Manage encryption with the CLI

ONTAP 9

NetApp
February 20, 2026

Table of Contents

Manage encryption with the CLI

Learn about ONTAP data at rest encryption

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 using NetApp Volume Encryption (NVE) supports data encryption one volume at a time
- Hardware-based encryption using NetApp Storage Encryption (NSE) supports full-disk encryption (FDE) of data as it is written.

Configure NetApp volume and aggregate encryption

Learn about ONTAP NetApp volume and aggregate encryption

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

With NVE, both metadata and data (including snapshots) 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 (OKM) 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. The VE license is included with ONTAP One. 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. Beginning with ONTAP 9.14.1, you can enable NVE on existing SVM root volumes.

> 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.

When NVE is enabled, 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 if 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 9.17.1, you can use Barbican KMS to protect NVE keys only for data SVMs.

- Beginning with ONTAP 9.10.1, you can use Azure Key Vault and Google Cloud KMS to protect NVE keys only for data SVMs. This is available for AWS's KMS beginning in 9.12.0.

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.

Cloud KMS providers such as Azure Key Vault and AWS KMS do not support KMIP. As a result, they are not listed on IMT.

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 Cloud Volumes ONTAP 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 SVM root volumes. You cannot encrypt data on MetroCluster metadata volumes. In versions of ONTAP earlier than 9.14.1, you cannot encrypt data on the SVM root volume with NVE. Beginning with ONTAP 9.14.1, ONTAP supports NVE on SVM root 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	MetroCluster is supported beginning with ONTAP 9.8. Beginning with ONTAP 9.6, NVE supports SVM scope for external key management only, not for Onboard Key Manager.
Storage efficiency	Deduplication, compression, compaction, FlexClone. Clones use the same key as the parent, even after splitting the clone from the parent. You should perform a `volume move` on a split clone, after which the split clone will have a different key.
Replication	• For volume replication, the source and destination volumes can have different encryption settings. Encryption can be configured for the source and unconfigured for the destination, and vice versa. Configured encryption on the source will not be replicated to the destination. Encryption must be configured manually on the source and destination. Refer to Configure NVE and Encrypt volume data with NVE. • 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	SnapLock is supported in both Compliance and Enterprise modes, for new volumes only. You cannot enable encryption on an existing SnapLock volume.
FlexGroup volumes	FlexGroup volumes 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.

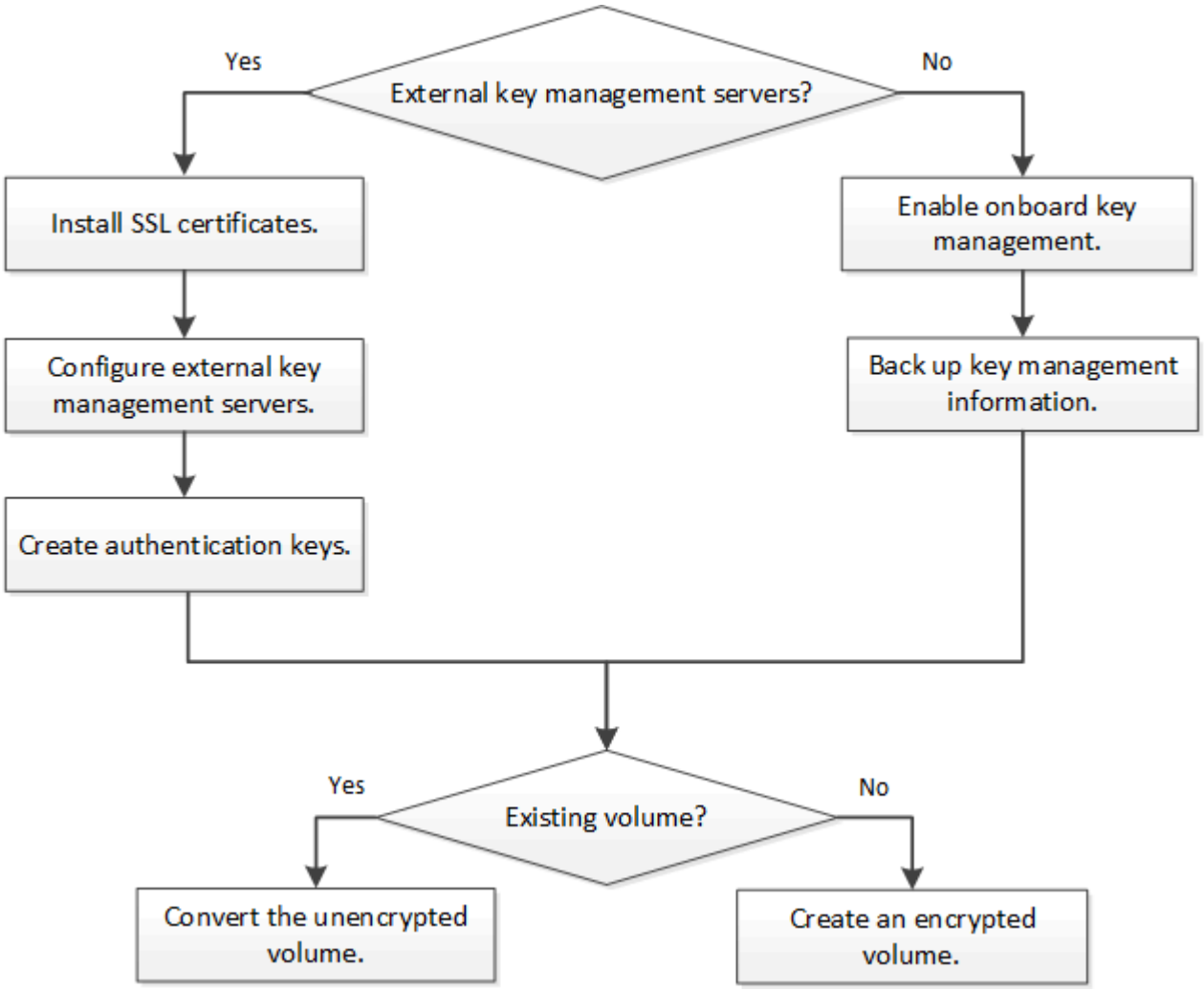
7-Mode transition	Beginning with 7-Mode Transition Tool 3.3, you can use the 7-Mode Transition Tool CLI to perform copy-based transition to NVE-enabled destination volumes on the clustered system.

Related information

- FAQ - NetApp Volume Encryption and NetApp Aggregate Encryption
- storage aggregate create

ONTAP 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 ONTAP 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.

Steps

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.

Install the volume encryption license on an ONTAP cluster

A VE license entitles you to use the feature on all nodes in the cluster. This license is required before you can encrypt data with NVE. It is included with ONTAP One.

Prior to ONTAP One, the VE license was included with the Encryption bundle. The Encryption bundle is no longer offered, but is still valid. Although not currently required, existing customers can choose to upgrade to ONTAP One.

Before you begin

- You must be a cluster administrator to perform this task.
- You must have received the VE license key from your sales representative or have ONTAP One installed.

Steps

1. Verify that the VE license is installed.

   The VE license package name is `VE`.

2. If the license is not installed, use System Manager or the ONTAP CLI to install it.

Configure external key management

Learn about configuring external key management with ONTAP NetApp Volume Encryption

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). In addition to the Onboard Key Manager, ONTAP supports several external key management servers.

Beginning with ONTAP 9.10.1, you can use Azure Key Vault or Google Cloud Key Manager Service to protect your NVE keys for data SVMs. Beginning with ONTAP 9.11.1, you can configure multiple external key managers in a cluster. See Configure clustered key servers. Beginning with ONTAP 9.12.0, you can use AWS' KMS to protect your NVE keys for data SVMs. Beginning with ONTAP 9.17.1, you can use OpenStack's Barbican KMS to protect your NVE keys for data SVMs.

Manage external key managers with ONTAP System Manager

Beginning with ONTAP 9.7, you can store and manage authentication and encryption keys with the Onboard Key Manager. Beginning with ONTAP 9.13.1, you can also use external key managers to store and manage these keys.

