NetApp ONTAP and Entrust KeyControl with nShield® HSM Integration Guide
1. Introduction

This document describes the configuration of NetApp ONTAP 9.8P3 (or later) data management software for integration with the Entrust KeyControl (formerly HyTrust KeyControl) 5.3 key management solution with an Entrust nShield hardware security module (HSM) root of trust. NetApp Storage Encryption (NSE) and NetApp Volume Encryption (NVE) solutions are compatible with the Entrust KeyControl solution. Entrust KeyControl can serve as a key manager for storage encryption by using an the open standard called the Key Management Interoperability Protocol (KMIP).

1.1. Hardware and software requirements

You must have Entrust KeyControl version 5.3 or later before you begin. ONTAP 9.8P3 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/.

1.2. Licensing requirements

You must have an Entrust KeyControl license prior to installation.

1.3. High-availability considerations

The Entrust KeyControl solution uses an active-active 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.

1.4. Product configuration

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

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetApp ONTAP</td>
<td>9.8P3</td>
</tr>
<tr>
<td>Product</td>
<td>Version</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Entrust KeyControl</td>
<td>5.3</td>
</tr>
<tr>
<td>nShield Security World software</td>
<td>12.60.11</td>
</tr>
<tr>
<td>nShield Connect XC</td>
<td>12.50.11 (12.60.10)</td>
</tr>
</tbody>
</table>
2. Procedures

2.1. Installation overview

1. Install the Entrust KeyControl server.
2. Configure the Entrust KeyControl server with high availability.
3. Generate a KMIP certificate for each controller/cluster.
4. Extract the signing certificates from the KeyControl server.
5. Import the KeyControl certificates in ONTAP.
6. Configure the KeyControl server as an ONTAP KMIP cluster node.

After completing these steps, see the Storage Encryption sections in the relevant documents in the ONTAP Documentation Center, https://docs.netapp.com/ontap-9/index.jsp:

- ONTAP System Administration Guide
- ONTAP Disk and Aggregates Power Guide
- ONTAP Command Reference

To manage storage encryption after it is set up, see the ONTAP Disk and Aggregates Power Guide.

2.2. Install the Entrust KeyControl server

The Entrust KeyControl server is a software solution deployed from an OVA or ISO image. NetApp recommends that you read the HyTrust KeyControl Installation Overview to fully understand the KeyControl server deployment. To configure a KeyControl cluster (active-active configuration is recommended), as performed in the NetApp ONTAP 9 integration validation, NetApp recommends the use of the OVA installation method for simplicity, as described in the HyTrust KeyControl OVA Installation instructions.

The KeyControl OVA must be deployed from vCenter, and not from an ESXi host.

After the KeyControl server is deployed, configure the first KeyControl node as described in the HyTrust Configuring the First KeyControl Node installation guide.

After completing this procedure, add the second node as described HyTrust Adding a New KeyControl Node to an Existing Cluster (OVA Installation) to create the recommended active-active cluster.
Although an active-active cluster is not a requirement, and a single KeyControl node can be deployed to perform the functions of KMIP, NetApp highly recommends deploying the solution with a minimum of two nodes for an active-active cluster solution that instantiates a highly available and robust architecture.

Your KeyControl license determines how many KeyControl nodes you can have in a cluster. For full information about the KeyControl licensing, see the HyTrust Managing the KeyControl License Admin page.

2.3. Configure the nShield HSM in the KeyControl server

See Entrust KeyControl nShield HSM Integration Guide.

2.4. Configure the KeyControl server as a KMIP node

To use external key management, NetApp encryption solutions require an external key management server such as the Entrust KeyControl server. To configure the KeyControl server as a KMIP node, see the HyTrust Configuring a KeyControl KMIP Server section of the Admin Guide.

In a configuration with external key management like in this integration, the KeyControl server is the KMIP node and ONTAP is the KMIP client.

