NetApp ONTAP and Entrust KeyControl

Integration Guide

20 Oct 2023

Contents

1. Introduction

This document describes the integration of the NetApp ONTAP data management software with the Entrust KeyControl Key Management Solution (KMS). Entrust KeyControl can serve as a KMS in NetApp ONTAP using the open standard Key Management Interoperability Protocol (KMIP).

1.1. Documents to read first

This guide describes how to configure the Entrust KeyControl server as a KMS in the NetApp ONTAP data management software.

To install and configure the Entrust KeyControl server as a KMIP server, see Entrust KeyControl Product Documentation at https://my.hytrust.com/s/product-guides. Also refer to the NetApp ONTAP online documentation.

1.2. Hardware and software requirements

You must have Entrust KeyControl v5.3 or later before you begin. ONTAP v9.8P3 or later is also required.

The NetApp Interoperability Matrix Tool defines the product components and versions that can be used to construct configurations that are supported by NetApp. See https://mysupport.netapp.com/matrix/.

1.3. Licensing requirements

You must have an Entrust KeyControl license prior to installation.

1.4. High-availability considerations

The Entrust KeyControl solution uses an active-active cluster deployment, which provides high-availability capability to manage encryption keys. NetApp highly recommends this deployment configuration.

In an active-active cluster, changes made to any KeyControl node in the cluster are automatically reflected on all nodes in the cluster. For full information about the Entrust KeyControl solution, see the HyTrust KeyControl Product Overview.

Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

1.5. Product configuration

The integration between NetApp ONTAP and Entrust KeyControl has been successfully tested in the following configurations:

Product	Version
NetApp ONTAP	9.8P3, 9.9.1, 9.10.1, 9.12.1
Entrust KeyControl	5.3, 5.4, 5.5.1, 10.0, 10.1, 10.1.1

2. Procedures

2.1. Installation overview

1. Install and configure Entrust KeyControl.
2. Import the KMIP certificates to ONTAP.
3. Configure ONTAP to use the KMIP certificates.

For additional information about NetApp ONTAP, see the ONTAP 9 Online Documentation.

2.2. Install and configure Entrust KeyControl

Follow the installation and set-up instructions in the `Entrust KeyControl nShield HSM Integration Guide`. You can access this in the Entrust Document Library.

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

2.3. Import the KMIP certificates to ONTAP

The certificates must be installed before running the key manager set-up.

You have to import the following files:

- A `<cert_name>.pem` file that includes both the client certificate and the private key. You will have to paste two sections from this the file into the corresponding prompts from ONTAP.
    - The client certificate section of the `<cert_name>.pem` file includes all the encrypted text and the BEGIN and END lines:

      ```
      "-----BEGIN CERTIFICATE-----"
      some text
      "-----END CERTIFICATE-----"
      ```

    - The private key section of the `<cert_name>.pem` file includes all the encrypted text and the BEGIN and END lines:

      ```
      "-----BEGIN PRIVATE KEY-----"
      some text
      "-----END PRIVATE KEY-----".
      ```

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

Import the previous certificates to ONTAP:

1. Run the `security certificate install` command as described in the *ONTAP 9 NetApp Encryption Power Guide*.
2. Install the NetApp cluster’s KMIP client certificate:

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

   <admin_svm_name> is the host name of the NetApp server.

   > The '-subtype kmip-cert' command has been DEPRECATED and will not be used.

1. Paste the public key certificate from `<cert_name>.pem`.

   When you are installing the client KMIP certificate, you will be prompted to paste the private key certificate from `<cert_name>.pem`. For example:

