Technical Report

NetApp ONTAP 9 External Key Management: Vormetric Key Management Integration Guide

Andrae Middleton, NetApp
August 2017 | TR-4618

Abstract

This guide describes how to use the Vormetric external key management solution for NetApp® ONTAP® 9 data management software. Topics include installing and configuring the Vormetric Key Management Interoperability Protocol key management server (KMIP server) and ONTAP 9 configuration details. This guide also offers a step-by-step example of the configuration steps using Vormetric as the KMIP server.

NetApp®

TABLE OF CONTENTS

LIST OF FIGURES

1 Introduction

Storage encryption (SE) is fully compatible with the Vormetric Data Security Manager (DSM). This means that Vormetric's DSM can serve as a key manager for SE through the use of an open standard called the Key Management Interoperability Protocol (KMIP). In addition to supporting SE, the DSM administers the Vormetric Transparent Encryption and Vormetric Application Encryption products.

This document describes the process of configuring NetApp ONTAP 9 data management software with a Vormetric DSM.

2 Before You Begin

2.1 Installation Overview

The following high-level configuration steps are required for installation:

1. Upload a KMIP license to the Vormetric DSM.
2. Add each NetApp client (cluster) with a unique KMIP client certificate to each DSM.
3. Generate a KMIP certificate for each controller or cluster.
4. Extract the signing certificates from the DSM.
5. Configure the DSM as an ONTAP KMIP server.

When these steps are complete, refer to the section "Storage Encryption" in the relevant ONTAP documentation:

- ONTAP 9 System Administration Guide
- ONTAP 9 Disk and Aggregates Power Guide
- ONTAP 9 Command Reference

To manage storage encryption after it is set up, see the ONTAP 9 Encryption Power Guide.

2.2 Hardware and Software Requirements

Before you begin, you must have Vormetric DSM version 5.3.1 or later, either virtual or physical. Data ONTAP 9.x or later is also required.

Note: Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to determine that the exact product and feature versions described in this document are supported for your environment.

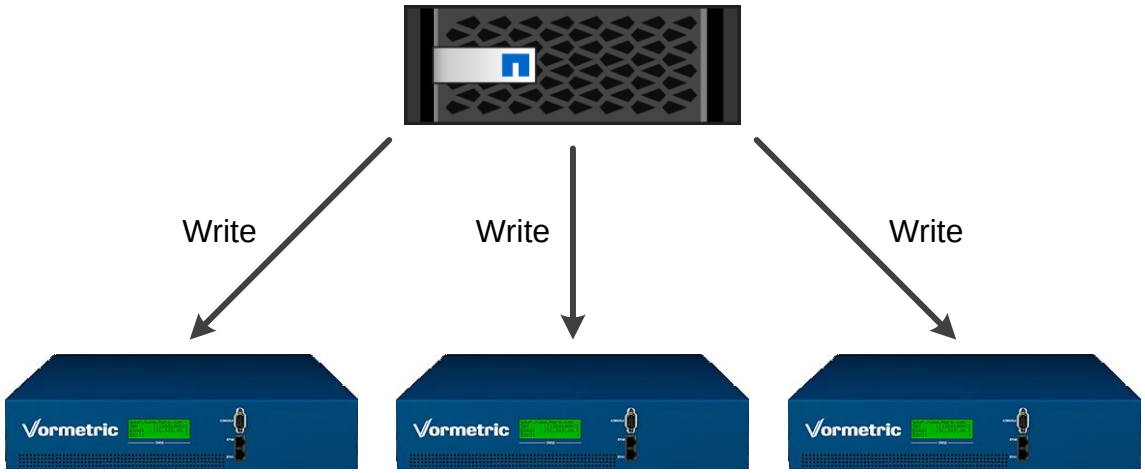
2.3 Licensing Requirements

You must have a Vormetric Data Security Manager v5.3.1 KMIP license. Obtain this license from Vormetric customer support. There are no additional ONTAP licensing requirements.

