# NetApp

# Configure external key management
ONTAP 9

NetApp
February 20, 2026

# Table of Contents

# 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.

> (i) 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
```

> (i) 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
```

> ℹ️
> - 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.

> ℹ️
> 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
```

> ℹ️
> 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
```