



NetApp ONTAP and Entrust KeyControl

Integration Guide

2025-02-06

Table of Contents

1. Introduction	1
1.1. Product configuration	1
1.2. Requirements	1
2. Deploy KeyControl	2
2.1. Deploy a KeyControl cluster	2
2.2. Create a KMIP Vault in KeyControl	2
2.3. KMIP server settings	6
2.4. Install a signed certificate from your local root CA in the KeyControl cluster	7
2.5. Create the KeyControl client certificate bundle	11
3. Deploy NetApp Simulate ONTAP	14
4. Integrate KeyControl with NetApp ONTAP	15
4.1. Install the KeyControl client bundle into NetApp ONTAP	15
4.2. Setup KeyControl as the external KMIP server	16
5. Test integration	17
5.1. Load the test scripts into NetApp ONTAP	17
5.2. Execute the kmip_before_reboot_test.sh test script	18
5.3. Execute the kmip_post_reboot_test.sh test script	21
5.4. Enable FIPS mode	24
5.5. Execute the before and post test scripts a second time	25
5.6. Verify FIPS mode is unchanged after reboot	32
6. Integrating with an HSM	33
7. Additional resources and related products	34
7.1. nShield Connect	34
7.2. nShield as a Service	34
7.3. KeyControl	34
7.4. Entrust products	34
7.5. nShield product documentation	34

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	9.14.1.P10
Entrust KeyControl	10.4.1 and 10.3.1

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.

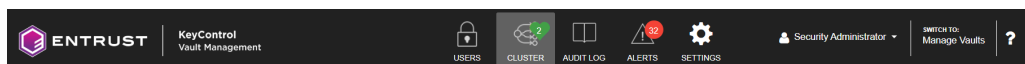
The following sections describe how to create the KeyControl KMIP Vault and certificates.

2.2. Create a KMIP Vault in KeyControl

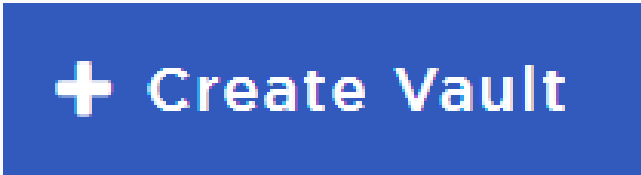
The KeyControl Vault appliance supports different type of vaults that can be used by all type of applications. This section describes how to create a KMIP Vault in the KeyControl Vault Server.

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

Create Vault **Cancel**

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



 [Copy](#)

User Name



 [Copy](#)

Temporary Password



 [Copy](#)

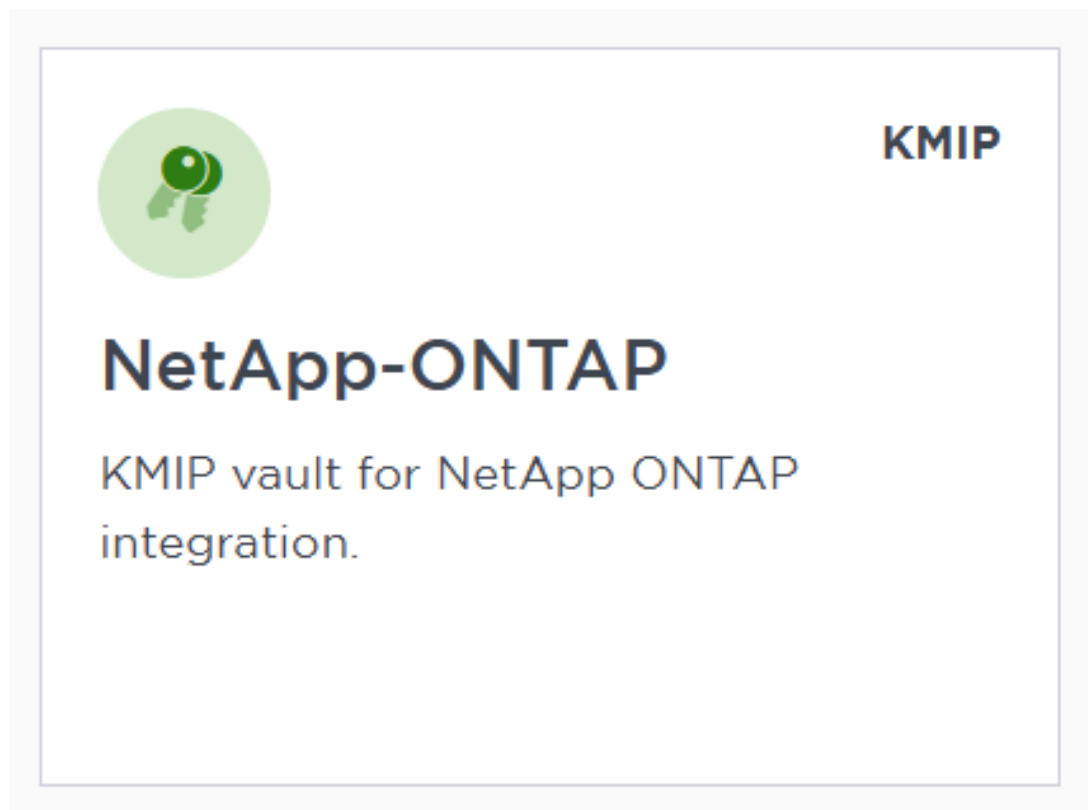
[Close](#)