2.4 High-Availability Considerations

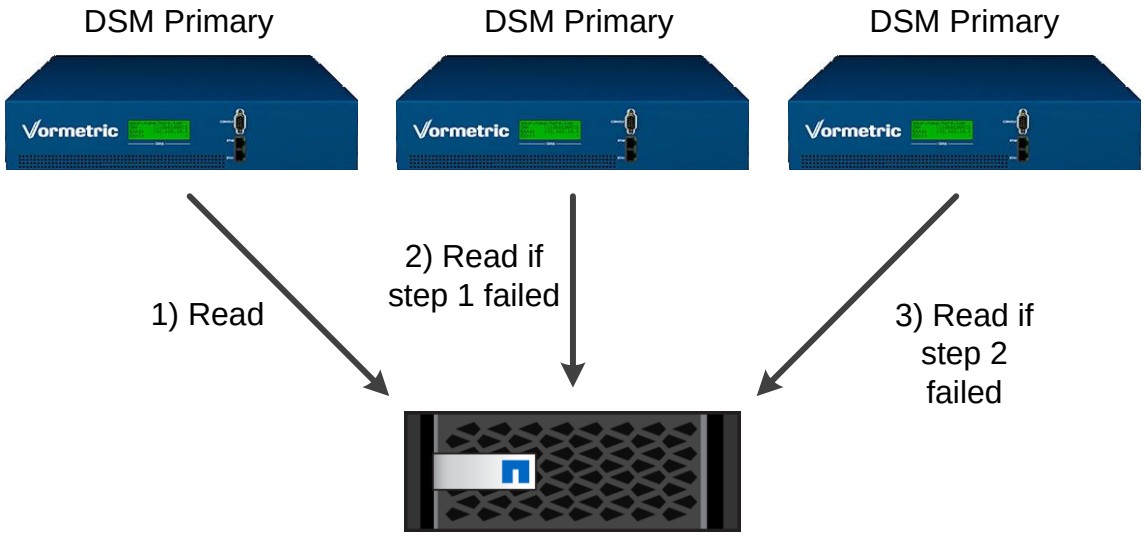
The SE high-availability (HA) model means that, when keys are created, they are written to all the DSMs that the storage encryption device knows about (Figure 1).

Figure 1) Key writing.



When keys are needed, each DSM is queried in turn for the keys (Figure 2).

Figure 2) Key queries.



This model is significantly different from Vormetric's standard HA model, which has a cluster containing an active primary DSM and several read-only failover DSMs. The SE model requires each DSM to be configured as an independent primary.

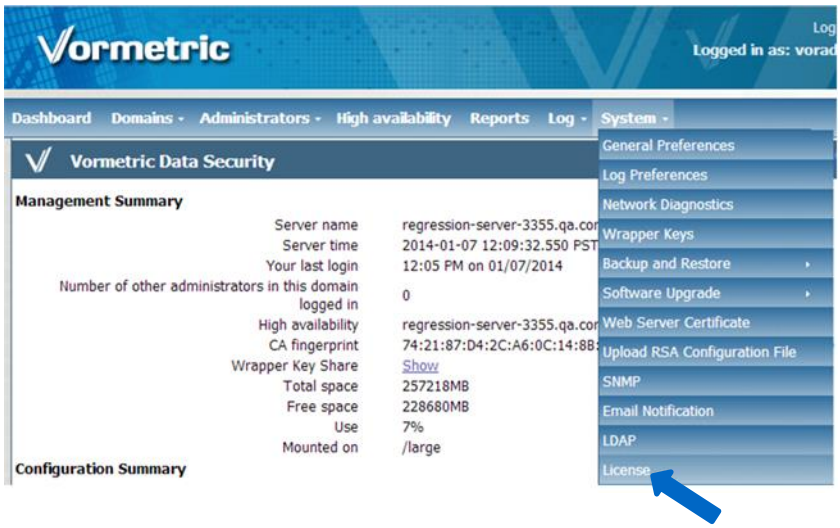
NetApp makes the following recommendations:

- If you already have a cluster of Vormetric DSMs, purchase one additional DSM and make it an independent primary DSM. Then configure the two primaries in SE.
- If you intend to use the Vormetric DSMs to manage the Vormetric Transparent Encryption or the Vormetric Application Encryption products, purchase three DSMs and configure them as just described.
- If you are purchasing the Vormetric DSM for the sole purpose of managing SE keys, purchase two DSMs and configure them both as independent primary DSMs.

