NetApp ONTAP and Entrust Cryptographic Security Platform Key Management Vault

Integration Guide

2026-08-03

© Entrust Corporation. All rights reserved.

Table of Contents

1. Introduction . . . 1
    1.1. Product configuration . . . 1
    1.2. Requirements . . . 1
2. Deploy Cryptographic Security Platform Key Management Vault . . . 2
    2.1. Deploy a Cryptographic Security Platform Key Management Vault cluster . . . 2
    2.2. Create a KMIP Vault in Cryptographic Security Platform Key Management Vault . . . 2
    2.3. KMIP server settings . . . 4
    2.4. Install a signed certificate from your local root CA in the Cryptographic Security Platform Key Management Vault cluster . . . 5
3. Deploy NetApp Simulate ONTAP . . . 9
4. Integrate Cryptographic Security Platform Key Management Vault with NetApp ONTAP . . . 11
    4.1. Create the Cryptographic Security Platform Key Management Vault client certificate bundle . . . 11
    4.2. Install the Cryptographic Security Platform Key Management Vault client bundle into NetApp ONTAP . . . 13
    4.3. Set up Cryptographic Security Platform Key Management Vault as the external KMIP server . . . 14
5. Test Integration . . . 16
    5.1. Load the test scripts into NetApp ONTAP . . . 16
    5.2. Execute the kmip_before_reboot_test.sh test script . . . 17
    5.3. Execute the kmip_post_reboot_test.sh test script . . . 20
    5.4. Enable FIPS mode . . . 22
    5.5. Execute the before and post test scripts a second time . . . 23
    5.6. Verify FIPS mode is unchanged after reboot . . . 28
6. HSM Integration . . . 30
7. Additional resources and related products . . . 31
    7.1. nShield as a Service . . . 31
    7.2. Entrust CSP Key Manager . . . 31
    7.3. Entrust products . . . 31
    7.4. nShield product documentation . . . 31

Chapter 1. Introduction

This guide describes the integration of NetApp ONTAP with the Entrust Cryptographic Security Platform Key Management Vault (KMS) using the KMIP open standard. Cryptographic Security Platform Key Management Vault manages encryption keys using multiple protocols, including KMIP.

1.1. Product configuration

Entrust has successfully tested the integration of Cryptographic Security Platform Key Management Vault with NetApp ONTAP in the following configurations:

Product	Version
NetApp ONTAP	9.17.1.P9 / 9.18.1.P5
Entrust Cryptographic Security Platform	1.4
Entrust Key Management Vault	10.5.3

1.2. Requirements

Before you begin, review the following documentation:

- NetApp ONTAP 9 Online Documentation
- Cryptographic Security Platform Vault v10.5.3 Online Documentation Set

Chapter 2. Deploy Cryptographic Security Platform Key Management Vault

2.1. Deploy a Cryptographic Security Platform Key Management Vault cluster

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

Follow the installation and setup instructions in the *Entrust Cryptographic Security Platform Key Management Vault nShield® HSM Integration Guide*. You can access it from the Entrust Document Library and from the nShield Product Documentation website.

Ensure that the KMIP Key Management Vault has been created and that certificates have been generated for NetApp ONTAP. These certificates are used in the configuration of the KMS described below.

Add a record in your DNS server for the Cryptographic Security Platform Key Management Vault cluster. Associate all Cryptographic Security Platform Key Management Vault cluster node IP addresses with the same record.

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

2.2. Create a KMIP Vault in Cryptographic Security Platform Key Management Vault

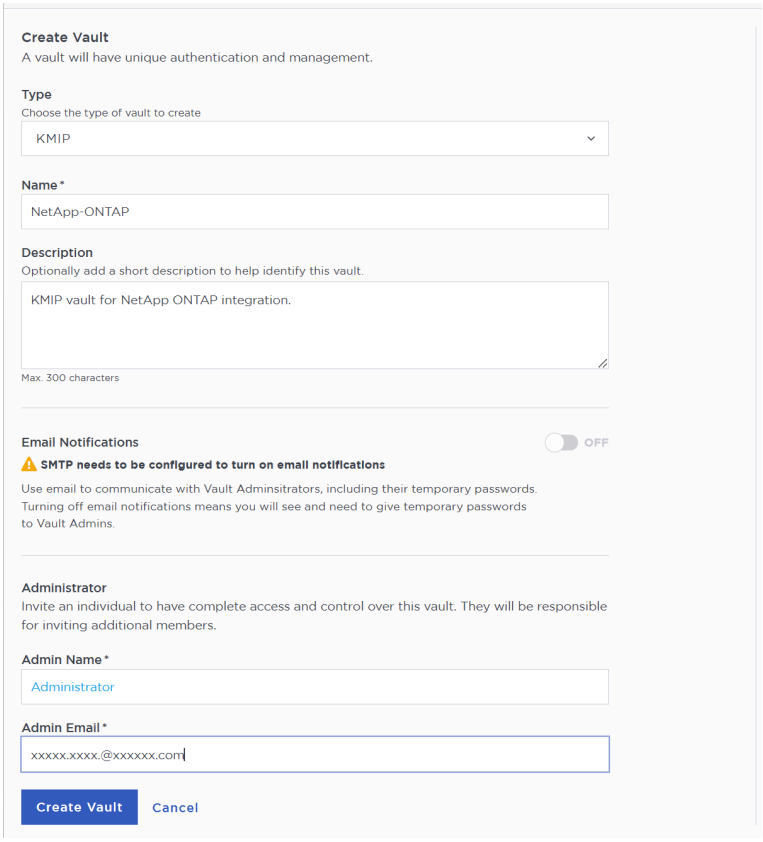
The Cryptographic Security Platform Key Management Vault appliance supports different types of vaults that can be used by all types of applications. This section describes how to create a KMIP Vault in the Cryptographic Security Platform Key Management Vault Server.