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

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIEkjCCA3qgAwIBAgIFAKCQaRQwDQYJKoZIhvcNAQELBQAwVzELMAkGA1UEBhMC
VVMxFTATBgNVBAoTDEh5VHJ1c3QgSW5jLjExMC8GA1UEAxMoSHlUcnVzdCBLZXlD
b250cm9sIENlcnRpZmljYXRlIEF1dGhvcml0eTAeFw0yMTA1MTgxNzUxMjdaFw0y
MjA1MTgxNzUxMjdaMDQxCzAJBgNVBAYTAlVTMRUwEwYDVQQKEwxIeVRydXN0IElu
.
.
.
DIwT2P7ReFy/3+nCV8Y7tUG75Lbb5jcooZ0nK5qNNZ8lZmAJ8i9ZHgEQdLZz1trI
BJdTMoP0AzeHN/mMS9snTQDyD2tpdjJl/G8DjXw9G1wChxSThL2flfnJub07l/TX
pGvXmlghJa56MTcjcaHNi6d3kO6h/RmCFof9mG13c/iD7S3ycWG05W02a4F8kJs+
G6I1P6d5zcsKLI8inzMb1J0q9aha7w==
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN PRIVATE KEY-----
MIIJQwIBADANBgkqhkiG9w0BAQEFAASCCS0wggkpAgEAAoICAQDLdLX5yX7gv/YG
gQgD9j8mZCRaxKFELnByVhY2C15UtSdcwdhqhf2yXufSbnnvvjdSGWGoBAyd2CXm
r+ufZiY05+KS6EJvXNaiWDfUabgp2r9PjzYQa6jU3XaUuMIUM3kilzF90sJyoKVz
.
.
.
0v33zLhL+BuXmWJiaoNEwBpS/4BThdlxgfHJO18iOTWlu5e2rTp6f9czsN+FHWKP
hvu/xt6sDh0HLRHnNHMlmdzcDm1dvjcW3Csndtf4feae/Kl/5IQ0rRT2sE1GuOFl
laZvSxpXpKV3soHrpF5iJDlepeW2ArY=
-----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: A0906914

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

2. Install the KMIP server certificate certification authority (CA):

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

For example:

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

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIID4jCCAsqgAwIBAgIEYJBpDzANBgkqhkiG9w0BAQsFADBXMQswCQYDVQQGEwJV
UzEVMBMGA1UEChMMSHlUcnVzdCBJbmMuMTEwLwYDVQQDEyhIeVRydXN0IEtleUNv
bnRyb2wgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4XDTExMDYwMTAwMDAwMFoXDTQ5
.
.
.
pooS3E8kATcvrkXkv7uaZSx72VvyGKqwuFdq2Nn3EHwQCTZjBUqyhqpu59fyuS0d
vo7ccvQ0887kXmnuj1IZM+++2G18ctUxr9XtT9PPt5GT0ZNPGh9mGZvSxE87BT7w
CR63EEBjz7fvAVMR3o5smprW6X7QPBbp4XnxfQ1rhxL9oXYC23I=
-----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: HyTrust KeyControl Certificate Authority
serial: 6090690F

The certificate's generated name for reference: HyTrustKeyControlCertificateAuthority
```

2.4. Configure ONTAP to use the KMIP certificates

You have to configure certain boot environment variables before you can configure ONTAP.

2.4.1. Configure bootarg.storageencryption.support

This `bootarg` is typically set during the manufacturing process. If the encrypted disks don’t show up at boot time, verify that it is set to `true`:

1. Halt the ONTAP boot process to bring up the `LOADER-(A,B)>` prompt.
2. Run

   ```
   LOADER-A> setenv bootarg.storageencryption.support true
   ```

3. Confirm that `bootarg.storageencryption.support` is set:

   ```
   LOADER-A> printenv bootarg.storageencryption.support
   true
   ```

2.4.2. Configure the NetApp Storage Encryption Solution

You can set up an external key management server so that your storage system can securely store and retrieve authentication keys for self-encrypting disks (SEDs) in a location separate from your data. You can link up to four key management servers.

NetApp recommends a minimum of two for redundancy and disaster recovery.

1. To set up external key management servers, run the `security key-manager setup` command.

   By default, the command runs on the local node hosting the cluster management LIF. This command must be run on each node in the cluster by using encrypting hard drives. By design, there should be an HA pair, unless the cluster has only one node.

2. Launch the key management setup wizard to configure ONTAP for storage encryption

```
mycluster::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

Enter the following commands at any time
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the key manager setup wizard. Any changes
you made before typing "exit" will be applied.

Restart the key manager setup wizard with "security key-manager setup". To accept a default
or omit a question, do not enter a value.

