Manage encryption with the CLI

ONTAP 9

NetApp
August 12, 2022

Table of Contents

Manage encryption with the CLI

NetApp Encryption overview with the CLI

NetApp offers both software- and hardware-based encryption technologies for ensuring that data at rest cannot be read if the storage medium is repurposed, returned, misplaced, or stolen.

- Software-based encryption supports data encryption one volume at a time.
- Hardware-based encryption supports full-disk encryption (FDE) of data as it is written.

You can work with encryption if the following apply:

- You want to use best practices, not explore every available option.
- You want to use the ONTAP command-line interface (CLI), not System Manager or an automated scripting tool.

Configure NetApp Volume Encryption

Configure NetApp Volume Encryption overview

NetApp Volume Encryption (NVE) is a software-based technology for encrypting data at rest one volume at a time. An encryption key accessible only to the storage system ensures that volume data cannot be read if the underlying device is repurposed, returned, misplaced, or stolen.

Understanding NVE

Both data, including Snapshot copies, and metadata are encrypted. Access to the data is given by a unique XTS-AES-256 key, one per volume. An external key management server or Onboard Key Manager serves keys to nodes:

- The external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP). It is a best practice to configure external key management servers on a different storage system from your data.
- The Onboard Key Manager is a built-in tool that serves keys to nodes from the same storage system as your data.

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. Whenever an external or onboard key manager is configured there is a change in how the encryption of data at rest is configured for brand new aggregates and brand new volumes. Brand new aggregates will have NetApp Aggregate Encryption (NAE) enabled by default. Brand new volumes that are not part of an NAE aggregate will have NetApp Volume Encryption (NVE) enabled by default. If a data storage virtual machine (SVM) is configured with its own key-manager using multi-tenant key management, then the volume created for that SVM is automatically configured with NVE.

You can enable encryption on a new or existing volume. NVE supports the full range of storage efficiency features, including deduplication and compression.

If you are using SnapLock, you can enable encryption only on new, empty SnapLock volumes. You cannot enable encryption on an existing SnapLock volume.

You can use NVE on any type of aggregate (HDD, SSD, hybrid, array LUN), with any RAID type, and in any supported ONTAP implementation, including ONTAP Select. You can also use NVE with hardware-based encryption to “double encrypt” data on self-encrypting drives.

AFF A220, AFF A800, FAS2720, FAS2750, and later systems store core dumps on their boot device. When NVE is enabled on these systems, the core dump is also encrypted.

Aggregate-level encryption

Ordinarily, every encrypted volume is assigned a unique key. When the volume is deleted, the key is deleted with it.

Beginning with ONTAP 9.6, you can use *NetApp Aggregate Encryption (NAE)* to assign keys to the containing aggregate for the volumes to be encrypted. When an encrypted volume is deleted, the keys for the aggregate are preserved. The keys are deleted the entire aggregate is deleted.

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

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.

NVE and NAE volumes can coexist on the same aggregate. Volumes encrypted under aggregate-level encryption are NAE volumes by default. You can override the default when you encrypt the volume.

You can use the `volume move` command to convert an NVE volume to an NAE volume, and vice versa. You can replicate an NAE volume to an NVE volume.

You cannot use `secure purge` commands on an NAE volume.

When to use external key management servers

Although it is less expensive and typically more convenient to use the onboard key manager, you should set up KMIP servers if any of the following are true:

- Your encryption key management solution must comply with Federal Information Processing Standards (FIPS) 140-2 or the OASIS KMIP standard.
- You need a multi-cluster solution, with centralized management of encryption keys.
- Your business requires the added security of storing authentication keys on a system or in a location different from the data.

Scope of external key management

The scope of external key management determines whether key management servers secure all the SVMs in the cluster or selected SVMs only:

- You can use a *cluster scope* to configure external key management for all the SVMs in the cluster. The cluster administrator has access to every key stored on the servers.
- Beginning with ONTAP 9.6, you can use an *SVM scope* to configure external key management for a

named SVM in the cluster. That's best for multitenant environments in which each tenant uses a different SVM (or set of SVMs) to serve data. Only the SVM administrator for a given tenant has access to the keys for that tenant.

- Beginning with ONTAP 9.10.1, you can use Azure Key Vault and Google Cloud KMS to protect NVE keys only for data vservers.

You can use both scopes in the same cluster. If key management servers have been configured for an SVM, ONTAP uses only those servers to secure keys. Otherwise, ONTAP secures keys with the key management servers configured for the cluster.

A list of validated external key managers is available in the NetApp Interoperability Matrix Tool (IMT). You can find this list by entering the term "key managers" into the IMT's search feature.

Support details

The following table shows NVE support details:

Resource or feature	Support details
Platforms	AES-NI offload capability required. See the Hardware Universe (HWU) to verify that NVE and NAE are supported for your platform.

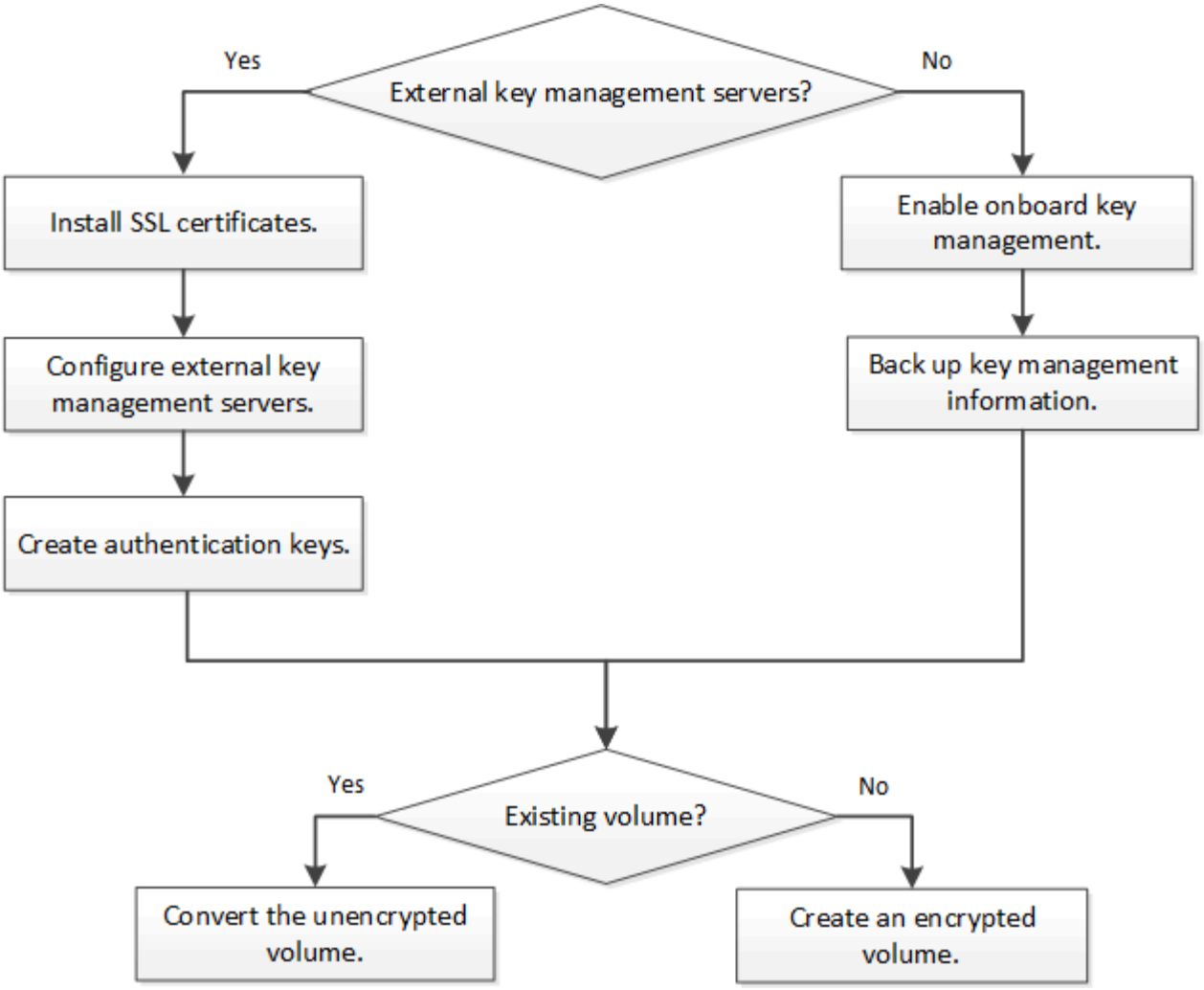
Encryption	Beginning with ONTAP 9.7, newly created aggregates and volumes are encrypted by default when you add a volume encryption (VE) license and have an onboard or external key manager configured. If you need to create an unencrypted aggregate, use the following command:
	
	`storage aggregate create -encrypt-with-aggr-key false`
	
	If you need to create a plain text volume, use the following command:
	
	`volume create -encrypt false`
	
	Encryption is not enabled by default when:
	
	• VE license is not installed.
	• Key manager is not configured.
	• Platform or software does not support encryption.
	• Hardware encryption is enabled.