Refer to Cryptographic Security Platform Vault for KMIP for more details.

1. Sign in to the Key Management 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 Key Management Vault interface, select **Create Vault**.
4. In the **Create Vault** page, create a **KMIP** Vault:

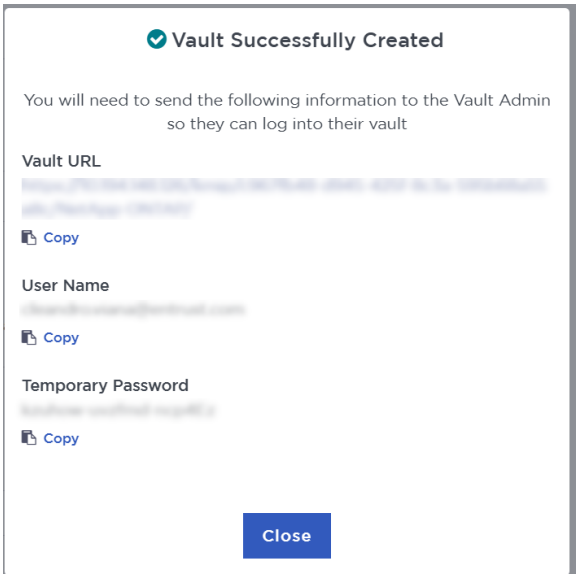
- For the **Type**, select **KMIP**.
- If you are using email to communicate with vault administrators, toggle **Email Notifications** to **On**.
  You must have SMTP configured to use this feature.
- Complete the other fields as required.

  For example:



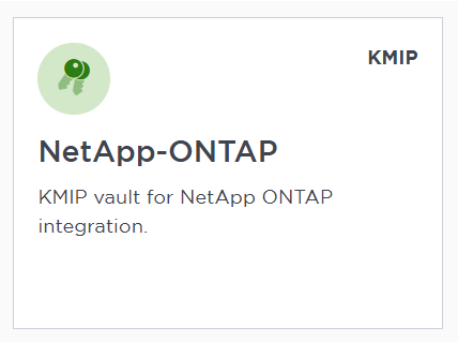
5. Select **Create Vault**.

   When created, the new vault's URL and sign-in credentials are emailed to the email address entered in the **Admin Email** field. This is the temporary password for the first sign-in to the KMIP vault in Cryptographic Security Platform Key Management Vault. In closed gap environments where email is not available, the URL and sign-in credentials are displayed in the Vault Successfully Created dialog. These can be copied and sent to the user.



6. Bookmark the KMIP vault URL and, if required, save the user name and temporary password.
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. In a web browser, navigate to the vault URL and sign in using the user name and temporary password. Change the initial password when prompted.
10. Sign in again to verify.

2.3. KMIP server settings

The KMIP server settings are set at the Cryptographic Security Platform Key Management Vault appliance level and apply to all the KMIP vaults in the appliance. After a KMIP vault is created, it is automatically set to **ENABLED**.

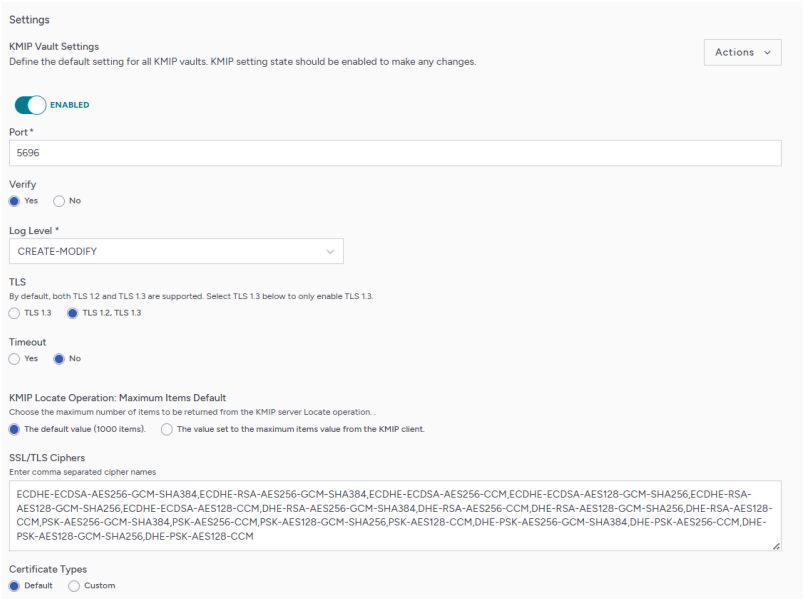
To use external key management and configure the Cryptographic Security Platform Key

Management Vault KMIP settings, refer to the Cryptographic Security Platform Key Management Vault for KMIP section of the admin guide.

