Manage NetApp encryption

ONTAP 9

NetApp
February 12, 2026

Table of Contents

Manage NetApp encryption

Unencrypt volume data in ONTAP

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

Before you begin

You must be a cluster administrator to perform this task.

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`

   Learn more about `volume move start` in the ONTAP command reference.

   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`

   Learn more about `volume show` in the ONTAP command reference.

   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 in ONTAP

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.

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. The requirement to specify you do not want the destination volume encrypted ensures that you do not inadvertently unencrypt the data on the volume.

Before you begin

You must be a cluster administrator to perform this task.

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`*

   Learn more about `volume move start` in the ONTAP command reference.

   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`

   Learn more about `volume show` in the ONTAP command reference.

   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%
   ```

Change the encryption key for a volume with the volume encryption rekey start command in ONTAP

It is a security best practice to change the encryption key for a volume periodically. Beginning 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 SVM`vs1`:

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

2. Verify the status of the rekey operation:

   `volume encryption rekey show`

   Learn more about `volume encryption rekey show` in the ONTAP command reference.

   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`

   Learn more about `volume show` in the ONTAP command reference.

   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 ONTAP 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. The moved volume can reside on the same aggregate or a different aggregate.

About this task

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

Before you begin

You must be a cluster administrator to perform this task.

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`

   Learn more about `volume move start` in the ONTAP command reference.

   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`

   Learn more about `volume show` in the ONTAP command reference.

   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 ONTAP 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.

Related information

- storage encryption disk modify

Delete an encrypted volume in ONTAP

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

Before you begin

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

Step

1. Delete an encrypted volume:

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

   Learn more about `volume delete` in the ONTAP command reference.

   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. This command requires advanced privileges. Learn more about `volume`

`delete` in the ONTAP command reference.

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

Learn about securely purging data from an encrypted ONTAP volume

Beginning with 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.

Considerations for using secure purge

- Volumes created in an aggregate enabled for NetApp Aggregate Encryption (NAE) do not support secure purge.
- 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.

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 snapshots 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.

ONTAP 9.7 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 snapshots in the volume, you must release the snapshots 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.

Scrub data from an encrypted ONTAP volume without a SnapMirror relationship

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

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.

Before you begin

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

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` *`volume_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 SVM`vs1`:

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

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

   `volume encryption secure-purge show`

Scrub data from an encrypted ONTAP volume with an SnapMirror asynchronous relationship

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

Before you begin

- 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, switch to the 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 the destination volume 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 SnapMirror asynchronous relationship.

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

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

5. If the files you want to securely purge are in the base snapshots, do the following:
   a. Create a snapshot on the destination volume in the SnapMirror asynchronous relationship:

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

   b. Update 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 SnapMirror asynchronous 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 volume_name`
   e. Delete the base snapshot:
      `snapshot delete -vserver svm_name -volume volume_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 SnapMirror asynchronous relationship.

   The following command securely purges the deleted files on “vol1” on SVM “vs1”:

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

7. Verify the status of the secure purge operation:

   `volume encryption secure-purge show`

Related information

- snapmirror update

Scrub data from an encrypted ONTAP volume with a SnapMirror synchronous relationship

Beginning with ONTAP 9.8, you can use a secure purge to non-disruptively "scrub" data on NVE-enabled volumes with a SnapMirror synchronous relationship.

About this task

A secure purge might 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.

Before you begin

- You must be a cluster 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. 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 the destination volume in the Asynchronous relationship to 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 SnapMirror synchronous relationship.

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

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -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 SnapMirror synchronous relationship:

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_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 SnapMirror synchronous relationship.

   The following command securely purges the deleted files on “vol1” on SVM “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
   ```

Related information

- snapmirror update

Change the ONTAP onboard key management passphrase

NetApp recommends that you change the onboard key management passphrase regularly. You must store the new passphrase in a secure location outside the storage system.

Before you begin

- You must be a cluster or SVM administrator to perform this task.
- Advanced privileges are required for this task.
- In a MetroCluster environment, after you update the passphrase on the local cluster, synchronize the passphrase update on the partner cluster.

Steps

1. Change to advanced privilege level:

   ```
   set -privilege advanced
   ```

2. Change the onboard key management passphrase. The command you use depends on the ONTAP version you are running.

   ONTAP 9.6 and later

   ```
   security key-manager onboard update-passphrase
   ```

   ONTAP 9.5 and earlier

   ```
   security key-manager update-passphrase
   ```

3. 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 operation displays the passphrase prompt again.