The Onboard Key Manager stores and manages keys in a secure database that is internal to the cluster. Its scope is the cluster. An external key manager stores and manages keys outside the cluster. Its scope can be the cluster or the storage VM. One or more external key managers can be used. The following conditions apply:

- If the Onboard Key Manager is enabled, an external key manager cannot be enabled at the cluster level, but it can be enabled at the storage VM level.
- If an external key manager is enabled at the cluster level, the Onboard Key Manager cannot be enabled.

When using external key managers, you can register up to four primary key servers per storage VM and cluster. Each primary key server can be clustered with up to three secondary key servers.

Configure an external key manager

To add an external key manager for a storage VM, you should add an optional gateway when you configure the network interface for the storage VM. If the storage VM was created without the network route, you will have to create the route explicitly for the external key manager. See Create a LIF (network interface).

Steps

You can configure an external key manager starting from different locations in System Manager.

1. To configure an external key manager, perform one of the following starting steps.

Workflow	Navigation	Starting step
Configure Key Manager	**Cluster** > **Settings**	Scroll to the **Security** section. Under **Encryption**, select ⚙. Select **External Key Manager**.
Add local tier	**Storage** > **Tiers**	Select **+ Add Local Tier**. Check the check box labeled "Configure Key Manager". Select **External Key Manager**.
Prepare storage	**Dashboard**	In the **Capacity** section, select **Prepare Storage**. Then, select "Configure Key Manager". Select **External Key Manager**.
Configure encryption (key manager at storage VM scope only)	**Storage** > **Storage VMs**	Select the storage VM. Select the **Settings** tab. In the **Encryption** section under **Security**, select ⚙.

2. To add a primary key server, select + Add , and complete the **IP Address or Host Name** and **Port** fields.
3. Existing installed certificates are listed in the **KMIP Server CA Certificates** and **KMIP Client Certificate** fields. You can perform any of the following actions:
   - Select ⌄ to select installed certificates that you want to map to the key manager. (Multiple service CA certificates can be selected, but only one client certificate can be selected.)

- Select **Add New Certificate** to add a certificate that has not already been installed and map it to the external key manager.
- Select ✕ next to the certificate name to delete installed certificates that you do not want to map to the external key manager.

4. To add a secondary key server, select **Add** in the **Secondary Key Servers** column, and provide its details.
5. Select **Save** to complete the configuration.

Edit an existing external key manager

If you have already configured an external key manager, you can modify its settings.

Steps

1. To edit the configuration of an external key manager, perform one of the following starting steps.

Scope	Navigation	Starting step
Cluster scope external key manager	**Cluster** > **Settings**	Scroll to the **Security** section. Under **Encryption**, select ⋮, then select **Edit External Key Manager**.
Storage VM scope external key manager	**Storage** > **Storage VMs**	Select the storage VM. Select the **Settings** tab. In the **Encryption** section under **Security**, select ⋮, then select **Edit External Key Manager**.

2. Existing key servers are listed in the **Key Servers** table. You can perform the following operations:
   - Add a new key server by selecting + Add .
   - Delete a key server by selecting ⋮ at the end of the table cell that contains the name of the key server. The secondary key servers associated with that primary key server are also removed from the configuration.

Delete an external key manager

An external key manager can be deleted if the volumes are unencrypted.

Steps

1. To delete an external key manager, perform one of the following steps.

Scope	Navigation	Starting step
Cluster scope external key manager	**Cluster** > **Settings**	Scroll to the **Security** section. Under **Encryption**, select select ⋮, then select **Delete External Key Manager**.
Storage VM scope external key manager	**Storage** > **Storage VMs**	Select the storage VM. Select the **Settings** tab. In the **Encryption** section under **Security**, select ⋮, then select **Delete External Key Manager**.

Migrate keys among key managers

When multiple key managers are enabled on a cluster, keys must be migrated from one key manager to another. This process is completed automatically with System Manager.

- If the Onboard Key Manager or an external key manager is enabled at a cluster level, and some volumes are encrypted, then when you configure an external key manager at the storage VM level, the keys must be migrated from the Onboard Key Manager or external key manager at the cluster level to the external key manager at the storage VM level. This process is completed automatically by System Manager.
- If volumes were created without encryption on a storage VM, then keys do not need to be migrated.

Install SSL certificates on the ONTAP 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.

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.

Before you begin

- 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.
- In a MetroCluster environment, you must install the same KMIP SSL certificates on both clusters.

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

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
   ```

Related information

- security certificate install

Enable external key management for NVE in ONTAP 9.6 and later

Use KMIP servers to secure the keys the cluster uses to access encrypted data. Beginning with ONTAP 9.6, you have the option to configure a separate external key manager to secure the keys that a data SVM uses to access encrypted data.

Beginning with 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.

About this task

You can connect up to four KMIP servers to a cluster or SVM. Use at least two servers 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>
  ```

  Learn more about `system license add` in the ONTAP command reference.

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.

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

Before you begin

- The KMIP SSL client and server certificates must have been installed.
- The KMIP server must be reachable from each node's node-management LIF.
- You must be a cluster or SVM administrator to perform this task.
- In a MetroCluster environment:
  - MetroCluster must be fully configured before enabling external key management.
  - You must install the same KMIP SSL certificate on both clusters.
  - An external key manager must be configured on both clusters.

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 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 can run the `security key-manager external modify` command to change the external key management configuration.
   > - In a MetroCluster environment, if you are configuring external key management for a data SVM, you do not have to repeat the `security key-manager external enable` command on the partner cluster.

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

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

```
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.
```

5. Optionally, convert plain text volumes to encrypted volumes.

   `volume encryption conversion start`

   An external key manager must be fully configured before you convert the volumes.

Related information

- Configure clustered external key servers
- system license add
- security key-manager key migrate

- security key-manager external add-servers
- security key-manager external show-status

Enable external key management for NVE 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.

About this task

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

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.
- In a MetroCluster environment, you must install the same KMIP SSL certificate on both clusters.

Steps

1. Configure key manager connectivity for cluster nodes:

   `security key-manager setup`

   The key manager setup starts.

   > In a MetroCluster environment, you must run this command on both clusters. Learn more about `security key-manager setup` in the ONTAP command reference.

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

   `security key-manager add -address key_management_server_ipaddress`

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

   > In a MetroCluster environment, you must run this command on both clusters.

4. Add an additional KMIP server for redundancy:

   `security key-manager add -address key_management_server_ipaddress`

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

   > In a MetroCluster environment, you must run this command on both clusters.

5. Verify that all configured KMIP servers are connected:

   ```
   security key-manager show -status
   ```

   Learn more about the commands described in this procedure in the ONTAP command reference.

   ```
   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
   ```

6. Optionally, convert plain text volumes to encrypted volumes.

   ```
   volume encryption conversion start
   ```

   An external key manager must be fully configured before you convert the volumes. In a MetroCluster environment, an external key manager must be configured on both sites.

Manage NVE keys for ONTAP data SVMs with a cloud provider

Beginning with 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 cloud-hosted application. Beginning with ONTAP 9.12.0, you can also protect NVE keys with AWS' KMS.

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

About this task

Key management with a cloud provider can be enabled with the CLI or the ONTAP REST API.

When using a cloud provider to protect your keys, 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 use the key management service.

When utilizing a cloud provider key management service, you should be aware of the following limitations:

- Cloud-provider key management is not available for NetApp Storage Encryption (NSE) and NetApp Aggregate Encryption (NAE). External KMIPs can be used instead.
- Cloud-provider key management is not available for MetroCluster configurations.
- Cloud-provider key management can only be configured on a data SVM.

Before you begin

- You must have configured the KMS on the appropriate cloud provider.
- The ONTAP cluster's nodes must support NVE.
- You must have installed the Volume Encryption (VE) and multi-tenant Encryption Key Management (MTEKM) licenses. These licenses are included with ONTAP One.
- You must be a cluster or SVM administrator.
- The data SVM must not include any encrypted volumes or employ a key manager. If the data SVM includes encrypted volumes, you must migrate them before configuring the KMS.

Enable external key management

Enabling external key management depends on the specific key manager you use. Choose the tab of the appropriate key manager and environment.

AWS

Before you begin

- You must create a grant for the AWS KMS key that will be used by the IAM role managing encryption. The IAM role must include a policy that allows the following operations:
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt`
    +
    For more information, see AWS documentation for grants.