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:



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

Actions

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-GCM-SHA384,DHE-PSK-AES256-CCM,DHE-PSK-AES128-GCM-SHA256,DHE-PSK-AES128-CCM

Certificate Types

☒ Default
☐ Custom

Apply

Cancel

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 *

Locality *

State *

Subject Alternative Names *
Define all the domain names and IP addresses that you want secured by this certificate

kcv-1041-node-1.interop.local x

kcv-1041-node-2.interop.local x

10.10.10.10 x

10.10.10.11 x

Press enter or tab after each value

Key Size *

4096

Country *

Organization *

Organization Unit *

Cancel

Download

Submit

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

NetApp ONTAP and Entrust KeyControl

8/34

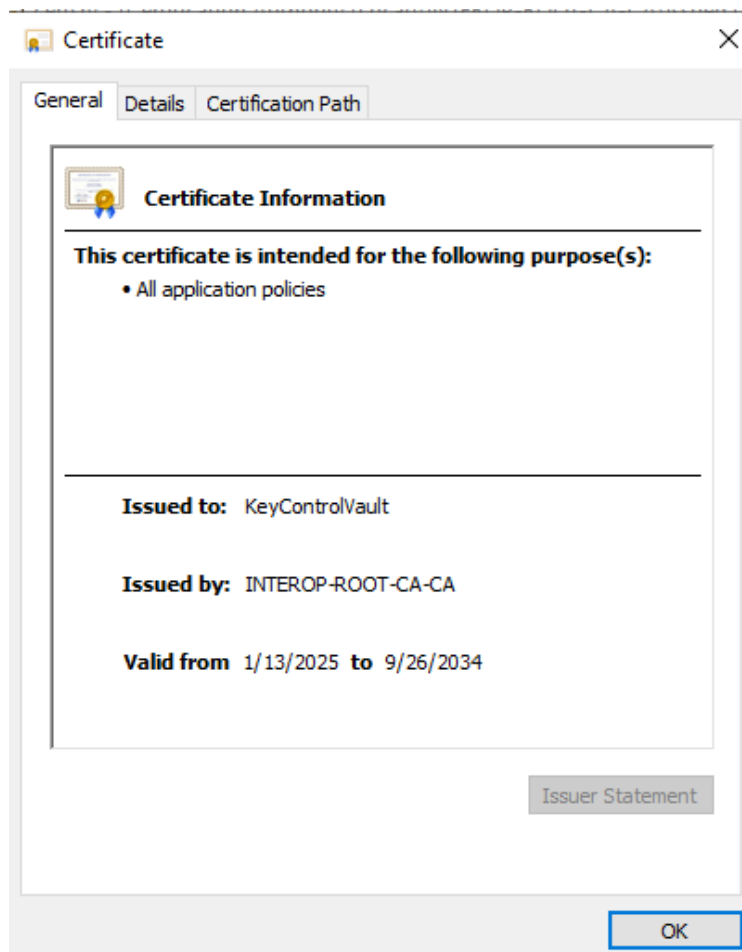
downloads folder.

