Datasheet

NetApp Volume Encryption

Key Benefits

Promote Data Integrity and Privacy

NVE is a software-based method to encrypt and protect data from theft if a disk is repurposed, sent in for return merchandise authorization, misplaced, or stolen.

Maintain Secure Posture Regardless of Physical Media

Using encryption at the volume level allows the encryption capability to exist independently of the physical media (for example, SSD, All Flash FAS, or even self-encrypting drives [SEDs]).

Maintain Storage Efficiencies

NVE allows you to encrypt your data while maintaining NetApp storage efficiencies such as deduplication and compression.

The Solution

This datasheet provides an overview of the NetApp® Volume Encryption (NVE) solution. A clear understanding of the essential components and details that make up the NVE solution is vital for an organization so that it can implement the most effective solution for its data encryption needs.

NetApp Volume Encryption

NVE is a software-based, data-at-rest encryption solution available starting with NetApp ONTAP® 9.1. NVE allows ONTAP to encrypt data (using AES 256-bit encryption) for each volume for granularity. Data can also be stored on disk without SEDs. NVE enables you to use storage efficiency features that would be lost with encryption at the application layer. Storage efficiencies are maintained because the data comes in from the network through NetApp WAFL® (Write Anywhere File Layout) to the RAID layer, which determines whether the data should be encrypted.

If data should be encrypted, it is sent to the cryptographic module (currently under test for FIPS 140-2 level 1 validation). The cryptographic module encrypts the data and sends it back to the RAID layer. The encrypted data is then sent to disk. With the NVE solution, the data is already encrypted on the way to the disk. Reads follow the reverse path. In summary, the data leaves the disk encrypted, is sent to RAID, is decrypted by the cryptographic module, and is then sent up the rest of the stack. This process is outlined in Figure 1.

Onboard Key Management

NVE uses onboard key management. NVE is comprised of a software cryptographic NVE can use onboard key management. NVE is composed of a software cryptographic module, encryption keys, and an onboard key manager. NVE leverages a unique XTS-AES-256 data encryption key for each volume. The encryption keys are stored within the onboard key manager, which keeps track of all the encryption keys used by ONTAP. The keys used for a data volume are unique to that data volume in that cluster. The keys are generated when the encrypted volume is created. ONTAP does not pregenerate or reuse keys. These keys are never displayed in plain text and are stored and protected by the onboard key manager.

NetApp®

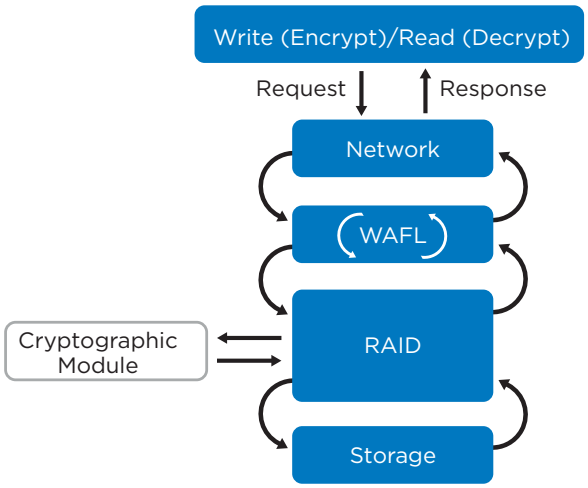

Figure 1) NVE cryptographic function.

NVE allows you to change the data encryption key on a volume nondisruptively so that your organization can define a key lifecycle management policy. After the existing data is encrypted with the new key, the old key is removed from the key table and cannot be used again. Encryption key management policies are determined and administrated by your organization's storage administrator. An encrypted backup of the keys and the passphrase used to derive them are required for recovery from a disaster recovery event.

External Key Management

Starting with ONTAP 9.3, NVE can use external key management with the industry standard OASIS Key Management Interoperability Protocol (KMIP). NVE volume encryption keys are stored on the external key manager. If the controller and disks are moved without access to the external key manager, the NVE volumes won't be accessible and cannot be decrypted.

Common Questions About NVE

- **Must all my volumes be encrypted, as is the case with NSE?**
  No. With NVE, you can choose which volumes to encrypt. See the Resources section for more information about NSE.
- **Can I use NSE drives as well as NVE?**
  Yes. NVE adds another layer of encryption on top of NSE drives.
- **Are NetApp storage efficiency technologies maintained when using NVE?**
  Yes. With NVE, the cryptographic module performs data encryption at the RAID layer, which allows storage efficiency functions to remain in place because they are performed prior to encryption.
- **Are NetApp Snapshot™ copies and NetApp FlexClone® volumes encrypted?**
  Yes.
- **Are root aggregate volumes and storage virtual machine volumes encrypted**?
  No. These volumes contain configuration information for the ONTAP storage system. Customer data should be stored on the data volumes. ONTAP actively prevents the creation of data volumes on root aggregates.
- **How does NVE protect a disk that was repurposed, sent in for return merchandise authorization, misplaced, or stolen?**
  Multiple encrypted volumes can reside on a single drive, and each has its own unique key. The encryption keys required to decrypt the data are not included on the disk. Thus, an attack would have to use brute force or it would have to cryptographically break AES-256 encryption multiple times to have access to any of the data on the drive. Because WAFL spreads data across drives, data decryption is highly unlikely.

NVE Basics

- Encrypts at volume level
- Software-based
- XTS-AES-256 encryption
- No need for SEDs
- Onboard key manager or external KMIP key manager
- FIPS 140-2 level 1 validation (pending)

Contact your account team to find out more about how the NSE and NVE solutions can support your organization's needs.

Resources

- NetApp Storage Encryption Datasheet
- NetApp Storage Encryption and NetApp Volume Encryption
- Security Hardening Guide for NetApp ONTAP 9
- Security Features in ONTAP 9 Datasheet

About NetApp

NetApp is the data authority for hybrid cloud. We provide a full range of hybrid cloud data services that simplify management of applications and data across cloud and on-premises environments to accelerate digital transformation. Together with our partners, we empower global organizations to unleash the full potential of their data to expand customer touchpoints, foster greater innovation and optimize their operations. For more information, visit www.netapp.com. #DataDriven