Technical Report

HyTrust KeyControl Key Management in ONTAP 9.3 or Later

Integration Guide

Andrae Middleton, NetApp
January 2019 | TR-4731

Abstract

This guide describes how to use the HyTrust KeyControl external key management solution for NetApp® ONTAP® 9.3 or later data management software. Topics include installation and configuration of the HyTrust KeyControl Key Management Interoperability Protocol Key Management server (KMIP server) and ONTAP 9.3 or later. This guide also offers a step-by-step example of the configuration steps, using HyTrust KeyControl as the KMIP server.

NetApp®

TABLE OF CONTENTS

1 Introduction

This document describes the configuration of NetApp ONTAP 9.3 (or later) data management software for integration with the HyTrust KeyControl key management solution.

NetApp Storage Encryption (NSE) and NetApp Volume Encryption (NVE) solutions are compatible with the HyTrust KeyControl solution, HyTrust KeyControl can serve as a key manager for storage encryption by using an open standard called the Key Management Interoperability Protocol (KMIP).

2 Before You Begin

2.1 Installation Overview

Here are the high-level configuration steps:

1. Install the HyTrust KeyControl server.
2. Configure the HyTrust 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 into ONTAP.
6. Configure the KeyControl server as an ONTAP KMIP server.

After completing these steps, see the Storage Encryption sections in the relevant documents in the ONTAP Documentation Center:

- 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 Hardware and Software Requirements

You must have HyTrust KeyControl version 4.2 or later before you begin. ONTAP 9.3 or later is also required.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

2.3 Licensing Requirements

You must have a HyTrust KeyControl license prior to installation. You can obtain this license from your HyTrust and NetApp account team or through HyTrust customer support.

2.4 High-Availability Considerations

The HyTrust 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 HyTrust KeyControl solution, see the HyTrust KeyControl Product Overview.

3 Installing the HyTrust KeyControl Server

The HyTrust 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 the VCenter server, 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 in the HyTrust Adding a New KeyControl Node to an Existing Cluster (OVA Installation) to create the recommended active-active cluster.

Note: 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.

After the additional node is added, authorize the new KeyControl node as described in HyTrust Authorizing a New KeyControl Node.

Note: 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.

4 Configuring the KeyControl Server

After the HyTrust 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.

5 Configuring the KeyControl Server as a KMIP Server

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

Note: When using external key management, as is the case in this solution, the KeyControl server is the KMIP server and ONTAP is the KMIP client.

Certificates are required to facilitate the KMIP communications from the KeyControl server to ONTAP and conversely. Although existing PKI infrastructures can be used to import certificates for use by KeyControl and ONTAP, 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 HyTrust KeyControl admin guide.

After you create and download these certificates, you need to upload/import them into the ONTAP cluster.

6 Import the KMIP Certificates into ONTAP

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

The following files need to be imported:

- A `<cert_name>.pem` file that includes **both** the client certificate and private key. The administrator needs to open this single file and paste the two sections of the file into the corresponding prompts from ONTAP.
  - The client certificate section of the <cert_name>.pem file includes the lines "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" and all text between them.
  - The private key section of the <cert_name>.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`.

To import the previous certificates to ONTAP, complete the following steps:

1. Run the `security certificate install` command as outlined in the ONTAP 9 NetApp Encryption Power Guide.
2. To install the NetApp cluster's KMIP client certificate, run the following command:

```
security certificate install -vserver <admin_svm_name> -type client -subtype kmip-cert
```

3. Paste the public key certificate contents section of the <cert_name>.pem file. Also, when installing the client KMIP certificate, you will be prompted to paste the private key certificate contents of the <cert_name>.pem file.
4. To install the KMIP server certificate certification authority (CA), run the following command:

```
security certificate install -vserver <admin_svm_name> -type server-ca -subtype kmip-cert -kmip-server-ip <kmip_server_ipaddress>
```

5. When prompted for additional CAs or intermediate certificates, you do not need to enter details.
6. When installing the KMIP server certificate CA, use a subnet address if you are using the same CA for multiple KMIP servers. If the servers are on different networks, you can use the subnet address 0.0.0.0 as a wildcard.

6.1 Configure ONTAP to Use the KMIP Certificates

ONTAP requires certain boot environment variables to be configured before ONTAP can be configured.

