



ONTAP® 9

NetApp® Encryption Power Guide

February 2018 | 215-11633_H0
doccomments@netapp.com

Updated for ONTAP 9.3

 **NetApp®**

Contents

Deciding whether to use the NetApp Encryption Power Guide	5
Configuring NetApp Volume Encryption	6
NetApp Volume Encryption workflow	7
Configuring NVE	8
Determining whether your cluster version supports NVE	8
Installing the license	8
Configuring external key management	9
Enabling onboard key management	12
Encrypting volume data with NVE	13
Enabling encryption on a new volume	13
Enabling encryption on an existing volume with the volume encryption conversion start command	14
Enabling encryption on an existing volume with the volume move start command	15
Configuring NetApp Storage Encryption	17
NetApp Storage Encryption workflow	18
Configuring external key management	18
Collecting network information (ONTAP 9.2 and earlier)	18
Installing SSL certificates on the cluster	19
Enabling external key management (ONTAP 9.3)	20
Enabling external key management (ONTAP 9.2 and earlier)	21
Creating authentication keys (ONTAP 9.3)	23
Creating authentication keys (ONTAP 9.2 and earlier)	24
Assigning a data authentication key to SEDs	25
Assigning a FIPS 140-2 authentication key to SEDs	26
Enabling cluster-wide FIPS-compliant mode for KMIP server connections	27
Configuring onboard key management	28
Enabling onboard key management	28
Viewing the keys generated by the Onboard Key Manager	29
Assigning a data authentication key to SEDs	30
Assigning a FIPS 140-2 authentication key to SEDs	31
Managing NetApp encryption	32
Unencrypting volume data	32
Moving an encrypted volume	33
Delegating authority to run the volume move command	34
Changing the encryption key for a volume with the volume encryption rekey start command	34
Changing the encryption key for a volume with the volume move start command	35
Deleting an encrypted volume	36

Restoring onboard key management encryption keys	37
Changing the onboard key management passphrase	38
Backing up onboard key management information manually	39
Restoring external key management authentication keys (9.3)	40
Restoring external key management authentication keys (9.2 and earlier)	40
Replacing an SED	41
Replacing SSL certificates	42
Making data on an SED inaccessible	43
Sanitizing an SED	44
Destroying an SED	45
Emergency shredding of data on an SED	46
Returning SEDs to service when authentication keys are lost	48
Returning SEDs to unprotected mode	49
Deleting an external key manager connection (9.3)	50
Deleting an external key manager connection (9.2 and earlier)	51
Transitioning to external key management from onboard key management	52
Transitioning to onboard key management from external key management	52
What happens when key management servers are not reachable during the boot process	53
NVE APIs	54
Where to find additional information	55
Copyright information	56
Trademark information	57
How to send comments about documentation and receive update notifications	58
Index	59

Deciding whether to use the NetApp Encryption Power Guide

NetApp offers both software- and hardware-based encryption technologies for ensuring that data at rest cannot be read if the storage medium is repurposed, returned, misplaced, or stolen.

- Software-based NetApp Volume Encryption (NVE) supports data encryption one volume at a time.
- Hardware-based NetApp Storage Encryption (NSE) supports full-disk encryption (FDE).

You should use this guide if you want to work with encryption in the following way:

- You want to use best practices, not explore every available option.
- You do not want to read a lot of conceptual background.
- You want to use the ONTAP command-line interface (CLI), not OnCommand System Manager or an automated scripting tool.

The encryption technologies are not supported by System Manager.

If this guide is not suitable for your situation, you should see the following documentation instead:

- [*ONTAP 9 commands*](#)
- [*NetApp Documentation: OnCommand Workflow Automation \(current releases\)*](#)

Configuring NetApp Volume Encryption

NetApp Volume Encryption (NVE) is a software-based technology for encrypting data at rest one volume at a time. An encryption key accessible only to the storage system ensures that volume data cannot be read if the underlying device is repurposed, returned, misplaced, or stolen.

Understanding NVE

Both data, including Snapshot copies, and metadata are encrypted. Access to the data is given by a unique XTS-AES-256 key, one per volume. An external key management server or Onboard Key Manager serves keys to nodes:

- The external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP).
- The Onboard Key Manager is a built-in tool that serves keys to nodes from the same storage system as your data.

You can enable encryption on a new or existing volume. NVE supports the full range of storage efficiency features, including deduplication and compression.

You can use NVE on any type of aggregate (HDD, SSD, hybrid, array LUN), with any RAID type, and in any supported ONTAP implementation, including ONTAP Select. You can also use NVE with NetApp Storage Encryption (NSE) to “double encrypt” data on NSE drives.

When to use KMIP servers

Although it is less expensive and typically more convenient to use the onboard key manager, you should set up KMIP servers if any of the following are true:

- Your encryption key management solution must comply with Federal Information Processing Standards (FIPS) 140-2 or the OASIS KMIP standard.
- You need a multi-cluster solution.
KMIP servers support multiple clusters with centralized management of encryption keys.
- Your business requires the added security of storing authentication keys on a system or in a location different from the data.
KMIP servers store authentication keys separately from your data.

Support details

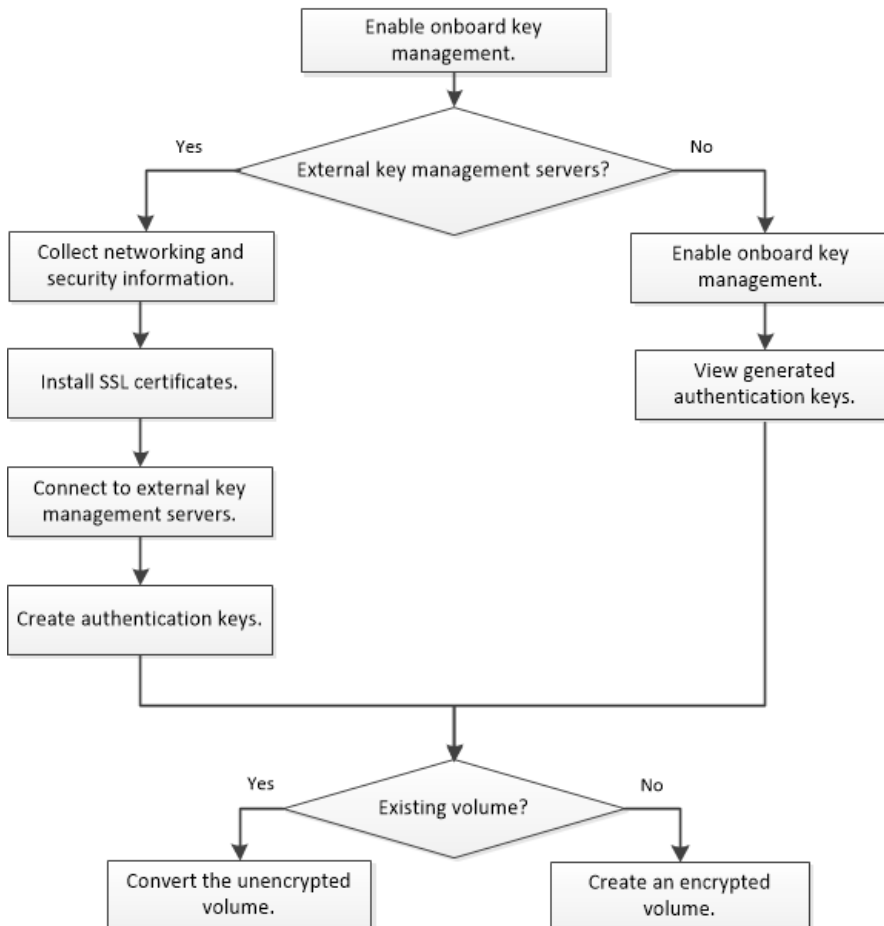
The following table shows NVE support details.

