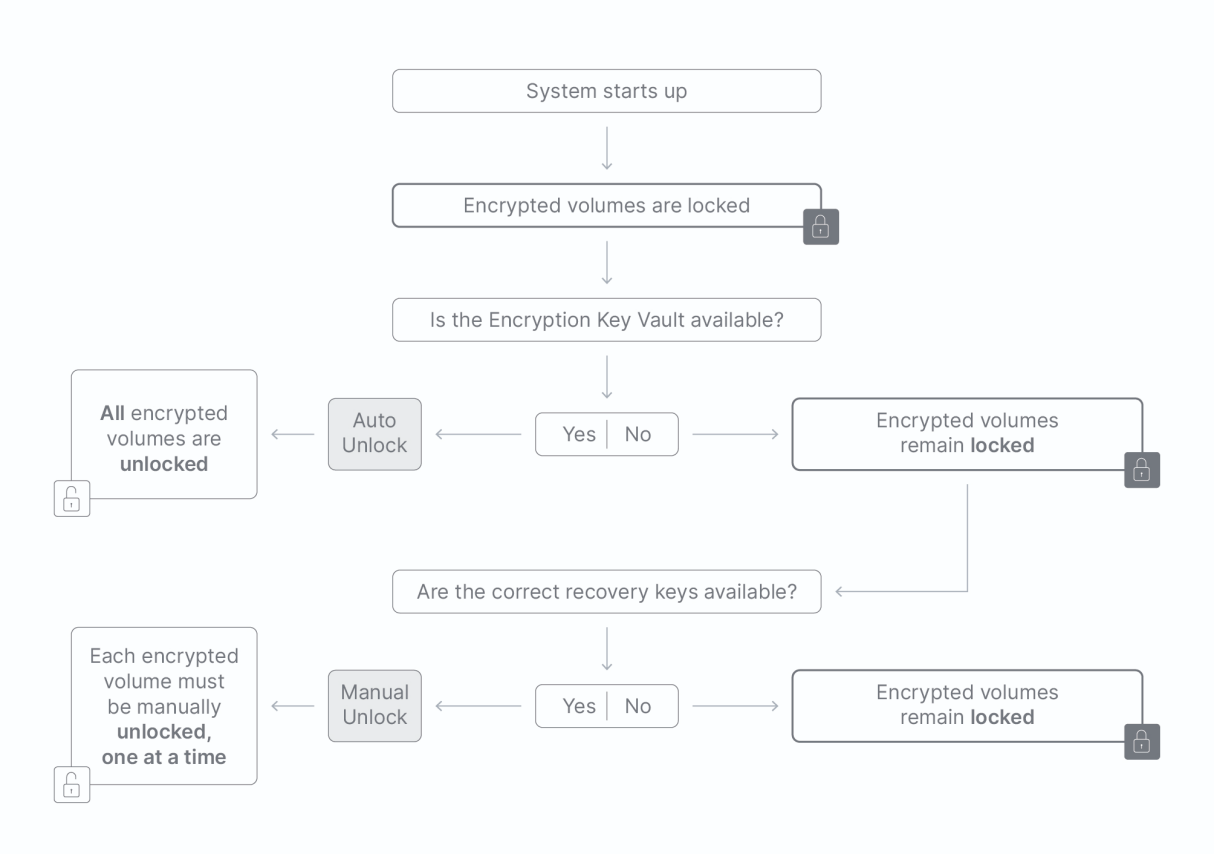

Figure 4: Unlocking process of encrypted volumes

Best Practices

The following sections provide recommendations on how to effectively implement and manage Synology's volume encryption solution.

Understand the scope of protection

Volume encryption protects **data-at-rest** against physical loss or theft of storage drives. It is important to recognize that while this feature adds an additional layer of security to your data, it cannot safeguard against all potential threats. For example, the following scenarios fall outside the scope of volume encryption's protection:

- Data-in-use or in-transit, including data temporarily stored in system memory
- Inadvertent or malicious data destruction
- Loss of an entire NAS system (only protected when using an external key vault)

Understanding these scenarios can help you make informed decisions regarding your data security strategies and determine how to implement additional security measures.

Set up the Encryption Key Vault first

Before creating your initial encrypted volume, we strongly recommend you to enable and set up the Encryption Key Vault in advance. Doing so will facilitate a more seamless volume creation process.

If you have not completed this preliminary setup, you will still be guided to do it during the volume creation process. However, when using the volume creation wizard, the only available storage location for the key vault is the default **Local** option. Therefore, if you want to utilize an external key vault, you must set it up beforehand.

Change the keys regularly

Prolonged use of a single key can expose you to security risks. Therefore, we recommend that you or your organization change both the volume encryption keys and the recovery keys on a regular basis. You can non-disruptively change both of these keys through the Storage Manager interface. Once the old keys are replaced, they become invalid and cannot be reused.

Store recovery keys separately

Make sure that you do not store recovery keys within encrypted volumes. Recovery keys are essential for accessing your data in case of a problem with the Encryption Key Vault. Therefore, it is vital that you keep your recovery keys in a separate location to ensure its security so you'll always be able to access your data.