NetApp ONTAP and Entrust KeyControl

Integration Guide

2025-06-30

Table of Contents

Chapter 1. Introduction

This document describes the integration of the NetApp ONTAP data management software with the Entrust KeyControl key management solution using the open standard KMIP protocol. KeyControl serves as a key manager for encryption keys by using various protocols, including KMIP.

1.1. Product configuration

Entrust has successfully tested the integration of KeyControl with NetApp ONTAP in the following configurations:

Product	Version
NetApp ONTAP	9.16.1.P3
Entrust KeyControl	10.4.3

1.2. Requirements

Before starting the integration process, familiarize yourself with:

- NetApp ONTAP 9 Online Documentation.
- Entrust KeyControl Online Documentation Set.

Chapter 2. Deploy KeyControl

2.1. Deploy a KeyControl cluster

For the purpose of this integration, a two-node cluster was deployed.

Follow the installation and setup instructions in the *KeyControl nShield HSM Integration Guide*. You can access it from the Entrust Document Library and from the nShield Product Documentation website.

Make sure the KeyControl KMIP Vault gets created and certificates are generated for NetApp ONTAP. These certificates are used in the configuration of the KMS described below.

Also add a record in your DNS server for the KeyControl cluster. Associate all KeyControl Cluster node IPs to the one record.

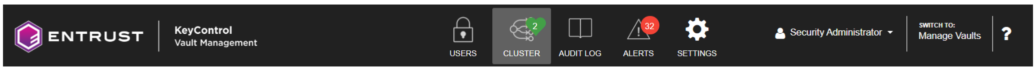
The following sections describe how to create the KeyControl KMIP Vault and certificates.

2.2. Create a KMIP Vault in KeyControl

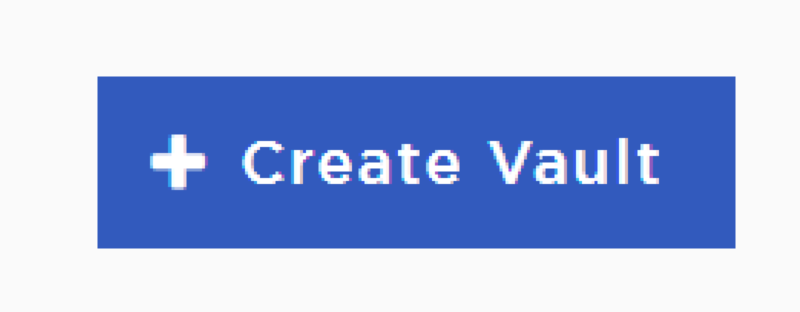
The KeyControl Vault appliance supports different type of vaults that can be used by all type of applications. This section describes how to create a KMIP Vault in the KeyControl Vault Server.

Refer to the Creating a Vault section of the admin guide for more details.

1. Sign in to the KeyControl Vault Server web user interface:
    a. Use your browser to access the IP address of the server.
    b. Sign in using the **secroot** credentials.
2. If not in the **Vault Management** interface, in the top menu bar, on the right side, select **Switch to: Manage Vaults**.



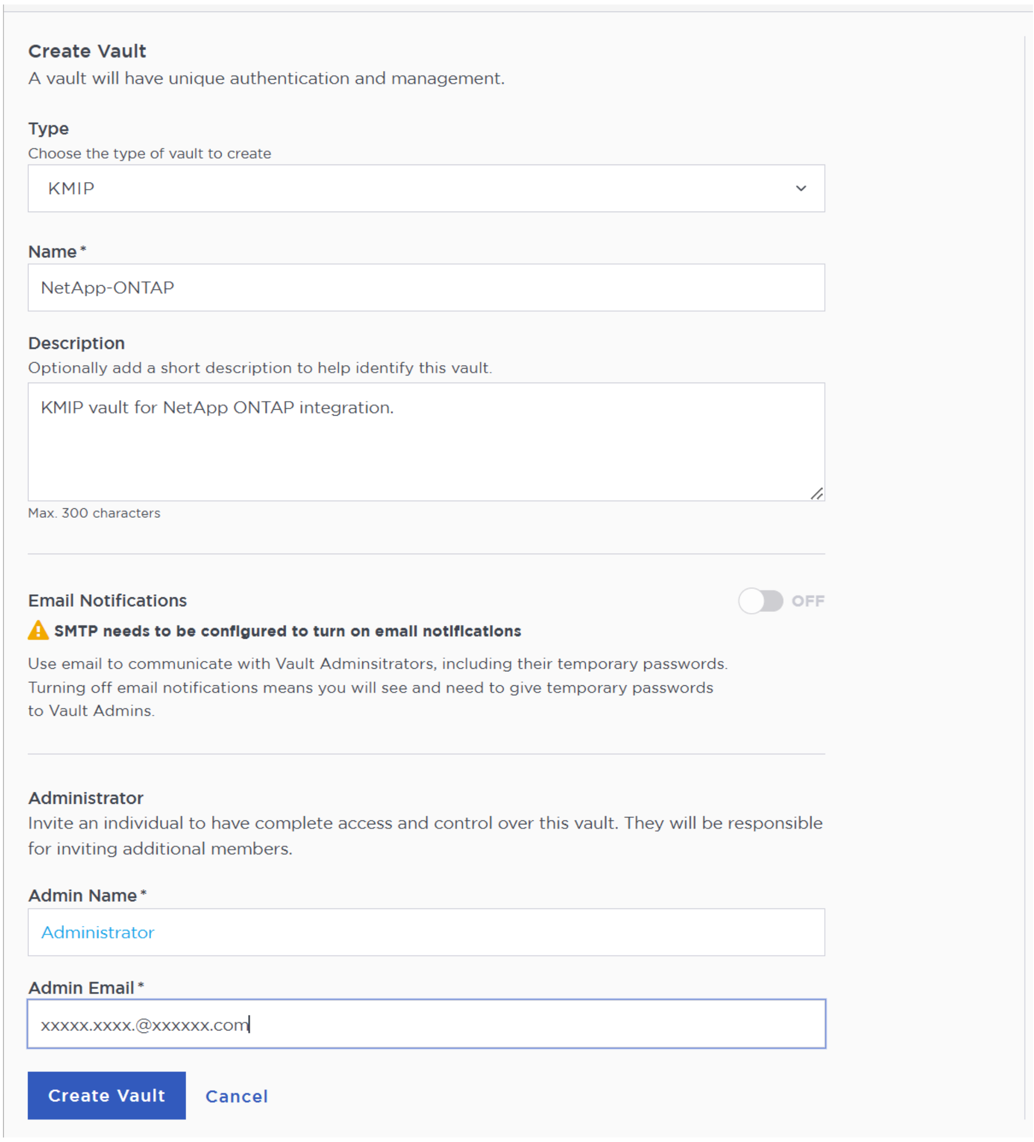
3. In the KeyControl Vault Management interface, select **Create Vault**.



4. In the **Create Vault** page, create a **KMIP** Vault:

Field	Value
Type	**KMIP**
Name	Vault name
Description	Vault description
Email Notifications	Enable it if using email to communicate with Vault administrators
Admin Name	Vault administrator username
Admin Email	Vault administrator email

For example:



Create Vault

A vault will have unique authentication and management.

Type

Choose the type of vault to create

KMIP

Name*

NetApp-ONTAP

Description

Optionally add a short description to help identify this vault.

KMIP vault for NetApp ONTAP integration.

Max. 300 characters

Email Notifications OFF

⚠ **SMTP needs to be configured to turn on email notifications**

Use email to communicate with Vault Adminsitrators, including their temporary passwords. Turning off email notifications means you will see and need to give temporary passwords to Vault Admins.

Administrator

Invite an individual to have complete access and control over this vault. They will be responsible for inviting additional members.

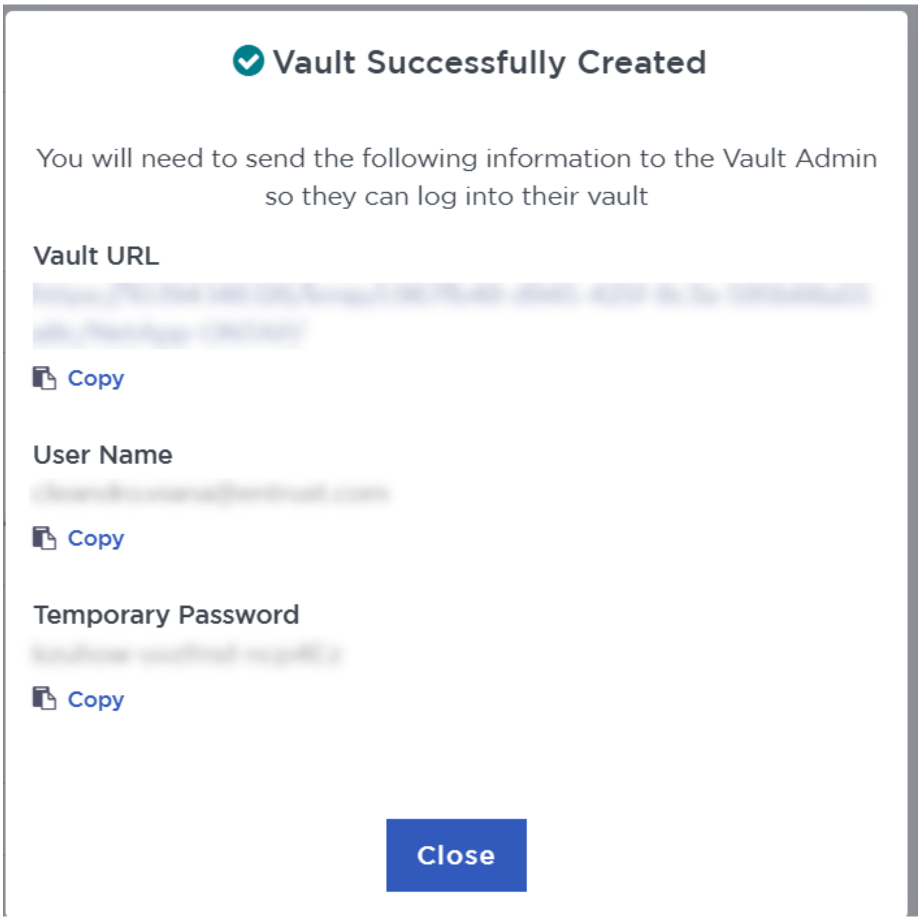
Admin Name*

Administrator

Admin Email*

xxxxx.xxxx.@xxxxxx.com

5. Select **Create Vault**.



Vault Successfully Created

You will need to send the following information to the Vault Admin so they can log into their vault