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:



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-----
MIIDFTCaAA2gAwbbbgIQepb3APptddd0v11kVoDg1jANBgkqhkiG9w0BAQsFADAd
.
.
.
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 **rootcert.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.

The screenshot shows the 'Certificate Types' configuration page in the KeyControl UI. It features two radio buttons: 'Default' and 'Custom', with 'Custom' selected. Below this, there are two sections for certificates. The first section, 'SSL Certificate*', has a 'Browse' button and a 'Preview' button showing 'keycontrolvault.cer'. The second section, 'CA Certificate*', also has a 'Browse' button and a 'Preview' button showing 'rootcert.pem.cer'. Below these sections is a question: 'Do you want to use this CA certificate to verify KMIP client certificate?' with 'Yes' and 'No' radio buttons, where 'No' is selected. Further down, there is a 'Private Key' section with a 'Browse' button, and a 'Password' section with an empty text input field. At the bottom, there are 'Apply' and 'Cancel' buttons.

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

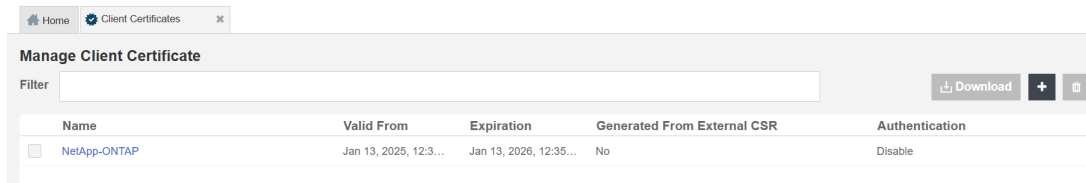
Certificate Name *

Certificate Expiration *

Certificate Signing Request (CSR)

☐ Encrypt Certificate Bundle

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



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

```
unzip NetApp-ONTAP_2025-01-13-17-37-32.zip
Archive: NetApp-ONTAP_2025-01-13-17-37-32.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](#)
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 per 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-----
MIIIEaDCCA1CgAwIBAgIEfhphJTANBgkqhkiG9w0BAQsFADBXMQswCQYDVQQGEwJV
.
.
.
Ib/yNAFPx5aYqVv7b1RKcNTUYnhn/dyGPUuVQgrtQRKx6tQUbLhIHW/z8qMzJf/w
hnQE/yaXuH13ofbRJ9Q9IxtYz4jtdLuEXQkVxUvu+weqYz6l+jl+7CeFv02yhjSd
bX8bICgNVFhPjoxY7/BLFCaBDhsnhYp09Wr1uXh6TxbmnxSwYipZLzBGpnagL47V
RMM5ZEqIjkwJh1CurTN5JuLFZPYV9zNNHKKEiQ==
-----END CERTIFICATE-----

Please enter Private Key: Press <Enter> when done
-----BEGIN PRIVATE KEY-----
MIIJQwIBADANBgkqhkiG9w0BAQEFAASCCS0wggkpAgEAAoICAQCj7+BP2YfDiUiW
.
.
.
QiHLPgQodyWE0z050+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
```

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.
```



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: 10.4.1
```

```

Executing script kmip_before_reboot_test - version 2.0
Testing DOT: NetApp Release 9.14.1P10: Thu Nov 28 12:32:16 UTC 2024 <10>
  with Key Manager: KeyControl 10.4.1
Step 1 - Get local node name
Local node name is mycluster-01
Step 2 - Check if key-servers are registered
Key server is configured and status is available
Step 3 - Turn on logging for key management

216 entries were modified.

Step 4 - Create a KMIP log file

Step 5 - Create data storage aggregate - test_aggr
[Job 32] Job succeeded: DONE

Sleeping for 10 seconds before checking if aggregate was created...
Step 6 - Verify aggregate exists
Aggregate was created successfully.
Step 7 - Create data vserver - test_vserver
[Job 33] Sleeping for 10 seconds before checking if vserver was created...
[Job 33] Job succeeded:
Vserver creation completed.

Step 8 - Verify vserver exists
Vserver was created successfully.
Step 9 - Create 2 encrypted volumes
[Job 34] Job succeeded: Successful

[Job 35] Job succeeded: Successful

Step 10 - Verify encrypted volumes are online