Resource or feature	Support details
Platforms	AES-NI offload capability required: FAS 2620, FAS 2650, FAS 6290, FAS 80xx, FAS 8200, FAS 9000, AFF A200, AFF A300, AFF A700, or AFF A700S.
ONTAP	All ONTAP implementations, except ONTAP Cloud.
Devices	HDD, SSD, hybrid, array LUN.
RAID	RAID0, RAID4, RAID-DP, RAID-TEC.
Volumes	Data volumes only. You cannot encrypt data on a root volume, an SVM root volume, or a MetroCluster metadata volume.
Storage efficiency	Deduplication, compression, compaction, FlexClone. Clones use the same key as the parent, even after splitting the clone from the parent. You are warned to rekey the split clone.

Resource or feature	Support details
Replication	<ul style="list-style-type: none"> For volume replication, the destination volume must have been enabled for encryption. For SVM replication, the destination volume is automatically encrypted, unless the destination does not contain a node that supports volume encryption, in which case replication succeeds, but the destination volume is not encrypted. For MetroCluster configurations, keys and passphrases are replicated to the partner site by the configuration replication service (CRS).
Compliance	Starting with ONTAP 9.2, SnapLock is supported.
FlexGroups	Starting with ONTAP 9.2, FlexGroups are supported.
7-Mode transition	Integration with the 7-Mode Transition Tool is not supported. Transition an existing volume as you would currently, then use <code>volume move</code> to enable encryption on the volume.

NetApp Volume Encryption workflow

You must configure key management services before you can enable volume encryption. You can enable encryption on a new volume or on an existing volume.



Configuring NVE

You must install the NVE license and configure key management services before you can encrypt data with NVE. Before installing the license, you should determine whether your ONTAP version supports NVE.

Determining whether your cluster version supports NVE

You should determine whether your cluster version supports NVE before you install the license. You can use the `version` command to determine the cluster version.

About this task

The cluster version is the lowest version of ONTAP running on any node in the cluster.

Step

1. Determine whether your cluster version supports NVE:

```
version -v
```

NVE is not supported if the command output displays the text “no-DARE” (for “no Data At Rest Encryption”).

Example

The following command determines whether NVE is supported on `cluster1`.

```
cluster1::> version -v
NetApp Release 9.1.1.0: Tue May 10 19:30:23 UTC 2016 <1no-DARE>
```

The text “1no-DARE” in the command output indicates that NVE is not supported on your cluster version.

Installing the license

An NVE license entitles you to use the feature on all nodes in the cluster. You must install the license before you can encrypt data with NVE.

Before you begin

You must be a cluster administrator to perform this task.

About this task

You should have received the NVE license key from your sales representative.

Steps

1. Install the NVE license for a node:

```
system license add -license-code license_key
```

Example

The following command installs the license with the key `AAAAAAAAAAAAAAAAAAAAAAAAAAAA`.

```
cluster1::> system license add -license-code AAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```


- Verify that the license is installed by displaying all the licenses on the cluster:

```
system license show
```

For complete command syntax, see the man page for the command.

Example

The following command displays all the licenses on `cluster1`:

```
cluster1::> system license show
```

The NVE license package name is “VE”.

Configuring external key management

You can use one or more external key management servers to secure the keys that the cluster uses to access encrypted data. An external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP).

Collecting network information (ONTAP 9.2 and earlier)

If you are using ONTAP 9.2 or earlier, you should fill out the network configuration worksheet before enabling external key management.

Note: Starting with ONTAP 9.3, the system discovers all needed network information automatically.

Item	Notes	Value
Key management network interface name		
Key management network interface IP address	IP address of node management LIF, in IPv4 or IPv6 format	
Key management network interface IPv6 network prefix length	If you are using IPv6, the IPv6 network prefix length	
Key management network interface subnet mask		
Key management network interface gateway IP address		
IPv6 address for the cluster network interface	Required only if you are using IPv6 for the key management network interface	
Port number for each KMIP server	Optional. The port number must be the same for all KMIP servers. If you do not provide a port number, it defaults to port 5696, which is the Internet Assigned Numbers Authority (IANA) assigned port for KMIP.	
Key tag name	Optional. The key tag name is used to identify all keys belonging to a node. The default key tag name is the node name.	

Related information

NetApp Technical Report 3954: NetApp Technical Report 3954: NetApp Storage Encryption Preinstallation Requirements and Procedures for IBM Tivoli Lifetime Key Manager

NetApp Technical Report 4074: NetApp Technical Report 4074: NetApp Storage Encryption Preinstallation Requirements and Procedures for SafeNet KeySecure

Installing SSL certificates on the cluster

The cluster and KMIP server use KMIP SSL certificates to verify each other's identity and establish an SSL connection. Before configuring the SSL connection with the KMIP server, you must install the KMIP client SSL certificates for the cluster, and the SSL public certificate for the root certificate authority (CA) of the KMIP server.

Before you begin

- The time must be synchronized on the server creating the certificates, the KMIP server, and the cluster.
- You must have obtained the public SSL KMIP client certificate (`client.pem`) for the cluster.
- You must have obtained the private SSL KMIP client certificate (`client_private.pem`) for the cluster.

The SSL KMIP client certificate must not be password-protected.

- You must have obtained the SSL public certificate for the root certificate authority (CA) (`key_management_server_ipaddress_CA.pem`) of the KMIP server.

Note: You can install the client and server certificates on the KMIP server before or after installing the certificates on the cluster.

About this task

In an HA pair, both nodes must use the same public and private KMIP SSL certificates. If you connect multiple HA pairs to the same KMIP server, all nodes in the HA pairs must use the same public and private KMIP SSL certificates.

Steps

1. Install the SSL KMIP client certificates for the cluster:

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

You are prompted to enter the SSL KMIP public and private certificates.

Example

```
cluster1::> security certificate install -vserver svml -type client -
subtype kmip-cert
```

2. Install the SSL public certificate for the root certificate authority (CA) of the KMIP server:

```
security certificate install -vserver admin_svm_name -type server-ca -
subtype kmip-cert
```

Example

```
cluster1::> security certificate install -vserver svml -type server-ca -
subtype kmip-cert
```

Enabling external key management (ONTAP 9.3)

You can use one or more KMIP servers to secure the keys that the cluster uses to access encrypted data. You can connect up to four KMIP servers to a node. A minimum of two servers is recommended for redundancy and disaster recovery.

Before you begin

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster administrator to perform this task.

About this task

ONTAP configures KMIP server connectivity for all nodes in the cluster.

Note: NVE support for KMIP server authentication is available starting in ONTAP 9.3.

Steps

1. If you are upgrading to ONTAP 9.3 from a previous version, delete any external key management configurations for the cluster:

```
security key-manager delete-kmip-config
```

Example

The following command deletes the external key management configurations for `cluster1`:

```
cluster1::> security key-manager delete-kmip-config
```

2. Configure key manager connectivity for cluster nodes:

```
security key-manager setup
```

The key manager setup wizard opens.

3. Enter the appropriate response at each prompt.
4. Add a KMIP server:

```
security key-manager add -address key_management_server_ipaddress
```

Example

```
cluster1::> security key-manager add -address 20.1.1.1
```

5. Add an additional KMIP server for redundancy:

```
security key-manager add -address key_management_server_ipaddress
```

Example

```
cluster1::> security key-manager add -address 20.1.1.2
```

6. Verify that all configured KMIP servers are connected:

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

For complete command syntax, see the man page.

Example

```
cluster1::> security key-manager show -status
```

Node	Port	Registered Key Manager	Status
cluster1-01	5696	20.1.1.1	available
cluster1-01	5696	20.1.1.2	available
cluster1-02	5696	20.1.1.1	available
cluster1-02	5696	20.1.1.2	available

Enabling onboard key management

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk (SED).

Before you begin

- If you are using NSE with an external key management (KMIP) server, you must have deleted the external key manager database.
Transitioning to onboard key management from external key management on page 52
- You must be a cluster administrator to perform this task.

About this task

You must run this command each time you add a node to the cluster.

Steps

1. Start the key manager setup wizard:

```
security key-manager setup
```

Example

The following command starts the key manager setup wizard on **cluster1**:

```
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 use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase: <32..256 UTF8 characters long text>
Reenter the cluster-wide passphrase: <32..256 UTF8 characters long text>
```

2. Enter **yes** at the prompt to configure onboard key management.
3. Enter a passphrase between 32 and 256 characters at the passphrase prompt.
4. Re-enter the passphrase at the passphrase confirmation prompt.
5. Verify that keys are configured for all nodes:

```
security key-manager key show
```

For complete command syntax, see the man page.