Vault URL

[redacted]

User Name

[redacted]

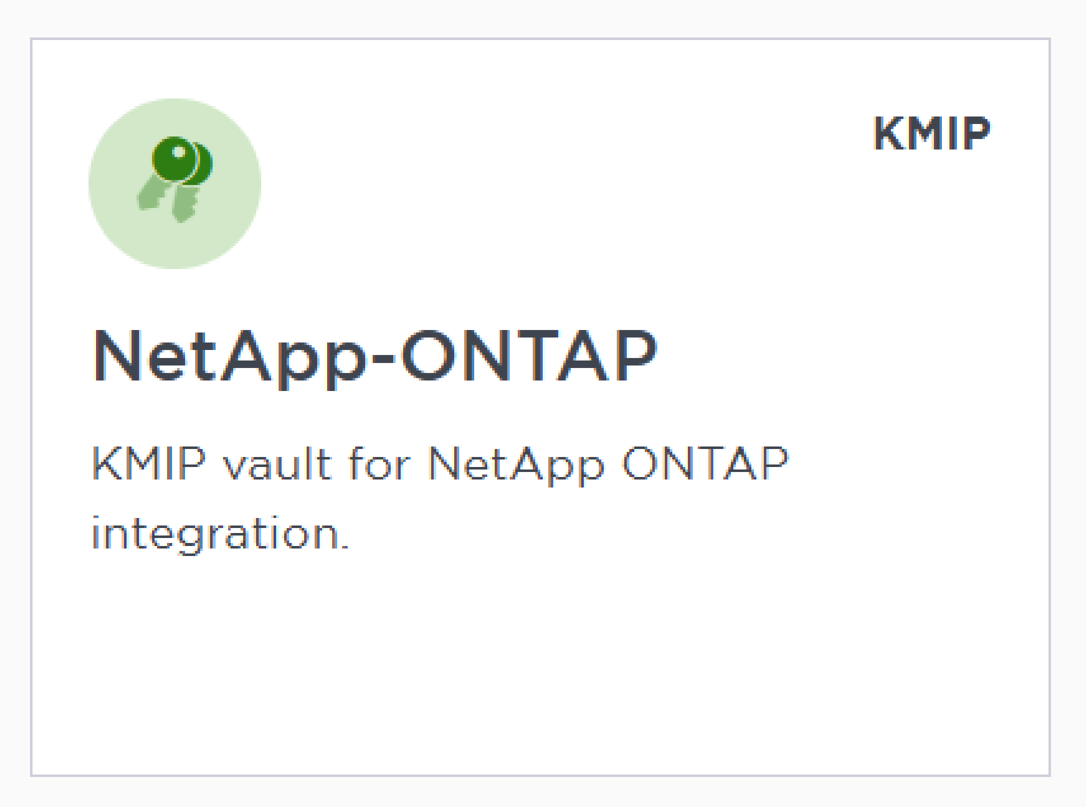
Temporary Password

[redacted]

The new vault’s URL and sign-in credentials will be emailed to the administrator’s email address entered above. This is the password that will be used to sign in for the first time to the KMIP vault’s space in KeyControl. In closed gap environments where email is not available, the URL and sign-in credentials are displayed at this time. That can be copied and sent to the user.

6. Bookmark the KMIP Vault URL.
7. Select **Close**.
8. The newly created Vault is added to the **Vault Management** dashboard and the KMIP server settings on the appliance are **enabled**.

   For example:



KMIP

NetApp-ONTAP

KMIP vault for NetApp ONTAP integration.

9. Sign in to the URL provided above with the temporary password. Change the initial password when prompted. Sign in again to verify.

2.3. KMIP server settings

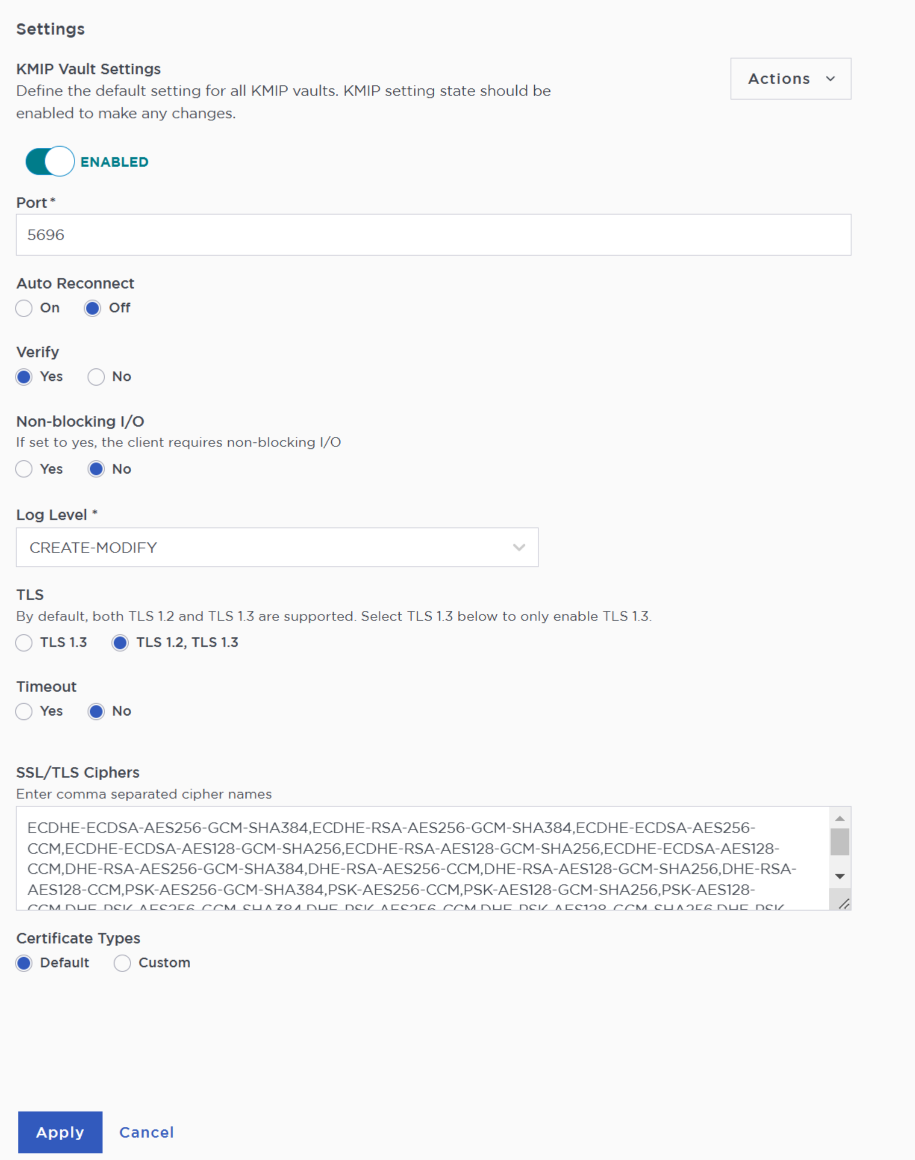
The KMIP server settings are set at the KeyControl appliance level and apply to all the KMIP vaults in the appliance. After a KMIP vault is created, it is automatically set to **ENABLED**.

To use external key management and configure the KeyControl Vault KMIP settings, refer to the KeyControl Vault for KMIP section of the admin guide.

When you are using external key management, as is the case in this solution, the KeyControl server is the KMIP server and the NetApp server is the KMIP client.

1. Log into the KeyControl server vault management UI as **secroot**.
2. Select the **Settings** icon on the top right to view/change the KMIP settings.

   The defaults settings are appropriate for most applications but you can change settings to suit your environment.



Settings

KMIP Vault Settings

Define the default setting for all KMIP vaults. KMIP setting state should be enabled to make any changes.

ENABLED

Port *

5696

Auto Reconnect

○ On ● Off

Verify

● Yes ○ No

Non-blocking I/O

If set to yes, the client requires non-blocking I/O

○ Yes ● No

Log Level *

CREATE-MODIFY

TLS

By default, both TLS 1.2 and TLS 1.3 are supported. Select TLS 1.3 below to only enable TLS 1.3.

