



Manage NetApp encryption

ONTAP 9

NetApp
November 04, 2021

Table of Contents

Manage NetApp encryption	1
Unencrypt volume data	1
Move an encrypted volume	1
Delegate authority to run the volume move command	2
Change the encryption key for a volume with the volume encryption rekey start command	3
Change the encryption key for a volume with the volume move start command	4
Rotate authentication keys for NetApp Storage Encryption	5
Delete an encrypted volume	6
Securely purge data on an encrypted volume	6
Change the onboard key management passphrase	11
Back up onboard key management information manually	13
Restore onboard key management encryption keys	14
Restore external key management encryption keys	15
Replace SSL certificates	17
Replace a FIPS drive or SED	17
Make data on a FIPS drive or SED inaccessible	19
Return a FIPS drive or SED to service when authentication keys are lost	24
Return a FIPS drive or SED to unprotected mode	26
Delete an external key manager connection	27
Modify external key management server properties	28
Transition to external key management from onboard key management	29
Transition to onboard key management from external key management	30
What happens when key management servers are not reachable during the boot process	31
Disable encryption by default with ONTAP 9.7 and later	32

Manage NetApp encryption

Unencrypt volume data

You can use the `volume move start` command to move and unencrypt volume data.

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](#)

Steps

1. Move an existing encrypted volume and unencrypt the data on the 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 moves an existing volume named `vol1` to the destination aggregate `aggr3` and unencrypts the data on the volume:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination  
-aggregate aggr3 -encrypt-destination false
```

The system deletes the encryption key for the volume. The data on the volume is unencrypted.

2. Verify that the volume is disabled for encryption:

```
volume show -encryption
```

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

The following command displays whether volumes on `cluster1` are encrypted:

```
cluster1::> volume show -encryption
```

Vserver	Volume	Aggregate	State	Encryption State
-----	-----	-----	-----	-----
vs1	vol1	aggr1	online	none

Move an encrypted volume

You can use the `volume move start` command to move an encrypted volume. The moved volume can reside on 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

The move will fail if the destination node or destination volume does not support volume encryption.

The `-encrypt-destination` option for `volume move start` defaults to `true` for encrypted volumes. Requiring you to specify explicitly that you do not want the destination volume to be encrypted ensures that you do not inadvertently unencrypt the data on the volume.

Steps

1. Move an existing encrypted volume and leave the data on the volume encrypted:

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate  
aggregate_name
```

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

The following command moves an existing volume named `vol1` to the destination aggregate `aggr3` and leaves the data on the volume encrypted:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination  
-aggregate aggr3
```

2. 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	aggr3	online	RW	200GB	160.0GB	20%

Delegate authority to run the volume move command

You can use the `volume move` command to encrypt an existing volume, move an encrypted volume, or unencrypt a volume. Cluster administrators can run `volume move` command themselves, or they can delegate the authority to run the command to SVM administrators.

About this task

By default, SVM administrators are assigned the `vsadmin` role, which does not include the authority to move volumes. You must assign the `vsadmin-volume` role to SVM administrators to enable them to run the `volume move` command.

Step

1. Delegate authority to run the `volume move` command:

```
security login modify -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role vsadmin-  
volume
```

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

The following command grants the SVM administrator authority to run the `volume move` command.

```
cluster1::>security login modify -vserver engData -user-or-group-name  
SVM-admin -application ssh -authmethod domain -role vsadmin-volume
```

Change the encryption key for a volume with the `volume encryption rekey start` command

It is a security best practice to change the encryption key for a volume periodically. Starting with ONTAP 9.3, you can use the `volume encryption rekey start` command to change the encryption key.

About this task

Once you start a rekey operation, it must complete. There is no returning to the old key. If you encounter a performance issue during the operation, you can run the `volume encryption rekey pause` command to pause the operation, and the `volume encryption rekey resume` command to resume the operation.

Until the rekey operation finishes, the volume will have two keys. New writes and their corresponding reads will use the new key. Otherwise, reads will use the old key.



You cannot use `volume encryption rekey start` to rekey a SnapLock volume.

Steps

1. Change an encryption key:

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

The following command changes the encryption key for `vol1` on `SVMvs1`:

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

2. Verify the status of the rekey operation:

```
volume encryption rekey show
```

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

The following command displays the status of the rekey operation:

```
cluster1::> volume encryption rekey show
```

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

3. When the rekey 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%

Change the encryption key for a volume with the volume move start command

It is a security best practice to change the encryption key for a volume periodically. You can use the `volume move start` command to change the encryption key. You must use `volume move start` in ONTAP 9.2 and earlier. The moved volume can reside on 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

You cannot use `volume move start` to rekey a SnapLock or FlexGroup volume.

Steps

1. Move an existing volume and change the encryption key:

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate
aggregate_name -generate-destination-key true
```

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

The following command moves an existing volume named **vol1** to the destination aggregate **aggr2** and changes the encryption key:

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

A new encryption key is created for the volume. The data on the volume remains encrypted.

2. 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%

Rotate authentication keys for NetApp Storage Encryption

You can rotate authentication keys when using NetApp Storage Encryption (NSE).

About this task

Rotating authentication keys in an NSE environment is supported if you are using External Key Manager (KMIP).



Rotating authentication keys in an NSE environment is not supported for Onboard Key Manager (OKM).