3 Uploading a KMIP License to the Vormetric DSM

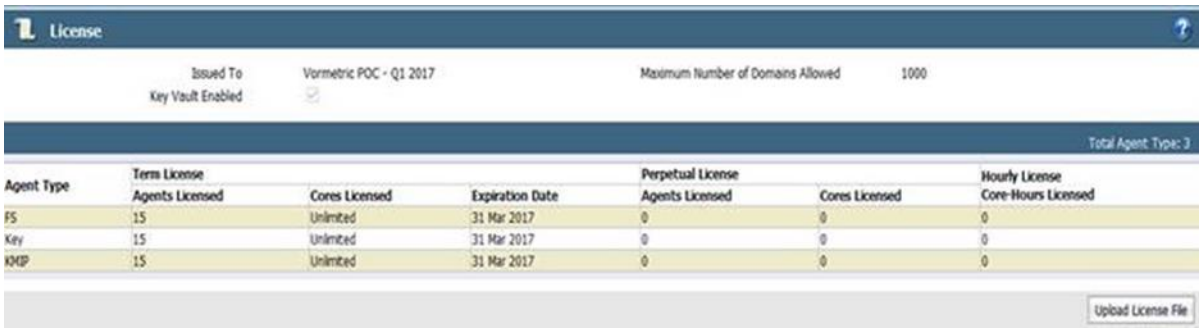
To upload a KMIP license to the Vormetric DSM, complete the following steps:

1. On the primary DSM, log in to the Management Console as an administrator of type System Administrator or All.
2. From the menu bar, select System > License. The License window opens.



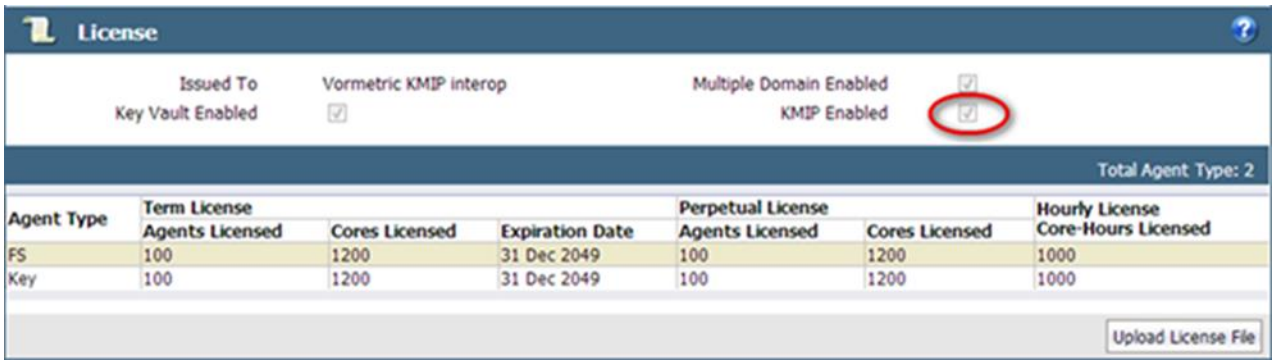
3. Click Upload License File. The Upload License File window opens.
4. Click Choose File and navigate to the license file.
5. Select the file, click Open, and then click Ok. The License window opens.
6. Confirm that the KMIP Enabled box is checked (depending on the DSM version).

Figure 3) Vormetric DSM License installation screen, DSM v5.2.4 and later.



Note that in version 5.2.4 and later of the Vormetric DSM, KMIP is licensed by the number of systems that need to connect for KMIP, as shown in Figure 3. In previous versions this was an on/off option, and the license screen appears as shown in Figure 4.

Figure 4) Vormetric License installation screen, DSM v5.2.3 and earlier.