○ TLS 1.3 ● TLS 1.2, TLS 1.3

Timeout

○ Yes ● No

SSL/TLS Ciphers

Enter comma separated cipher names

```
ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-RSA-AES256-GCM-SHA384,ECDHE-ECDSA-AES256-
CCM,ECDHE-ECDSA-AES128-GCM-SHA256,ECDHE-RSA-AES128-GCM-SHA256,ECDHE-ECDSA-AES128-
CCM,DHE-RSA-AES256-GCM-SHA384,DHE-RSA-AES256-CCM,DHE-RSA-AES128-GCM-SHA256,DHE-RSA-
AES128-CCM,PSK-AES256-GCM-SHA384,PSK-AES256-CCM,PSK-AES128-GCM-SHA256,PSK-AES128-
CCM,DHE-PSK-AES256-CCM-SHA384,DHE-PSK-AES256-CCM,DHE-PSK-AES128-CCM-SHA256,DHE-PSK-
```

Certificate Types

● Default ○ Custom

3. Select **Apply**.

2.4. Install a signed certificate from your local root CA in the KeyControl cluster

You can use any CA for this integration. This guide describes an integration in which a Microsoft Windows CA was configured as a local root CA.

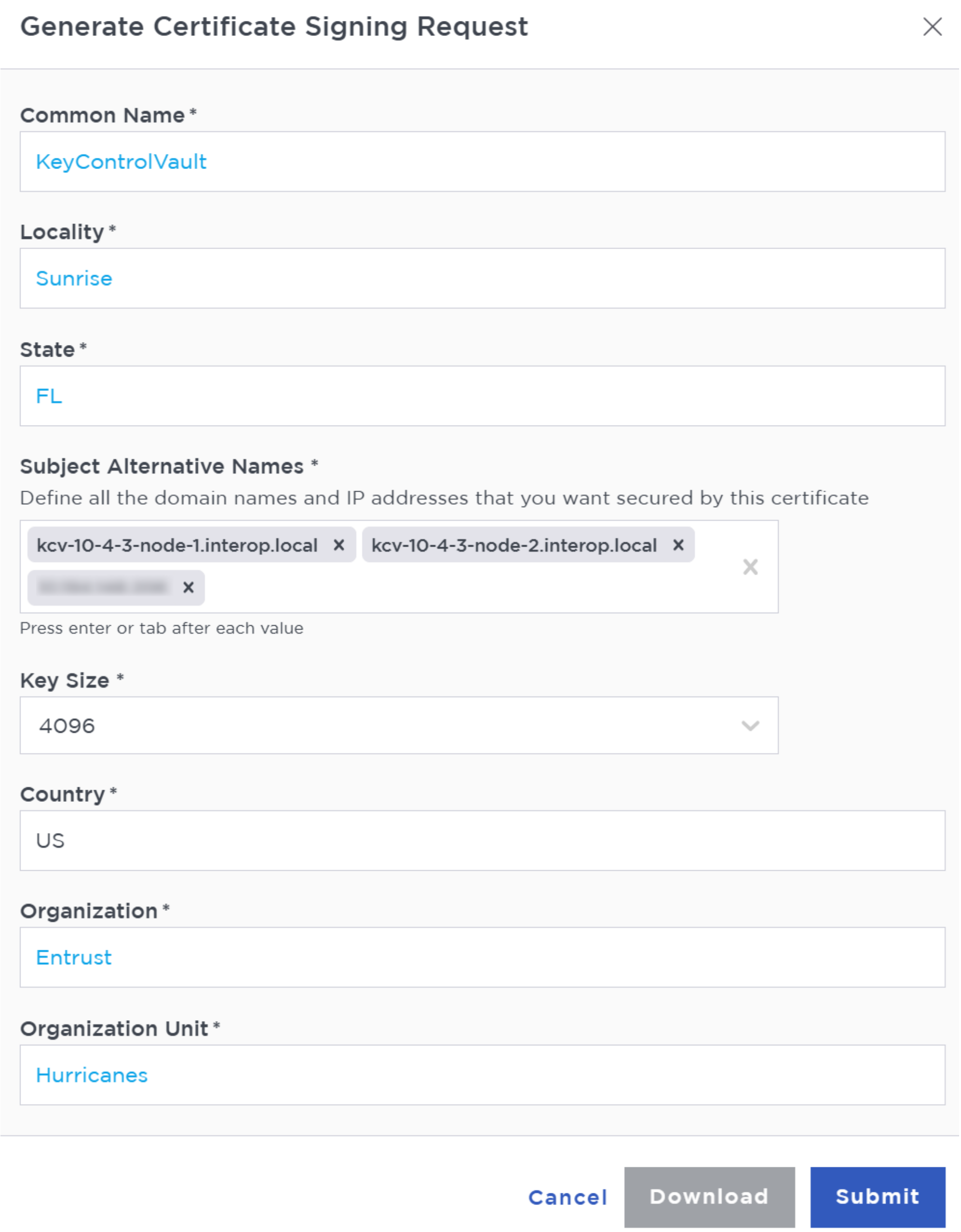
2.4.1. Create a CSR

1. Log into the KeyControl server vault management UI as **secroot**.
2. In the **Vault Management** dashboard, select the **Settings** icon on the top right.

3. Select the **Action** icon pull-down menu. Then select **Generate CSR**.
4. Enter your information.

   Include the FQDN and / or IP of all the KeyControl nodes in the **Subject Alternative Names**.

   For example:



Generate Certificate Signing Request

Common Name *
KeyControlVault

Locality *
Sunrise

State *
FL

Subject Alternative Names *
Define all the domain names and IP addresses that you want secured by this certificate
kcv-10-4-3-node-1.interop.local × kcv-10-4-3-node-2.interop.local × [redacted] ×
Press enter or tab after each value

Key Size *
4096

Country *
US

Organization *
Entrust

Organization Unit *
Hurricanes

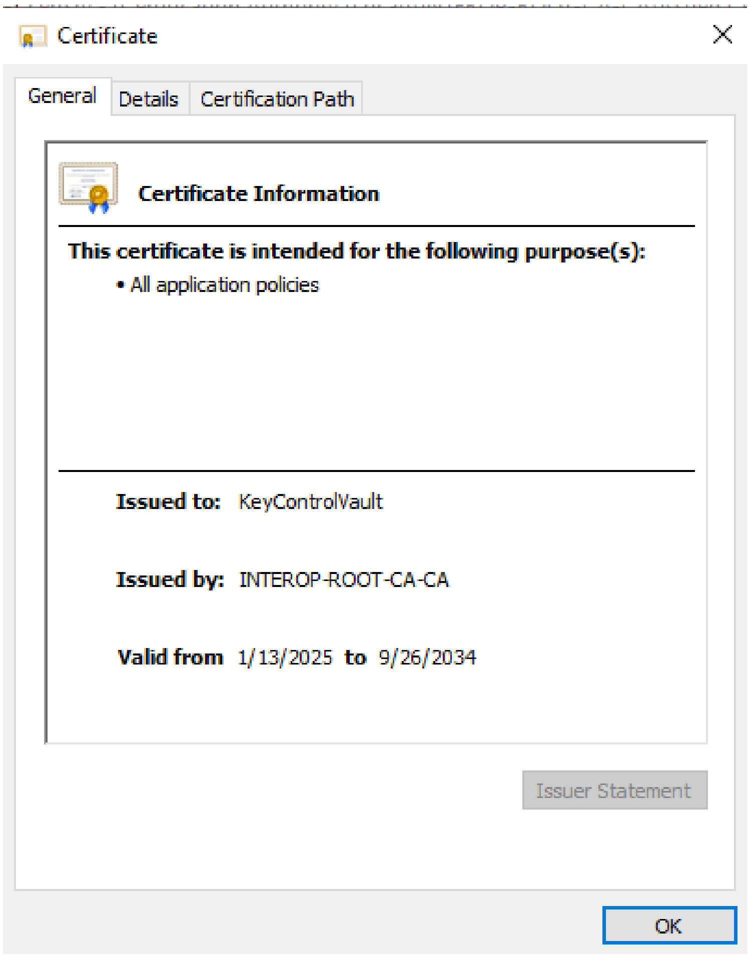
5. Select **Submit**.
6. Once Submitted, Select **Download**. The CSR **pem** file is downloaded to your downloads folder.

7. Store the file so it can be signed in the next section.

2.4.2. Sign the certificate

1. Log into your local root CA with Administrator privileges.
2. Transfer the CSR created above to a local folder in your local root CA server. (Downloads folder)
3. Launch the **Certificate Authority** application.
4. Right-click on the **<certification authority name>** in the left pane and select **All Tasks / Submit new request…**.
5. Select the copied CSR.
6. Select **certification authority name** / **Pending Request** in the left pane.
7. Right-click on the request in the right pane and select **All Tasks / Issue**.
8. Select **certification authority name** / **Issued Certificates** in the left pane.
9. Select the certificate.

   For example:



This certificate is intended for the following purpose(s):

- All application policies

Issued to: KeyControlVault

Issued by: INTEROP-ROOT-CA-CA

Valid from 1/13/2025 to 9/26/2034

10. Select the **Details** tab / **Copy to File...**. Follow the instructions, selecting **Base-64 encoded X.509** in **Export File Format**. Save as `keycontrolvault` in the `Downloads` folder.
11. Export the local root CA certificate in pem format.