Steps

1. Use the `security key-manager create-key` command to generate new authentication keys.

You need to generate new authentication keys before you can change the authentication keys.

2. Use the `storage encryption disk modify -disk * -data-key-id` command to change the authentication keys.

Delete an encrypted volume

You can use the `volume delete` command to delete an encrypted volume.

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](#)

- The volume must be offline.

Step

1. Delete an encrypted volume:

```
volume delete -vserver SVM_name -volume volume_name
```

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

The following command deletes an encrypted volume named `vol1`:

```
cluster1::> volume delete -vserver vs1 -volume vol1
```

Enter `yes` when you are prompted to confirm deletion.

The system deletes the encryption key for the volume after 24 hours.

Use `volume delete` with the `-force true` option to delete a volume and destroy the corresponding encryption key immediately. For more information, see the man page.

After you finish

You can use the `volume recovery-queue` command to recover a deleted volume during the retention period after issuing the `volume delete` command:

```
volume recovery-queue SVM_name -volume volume_name
```

[How to use the Volume Recovery feature](#)

Securely purge data on an encrypted volume

Securely purge data on an encrypted volume overview

Beginning in ONTAP 9.4, you can use secure purge to non-disruptively scrub data on NVE-enabled volumes. Scrubbing data on an encrypted volume ensures that it cannot be recovered from the physical media, for example, in cases of “spillage,” where data traces may have been left behind when blocks were overwritten, or for securely deleting a vacating tenant’s data.

Secure purge works only for previously deleted files on NVE-enabled volumes. You cannot scrub an unencrypted volume. You must use KMIP servers to serve keys, not the onboard key manager.

Secure purge functions differently depending upon your version of ONTAP.

- In ONTAP 9.8 and later:
 - Secure purge is supported by MetroCluster and FlexGroup.
 - If the volume being purged is the source of a SnapMirror relationship, you do not have to break the SnapMirror relationship to perform a secure purge.
 - The re-encryption method is different for volumes using SnapMirror data protection versus volumes not using SnapMirror data protection (DP) or those using SnapMirror extended data protection..
 - By default, volumes using SnapMirror data protection (DP) mode re-encrypt data using the volume move re-encryption method.
 - By default, volumes not using SnapMirror data protection or volumes using SnapMirror extended data protection (XDP) mode use the in-place re-encryption method.
 - These defaults can be changed using the `secure purge re-encryption-method [volume-move|in-place-rekey]` command.
 - By default, all Snapshot copies in FlexVol volumes are automatically deleted during the secure purge operation. By default, Snapshots in FlexGroup volumes and volumes using SnapMirror data protection are not automatically deleted during the secure purge operation. These defaults can be changed using the `secure purge delete-all-snapshots [true|false]` command.
 - In ONTAP 9.8 and earlier:
 - Secure purge does not support the following:
 - FlexClone
 - SnapVault
 - FabricPool
 - If the volume being purged is the source of a SnapMirror relationship, you must break the SnapMirror relationship before you can purge the volume.
- If there are busy Snapshot copies in the volume, you must release the Snapshot copies before you can purge the volume. For example, you may need to split a FlexClone volume from its parent.
- Successfully invoking the secure-purge feature triggers a volume move that re-encrypts the remaining, unpurged data with a new key.

The moved volume remains on the current aggregate. The old key is automatically destroyed, ensuring that purged data cannot be recovered from the storage media.

Securely purge data on an encrypted volume without a SnapMirror relationship

Beginning in ONTAP 9.4, you can use secure-purge to non-disruptively “scrub” data on NVE-enabled volumes.

What you’ll need

- You must be a cluster administrator to perform this task.
- Advanced privileges are required for this task.

About this task

Secure-purge may take from several minutes to many hours to complete, depending on the amount of data in the deleted files. You can use the `volume encryption secure-purge show` command to view the status of the operation. You can use the `volume encryption secure-purge abort` command to terminate the operation.



In order to do a secure purge on a SAN host, you must delete the entire LUN containing the files you want to purge, or you must be able to punch holes in the LUN for the blocks that belong to the files you want to purge. If you cannot delete the LUN or your host operating system does not support punching holes in the LUN, you cannot perform a secure purge.

Steps

1. Delete the files or the LUN you want to securely purge.
 - On a NAS client, delete the files you want to securely purge.
 - On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want to purge.

2. On the storage system, change to advanced privilege level:

```
set -privilege advanced
```

3. If the files you want to securely purge are in snapshots, delete the snapshots:

```
snapshot delete -vserver SVM_name -volume vol_name -snapshot
```

4. Securely purge the deleted files:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
```

The following command securely purges the deleted files on `vol1` on `SVMvs1`:

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume  
vol1
```

5. Verify the status of the secure-purge operation:

```
volume encryption secure-purge show
```

Securely purge data on an encrypted volume with an Asynchronous SnapMirror relationship

Beginning in ONTAP 9.8, you can use `secure-purge` to non-disruptively “scrub” data on NVE-enabled volumes with an Asynchronous SnapMirror relationship.

What you'll need

- You must be a cluster administrator to perform this task.
- Advanced privileges are required for this task.

About this task

Secure-purge may take from several minutes to many hours to complete, depending on the amount of data in the deleted files. You can use the `volume encryption secure-purge show` command to view the status of the operation. You can use the `volume encryption secure-purge abort` command to terminate the operation.