```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used%
test_vserver	test_vol_1	test_aggr	online	RW	20MB	18.77MB	1%
test_vserver	test_vol_2	test_aggr	online	RW	20MB	18.79MB	1%

```

2 entries were displayed.

Volume test_vol_1 was created successfully.
Volume test_vol_2 was created successfully.
Step 11 - Run key-manager key query

      Node: mycluster-01
      Vserver: mycluster
      Key Manager: xx.xxx.xxx.xxx:5696
      Key Manager Type: KMIP
      Key Manager Policy: -

Key Tag                                Key Type Encryption  Restored
-----
09f0e909-dce0-11ef-8bd5-0050568b2de8  VEK      XTS-AES-256  true
      Key ID: 000000000000000020000000000500903f4e84f2b556f26f515687f506a7b30000000000000000
06ac08eb-dce0-11ef-8bd5-0050568b2de8  VEK      XTS-AES-256  true
      Key ID: 000000000000000020000000000500d8407559fbc352b558db71f7a73f4da0000000000000000

      Node: mycluster-01
      Vserver: mycluster
      Key Manager: xx.xxx.xxx.xxx:5696
      Key Manager Type: KMIP
      Key Manager Policy: -

Key Tag                                Key Type Encryption  Restored
-----
09f0e909-dce0-11ef-8bd5-0050568b2de8  VEK      XTS-AES-256  true
      Key ID: 000000000000000020000000000500903f4e84f2b556f26f515687f506a7b30000000000000000
06ac08eb-dce0-11ef-8bd5-0050568b2de8  VEK      XTS-AES-256  true

```

Key ID: 000000000000000020000000000500d84075559fbc352b558db71f7a73f4da0000000000000000
4 entries were displayed.

Step 12 - Create NSE key

NSE key id is 00000000000000000200000000001008e2e389af67414b030ecc5315f6580840000000000000000

Step 13 - Get the NSE key

NSE key id is displayed.

Step 14 - Run key-manager key query

Node: mycluster-01

```
Vserver: mycluster
```

Key Manager: xx.xxx.xxx.xxx:5696

Key Manager Type: KMIP

Key Manager Policy: -

Key Tag	Key Type	Encryption	Restored
test	NSE-AK	AES-256	true
Key ID: 0000000000000000200000000001008e2e389af67414b030ecc5315f658084000000000000000			
09f0e909-dce0-11ef-8bd5-0050568b2de8	VEK	XTS-AES-256	true
Key ID: 000000000000000020000000000050903f4e84f2b556f26f515687f506a7b30000000000000000			
06ac08eb-dce0-11ef-8bd5-0050568b2de8	VEK	XTS-AES-256	true
Key ID: 000000000000000020000000000500d84075559fbc352b558db71f7a73f4da0000000000000000			

Node: mycluster-01

```
Vserver: mycluster
```

Key Manager: xx.xxx.xxx.xxx:5696

Key Manager Type: KMIP

Key Manager Policy: -

Key Tag	Key Type	Encryption	Restored
test	NSE-AK	AES-256	true
Key ID: 0000000000000000200000000001008e2e389af67414b030ecc5315f658084000000000000000009f0e909-dce0-11ef-8bd5-0050568b2de8			
VEK	XTS-AES-256	true	
Key ID: 000000000000000020000000000500903f4e84f2b556f26f515687f506a7b3000000000000000006ac08eb-dce0-11ef-8bd5-0050568b2de8			
VEK	XTS-AES-256	true	
Key ID: 000000000000000020000000000500d8407559fbc352b558db71f7a73f4da00000000000000000			

6 entries were displayed.

