Configure external key management

ONTAP 9

NetApp
February 20, 2026

Table of Contents

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`

   ```
   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.

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

Copyright information

Trademark information