In order to do a secure purge on a SAN host, you must delete the entire LUN containing the files you want to purge, or you must be able to punch holes in the LUN for the blocks that belong to the files you want purge. If you cannot delete the LUN or your host operating system does not support punching holes in the LUN, you cannot perform a secure purge.

Steps

1. On the storage system, change to advanced privilege level:

```
set -privilege advanced
```

2. Delete the files or the LUN you want to securely purge.

- On a NAS client, delete the files you want to securely purge.
- On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want to purge.

3. Prepare `vol_A` in the Asynchronous relationship to be securely purged:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name  
-prepare true
```

Repeat this step on each volume in your Asynchronous SnapMirror relationship.

4. If the files you want to securely purge are in snapshots, delete the snapshots:

```
snapshot delete -vserver SVM_name -volume vol_name -snapshot
```

5. If the files you want to securely purge are in the base snapshots, do the following:

- a. Create a snapshot on `vol_A` in the Asynchronous SnapMirror relationship:

```
volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume  
vol_name
```

- b. Update the SnapMirror to move the base snapshot forward:

```
snapmirror update -source-snapshot snapshot_name -destination-path  
destination_path
```

Repeat this step for each volume in the Asynchronous SnapMirror relationship.

- c. Repeat steps (a) and (b) equal to the number of base snapshots plus one.

For example, if you have two base snapshots, you should repeat steps (a) and (b) three times.

- d. Verify that the base snapshot is present:

```
snapshot show -vserver SVM_name -volume vol_name`
```

- e. Delete the base snapshot:

```
snapshot delete -vserver SVM_name -volume vol_name -snapshot snapshot
```

6. Securely purge the deleted files:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
```

Repeat this step on each volume in the Asynchronous SnapMirror relationship.

The following command securely purges the deleted files on `vol1` on `SVMvs1`:

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume  
vol1
```

7. Verify the status of the secure-purge operation:

```
volume encryption secure-purge show
```

Scrub data on an encrypted volume with a Synchronous SnapMirror relationship

Beginning in ONTAP 9.8, you can use `secure-purge` to non-disruptively “scrub” data on NVE-enabled volumes with a Synchronous SnapMirror relationship.

What you’ll need

- You must be a cluster administrator to perform this task.
- Advanced privileges are required for this task.

About this task

`Secure-purge` may take from several minutes to many hours to complete, depending on the amount of data in the deleted files. You can use the `volume encryption secure-purge show` command to view the status of the operation. You can use the `volume encryption secure-purge abort` command to terminate the operation.



In order to do a secure purge on a SAN host, you must delete the entire LUN containing the files you want to purge, or you must be able to punch holes in the LUN for the blocks that belong to the files you want purge. If you cannot delete the LUN or your host operating system does not support punching holes in the LUN, you cannot perform a secure purge.

Steps

1. On the storage system, change to advanced privilege level:

```
set -privilege advanced
```

2. Delete the files or the LUN you want to securely purge.

- On a NAS client, delete the files you want to securely purge.
- On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want to purge.

3. Prepare `vol_A` in the Asynchronous relationship be securely purged:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name  
-prepare true
```

Repeat this step for the other volume in your Synchronous SnapMirror relationship.

4. If the files you want to securely purge are in snapshots, delete the snapshots:

```
snapshot delete -vserver SVM_name -volume vol_A -snapshot snapshot
```

5. If the secure purge file is in the base or common snapshots, update the SnapMirror to move the common snapshot forward:

```
snapmirror update -source-snapshot snapshot_name -destination-path  
destination_path
```

There are two common snapshots, so this command must be issued twice.

6. If the secure purge file is in the application consistent snapshot, delete the snapshot on both volumes in the Synchronous SnapMirror relationship:

```
snapshot delete -vserver SVM_name -volume vol_name -snapshot snapshot
```

Perform this step on both volumes.

7. Securely purge the deleted files:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
```

Repeat this step on each volume in the synchronous SnapMirror relationship.

The following command securely purges the deleted files on vol1 on SMV vs1.

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume  
vol1
```

8. Verify the status of the secure-purge operation:

```
volume encryption secure-purge show
```

Change the onboard key management passphrase

It is a security best practice to change the onboard key management passphrase periodically. You should copy the new onboard key management passphrase to a secure location outside the storage system for future use.

What you'll need

- You must be a cluster or SVM administrator to perform this task.
- Advanced privileges are required for this task.

Steps

1. Change to advanced privilege level:

```
set -privilege advanced
```

2. Change the onboard key management passphrase:

For this ONTAP version...	Use this command...
ONTAP 9.6 and later	<code>security key-manager onboard update-passphrase</code>
ONTAP 9.5 and earlier	<code>security key-manager update-passphrase</code>

For complete command syntax, see the man pages.

The following ONTAP 9.6 command lets you change the onboard key management passphrase for `cluster1`:

```
cluster1::> security key-manager onboard update-passphrase
Warning: This command will reconfigure the cluster passphrase for
onboard key management for Vserver "cluster1".
Do you want to continue? {y|n}: y
Enter current passphrase:
Enter new passphrase:
```

3. Enter `y` at the prompt to change the onboard key management passphrase.
4. Enter the current passphrase at the current passphrase prompt.
5. At the new passphrase prompt, enter a passphrase between 32 and 256 characters, or for “cc-mode”, a passphrase between 64 and 256 characters.