```
cluster1::> volume create -vserver vs1 -volume voll -aggregate aggr1 -
encrypt true
```

The system creates an encryption key for the volume. Any data you put on the volume is encrypted.

2. Verify that the volume is enabled for encryption:

```
volume show -is-encrypted true
```

For complete command syntax, see the man page for the command.

Example

The following command displays the encrypted volumes on **cluster1**:

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
vs1	voll	aggr2	online	RW	200GB	160.0GB	20%

Enabling encryption on an existing volume with the volume encryption conversion start command

Starting with ONTAP 9.3, you can use the `volume encryption conversion start` command to enable encryption on an existing volume.

About this task

Once you start a conversion operation, it must complete. If you encounter a performance issue during the operation, you can run the `volume encryption conversion pause` command to pause the operation, and the `volume encryption conversion restart` command to resume the operation.

Note: You cannot use `volume encryption conversion start` to convert a SnapLock or FlexGroup volume. You must use the `volume move start` command.

[Enabling encryption on an existing volume with the volume move start command](#) on page 15

Steps

1. Enable encryption on an existing volume:

```
volume encryption conversion start -vserver SVM_name -volume volume_name
```

For complete command syntax, see the man page for the command.

Example

The following command enables encryption on the existing volume **voll**:

```
cluster1::> volume encryption conversion start -vserver vs1 -volume
voll
```

The system creates an encryption key for the volume. The data on the volume is encrypted.

2. Verify the status of the conversion operation:

```
volume encryption conversion show
```

For complete command syntax, see the man page for the command.

Example

The following command displays the status of the conversion operation:

```
cluster1::> volume encryption conversion show
```

Vserver	Volume	Start Time	Status
vs1	vol1	9/18/2017 17:51:41	Phase 2 of 2 is in progress.

3. When the conversion operation is complete, verify that the volume is enabled for encryption:

```
volume show -is-encrypted true
```

For complete command syntax, see the man page for the command.

Example

The following command displays the encrypted volumes on **cluster1**:

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
vs1	vol1	aggr2	online	RW	200GB	160.0GB	20%

Result

If you are using a KMIP server to authenticate nodes to the system, ONTAP automatically “pushes” an authentication key to the server when you encrypt a volume.

Enabling encryption on an existing volume with the volume move start command

You can use the `volume move start` command to enable encryption on an existing volume. You must use `volume move start` in ONTAP 9.2 and earlier, and in ONTAP 9.3, if you are enabling encryption on a SnapLock or FlexGroup volume. You can use the same aggregate or a different aggregate.

Before you begin

You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

[Delegating authority to run the volume move command](#) on page 34

About this task

Starting with ONTAP 9.2, you can enable encryption on a SnapLock or FlexGroup volume.

Steps

1. Move an existing volume and enable encryption on the volume:

```
volume move start -vserver SVM_name -volume volume_name -destination-  
aggregate aggregate_name -encrypt-destination true|false
```

For complete command syntax, see the man page for the command.

Example

The following command moves an existing volume named **vol1** to the destination aggregate **aggr2** and enables encryption on the volume:

```
cluster1::> volume move start -vserver vs1 -volume voll -destination-
aggregate aggr2 -encrypt-destination true
```

The system creates an encryption key for the volume. The data on the volume is encrypted.

2. Verify that the volume is enabled for encryption:

```
volume show -is-encrypted true
```

For complete command syntax, see the man page for the command.

Example

The following command displays the encrypted volumes on **cluster1**:

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
vs1	voll	aggr2	online	RW	200GB	160.0GB	20%

Result

If you are using a KMIP server to authenticate nodes to the system, ONTAP automatically “pushes” an authentication key to the server when you encrypt a volume.

Configuring NetApp Storage Encryption

NetApp Storage Encryption (NSE) supports "self-encrypting" disks (SEDs) that encrypt data as it is written. The data cannot be read without an encryption key stored on the disk. The encryption key, in turn, is accessible only to an authenticated node.

Understanding NSE

On an I/O request, a node authenticates itself to an SED using an authentication key retrieved from an external key management server or Onboard Key Manager:

- The external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP).
- The Onboard Key Manager is a built-in tool that serves authentication keys to nodes from the same storage system as your data.

NSE supports self-encrypting HDDs and SSDs. You can use NetApp Volume Encryption with NSE to "double encrypt" data on NSE drives.

When to use KMIP servers

Although it is less expensive and typically more convenient to use the onboard key manager, you should set up KMIP servers if any of the following are true:

- Your encryption key management solution must comply with Federal Information Processing Standards (FIPS) 140-2 or the OASIS KMIP standard.
- You need a multi-cluster solution.
KMIP servers support multiple clusters with centralized management of encryption keys.
- Your business requires the added security of storing authentication keys on a system or in a location different from the data.
KMIP servers stores authentication keys separately from your data.

Support details

The following table shows important NSE support details. See the Interoperability Matrix for the latest information about supported KMIP servers, storage systems, and disk shelves.

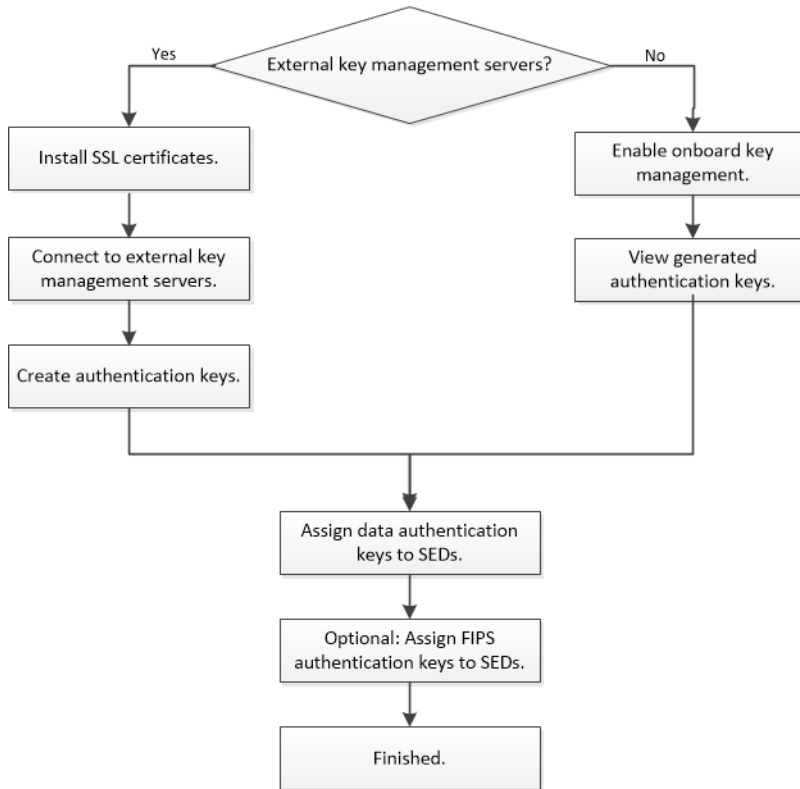
Resource or feature	Support details
MetroCluster	NSE does not support MetroCluster.
Non-homogenous disk sets	All disks for a node or HA pair must be self-encrypting. Conforming HA pairs can coexist with non-conforming HA pairs in the same cluster.
10 Gb network interfaces	Starting with ONTAP 9.3, NSE supports 10 Gb network interfaces for communications with external key management servers.
Ports for communication with the key management server	Starting with ONTAP 9.3, you can use any storage controller port for communication with the key management server. Otherwise, you should use port e0m for communication with key management servers. Depending on the storage controller model, certain network interfaces might not be available during the boot process for communication with key management servers.

Related information

[NetApp Interoperability Matrix Tool](#)

NetApp Storage Encryption workflow

You must configure key management services before the cluster can authenticate itself to the SED. You can use an external key management server or an onboard key manager.



Configuring external key management

You can use one or more external key management servers to secure the keys that the cluster uses to access encrypted data. An external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP).

Collecting network information (ONTAP 9.2 and earlier)

If you are using ONTAP 9.2 or earlier, you should fill out the network configuration worksheet before enabling external key management.

Note: Starting with ONTAP 9.3, the system discovers all needed network information automatically.

Item	Notes	Value
Key management network interface name		

Item	Notes	Value
Key management network interface IP address	IP address of node management LIF, in IPv4 or IPv6 format	
Key management network interface IPv6 network prefix length	If you are using IPv6, the IPv6 network prefix length	
Key management network interface subnet mask		
Key management network interface gateway IP address		
IPv6 address for the cluster network interface	Required only if you are using IPv6 for the key management network interface	
Port number for each KMIP server	Optional. The port number must be the same for all KMIP servers. If you do not provide a port number, it defaults to port 5696, which is the Internet Assigned Numbers Authority (IANA) assigned port for KMIP.	
Key tag name	Optional. The key tag name is used to identify all keys belonging to a node. The default key tag name is the node name.	

Related information

[NetApp Technical Report 3954: NetApp Technical Report 3954: NetApp Storage Encryption Preinstallation Requirements and Procedures for IBM Tivoli Lifetime Key Manager](#)
[NetApp Technical Report 4074: NetApp Technical Report 4074: NetApp Storage Encryption Preinstallation Requirements and Procedures for SafeNet KeySecure](#)

Installing SSL certificates on the cluster

The cluster and KMIP server use KMIP SSL certificates to verify each other's identity and establish an SSL connection. Before configuring the SSL connection with the KMIP server, you must install the KMIP client SSL certificates for the cluster, and the SSL public certificate for the root certificate authority (CA) of the KMIP server.

Before you begin

- The time must be synchronized on the server creating the certificates, the KMIP server, and the cluster.
- You must have obtained the public SSL KMIP client certificate (`client.pem`) for the cluster.
- You must have obtained the private SSL KMIP client certificate (`client_private.pem`) for the cluster.
The SSL KMIP client certificate must not be password-protected.
- You must have obtained the SSL public certificate for the root certificate authority (CA) (`key_management_server_ipaddress_CA.pem`) of the KMIP server.

Note: You can install the client and server certificates on the KMIP server before or after installing the certificates on the cluster.

About this task

In an HA pair, both nodes must use the same public and private KMIP SSL certificates. If you connect multiple HA pairs to the same KMIP server, all nodes in the HA pairs must use the same public and private KMIP SSL certificates.

Steps

1. Install the SSL KMIP client certificates for the cluster:

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

You are prompted to enter the SSL KMIP public and private certificates.

Example