When using external key management, as required for this integration, the Cryptographic Security Platform Key Management Vault server is the KMIP server and the NetApp server is the KMIP client.

1. Sign in to the Key Management Vault server vault management UI as **secroot**.
2. Select the **Settings** icon on the top right to view or change the KMIP settings.

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



3. If you changed any settings, select **Apply**.

2.4. Install a signed certificate from your local root CA in the Cryptographic Security Platform Key Management Vault 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.

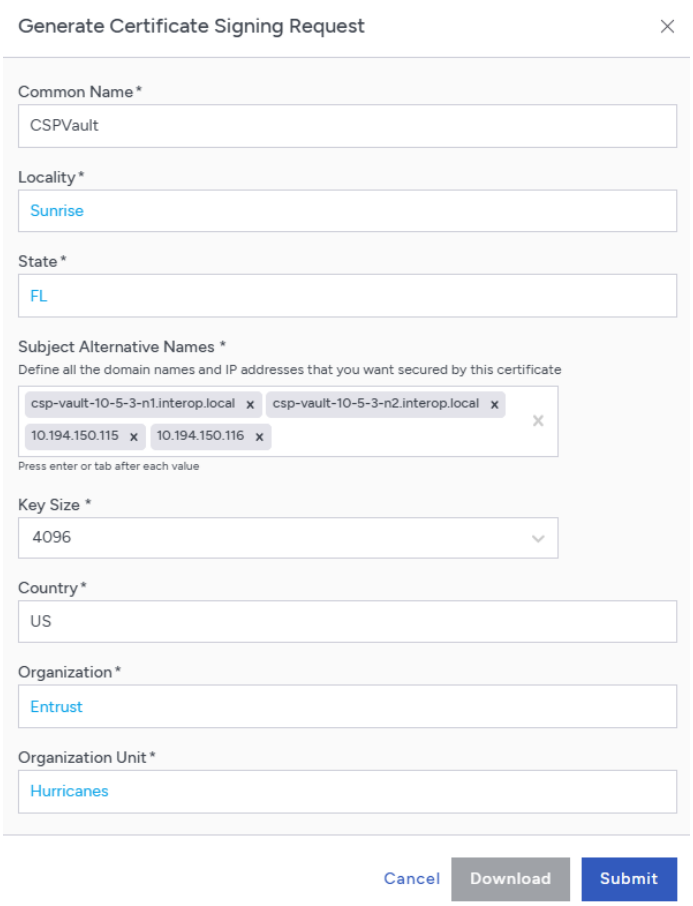
2.4.1. Create a CSR

1. Sign in to the Key Management Vault server vault management UI as **secroot**.
2. In the **Vault Management** dashboard, select the **Settings** icon on the top right.

3. From the **Action** drop-down menu, select **Generate CSR**.
4. Enter your information.

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

   For example:



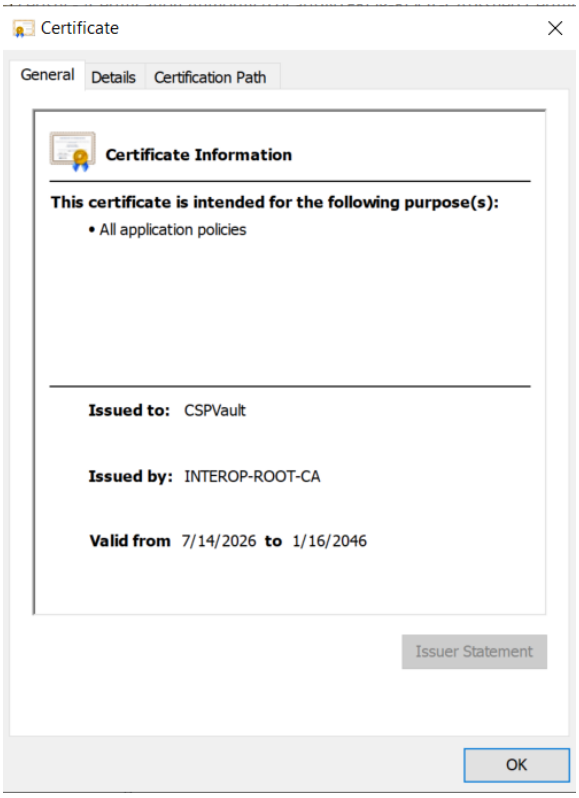
5. Select **Submit**.
6. After submitting the CSR, select **Download**. The CSR **pem** file is downloaded to your **Downloads** folder.
7. Store the file for signing in the next section.