ONTAP	All ONTAP implementations. Support for ONTAP Cloud is available in ONTAP 9.5 and later.
Devices	HDD, SSD, hybrid, array LUN.
RAID	RAID0, RAID4, RAID-DP, RAID-TEC.
Volumes	Data volumes and existing root volumes. You cannot encrypt data on an SVM root volume or MetroCluster metadata volumes.

Aggregate-level encryption	Beginning with ONTAP 9.6, NVE supports aggregate-level encryption (NAE): • You must use aggregate-level encryption if you plan to perform inline or background aggregate-level deduplication. • You cannot rekey an aggregate-level encryption volume. • Secure-purge is not supported on aggregate-level encryption volumes. • In addition to data volumes, NAE supports encryption of SVM root volumes and the MetroCluster metadata volume. NAE does not support encryption of the root volume.
SVM scope	Beginning with ONTAP 9.6, NVE supports SVM scope for external key management only, not for Onboard Key Manager. MetroCluster is supported beginning with ONTAP 9.8.
Storage efficiency	Deduplication, compression, compaction, FlexClone. Clones use the same key as the parent, even after splitting the clone from the parent. You are warned to rekey the split clone.
Replication	• For volume replication, the destination volume must have been enabled for encryption. Encryption can be configured for the source and unconfigured for the destination, and vice versa. • For SVM replication, the destination volume is automatically encrypted, unless the destination does not contain a node that supports volume encryption, in which case replication succeeds, but the destination volume is not encrypted. • For MetroCluster configurations, each cluster pulls external key management keys from its configured key servers. OKM keys are replicated to the partner site by the configuration replication service.
Compliance	Beginning with ONTAP 9.2, SnapLock is supported in both Compliance and Enterprise modes, for new volumes only. You cannot enable encryption on an existing SnapLock volume.
FlexGroups	Beginning with ONTAP 9.2, FlexGroups are supported. Destination aggregates must be of the same type as source aggregates, either volume-level or aggregate-level. Beginning with ONTAP 9.5, in-place rekey of FlexGroup volumes is supported.
7-Mode transition	Beginning with 7-Mode Transition Tool 3.3, you can use the 7-Mode Transition Tool CLI to perform copy-based transition to NVE-enabled destination volumes on the clustered system.

NetApp Volume Encryption workflow

You must configure key management services before you can enable volume encryption. You can enable encryption on a new volume or on an existing volume.



You must install the VE license and configure key management services before you can encrypt data with NVE. Before installing the license, you should determine whether your ONTAP version supports NVE.

Configure NVE

Determine whether your cluster version supports NVE

You should determine whether your cluster version supports NVE before you install the license. You can use the `version` command to determine the cluster version.

About this task

The cluster version is the lowest version of ONTAP running on any node in the cluster.

Step

1. Determine whether your cluster version supports NVE:

   ```
   version -v
   ```

   NVE is not supported if the command output displays the text “1Ono-DARE” (for “no Data At Rest Encryption”), or if you are using a platform that is not listed in Support details.

   The following command determines whether NVE is supported on `cluster1`.

```
cluster1::> version -v
NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <1Ono-DARE>
```

The text “1Ono-DARE” in the command output indicates that NVE is not supported on your cluster version.

Install the license

A VE license entitles you to use the feature on all nodes in the cluster. You must install the license before you can encrypt data with NVE.

What you’ll need

You must be a cluster administrator to perform this task.

About this task

You should have received the VE license key from your sales representative.

Steps

1. Install the VE license for a node:

   `system license add -license-code license_key`

   The following command installs the license with the key `AAAAAAAAAAAAAAAAAAAAAAAAAAAA`.

   ```
   cluster1::> system license add -license-code
   AAAAAAAAAAAAAAAAAAAAAAAAAAAA
   ```

2. Verify that the license is installed by displaying all the licenses on the cluster:

   `system license show`

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

   The following command displays all the licenses on `cluster1`:

   ```
   cluster1::> system license show
   ```

   The VE license package name is “VE”.

Configure external key management

Configure external key management overview

You can use one or more external key management servers to secure the keys that the cluster uses to access encrypted data. An external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP).

For ONTAP 9.1 and earlier versions, node management LIFs must be assigned to ports that are configured with the node management role before you can use the external key manager.

NetApp Volume Encryption (NVE) supports Onboard Key Manager in ONTAP 9.1 and later. Beginning in ONTAP 9.3, NVE supports external key management (KMIP) and Onboard Key Manager. Beginning in ONTAP 9.10.1, you can use Azure Key Vault or Google Cloud Key Manager Service to protect your NVE keys. Beginning in ONTAP 9.11.1, you can configure multiple external key managers in a cluster. See Configure clustered key servers.

Install SSL certificates on the cluster

The cluster and KMIP server use KMIP SSL certificates to verify each other's identity and establish an SSL connection. Before configuring the SSL connection with the KMIP server, you must install the KMIP client SSL certificates for the cluster, and the SSL public certificate for the root certificate authority (CA) of the KMIP server.

What you'll need

- The time must be synchronized on the server creating the certificates, the KMIP server, and the cluster.
- You must have obtained the public SSL KMIP client certificate for the cluster.
- You must have obtained the private key associated with the SSL KMIP client certificate for the cluster.

  The SSL KMIP client certificate must not be password-protected.
- You must have obtained the SSL public certificate for the root certificate authority (CA) of the KMIP server.

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

About this task

In an HA pair, both nodes must use the same public and private KMIP SSL certificates. If you connect multiple HA pairs to the same KMIP server, all nodes in the HA pairs must use the same public and private KMIP SSL certificates.

Steps

1. Install the SSL KMIP client certificates for the cluster:

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   You are prompted to enter the SSL KMIP public and private certificates.

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. Install the SSL public certificate for the root certificate authority (CA) of the KMIP server:

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

Enable external key management in ONTAP 9.6 and later (NVE)

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data. Beginning with ONTAP 9.6, you can use one or more KMIP servers to secure the keys a given SVM uses to access encrypted data.

Beginning in ONTAP 9.11.1, you can add up to 3 secondary key servers per primary key server to create a clustered key server. For more information, see Configure clustered external key servers.

Before you begin

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster or SVM administrator to perform this task.
- If you want to enable external key management for a MetroCluster environment, MetroCluster must be fully configured before enabling external key management.

About this task

You can connect up to four KMIP servers to a cluster or SVM. A minimum of two servers is recommended for redundancy and disaster recovery.

The scope of external key management determines whether key management servers secure all the SVMs in the cluster or selected SVMs only:

- You can use a *cluster scope* to configure external key management for all the SVMs in the cluster. The cluster administrator has access to every key stored on the servers.
- Beginning with ONTAP 9.6, you can use an *SVM scope* to configure external key management for a data SVM in the cluster. That's best for multitenant environments in which each tenant uses a different SVM (or set of SVMs) to serve data. Only the SVM administrator for a given tenant has access to the keys for that tenant.
- For multitenant environments, install a license for *MT_EK_MGMT* by using the following command:

  ```
  system license add -license-code <MT_EK_MGMT license code>
  ```

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

You can use both scopes in the same cluster. If key management servers have been configured for an SVM, ONTAP uses only those servers to secure keys. Otherwise, ONTAP secures keys with the key management servers configured for the cluster.

You can configure onboard key management at the cluster scope and external key management at the SVM scope. You can use the `security key-manager key migrate` command to migrate keys from onboard key management at the cluster scope to external key managers at the SVM scope.

