Why do data encryption in the NetApp Data ONTAP storage clusters, drives using NSE, or volumes using NVE?

Summary:

Confirm data security to stored business data in the infrastructure, configuring data encryption using drives (NSE) or volumes (NVE) in the storage arrays.

In-depth:

- To maintain security and compliance to end-users data, we need to configure encryption in NetApp storage devices.
- Use encrypting hardware (drives) or software (volumes) in storage infrastructure. It will protect businesses from the risk of data decryption/ misuse of data by any 3rd party actor(s), even though failed drive sent outside data center/ premises as a part of RMA process.
- While new storage site design, prefer the clients to purchase NSE drives. It may involve extra payment, as NSE drives are more expensive than non-NSE drives, but business/ end-users data will be safe and secured and cannot be decrypted without a key, as the encryption key vaulted by the client/ storage owner only.
- If a storage infrastructure site is already built and established, then prefer the clients to purchase an NVE license to enable logical volumes for the data encryption.

Process of configuration (where no implementation done for the clients):

a. Hardware:

i. Onboard key management means within the storage cluster using the NSE drives.

- This method is preferred as there is no external server(s) availability/ dependency/ requirement for any connection type.

Step 1: cluster_name::> security key-manager onboard enable

Step 2: At the passphrase prompt, enter a passphrase up to 256 characters and re-enter to confirm.

Step 3: cluster_name::> security key-manager key query -node node_name

Step 4: Please copy the passphrase to a secure location outside the storage cluster. It is backed up internally by the replicated database.

Step 5: cluster_name::> storage encryption disk modify -disk disk_ID(s) -data-key-id key_ID

Step 6: cluster_name::> storage encryption disk show

b. Software:

- This method is preferred as there is no external server(s) availability/ dependency/ requirement for any connection type.

Step 1: Determine whether the storage cluster version (Data ONTAP) supports NVE.

cluster_name::> version -v

NetApp Release 9.xPx: XXXXXXXXXXXXXXXX <1O>

1Ono-DARE: no, Data At Rest Encryption [then DOWNLOAD ONTAP 9.xPx WITH NETAPP VOLUME ENCRYPTION and update the firmware].

1O: yes, Data At Rest Encryption.

Step 2: Install the NVE license.

Step 3: cluster_name::> security key-manager onboard enable

Step 4: At the passphrase prompt, enter a passphrase up to 256 characters and re-enter to confirm.
Step 5: cluster_name::> security key-manager key query -node node_name
Step 6: Please copy the passphrase to a secure location outside the storage cluster. It is backed up internally by the replicated database.
Step 7: Various methods:
i. cluster_name::> storage aggregate create -aggregate aggregate_name -encrypt-with-aggr-key true
or,
ii. cluster_name::> volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -encrypt true
cluster_name::> volume show -is-encrypted true
or,
iii. cluster_name::> volume encryption conversion start -vserver vserver_name -volume volume_name
cluster_name::> volume encryption conversion show
cluster_name::> volume show -is-encrypted true

Reason(s) for the activity:

Benefits to the clients:

- It will maintain data compliance, confidentiality, and security.
- Follow the right design, capacity planning, and recommendations in storage arrays. Latency should not be there after implementing data encryption in clusters.
- The decryption of data by 3rd party actor not possible.
- Involves one-time additional cost to project only.

Where,

Abbreviation	Details
Data ONTAP/ ONTAP	The operating system of NetApp AFF/FAS array models [ONTAP or Data ONTAP or Clustered Data ONTAP (cDOT) or Data ONTAP 7-Mode is NetApp's proprietary operating system].
NSE	NetApp Storage Encryption
NVE	NetApp Volume Encryption
NetApp	Storage vendor.
RMA	Return Merchandise Authorization
aggr	Storage aggregate
vol	Storage volume
RDB	Replicated Database
9.xPx	“x” is sub-version
SSH	Secure Shell login using PuTTY.
CLI	Command Line Interface.

By:

Ashish Sharma

Senior SME