```
cluster1::> security certificate install -vserver svml -type client -
subtype kmip-cert
```

2. Install the SSL public certificate for the root certificate authority (CA) of the KMIP server:

```
security certificate install -vserver admin_svm_name -type server-ca -
subtype kmip-cert
```

Example

```
cluster1::> security certificate install -vserver svml -type server-ca -
subtype kmip-cert
```

Enabling external key management (ONTAP 9.3)

You can use one or more KMIP servers to secure the keys that the cluster uses to access encrypted data. You can connect up to four KMIP servers to a node. A minimum of two servers is recommended for redundancy and disaster recovery.

Before you begin

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster administrator to perform this task.

About this task

ONTAP configures KMIP server connectivity for all nodes in the cluster.

Note: NVE support for KMIP server authentication is available starting in ONTAP 9.3.

Steps

1. If you are upgrading to ONTAP 9.3 from a previous version, delete any external key management configurations for the cluster:

```
security key-manager delete-kmip-config
```

Example

The following command deletes the external key management configurations for `cluster1`:

```
cluster1::> security key-manager delete-kmip-config
```

2. Configure key manager connectivity for cluster nodes:

```
security key-manager setup
```

The key manager setup wizard opens.

3. Enter the appropriate response at each prompt.
4. Add a KMIP server:

```
security key-manager add -address key_management_server_ipaddress
```

Example

```
cluster1::> security key-manager add -address 20.1.1.1
```

5. Add an additional KMIP server for redundancy:

```
security key-manager add -address key_management_server_ipaddress
```

Example

```
cluster1::> security key-manager add -address 20.1.1.2
```

6. Verify that all configured KMIP servers are connected:

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

For complete command syntax, see the man page.

Example

```
cluster1::> security key-manager show -status
```

Node	Port	Registered Key Manager	Status
cluster1-01	5696	20.1.1.1	available
cluster1-01	5696	20.1.1.2	available
cluster1-02	5696	20.1.1.1	available
cluster1-02	5696	20.1.1.2	available

Enabling external key management (ONTAP 9.2 and earlier)

A node authenticates itself to the system using an authentication key retrieved from the KMIP server. You can connect up to four KMIP servers to a node. A minimum of two servers is recommended for redundancy and disaster recovery.

Before you begin

- If you are using NetApp Storage Encryption, all disks in the node or HA pair must be self-encrypting.
See the Interoperability Matrix for disks that support NSE.
- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster administrator to perform this task.

About this task

Each node in an HA pair must be able to access the other's disks in the event of a takeover. For that reason, you should configure key manager connectivity for each node in the pair.

Steps

1. Configure key manager connectivity for a node:

```
security key-manager setup -node node
```

`node` defaults to the current node.

The key manager setup wizard opens.

2. Enter the information you specified in the configuration worksheet:
 - Select `no` when prompted to use onboard key management.
 - Enter `e0m` as the network interface.
 - Enter the IP address of the node management LIF, in IPv4 or IPv6 format.

Example

```
cluster1::> security key-manager setup

Would you like to configure onboard key-management? {yes, no} [no]:
Would you like to use KMIP server configuration? {yes, no} [yes]:

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]:

Enter the IP address: [20.1.1.1]:
Enter the netmask: [255.255.1.1]:
Enter the gateway: [20.1.1.5]:
Would you like to configure an IPv6 address? {yes, no} [no]:
```

3. Repeat these steps for the partner node.
4. Add an additional KMIP server for redundancy:

```
security key-manager add -address key_management_server_ipaddress
```

Example

```
cluster1::> security key-manager add -address 20.1.1.2
```

5. Verify that all configured KMIP servers are connected:

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

For complete command syntax, see the man page.

Example

```
cluster1::> security key-manager show -status
```

Node	Registered Key Manager	Status
cluster1-01	20.1.1.1	available
cluster1-01	20.1.1.2	available
cluster1-02	20.1.1.1	available
cluster1-02	20.1.1.2	available

Related information

[NetApp Interoperability Matrix Tool](#)

Creating authentication keys (ONTAP 9.3)

You can use the `security key-manager create-key` command to create the authentication keys for a node and store them on the configured KMIP servers.

Before you begin

You must be a cluster administrator to perform this task.

About this task

If you are using NetApp Storage Encryption and your security setup requires you to use different keys for data authentication and FIPS 140-2 authentication, you should create a separate key for each. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

ONTAP creates authentication keys for all nodes in the cluster.

- This command is not supported when onboard key management is enabled.
- You receive a warning if the configured key management servers are already storing more than 128 authentication keys.

You can use the key management server software to delete any unused keys, then run the command again.

Steps

1. Create the authentication keys for cluster nodes:

```
security key-manager create-key
```

For complete command syntax, see the man page for the command.

Note: The key ID displayed in the output is an identifier used to refer to the authentication key. It is not the actual authentication key or the data encryption key.

Example

```
cluster1::> security key-manager create-key
(security key-manager create-key)
Verifying requirements...