If the specified “cc-mode” passphrase is less than 64 characters, there is a five-second delay before the key manager setup wizard displays the passphrase prompt again.

6. At the passphrase confirmation prompt, reenter the passphrase.

After you finish

In a MetroCluster environment, you must update the passphrase on the partner cluster:

- In ONTAP 9.5 and earlier, you must run `security key-manager update-passphrase` with the same passphrase on the partner cluster.
- In ONTAP 9.6 and later, you are prompted to run `security key-manager onboard sync` with the same passphrase on the partner cluster.

You should copy the onboard key management passphrase to a secure location outside the storage system for future use.

You should back up key management information manually whenever you change the onboard key management passphrase.

Backing up onboard key management information manually

Back up onboard key management information manually

You should copy onboard key management information to a secure location outside the storage system whenever you configure the Onboard Key Manager passphrase.

What you'll need

- You must be a cluster administrator to perform this task.
- Advanced privileges are required for this task.

About this task

All key management information is automatically backed up to the replicated database (RDB) for the cluster. You should also back up key management information manually for use in case of a disaster.

Steps

1. Change to advanced privilege level:

```
set -privilege advanced
```

2. Display the key management backup information for the cluster:

For this ONTAP version...	Use this command...
ONTAP 9.6 and later	<code>security key-manager onboard show-backup</code>
ONTAP 9.5 and earlier	<code>security key-manager backup show</code>

For complete command syntax, see the man pages.

The following 9.6 command displays the key management backup information for `cluster1`:

[illegible]

- ## Restore onboard key management encryption keys

What you'll need

- ## Transitioning to onboard key management from external key management

- You must be a cluster administrator to perform this task.

About this task

In ONTAP 9.6 and later, you can use the `security key-manager key query -node node` command to verify if your key needs to be restore.

In ONTAP 9.5 and earlier, you can use the `security key-manager key show` command to verify if your key needs to be restored.

Steps

1. If you are running ONTAP 9.8 and later, and your root volume is encrypted, do the following:

If you are running ONTAP 9.7 or earlier, or if you are running ONTAP 9.8 or later and your root volume is not encrypted, skip this step.

- a. Boot the node to the boot menu and select option (10) `Set onboard key management recovery secrets`.
- b. Enter `y` to use this option.
- c. At the prompt, enter the onboard key management passphrase for the cluster.
- d. At the prompt, enter the backup key data.

The node returns to the boot menu..

- e. From the boot menu, select option (1) `Normal Boot`.

2. Restore the key:

For this ONTAP version...	Use this command...
ONTAP 9.6 and later	<code>security key-manager onboard sync</code>
ONTAP 9.5 and earlier	<code>security key-manager setup -node node</code>

For complete command syntax, see the man pages.

The following ONTAP 9.6 command synchronize the keys in the onboard key hierarchy:

```
cluster1::> security key-manager onboard sync
```

```
Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1":: <32..256 ASCII characters long text>
```

3. At the passphrase prompt, enter the onboard key management passphrase for the cluster.

Restore external key management encryption keys

You can manually restore external key management encryption keys and “push” them to a different node. You might want to do this if you are restarting a node that was down

temporarily when you created the keys for the cluster.

What you'll need

You must be a cluster or SVM administrator to perform this task.

About this task

In ONTAP 9.6 and later, you can use the `security key-manager key query -node node_name` command to verify if your key needs to be restored.

In ONTAP 9.5 and earlier, you can use the `security key-manager key show` command to verify if your key needs to be restored.

Steps

- 1. If you are running ONTAP 9.8 or later and your root volume is encrypted, do the following:

If you are running ONTAP 9.7 or earlier, or if you are running ONTAP 9.8 or later and your root volume is not encrypted, skip this step.

- a. Set the bootargs:

```
setenv kmip.init.ipaddr <ip-address>
setenv kmip.init.netmask <netmask>
setenv kmip.init.gateway <gateway>
setenv kmip.init.interface e0M
boot_ontap
```
- b. Boot the node to the boot menu and select option (11) Configure node for external key management.
- c. Follow prompts to enter management certificate.

After all management certificate information is entered, the system returns to the boot menu.

- d. From the boot menu, select option (1) Normal Boot.

- 2. Restore the key:

For this ONTAP version...	Use this command...
ONTAP 9.6 and later	<pre>security key-manager external restore -vserver SVM -node node -key-server host_name IP_address:port -key-id key_id -key-tag key_tag</pre>
ONTAP 9.5 and earlier	<pre>security key-manager restore -node node -address IP_address -key-id key_id -key-tag key_tag</pre>



node defaults to all nodes. For complete command syntax, see the man pages. This command is not supported when onboard key management is enabled.

The following ONTAP 9.6 command restores external key management authentication keys to all nodes in cluster1:

```
clusterl::> security key-manager external restore
```

Replace SSL certificates

All SSL certificates have an expiration date. You must update your certificates before they expire to prevent loss of access to authentication keys.

What you'll need

- You must have obtained the replacement public and private certificates for the cluster.
- You must have obtained the replacement public certificate for the KMIP server.
- You must be a cluster or SVM administrator to perform this task.