2.4.2. Sign the CSR and issue a certificate

1. Sign in to your local root CA with administrator privileges.
2. Transfer the CSR created above to a local folder on the local root CA server, such as the **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. On the **Details** tab, select **Copy to File...**.
11. Follow the instructions, selecting **Base-64 encoded X.509** as the **Export File Format**. Save as `cspvault` in the `Downloads` folder.
12. Export the local root CA certificate as a `cer` file:

```
PS C:> certutil -store Root "INTEROP-ROOT-CA" .\rootcacert.cer
Root "Trusted Root Certification Authorities"
================ Certificate 9 ================
Serial Number: 289aeb6982de70894c2e8e29402a268a
Issuer: CN=INTEROP-ROOT-CA
 NotBefore: 1/16/2026 3:56 PM
 NotAfter: 1/16/2046 4:06 PM
Subject: CN=INTEROP-ROOT-CA
CA Version: V0.0
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): 2384515ade8d26d8ad04866d2bfe63fc453de58a
```

```
No key provider information
  Provider = Microsoft Software Key Storage Provider
  Simple container name: INTEROP-ROOT-CA
  Unique container name: 4b8be25ddd1badc35a2f2b7993eb732e_05c8de66-00f6-41ee-b681-f5c65b710b3f
Signature test passed
CertUtil: -store command completed successfully.
```

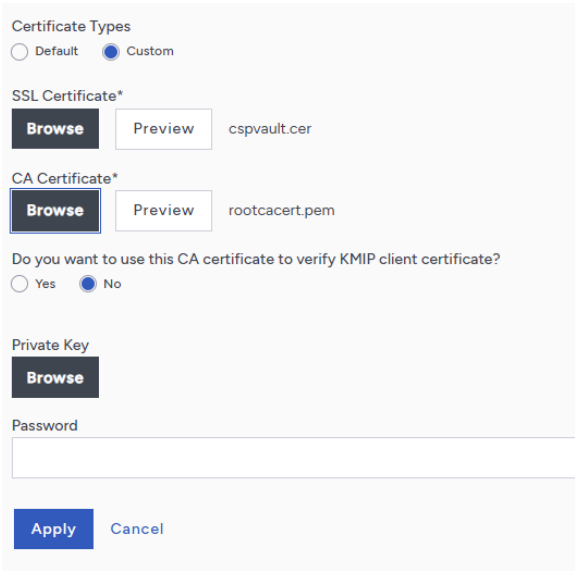
13. Encode the certificate as a `pem` file:

```
PS C:> certutil -encode rootcacert.cer rootcacert.pem
Input Length = 527
Output Length = 782
CertUtil: -encode command completed successfully.
```

14. Copy the `cspvault.cer` certificate and the `rootcacert.pem` to a location accessible by the Key Management Vault server.

2.4.3. Install certificate

1. Sign in to the Key Management Vault server vault management UI as **secroot**.
2. In the **Vault Management** dashboard, select the **Settings** icon on the top right.
3. In **Certificate Types**, select **Custom**.
4. Browse to and select the certificate as shown.



5. If required, make any other changes, however the other default settings are appropriate for most applications.
6. Select **Apply**.

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. For this integration, the **STORAGE SYSTEM NAME** is set to **mycluster**.

1. Download the simulator OVA file from Simulate ONTAP Download.
2. Deploy the virtual machine.

   Follow the instructions in the NetApp documentation.

   The virtual simulator software does not support volume encryption by default. Upgrade the virtual machine with an image that supports volume encryption. Contact NetApp for information about upgrading the image and for licenses that support volume encryption.

3. Add a record in your DNS server for the **Cluster Management**.
4. Configure the NTP server as explained in the NetApp documentation.
5. Install the root CA certificate from your root CA:
   a. Open a command window and sign in to the NetApp ONTAP Cluster Management.

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

   b. Install the root CA certificate.

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

   Please enter Certificate: Press <Enter> when done
   -----BEGIN CERTIFICATE-----
   MIICCzCCAWygAwIBAgIQKJrraYLecIlMLo4pQComijAKBggqhkjOPQQDBDAaMRgw
   FgYDVQQDEw9JTlRFUk9QLVJPT1QtQ0EwHhcNMjYwMTE2MTk1NjIzWhcNNDYwMTE2
   .
   .
   b2MHq2BkoBAaJQTWMIEn24S5s6/8Nq7qbLkNAkIBSG6Ok+8+nKjN2nagHu74vWsK
   Ysd5akN5ftyvliLbcFe08fUus/oWnV/+9PyNyWpYZ2yilg+bDeUNeMrYlYol4MY=
   -----END CERTIFICATE-----


   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
   serial: 289AEB6982DE70894C2E8E29402A268A

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

Make a note of the certificate's generated name above, for example, **INTEROP-ROOT-CA**.

It will be needed in section Set up Cryptographic Security Platform Key Management Vault as the external KMIP server.

Chapter 4. Integrate Cryptographic Security Platform Key Management Vault with NetApp ONTAP

4.1. Create the Cryptographic Security Platform Key Management Vault client certificate bundle

KMIP communications between the KMIP Key Management Vault and the NetApp ONTAP application require certificates. Use the built-in capabilities of Cryptographic Security Platform Key Management Vault to create and publish the certificate.

Generate a CSR on NetApp and use it here to create the certificate. NetApp generates the key, and only a client with the key can connect to the KMIP server. This provides a more controlled environment where the customer can control which clients can connect to the KMIP server and access the keys.