Step 15 - Run `debug smdb table cryptomodKeyTable show`

cryptomodKeyTable show output is

node	key-index	key-id	key
key-type	key-digest		

[illegible]

Step 16 - Check if key-servers are registered

Key server is configured and status is available

Step 17 - Get output of /cfc card/kmip/servers.cfg file

```
(system node systemshell)
xx.xxx.xxx.xxx:5696.host=xx.xxx.xxx.xxx
xx.xxx.xxx.xxx:5696.port=5696
xx.xxx.xxx.xxx:5696.trusted_file=/cfcard/kmip/certs/CA.pem
xx.xxx.xxx.xxx:5696.protocol=KMIP 4
```

```
xx.xxx.xxx.xxx:5696.timeout=25
xx.xxx.xxx.xxx:5696.nbio=1
xx.xxx.xxx.xxx:5696.cert_file=/cfcard/kmip/certs/client.crt
xx.xxx.xxx.xxx:5696.key_file=/cfcard/kmip/certs/client.key
xx.xxx.xxx.xxx:5696.ciphers="TLSv1.2:kRSA:!CAMELLIA:!IDEA:!RC2:!RC4:!SEED:!eNULL:!aNULL"
xx.xxx.xxx.xxx:5696.verify=true
```

```
xx.xxx.xxx.xxx:5696.host=xx.xxx.xxx.xxx
xx.xxx.xxx.xxx:5696.port=5696
xx.xxx.xxx.xxx:5696.trusted_file=/cfcard/kmip/certs/CA.pem
xx.xxx.xxx.xxx:5696.protocol=KMIP1_4
xx.xxx.xxx.xxx:5696.timeout=25
xx.xxx.xxx.xxx:5696.nbio=1
xx.xxx.xxx.xxx:5696.cert_file=/cfcard/kmip/certs/client.crt
xx.xxx.xxx.xxx:5696.key_file=/cfcard/kmip/certs/client.key
xx.xxx.xxx.xxx:5696.ciphers="TLSv1.2:kRSA:!CAMELLIA:!IDEA:!RC2:!RC4:!SEED:!eNULL:!aNULL"
xx.xxx.xxx.xxx:5696.verify=true
```

Step 18 - Get output of /cfcard/kmip/kmipcmd.log file
KmipDiscoverVersions succeeded

Step 19 - 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: 10.4.1
Executing script kmip_post_reboot_test - version 2.0
Testing DOT: NetApp Release 9.14.1P10: Thu Nov 28 12:32:16 UTC 2024 <10>
  with Key Manager: KeyControl 10.4.1
Step 1 - Get local node name
Local node name is mycluster-01
Step 2 - Check if key-servers are registered
Key server is configured and status is available
Step 3 - 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        18.76MB      1%
test_vserver test_vol_2 test_aggr  online    RW          20MB        18.76MB      1%
2 entries were displayed.

Volume test_vol_1 is online as expected.
                                     Volume test_vol_2 is online as expected.

Step 4 - Post Reboot - Get the NSE key
NSE key id is 000000000000000002000000000001008e2e389af67414b030ecc5315f658084000000000000000
Step 5 - 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: 000000000000000002000000000001008e2e389af67414b030ecc5315f658084000000000000000
09f0e909-dce0-11ef-8bd5-0050568b2de8  VEK        XTS-AES-256  true
Key ID: 00000000000000000200000000000500903f4e84f2b556f26f515687f506a7b30000000000000000
06ac08eb-dce0-11ef-8bd5-0050568b2de8  VEK        XTS-AES-256  true
```

```
Node: mycluster-01
Vserver: mycluster
Key Manager: xx.xxx.xxx.xx7:5696
Key Manager Type: KMIP
Key Manager Policy: -
```

```
Step 6 - Post Reboot - Run debug smdb table cryptomodKeyTable show
cryptomodKeyTable show output is
node          key-index key-id                                     key
key-type key-digest
```

```
(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.xx7:5696.host=xx.xxx.xxx.xx7
xx.xxx.xxx.xx7:5696.port=5696
xx.xxx.xxx.xx7:5696.trusted_file=/cfcard/kmip/certs/CA.pem
xx.xxx.xxx.xx7:5696.protocol=KMIP1_4
xx.xxx.xxx.xx7:5696.timeout=25
xx.xxx.xxx.xx7:5696.nbio=1
xx.xxx.xxx.xx7:5696.cert_file=/cfcard/kmip/certs/client.crt
xx.xxx.xxx.xx7:5696.key_file=/cfcard/kmip/certs/client.key
xx.xxx.xxx.xx7:5696.ciphers="TLSv1.2:kRSA:!CAMELLIA:!IDEA:!RC2:!RC4:!SEED:!eNULL:!aNULL"
xx.xxx.xxx.xx7:5696.verify=true
```

Step 10 - Post Reboot - Delete the encrypted volumes

```
[Job 38] Job succeeded: Successful
[Job 39] Job succeeded: Successful
2 entries were acted on.