    ```
    C:\Users\Administrator>certutil -ca.cert C:\Users\Administrator\Downloads\rootcacert.cer
    CA cert[0]: 3 -- Valid
    CA cert[0]:
    -----BEGIN CERTIFICATE-----
    MIIDFTCaaa2gAwbbbgIQepb3APptdddOv11kVoDg1jANBgkqhkiG9w0BAQsFADAd
    .
    .
    .
    18BAfZuJ/givxxk05ukP52FD3iVYMGoxWQ==
    -----END CERTIFICATE-----

    CertUtil: -ca.cert command completed successfully.
    ```

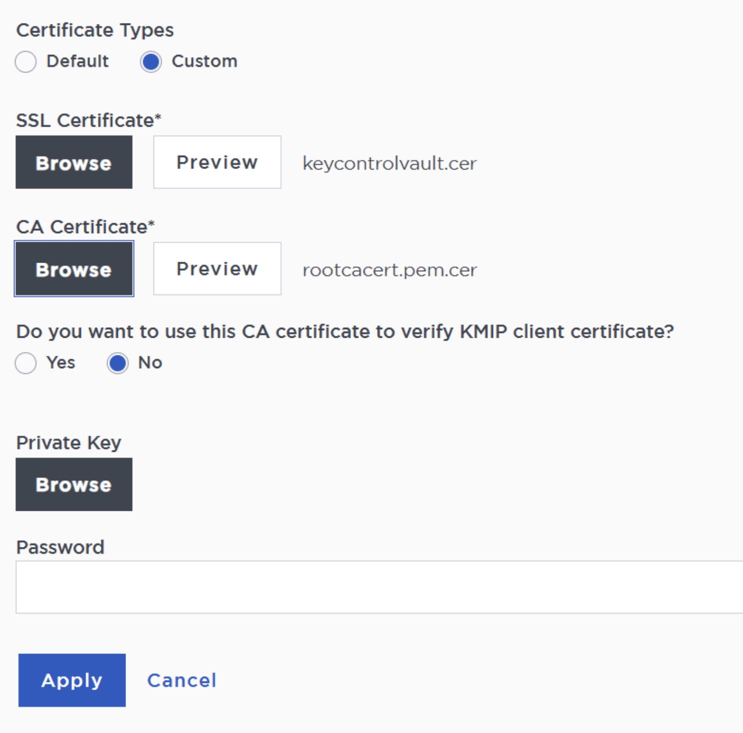
    Now make it in `pem` format:

    ```
    C:\Users\Administrator>certutil -encode C:\Users\Administrator\Downloads\rootcacert.cer
    C:\Users\Administrator\Downloads\rootcacert.pem.cer
    Input Length = 793
    Output Length = 1150
    CertUtil: -encode command completed successfully.
    ```

12. Copy the `keycontrolvault.cer` certificate and the `rootcacert.pem.cer` to a location accessible by the KeyControl server.

2.4.3. Install certificate

1. Log into the KeyControl server vault management UI as **secroot**.
2. In the **Vault Management** dashboard, select the **Settings** icon on the top right.
3. Select **Custom** radio button in **Certificate Types**.
4. Browse and select the certificate as shown.



Certificate Types

○ Default ● Custom

SSL Certificate*

Browse Preview keycontrolvault.cer

CA Certificate*

Browse Preview rootcacert.pem.cer

Do you want to use this CA certificate to verify KMIP client certificate?

○ Yes ● No

Private Key

Browse

Password

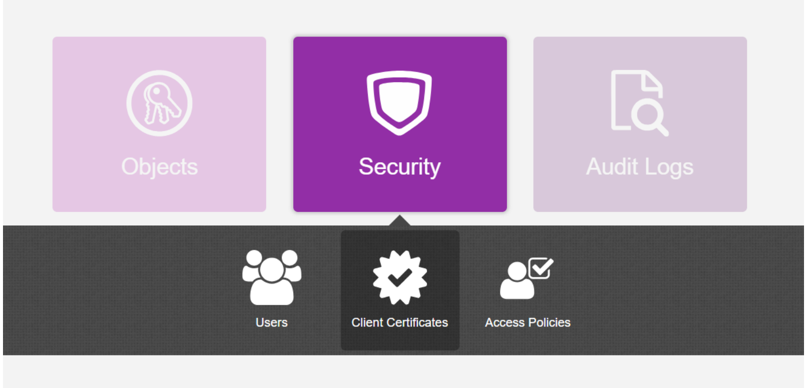
Apply Cancel

5. The other defaults settings are appropriate for most applications. Make any changes necessary.
6. Select **Apply**.

2.5. Create the KeyControl client certificate bundle

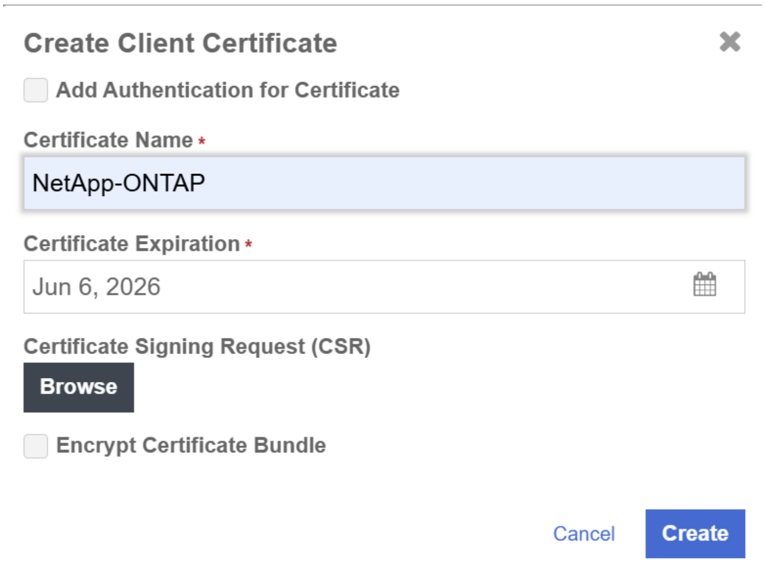
Certificates are required to facilitate the KMIP communications from the KeyControl KMIP Vault and NetApp ONTAP application and conversely. The built-in capabilities in KeyControl are used to create and publish the certificate.

1. Login to the KMIP Vault with the URL and credentials from Create a KMIP Vault in KeyControl.
2. Select **Security**, then **Client Certificates**.



3. In the **Manage Client Certificate** page, select the **+** icon on the right to create a new certificate. The **Create Client Certificate** dialog box appears.
4. In the **Create Client Certificate** dialog box:
   a. Enter the certificate name.
   b. Enter the expiration date.
   c. Leave **Certificate Signing Request (CSR)** field as default.
   d. Select **Create**.

   For example:



Create Client Certificate

□ Add Authentication for Certificate

Certificate Name *

NetApp-ONTAP

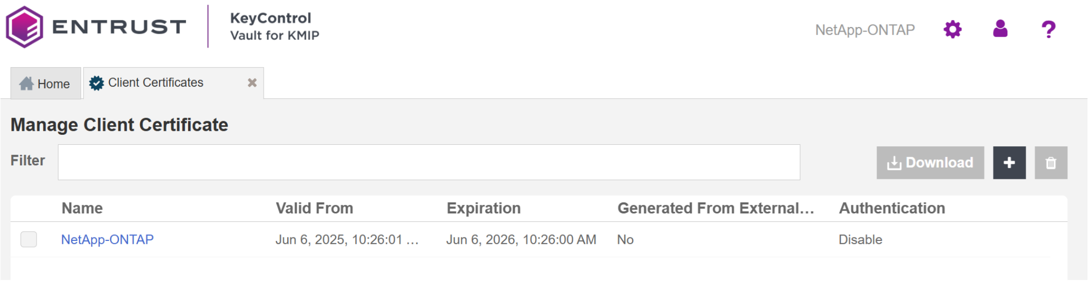
Certificate Expiration *

Jun 6, 2026

Certificate Signing Request (CSR)

□ Encrypt Certificate Bundle

The new certificates are added to the **Manage Client Certificate** pane.



Manage Client Certificate

Filter

Name	Valid From	Expiration	Generated From External...	Authentication
NetApp-ONTAP	Jun 6, 2025, 10:26:01 ...	Jun 6, 2026, 10:26:00 AM	No	Disable

5. Select the certificate and select the **Download** icon to download the certificate.
6. Unzip the downloaded file.

```
% unzip NetApp-ONTAP_2025-06-06-14-28-04.zip
Archive:  NetApp-ONTAP_2025-06-06-14-28-04.zip
  inflating: NetApp-ONTAP.pem
  inflating: cacert.pem
```

It contains the following:

- A `certname.pem` file that includes both the client certificate and private key. In this example, this file is called `NetApp-ONTAP.pem`.

  The client certificate section of the `certname.pem` file includes the lines “-----BEGIN CERTIFICATE-----" and “-----END CERTIFICATE-----" and all text between them.

  The private key section of the `certname.pem` file includes the lines “-----BEGIN PRIVATE KEY-----" and “-----END PRIVATE KEY-----" and all text in between them.

- A `cacert.pem` file which is the root certificate for the KMS cluster. It is always named `cacert.pem`.

7. These files will be used to establish trust between KeyControl and NetApp.

For more information on how to create a certificate bundle, see Establishing a Trusted Connection with a KeyControl-Generated CSR.

Chapter 3. Deploy NetApp Simulate ONTAP

This integration testing was performed using Simulate ONTAP configured as a single node. Simulate ONTAP 9.x is a virtual simulator for ONTAP® software. The virtual simulator was deployed as a virtual machine in VMware.

1. Download the simulator ova file from Simulate ONTAP Download

   If you get the following error when running version 9.16.1 of the simulator and try to upgrade to 9.16.1.P3, you have use version 9.14.1 of the simulator and then do the upgrade to 9.16.1.P3.

   ```
   Error: command failed: System management storage area of node(s) "mycluster-01" doesn't have minimum
   recommended space available for automated nondisruptive update procedure. Use the "volume show" command to
   check available space on root volumes. The recommended best practice is to have minimum 40GB space
   available in system management storage area before starting automated nondisruptive update. Contact NetApp
   Support for further assistance
   ```

2. Deploy the virtual machine. For the purpose on this integration, the **STORAGE SYSTEM NAME** is set to **mycluster**.
3. Add a record in your DNS server for the **Cluster Management**.
4. Configure the NTP server.# Follow the instructions in the NetApp documentation.
5. Install the root CA certificate from your root CA.