Steps

1. Configure key manager connectivity for the cluster:

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

The `security key-manager external enable` command replaces the `security key-manager setup` command. 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 configure cluster scope. You can run the `security key-manager external modify` command to change the external key management configuration.

The following command enables external key management for `cluster1` with three external key servers. The first key server is specified using its hostname and port, the second is specified using an IP address and the default port, and the third is specified using an IPv6 address and port:

```
clusterl::> security key-manager external enable -vserver cluster1 -key
-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. Configure a key manager an SVM:

   `security key-manager external enable -vserver SVM -key-servers host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert server_CA_certificates`

   If you run the command at the SVM login prompt, `SVM` defaults to the current SVM. You must be a cluster or SVM administrator to configure SVM scope. You can run the `security key-manager external modify` command to change the external key management configuration.

   The following command enables external key management for `svm1` with a single key server listening on the default port 5696:

   ```
   svm1l::> security key-manager external enable -vserver svm1 -key-servers
   keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
   SVM1ServerCaCert
   ```

3. Repeat the last step for any additional SVMs.

   You can also use the `security key-manager external add-servers` command to configure additional SVMs. The `security key-manager external add-servers` command replaces the `security key-manager add` command. For complete command syntax, see the man page.

4. Verify that all configured KMIP servers are connected:

   `security key-manager external show-status -node node_name`

The `security key-manager external show-status` command replaces the `security key-manager show -status` command. For complete command syntax, see the man page.

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  ---------------------------------------
-------------
node1
      svm1
               keyserver.svm1.com:5696                         available
      cluster1
               10.0.0.10:5696                                  available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234    available
               ks1.local:15696                                 available
node2
      svm1
               keyserver.svm1.com:5696                         available
      cluster1
               10.0.0.10:5696                                  available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234    available
               ks1.local:15696                                 available

8 entries were displayed.
```

Enable external key management in ONTAP 9.5 and earlier

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data. You can connect up to four KMIP servers to a node. A minimum of two servers is recommended for redundancy and disaster recovery.

What you'll need

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure an external key manager.

About this task

ONTAP configures KMIP server connectivity for all nodes in the cluster.

Steps

1. Configure key manager connectivity for cluster nodes:

   `security key-manager setup`

   The key manager setup starts.

2. Enter the appropriate response at each prompt.
3. Add a KMIP server:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   cluster1::> security key-manager add -address 20.1.1.1
   ```

4. Add an additional KMIP server for redundancy:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   cluster1::> security key-manager add -address 20.1.1.2
   ```

5. Verify that all configured KMIP servers are connected:

   `security key-manager show -status`

   For complete command syntax, see the man page.

   ```
   cluster1::> security key-manager show -status

   Node            Port      Registered Key Manager  Status
   --------------  ----      ----------------------  ---------------
   cluster1-01     5696      20.1.1.1                available
   cluster1-01     5696      20.1.1.2                available
   cluster1-02     5696      20.1.1.1                available
   cluster1-02     5696      20.1.1.2                available
   ```

Manage keys with Azure Key Vault or Google Cloud KMS

Beginning in ONTAP 9.10.1, you can use Azure Key Vault (AKV) and Google Cloud Platform's Key Management Service (Cloud KMS) to protect your ONTAP encryption keys in a Azure- or Google Cloud Platform-deployed application.

AKV and Cloud KMS can be used to protect NetApp Volume Encryption (NVE) keys only for data SVMs.

Key management with AKV or Cloud KMS can be enabled with the CLI or the ONTAP REST API.

When using AKV or Cloud KMS, be aware that by default a data SVM LIF is used to communicate with the cloud key management endpoint. A node management network is used to communicate with the cloud provider's authentication services (login.microsoftonline.com for Azure; oauth2.googleapis.com for Cloud KMS). If the cluster network is not configured correctly, the cluster will not properly utilize the key management service.

Prerequisites

- The ONTAP cluster's nodes must support NVE

- Volume Encryption (VE) license installed
- Multi-tenant Encryption Key Management (MTEKM) license installed
- You must be a cluster or SVM administrator

Limitations

- AKV and Cloud KMS are not available for NSE and NAE. External KMIPs can be used instead
- AKV and Cloud KMS are not available for MetroCluster configurations.
- AKV and Cloud KMS can only be configured on a data SVM

Enable external key management with the CLI

Enabling external key management depends on the specific key manager you use. If you are enabling AKV in a Cloud Volumes ONTAP, note that there is a separate procedure. Choose the tab of the key manager and environment that suits your needs:

Azure

Enable Azure Key Vault for ONTAP

1. Before you begin, you need to obtain the appropriate authentication credentials from your Azure account, either a client secret or certificate.
   You must also ensure all nodes in the cluster are healthy. You can check this with the command `cluster show`.
2. Set privileged level to advanced
   `set -priv advanced`
3. Enable AKV on the SVM
   `security key-manager external azure enable -client-id client_id -tenant-id tenant_id -name -key-id key_id -authentication-method {certificate|client-secret}`
   When prompted, enter either the client certificate or client secret from your Azure account.
4. Verify AKV is enabled correctly:
   `security key-manager external azure show vserver SVM_name`
   If the service reachability is not OK, establish the connectivity to the AKV key management service via data SVM LIF.

Google Cloud

Enable Cloud KMS with the CLI for ONTAP

1. Before you begin, you need to obtain the private key for the Google Cloud KMS account key file in a JSON format. This can be found in your GCP account.
   You must also ensure all nodes in the cluster are healthy. You can check this with the command `cluster show`.
2. Set privileged level to advanced
   `set -priv advanced`
3. Enable Cloud KMS on the SVM
   `security key-manager external gcp enable -vserver data_svm_name -project-id project_id-key-ring-name key_ring_name -key-ring-location key_ring_location -key-name key_name`
   When prompted, enter the contents of the JSON file with the Service Account Private Key
4. Verify that Cloud KMS is configured with the correct parameters:
   `security key-manager external gcp show vserver SVM_name`
   The status of `kms_wrapped_key_status` will be "`UNKNOWN`" if no encrypted volumes have been created.
   If the service reachability is not OK, establish the connectivity to the GCP key management service via data SVM LIF.

If one or more encrypted volumes is already configured for a data SVM and the corresponding NVE keys are managed by the admin SVM onboard key manager, those keys should be migrated to the external key management service. To do this with the CLI, run the command:
`security key-manager key migrate -from-Vserver admin_SVM -to-Vserver data_SVM`
New encrypted volumes cannot be created for the tenant's data vserver until all NVE keys of the data SVM are successfully migrated.

Enable onboard key management in ONTAP 9.6 and later (NVE)

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

What you'll need

- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure an external key manager.

About this task

You must run the `security key-manager onboard sync` command each time you add a node to the cluster.

If you have a MetroCluster configuration you must run `security key-manager onboard enable` on the local cluster first, then run `security key-manager onboard sync` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. You can use the `cc-mode-enabled=yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `cc-mode-enabled=yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.

When configuring ONTAP data at rest encryption, to meet the requirements for Commercial Solutions for Classified (CSfC) you must use NSE with NVE and ensure the Onboard Key Manager is enabled in Common Criteria mode. Refer to the CSfC Solution Brief for more information on CSfC.

When the Onboard Key Manager is enabled in Common Criteria mode (`cc-mode-enabled=yes`), system behavior is changed in the following ways:

- The system monitors for consecutive failed cluster passphrase attempts when operating in Common Criteria mode.

  If you fail to enter the correct cluster passphrase at boot, encrypted volumes are not mounted. To correct this, you must reboot the node and enter the correct cluster passphrase. Once booted, the system allows up to 5 consecutive attempts to correctly enter the cluster passphrase in a 24-hour period for any command that requires the cluster passphrase as a parameter. If the limit is reached (for example, you have failed to correctly enter the cluster passphrase 5 times in a row) then you must either wait for the 24-hour timeout period to elapse, or you must reboot the node, in order to reset the limit.

- System image updates use the NetApp RSA-3072 code signing certificate together with SHA-384 code signed digests to check the image integrity instead of the usual NetApp RSA-2048 code signing certificate and SHA-256 code signed digests.

  The upgrade command verifies that the image contents have not been altered or corrupted by checking various digital signatures. The image update process proceeds to the next step if validation succeeds; otherwise, the image update fails. See the "cluster image" man page for information concerning system updates.

