Datasheet

NetApp Volume Encryption and NetApp Aggregate Encryption

Key Benefits

Promote Data Integrity and Privacy
NVE and NAE are software-based methods to encrypt and protect data from theft if a disk is repurposed, sent in for Return Material Authorization, misplaced, or stolen.

Maintain Secure Posture Regardless of Physical Media
FIPS 140-2 compliant encryption at the volume level makes encryption independent of the physical media—for example, solid-state drives (SSDs), NetApp AFF, or even NetApp Storage Encryption (NSE) self-encrypting drive (SEDs).

Maintain Storage Efficiencies
NVE and NAE allow you to encrypt your data while maintaining NetApp storage efficiencies such as deduplication and compression. With NAE, you can also maintain aggregate deduplication.

The Solution

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

NetApp Volume Encryption and NetApp Aggregate Encryption

NVE is a software-based, data-at-rest encryption solution available starting with NetApp ONTAP® 9.1, and it has been FIPS 140-2 compliant since ONTAP 9.2. NVE allows ONTAP to encrypt data for each volume for granularity. NAE, available with ONTAP 9.6, is an outgrowth of NVE; it allows ONTAP to encrypt data for each volume, and the volumes can share keys across the aggregate. Both NVE and NAE use AES 256-bit encryption. Data can also be stored on disk without SEDs.

NVE and NAE enable 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® to the RAID layer, which determines whether the data should be encrypted. For greater storage efficiency, you can use aggregate deduplication with NAE. NVE volumes and NAE volumes can coexist on the same NAE aggregate. NAE aggregates do not support unencrypted volumes.

Here's how the process works: If data should be encrypted, it is sent to the cryptographic module (CryptoMod), which is FIPS 140-2 level 1 validated. The CryptoMod encrypts the data and sends it back to the RAID layer. The encrypted data is then sent to disk. So, with the combination of NVE and NAE, the data is already encrypted on the way to the disk. Reads follow the reverse path. In other words, the data leaves the disk encrypted, is sent to RAID, is decrypted by the CryptoMod, and is then sent up the rest of the stack. This process is outlined in Figure 1.

Onboard Key Management

The combined NVE and NAE solution is composed of a software CryptoMod, encryption keys, and an onboard key manager. For each volume, NVE uses a unique XTS-AES 256 data encryption key, which the onboard key manager stores. The key used for a data volume is unique to that data volume in that cluster and is generated when the encrypted volume is created. Similarly, NAE volumes use unique XTS-AES 256 data encryption keys per aggregate, which the onboard key manager also stores. NAE keys are generated when the encrypted aggregate is created. ONTAP does not

NetApp®

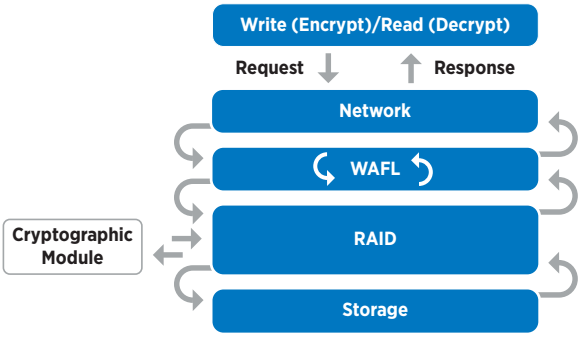

Figure 1) NVE and NAE cryptographic function.

pregenerate keys, reuse them, or display them in plain text; they are stored and protected by the onboard key manager.

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 administered by your organization's storage administrator. An encrypted backup of the keys and the passphrase used to derive them are required for disaster recovery.

External Key Management

NVE (starting with ONTAP 9.3) and NAE (starting with ONTAP 9.6) can use external key management with the industry-standard OASIS Key Management Interoperability Protocol (KMIP). Volume and aggregate encryption keys are stored on an external key manager. If the controller and disks are moved and no longer have access to the external key manager, the NVE and NAE volumes won't be accessible and cannot be decrypted.

Common Questions About NVE and NAE

Must all my volumes be encrypted, as is the case with NSE?
No. With NVE, you can choose which volumes to encrypt. For NAE aggregates, every volume must be either NVE or NAE encrypted. (See the Resources section for more information about NSE.)

Can I use NSE drives as well as NVE and NAE?
Yes. NVE and NAE add another layer of encryption on top of NSE drives.

Are NetApp storage efficiency technologies maintained when I use NVE and NAE?
Yes. With NVE and NAE, the CryptoMod performs data encryption at the RAID layer, which allows storage efficiency functions to remain in place because they are performed prior to encryption. With NAE, aggregate deduplication is enabled.

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 do NVE and NAE protect a disk that was repurposed, sent in for Return Material 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 and NAE Basics

- Encrypt at the 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 validated

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

Resources

- NetApp Storage Encryption datasheet
- NetApp Storage Encryption, NVMe Self-Encrypting Drives, NetApp Volume Encryption, and NetApp Aggregate Encryption datasheet
- 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