Node: cluster1-01
Creating authentication key...
Authentication key creation successful.
Key ID:
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C

Node: cluster1-01
Key manager restore operation initialized.
Successfully restored key information.

Node: cluster1-02
Key manager restore operation initialized.
Successfully restored key information.
```

2. Verify that the authentication keys have been created:

```
security key-manager query
```

For complete command syntax, see the man page.

Example

```

cluster1::> security key-manager query

(security key-manager query)

      Node: cluster1-01
      Key Manager: 20.1.1.1
      Count: 1

Key Tag      Key ID
-----
cluster1-01  F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C  yes

      Node: cluster1-02
      Key Manager: 20.1.1.1
      Count: 1

Key Tag      Key ID
-----
cluster1-02  F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C  yes

```

Creating authentication keys (ONTAP 9.2 and earlier)

You can use the `security key-manager create-key` command to create the authentication keys for a node and store them on the configured KMIP servers.

Before you begin

You must be a cluster administrator to perform this task.

About this task

If you are using NetApp Storage Encryption and your security setup requires you to use different keys for data authentication and FIPS 140-2 authentication, you should create a separate key for each. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

When you create an authentication key for a node, the system automatically “restores” the key from the KMIP server and “pushes” it to its partner node. Each node can then use the same key to access its own disks and to access its partner's disks in case of a takeover.

- This command is not supported when onboard key management is enabled.
- You receive a warning if the configured key management servers are already storing more than 128 authentication keys.

You can use the key management server software to delete any unused keys, then run the command again.

Steps

1. Create the authentication key that the current node and its partner will use to access storage:

```
security key-manager create-key
```

For complete command syntax, see the man page for the command.

Note: The key ID displayed in the output is an identifier used to refer to the authentication key. It is not the actual authentication key or the data encryption key.

Example

```

cluster1::> security key-manager create-key
(security key-manager create-key)
Verifying requirements...

Node: cluster1-01
Creating authentication key...

```



```

Authentication key creation successful.
Key ID:
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C

Node: cluster1-01
Key manager restore operation initialized.
Successfully restored key information.

Node: cluster1-02
Key manager restore operation initialized.
Successfully restored key information.

```

2. Verify that the authentication keys have been created:

```
security key-manager query
```

For complete command syntax, see the man page.

Example

```

cluster1::> security key-manager query

(security key-manager query)

      Node: cluster1-01
Key Manager: 20.1.1.1
      Count: 1

Key Tag      Key ID
-----
cluster1-01  F1CB30AFF1CB30B001010000000000A68B167F92DD54196297159B5968923C  yes

      Node: cluster1-02
Key Manager: 20.1.1.1
      Count: 1

Key Tag      Key ID
-----
cluster1-02  F1CB30AFF1CB30B001010000000000A68B167F92DD54196297159B5968923C  yes

```

Assigning a data authentication key to SEDs

You can use the `storage encryption disk modify` command to assign a data authentication key to an SED. Cluster nodes use this key to access data on the SED.

Before you begin

You must be a cluster administrator to perform this task.

About this task

An SED is protected from unauthorized access only if the authentication key ID for the node is set to a value other than the SED's default manufacturer secure ID (MSID), which the system evaluates to 0x0. When you assign an authentication key to an SED, the system changes the authentication key ID for the node to a non-MSID value.

Steps

1. Assign a data authentication key to SEDs:

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

For complete command syntax, see the man page for the command.

Note: You can use the `security key-manager query` command to view key IDs.

Example

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
```

```
Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

2. Verify that the authentication keys have been assigned:

```
storage encryption disk show
```

For complete command syntax, see the man page.

Example

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
0.0.0     data F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1     data F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
[...]
```

Assigning a FIPS 140-2 authentication key to SEDs

You can use the `storage encryption disk modify` command with the `-fips-key-id` option to assign a FIPS 140-2 authentication key to an SED. Cluster nodes use this key for SED operations other than data access, such as allowing firmware downloads.

Before you begin

The drive firmware must support FIPS 140-2 compliance. The Interoperability Matrix contains information about supported drive firmware versions.

About this task

Your security setup may require you to use different keys for data authentication and FIPS 140-2 authentication. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

Steps

1. Assign a FIPS 140-2 authentication key to SEDs:

```
storage encryption disk modify -disk disk_id -fips-key-id
fips_authentication_key_id
```

You can use the `security key-manager query` command to view key IDs.

Example

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
6A1E21D80000000010000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
```

```
Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

2. Verify that the authentication key has been assigned:

```
storage encryption disk show -fips
```

For complete command syntax, see the man page.

Example

```
cluster1::> storage encryption disk show -fips
Disk      Mode FIPS-Compliance Key ID
-----
2.10.0    full 6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
2.10.1    full 6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
[...]
```

Related information

[NetApp Interoperability Matrix Tool](#)

Enabling cluster-wide FIPS-compliant mode for KMIP server connections

You can use the `security config modify` command with the `-is-fips-enabled` option to enable cluster-wide FIPS-compliant mode for data in flight. Doing so forces the cluster to use OpenSSL in FIPS mode with TLS connections to KMIP servers.

Before you begin

All KMIP servers must support TLSv1.2. The system requires TLSv1.2 to complete the connection to the KMIP server when cluster-wide FIPS-compliant mode is enabled.

About this task

When you enable cluster-wide FIPS-compliant mode, the cluster will automatically select only TLS protocols. Cluster-wide FIPS-compliant mode is disabled by default.

You must reboot cluster nodes manually after modifying the cluster-wide security configuration.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Verify that TLSv1.2 is supported:

```
security config show -supported-protocols
```

For complete command syntax, see the man page.

Example

```
cluster1::> security config show
Cluster
Interface FIPS Mode Supported Protocols Supported Ciphers Cluster Security
-----
SSL        false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:
!aNULL:!EXP:
!eNULL
yes
```

3. Enable cluster-wide FIPS-compliant mode:

```
security config modify -is-fips-enabled true -interface SSL
```

For complete command syntax, see the man page.

4. Reboot cluster nodes manually.

5. Verify that cluster-wide FIPS-compliant mode is enabled:

```
security config show
```

Example

```
cluster1::> security config show
Cluster
Interface FIPS Mode Supported Protocols Supported Ciphers Cluster Security
-----
SSL true TLSv1.2, TLSv1.1 ALL:!LOW:
!aNULL:!EXP:
!eNULL:!RC4 yes
```

Configuring onboard key management

You can use the Onboard Key Manager to authenticate cluster nodes to an SED. The Onboard Key Manager is a built-in tool that serves authentication keys to nodes from the same storage system as your data.

Enabling onboard key management

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk (SED).

Before you begin

- If you are using NSE with an external key management (KMIP) server, you must have deleted the external key manager database.

[Transitioning to onboard key management from external key management](#) on page 52

- You must be a cluster administrator to perform this task.

About this task

You must run this command each time you add a node to the cluster.

Steps

1. Start the key manager setup wizard:

```
security key-manager setup
```

Example

The following command starts the key manager setup wizard on **cluster1**:

```
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 use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase: <32..256 UTF8 characters long text>
Reenter the cluster-wide passphrase: <32..256 UTF8 characters long text>
```

2. Enter **yes** at the prompt to configure onboard key management.
3. Enter a passphrase between 32 and 256 characters at the passphrase prompt.

4. Re-enter the passphrase at the passphrase confirmation prompt.
5. Verify that keys are configured for all nodes:

```
security key-manager key show
```

For complete command syntax, see the man page.