Enable AWS KMV on an ONTAP SVM

1. Before you begin, obtain both the access key ID and secret key from your AWS KMS.
2. Set the privilege level to advanced:
   `set -priv advanced`
3. Enable AWS KMS:
   `security key-manager external aws enable -vserver` *`svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. When prompted, enter the secret key.
5. Confirm the AWS KMS was configured correctly:
   `security key-manager external aws show -vserver` *`svm_name`*

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

Azure

Enable Azure Key Vault on an ONTAP SVM

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`. Learn more about `cluster show` in the ONTAP command reference.
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 the data SVM LIF.

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

Google Cloud

Enable Cloud KMS on an ONTAP SVM

1. Before you begin, 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`. Learn more about `cluster show` in the ONTAP command reference.
2. Set privileged level to advanced:
   `set -priv advanced`
3. Enable Cloud KMS on the SVM
   `security key-manager external gcp enable -vserver 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.

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

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 SVM until all NVE keys of the data SVM are successfully migrated.

Related information

- Encrypting volumes with NetApp encryption solutions for Cloud Volumes ONTAP
- security key-manager external

Manage ONTAP keys with Barbican KMS

Beginning with ONTAP 9.17.1, you can use OpenStack's Barbican KMS to protect ONTAP encryption keys. Barbican KMS is a service for securely storing and accessing keys. Barbican KMS can be used to protect NetApp Volume Encryption (NVE) keys for data SVMs. Barbican relies on OpenStack Keystone, OpenStack's identity service, for authentication.

About this task

You can configure key management with Barbican KMS with the CLI or the ONTAP REST API. With the 9.17.1 release, Barbican KMS support has the following limitations:

- Barbican KMS is not supported for NetApp Storage Encryption (NSE) and NetApp Aggregate Encryption (NAE). Alternatively, you can use external KMIPs or the Onboard Key Manager (OKM) for NSE and NVE keys.
- Barbican KMS is not supported for MetroCluster configurations.
- Barbican KMS can only be configured for a data SVM. It is not available for the admin SVM.

Unless otherwise noted, administrators at the `admin` privilege level can perform the following procedures.

Before you begin

- Barbican KMS and OpenStack Keystone must be configured. The SVM you are using with Barbican must have network access to the Barbican and OpenStack Keystone servers.
- If you are using a custom Certificate Authority (CA) for the Barbican and OpenStack Keystone servers, you must install the CA certificate with `security certificate install -type server-ca -vserver <admin_svm>`.

Create and activate a Barbican KMS configuration

You can create a new Barbican KMS configuration for an SVM and activate it. An SVM can have multiple inactive Barbican KMS configurations, but only one can be active at a time.

Steps

1. Create a new inactive Barbican KMS configuration for an SVM:

```
security key-manager external barbican create-config -vserver <svm_name>
-config-name <unique_config_name> -key-id <key_id> -keystone-url
<keystone_url> -application-cred-id
<keystone_applications_credentials_id>
```

   - `-key-id` is the key identifier of the Barbican key encryption key (KEK). Enter a full URL, including `https://`.

     Some URLs include the question mark (?) character. The question mark activates the ONTAP command line active help. In order to enter a URL with a question mark, you need to first disable active help with the command `set -active-help false`. Active help can later be re-enabled with the command `set -active-help true`. Learn more in the ONTAP command reference.

   - `-keystone-url` is the URL of the OpenStack Keystone authorization host. Enter a full URL, including `https://`.
   - `-application-cred-id` is the application credentials ID.

     After entering this command, you will be prompted for the application credentials secret key. This command creates an inactive Barbican KMS configuration.

     The following example creates a new inactive Barbican KMS configuration named `config1` for the SVM `svm1`:

```
cluster1::> security key-manager external barbican create-config
-vserver svm1 -config-name config1 -keystone-url
https://172.21.76.152:5000/v3 -application-cred-id app123 -key-id
https://172.21.76.153:9311/v1/secrets/<id_value>

Enter the Application Credentials Secret for authentication with
Keystone: <key_value>
```

2. Activate the new Barbican KMS configuration:

```
security key-manager keystore enable -vserver <svm_name> -config-name
<unique_config_name> -keystore barbican
```

You can use this command to switch between Barbican KMS configurations. If there is already an active Barbican KMS configuration on the SVM, it will be made inactive and the new configuration will be activated.

3. Verify that the new Barbican KMS configuration is active:

```
security key-manager external barbican check -vserver <svm_name> -node
<node_name>
```

This command will provide the status of the active Barbican KMS configuration on the SVM or node. For example, if the SVM `svm1` on node `node1` has an active Barbican KMS configuration, the following command will return the status of that configuration:

```
cluster1::> security key-manager external barbican check -node node1

Vserver: svm1
Node: node1

Category: service_reachability
              Status: OK

Category: kms_wrapped_key_status
              Status: OK
```

Update the credentials and settings of a Barbican KMS configuration

You can view and update the current settings of an active or inactive Barbican KMS configuration.

Steps

1. View the current Barbican KMS configurations for an SVM:

```
security key-manager external barbican show -vserver <svm_name>
```

The key ID, OpenStack Keystone URL, and application credentials ID are displayed for each Barbican KMS configuration on the SVM.

2. Update the settings of a Barbican KMS configuration:

```
security key-manager external barbican update-config -vserver <svm_name>
-config-name <unique_config_name> -timeout <timeout> -verify
<true|false> -verify-host <true|false>
```

This command updates the timeout and verification settings of the specified Barbican KMS configuration. `timeout` determines the time in seconds ONTAP will wait for Barbican to respond before the connection fails. The default `timeout` is ten seconds. `verify` and `verify-host` determine if the identity and hostname respectively of Barbican host should be verified before connecting. By default, these parameters are set to `true`. The `vserver` and `config-name` parameters are required. The other parameters are optional.

3. If needed, update the credentials of an active or inactive Barbican KMS configuration:

```
security key-manager external barbican update-credentials -vserver
<svm_name> -config-name <unique_config_name> -application-cred-id
<keystone_applications_credentials_id>
```

After entering this command, you will be prompted for the new application credentials secret key.

4. If needed, restore a missing SVM key encryption key (KEK) for an active Barbican KMS configuration:
   a. Restore a missing SVM KEK with `security key-manager external barbican restore`:

```
security key-manager external barbican restore -vserver <svm_name>
```

This command will restore the SVM KEK for the active Barbican KMS configuration by communicating with the Barbican server.

5. If needed, rekey the SVM KEK for a Barbican KMS configuration:
   a. Set the privilege level to advanced:

```
set -privilege advanced
```

   b. Rekey the SVM KEK with `security key-manager external barbican rekey-internal`:

```
security key-manager external barbican rekey-internal -vserver
<svm_name>
```

This command generates a new SVM KEK for the specified SVM and re-wraps the volume encryption keys with the new SVM KEK. The new SVM KEK will be protected by the active Barbican KMS configuration.

Migrate keys between Barbican KMS and the Onboard Key Manager

You can migrate keys from Barbican KMS to the Onboard Key Manager (OKM), and vice-versa. To learn more about the OKM, refer to Enable onboard key management in ONTAP 9.6 and later.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. If needed, migrate keys from Barbican KMS to the OKM:

```
security key-manager key migrate -from-vserver <svm_name> -to-vserver
<admin_svm_name>
```

`svm_name` is the name of the SVM with the Barbican KMS configuration.

3. If needed, migrate keys from the OKM to Barbican KMS:

```
security key-manager key migrate -from-vserver <admin_svm_name> -to
-vserver <svm_name>
```

Disable and delete a Barbican KMS configuration

You can disable an active Barbican KMS configuration with no encrypted volumes, and you can delete an inactive Barbican KMS configuration.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Disable an active Barbican KMS configuration:

```
security key-manager keystore disable -vserver <svm_name>
```

If NVE encrypted volumes exist on the SVM, you must decrypt them or migrate the keys before disabling the Barbican KMS configuration. Activating a new Barbican KMS configuration does not require decrypting NVE volumes or migrating keys, and will disable the current active Barbican KMS configuration.