   ```
   mycluster::> security certificate install -vserver mycluster -type server-ca -subtype kmip-cert

   ...

   You should keep a copy of the CA-signed digital certificate for future reference.

   The installed certificate's CA and serial number for reference:
   CA: INTEROP-ROOT-CA-CA
   serial: 7A96F700FA6D70984EBF5D645680E0D6

   The certificate's generated name for reference: INTEROP-ROOT-CA-CA
   ```

Note the certificate’s generated name above, e.g. **interop-CONTROLLER-CA-CA**. It will be needed in section Setup KeyControl as the external KMIP server.

Chapter 4. Integrate KeyControl with NetApp ONTAP

4.1. Install the KeyControl client bundle into NetApp ONTAP

1. Open a command window and remote login into the NetApp ONTAP Cluster Management.

   ```
   % ssh admin@xxx.xxx.xxx.xxx
   ```

2. Install the KeyControl Client Certificate into NetApp ONTAP.

   Paste the certificate section from the `NetApp-ONTAP.pem` file from section Create the KeyControl client certificate bundle when prompted. Paste the private key section when prompted.

   ```
   mycluster::> security certificate install -vserver mycluster -type client -subtype kmip-cert
   Please enter Certificate: Press <Enter> when done
   -----BEGIN CERTIFICATE-----
   MIIEaDCCA1CgAwIBAgIEfhphJTANBgkqhkiG9w0BAQsFADBXMQswCQYDVQQGEwJV
   .
   .
   .
   Ib/yNAFPx5aYqVv7b1RKCnTUYnhn/dyGPUuVQgrtQRKx6tQUbLhIHW/z8qMzJf/w
   hnQE/yaXuHl3ofbRJ9Q9IxtYz4jtdluEXQkVxUvu+weqYz6l+jl+7CeFvO2yhjSd
   bX8bICgNVFhPjoxY7/BLFCaBDhsnhYpO9Wr1uXh6TxbmnxSwYipZLzBGpnagl47V
   RMM5ZEqIjkwJh1CurTN5JuLFZPYV9zNNHKKEiQ==
   -----END CERTIFICATE-----

   Please enter Private Key: Press <Enter> when done
   -----BEGIN PRIVATE KEY-----
   MIIJQwIBADANBgkqhkiG9w0BAQEFAASCCS0wggkpAgEAAoICAQCj7+BP2YfDiUiW
   .
   .
   .
   QiHLPgQodyWE0zO50+2c/vBopas2bCz8y/klWwm87Er8LAqP3PhFcGMe4+NlFB4V
   W0toY9yZQ6MI6mtMCtISGPnCOdpcKv8SF8Btf76PTlpUzzJ3qBbg+3XytojZ4udg
   T0ScRW+7m8qKuyJCbC7oLyEaeuMcU/A=
   -----END PRIVATE KEY-----

   Enter certificates of certification authorities (CA) which form the certificate chain of the client
   certificate.
   This starts with the issuing CA certificate of the client certificate and can range up to the root CA
   certificate.

   Do you want to continue entering root and/or intermediate certificates {y|n}: n

   You should keep a copy of the private key and the CA-signed digital certificate for future reference.

   The installed certificate's CA and serial number for reference:
   CA: HyTrust KeyControl Certificate Authority
   serial: 7E1A6125
   ```

```
The certificate's generated name for reference: NetApp-ONTAP
```

3. Note the certificate’s generated name above, e.g. **NetApp-ONTAP**. It will be needed in section Setup KeyControl as the external KMIP server.

4.2. Setup KeyControl as the external KMIP server

1. Open a command window and remote login into the NetApp ONTAP Cluster Management.
2. Enable the external KMIP server.

   The argument of **-client-cert** is the certificate’s generated name from section Install the KeyControl client bundle into NetApp ONTAP: **NetApp-ONTAP**. The argument of **-server-ca-certs** is the certificate’s generated name from section Deploy NetApp Simulate ONTAP: **INTEROP-ROOT-CA-CA**.

   Notice the IP of both nodes in the KeyControl cluster.

   ```
   mycluster::> security key-manager external enable -key-servers xx.xxx.xxx.xxx:5696,xx.xxx.xxx.xxx:5696
   -client-cert NetApp-ONTAP -server-ca-certs INTEROP-ROOT-CA-CA
   ```

   For testing the integration, we used only the primary KeyControl node’s IP address.

3. Verify the external key-management is configured.

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

   Node  Vserver  Primary Key Server                                 Status
   ----  -------  -------------------------------------------------  ------------
   mycluster-01
         mycluster
                  xx.xxx.xxx.xxx:5696                                available
                  xx.xxx.xxx.xxx:5696                                available
   2 entries were displayed.
   ```

Chapter 5. Test integration

This test procedure requires test scripts available from NetApp. The output files resulting from executing the test scripts need to be sent back to NetApp for verification.

5.1. Load the test scripts into NetApp ONTAP

1. Open a command window and remote login into the NetApp ONTAP Cluster Management.
2. Set diagnostics.

```
mycluster::> set diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y

mycluster::*>
```

3. Enter system shell.

   Provide the password when prompted.

```
mycluster::*> systemshell -node mycluster-01
  (system node systemshell)
diag@127.0.0.1's password:

Warning:  The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly.  Use this environment
only when directed to do so by support personnel.

mycluster-01%
```

4. Copy the test script files from a server of your choice into the Systemshell of the NetApp ONTAP node.

   Provide the password when prompted.

```
mycluster-01% scp root@xx.xxx.xxx.xxx:/root/Downloads/kmip_before_reboot_test.sh .
kmip_before_reboot_test.sh                                                            100% 7346   731.0KB/s
00:00
SSH terminating : scp.c : main : 690,errs = 0.

mycluster-01% scp root@xx.xxx.xxx.xxx:/root/Downloads/kmip_post_reboot_test.sh .
kmip_post_reboot_test.sh                                                              100% 6047     3.6MB/s
00:00
SSH terminating : scp.c : main : 690,errs = 0.
```

ℹ The test scripts were provided by NetApp.

5. Verify the test scripts files are in the current directory.

```
mycluster-01% ls
kmip_before_reboot_test.sh      kmip_post_reboot_test.sh
```

5.2. Execute the kmip_before_reboot_test.sh test script

1. Open a command window and remote login into the NetApp ONTAP Cluster Management.
2. Set diagnostics.

```
mycluster::> set diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y

mycluster::*>
```

3. Enter Systemshell.

   Provide the password when prompted.

```
mycluster::*> systemshell -node mycluster-01
  (system node systemshell)
diag@127.0.0.1's password:

Warning:  The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly.  Use this environment
only when directed to do so by support personnel.

mycluster-01%
```

4. Execute the `kmip_before_reboot_test.sh` test script and redirect the output to file `kmip_before_reboot_test.txt`.

   KeyControl presents itself as a single entity even though it may be composed of multiple nodes (two in this test case). Therefore, select **no** if the **Please enter whether this is a clustered key-server config (yes or no):** question is shown.

```
mycluster-01% bash kmip_before_reboot_test.sh | tee kmip_before_reboot_test.txt

Please enter key server name: KeyControl
Please enter key server version: 10.4.3
Please enter whether this is a clustered key-server config (yes or no): no
Executing script kmip_before_reboot_test - version 2.3
Testing DOT: NetApp Release 9.16.1P3: Thu Apr 24 02:50:10 UTC 2025 <1O>
 with Key Manager: KeyControl 10.4.3
Tesing with clustered key servers: no
Step 1 - Get local node name
Local node name is mycluster-01
```

```
Step 2 - Get admin vserver name where EKM is configured
Admin vserver name is mycluster
Step 3 - Check if key-servers are registered
Key server is configured and status is available

                Node: mycluster-01
             Vserver: mycluster
     Key Server Port: 5696
 KMIP is operational: true

Key Server           Role           Server Status     Reason
-------------------  ------------   ---------------   ------
XX.XXX.XXX.XX6       primary        available          -

Clustered key servers are not configured as expected
                                                    Step 4 - Turn on logging for key management

284 entries were modified.

Step 5 - Enable KMIP logging for key management

1 entry was modified.

Step 6 - Create data storage aggregate - test_aggr
[Job 161] Job succeeded: DONE

Sleeping for 10 seconds before checking if aggregate was created...
Step 7 - Verify aggregate exists
Aggregate was created successfully.
Step 8 - Create data vserver - test_vserver
[Job 162] Job succeeded:
Vserver creation completed.

Sleeping for 10 seconds before checking if vserver was created...
Step 9 - Verify vserver exists
Vserver was created successfully.
Step 10 - Create 2 encrypted volumes
[Job 163] Job succeeded: Successful

[Job 164] Job succeeded: Successful

Step 11 - Verify encrypted volumes are online
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
test_vserver test_vol_1 test_aggr   online     RW         20MB    18.76MB    1%
test_vserver test_vol_2 test_aggr   online     RW         20MB    18.76MB    1%
2 entries were displayed.

Volume test_vol_1 was created successfully.
Volume test_vol_2 was created successfully.
Step 12 - Run key-manager key query

               Node: mycluster-01
            Vserver: mycluster
        Key Manager: XX.XXX.XXX.XX6:5696
   Key Manager Type: KMIP
 Key Manager Policy: -

Key Tag                               Key Type Encryption   Restored
------------------------------------  -------- ------------ --------
693e2a8f-506b-11f0-be40-0050568b2de8  VEK      XTS-AES-256  true
    Key ID: 000000000000000002000000000005004102ebb412bcc8fdc78e34151553a2f50000000000000000
67c26dfa-506b-11f0-be40-0050568b2de8  VEK      XTS-AES-256  true
    Key ID: 00000000000000000200000000000500bb9c5cba1c36533832e0521d2c2b04c90000000000000000
2 entries were displayed.