1. Open a command window and sign in to the NetApp ONTAP Cluster Management.

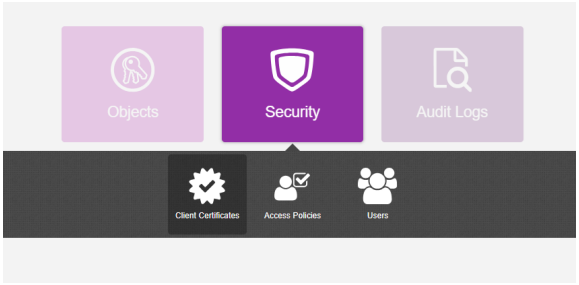
```
% ssh admin@xxx.xxx.xxx.xxx
```

2. Generate a CSR:

```
mycluster::> security certificate generate-csr -common-name netapp-ontap -size 4096 -country US -state
Florida -locality Sunrise -organization Hurricanes

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIE4jCCAsoCAQAwXTEVMBMGA1UEAxMMbmV0YXBwLW9udGFwMQswCQYDVQQGEwJV
UzEQMA4GA1UECBMHRmxvcmlkYTEQMA4GA1UEBxMHU3VucmlzZTETMBEGA1UEChMK
SHVycmljYW5lczCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAM15HBg3
5/bBVJTM7lOndqEbtMgayuJQnJURRDmDpMvcK/h+Jn4NkXTbWEsVVoNVD/8G762k
tqpR3Uh7txSG9MdRfdeyi7EayOLn
.
.
lvzprp6tloNvy4oXiEm+5l8HEj6jKDQkP4CdbW+BhutYKBYVdvs3WwV+ULUv8hcH
PIHrVZa2
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN PRIVATE KEY-----
MIIJQgIBADANBgkqhkiG9w0BAQEFAASCCSwwggkoAgEAAoICAQDNeRwYN+f2wVSU
zO5Tp3ahG7TIGsriUJyVEUQ5g6TL3Cv4fiZ+DZF021hLFVaDVQ//Bu+tpLaqUd1I
.
.
0gN2EblsgJ1ZPgBKK+yLNKYTPvORQw==
-----END PRIVATE KEY-----

Note: Keep a copy of your certificate request and private key for future reference.
```

Store the CSR certificate as `netapp.csr`.

3. Sign in to the KMIP Vault with the URL and credentials provided when you created the KMIP vault.
4. Select **Security**, then **Client Certificates**.



5. In the **Manage Client Certificate** page, select the **+** icon on the right to create a new certificate. The **Create Client Certificate** dialog box appears.
6. In the **Create Client Certificate** dialog box:

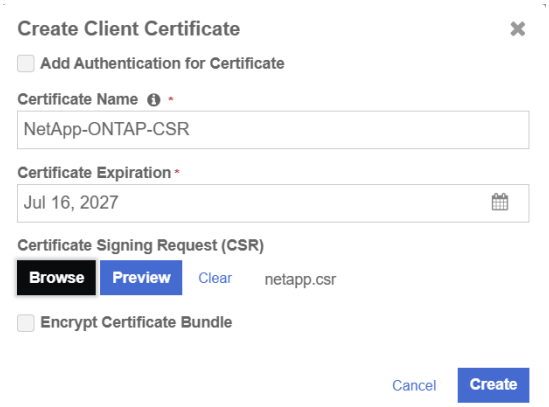
   a. Enter the certificate name.

   b. Enter the expiration date.

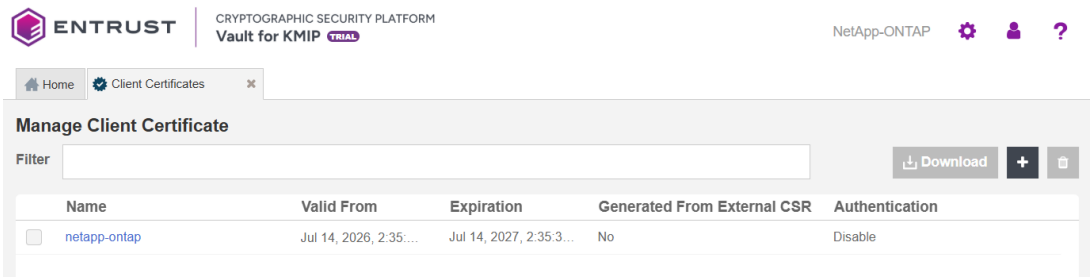
   c. For the **Certificate Signing Request (CSR)** field, browse for your `netapp.csr` file.

   d. Select **Create**.

   For example:



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



7. Select the certificate and then select the **Download** icon to download the certificate.
8. Unzip the downloaded file.

```
% unzip netapp-ontap_2026-07-14-18-37-32.zip
Archive:  netapp-ontap_2026-07-14-18-37-32.zip
  inflating: netapp-ontap.pem
  inflating: cacert.pem
```

   It contains the following items:

   - A `certname.pem` file that includes both the client certificate and private key. In this example, the 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 that is the root certificate for the KMS cluster. It is always named `cacert.pem`.
9. These files are used to establish trust between Cryptographic Security Platform Key Management Vault and NetApp.

For more information about creating a certificate bundle, refer to Establishing a Trusted Connection with a Cryptographic Security Platform Key Management Vault Generated CSR.

4.2. Install the Cryptographic Security Platform Key Management Vault client bundle into NetApp ONTAP

1. Open a command window and sign in to the NetApp ONTAP Cluster Management.

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

2. Install the Cryptographic Security Platform Key Management Vault Client Certificate into NetApp ONTAP.

   When prompted for the certificate section, copy it from the `netapp-ontap.pem` file. When prompet for the private key section, copy it from the `netapp.csr` file used to store the CSR. This is the private key that was created when you generated the NetApp CSR.