The Onboard Key Manager stores keys in volatile memory. Volatile memory contents are cleared when the system is rebooted or halted. Under normal operating conditions, volatile memory contents will be cleared within 30s when a system is halted.

Steps

1. Start the key manager setup:

   `security key-manager onboard enable -cc-mode-enabled yes|no`

   Set `cc-mode-enabled=yes` to require that users enter the key manager passphrase after a reboot. For NVE, if you set `cc-mode-enabled=yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. The `- cc-mode-enabled` option is not supported in MetroCluster configurations. The `security key-manager onboard enable` command replaces the `security key-manager setup` command.

   The following example starts the key manager setup command on cluster1 without requiring that the passphrase be entered after every reboot:

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

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

2. At the 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 operation displays the passphrase prompt again.

3. At the passphrase confirmation prompt, reenter the passphrase.
4. Verify that the authentication keys have been created:

   `security key-manager key query -key-type NSE-AK`

   The `security key-manager key query` command replaces the `security key-manager query key` command. For complete command syntax, see the man page.

   The following example verifies that authentication keys have been created for `cluster1`:

   ```
   cluster1::> security key-manager key query -key-type NSE-AK
          Vserver: cluster1
      Key Manager: onboard
             Node: node1
   ```

```
Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: svm1
   Key Manager: onboard
          Node: node1
    Key Server: keyserver.svm1.com:5965

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
eb9f8311-e8d8-487e-9663-7642d7788a75     VEK       yes
    Key ID:
000000000000000002000000000004001cb18336f7c8223743d3e75c6a7726e00000000
00000000
9d09cbbf-0da9-4696-87a1-8e083d8261bb     VEK       yes
    Key ID:
000000000000000002000000000004064f2e1533356a470385274a9c3ffb97700000000
00000000

       Vserver: cluster1
   Key Manager: onboard
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: svm1
   Key Manager: onboard
          Node: node2
    Key Server: keyserver.svm1.com:5965
```

```
Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
eb9f8311-e8d8-487e-9663-7642d7788a75  VEK       yes
    Key ID:
000000000000000002000000000004001cb18336f7c8223743d3e75c6a7726e00000000
00000000
9d09cbbf-0da9-4696-87a1-8e083d8261bb  VEK       yes
    Key ID:
000000000000000002000000000004064f2e1533356a470385274a9c3ffb97700000000
00000000
```

After you finish

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

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

Enable onboard key management in ONTAP 9.5 and earlier (NVE)

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

What you'll need

- If you are using NSE with an external key management (KMIP) server, you must have deleted the external key manager database.

  Transitioning to onboard key management from external key management

- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure the Onboard Key Manager.

About this task

You must run the `security key-manager setup` command each time you add a node to the cluster.

If you have a MetroCluster configuration, review these guidelines:

- In ONTAP 9.5, you must run `security key-manager setup` on the local cluster and `security key-manager setup -sync-metrocluster-config yes` on the remote cluster, using the same passphrase on each.
- Prior to ONTAP 9.5, you must run `security key-manager setup` on the local cluster, wait approximately 20 seconds, and then run `security key-manager setup` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume`

`move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.

After a failed passphrase attempt, you must reboot the node again.

Steps

1. Start the key manager setup:

   `security key-manager setup -enable-cc-mode yes|no`

   Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the key manager passphrase after a reboot. For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted.

   The following example starts setting up the key manager on cluster1 without requiring that the passphrase be entered after every reboot:

   ```
   cluster1::> security key-manager setup
   Welcome to the key manager setup wizard, which will lead you through
   the steps to add boot information.

   ...

   Would you like to use onboard key-management? {yes, no} [yes]:
   Enter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   ```

2. Enter `yes` at the prompt to configure onboard key management.
3. At the 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 operation displays the passphrase prompt again.

4. At the passphrase confirmation prompt, reenter the passphrase.
5. Verify that keys are configured for all nodes:

   `security key-manager key show`

   For the complete command syntax, see the man page.

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

Node: node1
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

After you finish

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

All key management information is automatically backed up to the replicated database (RDB) for the cluster.

Whenever you configure the Onboard Key Manager passphrase, you should also back up the information manually to a secure location outside the storage system for use in case of a disaster. See Back up onboard key management information manually.

Enable onboard key management in newly added nodes

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

For ONTAP 9.5 and earlier, you must run the `security key-manager setup` command each time you add a node to the cluster.

For ONTAP 9.6 and later, you must run the `security key-manager sync` command each time you add a node to the cluster.

If you add a node to a cluster that has onboard key management configured, you will run this command to refresh the missing keys.

If you have a MetroCluster configuration, review these guidelines:

- Beginning with ONTAP 9.6, you must run `security key-manager onboard enable` on the local cluster first, then run `security key-manager onboard sync` on the remote cluster, using the same passphrase on each.

- In ONTAP 9.5, you must run `security key-manager setup` on the local cluster and `security key-manager setup -sync-metrocluster-config yes` on the remote cluster, using the same passphrase on each.
- Prior to ONTAP 9.5, you must run `security key-manager setup` on the local cluster, wait approximately 20 seconds, and then run `security key-manager setup` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.

After a failed passphrase attempt, you must reboot the node again.

Encrypt volume data with NVE

Encrypt volume data with NVE overview

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

Enable aggregate-level encryption with VE license

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

What you'll need

You must be a cluster administrator to perform this task.

About this task

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

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

Steps

1. Enable or disable aggregate-level encryption:

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

For complete command syntax, see the man pages.

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

- ONTAP 9.7 or later:

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

- ONTAP 9.6 or earlier:

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

2. Verify that the aggregate is enabled for encryption:

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

For complete command syntax, see the man page.

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

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

After you finish

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

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

Enable encryption on a new volume

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

About this task

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

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

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

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

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

Steps

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Verify that volumes are enabled for encryption:

   `volume show -is-encrypted true`

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

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

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

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

Result

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

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

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

About this task

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

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

Steps

1. Enable encryption on an existing volume:

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

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

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

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

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

2. Verify the status of the conversion operation:

   `volume encryption conversion show`

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

   The following command displays the status of the conversion operation:

   ```
   cluster1::> volume encryption conversion show

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

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

   `volume show -is-encrypted true`

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

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

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

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

Result

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

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

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

What you'll need

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

Delegating authority to run the volume move command

About this task

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

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

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

Steps

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. View the encryption type of cluster volumes:

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

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

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

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

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

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

3. Verify that volumes are enabled for encryption:

   `volume show -is-encrypted true`

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

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

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

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

Result

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

Enable node root volume encryption

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

What you’ll need

- Your system must be using an HA configuration.

  Root volume encryption is not supported on single node configurations.

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

About this task

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

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

Steps

1. Encrypt the root volume:

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

2. Verify the status of the conversion operation:

   ```
   volume encryption conversion show
   ```

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

   ```
   volume show -fields
   ```

   The following shows example output for an encrypted volume.

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

Configure NetApp hardware-based encryption

Configure NetApp hardware-based encryption overview

NetApp hardware-based encryption supports full-disk encryption (FDE) of data as it is written. The data cannot be read without an encryption key stored on the firmware. The encryption key, in turn, is accessible only to an authenticated node.

Understanding NetApp hardware-based encryption

A node authenticates itself to a self-encrypting drive using an authentication key retrieved from an external key management server or Onboard Key Manager:

- The external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP). It is a best practice to configure external key management servers on a different storage system from your data.
- The Onboard Key Manager is a built-in tool that serves authentication keys to nodes from the same storage system as your data.

You can use NetApp Volume Encryption with hardware-based encryption to “double encrypt” data on self-encrypting drives.

AFF A220, AFF A800, FAS2720, FAS2750, and later systems store core dumps on their boot device. When self-encrypting drives are enabled on these systems, the core dump is also encrypted.

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.

Supported drive types

Two types of self-encrypting drive are supported:

- Self-encrypting FIPS-certified SAS or NVMe drives are supported on all FAS and AFF systems. These drives, called *FIPS drives,* conform to the requirements of Federal Information Processing Standard Publication 140-2, level 2. The certified capabilities enable protections in addition to encryption, such as preventing denial-of-service attacks on the drive. FIPS drives cannot be mixed with other types of drives on the same node or HA pair.
- Beginning with ONTAP 9.6, self-encrypting NVMe drives that have not undergone FIPS testing are supported on AFF A800, A320, and later systems. These drives, called *SEDs*, offer the same encryption capabilities as FIPS drives, but can be mixed with non-SEDs on the same node or HA pair.