Example

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID                                     Used By
-----
0000000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
00000000000000000000200000000000A001C72BB549425E31F89754F99C5314947 SVM-KEK
00000000000000000000200000000000A003F31AF41EA0D55F534D8A58AD63011E6 SVM-KEK
00000000000000000000200000000000A006118875D8F90D3B95355418D73FC14C0 SVM-KEK
00000000000000000000200000000000A00AA32BFB16960116E1D91140EDA72D97A SVM-KEK
00000000000000000000200000000000A00ED1742ABF87BD99BB44429E5E5007ADE SVM-KEK

Node: node2
Key Store: onboard
Key ID                                     Used By
-----
0000000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
00000000000000000000200000000000A001C72BB549425E31F89754F99C5314947 SVM-KEK
00000000000000000000200000000000A003F31AF41EA0D55F534D8A58AD63011E6 SVM-KEK
00000000000000000000200000000000A006118875D8F90D3B95355418D73FC14C0 SVM-KEK
00000000000000000000200000000000A00AA32BFB16960116E1D91140EDA72D97A SVM-KEK
```

After you finish

Copy the passphrase to a secure location outside the storage system for future use.

All key management information is automatically backed up to the replicated database (RDB) for the cluster. You should also back up the information manually for use in case of a disaster.

Viewing the keys generated by the Onboard Key Manager

You can use the `security key-manager key show` command to view the authentication keys generated by the Onboard Key Manager. These are the keys you assign to SEDs for data and optional FIPS 140-2 authentication.

Before you begin

You must be a cluster administrator to perform this task.

About this task

The Onboard Key Manager generates two keys, one for data authentication and one for FIPS 140-2 authentication, in case your security setup requires you to use a different key for each. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

The Onboard Key Manager automatically assigns the keys generated for the current node to its partner node. Each node can then use the same key to access its own disks and to access its partner's disks in case of a takeover.

Step

1. View the authentication keys generated by the Onboard Key Manager:

```
security key-manager key show
```

For complete command syntax, see the man page.

Note: The key ID displayed in the output is an identifier used to refer to the authentication key. It is not the actual authentication key or the data encryption key.

Example

```
cluster1::> security key-manager key show

Node: cluster1-01
Key Store: onboard
Key ID
-----
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A

Node: cluster1-02
Key Store: onboard
Key ID
-----
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
4 entries were displayed.
```

Assigning a data authentication key to SEDs

You can use the `storage encryption disk modify` command to assign a data authentication key to an SED. Cluster nodes use this key to access data on the SED.

Before you begin

You must be a cluster administrator to perform this task.

About this task

An SED is protected from unauthorized access only if the authentication key ID for the node is set to a value other than the SED's default manufacturer secure ID (MSID), which the system evaluates to 0x0. When you assign an authentication key to an SED, the system changes the authentication key ID for the node to a non-MSID value.

Steps

1. Assign a data authentication key to SEDs:

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

For complete command syntax, see the man page for the command.

Note: You can use the `security key-manager query` command to view key IDs.

Example

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C

Info: Starting modify on 14 disks.
View the status of the operation by using the
storage encryption disk show-status command.
```

2. Verify that the authentication keys have been assigned:

```
storage encryption disk show
```

For complete command syntax, see the man page.

Example

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
0.0.0    data F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1    data F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
[...]
```

Assigning a FIPS 140-2 authentication key to SEDs

You can use the `storage encryption disk modify` command with the `-fips-key-id` option to assign a FIPS 140-2 authentication key to an SED. Cluster nodes use this key for SED operations other than data access, such as allowing firmware downloads.

Before you begin

The drive firmware must support FIPS 140-2 compliance. The Interoperability Matrix contains information about supported drive firmware versions.

About this task

Your security setup may require you to use different keys for data authentication and FIPS 140-2 authentication. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

Steps

1. Assign a FIPS 140-2 authentication key to SEDs:

```
storage encryption disk modify -disk disk_id -fips-key-id
fips_authentication_key_id
```

You can use the `security key-manager query` command to view key IDs.

Example

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
6A1E21D800000000010000000000005A1FB4EE8F62FD6D8AE6754C9019F35A

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

2. Verify that the authentication key has been assigned:

```
storage encryption disk show -fips
```

For complete command syntax, see the man page.

Example

```
cluster1::> storage encryption disk show -fips
Disk      Mode FIPS-Compliance Key ID
-----
2.10.0    full 6A1E21D800000000010000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
2.10.1    full 6A1E21D800000000010000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
[...]
```

Managing NetApp encryption

ONTAP offers a rich set of services for managing encryption. You can restore authentication keys, replace SSL certificates, return SEDs to service when authentication keys are no longer available, and much more.

Unencrypting volume data

You can use the `volume move start` command to unencrypt volume data.

Before you begin

You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

[Delegating authority to run the volume move command](#) on page 34

Steps

1. Move an existing volume and unencrypt the data on the volume:

```
volume move start -vserver SVM_name -volume volume_name -destination-
aggregate aggregate_name -encrypt-destination false
```

For complete command syntax, see the man page for the command.

Example

The following command moves an existing volume named `vol1` to the destination aggregate `aggr3` and unencrypts the data on the volume:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination-
aggregate aggr3 -encrypt-destination false
```

The system deletes the encryption key for the volume. The data on the volume is unencrypted.

2. Verify that the volume is disabled for encryption:

```
volume show -encryption
```

For complete command syntax, see the man page for the command.

Example

The following command displays whether volumes on `cluster1` are encrypted:

```
cluster1::> volume show -encryption
```

Vserver	Volume	Aggregate	State	Encryption State
vs1	vol1	aggr1	online	none

Moving an encrypted volume

You can use the `volume move start` command to move an encrypted volume. The moved volume can reside on the same aggregate or a different aggregate.

Before you begin

You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

[Delegating authority to run the volume move command](#) on page 34

About this task

The `-encrypt-destination` option for `volume move start` defaults to `true` for encrypted volumes. Requiring you to specify explicitly that you do not want the destination volume to be encrypted ensures that you do not inadvertently unencrypt the data on the volume.

Steps

1. Move an existing volume and leave the data on the volume encrypted:

```
volume move start -vserver SVM_name -volume volume_name -destination-
aggregate aggregate_name
```

For complete command syntax, see the man page for the command.

Example

The following command moves an existing volume named `vol1` to the destination aggregate `aggr3` and leaves the data on the volume encrypted:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination-
aggregate aggr3
```

2. Verify that the volume is enabled for encryption:

```
volume show -is-encrypted true
```

For complete command syntax, see the man page for the command.

Example

The following command displays the encrypted volumes on `cluster1`:

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
vs1	vol1	aggr3	online	RW	200GB	160.0GB	20%

Delegating authority to run the volume move command

You can use the `volume move` command to encrypt an existing volume, move an encrypted volume, or unencrypt a volume. Cluster administrators can run `volume move` command themselves, or they can delegate the authority to run the command to SVM administrators.

About this task

By default, SVM administrators are assigned the `vsadmin` role, which does not include the authority to move volumes. You must assign the `vsadmin-volume` role to SVM administrators to enable them to run the `volume move` command.

Step

1. Delegate authority to run the `volume move` command:

```
security login modify -vserver SVM_name -user-or-group-name
user_or_group_name -application application -authmethod
authentication_method -role vsadmin-volume
```

For complete command syntax, see the man page for the command.

Example

The following command grants the SVM administrator authority to run the `volume move` command.

