Configure external key management

ONTAP 9

NetApp
May 19, 2022

Table of Contents

Configure external key management

Configure external key management overview

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

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

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

Collect network information in ONTAP 9.2 and earlier

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

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

Item	Notes	Value
Key management network interface name		
Key management network interface IP address	IP address of node management LIF, in IPv4 or IPv6 format	
Key management network interface IPv6 network prefix length	If you are using IPv6, the IPv6 network prefix length	
Key management network interface subnet mask		
Key management network interface gateway IP address		
IPv6 address for the cluster network interface	Required only if you are using IPv6 for the key management network interface	

Port number for each KMIP server	Optional. The port number must be the same for all KMIP servers. If you do not provide a port number, it defaults to port 5696, which is the Internet Assigned Numbers Authority (IANA) assigned port for KMIP.	
Key tag name	Optional. The key tag name is used to identify all keys belonging to a node. The default key tag name is the node name.	

Related information

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

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

Install SSL certificates on the cluster

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

What you'll need

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

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

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

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

About this task

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

Steps

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

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

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

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

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

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

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

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

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

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

Before you begin

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

Steps

1. Configure key manager connectivity for the cluster:

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

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

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

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

2. Verify that all configured KMIP servers are connected:

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

```
-server host_name|IP_address:port -key-server-status available|not-
responding|unknown
```

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

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

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

6 entries were displayed.
```

Enable external key management in ONTAP 9.5 and earlier

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

What you'll need

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

About this task

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

Steps

1. Configure key manager connectivity for cluster nodes:

   ```
   security key-manager setup
   ```

   The key manager setup starts.

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

   `security key-manager add -address key_management_server_ipaddress`

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

4. Add an additional KMIP server for redundancy:

   `security key-manager add -address key_management_server_ipaddress`

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

5. Verify that all configured KMIP servers are connected:

   `security key-manager show -status`

   For complete command syntax, see the man page.

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

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

Configure clustered external key servers

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

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

Before you begin

- KMIP key management is already enabled for the SVM.
- This process only supports key servers that use KMIP. For a list of supported key servers, check the NetApp Interoperability Matrix Tool.

- All nodes in the cluster must be running ONTAP 9.11.1 or later.
- The order of servers list arguments in the `-secondary-key-servers` parameter reflects the access order of the external key management (KMIP) servers.

Create a clustered key server

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

Add primary and secondary key servers to an SVM

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

Add secondary key servers to an existing primary key server

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

Modify clustered key servers

You can modify external key servers clusters by changing the status (primary or secondary) of particular key servers, add and removing secondary key servers, or by changing the access order of secondary key servers.

Converting primary and secondary key servers

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

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

Modifying secondary key servers

Secondary key servers are managed with the `-secondary-key-servers` parameter of the `security key-manager external modify-server` command. The `-secondary-key-servers` parameter accepts a comma-separated list. The specified order of the secondary key servers in the list determines the

access sequence for the secondary key servers. The access order can be modified by running the command `security key-manager external modify-server` with the secondary key servers entered in a different sequence.

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

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

Create authentication keys in ONTAP 9.6 and later

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

What you'll need

You must be a cluster administrator to perform this task.

About this task

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

ONTAP creates authentication keys for all nodes in the cluster.

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

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

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

  You can use the `security key-manager key delete` command to delete any unused keys. The `security key-manager key delete` command fails if the given key is currently in use by ONTAP. (You must have privileges greater than "admin" to use this command.)

Steps

1. Create the authentication keys for cluster nodes:

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

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

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

```
cluster1::> security key-manager key create
Key ID:
000000000000000002000000000001006268333f870860128fbe17d393e5083b00000000
00000000
```

2. Verify that the authentication keys have been created:

   `security key-manager key query -node node`

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

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

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

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

       Vserver: cluster1
   Key Manager: external
          Node: node2

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

Create authentication keys in ONTAP 9.5 and earlier

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

What you'll need

You must be a cluster administrator to perform this task.

About this task

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

ONTAP creates authentication keys for all nodes in the cluster.

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

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

Steps

1. Create the authentication keys for cluster nodes:

   `security key-manager create-key`

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

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

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

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

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

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

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

2. Verify that the authentication keys have been created:

   `security key-manager query`

   For complete command syntax, see the man page.

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

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

  (security key-manager query)

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

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


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

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

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

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

What you'll need

You must be a cluster administrator to perform this task.

About this task

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

Steps

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

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

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

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

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

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

2. Verify that the authentication keys have been assigned:

`storage encryption disk show`

For complete command syntax, see the man page.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
[...]
```