3. Delete an inactive Barbican KMS configuration:

```
security key-manager keystore delete -vserver <svm_name> -config-name
<unique_config_name> -type barbican
```

Enable onboard key management for NVE in ONTAP 9.6 and later

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

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 the `security key-manager onboard enable` command on the local cluster first, then run the `security key-manager onboard sync` command on the remote cluster, using the same passphrase on each. When you run the `security key-manager onboard enable` command from the local cluster and then synchronize on the remote cluster, you do not need to run the `enable` command again from the remote cluster.

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

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. See CSfC Solution Brief.

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 cluster passphrase 5 times, wait 24 hours or reboot the node 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 system proceeds to the next step in the image update process if validation succeeds; otherwise, it fails the image update. Learn more about `cluster image` in the ONTAP command reference.

The Onboard Key Manager stores keys in volatile memory. Volatile memory contents are cleared when the system is rebooted or halted. The system clears volatile memory within 30 seconds when it is halted.

Before you begin

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

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.

2. 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.

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

5. Optionally, you can convert plain text volumes to encrypted volumes.

   `volume encryption conversion start`

   The Onboard Key Manager must be fully configured before you convert the volumes. In a MetroCluster environment, the Onboard Key Manager must be configured on both sites.

After you finish

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

After configuring the Onboard Key Manager passphrase, manually back up the information to a secure location outside the storage system. See Back up onboard key management information manually.

Related information

- cluster image commands
- security key-manager external enable
- security key-manager key query
- security key-manager onboard enable

Enable onboard key management for NVE in ONTAP 9.5 and earlier

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.

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.

Before you begin

- If you use NSE or NVE with an external key management (KMIP) server, delete the external key manager database.

  Transitioning to onboard key management from external key management

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

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 show-key-store`

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

Node: node1
Key Store: onboard
Key ID                                                               Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                                               Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK
```

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

6. Optionally, convert plain text volumes to encrypted volumes.

   `volume encryption conversion start`

   Configure the Onboard Key Manager before converting volumes. In MetroCluster environments, configure it on both sites.

After you finish

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

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

Related information

- Back up onboard key management information manually
- Transitioning to onboard key management from external key management
- security key-manager show-key-store

Enable onboard key management in newly added ONTAP 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 9.6 and later, you must run the `security key-manager onboard sync` command each time you add a node to the cluster.

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

If you add a node to a cluster with onboard key management, run this command to refresh 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.

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

- 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`.

If the passphrase attempt fails, reboot the node. After the reboot, you can try entering the passphrase again.

Related information

- cluster image commands
- security key-manager external enable
- security key-manager onboard enable

Encrypt volume data with NVE or NAE

Learn about encrypting ONTAP volume data with NVE

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 in ONTAP

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.

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). All volumes in an NAE aggregate must be encrypted with NAE or NVE encryption. With aggregate-level encryption, volumes you create in the aggregate are encrypted with NAE encryption by default. You can override the default to use NVE encryption instead.

Plain text volumes are not supported in NAE aggregates.

Before you begin

You must be a cluster administrator to perform this task.

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`

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

   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
```

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

2. Verify that the aggregate is enabled for encryption:

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

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.
```

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

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 in ONTAP

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

About this task

You can encrypt volumes using NetApp Volume Encryption (NVE) and, beginning with ONTAP 9.6, NetApp Aggregate Encryption (NAE). To learn more about NAE and NVE, refer to the volume encryption overview.

Learn more about the commands described in this procedure in the ONTAP command reference.

The procedure to enable encryption on a new volume in ONTAP varies based on the version of ONTAP you are using and your specific configuration:

- 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`.
- In ONTAP 9.6 and earlier releases, you must use `-encrypt true` with `volume create` commands to enable encryption (provided you did not enable `cc-mode`).
- If you want to create an NAE volume in ONTAP 9.6, you must enable NAE at the aggregate level. Refer to

Enable aggregate-level encryption with the VE license for more details on this task.

- Beginning with ONTAP 9.7, newly created volumes are encrypted by default when you have the VE license and onboard or external key management. By default, new volumes created in an NAE aggregate will be of type NAE rather than NVE.
  - In ONTAP 9.7 and later releases, if you add `-encrypt true` to the `volume create` command to create a volume in an NAE aggregate, the volume will have NVE encryption instead of NAE. All volumes in an NAE aggregate must be encrypted with either NVE or NAE.

Plaintext volumes are not supported in NAE aggregates.

Steps

1. Create a new volume and specify whether encryption is enabled on the volume. If the new volume is in an NAE aggregate, by default the volume will be an NAE volume:

To create…	Use this command…
An NAE volume	`volume create -vserver` *SVM_name* `-volume` *volume_name* `-aggregate` *aggregate_name*
An NVE volume	`volume create -vserver` *SVM_name* `-volume` *volume_name* `-aggregate` *aggregate_name* `-encrypt true` + In ONTAP 9.6 and earlier where NAE is not supported, `-encrypt true` specifies that the volume should be encrypted with NVE. In ONTAP 9.7 and later where volumes are created in NAE aggregates, `-encrypt true` overrides the default encryption type of NAE to create an NVE volume instead.
A plain text volume	`volume create -vserver` *SVM_name* `-volume` *volume_name* `-aggregate` *aggregate_name* `-encrypt false`

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

2. Verify that volumes are enabled for encryption:

   ```
   volume show -is-encrypted true
   ```

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

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 NAE or NVE on an existing ONTAP volume

You can use either the `volume move start` or the `volume encryption conversion start` command to enable encryption on an existing volume.

About this task

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. Alternatively, you can use the `volume move start` command.

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

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.

After you start a conversion operation, it must be completed. 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`

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

   The following command enables encryption on 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`

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

   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 completed, verify that the volume is enabled for encryption:

   `volume show -is-encrypted true`

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

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

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

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

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 can use the same aggregate or a different aggregate.

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* (meaning it uses NetApp Volume Encryption). 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.
- Beginning with ONTAP 9.14.1, you can encrypt an SVM root volume with NVE. For more information, see Configure NetApp Volume Encryption on an SVM root volume.

Before you begin

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

Delegating authority to run the volume move command

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`

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

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.

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

   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`

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

   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.

Configure NVE on an ONTAP SVM root volume

Beginning with ONTAP 9.14.1, you can enable NetApp Volume Encryption (NVE) on a storage VM (SVM) root volume. With NVE, the root volume is encrypted with a unique key, enabling greater security on the SVM.

About this task

NVE on an SVM root volume can only be enabled after the SVM has been created.

Before you begin

- The SVM root volume must not be on an aggregate encrypted with NetApp Aggregate Encryption (NAE).
- You must have enabled encryption with the Onboard Key Manager or an external key manager.
- You must be running ONTAP 9.14.1 or later.
- To migrate an SVM containing a root volume encrypted with NVE, you must convert the SVM root volume to a plain text volume after the migration completes then re-encrypt the SVM root volume.
  - If the destination aggregate of the SVM migration uses NAE, the root volume inherits NAE by default.
- If the SVM is in an SVM disaster recovery relationship:
  - Encryption settings on a mirrored SVM are not copied to the destination. If you enable NVE on the source or destination, you must separately enable NVE on the mirrored SVM root volume.
  - If all aggregates in the destination cluster use NAE, the SVM root volume will use NAE.

Steps

You can enable NVE on an SVM root volume with the ONTAP CLI or System Manager.

CLI

You can enable NVE on the SVM root volume in-place or by moving the volume between aggregates.

Encrypt the root volume in place

1. Convert the root volume to an encrypted volume:

   ```
   volume encryption conversion start -vserver svm_name -volume volume
   ```

2. Confirm the encryption succeeded. The `volume show -encryption-type volume` displays a list of all volumes using NVE.

Encrypt the SVM root volume by moving it

1. Initiate a volume move:

   ```
   volume move start -vserver svm_name -volume volume -destination-aggregate
   aggregate -encrypt-with-aggr-key false -encrypt-destination true
   ```

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

2. Confirm the `volume move` operation succeeded with the `volume move show` command. The `volume show -encryption-type volume` displays a list of all volumes using NVE.

System Manager

1. Navigate to **Storage** > **Volumes**.
2. Next to the name of the SVM root volume you want to encrypt, select ⋮ then **Edit**.
3. Under the **Storage and Optimization** heading, select **Enable encryption**.
4. Select **Save**.

Configure NVE on an ONTAP node root volume

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

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 and, beginning with ONTAP 9.14.1, NVE.

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.

Before you begin

- Your system must be using an HA configuration.
- 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).

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

Learn about ONTAP hardware-based encryption

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.

When self-encrypting drives are enabled, 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 self-encrypting drive types

Two types of self-encrypting drives 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-encrypting drives on the same node or HA pair.
- All FIPS validated drives use a firmware cryptographic module that has been through FIPS validation. The FIPS drive cryptographic module does not use any keys that are generated outside of the drive (the authentication passphrase that is input to the drive is used by the drive’s firmware cryptographic module to obtain a key encryption key).

Non-encrypting drives are drives that are not SEDs or FIPS drives.

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

When to use external key management

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

- Your organization’s policy requires a key management solution that uses a FIPS 140-2 Level 2 (or higher) cryptographic module.
- 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.

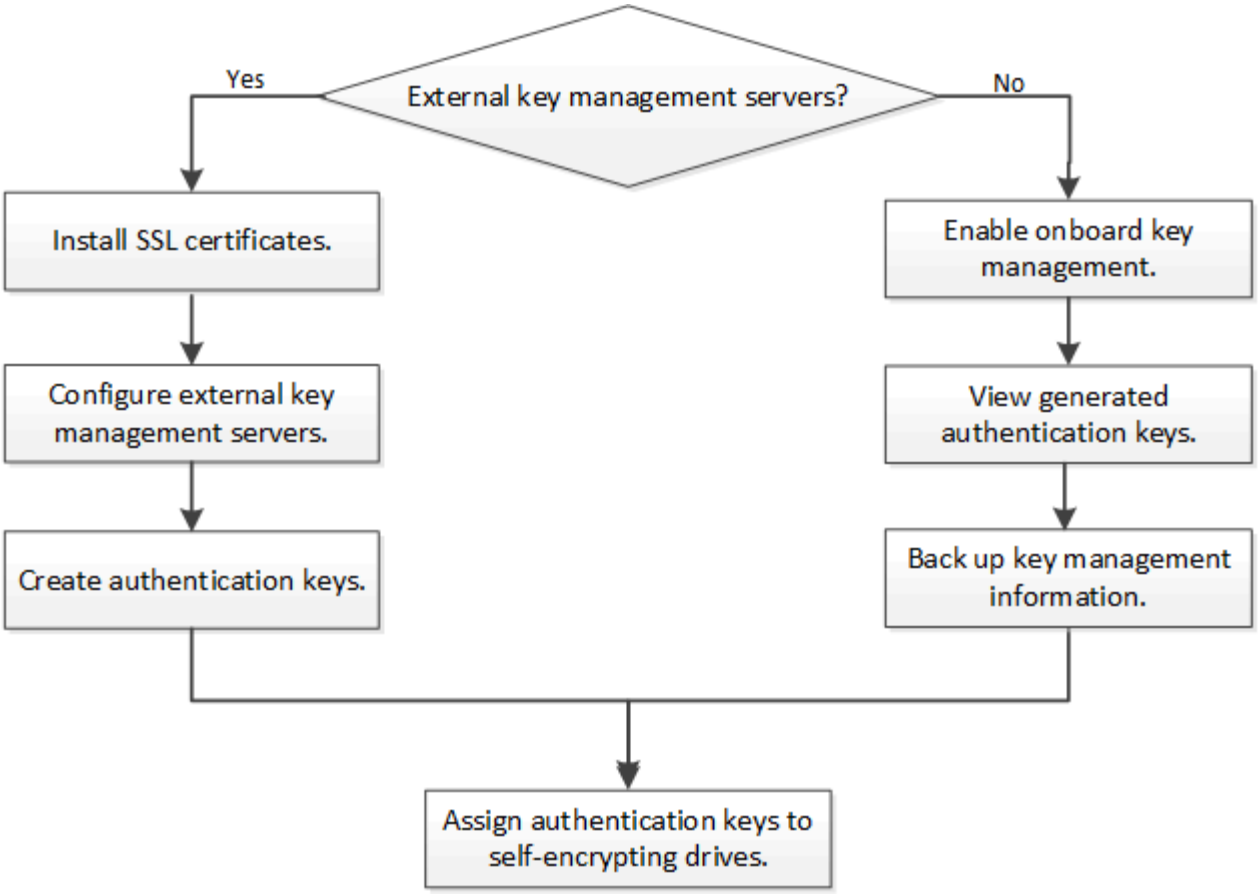
Support details

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-encrypting drives 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.

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.



Related information

- NetApp Hardware Universe
- NetApp Volume Encryption and NetApp Aggregate Encryption

Configure external key management

Learn about configuring ONTAP external key management

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).

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

Install SSL certificates on the ONTAP 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.

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.

Before you begin

- 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.
- In a MetroCluster environment, you must install the same KMIP SSL certificates on both clusters.

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

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
   ```