Step 11 - Post Reboot - Delete the data vserver - test_vserver
[Job 40]
Step 12 - Post Reboot - Delete the data aggregate - test_aggr
[Job 42] Job succeeded: DONE

Step 13 - Turn off logging for key management

216 entries were modified.

Step 14 - Delete a KMIP log file

Step 15 - 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: 10.4.1
Executing script kmip_before_reboot_test - version 2.0
Testing DOT: NetApp Release 9.14.1P10: Thu Nov 28 12:32:16 UTC 2024 <10>
  with Key Manager: KeyControl 10.4.1
Step 1 - Get local node name
Local node name is mycluster-01
Step 2 - Check if key-servers are registered
Key server is configured and status is available
Step 3 - Turn on logging for key management

216 entries were modified.

Step 4 - Create a KMIP log file

Step 5 - Create data storage aggregate - test_aggr
[Job 45] Job succeeded: DONE

Sleeping for 10 seconds before checking if aggregate was created...
Step 6 - Verify aggregate exists
Aggregate was created successfully.
Step 7 - Create data vserver - test_vserver
[Job 46] Sleeping for 10 seconds before checking if vserver was created...
[Job 46] Job succeeded:
Vserver creation completed.

Step 8 - Verify vserver exists
Vserver was created successfully.
Step 9 - Create 2 encrypted volumes
[Job 47] Job succeeded: Successful

[Job 48] Job succeeded: Successful

Step 10 - Verify encrypted volumes are online
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used%
-----	-----	-----	-----	-----	-----	-----	-----

```
test_vserver test_vol_1 test_aggr  online  RW      20MB    18.77MB    1%
test_vserver test_vol_2 test_aggr  online  RW      20MB    18.79MB    1%
2 entries were displayed.
```

Volume test_vol_1 was created successfully.
Volume test_vol_2 was created successfully.
Step 11 - 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
ddb9ecd0-dce2-11ef-a576-0050568b2de8	VEK	XTS-AES-256	true
Key ID: 00000000000000002000000000050041f10f2d23caf84391b6579a45ee8a5f0000000000000000			
dab1e555-dce2-11ef-a576-0050568b2de8	VEK	XTS-AES-256	true
Key ID: 000000000000000020000000000500ef91891b7c136f55c266c1740cc959f90000000000000000			

```
Node: mycluster-01
Vserver: mycluster
Key Manager: xx.xxx.xxx.xx7:5696
Key Manager Type: KMIP
Key Manager Policy: -
```

Key Tag	Key Type	Encryption	Restored
ddb9ecd0-dce2-11ef-a576-0050568b2de8	VEK	XTS-AES-256	true
Key ID: 00000000000000002000000000050041f10f2d23caf84391b6579a45ee8a5f00000000000000000			
dab1e555-dce2-11ef-a576-0050568b2de8	VEK	XTS-AES-256	true
Key ID: 000000000000000020000000000500ef91891b7c136f55c266c1740cc959f90000000000000000			

4 entries were displayed.

Step 12 - Create NSE key
NSE key id is 0000000000000000200000000001008a457ba6bf6e5b7a30ee1280dc56a60500000000000000
Step 13 - Get the NSE key
NSE key id is displayed.
Step 14 - 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: 0000000000000000200000000001008a457ba6bf6e5b7a30ee1280dc56a6050000000000000000			
ddb9ecd0-dce2-11ef-a576-0050568b2de8	VEK	XTS-AES-256	true
Key ID: 00000000000000002000000000050041f10f2d23caf84391b6579a45ee8a5f00000000000000000			
dab1e555-dce2-11ef-a576-0050568b2de8	VEK	XTS-AES-256	true
Key ID: 000000000000000020000000000500ef91891b7c136f55c266c1740cc959f90000000000000000			

```
Node: mycluster-01
Vserver: mycluster
Key Manager: xx.xxx.xxx.xx7:5696
Key Manager Type: KMIP
Key Manager Policy: -
```