You can install the replacement client and server certificates on the KMIP server before or after installing the certificates on the cluster.

Steps

1. Install the new KMIP server-ca certificate:

```
security certificate install -type server-ca -vserver <>`
```

2. Install the new KMIP client certificate:

```
security certificate install -type client -vserver <>
```

3. Update the key manager configuration to use the newly installed certificates:

```
security key-manager external modify -vserver <> -client-cert <> -server-ca  
-certs <>
```



Updating the key manager configuration to use the newly installed certificates will return an error if the public/private keys of the new client certificate are different from the keys previously configured. Contact NetApp support for instructions on how to override this error.

Replace a FIPS drive or SED

You can replace a FIPS drive or SED the same way you replace an ordinary disk. Make sure to assign new data authentication keys to the replacement drive. For a FIPS drive, you may also want to assign a new FIPS 140-2 authentication key.

What you'll need

- You must know the key ID for the authentication key used by the drive.
- You must be a cluster administrator to perform this task.

Steps

1. Ensure that the disk has been marked as failed:

```
storage disk show -broken
```

For complete command syntax, see the man page.

```
cluster1::> storage disk show -broken
Original Owner: cluster1-01
Checksum Compatibility: block
```

											Usable
Physical											
Disk	Outage	Reason	HA	Shelf	Bay	Chan	Pool	Type	RPM		Size
Size											
-----	----	-----	----	-----	----	-----	-----	-----	-----	-----	-----
0.0.0	admin	failed	0b	1	0	A	Pool0	FCAL	10000		132.8GB
133.9GB											
0.0.7	admin	removed	0b	2	6	A	Pool1	FCAL	10000		132.8GB
134.2GB											
[...]											

2. Remove the failed disk and replace it with a new FIPS drive or SED, following the instructions in the hardware guide for your disk shelf model.
3. Assign ownership of the newly replaced disk:

```
storage disk assign -disk disk_name -owner node
```

For complete command syntax, see the man page.

```
cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
```

4. Confirm that the new disk has been assigned:

```
storage encryption disk show
```

For complete command syntax, see the man page.

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
-----
0.0.0     data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.0    data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1    data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
2.1.1     open 0x0
[...]
```

5. Assign the data authentication keys to the FIPS drive or SED.

[Assigning a data authentication key to a FIPS drive or SED \(external key management\)](#)

6. If necessary, assign a FIPS 140-2 authentication key to the FIPS drive.

[Assigning a FIPS 140-2 authentication key to a FIPS drive](#)

Make data on a FIPS drive or SED inaccessible

Make data on a FIPS drive or SED inaccessible overview

If you want to make data on a FIPS drive or SED permanently inaccessible, but keep the drive's unused space available for new data, you can sanitize the disk. If you want to make data permanently inaccessible and you do not need to reuse the drive, you can destroy it.

- Disk sanitization

When you sanitize a self-encrypting drive, the system changes the disk encryption key to a new random value, resets the power-on lock state to false, and sets the key ID to a default value, either the manufacturer secure ID 0x0 (SAS drives) or a null key (NVMe drives). Doing so renders the data on the disk inaccessible and impossible to retrieve. You can reuse sanitized disks as non-zeroed spare disks.

- Disk destroy

When you destroy a FIPS drive or SED, the system sets the disk encryption key to an unknown random value and locks the disk irreversibly. Doing so renders the disk permanently unusable and the data on it permanently inaccessible.

You can sanitize or destroy individual self-encrypting drives, or all the self-encrypting drives for a node.

Sanitize a FIPS drive or SED

If you want to make data on a FIPS drive or SED permanently inaccessible, and use the drive for new data, you can use the `storage encryption disk sanitize` command to sanitize the drive.

What you'll need

You must be a cluster administrator to perform this task.

About this task

When you sanitize a self-encrypting drive, the system changes the disk encryption key to a new random value, resets the power-on lock state to false, and sets the key ID to a default value, either the manufacturer secure ID 0x0 (SAS drives) or a null key (NVMe drives). Doing so renders the data on the disk inaccessible and impossible to retrieve. You can reuse sanitized disks as non-zeroed spare disks.

Steps

1. Migrate any data that needs to be preserved to an aggregate on another disk.
2. Delete the aggregate on the FIPS drive or SED to be sanitized:

```
storage aggregate delete -aggregate aggregate_name
```

For complete command syntax, see the man page.

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

3. Identify the disk ID for the FIPS drive or SED to be sanitized:

```
storage encryption disk show
```

For complete command syntax, see the man page.

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
-----
0.0.0     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.2    data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. Sanitize the drive:

```
storage encryption disk sanitize -disk disk_id
```

You can use this command to sanitize hot spare or broken disks only. To sanitize all disks regardless of type, use the `-force-all-state` option. For complete command syntax, see the man page.



You are prompted to enter a confirmation phrase before continuing. Enter the phrase exactly as shown on the screen.