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

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIEaDCCA1CgAwIBAgIEfhphJTANBgkqhkiG9w0BAQsFADBXMQswCQYDVQQGEwJV
.
.
.
RMM5ZEqIjkwJh1CurTN5JuLFZPYV9zNNHKKEiQ==
-----END CERTIFICATE-----

Please enter Private Key: Press <Enter> when done
-----BEGIN PRIVATE KEY-----
MIIJQwIBADANBgkqhkiG9w0BAQEFAASCCS0wggkpAgEAAoICAQCj7+BP2YfDiUiW
.
.
.
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: 732B155A

The certificate's generated name for reference: netapp-ontap
```

3. Make a note of the certificate's generated name above, for example, **netapp-ontap**. It will be needed in section Set up Cryptographic Security Platform Key Management Vault as the external KMIP server.

4.3. Set up Cryptographic Security Platform Key Management Vault as the external KMIP server

1. Open a command window and sign in to the NetApp ONTAP Cluster Management.
2. Enable the external KMIP server. Include the following arguments:
   - `-client-cert`: The name of the certificate that was generated in Install the Cryptographic Security Platform Key Management Vault client bundle into NetApp ONTAP, for example, `netapp-ontap`.
   - `-server-ca-certs`: The name of the certificate that was generated in Deploy NetApp Simulate ONTAP, for example, `INTEROP-ROOT-CA`.

     Use the IP addresses of both nodes in the Key Management Vault 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
```

For this integration test, only the primary Key Management Vault node's IP address was used.

3. Verify that 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 procedure requires test scripts obtained from NetApp. Send the output files generated by the test scripts to NetApp for verification.

5.1. Load the test scripts into NetApp ONTAP

1. Open a command window and sign in to the NetApp ONTAP Cluster Management.
2. Unlock and set the password for the `diag` user:

```
mycluster::> security login unlock -username diag
mycluster::> security login password -username diag
```

3. Set diagnostics:

```
mycluster::> set diag

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

4. 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.
```

5. 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.

6. Verify the test script 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 sign in to 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
```

3. Enter Systemshell:

```
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.
```

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

   Cryptographic Security Platform Key Management Vault presents itself as a single entity even though it may be composed of multiple nodes (two in this test case). If the `Please enter whether this is a clustered key-server config` prompt appears, enter `no`.

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

Please enter key server name: CSP Vault
Please enter key server version: 10.5.3
Please enter whether this is a clustered key-server config (yes or no): no
```

▼ *Example output*

```
Executing script kmip_before_reboot_test - version 2.3
Testing DOT: NetApp Release 9.17.1P9: Wed Jun 24 13:09:36 UTC 2026 <1O>
 with Key Manager: CSP Vault 10.5.3
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.xxx       primary        available         -

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

343 entries were modified.

Step 5 - Enable KMIP logging for key management

1 entry was modified.

Step 6 - Create data storage aggregate - test_aggr
[Job 32] 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 33] Sleeping for 10 seconds before checking if vserver was created...
[Job 33] Job succeeded:
Vserver creation completed.

Step 9 - Verify vserver exists
Vserver was created successfully.
Step 10 - Create 2 encrypted volumes
[Job 34] Job succeeded: Successful

[Job 35] 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    18.78MB    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.xxx:5696
   Key Manager Type: KMIP
 Key Manager Policy: -

Key Tag                                 Key Type Encryption   Restored
--------------------------------------  -------- ------------ --------
6101d2fb-8443-11f1-b8da-005056b1584e  VEK      XTS-AES-256  true
    Key ID: 00000000000000000200000000000050038c0edc571a3036eced32d03f3588a490000000000000000
5f12713a-8443-11f1-b8da-005056b1584e  VEK      XTS-AES-256  true
    Key ID: 00000000000000000200000000000500b66f9fb3479471d9b7ba982e3da265b70000000000000000
2 entries were displayed.
```

```
Step 13 - Create NSE key
NSE key id is  000000000000000002000000000000100fe73b73aee19dec2141a0d72066bca0f0000000000000000
Step 14 - Get the NSE key
NSE key id is 000000000000000002000000000000100fe73b73aee19dec2141a0d72066bca0f0000000000000000
Step 15 - 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: 000000000000000002000000000000100fe73b73aee19dec2141a0d72066bca0f0000000000000000
6101d2fb-8443-11f1-b8da-005056b1584e  VEK      XTS-AES-256  true
    Key ID: 000000000000000002000000000000050038c0edc571a3036eced32d03f3588a490000000000000000
5f12713a-8443-11f1-b8da-005056b1584e  VEK      XTS-AES-256  true
    Key ID: 000000000000000002000000000000500b66f9fb3479471d9b7ba982e3da265b70000000000000000
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         000000000000000002000000000000500b66f9fb3479471d9b7ba982e3da265b70000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000 XTS-AES-256 b50d922347f7a4c01b801bc5c501178636b9d465e8d609caa77d98fc30c823c1
mycluster-01 1         000000000000000002000000000000050038c0edc571a3036eced32d03f3588a490000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000 XTS-AES-256 8c2d9619a2d2c1e39a0c4d1dc6302f576c562d177284b1b3c912a9c02193cf3b
mycluster-01 2         000000000000000002000000000000100fe73b73aee19dec2141a0d72066bca0f0000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
NSE-AK      4f69121ddb4418e13eb64b4374f1c3a2747d144e59751645aefee01f4b605fa0
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.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
xx.xxx.xxx.xxx:5696.netapp_keystore_uuid=c8cad565-8442-11f1-b8da-005056b1584e

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 signing in to the cluster again.