Step 13 - Create NSE key
```

```
                        NSE key id is
0000000000000000020000000000010044a2413d1cbeddbe4ec7f520a20b2cf10000000000000000

Step 14 - Get the NSE key

NSE key id is 0000000000000000020000000000010044a2413d1cbeddbe4ec7f520a20b2cf10000000000000000
Step 15 - Run key-manager key query

               Node: mycluster-01
            Vserver: mycluster
        Key Manager: XX.XXX.XXX.XX6:5696
   Key Manager Type: KMIP
 Key Manager Policy: -

Key Tag                               Key Type Encryption   Restored
------------------------------------  -------- ------------ --------
test                                  NSE-AK   AES-256      true
    Key ID: 0000000000000000020000000000010044a2413d1cbeddbe4ec7f520a20b2cf10000000000000000
693e2a8f-506b-11f0-be40-0050568b2de8  VEK      XTS-AES-256  true
    Key ID: 000000000000000002000000000005004102ebb412bcc8fdc78e34151553a2f50000000000000000
67c26dfa-506b-11f0-be40-0050568b2de8  VEK      XTS-AES-256  true
    Key ID: 00000000000000000200000000000500bb9c5cba1c36533832e0521d2c2b04c90000000000000000
3 entries were displayed.

Step 16 - Run debug smdb table cryptomodKeyTable show
                                                     cryptomodKeyTable show output is
node         key-index key-id                                                                           key
key-type    key-digest
------------ --------- --------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------
--------------------- ----------- ----------------------------------------------------------------
mycluster-01 0         00000000000000000200000000000500bb9c5cba1c36533832e0521d2c2b04c90000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000 XTS-AES-256 9dbb47b40182c845ac7d1b3929a69c4f153a093c0b0dc3d39d7c25c3f1738bea
mycluster-01 1         000000000000000002000000000005004102ebb412bcc8fdc78e34151553a2f50000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000 XTS-AES-256 2a9b3355b4a88cca2a7f1d6219de2674c92baeda0ecc78aeea5b8e14931188eb
mycluster-01 2         0000000000000000020000000000010044a2413d1cbeddbe4ec7f520a20b2cf10000000000000000
0000000000000000000000000000000000000000000000000000000000000000
NSE-AK      a571b55cb95a398dd89ea9f10788fb26d72366c66d7ce9d7eb4a69aefed67890
3 entries were displayed.

Step 17 - Check if key-servers are registered
                                             Key server is configured and status is available
Step 18 - Get output of /cfcard/kmip/servers.cfg file

  (system node systemshell)
XX.XXX.XXX.XX6:5696.host=XX.XXX.XXX.XX6
XX.XXX.XXX.XX6:5696.port=5696
XX.XXX.XXX.XX6:5696.trusted_file=/cfcard/kmip/certs/CA.pem
XX.XXX.XXX.XX6:5696.protocol=KMIP1_4
XX.XXX.XXX.XX6:5696.timeout=25
XX.XXX.XXX.XX6:5696.nbio=1
XX.XXX.XXX.XX6:5696.cert_file=/cfcard/kmip/certs/client.crt
XX.XXX.XXX.XX6:5696.key_file=/cfcard/kmip/certs/client.key
XX.XXX.XXX.XX6:5696.ciphers="TLSv1.2:kRSA:!CAMELLIA:!IDEA:!RC2:!RC4:!SEED:!eNULL:!aNULL"
XX.XXX.XXX.XX6:5696.verify=true
XX.XXX.XXX.XX6:5696.netapp_keystore_uuid=559433ba-42e4-11f0-9158-0050568b2de8

Step 19 - Get output of /cfcard/kmip/kmipcmd.log file
                                                     KmipDiscoverVersions succeeded
Step 20 - Turn on AUTOBOOT

  (system node systemshell)

Node: mycluster-01
AUTOBOOT="true"
```

```
1 entry was acted on.

Manually reboot the local node and wait 10 minutes before logging back and in running
kmip_post_reboot_test.sh
```

5. Exit Systemshell.

```
mycluster-01% exit
```

6. Reboot the node.

   Wait 10 minutes before logging back into the cluster.

```
mycluster::*> reboot -node mycluster-01
  (system node reboot)

Warning: Are you sure you want to reboot node "mycluster-01"? {y|n}: y


Connection to xxx.xxx.xxx.xxx closed.
```

5.3. Execute the kmip_post_reboot_test.sh test script

1. Open a command window and remote login into the NetApp ONTAP Cluster Management.
2. Set diagnostics.

```
mycluster::> set diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y

mycluster::*>
```

3. Enter Systemshell.

   Provide the password when prompted.

```
mycluster::*> systemshell -node mycluster-01
  (system node systemshell)
diag@127.0.0.1's password:

Warning:  The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly.  Use this environment
only when directed to do so by support personnel.

mycluster-01%
```

4. Execute the `kmip_post_reboot_test.sh` test script and redirect the output to file `kmip_post_reboot_test.txt`.

```
mycluster-01% bash kmip_post_reboot_test.sh | tee kmip_post_reboot_test.txt

Please enter key server name: KeyControl
Please enter key server version: 10.4.3
Please enter whether this is a clustered key-server config (yes or no): no
Executing script kmip_post_reboot_test - version 2.3
Testing DOT: NetApp Release 9.16.1P3: Thu Apr 24 02:50:10 UTC 2025 <1O>
 with Key Manager: KeyControl 10.4.3
Tesing with clustered key servers: no
Step 1 - Get local node name
Local node name is mycluster-01
Step 2 - Get admin vserver name where EKM is configured
Admin vserver name is mycluster
Step 3 - Check if key-servers are registered
Key server is configured and status is available

                Node: mycluster-01
             Vserver: mycluster
     Key Server Port: 5696
 KMIP is operational: true

Key Server           Role           Server Status     Reason
-------------------  ------------   ---------------   ------
XX.XXX.XXX.XX6       primary        available         -

Clustered key servers are not configured as expected
Step 4 - Post Reboot - Verify encrypted volumes are online
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
test_vserver test_vol_1 test_aggr   online     RW         20MB    18.75MB    1%
test_vserver test_vol_2 test_aggr   online     RW         20MB    18.75MB    1%
2 entries were displayed.

Volume test_vol_1 is online as expected.
Volume test_vol_2 is online as expected.
Step 5 - Post Reboot - Get the NSE key
NSE key id is 0000000000000000020000000000010044a2413d1cbeddbe4ec7f520a20b2cf10000000000000000
Step 6 - Post Reboot - Run key-manager key query

               Node: mycluster-01
            Vserver: mycluster
        Key Manager: XX.XXX.XXX.XX6:5696
   Key Manager Type: KMIP
 Key Manager Policy: -

Key Tag                               Key Type Encryption   Restored
------------------------------------  -------- ------------ --------
test                                  NSE-AK   AES-256      true
    Key ID: 0000000000000000020000000000010044a2413d1cbeddbe4ec7f520a20b2cf10000000000000000
693e2a8f-506b-11f0-be40-0050568b2de8  VEK      XTS-AES-256  true
    Key ID: 000000000000000002000000000005004102ebb412bcc8fdc78e34151553a2f50000000000000000
67c26dfa-506b-11f0-be40-0050568b2de8  VEK      XTS-AES-256  true
    Key ID: 00000000000000000200000000000500bb9c5cba1c36533832e0521d2c2b04c90000000000000000
3 entries were displayed.

Step 7 - Post Reboot - Run debug smdb table cryptomodKeyTable show
cryptomodKeyTable show output is
node         key-index key-id                                                                            key
key-type key-digest
------------ --------- --------------------------------------------------------------------------------
---------------------------------------------------------------- --------
----------------------------------------------------------------
```

```
mycluster-01 0         00000000000000000200000000000100 44a2413d1cbeddbe4ec7f520a20b2cf10000000000000000
0000000000000000000000000000000000000000000000000000000000000000 NSE-AK
a571b55cb95a398dd89ea9f10788fb26d72366c66d7ce9d7eb4a69aefed67890
mycluster-01 1         000000000000000002000000000005004102ebb412bcc8fdc78e34151553a2f50000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000 XTS-AES-256 2a9b3355b4a88cca2a7f1d6219de2674c92baeda0ecc78aeea5b8e14931188eb
mycluster-01 2         00000000000000000200000000000500bb9c5cba1c36533832e0521d2c2b04c90000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000 XTS-AES-256 9dbb47b40182c845ac7d1b3929a69c4f153a093c0b0dc3d39d7c25c3f1738bea
3 entries were displayed.

Step 8 - Post Reboot - Get output of /cfcard/kmip/servers.cfg file

  (system node systemshell)
XX.XXX.XXX.XX6:5696.host=XX.XXX.XXX.XX6
XX.XXX.XXX.XX6:5696.port=5696
XX.XXX.XXX.XX6:5696.trusted_file=/cfcard/kmip/certs/CA.pem
XX.XXX.XXX.XX6:5696.protocol=KMIP1_4
XX.XXX.XXX.XX6:5696.timeout=25
XX.XXX.XXX.XX6:5696.nbio=1
XX.XXX.XXX.XX6:5696.cert_file=/cfcard/kmip/certs/client.crt
XX.XXX.XXX.XX6:5696.key_file=/cfcard/kmip/certs/client.key
XX.XXX.XXX.XX6:5696.ciphers="TLSv1.2:kRSA:!CAMELLIA:!IDEA:!RC2:!RC4:!SEED:!eNULL:!aNULL"
XX.XXX.XXX.XX6:5696.verify=true
XX.XXX.XXX.XX6:5696.netapp_keystore_uuid=559433ba-42e4-11f0-9158-0050568b2de8

Step 9 - Post Reboot - Compare /cfcard/kmip/servers.cfg files
The /cfcard/kmip/servers.cfg output before reboot is the same after rebooting
Step 10 - Post Reboot - Delete the NSE key


Step 11 - Post Reboot - Delete the encrypted volumes

[Job 167] Job succeeded: Successful
[Job 168] Job succeeded: Successful
2 entries were acted on.