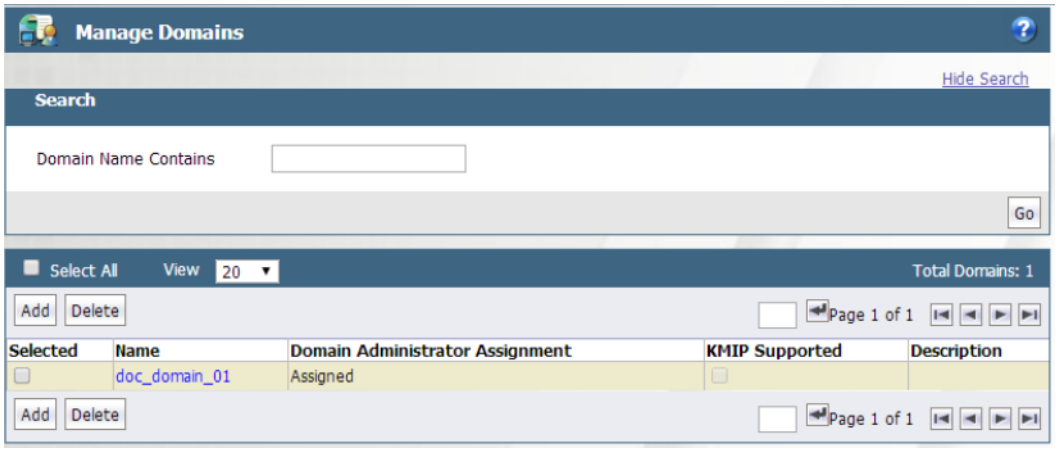


3.1 Adding a Domain

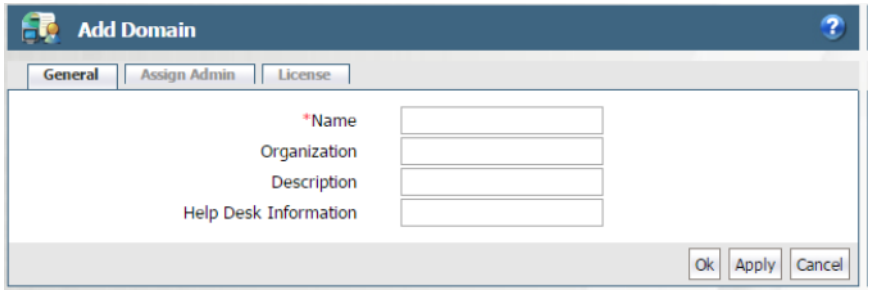
To add a domain, follow these steps:

1. If you are already logged in to the management console, log out and log in again as the DSM System Administrator admin. Otherwise, just log in as admin.
2. Select Domains > Manage Domains. The Manage Domains window opens.

If you are in a domain, click Exit Domain to exit the domain and then click Manage Domains.



3. Click Add. The Add Domain window opens.



4. In the General tab, fill in the following fields:
   a. **Name.** Enter a name of up to 64 characters for the new domain.
   b. **Organization.** (Optional) Enter the name of the organization responsible for or administered by this domain.

c. **Description.** (Optional) Enter a phrase or string of up to 256 characters to help identify the domain.

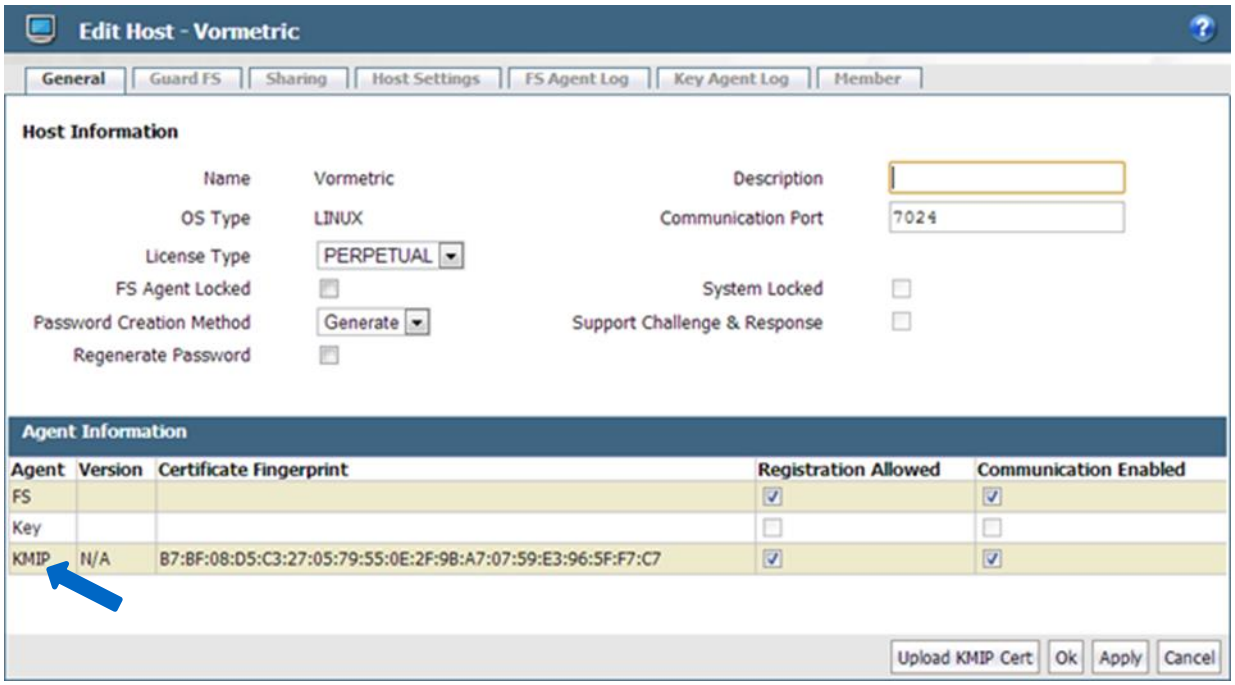
d. **Help Desk Information.** (Optional) Enter the phone number to call to get the response string for challenge-response authentication. If you leave this box empty, the default message is “Please contact a Security Server administrator for a response.” (The term “Security Server” refers to the DSM.)