Configuring bootarg.storageencryption.support

This bootarg is typically set during the manufacturing process. However, if the encrypted disks don't show up at boot time, follow these steps to verify that the preceding bootarg is set to true:

1. Halt the ONTAP boot process to bring up the LOADER-(A,B)> prompt and run the following command:

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

2. To confirm that this value is set:

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

The output should appear as follows:

```
Variable Name        Value
--------------------    ------------------------------------------------
bootarg.storageencryption.support   true
```

Configuring 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. With this consideration, if nodes 5 and 6 with encrypting drives are added to an existing 4-node cluster, and the cluster management LIF is located on node 1, the correct commands would be:

```
security key-manager setup -node clustername-05
security key-manager setup -node clustername-06
```

2. Launch the key management setup wizard to configure ONTAP for storage encryption (IPv4):

```
cluster1::> 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 onboard key management? {yes, no} [yes]: no
Would you like to configure the KMIP server environment? {yes, no} [yes]: yes

You will now be prompted for a subset of your network configuration
setup. These parameters will define a pre-boot network environment,
allowing secure connections to the registered key server.

Enter the TCP port number for KMIP server [5696]:
Enter the network interface [e0c]:
Would you like to configure an IPv4 address? {yes, no} [yes]:yes

Enter the IP address [10.63.55.148]: < is set to the application IP address of the appliance, not
the management IP >
Enter the netmask [255.255.192.0]: < is the netmask of the appliance >
Enter the gateway [10.63.0.1]: < is the gateway of the appliance >
Would you like to configure an IPv6 address? {yes, no} [no]: no
```

   – For IPv6:

```
cluster1::> security key-manager setup -node cluster1
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 onboard key management? {yes, no} [yes]: no
Would you like to configure the KMIP server environment? {yes, no} [yes]: yes

You will now be prompted for a subset of your network configuration
setup. These parameters will define a pre-boot network environment,
allowing secure connections to the registered key server.
```

```
Enter the TCP port number for KMIP server [5696]:
Enter the network interface [e0c]:
Would you like to configure an IPv4 address? {yes, no} [yes]:
no

Would you like to configure an IPv6 address? {yes, no} [yes]:
yes
Enter the IPV6 address: fd20:8b1e:b255:208:250:56ff:fea2:206 < is set to the application IPv6
address of the  appliance, not the  management IP >
Enter the IPv6 address prefix length [64]: <IPv6 address prefix length of the  appliance >
Enter the IPv6 gateway: fd20:8b1e:b255:208:250:56ff:fea2:200 <IPv6 gateway of the  appliance >.
```

In the previous commands:

- <Network Interface> is set to the NetApp port on which the node management LIF is located, including VLAN if required (for example, e0M, e0a, e0a-16, a0a-16). This interface cannot participate in network trunking or VIF configuration.
- <IP Address> is set to the application IP address of the appliance, not the management IP.
- <Netmask> is the netmask of the appliance.
- <Gateway> is the gateway of the appliance.

Configuring 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 please see the ONTAP 9 NetApp Encryption Power Guide.

Verifying External Key Manager Communication with the Cluster (ONTAP)

Run the following commands:

- `security key-manager query` (Look for `Server Status`, under the key manager IP address.)
- `security key-manager show -status` (Look for `Server Status`, under the key manager IP address.)

Verifying External Key Manager Communication on the HyTrust KeyControl Server

To verify that ONTAP is communicating and requesting keys from the KeyControl server, use the Objects tab in the KeyControl UI as described in the Managing KMIP Objects section of the HyTrust KeyControl admin guide.

Note: You might have to refresh the tab/page (using the refresh list in the KeyControl UI) to view the updated requests. Additionally, if any changes are made to the certificates or KMIP configuration, you may need to restart the KMIP server, as outlined in the Restarting a KMIP Server section of the HyTrust KeyControl admin guide.

It is important to note that restarting the KMIP server does not restart the KeyControl server, just the KMIP service.

Appendix A: Deleting Certificates

Before installing new certificates, old certificates must be removed to make sure that the updated certificates are used. Follow these steps to completely remove all certificates from an SE system.

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
```

3. After deleting the old certificates, you can install the new ones.

Appendix B: Replacing 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 certificates, follow the steps in section 6.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.