Certificates are required to facilitate the KMIP communications from the KeyControl server to ONTAP and from ONTAP to the KeyControl server.

Existing PKI infrastructures can be used to import certificates for use by KeyControl and ONTAP. However, the simplest solution is to leverage the built-in capabilities in the KeyControl server to create and publish the certificates. To perform this operation, create the certificate bundle as described in the Creating KMIP Client Certificate Bundles section of the Entrust KeyControl Admin Guide.

When you are creating the client certificate in KeyControl, do not use a password in the certificates.

After you created and downloaded these certificates, you need to upload or import them into the ONTAP cluster.

2.5. Configure the KeyControl server

After the Entrust KeyControl server is deployed and the initial installation is complete, you can configure the network settings, e-mail server preferences, and certificate
configuration. For these procedures, see the *HyTrust KeyControl System Configuration Admin Guide*.

# 2.6. Import the KMIP certificates to ONTAP

The certificates must be installed before running the key manager setup.

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 -subtype kmip-cert
   
   <admin_svm_name> is the host name of the NetApp server.
   ```

3. 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`.

   Example:

   ```
   mycluster::> security certificate install -vserver mycluster -type client -subtype kmip-cert
   ```
Please enter Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----
MIIEkjCCA3qgAwIBAgIFAKCQaRQwDQYJKoZIhvcNAQELBQAwVzELMAkGA1UEBhMC
VVMxFTATugMBVQAYYFQTQMDQYJKoZIhvcNAQEFBQAwUEggMBGQGCCsGAQUFBgcg
JhGZIhvcNAQEFBQAwUEggMBQGCCsGAQUFBgcgJhGZIhvcNAQFEJTAQIBNAJGCCsG
AQUFBgcgJhGZIhvcNAQEFBgwGBSAsSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQG
CSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQ
GCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQ
GCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQ
GCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQ
GCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQ
GCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQ
GCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQ
GCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQ
GCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQ
GCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQ
GCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQ
GCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQ
GCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQ
GCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQ
GCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQ
GCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQ
GCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQ
GCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQQGCSQ
-----END CERTIFICATE-----

Please enter Private Key: Press <Enter> when done

-----BEGIN PRIVATE KEY-----
MIIJQwIBADANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAy2JX9w+qPtvUeWJ
n1vDQ56l1v24KbipN1xQ3hZj4C3OyjP35dGC52HcVHfKjXUAj9QjkncJ8z35t\
5yN9PFLHmZMlqX4U2nLm9gJk5cIzQ0HqRzv0+DkRz3H3p6Bh5J8Y605fO\
-----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

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

```
security certificate install -vserv <admin_svm_name> -type server-ca -subtype kmip-cert
```

Example:
2.6.1. Configure ONTAP to use the KMIP certificates

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

2.6.1.1. 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

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
2.6.1.2. 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
   ```

2.6.1.3. 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).

   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.
```

2.6.1.4. 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.
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 were 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
```
Contact Us

Web site
https://www.entrust.com

Support
https://nshieldsupport.entrust.com

Email Support
nShield.support@entrust.com

Online documentation:
Available from the Support site listed above.

You can also contact our Support teams by telephone, using the following numbers:

Europe, Middle East, and Africa
United Kingdom:
+44 1223 622444
One Station Square
Cambridge, UK CB1 2GA

Americas
Toll Free:
+1 833 425 1990

Fort Lauderdale:
+1 954 953 5229
Sawgrass Commerce Center – A
Suite 130
13800 NW 14 Street
Sunrise, FL 33323 USA

Asia Pacific
Australia:
+61 8 9126 9070
World Trade Centre Northbank Wharf
Siddeley St
Melbourne VIC 3005 Australia

Japan:
+81 50 3196 4994

Hong Kong:
+852 3008 3188
31/F, Hysan Place,
500 Hennessy Road,
Causeway Bay
ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they’re crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it’s no wonder the world’s most entrusted organizations trust us.