Encrypt volume data with NVE

ONTAP 9

NetApp
November 28, 2022

Table of Contents

Encrypt volume data with NVE

Encrypt volume data with NVE overview

Beginning with ONTAP 9.7, aggregate and volume encryption is enabled by default when you have the VE license and onboard or external key management. For ONTAP 9.6 and earlier, you can enable encryption on a new volume or on an existing volume. You must have installed the VE license and enabled key management before you can enable volume encryption. NVE is FIPS-140-2 level 1 compliant.

Enable aggregate-level encryption with VE license

Beginning with ONTAP 9.7, newly created aggregates and volumes are encrypted by default when you have the VE license and onboard or external key management. Beginning with ONTAP 9.6, you can use aggregate-level encryption to assign keys to the containing aggregate for the volumes to be encrypted. Volumes you create in the aggregate are encrypted by default. You can override the default when you encrypt the volume.

What you'll need

You must be a cluster administrator to perform this task.

About this task

You must use aggregate-level encryption if you plan to perform inline or background aggregate-level deduplication. Aggregate-level deduplication is otherwise not supported by NVE.

An aggregate enabled for aggregate-level encryption is called an *NAE aggregate* (for NetApp Aggregate Encryption). Plain text volumes are not supported in NAE aggregates.

Steps

1. Enable or disable aggregate-level encryption:

To…	Use this command…
Create an NAE aggregate with ONTAP 9.7 or later	`storage aggregate create -aggregate aggregate_name -node node_name`
Create an NAE aggregate with ONTAP 9.6	`storage aggregate create -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true`
Convert a non-NAE aggregate to an NAE aggregate	`storage aggregate modify -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true`

Convert an NAE aggregate to a non-NAE aggregate	`storage aggregate modify -aggregate aggregate_name -node node_name -encrypt-with -aggr-key false`

For complete command syntax, see the man pages.

The following command enables aggregate-level encryption on `aggr1`:

- ONTAP 9.7 or later:

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 or earlier:

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

2. Verify that the aggregate is enabled for encryption:

`storage aggregate show -fields encrypt-with-aggr-key`

For complete command syntax, see the man page.

The following command verifies that `aggr1` is enabled for encryption:

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate            encrypt-aggr-key
-------------------- ----------------
aggr0_vsim4          false
aggr1                true
2 entries were displayed.
```

After you finish

Run the `volume create` command to create the encrypted volumes.

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically “pushes” an encryption key to the server when you encrypt a volume.

Enable encryption on a new volume

You can use the `volume create` command to enable encryption on a new volume.

About this task

Beginning with ONTAP 9.2, you can enable encryption on a SnapLock volume.

Beginning with ONTAP 9.4, if you enable “cc-mode” when you set up the Onboard Key Manager, volumes you create with the `volume create` command are automatically encrypted, whether or not you specify `-encrypt true`.

Beginning with ONTAP 9.6, you can use aggregate-level encryption to assign keys to the containing aggregate for the volumes to be encrypted. Volumes you create in the aggregate are encrypted by default. You can use the `-encrypt` option to override the default when you create the volume.

Beginning with ONTAP 9.7, newly created volumes are encrypted by default when you have the VE license and onboard or external key management.

A volume encrypted with a unique key is called an *NVE volume*. A volume encrypted with an aggregate-level key is called an *NAE aggregate* (for NetApp Aggregate Encryption). Plaintext volumes are not supported in NAE aggregates.

Steps

1. Create a new volume and specify whether encryption is enabled on the volume:

To create…	Use this command…
An ONTAP 9.7 or later NAE volume	`volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name`
An ONTAP 9.6 NAE volume (assuming aggregate-level encryption is enabled)	`volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name`
An ONTAP 9.7 or later NVE volume	`volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name`
An ONTAP 9.6 or earlier NVE volume	`volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt true`
A plain text volume	`volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt false`

For complete command syntax, see the man page for the command.

Beginning with ONTAP 9.7 or later, the following command creates an NAE volume named `vol1` on `aggr1`:

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1
```

Using ONTAP 9.6, assuming aggregate-level encryption is enabled, the following command creates an NAE volume named `vol1` on `aggr1`:

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1
```

Beginning with ONTAP 9.7 or later, the following command creates an NVE volume named `vol2` on `aggr1`:

```
cluster1::> volume create -vserver vs1 -volume vol2 -aggregate aggr1
```

Using ONTAP 9.6 or earlier, the following command creates an NVE volume named `vol2` on `aggr1`:

```
cluster1::> volume create -vserver vs1 -volume vol2 -aggregate aggr1
-encrypt true
```

The following command creates a plaintext volume named `vol3` on `aggr1`:

```
cluster1::> volume create -vserver vs1 -volume vol3 -aggregate aggr1
-encrypt false
```

2. Verify that volumes are enabled for encryption:

   `volume show -is-encrypted true`

   For complete command syntax, see the man page for the command.

   The following command displays the encrypted volumes on `cluster2`:

```
cluster2::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Result

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically “pushes” an encryption key to the server when you encrypt a volume.