When to use KMIP servers

Although it is less expensive and typically more convenient to use the onboard key manager, you should set up KMIP servers if any of the following are true:

- Your encryption key management solution must comply with FIPS 140-2 level 2 or higher.
- You need a multi-cluster solution, with centralized management of encryption keys.
- Your business requires the added security of storing authentication keys on a system or in a location different from the data.

Support details

The following table shows important hardware encryption support details. See the Interoperability Matrix for the latest information about supported KMIP servers, storage systems, and disk shelves.

Resource or feature	Support details
Non-homogeneous disk sets	• FIPS drives cannot be mixed with other types of drives on the same node or HA pair. Conforming HA pairs can coexist with non-conforming HA pairs in the same cluster. • SEDs can be mixed with non-SEDs on the same node or HA pair.

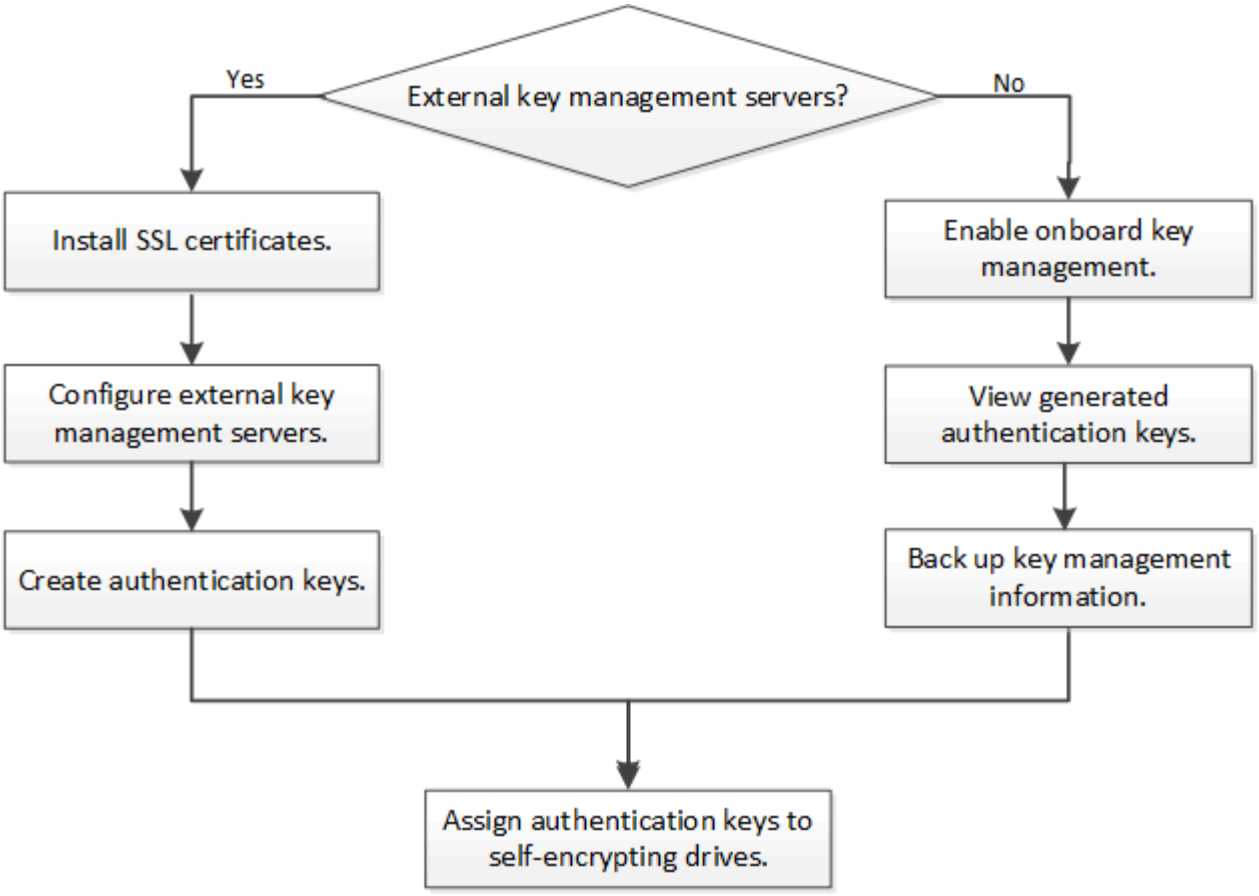
Drive type	• FIPS drives can be SAS or NVMe drives. • SEDs must be NVMe drives.
10 Gb network interfaces	Beginning with ONTAP 9.3, KMIP key management configurations support 10 Gb network interfaces for communications with external key management servers.
Ports for communication with the key management server	Beginning with ONTAP 9.3, you can use any storage controller port for communication with the key management server. Otherwise, you should use port e0m for communication with key management servers. Depending on the storage controller model, certain network interfaces might not be available during the boot process for communication with key management servers.
MetroCluster (MCC)	• NVMe drives support MCC. • SAS drives do not support MCC.

Related information

NetApp Hardware Universe

Hardware-based encryption workflow

You must configure key management services before the cluster can authenticate itself to the self-encrypting drive. You can use an external key management server or an onboard key manager.



Configure external key management

Configure external key management overview

You can use one or more external key management servers to secure the keys that the cluster uses to access encrypted data. An external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP).

For ONTAP 9.1 and earlier versions, node management LIFs must be assigned to ports that are configured with the node management role before you can use the external key manager.

NetApp Volume Encryption (NVE) can be implemented with Onboard Key Manager in ONTAP 9.1 and later. In ONTAP 9.3 and later, NVE can be implemented with external key management (KMIP) and Onboard Key Manager. Beginning in ONTAP 9.11.1, you can configure multiple external key managers in a cluster. See Configure clustered key servers.

Collect network information in ONTAP 9.2 and earlier

If you are using ONTAP 9.2 or earlier, you should fill out the network configuration worksheet before enabling external key management.

Beginning with ONTAP 9.3, the system discovers all needed network information automatically.

Item	Notes	Value

Key management network interface name		
Key management network interface IP address	IP address of node management LIF, in IPv4 or IPv6 format	
Key management network interface IPv6 network prefix length	If you are using IPv6, the IPv6 network prefix length	
Key management network interface subnet mask		
Key management network interface gateway IP address		
IPv6 address for the cluster network interface	Required only if you are using IPv6 for the key management network interface	
Port number for each KMIP server	Optional. The port number must be the same for all KMIP servers. If you do not provide a port number, it defaults to port 5696, which is the Internet Assigned Numbers Authority (IANA) assigned port for KMIP.	
Key tag name	Optional. The key tag name is used to identify all keys belonging to a node. The default key tag name is the node name.	

Related information

NetApp Technical Report 3954: NetApp Storage Encryption Preinstallation Requirements and Procedures for IBM Tivoli Lifetime Key Manager

NetApp Technical Report 4074: NetApp Storage Encryption Preinstallation Requirements and Procedures for SafeNet KeySecure

Install SSL certificates on the cluster

The cluster and KMIP server use KMIP SSL certificates to verify each other's identity and establish an SSL connection. Before configuring the SSL connection with the KMIP server, you must install the KMIP client SSL certificates for the cluster, and the SSL public certificate for the root certificate authority (CA) of the KMIP server.

What you'll need

- The time must be synchronized on the server creating the certificates, the KMIP server, and the cluster.
- You must have obtained the public SSL KMIP client certificate for the cluster.

- You must have obtained the private key associated with the SSL KMIP client certificate for the cluster.

  The SSL KMIP client certificate must not be password-protected.

- You must have obtained the SSL public certificate for the root certificate authority (CA) of the KMIP server.

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

About this task

In an HA pair, both nodes must use the same public and private KMIP SSL certificates. If you connect multiple HA pairs to the same KMIP server, all nodes in the HA pairs must use the same public and private KMIP SSL certificates.

Steps

1. Install the SSL KMIP client certificates for the cluster:

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   You are prompted to enter the SSL KMIP public and private certificates.