```
cluster1::>security login modify -vserver engData -user-or-group-name
SVM-admin -application ssh -authmethod domain -role vsadmin-volume
```

Changing the encryption key for a volume with the volume encryption rekey start command

It is a security best practice to change the encryption key for a volume periodically. Starting with ONTAP 9.3, you can use the `volume encryption rekey start` command to change the encryption key.

About this task

Once you start a rekey operation, it must complete. There is no returning to the old key. If you encounter a performance issue during the operation, you can run the `volume encryption rekey pause` command to pause the operation, and the `volume encryption rekey restart` command to resume the operation.

Until the rekey operation finishes, the volume will have two keys. New writes and their corresponding reads will use the new key. Otherwise, reads will use the old key.

Note: You cannot use `volume encryption rekey start` to rekey a SnapLock or FlexGroup volume. You must use the `volume move start` command.

[Changing the encryption key for a volume with the volume move start command](#) on page 35

Steps

1. Change an encryption key:

```
volume encryption rekey start -vserver SVM_name -volume volume_name
```

Example

The following command changes the encryption key for `vol1` on SVM `vs1`:

```
cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
```

2. Verify the status of the rekey operation:

```
volume encryption rekey show
```

For complete command syntax, see the man page for the command.

Example

The following command displays the status of the rekey operation:

```
cluster1::> volume encryption rekey show

Vserver      Volume      Start Time          Status
-----      -
vs1          vol1        9/18/2017 17:51:41  Phase 2 of 2 is in progress.
```

3. When the rekey operation is complete, verify that the volume is enabled for encryption:

```
volume show -is-encrypted true
```

For complete command syntax, see the man page for the command.

Example

The following command displays the encrypted volumes on `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver      Volume      Aggregate  State  Type  Size  Available  Used
-----      -
vs1          vol1        aggr2      online RW   200GB   160.0GB   20%
```

Changing the encryption key for a volume with the volume move start command

It is a security best practice to change the encryption key for a volume periodically. You can use the `volume move start` command to change the encryption key. You must use `volume move start` in ONTAP 9.2 and earlier, and in ONTAP 9.3, if you are rekeying a SnapLock or FlexGroup volume. The moved volume can reside on the same aggregate or a different aggregate.

Before you begin

You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

[Delegating authority to run the volume move command](#) on page 34

About this task

Starting with ONTAP 9.2, you can rekey a SnapLock or FlexGroup volume.

Steps

1. Move an existing volume and change the encryption key:

```
volume move start -vserver SVM_name -volume volume_name -destination-
aggregate aggregate_name -generate-destination-key true
```

For complete command syntax, see the man page for the command.

Example

The following command moves an existing volume named **vol1** to the destination aggregate **aggr2** and changes the encryption key:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination-
aggregate aggr2 -generate-destination-key true
```

A new encryption key is created for the volume. The data on the volume remains encrypted.

2. Verify that the volume is enabled for encryption:

```
volume show -is-encrypted true
```

For complete command syntax, see the man page for the command.

Example

The following command displays the encrypted volumes on **cluster1**:

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
vs1	vol1	aggr2	online	RW	200GB	160.0GB	20%

Deleting an encrypted volume

You can use the `volume delete` command to delete an encrypted volume.

Before you begin

- You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.
[Delegating authority to run the volume move command](#) on page 34
- The volume must be offline.

Step

1. Delete an encrypted volume:

```
volume delete -vserver SVM_name -volume volume_name
```

For complete command syntax, see the man page for the command.

Example

The following command deletes an encrypted volume named **vol1**:

```
cluster1::> volume delete -vserver vs1 -volume vol1
```

Enter `yes` when you are prompted to confirm deletion.

The system deletes the encryption key for the volume after 24 hours.

Use `volume delete` with the `-force true` option to delete a volume and destroy the corresponding encryption key immediately. For more information, see the man page.

After you finish

You can use the `volume recovery-queue` command to recover a deleted volume during the retention period after issuing the `volume delete` command:

```
volume recovery-queue SVM_name -volume volume_name
```

[How to use the Volume Recovery feature](#)

Restoring onboard key management encryption keys

Occasionally, you may need to restore an onboard key management encryption key. You can use the `security key-manager key show` command to verify that a key needs to be restored, and the `security key-manager setup` command to restore the key.

Before you begin

- If you are using NSE with an external key management (KMIP) server, you must have deleted the external key manager database.

[Transitioning to onboard key management from external key management](#) on page 52

- You must be a cluster administrator to perform this task.

Steps

1. Verify that a key needs to be restored:

```
security key-manager key show
```

For complete command syntax, see the man page.

Example

The following example shows that the encryption key on node 3 needs to be restored:

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID                                     Used By
-----
000000000000000002000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
00000000000000000200000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
0000000000000000020000000000A001C72BB549425E31F89754F99C5314947 SVM-KEK
0000000000000000020000000000A003F31AF41EA0D55F534D8A58AD63011E6 SVM-KEK
0000000000000000020000000000A006118875D8F90D3B95355418D73FC14C0 SVM-KEK
0000000000000000020000000000A00AA32BFB16960116E1D91140EDA72D97A SVM-KEK
0000000000000000020000000000A00ED1742ABF87BD99BB44429E5E5007ADE SVM-KEK

Node: node2
Key Store: onboard
Key ID                                     Used By
-----
000000000000000002000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
00000000000000000200000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
0000000000000000020000000000A001C72BB549425E31F89754F99C5314947 SVM-KEK
0000000000000000020000000000A003F31AF41EA0D55F534D8A58AD63011E6 SVM-KEK
0000000000000000020000000000A006118875D8F90D3B95355418D73FC14C0 SVM-KEK
0000000000000000020000000000A00AA32BFB16960116E1D91140EDA72D97A SVM-KEK

Node: node3
Key Store: onboard
Key ID                                     Used By
-----
0000000000000000020000000000A00ED1742ABF87BD99BB44429E5E5007ADE SVM-KEK
14 entries were displayed.
```

Error: One or more nodes have onboard key management keys that need to be

```
restored. To identify the nodes, run "security key-manager key show
-restored no". Then, restore the keys on those nodes using the command
"security key-manager setup -node <nodename>".
```

2. Start the key manager setup wizard:

```
security key-manager setup
```

Example

The following command starts the key manager setup wizard on **cluster1**:

```
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 use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase: <32..256 UTF8 characters long text>
Reenter the cluster-wide passphrase: <32..256 UTF8 characters long text>
```

Changing the onboard key management passphrase

It is a security best practice to change the onboard key management passphrase periodically. You can use the `security key-manager update-passphrase` command to change the onboard key management passphrase.

Before you begin

- You must be a cluster administrator to perform this task.
- Advanced privileges are required for this task.

Steps

1. Change to advanced privilege level:


```
set -privilege advanced
```
2. Change the onboard key management passphrase:


```
security key-manager update-passphrase
```

Example

The following command lets you change the key management passphrase for **cluster1**:

```
cluster1::> security key-manager update-passphrase
Warning: This command will reconfigure the cluster passphrase for
onboard key-management.
Do you want to continue? {y|n}:
Enter current passphrase: <32..256 UTF8 characters long text>
Enter new passphrase: <32..256 UTF8 characters long text>
Reenter the new passphrase: <32..256 UTF8 characters long text>
```

3. Enter **y** at the prompt to change the onboard key management passphrase.

4. Enter the current passphrase at the current passphrase prompt.
5. Enter the new passphrase at the new passphrase prompt.
6. Reenter the new passphrase at the passphrase confirmation prompt.

After you finish

You should copy the onboard key management passphrase to a secure location outside the storage system for future use.

You should back up key management information manually whenever you change the onboard key management passphrase.

[Backing up onboard key management information manually](#) on page 39

Backing up onboard key management information manually

You should back up onboard key management information manually whenever you change the Onboard Key Manager passphrase. You can use the `security key-manager backup show` command to display the key management backup information for the cluster. You can then copy the backup information to a secure location outside the storage system.

Before you begin

You must be a cluster administrator to perform this task.

About this task

All key management information is automatically backed up to the replicated database (RDB) for the cluster. You should also back up key management information manually for use in case of a disaster.

Step

1. Display the key management backup information for the cluster:

```
security key-manager backup show
```

Example

The following command displays the key management backup information for `cluster1` in a hex dump:

```
security key-manager backup show
----BEGIN BACKUP-----
cb5101eab69b7d832287d16b2a02debe
d6f9b7798979c2d70a3c2ac231873a00
d9994b44c61160de3ae02250fb8e7803
90989a7ebf7a3ed8c89f8073dde3c558
6effff9497f7666cc990c3398f86df3e
7ecf4ca826736ecd1a761b102184861b
....
----END BACKUP-----
```

After you finish

You should copy the backup information to a secure location outside the storage system for use in case of a disaster.

Restoring external key management authentication keys (9.3)

You can use the `security key-manager restore` command to manually restore external key management authentication keys and “push” them to a different node. You might want to do this if you are adding a new node to the cluster, or restarting a node that was down temporarily when you created the keys for the cluster.