5. Click Apply to save the domain information.
6. Click the Assign Admin tab to assign an administrator. If you do not assign an administrator when you add the domain, you can edit the domain later to add an administrator. However, you cannot switch to the domain until you assign an administrator.
7. (Optional) Click the License tab to allocate licenses or license hours per agent on this domain.
8. Click Ok. The Domains window opens with the name and description of the new domain.

After the domain is created and has an assigned DSM Domain Administrator, hosts can be added to it.

4 Add a NetApp Cluster with a Unique Client Certificate to Each DSM as a Host

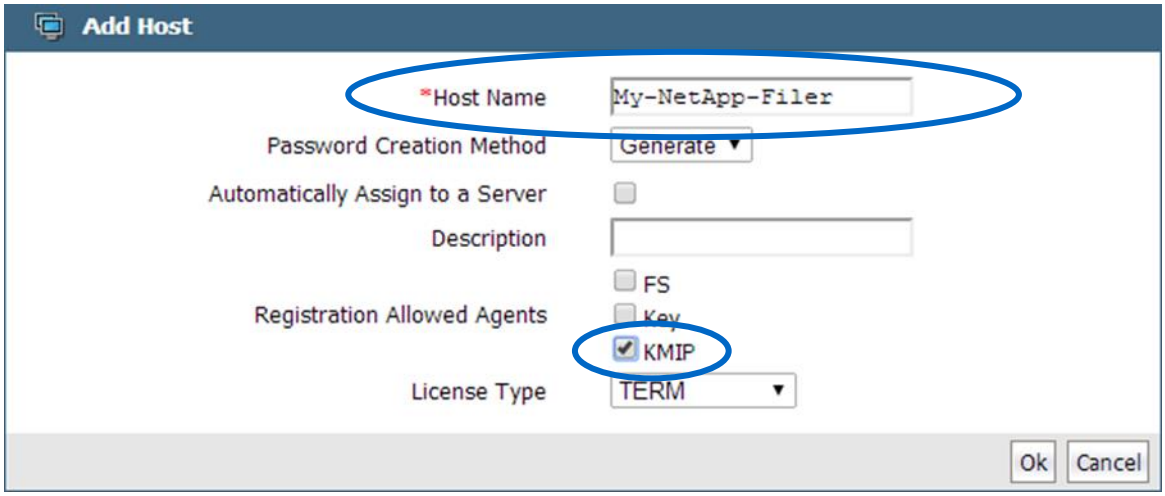
NetApp controllers are managed as hosts in the DSM. The NetApp controller appears in the DSM Management Console as a KMIP agent type because it uses the KMIP protocol to communicate.



To add a NetApp controller as a host, complete the following steps:

1. To switch to the domain that serves the KMIP clients, select Domain > Switch Domains, select a domain, and click Switch to Domain.
2. From the menu bar, select Hosts > Hosts. The Hosts window opens.
3. Click Add. The Add Host window opens.
4. In the Host Name field, enter the name of your NetApp cluster. This name is used when you generate the certificate. You must use exactly the same name when you upload the certificate.