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. Install the SSL public certificate for the root certificate authority (CA) of the KMIP server:

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

Enable external key management in ONTAP 9.6 and later (HW-based)

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data. You can connect up to four KMIP servers to a node. A minimum of two servers is recommended for redundancy and disaster recovery.

Beginning in ONTAP 9.11.1, you can add up to 3 secondary key servers per primary key server to create a clustered key server. For more information, see Configure clustered external key servers.

Before you begin

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure an external key manager.

Steps

1. Configure key manager connectivity for the cluster:

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

> The `security key-manager external enable` command replaces the `security key-manager setup` command. You can run the `security key-manager external modify` command to change the external key management configuration. For complete command syntax, see the man pages.

The following command enables external key management for `cluster1` with three external key servers. The first key server is specified using its hostname and port, the second is specified using an IP address and the default port, and the third is specified using an IPv6 address and port:

```
cluster1::> security key-manager external enable -key-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. Verify that all configured KMIP servers are connected:

`security key-manager external show-status -node node_name -vserver SVM -key -server host_name|IP_address:port -key-server-status available|not-responding|unknown`

> The `security key-manager external show-status` command replaces the `security key-manager show -status` command. For complete command syntax, see the man page.

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  ---------------------------------------
-------------
node1
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available
node2
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available

6 entries were displayed.
```

Enable external key management in ONTAP 9.5 and earlier

You can use one or more KMIP servers to secure the keys the cluster uses to access

encrypted data. You can connect up to four KMIP servers to a node. A minimum of two servers is recommended for redundancy and disaster recovery.

What you'll need

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure an external key manager.

About this task

ONTAP configures KMIP server connectivity for all nodes in the cluster.

Steps

1. Configure key manager connectivity for cluster nodes:

   `security key-manager setup`

   The key manager setup starts.

2. Enter the appropriate response at each prompt.
3. Add a KMIP server:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   cluster1::> security key-manager add -address 20.1.1.1
   ```

4. Add an additional KMIP server for redundancy:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   cluster1::> security key-manager add -address 20.1.1.2
   ```

5. Verify that all configured KMIP servers are connected:

   `security key-manager show -status`

   For complete command syntax, see the man page.

   ```
   cluster1::> security key-manager show -status

   Node            Port      Registered Key Manager  Status
   --------------  ----      ----------------------  ---------------
   cluster1-01     5696      20.1.1.1                available
   cluster1-01     5696      20.1.1.2                available
   cluster1-02     5696      20.1.1.1                available
   cluster1-02     5696      20.1.1.2                available
   ```

Configure clustered external key servers

Beginning in ONTAP 9.11.1, you can configure connectivity to clustered external key management servers on an SVM. With clustered key servers, you can designate primary and secondary key servers on a SVM. When registering keys, ONTAP will first attempt to access a primary key server before sequentially attempting to access secondary servers until the operation completes successfully, preventing duplication of keys.

External key servers can be used for NSE, NVE, NAE, and SED keys. An SVM can support up to four primary external KMIP servers. Each primary server can support up to three secondary key servers.

Before you begin

- KMIP key management is already enabled for the SVM.
- This process only supports key servers that use KMIP. For a list of supported key servers, check the NetApp Interoperability Matrix Tool.
- All nodes in the cluster must be running ONTAP 9.11.1 or later.
- The order of servers list arguments in the `-secondary-key-servers` parameter reflects the access order of the external key management (KMIP) servers.

Create a clustered key server

The configuration procedure depends on whether or not you have configured a primary key server.

Add primary and secondary key servers to an SVM

1. Confirm that no key management has been enabled for the cluster:
   `security key-manager external show -vserver` *`vserver_name`*
   If the SVM already has the maximum of four primary key servers enabled, you must remove one of the existing primary key servers before adding a new one.
2. Enable the primary key manager:
   `security key-manager external enable -vserver` *`vserver_name`* `-key-servers` *`server_ip`* `-client-cert` *`client_cert_name`* `-server-ca-certs` *`server_ca_cert_names`*
3. Modify the primary key server to add secondary key servers. The `-secondary-key-servers` parameter accepts a comma-separated list of up to three key servers.
   `security key-manager external modify-server -vserver` *`vserver_name`* `-key -servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*

Add secondary key servers to an existing primary key server

1. Modify the primary key server to add secondary key servers. The `-secondary-key-servers` parameter accepts a comma-separated list of up to three key servers.
   `security key-manager external modify-server -vserver` *`vserver_name`* `-key -servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*
   For more information about secondary key servers, see Modifying secondary key servers.

Modify clustered key servers

You can modify external key servers clusters by changing the status (primary or secondary) of particular key

servers, add and removing secondary key servers, or by changing the access order of secondary key servers.

Converting primary and secondary key servers

To convert a primary key server into a secondary key server, you must first remove it from the SVM with the `security key-manager external remove-servers` command.

To convert a secondary key server into a primary key server, you must first remove the secondary key server from its existing primary key server. See Modifying secondary key servers. If you convert a secondary key server to a primary server while removing an existing key, attempting to add a new server before completing the removal and conversion can result in the the duplication of keys.

Modifying secondary key servers

Secondary key servers are managed with the `-secondary-key-servers` parameter of the `security key-manager external modify-server` command. The `-secondary-key-servers` parameter accepts a comma-separated list. The specified order of the secondary key servers in the list determines the access sequence for the secondary key servers. The access order can be modified by running the command `security key-manager external modify-server` with the secondary key servers entered in a different sequence.

To remove a secondary key server, the `-secondary-key-servers` arguments should include the key servers you want to keep while omitting the one to be removed. To remove all secondary key servers, use the argument `-`, signifying none.

For additional information, refer to the `security key-manager external` page in the ONTAP command reference.

Create authentication keys in ONTAP 9.6 and later

You can use the `security key-manager key create` command to create the authentication keys for a node and store them on the configured KMIP servers.

What you'll need

You must be a cluster administrator to perform this task.

About this task

If your security setup requires you to use different keys for data authentication and FIPS 140-2 authentication, you should create a separate key for each. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

ONTAP creates authentication keys for all nodes in the cluster.

- This command is not supported when Onboard Key Manager is enabled. However, two authentication keys are created automatically when Onboard Key Manager is enabled. The keys can be viewed with the following command:

  ```
  security key-manager key query -key-type NSE-AK
  ```

- You receive a warning if the configured key management servers are already storing more than 128 authentication keys.

  You can use the `security key-manager key delete` command to delete any unused keys. The

`security key-manager key delete` command fails if the given key is currently in use by ONTAP. (You must have privileges greater than “admin” to use this command.)

Steps

1. Create the authentication keys for cluster nodes:

   `security key-manager key create -key-tag passphrase_label -prompt-for-key true|false`

   > Setting `prompt-for-key=true` causes the system to prompt the cluster administrator for the passphrase to use when authenticating encrypted drives. Otherwise, the system automatically generates a 32-byte passphrase. The `security key-manager key create` command replaces the `security key-manager create-key` command. For complete command syntax, see the man page.

   The following example creates the authentication keys for `cluster1`, automatically generating a 32-byte passphrase:

   ```
   cluster1::> security key-manager key create
   Key ID:
   000000000000000002000000000001006268333f870860128fbe17d393e5083b0000000000000000
   ```

2. Verify that the authentication keys have been created:

   `security key-manager key query -node node`

   > The `security key-manager key query` command replaces the `security key-manager query key` command. For complete command syntax, see the man page. The key ID displayed in the output is an identifier used to refer to the authentication key. It is not the actual authentication key or the data encryption key.

   The following example verifies that authentication keys have been created for `cluster1`:

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: external
          Node: node1

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

Create authentication keys in ONTAP 9.5 and earlier

You can use the `security key-manager create-key` command to create the authentication keys for a node and store them on the configured KMIP servers.

What you'll need

You must be a cluster administrator to perform this task.

About this task

If your security setup requires you to use different keys for data authentication and FIPS 140-2 authentication, you should create a separate key for each. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

ONTAP creates authentication keys for all nodes in the cluster.

- This command is not supported when onboard key management is enabled.
- You receive a warning if the configured key management servers are already storing more than 128 authentication keys.

  You can use the key management server software to delete any unused keys, then run the command again.