```
cluster1::> storage encryption disk sanitize -disk 1.10.2
```

```
Warning: This operation will cryptographically sanitize 1 spare or  
broken self-encrypting disk on 1 node.
```

```
To continue, enter sanitize disk: sanitize disk
```

```
Info: Starting sanitize on 1 disk.
```

```
View the status of the operation using the  
storage encryption disk show-status command.
```

Destroy a FIPS drive or SED

If you want to make data on a FIPS drive or SED permanently inaccessible and you do not need to reuse the drive, you can use the `storage encryption disk destroy` command to destroy the disk.

What you'll need

You must be a cluster administrator to perform this task.

About this task

When you destroy a FIPS drive or SED, the system sets the disk encryption key to an unknown random value and locks the drive irreversibly. Doing so renders the disk virtually unusable and the data on it permanently inaccessible. However, you can reset the disk to its factory-configured settings using the PSID printed on the disk's label. For more information, see [Returning a FIPS drive or SED to service when authentication keys are lost](#).



You should not destroy a FIPS drive or SED unless you have the Non-Returnable Disk Plus service (NRD Plus). Destroying a disk voids its warranty.

Steps

1. Migrate any data that needs to be preserved to an aggregate for a different disk.
2. Delete the aggregate on the FIPS drive or SED to be destroyed:

```
storage aggregate delete -aggregate aggregate_name
```

For complete command syntax, see the man page.

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

3. Identify the disk ID for the FIPS drive or SED to be destroyed:

```
storage encryption disk show
```

For complete command syntax, see the man page.

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
-----
0.0.0     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.2    data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. Destroy the disk:

```
storage encryption disk destroy -disk disk_id
```

For complete command syntax, see the man page.



You are prompted to enter a confirmation phrase before continuing. Enter the phrase exactly as shown on the screen.

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
self-encrypting disks on 1 node.
You cannot reuse destroyed disks unless you revert
them to their original state using the PSID value.
To continue, enter
    destroy disk
:destroy disk

Info: Starting destroy on 1 disk.
View the status of the operation by using the
"storage encryption disk show-status" command.
```

Emergency shredding of data on an FIPS drive or SED


In case of a security emergency, you can instantly prevent access to a FIPS drive or SED, even if power is not available to the storage system or the KMIP server.

What you'll need

- You must be using a KMIP server, and the KMIP server must be configured with an easily destroyed authentication item (for example, a smart card or USB drive).
- You must be a cluster administrator to perform this task.

Step

1. Perform emergency shredding of data on a FIPS drive or SED:

If...	Then...
Power is available to the storage system and you have time to take the storage system offline gracefully	<ol style="list-style-type: none"> a. If the storage system is configured as an HA pair, disable takeover. b. Take all aggregates offline and delete them. c. Set the privilege level to advanced: <code>set -privilege advanced</code> d. If the drive is in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID: <code>storage encryption disk modify -disk * -fips-key-id 0x0</code> e. Halt the storage system. f. Boot into maintenance mode. g. Sanitize or destroy the disks: <ul style="list-style-type: none"> ◦ If you want to make the data on the disks inaccessible and still be able to reuse the disks, sanitize the disks: <code>disk encrypt sanitize -all</code> ◦ If you want to make the data on the disks inaccessible and you do not need to save the disks, destroy the disks: <code>disk encrypt destroy disk_id1 disk_id2 ...</code> <div>  <p>The <code>disk encrypt sanitize</code> and <code>disk encrypt destroy</code> commands are reserved for maintenance mode only. These commands must be run on each HA node, and are not available for broken disks.</p> </div> <ol style="list-style-type: none"> h. Repeat these steps for the partner node. This leaves the storage system in a permanently disabled state with all data erased. To use the system again, you must reconfigure it.

If...	Then...
Power is available to the storage system and you must shred the data immediately	<ol style="list-style-type: none"> If the storage system is configured as an HA pair, disable takeover. Set the privilege level to advanced: <pre>set -privilege advanced</pre> Sanitize or destroy the disks: <ul style="list-style-type: none"> If you want to make the data on the disks inaccessible and still be able to reuse the disks, sanitize the disks: <pre>storage encryption disk sanitize -disk * -force-all-states true</pre> If you want to make the data on the disks inaccessible and you do not need to save the disks, destroy the disks: <pre>storage encryption disk destroy -disk * -force-all-states true</pre> The storage system panics, leaving the system in a permanently disabled state with all data erased. To use the system again, you must reconfigure it.
Power is available to the KMIP server but not to the storage system	<ol style="list-style-type: none"> Log in to the KMIP server. Destroy all keys associated with the FIPS drives or SEDs that contain the data you want to prevent access to. This prevents access to disk encryption keys by the storage system.
Power is not available to the KMIP server or the storage system	Destroy the authentication item for the KMIP server (for example, the smart card). This prevents access to disk encryption keys by the storage system.

For complete command syntax, see the man pages.

Return a FIPS drive or SED to service when authentication keys are lost

The system treats a FIPS drive or SED as broken if you lose the authentication keys for it permanently and cannot retrieve them from the KMIP server. Although you cannot access or recover the data on the disk, you can take steps to make the SED's unused space available again for data.

What you'll need

You must be a cluster administrator to perform this task.

About this task

You should use this process only if you are certain that the authentication keys for the FIPS drive or SED are

permanently lost and that you cannot recover them.