Step 12 - Post Reboot - Delete the data vserver - test_vserver
[Job 169]
Step 13 - Post Reboot - Delete the data aggregate - test_aggr
[Job 171] Job succeeded: DONE

Step 14 - Turn off logging for key management

284 entries were modified.

Step 15 - Enable KMIP logging for key management

1 entry was modified.

Step 16 - Post Reboot - Verify no keys are observed in key query
No keys are on the cluster as expected.
```

5. Exit Systemshell.

```
mycluster-01% exit
```

5.4. Enable FIPS mode

1. Open a command window and remote login into the NetApp ONTAP Cluster

Management.

2. Set diagnostics.

```
mycluster::> set diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y

mycluster::*>
```

3. Enable FIPS mode.

```
mycluster::*> security config modify -interface SSL -is-fips-enabled true

Warning: This command will enable FIPS compliance and can potentially cause some non-compliant components
to fail.
         MetroCluster and Vserver DR require FIPS to be enabled on both sites in order to be compatible. An
SNMP users
         or SNMP traphosts that are non-compliant to FIPS will be deleted automatically. An SNMPv1 user,
SNMPv2c user
         or SNMPv3 user (with none or MD5 as authentication protocol or none or DES as encryption protocol
or both) is
         non-compliant to FIPS. An SNMPv1 traphost or SNMPv3 traphost (configured with an SNMPv3 user non-
compliant to
         FIPS) is non-compliant to FIPS.
Do you want to continue? {y|n}: y
```

4. Reboot all nodes in the cluster.

   Wait 10 minutes before logging back into the cluster.

```
mycluster::*> reboot -node *
  (system node reboot)

Warning: Are you sure you want to reboot node "mycluster-01"? {y|n}: Y
1 entry was acted on.


Connection to xx.xxx.xxx.xxx closed.
```

5. Log back into the NetApp ONTAP Cluster Management.
6. Set diagnostics.

```
mycluster::> set diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y

mycluster::*>
```

7. Verify FIPS mode is enabled.

```
mycluster::*> security config show
```

```
Cluster    Supported
FIPS Mode  Protocols Supported Cipher Suites
---------- --------- -----------------------------------------------------------
true       TLSv1.3,  TLS_RSA_WITH_AES_128_CCM, TLS_RSA_WITH_AES_128_CCM_8,
           TLSv1.2   TLS_RSA_WITH_AES_128_GCM_SHA256,
                     TLS_RSA_WITH_AES_128_CBC_SHA,
                     TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CCM,

 ...


                     TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA,
                     TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA,
                     TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA,
                     TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384
```

5.5. Execute the before and post test scripts a second time

1. Open a command window and remote login into the NetApp ONTAP Cluster Management.
2. Set diagnostics.

```
mycluster::> set diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y

mycluster::*>
```

3. Enter Systemshell.

   Provide the password when prompted.

```
mycluster::*> systemshell -node mycluster-01
  (system node systemshell)
diag@127.0.0.1's password:

Warning:  The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly.  Use this environment
only when directed to do so by support personnel.

mycluster-01%
```

4. Execute the `kmip_before_reboot_test.sh` test script and redirect the output to file `kmip_before_reboot_test_fips.txt`.

```
mycluster-01% bash kmip_before_reboot_test.sh | tee kmip_before_reboot_test_fips.txt

Please enter key server name: KeyControl
Please enter key server version: 10.4.3
Please enter whether this is a clustered key-server config (yes or no): no
Executing script kmip_before_reboot_test - version 2.3
Testing DOT: NetApp Release 9.16.1P3: Thu Apr 24 02:50:10 UTC 2025 <1O>
 with Key Manager: KeyControl 10.4.3
```

```
Tesing with clustered key servers: no
Step 1 - Get local node name
Local node name is mycluster-01
Step 2 - Get admin vserver name where EKM is configured
Admin vserver name is mycluster
Step 3 - Check if key-servers are registered
Key server is configured and status is available

                Node: mycluster-01
             Vserver: mycluster
     Key Server Port: 5696
 KMIP is operational: true

Key Server           Role           Server Status     Reason
-------------------  ------------   ---------------   ------
XX.XXX.XXX.XX6       primary        available         -

Clustered key servers are not configured as expected
Step 4 - Turn on logging for key management

284 entries were modified.

Step 5 - Enable KMIP logging for key management

1 entry was modified.

Step 6 - Create data storage aggregate - test_aggr
[Job 177] Job succeeded: DONE

Sleeping for 10 seconds before checking if aggregate was created...
Step 7 - Verify aggregate exists
Aggregate was created successfully.
Step 8 - Create data vserver - test_vserver
[Job 178] Sleeping for 10 seconds before checking if vserver was created...
[Job 178] Job succeeded:
Vserver creation completed.

Step 9 - Verify vserver exists
Vserver was created successfully.
Step 10 - Create 2 encrypted volumes
[Job 179] Job succeeded: Successful

[Job 180] Job succeeded: Successful

Step 11 - Verify encrypted volumes are online
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
test_vserver test_vol_1 test_aggr   online     RW         20MB    18.75MB    1%
test_vserver test_vol_2 test_aggr   online     RW         20MB    18.76MB    1%
2 entries were displayed.

Volume test_vol_1 was created successfully.
Volume test_vol_2 was created successfully.
Step 12 - Run key-manager key query

               Node: mycluster-01
            Vserver: mycluster
        Key Manager: XX.XXX.XXX.XX6:5696
   Key Manager Type: KMIP
 Key Manager Policy: -

Key Tag                               Key Type Encryption   Restored
------------------------------------  -------- ------------ --------
40f653bd-5103-11f0-9478-0050568b2de8  VEK      XTS-AES-256  true
    Key ID: 00000000000000000020000000000500bc9dbeec5db9a3106c920c4c65af30860000000000000000
3ee2ce15-5103-11f0-9478-0050568b2de8  VEK      XTS-AES-256  true
    Key ID: 00000000000000000020000000000500cdbdc1f1aad97bdeff91cecf93c4a7910000000000000000
```

```
2 entries were displayed.

Step 13 - Create NSE key
NSE key id is  000000000000000002000000000001007e8c53f2b60ce82be0cea3e55085fa140000000000000000
Step 14 - Get the NSE key
                         NSE key id is
000000000000000002000000000001007e8c53f2b60ce82be0cea3e55085fa140000000000000000
Step 15 - Run key-manager key query

               Node: mycluster-01
            Vserver: mycluster
        Key Manager: XX.XXX.XXX.XX6:5696
   Key Manager Type: KMIP
 Key Manager Policy: -

Key Tag                               Key Type Encryption   Restored
------------------------------------  -------- ------------ --------
test                                  NSE-AK   AES-256      true
    Key ID: 000000000000000002000000000001007e8c53f2b60ce82be0cea3e55085fa140000000000000000
40f653bd-5103-11f0-9478-0050568b2de8  VEK      XTS-AES-256  true
    Key ID: 00000000000000000200000000000500bc9dbeec5db9a3106c920c4c65af30860000000000000000
3ee2ce15-5103-11f0-9478-0050568b2de8  VEK      XTS-AES-256  true
    Key ID: 00000000000000000200000000000500cdbdc1f1aad97bdeff91cecf93c4a7910000000000000000
3 entries were displayed.

Step 16 - Run debug smdb table cryptomodKeyTable show
                                                     cryptomodKeyTable show output is
node         key-index key-id                                                                           key
key-type    key-digest
------------ --------- --------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------
--------------------- ----------- ----------------------------------------------------------------
mycluster-01 0         00000000000000000200000000000500cdbdc1f1aad97bdeff91cecf93c4a7910000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000 XTS-AES-256 e6015f0ec69b1caa10b7c1e68a2f04dfc144b2884819ecb2fd64fd5b765c0198
mycluster-01 1         00000000000000000200000000000500bc9dbeec5db9a3106c920c4c65af30860000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000 XTS-AES-256 4a0c5ab1545b9bba62791cb3e7ba42bc7e295d002cb8a91072c57e54a3632a56
mycluster-01 2         000000000000000002000000000001007e8c53f2b60ce82be0cea3e55085fa140000000000000000
0000000000000000000000000000000000000000000000000000000000000000
NSE-AK      ccdb85becaaa34f3301748938ce9d6ea63dfe809f99fe70cd7867dc272654a87
3 entries were displayed.