Steps

1. Create the authentication keys for cluster nodes:

   `security key-manager create-key`

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

   > The key ID displayed in the output is an identifier used to refer to the authentication key. It is not the actual authentication key or the data encryption key.

   The following example creates the authentication keys for `cluster1`:

   ```
   cluster1::> security key-manager create-key
      (security key-manager create-key)
   Verifying requirements...

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   Node: cluster1-01
   Key manager restore operation initialized.
   Successfully restored key information.

   Node: cluster1-02
   Key manager restore operation initialized.
   Successfully restored key information.
   ```

2. Verify that the authentication keys have been created:

   `security key-manager query`

   For complete command syntax, see the man page.

   The following example verifies that authentication keys have been created for `cluster1`:

```
cluster1::> security key-manager query

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-01     NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C


          Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-02     NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
```

Assign a data authentication key to a FIPS drive or SED (external key management)

You can use the `storage encryption disk modify` command to assign a data authentication key to a FIPS drive or SED. Cluster nodes use this key to lock or unlock encrypted data on the drive.

What you'll need

You must be a cluster administrator to perform this task.

About this task

A self-encrypting drive is protected from unauthorized access only if its authentication key ID is set to a non-default value. The manufacturer secure ID (MSID), which has key ID 0x0, is the standard default value for SAS drives. For NVMe drives, the standard default value is a null key, represented as a blank key ID. When you assign the key ID to a self-encrypting drive, the system changes its authentication key ID to a non-default value.

Steps

1. Assign a data authentication key to a FIPS drive or SED:

   `storage encryption disk modify -disk` *`disk_ID`* `-data-key-id` *`key_ID`*

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

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

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

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

2. Verify that the authentication keys have 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
[...]
```

Configure onboard key management

Enable onboard key management in ONTAP 9.6 and later

You can use the Onboard Key Manager to authenticate cluster nodes to a FIPS drive or SED. The Onboard Key Manager is a built-in tool that serves authentication keys to nodes from the same storage system as your data. The Onboard Key Manager is FIPS-140-2 level 1 compliant.

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

What you'll need

- If you are using NSE with an external key management (KMIP) server, you must have deleted the external key manager database.

  Transitioning to onboard key management from external key management

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

- You must configure the MetroCluster environment before the Onboard key manager is configured.

About this task

You must run the `security key-manager onboard enable` command each time you add a node to the cluster. In MetroCluster configurations, you must run `security key-manager onboard enable` on the local cluster first, then run `security key-manager onboard sync` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. Except in MetroCluster, you can use the `cc-mode-enabled=yes` option to require that users enter the passphrase after a reboot.

When the Onboard Key Manager is enabled in Common Criteria mode (`cc-mode-enabled=yes`), system behavior is changed in the following ways:

- The system monitors for consecutive failed cluster passphrase attempts when operating in Common Criteria mode.

  If NetApp Storage Encryption (NSE) is enabled and you fail to enter the correct cluster passphrase at boot, the system cannot authenticate to its drives and automatically reboots. To correct this, you must enter the correct cluster passphrase at the boot prompt. Once booted, the system allows up to 5 consecutive attempts to correctly enter the cluster passphrase in a 24-hour period for any command that requires the cluster passphrase as a parameter. If the limit is reached (for example, you have failed to correctly enter the cluster passphrase 5 times in a row) then you must either wait for the 24-hour timeout period to elapse, or you must reboot the node, in order to reset the limit.

- System image updates use the NetApp RSA-3072 code signing certificate together with SHA-384 code signed digests to check the image integrity instead of the usual NetApp RSA-2048 code signing certificate and SHA-256 code signed digests.

  The upgrade command verifies that the image contents have not been altered or corrupted by checking various digital signatures. The image update process proceeds to the next step if validation succeeds; otherwise, the image update fails. See the “cluster image” man page for information concerning system updates.

The Onboard Key Manager stores keys in volatile memory. Volatile memory contents are cleared when the system is rebooted or halted. Under normal operating conditions, volatile memory contents will be cleared within 30s when a system is halted.

Steps

1. Start the key manager setup command:

   ```
   security key-manager onboard enable -cc-mode-enabled yes|no
   ```

   Set `cc-mode-enabled=yes` to require that users enter the key manager passphrase after a reboot. The `– cc-mode-enabled` option is not supported in MetroCluster configurations. The `security key-manager onboard enable` command replaces the `security key-manager setup` command.

   The following example starts the key manager setup command on cluster1 without requiring that the passphrase be entered after every reboot:

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

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

2. At the 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 operation displays the passphrase prompt again.

3. At the passphrase confirmation prompt, reenter the passphrase.
4. Verify that the authentication keys have been created:

   `security key-manager key query -node node`

   The `security key-manager key query` command replaces the `security key-manager query key` command. For complete command syntax, see the man page.

   The following example verifies that authentication keys have been created for `cluster1`:

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: onboard
          Node: node1

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: onboard
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

After you finish

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

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

Enable onboard key management in ONTAP 9.5 and earlier

You can use the Onboard Key Manager to authenticate cluster nodes to a FIPS drive or SED. The Onboard Key Manager is a built-in tool that serves authentication keys to nodes from the same storage system as your data. The Onboard Key Manager is FIPS-140-2 level 1 compliant.

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting

disk.

What you'll need

- If you are using NSE with an external key management (KMIP) server, you must have deleted the external key manager database.

  Transitioning to onboard key management from external key management

- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before the Onboard Key Manager is configured.

About this task

You must run the `security key-manager setup` command each time you add a node to the cluster.

If you have a MetroCluster configuration, review these guidelines:

- In ONTAP 9.5, you must run `security key-manager setup` on the local cluster and `security key-manager setup -sync-metrocluster-config yes` on the remote cluster, using the same passphrase on each.
- Prior to ONTAP 9.5, you must run `security key-manager setup` on the local cluster, wait approximately 20 seconds, and then run `security key-manager setup` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.

After a failed passphrase attempt, you must reboot the node again.

Steps

1. Start the key manager setup:

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the key manager passphrase after a reboot. For NVE, if you set `-enable-cc -mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted.

   The following example starts setting up the key manager on cluster1 without requiring that the passphrase be entered after every reboot:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Enter `yes` at the prompt to configure onboard key management.
3. At the 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 operation displays the passphrase prompt again.

4. At the passphrase confirmation prompt, reenter the passphrase.
5. Verify that keys are configured for all nodes:

   `security key-manager key show`

   For the complete command syntax, see the man page.

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

Node: node1
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------
--------
000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000020000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------
--------
000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000020000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

After you finish

All key management information is automatically backed up to the replicated database (RDB) for the cluster.

Whenever you configure the Onboard Key Manager passphrase, you should also back up the information manually to a secure location outside the storage system for use in case of a disaster. See Back up onboard key management information manually.

Assign a data authentication key to a FIPS drive or SED (onboard key management)

You can use the `storage encryption disk modify` command to assign a data authentication key to a FIPS drive or SED. Cluster nodes use this key to access data on the drive.

What you'll need

You must be a cluster administrator to perform this task.

About this task

A self-encrypting drive is protected from unauthorized access only if its authentication key ID is set to a non-default value. The manufacturer secure ID (MSID), which has key ID 0x0, is the standard default value for SAS drives. For NVMe drives, the standard default value is a null key, represented as a blank key ID. When you assign the key ID to a self-encrypting drive, the system changes its authentication key ID to a non-default value.

Steps

1. Assign a data authentication key to a FIPS drive or SED:

   `storage encryption disk modify -disk disk_ID -data-key-id key_ID`

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

   > ⓘ You can use the `security key-manager query -key-type NSE-AK` command to view key IDs.

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   000000000000000002000000000010019215b9738bc7b43d4698c80246db1f4

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

2. Verify that the authentication keys have 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
000000000000000002000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1   data
000000000000000002000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

Assign a FIPS 140-2 authentication key to a FIPS drive

You can use the `storage encryption disk modify` command with the `-fips-key-id` option to assign a FIPS 140-2 authentication key to a FIPS drive. Cluster nodes use this key for drive operations other than data access, such as preventing denial-of-service attacks on the drive.

What you'll need

The drive firmware must support FIPS 140-2 compliance. The NetApp Interoperability Matrix Tool contains information about supported drive firmware versions.

About this task

Your security setup may require you to use different keys for data authentication and FIPS 140-2 authentication. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

Steps

1. You must first ensure you have assigned a data authentication key. This can be done with using an external key manager or an onboard key manager. Verify the key is assigned with the command `storage encryption disk show`.
2. Assign a FIPS 140-2 authentication key to SEDs:

   `storage encryption disk modify -disk` *`disk_id`* `-fips-key-id` *`fips_authentication_key_id`*

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

   ```
   cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
   6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A

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

3. Verify that the authentication key has been assigned:

```
storage encryption disk show -fips
```

For complete command syntax, see the man page.

```
cluster1::> storage encryption disk show -fips
Disk    Mode FIPS-Compliance Key ID
------  ----
-------------------------------------------------------------------
2.10.0  full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
2.10.1  full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
[...]
```

Enable cluster-wide FIPS-compliant mode for KMIP server connections

You can use the `security config modify` command with the `-is-fips-enabled` option to enable cluster-wide FIPS-compliant mode for data in flight. Doing so forces the cluster to use OpenSSL in FIPS mode when connecting to KMIP servers.