Related information

- security certificate install

Enable external key management for hardware-based encryption in ONTAP 9.6 and later

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 with 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.
- In a MetroCluster environment:
  - You must configure the MetroCluster environment before you configure an external key manager.

- You must install the same KMIP SSL certificate on both clusters.

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. Learn more about `security key-manager external enable` in the ONTAP command reference.
   - In a MetroCluster environment, if you are configuring external key management for the admin SVM, you must repeat the `security key-manager external enable` command on the partner cluster.

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

```
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.
```

Related information

- Configure clustered external key servers
- security-key-manager-external-enable
- security-key-manager-external-show-status

Enable external key management for hardware-based encryption 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.

About this task

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

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.
- In a MetroCluster environment, you must install the same KMIP SSL certificate on both clusters.

Steps

1. Configure key manager connectivity for cluster nodes:

   ```
   security key-manager setup
   ```

   The key manager setup starts.

In a MetroCluster environment, you must run this command on both clusters. Learn more about `security key-manager setup` in the ONTAP command reference.

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
   ```

   In a MetroCluster environment, you must run this command on both clusters.

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
   ```

   In a MetroCluster environment, you must run this command on both clusters.

5. Verify that all configured KMIP servers are connected:

   `security key-manager show -status`

   Learn more about the commands described in this procedure in the ONTAP command reference.

   ```
   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
   ```

6. Optionally, convert plain text volumes to encrypted volumes.

   `volume encryption conversion start`

   An external key manager must be fully configured before you convert the volumes. In a MetroCluster environment, an external key manager must be configured on both sites.

Configure clustered external key servers in ONTAP

Beginning with 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 an SVM. When registering or retrieving keys, ONTAP first attempts to access the primary key server before sequentially attempting to access secondary servers until the operation completes successfully.

You can use external key servers for NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE), and NetApp Aggregate Encryption (NAE) keys. An SVM can support up to four primary external KMIP servers. Each primary server can support up to three secondary key servers.

About this task

- This process only supports key servers that use KMIP. For a list of supported key servers, check the NetApp Interoperability Matrix Tool.

Before you begin

- KMIP key management must be enabled for the SVM.
- All nodes in the cluster must be running ONTAP 9.11.1 or later.
- The order of servers listed 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

Steps

1. Confirm that no key management has been enabled for the cluster (admin SVM):

   ```
   security key-manager external show -vserver <svm_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 <svm_name> -key-servers
   <primary_key_server_ip> -client-cert <client_cert_name> -server-ca-certs
   <server_ca_cert_names>
   ```

   - If you don't specify a port in the `-key-servers` parameter, the default port 5696 is used.

   > If you are running the `security key-manager external enable` command for the admin SVM in a MetroCluster configuration, you must run the command on both clusters. If you are running the command for an individual data SVM, you don't need to run the command on both clusters. NetApp strongly recommends using the same key servers on both clusters.

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 <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

   - Do not include a port number for secondary key servers in the `-secondary-key-servers` parameter. It uses the same port number as the primary key server.

   > If you are running the `security key-manager external` command for the admin SVM in a MetroCluster configuration, you must run the command on both clusters. If you are running the command for an individual data SVM, you don't need to run the command on both clusters. NetApp strongly recommends using the same key servers on both clusters.