4. At the passphrase confirmation prompt, reenter the passphrase.
5. If you are in a MetroCluster configuration, synchronize the updated passphrase on the partner cluster.
   a. Synchronize the passphrase on the partner cluster by choosing the correct command for your ONTAP version:

      ONTAP 9.6 and later

      ```
      security key-manager onboard sync
      ```

      ONTAP 9.5 and earlier

      - In ONTAP 9.5, run:

        ```
        security key-manager setup -sync-metrocluster-config
        ```

      - In ONTAP 9.4 and earlier, after you’ve updated the passphrase on the local cluster, wait 20 seconds, and then run the following command on the partner cluster:

        ```
        security key-manager setup
        ```

   b. Enter the new passphrase when prompted.

      The same passphrase must be used on both clusters.

After you finish

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

Back up key management information manually whenever you change the onboard key management passphrase.

Related information

- Back up onboard key management information manually
- security key-manager onboard update-passphrase

Back up ONTAP 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.

Before you begin

- 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	`security key-manager onboard show-backup`
ONTAP 9.5 and earlier	`security key-manager backup show`

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

```
cluster1::> security key-manager onboard show-backup

     --------------------------BEGIN BACKUP--------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAACEAAAAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAAAA
     IgAAAAAAAAAAoAAAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAAACQAAAAAAAAAAgAAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAYAQAAAAAAAADA5/ccAAAAAIgAAAAAAAAAAoAAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAAACAAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAAACIAAAAAAAAAAA
     KAAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAAkAAAAAAAAAAAIAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAwAAABgBAAAAAAAAAAA
     1cNLLwAAAAiAAAAAAAAAACgAAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAAIAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAIgAAAAAAAAAAoAAAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAAACAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAAACQAAAAAAAAAAA
     gAAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------END BACKUP---------------------------
```


3. Copy the backup information to a secure location outside the storage system for use in case of a disaster.

Related information

- security key-manager onboard show-backup
- security key-manager backup show

Restore onboard key management encryption keys in ONTAP

Occasionally, you may need to restore an onboard key management encryption key. Once you have verified that a key needs to be restored, you can set up the Onboard Key Manager to restore the key.The procedure you follow to restore your onboard key

management encryption keys varies based on your version of ONTAP.

Before you begin

- Delete the external key manager database if you use NSE with an external KMIP server. For details, see Transition from external key management to ONTAP onboard key management.
- You must be a cluster administrator to perform this task.

If you are using NSE on a system with a Flash Cache module, you should also enable NVE or NAE. NSE does not encrypt data that resides on the Flash Cache module.

ONTAP 9.6 and later

If you are running ONTAP 9.8 or later and your root volume is encrypted, follow the procedure for ONTAP 9.8 or later with encrypted root volume.

1. Verify that the key needs to be restored:
   `security key-manager key query -node` *node*

   Learn more about `security key-manager key query` in the ONTAP command reference.

2. Restore the key:
   `security key-manager onboard sync`

   Learn more about `security key-manager onboard sync` in the ONTAP command reference.

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

ONTAP 9.8 or later with encrypted root volume

If you are running ONTAP 9.8 and later, and your root volume is encrypted, you must set an onboard key management recovery passphrase with the boot menu. This process is also necessary if you do a boot media replacement.

1. Boot the node to the boot menu and select option `(10) Set onboard key management recovery secrets`.
2. Enter `y` to use this option.
3. At the prompt, enter the onboard key management passphrase for the cluster.
4. At the prompt, enter the backup key data.

   After you enter the backup key data, the node returns to the boot menu.

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

ONTAP 9.5 and earlier

1. Verify that the key needs to be restored:
   `security key-manager key show`
2. Restore the key:
   `security key-manager setup -node` *node*

Learn more about `security key-manager setup` in the ONTAP command reference.

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

Restore ONTAP 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.

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.

If you are using NSE on a system with a Flash Cache module, you should also enable NVE or NAE. NSE does not encrypt data that resides on the Flash Cache module.

Learn more about `security key-manager key query` in the ONTAP command reference.

Before you begin

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

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	`security key-manager external restore -vserver SVM -node node -key-server host_name|IP_address:port -key-id key_id -key-tag key_tag`
ONTAP 9.5 and earlier	`security key-manager restore -node node -address IP_address -key-id key_id -key-tag key_tag`

`node` defaults to all nodes.

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`:

```
cluster1::> security key-manager external restore
```

Related information

- security key-manager external restore

Replace KMIP SSL certificates on the ONTAP cluster

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

Before you begin

- You must have obtained the replacement public certificate and private key for the cluster (KMIP client certificate).
- You must have obtained the replacement public certificate for the KMIP server (KMIP server-ca certificate).
- You must be a cluster or SVM administrator to perform this task.
- If you are replacing the KMIP SSL certificates in a MetroCluster environment, you must install the same replacement KMIP SSL certificate on both clusters.