```
mycluster::*> reboot -node mycluster-01
```

5.3. Execute the kmip_post_reboot_test.sh test script

1. Open a command window and sign in to the NetApp ONTAP Cluster Management.
2. Set diagnostics:

```
mycluster::> set diag
```

3. Enter Systemshell.

   Provide the password when prompted.

```
mycluster::*> systemshell -node mycluster-01
```

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

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

Please enter key server name: CSP Vault
Please enter key server version: 10.5.3
Please enter whether this is a clustered key-server config (yes or no): no
```

▼ *Example output*

```
Executing script kmip_post_reboot_test - version 2.3
Testing DOT: NetApp Release 9.17.1P9: Wed Jun 24 13:09:36 UTC 2026 <1O>
 with Key Manager: CSP Vault 10.5.3
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.xxx       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    18.74MB    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 0000000000000000020000000000100fe73b73aee19dec2141a0d72066bca0f0000000000000000
Step 6 - Post Reboot - 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: 0000000000000000020000000000100fe73b73aee19dec2141a0d72066bca0f0000000000000000
6101d2fb-8443-11f1-b8da-005056b1584e  VEK      XTS-AES-256  true
    Key ID: 0000000000000000020000000000050038c0edc571a3036eced32d03f3588a490000000000000000
5f12713a-8443-11f1-b8da-005056b1584e  VEK      XTS-AES-256  true
    Key ID: 0000000000000000020000000000500b66f9fb3479471d9b7ba982e3da265b70000000000000000
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         0000000000000000020000000000100fe73b73aee19dec2141a0d72066bca0f0000000000000000
0000000000000000000000000000000000000000000000000000000000000000 NSE-AK
4f69121ddb4418e13eb64b4374f1c3a2747d144e59751645aefee01f4b605fa0
mycluster-01 1         0000000000000000020000000000500b66f9fb3479471d9b7ba982e3da265b70000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000 XTS-AES-256 b50d922347f7a4c01b801bc5c501178636b9d465e8d609caa77d98fc30c823c1
mycluster-01 2         0000000000000000020000000000050038c0edc571a3036eced32d03f3588a490000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000 XTS-AES-256 8c2d9619a2d2c1e39a0c4d1dc6302f576c562d177284b1b3c912a9c02193cf3b
3 entries were displayed.

Step 8 - Post Reboot - Get output of /cfcard/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=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
xx.xxx.xxx.xxx:5696.netapp_keystore_uuid=c8cad565-8442-11f1-b8da-005056b1584e

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

Step 12 - Post Reboot - Delete the data vserver - test_vserver
[Job 40]
Step 13 - Post Reboot - Delete the data aggregate - test_aggr
[Job 42] Job succeeded: DONE

Step 14 - Turn off logging for key management

343 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 sign in to the NetApp ONTAP Cluster Management.
2. Set diagnostics:

```
mycluster::> set diag
```

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 signing in to the cluster again.

```
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. Sign in to the NetApp ONTAP Cluster Management again.
6. Set diagnostics:

```
mycluster::> set diag
```

7. Verify that 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 sign in to the NetApp ONTAP Cluster Management.
2. Set diagnostics:

```
mycluster::> set diag
```

3. Enter Systemshell.

Provide the password when prompted.

```
mycluster::*> systemshell -node mycluster-01
```

4. Execute the `kmip_before_reboot_test.sh` test script and redirect the output to `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: CSP Vault
Please enter key server version: 10.5.3
Please enter whether this is a clustered key-server config (yes or no): no
```

▼ *Example output*

```
Executing script kmip_before_reboot_test - version 2.3
Testing DOT: NetApp Release 9.17.1P9: Wed Jun 24 13:09:36 UTC 2026 <1O>
 with Key Manager: CSP Vault 10.5.3
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.xxx       primary        available         -

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

343 entries were modified.

Step 5 - Enable KMIP logging for key management

1 entry was modified.

Step 6 - Create data storage aggregate - test_aggr
[Job 45] 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 46]
Vserver creation completed.Sleeping for 10 seconds before checking if vserver was created...
[Job 46] Job succeeded:
Vserver creation completed.

Step 9 - Verify vserver exists
Vserver was created successfully.
Step 10 - Create 2 encrypted volumes
[Job 47] Job succeeded: Successful
```

```
[Job 48] 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    18.78MB    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.xxx:5696
   Key Manager Type: KMIP
 Key Manager Policy: -

Key Tag                                 Key Type Encryption   Restored
--------------------------------------  -------- ------------ --------
f3eed91d-8445-11f1-8792-005056b1584e  VEK      XTS-AES-256  true
    Key ID: 00000000000000000200000000000050071e8a5cdfad40ebd604f6995b1438135000000000000000
f2084ec4-8445-11f1-8792-005056b1584e  VEK      XTS-AES-256  true
    Key ID: 00000000000000000200000000000500ad6132942b75b7b577a3064c840507540000000000000000
2 entries were displayed.