Add secondary key servers to an existing primary key server

Steps

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 <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

   - Do not include a port number for secondary key servers in the `-secondary-key-servers` parameter. It uses the same port number as the primary key servers.

If you are running the `security key-manager external modify-server` command for the admin SVM in a MetroCluster configuration, you must run the command on both clusters. If you are running the command for an individual data SVM, you don't need to run the command on both clusters. NetApp strongly recommends using the same key servers on both clusters.

For more information about secondary key servers, see Modify secondary key servers.

Modify clustered key servers

You can modify clustered external key servers by adding and removing secondary key servers, changing the access order of secondary key servers, or by changing the designation (primary or secondary) of particular key servers. If you modify clustered external key servers in a MetroCluster configuration, NetApp strongly recommends using the same key servers on both clusters.

Modify secondary key servers

Use the `-secondary-key-servers` parameter of the `security key-manager external modify-server` command to manage secondary key servers . 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. You can modify the access order by running the command `security key-manager external modify-server` with the secondary key servers entered in a different sequence. Do not include a port number for secondary key servers.

If you are running the `security key-manager external modify-server` command for the admin SVM in a MetroCluster configuration, you must run the command on both clusters. If you are running the command for an individual data SVM, you don't need to run the command on both clusters.

To remove a secondary key server, include the key servers you want to keep in the `-secondary-key -servers` parameter and omit the one you want to remove. To remove all secondary key servers, use the argument `-`, signifying none.

Convert primary and secondary key servers

You can use the following steps to change the designation (primary or secondary) of particular key servers.

Convert a primary key server into a secondary key server

Steps

1. Remove the primary key server from the SVM:

   `security key-manager external remove-servers`

   > If you are running the `security key-manager external remove-servers` command for the admin SVM in a MetroCluster configuration, you must run the command on both clusters. If you are running the command for an individual data SVM, you don't need to run the command on both clusters.

2. Perform the Create a clustered key server procedure using the former primary key server as a secondary key server.

Convert a secondary key server into a primary key server

Steps

1. Remove the secondary key server from its existing primary key server:

   `security key-manager external modify-server -secondary-key-servers`

   > - If you are running the `security key-manager external modify-server -secondary-key-servers` command for the admin SVM in a MetroCluster configuration, you must run the command on both clusters. If you are running the command for an individual data SVM, you don't need to run the command on both clusters.
   > - If you convert a secondary key server to a primary key server while removing an existing key server, attempting to add a new key server before completing the removal and conversion can result in the the duplication of keys.

2. Perform the Create a clustered key server procedure using the former secondary key server as the primary key server of the new clustered key server.

Refer to Modify secondary key servers for more information.

Related information

- Learn more about `security key-manager external` 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.

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's 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.)

> In a MetroCluster environment, before you delete a key, you must make sure that the key is not in use on the partner cluster. You can use the following commands on the partner cluster to check that the key is not in use:
>
> - `storage encryption disk show -data-key-id <key-id>`
> - `storage encryption disk show -fips-key-id <key-id>`

Before you begin

You must be a cluster administrator to perform this task.

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

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

```
cluster1::> security key-manager key create
Key ID: <id_value>
```

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.
>
> 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: <id_value>
node1                                    NSE-AK    yes
    Key ID: <id_value>

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID: <id_value>
node2                                    NSE-AK    yes
    Key ID: <id_value>
```

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

Related information

- storage encryption disk show

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.

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.

Before you begin

You must be a cluster administrator to perform this task.

Steps

1. Create the authentication keys for cluster nodes:

   `security key-manager create-key`

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

   > 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: <id_value>

   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`

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

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: <id_value>


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

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-02     NSE-AK    yes
       Key ID: <id_value>
```

Assign a data authentication key to a FIPS drive or SED with ONTAP 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.

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.

This procedure is not disruptive.

Before you begin

You must be a cluster administrator to perform this task.

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`

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

> 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
<id_value>

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`

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

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

Related information

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

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.

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.

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

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. If validation works, the image update goes to the next step. If validation does not work, the image update fails. Learn more about `cluster image` in the ONTAP command reference.

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.

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.
- You must configure the MetroCluster environment before you configure the Onboard Key Manager.

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:

2. 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 system creates the authentication keys:

```
security key-manager key query -node node
```

> The `security key-manager key query` command replaces the `security key-manager query key` command.

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

After you finish

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

The system automatically backs up key management information to the replicated database (RDB) for the cluster. You should also back up this information manually for disaster recovery.

Related information

- cluster image commands
- security key-manager external enable
- security key-manager key query
- security key-manager onboard enable
- Transitioning to onboard key management from external key management

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. Enable Onboard Key Manager on each cluster that accesses encrypted volumes or self-encrypting disks.

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.

Before you begin

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

  Transitioning to onboard key management from external key management

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

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 show-key-store`

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

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

Node: node1
Key Store: onboard
Key ID                                                               Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                                               Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK
```

After you finish

ONTAP automatically backs up key management information to the replicated database (RDB) for the cluster.

After you configure the Onboard Key Manager passphrase, manually back up the information to a secure location outside the storage system. See Back up onboard key management information manually.

Related information

- Back up onboard key management information manually
- security key-manager setup
- security key-manager show-key-store
- Transitioning to onboard key management from external key management

Assign a data authentication key to a FIPS drive or SED with ONTAP 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.

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.

Before you begin

You must be a cluster administrator to perform this task.

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`*

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

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

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

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

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

2. Verify that the authentication keys have been assigned:

```
storage encryption disk show
```

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

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

Related information

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

Assign a FIPS 140-2 authentication key to an ONTAP 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.

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.

This procedure is not disruptive.

Before you begin

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

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
<id_value>

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`

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

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

Related information

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

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

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.

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.

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.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Verify that TLSv1.2 is supported:

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

   Learn more about `security config show` in the ONTAP command reference.

   ```
   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
   ```

   Learn more about `security config modify` in the ONTAP command reference.

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 in ONTAP

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

Before you begin

You must be a cluster administrator to perform this task.

Steps

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

   `volume move start -vserver` *`SVM_name`* `-volume volume_name -destination-aggregate` *`aggregate_name`* `-encrypt-destination false`

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

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

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

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

2. Verify that the volume is disabled for encryption:

   `volume show -encryption`

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

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

   ```
   cluster1::> volume show -encryption

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

Move an encrypted volume in ONTAP

You can use the `volume move start` command to move an encrypted volume. The moved volume can reside on the same aggregate or a different aggregate.

About this task

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

The `-encrypt-destination` option for `volume move start` defaults to true for encrypted volumes. The requirement to specify you do not want the destination volume encrypted ensures that you do not inadvertently

unencrypt the data on the volume.

Before you begin

You must be a cluster administrator to perform this task.

Steps

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

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

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

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

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

2. Verify that the volume is enabled for encryption:

   `volume show -is-encrypted true`

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

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

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

   Vserver  Volume  Aggregate  State  Type  Size  Available  Used
   -------  ------  ---------  -----  ----  -----  ---------  ----
   vs1      vol1    aggr3     online    RW  200GB    160.0GB  20%
   ```

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

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

About this task

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

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

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

Steps

1. Change an encryption key:

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

   The following command changes the encryption key for `vol1` on SVM`vs1`:

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

2. Verify the status of the rekey operation:

   `volume encryption rekey show`

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

   The following command displays the status of the rekey operation:

   ```
   cluster1::> volume encryption rekey show

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

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

   `volume show -is-encrypted true`

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

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

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

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

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

It is a security best practice to change the encryption key for a volume periodically. You can use the `volume move start` command to change the encryption key. The moved volume can reside on the same aggregate or a different aggregate.

About this task

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

Before you begin

You must be a cluster administrator to perform this task.

Steps

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

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

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

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

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

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

2. Verify that the volume is enabled for encryption:

   `volume show -is-encrypted true`

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

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

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

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

Rotate authentication keys for ONTAP NetApp Storage Encryption

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

About this task

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

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

Steps

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

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

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

Related information

- storage encryption disk modify

Delete an encrypted volume in ONTAP

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

Before you begin

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

Step

1. Delete an encrypted volume:

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

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

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

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

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

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

   Use `volume delete` with the `-force true` option to delete a volume and destroy the corresponding encryption key immediately. This command requires advanced privileges.
   Learn more about `volume delete` in the ONTAP command reference.