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 <>
```

If you are running ONTAP 9.6 or later in a MetroCluster environment, and you want to modify the key manager configuration on the admin SVM, you must run the command on both clusters in the configuration.

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 installed. See the NetApp Knowledge Base: The new client certificate public or private keys are different from the existing client certificate for instructions on how to override this error.

Related information

- security certificate install
- security key-manager external modify

Replace a FIPS drive or SED in ONTAP

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.

If an HA pair is using encrypting SAS or NVMe drives (SED, NSE, FIPS), you must follow the instructions in the topic Returning a FIPS drive or SED to unprotected mode for all drives within the HA pair prior to initializing the system (boot options 4 or 9). Failure to do this may result in future data loss if the drives are repurposed.

Before you begin

- 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
   ```

   Learn more about `storage disk show` in the ONTAP command reference.

```
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`

   Learn more about `storage disk assign` in the ONTAP command reference.

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

4. Confirm that the new disk has been assigned:

   `storage encryption disk show`

   Learn more about `storage encryption disk show` in the ONTAP command reference.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data <id_value>
   0.0.1   data <id_value>
   1.10.0  data <id_value>
   1.10.1  data <id_value>
   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

Related information

- storage disk assign
- storage disk show
- storage encryption disk show

Make data on a FIPS drive or SED inaccessible

Learn about making ONTAP data on a FIPS drive or SED inaccessible

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 in ONTAP

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.

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.

Before you begin

You must be a cluster administrator to perform this task.

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`

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

   Learn more about `storage aggregate delete` in the ONTAP command reference.

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

   `storage encryption disk show -fields data-key-id,fips-key-id,owner`

   Learn more about `storage encryption disk show` in the ONTAP command reference.

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

4. 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 1.10.2 -fips-key-id 0x0

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

5. 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. Learn more about `storage encryption disk sanitize` in the ONTAP command reference.

ONTAP will prompt you 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.
```

6. Unfail the sanitized disk: `storage disk unfail -spare true -disk disk_id`
7. Check whether the disk has an owner: `storage disk show -disk disk_id`
   If the disk does not have an owner, assign one. `storage disk assign -owner node -disk disk_id`
8. Enter the nodeshell for the node that owns the disks you want to sanitize:

   `system node run -node node_name`

   Run the `disk sanitize release` command.

9. Exit the nodeshell. Unfail the disk again: `storage disk unfail -spare true -disk disk_id`
10. Verify that the disk is now a spare and ready to be reused in an aggregate: `storage disk show -disk disk_id`

Related information

- storage disk assign
- storage disk show
- storage disk unfail
- storage encryption disk modify
- storage encryption disk sanitize
- storage encryption disk show-status

Destroy a FIPS drive or SED in ONTAP

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.

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 physical secure ID

(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.

Before you begin

You must be a cluster administrator to perform this task.

Steps

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

   `storage aggregate delete -aggregate aggregate_name`

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

   Learn more about `storage aggregate delete` in the ONTAP command reference.

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

   `storage encryption disk show`

   Learn more about `storage encryption disk show` in the ONTAP command reference.

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

4. Destroy the disk:

   `storage encryption disk destroy -disk disk_id`

   Learn more about `storage encryption disk destroy` in the ONTAP command reference.