Steps

1. Return a FIPS drive or SED to service:

If the SEDS are...	Use these steps...
Not in FIPS-compliance mode, or in FIPS-compliance mode and the FIPS key is available	<ol style="list-style-type: none">a. Sanitize the broken disk: <code>storage encryption disk sanitize -disk disk_id</code>b. Set the privilege level to advanced: <code>set -privilege advanced</code>c. Unfail the sanitized disk: <code>storage disk unfail -spare true -disk disk_id</code>d. Check whether the disk has an owner: <code>storage disk show -disk disk_id</code>e. If the disk does not have an owner, assign one, then unfail the disk again: <code>storage disk assign -owner node -disk disk_id</code> <code>storage disk unfail -spare true -disk disk_id</code>f. Verify that the disk is now a spare and ready to be reused in an aggregate: <code>storage disk show -disk disk_id</code>

If the SEDS are...	Use these steps...
In FIPS-compliance mode, the FIPS key is not available, and the SEDs have a PSID printed on the label	<ol style="list-style-type: none"> Obtain the PSID of the disk from the disk label. Set the privilege level to advanced: <code>set -privilege advanced</code> Reset the disk to its factory-configured settings: <code>storage encryption disk revert-to-original-state -disk disk_id -psid disk_physical_secure_id</code> Unfail the sanitized disk: <code>storage disk unfail -spare true -disk disk_id</code> Check whether the disk has an owner: <code>storage disk show -disk disk_id</code> If the disk does not have an owner, assign one, then unfail the disk again: <code>storage disk assign -owner node -disk disk_id</code> <code>storage disk unfail -spare true -disk disk_id</code> Verify that the disk is now a spare and ready to be reused in an aggregate: <code>storage disk show -disk disk_id</code>

For complete command syntax, see the man pages.

Return a FIPS drive or SED to unprotected mode

A FIPS drive or SED is protected from unauthorized access only if the authentication key ID for the node is set to a value other than the default. You can return a FIPS drive or SED to unprotected mode by using the `storage encryption disk modify` command to set the key ID to the default.

What you'll need

You must be a cluster administrator to perform this task.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. If a FIPS drive is running in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID 0x0:

```
storage encryption disk modify -disk disk_id -fips-key-id 0x0
```

You can use the `security key-manager query` command to view key IDs.

```
cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id 0x0
```

```
Info: Starting modify on 14 disks.  
      View the status of the operation by using the  
      storage encryption disk show-status command.
```

3. Set the data authentication key ID for the node back to the default MSID 0x0:

```
storage encryption disk modify -disk disk_id -data-key-id 0x0
```

The value of `-data-key-id` should be set to 0x0 whether you are returning a SAS or NVMe drive to unprotected mode.

You can use the `security key-manager query` command to view key IDs.

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id 0x0
```

```
Info: Starting modify on 14 disks.  
      View the status of the operation by using the  
      storage encryption disk show-status command.
```

Delete an external key manager connection

You can disconnect a KMIP server from a node when you no longer need the server. You might disconnect a KMIP server when you are transitioning to volume encryption, for example.

What you'll need

You must be a cluster or SVM administrator to perform this task.

About this task

When you disconnect a KMIP server from one node in an HA pair, the system automatically disconnects the server from all cluster nodes.



If you plan to continue using external key management after disconnecting a KMIP server, make sure another KMIP server is available to serve authentication keys.

Step

1. Disconnect a KMIP server from the current node:

For this ONTAP version...	Use this command...
ONTAP 9.6 and later	<code>security key-manager external remove-servers -vserver SVM -key-servers host_name IP_address:port,...</code>
ONTAP 9.5 and earlier	<code>security key-manager delete -address key_management_server_ipaddress</code>

For complete command syntax, see the man pages.

The following ONTAP 9.6 command disables the connections to two external key management servers for `cluster1`, the first named `ks1`, listening on the default port 5696, the second with the IP address 10.0.0.20, listening on port 24482:

```
cluster1::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

Modify external key management server properties

Starting with ONTAP 9.6, you can use the `security key-manager external modify-server` command to change the I/O timeout and username of an external key management server.

What you'll need

- You must be a cluster or SVM administrator to perform this task.
- Advanced privileges are required for this task.

Steps

1. On the storage system, change to advanced privilege level:

```
set -privilege advanced
```

2. Modify external key manager server properties for the cluster:

```
security key-manager external modify-server -vserver admin_SVM -key-server
host_name|IP_address:port,... -timeout 1...60 -username user_name
```



The timeout value is expressed in seconds. If you modify the user name, you are prompted to enter a new password. If you run the command at the cluster login prompt, `admin_SVM` defaults to the admin SVM of the current cluster. You must be the cluster administrator to modify external key manager server properties.

The following command changes the timeout value to 45 seconds for the `cluster1` external key management server listening on the default port 5696:

```
cluster1::> security key-manager external modify-server -vserver  
cluster1 -key-server ks1.local -timeout 45
```

3. Modify external key manager server properties for an SVM (NVE only):

```
security key-manager external modify-server -vserver SVM -key-server  
host_name|IP_address:port,... -timeout 1...60 -username user_name
```



The timeout value is expressed in seconds. If you modify the user name, you are prompted to enter a new password. If you run the command at the SVM login prompt, *SVM* defaults to the current SVM. You must be the cluster or SVM administrator to modify external key manager server properties.

The following command changes the username and password of the *svm1* external key management server listening on the default port 5696:

```
svm1::> security key-manager external modify-server -vserver svm11 -key  
-server ks1.local -username svm1user  
Enter the password:  
Reenter the password:
```

4. Repeat the last step for any additional SVMs.

Transition to external key management from onboard key management

If you want to switch to external key management from onboard key management, you must delete the onboard key management configuration before you can enable external key management.