Enable encryption on an existing volume with the volume encryption conversion start command

Beginning with ONTAP 9.3, you can use the `volume encryption conversion start` command to enable encryption of an existing volume "in place," without having to move the volume to a different location.

About this task

Once you start a conversion operation, it must complete. If you encounter a performance issue during the operation, you can run the `volume encryption conversion pause` command to pause the operation, and the `volume encryption conversion resume` command to resume the operation.

You cannot use `volume encryption conversion start` to convert a SnapLock volume.

Steps

1. Enable encryption on an existing volume:

   `volume encryption conversion start -vserver SVM_name -volume volume_name`

   For complete command syntax, see the man page for the command.

   The following command enables encryption on the existing volume `vol1`:

   ```
   cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
   ```

   The system creates an encryption key for the volume. The data on the volume is encrypted.

2. Verify the status of the conversion operation:

   `volume encryption conversion show`

   For complete command syntax, see the man page for the command.

   The following command displays the status of the conversion operation:

   ```
   cluster1::> volume encryption conversion show

   Vserver   Volume   Start Time           Status
   -------   ------   ------------------   --------------------------
   vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. When the conversion operation is complete, verify that the volume is enabled for encryption:

   `volume show -is-encrypted true`

   For complete command syntax, see the man page for the command.

   The following command displays the encrypted volumes on `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Result

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically “pushes” an encryption key to the server when you encrypt a volume.

Enable encryption on an existing volume with the volume move start command

You can use the `volume move start` command to enable encryption by moving an existing volume. You must use `volume move start` in ONTAP 9.2 and earlier. You can use the same aggregate or a different aggregate.

What you’ll need

You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

Delegating authority to run the volume move command

About this task

Beginning with ONTAP 9.8, you can use `volume move start` to enable encryption on a SnapLock or FlexGroup volume.

Beginning with ONTAP 9.4, if you enable “cc-mode” when you set up the Onboard Key Manager, volumes you create with the `volume move start` command are automatically encrypted. You need not specify `-encrypt-destination true`.

Beginning with ONTAP 9.6, you can use aggregate-level encryption to assign keys to the containing aggregate for the volumes to be moved. A volume encrypted with a unique key is called an *NVE volume*. A volume encrypted with an aggregate-level key is called an *NAE volume* (for NetApp Aggregate Encryption). Plaintext volumes are not supported in NAE aggregates.

Steps

1. Move an existing volume and specify whether encryption is enabled on the volume:

To convert…	Use this command…
A plaintext volume to an NVE volume	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination true`

An NVE or plaintext volume to an NAE volume (assuming aggregate-level encryption is enabled on the destination)	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true`
An NAE volume to an NVE volume	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false`
An NAE volume to a plaintext volume	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false`
An NVE volume to a plaintext volume	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false`

For complete command syntax, see the man page for the command.

The following command converts a plaintext volume named `vol1` to an NVE volume:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

Assuming aggregate-level encryption is enabled on the destination, the following command converts an NVE or plaintext volume named `vol1` to an NAE volume:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

The following command converts an NAE volume named `vol2` to an NVE volume:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

The following command converts an NAE volume named `vol2` to a plaintext volume:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

The following command converts an NVE volume named `vol2` to a plaintext volume:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. View the encryption type of cluster volumes:

   `volume show -fields encryption-type none|volume|aggregate`

   The `encryption-type` field is available in ONTAP 9.6 and later.

   For complete command syntax, see the man page for the command.

   The following command displays the encryption type of volumes in `cluster2`:

```
cluster2::> volume show -fields encryption-type

vserver  volume  encryption-type
-------  ------  ---------------
vs1      vol1    none
vs2      vol2    volume
vs3      vol3    aggregate
```

3. Verify that volumes are enabled for encryption:

   `volume show -is-encrypted true`

   For complete command syntax, see the man page for the command.

   The following command displays the encrypted volumes on `cluster2`:

```
cluster2::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Result

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically “pushes” an encryption key to the server when you encrypt a volume.

Enable node root volume encryption

Beginning with ONTAP 9.8, you can use NetApp Volume Encryption to protect the root volume of your node.

What you’ll need

- Your system must be using an HA configuration.

  Root volume encryption is not supported on single node configurations.

- Your node root volume must already be created.
- Your system must have an onboard key manager or an external key management server using the Key Management Interoperability Protocol (KMIP).

About this task

This procedure applies to the node root volume. It does not apply to SVM root volumes. SVM root volumes can be protected through aggregate-level encryption.

Once root volume encryption begins, it must complete. You cannot pause the operation. Once encryption is complete, you cannot assign a new key to the root volume and you cannot perform a secure-purge operation.

Steps

1. Encrypt the root volume:

   ```
   volume encryption conversion start -vserver SVM_name -volume root_vol_name
   ```

2. Verify the status of the conversion operation:

   ```
   volume encryption conversion show
   ```

3. When the conversion operation is complete, verify that the volume is encrypted:

   ```
   volume show -fields
   ```

   The following shows example output for an encrypted volume.

   ```
   ::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
   vserver    volume is-encrypted
   ---------- ------ ------------
   xyz        vol0   true
   ```

Copyright information

Trademark information