After you finish

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

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

How to use the Volume Recovery feature

Securely purge data on an encrypted volume

Learn about securely purging data from an encrypted ONTAP volume

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

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

Considerations for using secure purge

- Volumes created in an aggregate enabled for NetApp Aggregate Encryption (NAE) do not support secure purge.
- Secure purge works only for previously deleted files on NVE-enabled volumes.
- You cannot scrub an unencrypted volume.
- You must use KMIP servers to serve keys, not the onboard key manager.

Secure purge functions differently depending upon your version of ONTAP.

ONTAP 9.8 and later

- Secure purge is supported by MetroCluster and FlexGroup.
- If the volume being purged is the source of a SnapMirror relationship, you do not have to break the SnapMirror relationship to perform a secure purge.
- The re-encryption method is different for volumes using SnapMirror data protection versus volumes not using SnapMirror data protection (DP) or those using SnapMirror extended data protection..
  - By default, volumes using SnapMirror data protection (DP) mode re-encrypt data using the volume move re-encryption method.
  - By default, volumes not using SnapMirror data protection or volumes using SnapMirror extended data protection (XDP) mode use the in-place re-encryption method.
  - These defaults can be changed using the `secure purge re-encryption-method [volume-move|in-place-rekey]` command.
- By default, all snapshots in FlexVol volumes are automatically deleted during the secure purge operation. By default, Snapshots in FlexGroup volumes and volumes using SnapMirror data protection are not automatically deleted during the secure purge operation. These defaults can be changed using the `secure purge delete-all-snapshots [true|false]` command.

ONTAP 9.7 and earlier:

- Secure purge does not support the following:
  - FlexClone
  - SnapVault
  - FabricPool
- If the volume being purged is the source of a SnapMirror relationship, you must break the SnapMirror relationship before you can purge the volume.

  If there are busy snapshots in the volume, you must release the snapshots before you can purge the volume. For example, you may need to split a FlexClone volume from its parent.
- Successfully invoking the secure-purge feature triggers a volume move that re-encrypts the remaining, unpurged data with a new key.

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

Scrub data from an encrypted ONTAP volume without a SnapMirror relationship

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

About this task

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

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

Before you begin

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

Steps

1. Delete the files or the LUN you want to securely purge.
   - On a NAS client, delete the files you want to securely purge.
   - On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want to purge.
2. On the storage system, change to advanced privilege level:

   `set -privilege advanced`

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

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

4. Securely purge the deleted files:

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

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

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

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

   `volume encryption secure-purge show`

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

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

Before you begin

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

About this task

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

of the operation. You can use the `volume encryption secure-purge abort` command to terminate the operation.

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

Steps

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

   ```
   set -privilege advanced
   ```

2. Delete the files or the LUN you want to securely purge.
   - On a NAS client, delete the files you want to securely purge.
   - On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want to purge.
3. Prepare the destination volume in the Asynchronous relationship to be securely purged:

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

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

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

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

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

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

   b. Update SnapMirror to move the base snapshot forward:

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

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

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

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

   d. Verify that the base snapshot is present:

      ```
      snapshot show -vserver SVM_name -volume volume_name
      ```

   e. Delete the base snapshot:

      ```
      snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot
      ```

6. Securely purge the deleted files:

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

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

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

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

7. Verify the status of the secure purge operation:

   `volume encryption secure-purge show`

Related information

- snapmirror update

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

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

About this task

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

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

Before you begin

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

Steps

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

   `set -privilege advanced`

2. Delete the files or the LUN you want to securely purge.
   - On a NAS client, delete the files you want to securely purge.
   - On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want to purge.
3. Prepare the destination volume in the Asynchronous relationship to be securely purged:

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

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

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

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

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

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

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

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

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

Perform this step on both volumes.

7. Securely purge the deleted files:

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

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

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

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

8. Verify the status of the secure purge operation:

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

Related information

- snapmirror update

Change the ONTAP onboard key management passphrase

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

Before you begin

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

- Advanced privileges are required for this task.
- In a MetroCluster environment, after you update the passphrase on the local cluster, synchronize the passphrase update on the partner cluster.

Steps

1. Change to advanced privilege level:

   ```
   set -privilege advanced
   ```

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

   ONTAP 9.6 and later

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

   ONTAP 9.5 and earlier

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

3. Enter a passphrase between 32 and 256 characters, or for “cc-mode”, a passphrase between 64 and 256 characters.

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

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

      ONTAP 9.6 and later

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

      ONTAP 9.5 and earlier

      - In ONTAP 9.5, run:

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

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

        ```
        security key-manager setup
        ```

   b. Enter the new passphrase when prompted.

      The same passphrase must be used on both clusters.

After you finish

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

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

Related information

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

Back up ONTAP onboard key management information manually

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

Before you begin

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

About this task

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

Steps

1. Change to advanced privilege level:

   ```
   set -privilege advanced
   ```

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

For this ONTAP version…	Use this command…
ONTAP 9.6 and later	`security key-manager onboard show-backup`
ONTAP 9.5 and earlier	`security key-manager backup show`

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

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

     --------------------------BEGIN BACKUP--------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAAACgAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAAAA
     IgAAAAAAAAAAoAAAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAAACQAAAAAAAAAAgAAAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAYAQAAAAAAAAADA5/ccAAAAAAIgAAAAAAAAAAAoAAAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAAACIAAAAAAAAAA
     KAAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAAgAAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAAkAAAAAAAAAAAIAAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAAwAAABgBAAAAAAAAAA
     1cNLLwAAAAAAiAAAAAAAAAAACgAAAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAAAIAAAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAAAIgAAAAAAAAAAAoAAAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAAACAAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAAACQAAAAAAAAAA
     gAAAAAAAAAAAN3Zq7AAAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------END BACKUP---------------------------
```

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

Related information

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

Restore onboard key management encryption keys in ONTAP

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

Before you begin

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

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

ONTAP 9.6 and later

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

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

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

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

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

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

ONTAP 9.8 or later with encrypted root volume

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

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

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

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

ONTAP 9.5 and earlier

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

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

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

Restore ONTAP external key management encryption keys

You can manually restore external key management encryption keys and push them to a different node. You might want to do this if you are restarting a node that was down temporarily when you created the keys for the cluster.

About this task

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

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

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

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

Before you begin

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

Steps

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

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

   a. Set the bootargs:

      ```
      setenv kmip.init.ipaddr <ip-address>

      setenv kmip.init.netmask <netmask>

      setenv kmip.init.gateway <gateway>

      setenv kmip.init.interface e0M

      boot_ontap
      ```

   b. Boot the node to the boot menu and select option `(11) Configure node for external key management`.

   c. Follow prompts to enter management certificate.

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

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

2. Restore the key:

For this ONTAP version…	Use this command…

ONTAP 9.6 and later	`security key-manager external restore -vserver SVM -node node -key-server host_name|IP_address:port -key-id key_id -key-tag key_tag`
ONTAP 9.5 and earlier	`security key-manager restore -node node -address IP_address -key-id key_id -key-tag key_tag`

`node` defaults to all nodes.

This command is not supported when onboard key management is enabled.

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

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

Related information

- security key-manager external restore

Replace KMIP SSL certificates on the ONTAP cluster

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

Before you begin

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

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

Steps

1. Install the new KMIP server-ca certificate:

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

2. Install the new KMIP client certificate:

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

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

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

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

Updating the key manager configuration to use the newly installed certificates will return an error if the public/private keys of the new client certificate are different from the keys previously installed. See the NetApp Knowledge Base: The new client certificate public or private keys are different from the existing client certificate for instructions on how to override this error.

Related information

- security certificate install
- security key-manager external modify

Replace a FIPS drive or SED in ONTAP

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

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

Before you begin

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

Steps

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

   ```
   storage disk show -broken
   ```

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

```
cluster1::> storage disk show -broken
Original Owner: cluster1-01
  Checksum Compatibility: block
                                                                    Usable
Physical
    Disk   Outage Reason HA Shelf Bay Chan   Pool  Type    RPM     Size
Size
    ------ ---- ------------ ---- --- ---- ------ -----  -----  -------
-------
    0.0.0  admin  failed  0b    1   0    A  Pool0  FCAL  10000  132.8GB
133.9GB
    0.0.7  admin  removed 0b    2   6    A  Pool1  FCAL  10000  132.8GB
134.2GB
[...]
```

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

   `storage disk assign -disk disk_name -owner node`

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

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

4. Confirm that the new disk has been assigned:

   `storage encryption disk show`

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

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

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

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

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

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

Related information

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

Make data on a FIPS drive or SED inaccessible

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

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

- Disk sanitization

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

- Disk destroy

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

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

Sanitize a FIPS drive or SED in ONTAP

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

About this task

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

Before you begin

You must be a cluster administrator to perform this task.

Steps

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

   `storage aggregate delete -aggregate aggregate_name`

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

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

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

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

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

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

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

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

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

   ```
   cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

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

5. Sanitize the drive:

   `storage encryption disk sanitize -disk disk_id`

   You can use this command to sanitize hot spare or broken disks only. To sanitize all disks regardless of type, use the `-force-all-state` option.
   Learn more about `storage encryption disk sanitize` in the ONTAP command reference.