Before you begin

- The storage controller must be configured in FIPS-compliant mode.
- All KMIP servers must support TLSv1.2. The system requires TLSv1.2 to complete the connection to the KMIP server when cluster-wide FIPS-compliant mode is enabled.

About this task

When you enable cluster-wide FIPS-compliant mode, the cluster will automatically use only TLS1.2 and FIPS-validated cipher suites. Cluster-wide FIPS-compliant mode is disabled by default.

You must reboot cluster nodes manually after modifying the cluster-wide security configuration.

ONTAP 9.11.1RC1 consideration

Due to a change in ONTAP version 9.11.1RC1, FIPS 140-2 compliance management mode no longer uses FIPS 140-2 validated software module.

ONTAP 9.11.1RC1 upgraded the OpenSSL version used for management and control plane connections for HTTPS. This version of OpenSSL (OpenSSL 3.x FIPS Provider) has not yet completed the FIPS 140-2 Cryptographic Module Validation Program (CMVP) validation process.

When FIPS compliance mode is enabled, encryption algorithms used for HTTPS connections are identical to the OpenSSL Project OpenSSL 3.x FIPS Provider algorithms that were issued in Cryptographic Algorithm Validation Program (CAVP) certificate A1938. **This change only affects ONTAP systems configured in FIPS compliance mode.**

This issue will be fixed once the upgraded OpenSSL module present in ONTAP 9.11.1RC1 completes FIPS 140-2 validation with NIST. If your environment requires ONTAP cluster management control plane run with a FIPS 140-2 CMVP validated module, then it is recommended to not upgrade to 9.11.1RC1.

This does not affect NetApp encryption at rest technologies like NSE, NVE, and NAE, as those features use a different cryptographic module than the one provided by OpenSSL in ONTAP.

For more information, see Upgrading to ONTAP 9.11.1RC1 results in FIPS 140-2 compliance management configuration that is not validated.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Verify that TLSv1.2 is supported:

   ```
   security config show -supported-protocols
   ```

   For complete command syntax, see the man page.

   ```
   cluster1::> security config show
             Cluster                                                 Cluster
   Security
   Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
   Ready
   --------- ---------- ----------------------- -----------------
   ----------------
   SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:         yes
                                                !aNULL:!EXP:
                                                !eNULL
   ```

3. Enable cluster-wide FIPS-compliant mode:

   ```
   security config modify -is-fips-enabled true -interface SSL
   ```

   For complete command syntax, see the man page.

4. Reboot cluster nodes manually.
5. Verify that cluster-wide FIPS-compliant mode is enabled:

   ```
   security config show
   ```

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       true       TLSv1.2, TLSv1.1        ALL:!LOW:         yes
                                              !aNULL:!EXP:
                                              !eNULL:!RC4
```

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. 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`

   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. This command requires advanced privileges. 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`

Securely purge data on an encrypted volume

Securely purge data on an encrypted volume overview

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 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.

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 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 with 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 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 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
   ```

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

Beginning with ONTAP 9.8, you can use a 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 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 Asynchronous SnapMirror relationship.

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

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

5. If the files you want to securely purge are in the base Snapshot copies, do the following:
   a. Create a Snapshot copy on the destination volume in the Asynchronous SnapMirror relationship:

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

   b. Update SnapMirror to move the base Snapshot copy 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 Snapshot copies plus one.

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

   d. Verify that the base Snapshot copy is present:

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

   e. Delete the base Snapshot copy:

      ```
      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 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
   ```

Scrub data on an encrypted volume with a Synchronous SnapMirror relationship

Beginning with ONTAP 9.8, you can use a 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

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.

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 Synchronous SnapMirror relationship.

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

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

5. If the secure purge file is in the base or common Snapshot copies, update the SnapMirror to move the common Snapshot copy forward:

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

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

6. If the secure purge file is in the application-consistent Snapshot copy, delete the Snapshot copy 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	`security key-manager onboard update-passphrase`
ONTAP 9.5 and earlier	`security key-manager update-passphrase`

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

For complete command syntax, see the man pages.

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

+

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

      -------------------------BEGIN BACKUP-------------------------
      TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAADuD+byAAAAACEAAAAAAAAA
      QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
      dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
      3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
      IgAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
      QRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
      BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
      AQAAAAMAAAAYAQAAAAAADA5/ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAA
      AAAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAACIAAAAAAAAA
      KAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
      AAAAAAAAAAAkAAAAAAAAAIAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
      LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
      1cNLLwAAAAiAAAAAAAAACgAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAIAAAAAAAkA
      ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAIgAAAAAAAAoAAAAAAAAJ4/cQsAAAAA
      AAAAAAAAAACAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAACQAAAAAAAA
      gAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
      rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      -------------------------END BACKUP-------------------------
```

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

Restore onboard key management encryption keys

If need to restore an onboard key management encryption key, you first verify that a key needs to be restored, then you can set up the Onboard Key Manager to restore the key.

Before you begin

- If you are using NSE with an external key management (KMIP) server, you must have deleted the external key manager database.

  Transitioning to onboard key management from external key management

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

Steps for ONTAP 9.6 and later

1. Verify that the key needs to be restored:
   `security key-manager key query -node node`
2. If you are running ONTAP 9.8 and later, and your root volume is encrypted, complete Steps if the root volume is encrypted.

   If you are running ONTAP 9.6 or 9.7, or if you are running ONTAP 9.8 or later and your root volume is not encrypted, skip this step.
3. Restore the key:
   `security key-manager onboard sync`

   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>
   ```
4. At the passphrase prompt, enter the onboard key management passphrase for the cluster.

Steps for ONTAP 9.5 and earlier

1. Verify that the key needs to be restored:
   `security key-manager key show`
2. If you are running ONTAP 9.8 and later, and your root volume is encrypted, complete these steps:

   If you are running ONTAP 9.6 or 9.7, or if you are running ONTAP 9.8 or later and your root volume is not encrypted, skip this step.
3. Restore the key:
   `security key-manager setup -node node`

   For complete command syntax, see the man pages.
4. At the passphrase prompt, enter the onboard key management passphrase for the cluster.

Steps if the root volume is encrypted

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.

   The node returns to the boot menu.

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

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	`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. 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.

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.

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 installed. See the Knowledge Base article The new client certificate public or private keys are different from the existing client certificate 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.

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.

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 -fields data-key-id,fips-key-id,owner`

   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
1.10.2  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

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. 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 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.

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`

   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
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

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 a 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

- 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>

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.

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.
include::../_include/unpartition-disk.adoc[]

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`*
	g. If the disk does not have an owner, assign one, then unfail the disk again:
	`storage disk assign -owner node -disk` *`disk_id`*
	`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. Unfail the sanitized disk: `storage disk unfail -spare true -disk` *`disk_id`* e. Check whether the disk has an owner: `storage disk show -disk` *`disk_id`* f. If the disk does not have an owner, assign one, then unfail the disk again: `storage disk assign -owner node -disk` *`disk_id`* `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`*

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.

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.

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.
```

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.

```
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.

Remove an external key manager connection

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.

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	`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`

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:

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

Modify 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.

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:

   ```
   clusterl::> 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:

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

For complete command syntax, see the ONTAP manual pages.

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.

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.

Procedure

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
   ```

ONTAP 9.5 and earlier

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

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.
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

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. You can disable encryption by default for the entire cluster, 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 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
```