Step 13 - Create NSE key
NSE key id is  00000000000000000200000000000100c73d13795c2040a1abbfc5d48444bfe40000000000000000
Step 14 - Get the NSE key
NSE key id is 00000000000000000200000000000100c73d13795c2040a1abbfc5d48444bfe40000000000000000
Step 15 - 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: 00000000000000000200000000000100c73d13795c2040a1abbfc5d48444bfe40000000000000000
f3eed91d-8445-11f1-8792-005056b1584e  VEK      XTS-AES-256  true
    Key ID: 00000000000000000200000000000050071e8a5cdfad40ebd604f6995b1438135000000000000000
f2084ec4-8445-11f1-8792-005056b1584e  VEK      XTS-AES-256  true
    Key ID: 00000000000000000200000000000500ad6132942b75b7b577a3064c840507540000000000000000
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         00000000000000000200000000000500ad6132942b75b7b577a3064c840507540000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000 XTS-AES-256 844c23e85be1f4dadf882bd917a41a40238eb04550ad79706971fc545fa65378
mycluster-01 1         00000000000000000200000000000050071e8a5cdfad40ebd604f6995b1438135000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000 XTS-AES-256 cbc0de60041c27c9b22e2722ec9b3e554587af62bb8a1f0ab606d4fb5462f761
mycluster-01 2         00000000000000000200000000000100c73d13795c2040a1abbfc5d48444bfe40000000000000000
0000000000000000000000000000000000000000000000000000000000000000
NSE-AK      a2b1e0c59acbaff10a4db7a70985b6b5f67441359bc4eabc24b740879ed5861c
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.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+FIPS:!eNULL:!aNULL"
xx.xxx.xxx.xxx:5696.verify=true
xx.xxx.xxx.xxx:5696.netapp_keystore_uuid=c8cad565-8442-11f1-b8da-005056b1584e

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 signing in to the cluster again.

```
mycluster::*> reboot -node mycluster-01
```

7. Sign in to the NetApp ONTAP Cluster Management again.
8. Set diagnostics:

```
mycluster::> set diag
```

9. Enter Systemshell:

```
mycluster::*> systemshell -node mycluster-01
```

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

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

▼ *Example output*

```
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 00000000000000000200000000000100c73d13795c2040a1abbfc5d48444bfe40000000000000000
Step 6 - Post Reboot - 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: 00000000000000000200000000000100c73d13795c2040a1abbfc5d48444bfe40000000000000000
f3eed91d-8445-11f1-8792-005056b1584e  VEK      XTS-AES-256  true
    Key ID: 00000000000000000200000000000050071e8a5cdfad40ebd604f6995b14381350000000000000000
f2084ec4-8445-11f1-8792-005056b1584e  VEK      XTS-AES-256  true
    Key ID: 00000000000000000200000000000500ad6132942b75b7b577a3064c84050754000000000000000
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         00000000000000000200000000000100c73d13795c2040a1abbfc5d48444bfe40000000000000000
00000000000000000000000000000000000000000000000000000000000000000 NSE-AK
a2b1e0c59acbaff10a4db7a70985b6b5f67441359bc4eabc24b740879ed5861c
mycluster-01 1         00000000000000000200000000000050071e8a5cdfad40ebd604f6995b14381350000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000 XTS-AES-256 cbc0de60041c27c9b22e2722ec9b3e554587af62bb8a1f0ab606d4fb5462f761
mycluster-01 2         00000000000000000200000000000500ad6132942b75b7b577a3064c84050754000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000 XTS-AES-256 844c23e85be1f4dadf882bd917a41a40238eb04550ad79706971fc545fa65378
3 entries were displayed.

Step 8 - Post Reboot - Get output of /cfcard/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=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+FIPS:!eNULL:!aNULL"
xx.xxx.xxx.xxx:5696.verify=true
xx.xxx.xxx.xxx:5696.netapp_keystore_uuid=c8cad565-8442-11f1-b8da-005056b1584e

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 51] Job succeeded: Successful
[Job 52] Job succeeded: Successful
2 entries were acted on.

Step 12 - Post Reboot - Delete the data vserver - test_vserver
[Job 53]
Step 13 - Post Reboot - Delete the data aggregate - test_aggr
[Job 55] Job succeeded: DONE

Step 14 - Turn off logging for key management

343 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:

```
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 *
```

4. Sign in to the NetApp ONTAP Cluster Management again.
5. Set diagnostics:

```
mycluster::> set diag
```

6. Verify that 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. HSM Integration

For information about integrating Cryptographic Security Platform Key Management Vault with a Hardware Security Module (HSM), consult your HSM vendor. If you use an Entrust nShield HSM, refer to the **Entrust Cryptographic Security Platform Key Management Vault nShield HSM Integration Guide** available in the Entrust Documentation Library.

Chapter 7. Additional resources and related products

7.1. nShield as a Service

7.2. Entrust CSP Key Manager

7.3. Entrust products

7.4. nShield product documentation