What you'll need

- For hardware-based encryption, you must reset the data keys of all FIPS drives or SEDs to the default value.

[Returning a FIPS drive or SED to unprotected mode](#)

- For software-based encryption, you must unencrypt all volumes.

[Unencrypting volume data](#)

- You must be a cluster administrator to perform this task.

Step

1. Delete the onboard key management configuration for a cluster:

For this ONTAP version...	Use this command...
ONTAP 9.6 and later	<code>security key-manager onboard disable -vserver SVM</code>
ONTAP 9.5 and earlier	<code>security key-manager delete-key-database</code>

For complete command syntax, see the man pages.

The following ONTAP 9.6 command deletes the onboard key management configuration for `cluster1`:

```
cluster1::> security key-manager onboard disable
```

Transition to onboard key management from external key management

If you want to switch to onboard key management from external key management, you must delete the external key management configuration before you can enable onboard key management.

What you'll need

- For hardware-based encryption, you must reset the data keys of all FIPS drives or SEDs to the default value.

[Returning a FIPS drive or SED to unprotected mode](#)

- You must have deleted all external key manager connections.

[Deleting an external key manager connection](#)

- You must be a cluster administrator to perform this task.

Steps

1. Delete the external key management configuration for a cluster:

```
security key-manager delete-kmip-config
```

For this ONTAP version...	Use this command...
ONTAP 9.6 and later	<code>security key-manager external disable -vserver admin_SVM</code>
ONTAP 9.5 and earlier	<code>security key-manager delete-kmip-config</code>



For complete command syntax, see the man pages. The ONTAP 9.6 version of the command requires advanced privilege level.

The following ONTAP 9.6 commands delete the external key management configurations for `cluster1`:

```
cluster1::> set -privilege advanced
cluster1::> security key-manager external disable
```

What happens when key management servers are not reachable during the boot process

ONTAP takes certain precautions to avoid undesired behavior in the event that a storage system configured for NSE cannot reach any of the specified key management servers during the boot process.

If the storage system is configured for NSE, the SEDs are rekeyed and locked, and the SEDs are powered on, the storage system must retrieve the required authentication keys from the key management servers to authenticate itself to the SEDs before it can access the data.

The storage system attempts to contact the specified key management servers for up to three hours. If the storage system cannot reach any of them after that time, the boot process stops and the storage system halts.

If the storage system successfully contacts any specified key management server, it then attempts to establish an SSL connection for up to 15 minutes. If the storage system cannot establish an SSL connection with any specified key management server, the boot process stops and the storage system halts.

While the storage system attempts to contact and connect to key management servers, it displays detailed information about the failed contact attempts at the CLI. You can interrupt the contact attempts at any time by pressing Ctrl-C.

As a security measure, SEDs allow only a limited number of unauthorized access attempts, after which they disable access to the existing data. If the storage system cannot contact any specified key management servers to obtain the proper authentication keys, it can only attempt to authenticate with the default key which leads to a failed attempt and a panic. If the storage system is configured to automatically reboot in case of a panic, it enters a boot loop which results in continuous failed authentication attempts on the SEDs.

Halting the storage system in these scenarios is by design to prevent the storage system from entering a boot loop and possible unintended data loss as a result of the SEDs locked permanently due to exceeding the safety limit of a certain number of consecutive failed authentication attempts. The limit and the type of lockout protection depends on the manufacturing specifications and type of SED:

SED type	Number of consecutive failed authentication attempts resulting in lockout	Lockout protection type when safety limit is reached
HDD	1024	Permanent. Data cannot be recovered, even when the proper authentication key becomes available again.

SED type	Number of consecutive failed authentication attempts resulting in lockout	Lockout protection type when safety limit is reached
X440_PHM2800MCTO 800GB NSE SSDs with firmware revisions NA00 or NA01	5	Temporary. Lockout is only in effect until disk is power-cycled.
X577_PHM2800MCTO 800GB NSE SSDs with firmware revisions NA00 or NA01	5	Temporary. Lockout is only in effect until disk is power-cycled.
X440_PHM2800MCTO 800GB NSE SSDs with higher firmware revisions	1024	Permanent. Data cannot be recovered, even when the proper authentication key becomes available again.
X577_PHM2800MCTO 800GB NSE SSDs with higher firmware revisions	1024	Permanent. Data cannot be recovered, even when the proper authentication key becomes available again.
All other SSD models	1024	Permanent. Data cannot be recovered, even when the proper authentication key becomes available again.

For all SED types, a successful authentication resets the try count to zero.

If you encounter this scenario where the storage system is halted due to failure to reach any specified key management servers, you must first identify and correct the cause for the communication failure before you attempt to continue booting the storage system.

Disable encryption by default with ONTAP 9.7 and later

Starting with ONTAP 9.7, aggregate and volume encryption is enabled by default if you have a volume encryption (VE) licence and use an onboard or external key manager. You can disable encryption by default if required.

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.

Step

1. To disable encryption by default in ONTAP 9.7 or later, run the following command:

```
options -option-name encryption.data_at_rest_encryption.disable_by_default
-vserver (vservename or * for all) -option-value on
```

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

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.