Step 17 - Check if key-servers are registered
                                             Key server is configured and status is available
                                                                                             Step 18 - Get
output of /cfcard/kmip/servers.cfg file

  (system node systemshell)
XX.XXX.XXX.XX6:5696.host=XX.XXX.XXX.XX6
XX.XXX.XXX.XX6:5696.port=5696
XX.XXX.XXX.XX6:5696.trusted_file=/cfcard/kmip/certs/CA.pem
XX.XXX.XXX.XX6:5696.protocol=KMIP1_4
XX.XXX.XXX.XX6:5696.timeout=25
XX.XXX.XXX.XX6:5696.nbio=1
XX.XXX.XXX.XX6:5696.cert_file=/cfcard/kmip/certs/client.crt
XX.XXX.XXX.XX6:5696.key_file=/cfcard/kmip/certs/client.key
XX.XXX.XXX.XX6:5696.ciphers="TLSv1.2+FIPS:!eNULL:!aNULL"
XX.XXX.XXX.XX6:5696.verify=true
XX.XXX.XXX.XX6:5696.netapp_keystore_uuid=559433ba-42e4-11f0-9158-0050568b2de8

Step 19 - Get output of /cfcard/kmip/kmipcmd.log file
                                                     KmipDiscoverVersions succeeded
Step 20 - Turn on AUTOBOOT

  (system node systemshell)
```

```
Node: mycluster-01
AUTOBOOT="true"
1 entry was acted on.

Manually reboot the local node and wait 10 minutes before logging back and in running
kmip_post_reboot_test.sh
```

5. Exit Systemshell.

```
mycluster-01% exit
```

6. Reboot the node.

   Wait 10 minutes before logging back into the cluster.

```
mycluster::*> reboot -node mycluster-01
  (system node reboot)

Warning: Are you sure you want to reboot node "mycluster-01"? {y|n}: y


Connection to xxx.xxx.xxx.xxx closed.
```

7. Log back into the NetApp ONTAP Cluster Management.
8. Set diagnostics.

```
mycluster::> set diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y

mycluster::*>
```

9. Enter Systemshell. Provide the password when prompted.

```
mycluster::*> systemshell -node mycluster-01
  (system node systemshell)
diag@127.0.0.1's password:

Warning:  The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly.  Use this environment
only when directed to do so by support personnel.

mycluster-01%
```

10. Execute the `kmip_post_reboot_test.sh` test script and redirect the output to file `kmip_post_reboot_test_fips.txt`.

```
mycluster-01% bash kmip_post_reboot_test.sh | tee kmip_post_reboot_test_fips.txt

Please enter key server name: KeyControl
Please enter key server version: 10.4.3
Please enter whether this is a clustered key-server config (yes or no): no
Executing script kmip_post_reboot_test - version 2.3
Testing DOT: NetApp Release 9.16.1P3: Thu Apr 24 02:50:10 UTC 2025 <1O>
 with Key Manager: KeyControl 10.4.3
Tesing with clustered key servers: no
Step 1 - Get local node name
Local node name is mycluster-01
Step 2 - Get admin vserver name where EKM is configured
Admin vserver name is mycluster
Step 3 - Check if key-servers are registered
Key server is configured and status is available

                Node: mycluster-01
             Vserver: mycluster
     Key Server Port: 5696
 KMIP is operational: true

Key Server           Role           Server Status     Reason
-------------------  ------------   ---------------   ------
XX.XXX.XXX.XX6       primary        available         -

Clustered key servers are not configured as expected
Step 4 - Post Reboot - Verify encrypted volumes are online
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
test_vserver test_vol_1 test_aggr   online     RW         20MB    18.75MB    1%
test_vserver test_vol_2 test_aggr   online     RW         20MB    18.75MB    1%
2 entries were displayed.

Volume test_vol_1 is online as expected.
Volume test_vol_2 is online as expected.
Step 5 - Post Reboot - Get the NSE key
NSE key id is 000000000000000002000000000001007e8c53f2b60ce82be0cea3e55085fa140000000000000000
                                                                                              Step 6 - Post
Reboot - Run key-manager key query

               Node: mycluster-01
            Vserver: mycluster
        Key Manager: XX.XXX.XXX.XX6:5696
   Key Manager Type: KMIP
 Key Manager Policy: -

Key Tag                               Key Type Encryption   Restored
------------------------------------  -------- ------------ --------
test                                  NSE-AK   AES-256      true
    Key ID: 000000000000000002000000000001007e8c53f2b60ce82be0cea3e55085fa140000000000000000
40f653bd-5103-11f0-9478-0050568b2de8  VEK      XTS-AES-256  true
    Key ID: 00000000000000000200000000000500bc9dbeec5db9a3106c920c4c65af30860000000000000000
3ee2ce15-5103-11f0-9478-0050568b2de8  VEK      XTS-AES-256  true
    Key ID: 00000000000000000200000000000500cdbdc1f1aad97bdeff91cecf93c4a7910000000000000000
3 entries were displayed.

Step 7 - Post Reboot - Run debug smdb table cryptomodKeyTable show
cryptomodKeyTable show output is
node         key-index key-id                                                                           key
key-type key-digest
------------ --------- --------------------------------------------------------------------------------
---------------------------------------------------------------- --------
----------------------------------------------------------------
mycluster-01 0         000000000000000002000000000001007e8c53f2b60ce82be0cea3e55085fa140000000000000000
0000000000000000000000000000000000000000000000000000000000000000 NSE-AK
ccdb85becaaa34f3301748938ce9d6ea63dfe809f99fe70cd7867dc272654a87
mycluster-01 1         00000000000000000200000000000500cdbdc1f1aad97bdeff91cecf93c4a7910000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000 XTS-AES-256 e6015f0ec69b1caa10b7c1e68a2f04dfc144b2884819ecb2fd64fd5b765c0198
mycluster-01 2         00000000000000000200000000000500bc9dbeec5db9a3106c920c4c65af30860000000000000000
```

```
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000 XTS-AES-256 4a0c5ab1545b9bba62791cb3e7ba42bc7e295d002cb8a91072c57e54a3632a56
3 entries were displayed.

Step 8 - Post Reboot - Get output of /cfcard/kmip/servers.cfg file

  (system node systemshell)
XX.XXX.XXX.XX6:5696.host=XX.XXX.XXX.XX6
XX.XXX.XXX.XX6:5696.port=5696
XX.XXX.XXX.XX6:5696.trusted_file=/cfcard/kmip/certs/CA.pem
XX.XXX.XXX.XX6:5696.protocol=KMIP1_4
XX.XXX.XXX.XX6:5696.timeout=25
XX.XXX.XXX.XX6:5696.nbio=1
XX.XXX.XXX.XX6:5696.cert_file=/cfcard/kmip/certs/client.crt
XX.XXX.XXX.XX6:5696.key_file=/cfcard/kmip/certs/client.key
XX.XXX.XXX.XX6:5696.ciphers="TLSv1.2+FIPS:!eNULL:!aNULL"
XX.XXX.XXX.XX6:5696.verify=true
XX.XXX.XXX.XX6:5696.netapp_keystore_uuid=559433ba-42e4-11f0-9158-0050568b2de8

Step 9 - Post Reboot - Compare /cfcard/kmip/servers.cfg files
The /cfcard/kmip/servers.cfg output before reboot is the same after rebooting
Step 10 - Post Reboot - Delete the NSE key


Step 11 - Post Reboot - Delete the encrypted volumes

[Job 184] Job succeeded: Successful
[Job 185] Job succeeded: Successful
2 entries were acted on.

Step 12 - Post Reboot - Delete the data vserver - test_vserver
[Job 186]
Step 13 - Post Reboot - Delete the data aggregate - test_aggr
[Job 188] Job succeeded: DONE

Step 14 - Turn off logging for key management

284 entries were modified.

Step 15 - Enable KMIP logging for key management

1 entry was modified.

Step 16 - Post Reboot - Verify no keys are observed in key query
No keys are on the cluster as expected.
```

11. Copy the test script output files to a server of your choice.

    Provide the password when prompted.

```
mycluster-01% scp *.txt root@xxx.xxx.xxx.xxx:/root/Downloads/.

kmip_before_reboot_test.txt
100%   16KB   4.9MB/s   00:00
kmip_before_reboot_test_fips.txt
100%   14KB   7.3MB/s   00:00
kmip_post_reboot_test.txt
100%   14KB   9.5MB/s   00:00
kmip_post_reboot_test_fips.txt
100%   14KB  15.0MB/s   00:00
SSH terminating : scp.c : main : 690,errs = 0.
```

12. Send these output files to NetApp for verification.

5.6. Verify FIPS mode is unchanged after reboot

1. Exit Systemshell.

```
mycluster-01% exit
```

2. Disable FIPS mode.

```
mycluster::*> security config modify -interface SSL -is-fips-enabled false
```

3. Reboot all nodes in the cluster.

```
mycluster::*> reboot -node *
  (system node reboot)

Warning: Are you sure you want to reboot node "mycluster-01"? {y|n}: Y
1 entry was acted on.


Connection to xx.xxx.xxx.xxx closed.
```

4. Log back into the NetApp ONTAP Cluster Management.
5. Set diagnostics.

```
mycluster::> set diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y

mycluster::*>
```

6. Verify FIPS mode is disabled on the cluster.

```
mycluster::*> security config show
Cluster    Supported
FIPS Mode  Protocols Supported Cipher Suites
---------- --------- -----------------------------------------------------------
false      TLSv1.3,  TLS_RSA_WITH_AES_128_CCM, TLS_RSA_WITH_AES_128_CCM_8,
           TLSv1.2   TLS_RSA_WITH_AES_128_GCM_SHA256,
                     TLS_RSA_WITH_AES_128_CBC_SHA,
                     TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CCM,

 ...

                     TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA,
                     TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA,
                     TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384,
                     TLS_CHACHA20_POLY1305_SHA256
```

Chapter 6. Integrating with an HSM

For guidance on integrating the KeyControl with a Hardware Security Module (HSM), consult with your HSM vendor. If you are using an Entrust nShield HSM, refer to the **Entrust KeyControl Vault nShield HSM Integration Guide** available at Entrust documentation library.

Chapter 7. Additional resources and related products

7.1. nShield Connect

7.2. nShield as a Service

7.3. KeyControl

7.4. Entrust products

7.5. nShield product documentation