5. Leave Password Creation Method as Generate.
6. Leave Automatically Assign to a Server unchecked.
7. (Optional) In the Description field, enter a description for the NetApp controller.
8. For Registration Allowed Agents, check the KMIP box.
9. From the License Type list, select the option specified in your license.



10. Click Ok. The Hosts window opens.
11. Click the host name of the host you just added. The Edit Host window opens.
12. Under the General tab in the Agent Information area, select Communication Enabled in the KMIP row.
13. The Certificate Fingerprint column should be empty.
14. Click Ok. The Hosts window opens.
15. Repeat steps 3 through 14 for all the NetApp controllers.

Because each DSM is configured as an independent primary DSM (as described in the section “High-Availability Considerations”), this entire process must be performed on each DSM.

5 Confirm the Version of ONTAP

ONTAP 9.x or later should be installed. Use caution when running ONTAP 9.x or later. Systems running SE should not be downgraded below 8.3.2, because challenges can arise with recognizing disks or KMIP functionality.

6 Establish Trust Between the Vormetric DSMs and the NetApp Controllers

The KMIP protocol requires the use of a mutually authenticated TLS connection between a KMIP client and a KMIP server. In other words, the client must cryptographically trust that it’s talking to the server, and the server must cryptographically trust that it’s talking to the client. This trust is built through the use of certificates. This section describes procedures for creating certificates and moving them around so that the Vormetric DSM and the NetApp controller trust each other.

6.1 Extract the Signing CA Certificate from Each DSM

For this first step, it is necessary to acquire the internal CA certificate used inside the DSM. This certificate is used to reassure the NetApp cluster that it is indeed talking to the Vormetric DSM. This CA certificate must be acquired from each DSM.

The name of the file containing the CA certificate has a special format; it must look like `DSM_CA.pem`. This example is used for the rest of this document.

There are two methods for acquiring this certificate. The first is on Windows, using a browser to connect to the UI. The second is on Linux, using the `openssl` command to talk to the UI port.

Extracting the CA Certificate on Windows by Using a Web Browser

1. Navigate to the DSM UI.
2. Click the lock icon (Chrome) or the certificate error (IE).
3. Click Certificate Information (Chrome) or View Certificates (IE). The Certificate Information window opens.
4. Click the Certification Path tab.
5. Select the top certificate, which starts with `CG CA (S)` on […].
6. Click View Certificate.
7. Click the Details tab.
8. Click Copy to File.
9. Click Next, select Base-64 encoded X.509, and click Next again.
10. Enter a file name for the certificate.
11. Click Next and then click Finish.
12. Locate the file you just saved and open it with a text editor. It should start with `-----BEGIN CERTIFICATE-----` and end with `-----END CERTIFICATE-----`. It's generally easiest to copy the contents of this file to the file `DSM_CA.pem`.

Extracting the CA Certificate on Linux with OpenSSL

Alternatively, you can acquire the same certificate through a different procedure on Linux by using the OpenSSL program. To do so, complete the following steps:

1. Locate a Linux machine with the `openssl` utility installed.
2. Run the following command:

```
openssl s_client -connect your.dsm.name.com:8443 -showcerts
```

3. A lot of output scrolls past. The second block of base-64 encoded text (between `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE -----`) is the certificate of interest. Copy this text into the file `DSM_CA.pem`.

Testing the CA Certificate

To quickly test the certificate, use the `openssl` command:

```
$ openssl s_client -connect kmip-interop.vormetric.com:5696 -showcerts -CAfile DSM_CA.pem
```

A lot of output scrolls past; look for the very last line:

```
    Verify return code: 0 (ok)
```

If you see this line, your certificate file is valid.This process (all of section 6.1) must be repeated for each primary DSM, unless the DSMs are all using the same CA. In that case, the process does not need to be repeated.

6.2 Create a Certificate for the Controller

After creating certificates that identify the DSMs, you must create certificates that identify the NetApp cluster. For this purpose, use openssl to create self-signed certificates. Normally, NetApp recommends against the use of self-signed certificates, but in this case you explicitly approve and use these certificates.