Key Tag	Key Type	Encryption	Restored
test	NSE-AK	AES-256	true
Key ID: 0000000000000000200000000001008a457ba6bf6e5b7a30ee1280dc56a6050000000000000000			
ddb9ecd0-dce2-11ef-a576-0050568b2de8	VEK	XTS-AES-256	true

```

Key ID: 000000000000000020000000000050041f10f2d23caf84391b6579a45ee8a5f00000000000000
dable555-dce2-11ef-a576-0050568b2de8 VEK XTS-AES-256 true
Key ID: 0000000000000000200000000000500ef91891b7c136f55c266c1740cc959f9000000000000000
6 entries were displayed.

Step 15 - Run debug smdb table cryptomodKeyTable show
cryptomodKeyTable show output is
node          key-index key-id                                     key
key-type      key-digest
-----
-----
mycluster-01 0          00000000000000000000200000000000500ef91891b7c136f55c266c1740cc959f90000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 XTS-AES-256
0572e25a6da0af547827a838db9cd19a1bc292e31665e2d0d93d15866a8819f3
mycluster-01 1          0000000000000000000020000000000050041f10f2d23caf84391b6579a45ee8a5f000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 XTS-AES-256
cf9d08c00dc49ee483e59185ccbc2d0cb428c2b9b0b5ec916adb9d803a2668a6
mycluster-01 2          000000000000000000002000000000001008a457ba6bf6e5b7a30ee1280dc56a60500000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 NSE-AK
79d2a7fbbe927b0f76291b760e919c90efd183cc5f3f312c568133f58172e30a
3 entries were displayed.

Step 16 - Check if key-servers are registered
Key server is configured and status is available

Step 17 - 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.xx7:5696.host=xx.xxx.xxx.xx7
xx.xxx.xxx.xx7:5696.port=5696
xx.xxx.xxx.xx7:5696.trusted_file=/cfcard/kmip/certs/CA.pem
xx.xxx.xxx.xx7:5696.protocol=KMIP1_4
xx.xxx.xxx.xx7:5696.timeout=25
xx.xxx.xxx.xx7:5696.nbio=1
xx.xxx.xxx.xx7:5696.cert_file=/cfcard/kmip/certs/client.crt
xx.xxx.xxx.xx7:5696.key_file=/cfcard/kmip/certs/client.key
xx.xxx.xxx.xx7:5696.ciphers="TLSv1.2+FIPS:!eNULL:!aNULL"
xx.xxx.xxx.xx7:5696.verify=true

Step 18 - Get output of /cfcard/kmip/kmipcmd.log file
KmpDiscoverVersions succeeded
Step 19 - 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: 10.4.1
Executing script kmip_post_reboot_test - version 2.0
Testing DOT: NetApp Release 9.14.1P10: Thu Nov 28 12:32:16 UTC 2024 <10>
with Key Manager: KeyControl 10.4.1
Step 1 - Get local node name
Local node name is mycluster-01
Step 2 - Check if key-servers are registered
Key server is configured and status is available
Step 3 - 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 18.46MB 2%
test_vserver test_vol_2 test_aggr online RW 20MB 18.47MB 2%
2 entries were displayed.
```

Volume test_vol_1 is online as expected.

Volume test_vol_2 is online as expected.

Step 4 - Post Reboot - Get the NSE key

NSE key id is 00000000000000002000000000001008a457ba6bf6e5b7a30ee1280dc56a6050000000000000000

Step 5 - 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: 0000000000000000200000000001008a457ba6bf6e5b7a30ee1280dc56a60500000000000000			
ddb9ecd0-dce2-11ef-a576-0050568b2de8	VEK	XTS-AES-256	true
Key ID: 00000000000000002000000000050041f10f2d23caf84391b65f79a45ee8a5f00000000000000			
dab1e555-dce2-11ef-a576-0050568b2de8	VEK	XTS-AES-256	true
Key ID: 000000000000000020000000000500ef91891b7c136f55c266c1740cc959f900000000000000			

```
Node: mycluster-01
Vserver: mycluster
Key Manager: xx.xxx.xxx.xx7:5696
Key Manager Type: KMIP
Key Manager Policy: -
```