Would you like to configure the Onboard Key Manager? {yes, no} [yes]: no
Would you like to configure the KMIP server environment? {yes, no} [yes]: yes
```

2.4.3. Configure the NetApp Volume Encryption Solution

You can set up an external key management server so that your storage system can securely store and retrieve authentication keys for the NetApp Volume Encryption (NVE) solution. NetApp recommends a minimum of two for redundancy and disaster recovery.

For NVE configuration details, see the *ONTAP 9 NetApp Encryption Power Guide*.

1. Add the KeyControl node(s). For example:

```
mycluster::> security key-manager external add-servers -vserver mycluster -key-servers xxx.xxx.xxx.xxx:5696

Successfully queued job "31" to sync key cache for the given key management server.
```

   Repeat the `add-servers` command for every node in the KeyControl cluster.

2. Verify the communication between the external Key Manager and the cluster (ONTAP).

```
mycluster::security> security key-manager query
No matching keys found.

If any listed keys have "no" in the "Restored" column, run "security key-manager restore" to restore those keys.
```

```
mycluster::security> security key-manager show -status
Node                    Port    Registered Key Manager       Status
----------------------  ------  ---------------------------  ---------------
mycluster-01            5696    xxx.xxx.xxx.xxx               available
mycluster-01            5696    xxx.xxx.xxx.xxx               available
2 entries were displayed.
```

2.4.4. Verify the communication with the external Key Manager on the Entrust KeyControl server

To verify that ONTAP is communicating and requesting keys from the KeyControl server, use the **Objects** tab in the KeyControl user interface. See *Managing KMIP Objects* in the *HyTrust KeyControl Admin Guide*.

You might have to refresh the tab or page by refreshing the list in the KeyControl user interface to view the updated requests.

If the certificates or the KMIP configuration have been changed, you may need to restart the KMIP server. See section *Restarting a KMIP Server* in the *HyTrust KeyControl admin guide*.

Restarting the KMIP server does not restart the KeyControl server. It only restarts the KMIP service.

2.5. Integrate with an HSM

For guidance on integrating Entrust 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 nShield HSM Integration Guide available at *Entrust documentation library.*.

2.6. Rekeying NetApp Volumes

Rekeying is only possible on non-root and non-node volumes that are encrypted.

```
mycluster::> volume encryption rekey start -vserver test_vserver -volume test_vol

Warning: The rekey operation scans and rekeys all of the data in the specified volume. It might take a significant amount
of time, and might degrade performance during that time.
Do you want to continue? {y|n}: y
Rekey started on volume "test_vol". Run "volume encryption rekey show -volume test_vol -vserver test_vserver" to see the
status of this operation.
```

To verify the rekey operation in KeyControl Vault Manager, go to the Objects tab and verify the old Symmetric Keys have been Destroyed and the new Symmetric Keys have been Activated. For more guidance on rekeying, refer to the NetApp documentation:

https://docs.netapp.com/us-en/ontap/encryption-at-rest/rekey-encrypted-volume-task.html

3. Manage certificates

3.1. Delete certificates

Before installing new certificates, old certificates must be removed to make sure that the updated certificates are used.

1. Disable the connection to the key management (KMIP) server:

   ```
   Security key-manager delete -address <IP_Address_of_KMIP_Server>
   ```

2. Remove all certificates for the cluster:

   ```
   security certificate delete -vserver <admin_svm_name> -common-name <fqdn_or_custom_common_name> -ca <certificate
   authority> -type client -subtype kmip-cert
   security certificate delete -vserver <admin_svm_name> -common-name <fqdn_or_custom_common_name> -ca
   <certificate_authority> -type server-ca -subtype kmip-cert
   ```

The old certificates are deleted. You can install the new ones.

3.2. Replace SSL certificates

All SSL certificates have an expiration period after initial creation. After a predetermined time, the certificates are no longer valid. They should be replaced before the expiration date.

To replace the certificates, follow the steps in Import the KMIP certificates into ONTAP.

3.3. Clean up key servers

1. Ensure that any encrypted volumes are properly deleted:

   ```
   volume delete -vserver <vserver> -volume <env_vol> -force true -disable-offline-check true
   ```

2. Disable external key management on `vserver`:

   ```
   set advanced
   security key-manager external disable -vserver <vserver>
   set admin
   ```

3.4. Set up new key servers

1. Install the new certificates:

```
security certificate install -vserver <vserver> -type server-ca
security certificate install -vserver <vserver> -type client
```

2. Enable a new external key management on the `vserver`:

```
security key-manager external enable -key-servers <new_key_server> -client-cert <client-cert-name> -server-ca-certs
<server-ca-cert-name> -vserver <vserver>
```

3. Verify that external key management is enabled and that its status is `available`:

```
security key-manager external show-status
```