ONTAP will prompt you to enter a confirmation phrase before continuing. Enter the phrase exactly as shown on the screen.

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

Warning: This operation will cryptographically sanitize 1 spare or
broken self-encrypting disk on 1 node.
         To continue, enter sanitize disk: sanitize disk

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

6. Unfail the sanitized disk:
   `storage disk unfail -spare true -disk disk_id`
7. Check whether the disk has an owner:
   `storage disk show -disk disk_id`

   If the disk does not have an owner, assign one.
   `storage disk assign -owner node -disk disk_id`
8. Enter the nodeshell for the node that owns the disks you want to sanitize:

   `system node run -node node_name`

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

Related information

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

Destroy a FIPS drive or SED in ONTAP

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

About this task

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

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

Before you begin

You must be a cluster administrator to perform this task.

Steps

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

   `storage aggregate delete -aggregate aggregate_name`

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

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

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

   `storage encryption disk show`

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

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

4. Destroy the disk:

   `storage encryption disk destroy -disk disk_id`

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

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

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

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

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

Related information

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

Emergency shred data on a FIPS drive or SED in ONTAP

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

Before you begin

- If you are using a KMIP server that has no available power, the KMIP server must be configured with an easily destroyed authentication item (for example, a smart card or USB drive).
- You must be a cluster administrator to perform this task.

Step

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

If…	Then…

Power is available to the storage system and you have time to take the storage system offline gracefully	a. If the storage system is configured as an HA pair, disable takeover.
	b. Take all aggregates offline and delete them.
	c. Set the privilege level to advanced:
	`set -privilege advanced`
	d. If the drive is in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID:
	`storage encryption disk modify -disk * -fips-key -id 0x0`
	e. Halt the storage system.
	f. Boot into maintenance mode.
	g. Sanitize or destroy the disks:
	◦ If you want to make the data on the disks inaccessible and still be able to reuse the disks, sanitize the disks:
	`disk encrypt sanitize -all`
	◦ If you want to make the data on the disks inaccessible and you do not need to save the disks, destroy the disks:
	`disk encrypt destroy disk_id1 disk_id2 …`
	The `disk encrypt sanitize` and `disk encrypt destroy` commands are reserved for maintenance mode only. These commands must be run on each HA node, and are not available for broken disks.
	h. Repeat these steps for the partner node.
	This leaves the storage system in a permanently disabled state with all data erased. To use the system again, you must reconfigure it.

<table>
<tr><td rowspan="2">Power is available to the storage system and you must shred the data immediately</td><td><ol type="a">
If you want to make the data on the disks inaccessible and still be able to reuse the disks, sanitize the disks:
If the storage system is configured as an HA pair, disable takeover.
Set the privilege level to advanced:
<pre>set -privilege advanced</pre>
If the drive is in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID:
<pre>storage encryption disk modify -disk * -fips-key-id 0x0</pre>
Sanitize the disk:
<pre>storage encryption disk sanitize -disk * -force-all-states true</pre></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:
<pre>set -privilege advanced</pre>
Destroy the disks:
<pre>storage encryption disk destroy -disk * -force-all-states true</pre></td></tr>
<tr><td colspan="2">The storage system panics, leaving the system in a permanently disabled state with all data erased. To use the system again, you must reconfigure it.</td></tr>
<tr><td>Power is available to the KMIP server but not to the storage system</td><td colspan="2"><ol type="a">
Log in to the KMIP server.
Destroy all keys associated with the FIPS drives or SEDs that contain the data you want to prevent access to.
This prevents access to disk encryption keys by the storage system.</td></tr>
<tr><td>Power is not available to the KMIP server or the storage system</td><td colspan="2">Destroy the authentication item for the KMIP server (for example, the smart card). This prevents access to disk encryption keys by the storage system.</td></tr>
</table>

Related information

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

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

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

Before you begin

You must be a cluster administrator to perform this task.

About this task

You should use this process only if you are certain that the authentication keys for the FIPS drive or SED are permanently lost and that you cannot recover them.

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

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

Steps

1. Return a FIPS drive or SED to service:

If the SEDS are…	Use these steps…

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

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

Related information

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

Return a FIPS drive or SED to unprotected mode in ONTAP

A FIPS drive or SED is protected from unauthorized access only if the authentication key ID for the node is set to a value other than the default. You can return a FIPS drive or SED to unprotected mode by using the `storage encryption disk modify` command to set the key ID to the default. A FIPS drive or SED in unprotected mode uses the default encryption keys, while a FIPS drive or SED in protected mode uses supplied, secret encryption keys. If there is encrypted data on the drive and the drive is reset to unprotected mode, the data is still encrypted and is not exposed.

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

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

Before you begin

You must be a cluster administrator to perform this task.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

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

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

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

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

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

   Confirm the operation succeeded with the command:

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

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

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

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

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

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

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

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

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

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

   Confirm the operation succeeded with the command:

   `storage encryption disk show-status`

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

Maintenance mode

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

Steps

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

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

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

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

3. Confirm the FIPS authentication key was successfully rekeyed:

```
disk encrypt show_fips
```

4. Confirm data authentication key was successfully rekeyed with:

```
disk encrypt show
```

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

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

Related information

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

Remove an external key manager connection in ONTAP

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

About this task

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

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

Before you begin

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

Step

1. Disconnect a KMIP server from the current node:

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

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

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

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

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

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

Modify ONTAP external key management server properties

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

Before you begin

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

Steps

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

   ```
   set -privilege advanced
   ```

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

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

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

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

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

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

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

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

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

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

4. Repeat the last step for any additional SVMs.

Related information

- security key-manager external modify-server

Transition to external key management from onboard key management in ONTAP

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

Before you begin

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

  Returning a FIPS drive or SED to unprotected mode

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

  Unencrypting volume data

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

Step

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

For this ONTAP version…	Use this command…

ONTAP 9.6 and later	`security key-manager onboard disable -vserver SVM`
ONTAP 9.5 and earlier	`security key-manager delete-key-database`

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

Switch from external key management to ONTAP onboard key management

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

Before you begin

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

  Returning a FIPS drive or SED to unprotected mode

- You must have deleted all external key manager connections.

  Deleting an external key manager connection

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

Steps

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

ONTAP 9.6 and later

1. Change to the advanced privilege level:

   ```
   set -privilege advanced
   ```

2. Use the command:

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

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

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

ONTAP 9.5 and earlier

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

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

Related information

- security key-manager external disable

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

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

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

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

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

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

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

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

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

X577_PHM2800MCTO 800GB NSE SSDs with firmware revisions NA00 or NA01	5	Temporary. Lockout is only in effect until disk is power-cycled.
X440_PHM2800MCTO 800GB NSE SSDs with higher firmware revisions	1024	Permanent. Data cannot be recovered, even when the proper authentication key becomes available again.
X577_PHM2800MCTO 800GB NSE SSDs with higher firmware revisions	1024	Permanent. Data cannot be recovered, even when the proper authentication key becomes available again.
All other SSD models	1024	Permanent. Data cannot be recovered, even when the proper authentication key becomes available again.

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

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

Disable ONTAP encryption by default

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

Before you begin

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

Step

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

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

Copyright information

Trademark information