Key Tag	Key Type	Encryption	Restored
test	NSE-AK	AES-256	true
Key ID: 0000000000000000200000000001008a457ba6bf6e5b7a30ee1280dc56a60500000000000000			
ddb9ecd0-dce2-11ef-a576-0050568b2de8	VEK	XTS-AES-256	true
Key ID: 00000000000000002000000000050041f10f2d23caf84391b6579a45ee8a5f0000000000000000			
dab1e555-dce2-11ef-a576-0050568b2de8	VEK	XTS-AES-256	true
Key ID: 000000000000000020000000000500ef91891b7c136f55c266c1740cc959f9000000000000000			

6 entries were displayed.

Step 6 - Post Reboot - Run debug smdb table cryptomodKeyTable show

cryptomodKeyTable show output is

node	key-index	key-id
1	1	1
2	2	2
3	3	3
4	4	4
5	5	5
6	6	6
7	7	7
8	8	8
9	9	9
10	10	10
11	11	11
12	12	12
13	13	13
14	14	14
15	15	15
16	16	16
17	17	17
18	18	18
19	19	19
20	20	20
21	21	21
22	22	22
23	23	23
24	24	24
25	25	25
26	26	26
27	27	27
28	28	28
29	29	29
30	30	30
31	31	31
32	32	32
33	33	33
34	34	34
35	35	35
36	36	36
37	37	37
38	38	38
39	39	39
40	40	40
41	41	41
42	42	42
43	43	43
44	44	44
45	45	45
46	46	46
47	47	47
48	48	48
49	49	49
50	50	50
51	51	51
52	52	52
53	53	53
54	54	54
55	55	55
56	56	56
57	57	57
58	58	58
59	59	59
60	60	60
61	61	61
62	62	62
63	63	63
64	64	64
65	65	65
66	66	66
67	67	67
68	68	68
69	69	69
70	70	70
71	71	71
72	72	72
73	73	73
74	74	74
75	75	75
76	76	76
77	77	77
78	78	78
79	79	79
80	80	80
81	81	81
82	82	82
83	83	83
84	84	84
85	85	85
86	86	86
87	87	87
88	88	88
89	89	89
90	90	90
91	91	91
92	92	92
93	93	93
94	94	94
95	95	95
96	96	96
97	97	97
98	98	98
99	99	99
100	100	100

key-type key-digest

key

[illegible]

Step 7 - Post Reboot - Get output of /cfc card/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/knip/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.xx7:5696.host=xx.xxx.xxx.xx7
xx.xxx.xxx.xx7:5696.port=5696
xx.xxx.xxx.xx7:5696.trusted_file=/cfcard/kmip/certs/CA.pem
xx.xxx.xxx.xx7:5696.protocol=KMIP1_4
xx.xxx.xxx.xx7:5696.timeout=25
xx.xxx.xxx.xx7:5696.nbio=1
xx.xxx.xxx.xx7:5696.cert_file=/cfcard/kmip/certs/client.crt
xx.xxx.xxx.xx7:5696.key_file=/cfcard/kmip/certs/client.key
xx.xxx.xxx.xx7:5696.ciphers="TLSv1.2+FIPS:!eNULL:!aNULL"
xx.xxx.xxx.xx7:5696.verify=true
```

Step 8 - Post Reboot - Compare /cfcard/kmip/servers.cfg files

The /cfcard/kmip/servers.cfg output before reboot is the same after rebooting

Step 9 - Post Reboot - Delete the NSE key

Step 10 - Post Reboot - Delete the encrypted volumes

[Job 55] Job succeeded: Successful

[Job 56] Job succeeded: Successful

2 entries were acted on.

Step 11 - Post Reboot - Delete the data vserver - test_vserver

[Job 57]

Step 12 - Post Reboot - Delete the data aggregate - test_aggr

[Job 59] Job succeeded: DONE

Step 13 - Turn off logging for key management

216 entries were modified.

Step 14 - Delete a KMIP log file

Step 15 - 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