To create a self-signed certificate by using the openssl utility on a Linux machine, complete the following steps:

1. Create a 2048-bit RSA key.

```
$ openssl genrsa –out client_private.pem 2048
```

2. Create a self-signed certificate using that key.

```
$ openssl req -new -x509 -key client_private.pem -out client.pem -days 365
```

3. Follow the prompts. When asked for the common name, enter the cluster name that you supplied when you added the NetApp cluster to the DSM. This name must be a perfect match.

You now have two files: `client_private.pem` and `client.pem`. The first contains the key, and the second contains the certificate.

6.3 Upload the NetApp Cluster's KMIP Client Certificates to the DSM

First, provide the NetApp cluster's KMIP client certificate that you just created to the DSM. Each NetApp cluster's KMIP client certificate is uploaded to the corresponding host in the DSM. To upload the client certificates, complete the following steps:

1. To switch to the domain that serves the KMIP clients, click Domain > Switch Domains, select a domain, and then click Switch to Domain.
2. From the menu bar, select Hosts > Hosts. The Hosts window opens.
3. Click the host name for the target cluster. The Edit Host page opens.
4. Click the Upload KMIP Cert button in the lower-right corner.
5. Navigate to the corresponding NetApp cluster and click OK.

Repeat this process in the DSM for each controller. Then repeat it again on each DSM. That is, if you have two DSMs and two controllers, create two certificates (one for each controller) and upload each of those certificates to its corresponding host on the first DSM. Then upload each of those certificates to its corresponding host on the second DSM.

6.4 Import the Certificates into ONTAP

Note: The certificates must be installed prior to running the key-manager setup operation (see the section "Configuring the Storage Encryption System").

To review, import the following files:

- The NetApp cluster's KMIP client certificate.
- The private key that corresponds to that certificate.
- `1.2.3.4_CA.pem`, the signing certificate for the DSM. There is one of these for each DSM.

To import certificates into clustered Data ONTAP, use the security certificate install command as follows, and as outlined in the ONTAP 9 NetApp Encryption Power Guide:

1. 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
```

2. You are then prompted to paste in the certificate contents (the contents of `client.pem`). In addition, you are asked to paste in the private key (the contents of `client_private.pem`) when installing the client KMIP certificate.

To install the KMIP server certificate CA, run the following command:

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

When asked about additional CAs or intermediate certificates, it is not necessary to enter anything.

Note: When installing the KMIP server 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.

6.5 Configure ONTAP to Use These Certificates

Before ONTAP can be configured, certain boot environment variables must be configured.

Configuring BOOTARG.STORAGEENCRYPTION.SUPPORT

`BOOTARG.STORAGEENCRYPTION.SUPPORT` is typically set during the manufacturing process. However, if the encrypted disks do not show up at boot time, follow these steps to verify that the preceding bootarg is set to true:

1. Halt ONTAP and stop at the `LOADER-(A,B)>` prompt and run the following command:

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

2. Confirm that this value is set.

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

3. The output should look like this:

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

Configuring the Storage Encryption System

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. A minimum of two is recommended for redundancy and disaster recovery.

To set up external key management servers, complete the following steps:

1. 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 node 5 and node 6 with encrypting drives are added to an existing four-node cluster and the cluster management LIF is located on node 1, then run the following commands:

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

2. Run the following CLI to launch the key management setup wizard and 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 Vormetric
appliance, not the Vormetric management IP >
Enter the netmask [255.255.192.0]: < is the netmask of the Vormetric appliance >
Enter the gateway [10.63.0.1]: < is the gateway of the Vormetric appliance >
Would you like to configure an IPv6 address? {yes, no} [no]: no
```