   > 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.
```

Related information

- storage encryption disk destroy
- storage encryption disk show
- storage encryption disk show-status

Emergency shred data on a FIPS drive or SED in ONTAP

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.

Before you begin

- If you are using a KMIP server that has no available power, 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	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:
	`set -privilege advanced`
	d. If the drive is in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID:
	`storage encryption disk modify -disk * -fips-key -id 0x0`
	e. Halt the storage system.
	f. Boot into maintenance mode.
	g. Sanitize or destroy the disks:
	◦ If you want to make the data on the disks inaccessible and still be able to reuse the disks, sanitize the disks:
	`disk encrypt sanitize -all`
	◦ If you want to make the data on the disks inaccessible and you do not need to save the disks, destroy the disks:
	`disk encrypt destroy disk_id1 disk_id2 …`
	ⓘ The `disk encrypt sanitize` and `disk encrypt destroy` commands are reserved for maintenance mode only. These commands must be run on each HA node, and are not available for broken disks.
	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.

<table>
<tr><td rowspan="2">Power is available to the storage system and you must shred the data immediately</td><td><ol type="a">
If you want to make the data on the disks inaccessible and still be able to reuse the disks, sanitize the disks:
If the storage system is configured as an HA pair, disable takeover.
Set the privilege level to advanced:

<code>set -privilege advanced</code>
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>
Sanitize the disk:

<code>storage encryption disk sanitize -disk * -force-all-states true</code></td><td><ol type="a">
If you want to make the data on the disks inaccessible and you do not need to save the disks, destroy the disks:
If the storage system is configured as an HA pair, disable takeover.
Set the privilege level to advanced:

<code>set -privilege advanced</code>
Destroy the disks: <code>storage encryption disk destroy -disk * -force -all-states true</code></td></tr>
<tr><td colspan="2">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.</td></tr>
<tr><td>Power is available to the KMIP server but not to the storage system</td><td colspan="2"><ol type="a">
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.</td></tr>
<tr><td>Power is not available to the KMIP server or the storage system</td><td colspan="2">Destroy the authentication item for the KMIP server (for example, the smart card). This prevents access to disk encryption keys by the storage system.</td></tr>
</table>

Related information

- storage encryption disk destroy
- storage encryption disk modify
- storage encryption disk sanitize

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

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.

Before you begin

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.

If the disks are partitioned, they must first be unpartitioned before you can start this process.

> The command to unpartition a disk is only available at the diag level and should be performed only under NetApp Support supervision. **It is highly recommended that you contact NetApp Support before you proceed.** You can also refer to the NetApp Knowledge Base: How to unpartition a spare drive in ONTAP.

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	a. Set the privilege level to advanced:
	`set -privilege advanced`
	b. Reset the FIPS key to the default manufacture secure ID 0x0:
	`storage encryption disk modify -fips-key-id 0x0 -disk` *`disk_id`*
	c. Verify the operation succeeded:
	`storage encryption disk show-status`
	If the operation failed, use the PSID process in this topic.
	d. Sanitize the broken disk:
	`storage encryption disk sanitize -disk` *`disk_id`*
	Verify the operation succeeded with the command `storage encryption disk show-status` before proceeding to the next step.
	e. Unfail the sanitized disk:
	`storage disk unfail -spare true -disk` *`disk_id`*
	f. Check whether the disk has an owner:
	`storage disk show -disk` *`disk_id`*
	If the disk does not have an owner, assign one.
	`storage disk assign -owner node -disk` *`disk_id`*
	1. Enter the nodeshell for the node that owns the disks you want to sanitize:
	`system node run -node` *`node_name`*
	Run the `disk sanitize release` command.
	g. Exit the nodeshell. Unfail the disk again:
	`storage disk unfail -spare true -disk` *`disk_id`*
	h. Verify that the disk is now a spare and ready to be reused in an aggregate:
	`storage disk show -disk` *`disk_id`*

In FIPS-compliance mode, the FIPS key is not available, and the SEDs have a PSID printed on the label	a. Obtain the PSID of the disk from the disk label. b. Set the privilege level to advanced: `set -privilege advanced` c. Reset the disk to its factory-configured settings: `storage encryption disk revert-to-original-state -disk` *`disk_id`* `-psid` *`disk_physical_secure_id`* Verify the operation succeeded with the command `storage encryption disk show-status` before proceeding to the next step. d. If you are running ONTAP 9.8P5 or earlier, skip to the next step. If you are running ONTAP 9.8P6 or later, unfail the sanitized disk. `storage disk unfail -disk` *`disk_id`* e. Check whether the disk has an owner: `storage disk show -disk` *`disk_id`* If the disk does not have an owner, assign one. `storage disk assign -owner node -disk` *`disk_id`* 1. Enter the nodeshell for the node that owns the disks you want to sanitize: `system node run -node` *`node_name`* Run the `disk sanitize release` command. f. Exit the nodeshell.. Unfail the disk again: `storage disk unfail -spare true -disk` *`disk_id`* g. Verify that the disk is now a spare and ready to be reused in an aggregate: `storage disk show -disk` *`disk_id`*

Related information

- storage encryption disk modify
- storage encryption disk revert-to-original-state
- storage encryption disk sanitize
- storage encryption disk show-status

Return a FIPS drive or SED to unprotected mode in ONTAP

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. A FIPS drive or SED in unprotected mode uses the default encryption keys, while a FIPS drive or SED in protected mode uses supplied, secret encryption keys. If there is encrypted data on the drive and the drive is reset to unprotected mode, the data is still encrypted and is not exposed.

Follow this procedure to ensure that any encrypted data becomes inaccessible after the FIPS drive or SED is returned to unprotected mode. Once the FIPS and data key IDs are reset, any existing data can not be decrypted and becomes inaccessible unless the original keys are restored.

If an HA pair is using encrypting SAS or NVMe drives (SED, NSE, FIPS), you must follow this process for all drives within the HA pair prior to initializing the system (boot options 4 or 9). Failure to do this may result in future data loss if the drives are repurposed.

Before you begin

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.
   ```