3. Run the following CLI to configure Data ONTAP for storage encryption. (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 Vormetric appliance, not the Vormetric management IP >
Enter the IPv6 address prefix length [64]: <IPv6 address prefix length of the Vormetric appliance
>
Enter the IPv6 gateway: fd20:8b1e:b255:208:250:56ff:fea2:200 <IPv6 gateway of the Vormetric
appliance >.
```

- `<Network Interface>` is set to the NetApp port the node management LIF is located on, including the VLAN if required (examples include e0M, e0a, e0a-16, and a0a-16). This interface cannot participate in network trunking or VIF configuration.

- <IP Address> is set to the application IP address of the Vormetric appliance, not the Vormetric management IP.
- <Netmask> is the netmask of the Vormetric appliance.
- <Gateway> is the gateway of the Vormetric appliance.

Verifying External Key Manager Communication with the Cluster

The following commands can be used to verify cluster communications with the key manager:

- **Security key-manager query.** This command is used by the cluster to retrieve and validate the key ID info from the key manager.
- **Security key-manager show.** This command can be used to display the key management servers confiugured on the cluster.

For more details on key manager commands and configuration see the ONTAP 9 security key manager command pages.

Appendix A: Deleting Certificates

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

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, and they should be replaced before the expiration date. To replace certificates, follow the steps described in the section “Establish Trust Between the Vormetric DSMs and the NetApp Controllers.”

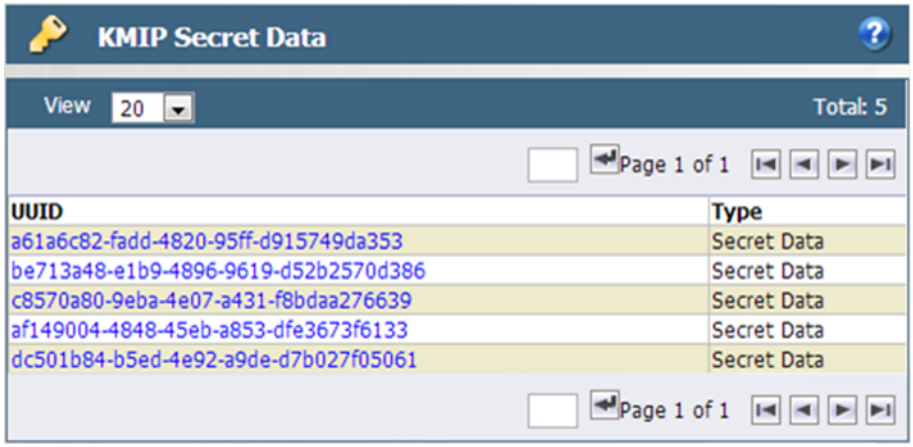
Appendix C: Viewing KMIP Keys on the DSM

When a NetApp controller boots, the SEDs need passphrases. The NetApp controller uses KMIP to retrieve the passphrases from the DSM. The passphrases are stored as secret data, not as keys. For security reasons, the form of the data is opaque to KMIP, and the value is never displayed in the DSM.

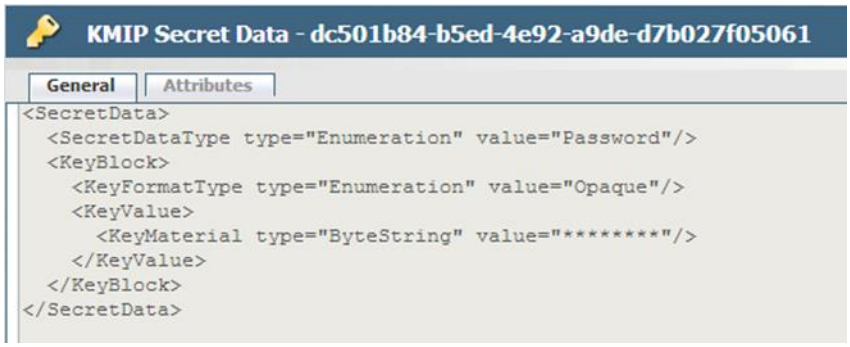
To see the KMIP secret data, complete the following steps:

1. On the primary DSM, log in to the management console as an administrator of type System Administrator or All.
2. To switch to the domain that serves the KMIP clients, select Domain > Switch Domains.
3. Select a domain and click Switch to Domain.

4. Select Keys > KMIP Secret Data. The KMIP Secret Data window opens, showing the following columns:
   - **UUID (Universal Unique Identifier).** This 128-bit identifier is a pointer to the KMIP passphrase. Click the UUID to open a text window that displays the passphrase or key for the self-encrypting drives and other passphrases in the system, such as secret data.
   - **Type.** Displays the classification or type of passphrase represented by the UUID.



5. Click the UUID to see the secret data in XML format.



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.

Copyright Information

Trademark Information