   Confirm the operation succeeded with the command:

   ```
   storage encryption disk show-status
   ```

   Repeat the show-status command until the numbers in "Disks Begun" and "Disks Done" are the same.

```
cluster1:: storage encryption disk show-status

            FIPS    Latest   Start               Execution   Disks
Disks Disks
Node        Support Request  Timestamp           Time (sec)  Begun
Done  Successful
-------     ------- -------- ------------------  ---------- ------
------  ----------
cluster1    true    modify   1/18/2022 15:29:38    3           14     5
5
1 entry was displayed.
```

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.
```

   Confirm the operation succeeded with the command:

   `storage encryption disk show-status`

   Repeat the show-status command until the numbers are the same. The operation is complete when the numbers in "disks begun" and "disks done" are the same.

Maintenance mode

Beginning with ONTAP 9.7, you can rekey a FIPS drive from maintenance mode. You should only use maintenance mode if you cannot use the ONTAP CLI instructions in the earlier section.

Steps

1. Set the FIPS authentication key ID for the node back to the default MSID 0x0:

   `disk encrypt rekey_fips 0x0` *`disklist`*

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

```
disk encrypt rekey 0x0 disklist
```

3. Confirm the FIPS authentication key was successfully rekeyed:

```
disk encrypt show_fips
```

4. Confirm data authentication key was successfully rekeyed with:

```
disk encrypt show
```

Your output will likely display either the default MSID 0x0 key ID or the 64-character value held by the key server. The `Locked?` field refers to data-locking.

```
Disk       FIPS Key ID                 Locked?
---------- --------------------------- -------
0a.01.0    0x0                          Yes
```

Related information

- storage encryption disk modify
- storage encryption disk show-status

Remove an external key manager connection in ONTAP

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

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.

Before you begin

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

Step

1. Disconnect a KMIP server from the current node:

For this ONTAP version…	Use this command…
ONTAP 9.6 and later	`security key-manager external remove-servers -vserver SVM -key-servers host_name|IP_address:port,…`

ONTAP 9.5 and earlier	`security key-manager delete -address key_management_server_ipaddress`

In a MetroCluster environment, you must repeat these commands on both clusters for the admin SVM.

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:

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

Learn more about `security key-manager external remove-servers` and `security key-manager delete` in the ONTAP command reference.

Modify ONTAP external key management server properties

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

Before you begin

- You must be a cluster or SVM administrator to perform this task.
- Advanced privileges are required for this task.
- In a MetroCluster environment, you must repeat these steps on both clusters for the admin SVM.

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.

Related information

- security key-manager external modify-server

Transition to external key management from onboard key management in ONTAP

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.

Before you begin

- 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	`security key-manager onboard disable -vserver SVM`
ONTAP 9.5 and earlier	`security key-manager delete-key-database`

Learn more about `security key-manager onboard disable` and `security key-manager delete-key-database` in the ONTAP command reference.

Switch from external key management to ONTAP onboard key management

To switch to onboard key management, delete the external key management configuration before you enable onboard key management.

Before you begin

- 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

The steps to transition your key management depend on the version of ONTAP you are using.

ONTAP 9.6 and later

1. Change to the advanced privilege level:

   ```
   set -privilege advanced
   ```

2. Use the command:

   ```
   security key-manager external disable -vserver admin_SVM
   ```

   > In a MetroCluster environment, you must repeat the command on both clusters for the admin SVM.

Learn more about `security key-manager external disable` in the ONTAP command reference.

ONTAP 9.5 and earlier

Use the command:
`security key-manager delete-kmip-config`

Learn more about `security key-manager delete-kmip-config` in the ONTAP command reference.

Related information

- security key-manager external disable

What happens when key management servers are not reachable during the ONTAP 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.
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 ONTAP encryption by default

Beginning with ONTAP 9.7, aggregate and volume encryption is enabled by default if you have a volume encryption (VE) license and use an onboard or external key manager. If necessary, you can disable encryption by default for the entire cluster.

Before you begin

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 for the entire cluster in ONTAP 9.7 or later, run the following command:

   ```
   options -option-name encryption.data_at_rest_encryption.disable_by_default
   -option-value on
   ```

Copyright information

Trademark information