Before you begin

You must be a cluster administrator to perform this task.

About this task

You can use the `security key-manager query` command to determine if a key has been restored.

This command is not supported when onboard key management is enabled.

Step

1. Restore the current node's authentication keys and key IDs to a different node:

```
security key-manager restore -node node
```

`node` defaults to all nodes. For complete command syntax, see the man page for the command.

Example

```
cluster1::> security key-manager restore -node cluster1-02
(security key-manager restore)

      Node: cluster1-02
Key Manager: 20.1.1.1
      Count: 2

Key IDs
-----
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
```

Restoring external key management authentication keys (9.2 and earlier)

You can use the `security key-manager restore` command to manually restore external key management authentication keys and “push” them to a different node. You might want to do this if you are adding a new node to the cluster, or restarting a node that was down temporarily when you created the keys for its partner.

Before you begin

You must be a cluster administrator to perform this task.

About this task

When you create an authentication key for a node, the system automatically “restores” the key from the KMIP server and “pushes” it to its partner node. The partner can then use the key to access the node's disks in the event of a takeover. The `security key-manager restore` command lets you restore authentication keys manually, to any node in the cluster. You can use the `security key-manager query` command to determine if a key has been restored.

This command is not supported when onboard key management is enabled.

Step

1. Restore the current node's authentication keys and key IDs to a different node:

```
security key-manager restore -node node
```

`node` defaults to all nodes. For complete command syntax, see the man page for the command.

Example

```
cluster1::> security key-manager restore -node cluster1-02
(security key-manager restore)

      Node: cluster1-02
Key Manager: 20.1.1.1
      Count: 2

Key IDs
-----
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
```

Replacing an SED

You can replace an SED the same way you replace an ordinary disk. You must rekey the SED to enable NSE.

Before you begin

- You must know the key ID for the authentication key used by the SED.
- You must be a cluster administrator to perform this task.

Steps

1. Ensure that the disk has been marked as failed:

```
storage disk show -broken
```

For complete command syntax, see the man page.

Example

```
cluster1::> storage disk show -broken
Original Owner: cluster1-01
Checksum Compatibility: block

  Disk  Outage Reason HA Shelf Bay Chan  Pool  Type  RPM  Usable Physical
  -----
  0.0.0  admin  failed  0b   1   0   A  Pool0 FCAL  10000  132.8GB  133.9GB
  0.0.7  admin  removed 0b   2   6   A  Pool1 FCAL  10000  132.8GB  134.2GB
[...]
```

2. Remove the failed disk and replace it with a new SED, following the instructions in the hardware guide for your disk shelf model.

3. Assign ownership of the newly replaced SED:

```
storage disk assign -disk disk_name -owner node
```

For complete command syntax, see the man page.

Example

```
cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
```

4. Confirm that the new disk has been assigned:

```
storage encryption disk show
```

For complete command syntax, see the man page.

Example

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
0.0.0    data F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1    data F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.0   data F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1   data F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
2.1.1    open 0x0
[...]
```

5. Assign the authentication keys to the SED.

[Assigning a data authentication key to SEDs](#) on page 25

Replacing SSL certificates

All SSL certificates have an expiration date. You must update your certificates before they expire to prevent loss of access to authentication keys.

Before you begin

- You must have obtained the replacement public and private certificates for the cluster.
- You must have obtained the replacement public certificate for the KMIP server.

Note: You can install the replacement client and server certificates on the KMIP server before or after installing the certificates on the cluster.

Steps

1. Disable the connection to the KMIP server:

```
security key-manager delete -address key_management_server_ipaddress
```

Example

```
cluster1::> security key-manager delete -address 20.1.0.0
```

2. Delete the client 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
```

Example

```
cluster1::> security certificate delete -vserver vs0 -common-name
www.example.com -ca "Verisign Inc" -type client -subtype kmip-cert
```

3. Delete the KMIP server certificate:

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

Example

```
cluster1::> security certificate delete -vserver vs0 -common-name
www.example.com -ca "Verisign Inc" -type server-ca -subtype kmip-cert
```

4. Install the replacement client and server certificates.

[Installing SSL certificates on the cluster](#) on page 10

5. Connect to the KMIP server.

[Connecting to external key management servers](#) on page 21

Making data on an SED inaccessible

If you want to make data on an SED permanently inaccessible, but keep the SED's unused space available for new data, you can sanitize the disk. If you want to make data permanently inaccessible and you do not need to reuse the SED, you can destroy it.

- Disk sanitization

When you sanitize an SED, the system changes the disk encryption key to a new random value, resets the power-on lock state to false, and sets the key ID to the default manufacturer secure ID (MSID). Doing so renders the data on the disk inaccessible and impossible to retrieve. You can reuse sanitized disks as non-zeroed spare disks.

- Disk destroy

When you destroy an SED, the system sets the disk encryption key to an unknown random value and locks the disk irreversibly. Doing so renders the disk permanently unusable and the data on it permanently inaccessible.

You can sanitize or destroy individual SEDs, or all the SEDs for a node.

If you think an SED might need to be sanitized

Disk sanitization can be time-consuming. If you think an SED might need to be sanitized, following some simple guidelines will reduce the time it takes to complete the process:

- Make sure disk aggregates are no larger than necessary.
If aggregates are larger than needed, sanitization requires more time, disk space, and bandwidth.
- When you back up aggregates containing sensitive data, avoid backing them up to aggregates that also contain large amounts of nonsensitive data.
Doing so reduces the amount of time you will need to move the nonsensitive data before sanitizing the SED containing the sensitive data.

Choices

- [Sanitizing an SED](#) on page 44
- [Destroying an SED](#) on page 45
- [Emergency shredding of data on an SED](#) on page 46

Sanitizing an SED

If you want to make data on an SED permanently inaccessible, but keep the SED's unused space available for new data, you can use the `storage encryption disk sanitize` command to sanitize the SED.

Before you begin

You must be a cluster administrator to perform this task.

About this task

When you sanitize an SED, the system changes the disk encryption key to a new random value, resets the power-on lock state to false, and sets the authentication key ID to the default manufacturer secure ID (MSID). Doing so renders the data on the disk inaccessible and impossible to retrieve. You can reuse sanitized disks as non-zeroed spare disks.

Steps

1. Migrate any data that needs to be preserved to an aggregate for a different disk.
2. Delete the aggregate on the SED to be sanitized:

```
storage aggregate delete -aggregate aggregate_name
```

For complete command syntax, see the man page.

Example

```
cluster1::> storage aggregate delete -aggregate aggr1
```

3. Identify the disk ID for the SED to be sanitized:

```
storage encryption disk show
```

For complete command syntax, see the man page.

Example

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
0.0.0    data F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1    data F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.2   data F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. Sanitize the disk:

```
storage encryption disk sanitize -disk disk_id
```

You can use this command to sanitize hot spare or broken disks only. To sanitize all disks regardless of type, use the `-force-all-state` option. For complete command syntax, see the man page.

Note: You are prompted to enter a confirmation phrase before continuing. Enter the phrase exactly as shown on the screen.

Example

```
cluster1::> storage encryption disk sanitize -disk 1.10.2

Warning: This operation will cryptographically sanitize 1 spare or
broken
        self-encrypting disk on 1 node.
        To continue, enter
          sanitize disk
        :sanitize disk

Info: Starting sanitize on 1 disk.
      View the status of the operation using the
      storage encryption disk show-status command.
```

Destroying an SED

If you want to make SED data permanently inaccessible and you do not need to reuse the SED, you can use the `storage encryption disk destroy` command to destroy the disk.

Before you begin

You must be a cluster administrator to perform this task.

About this task

When you destroy an SED, the system sets the disk encryption key to an unknown random value and locks the disk irreversibly. Doing so renders the disk permanently unusable and the data on it permanently inaccessible.

Steps

1. Migrate any data that needs to be preserved to an aggregate for a different disk.
2. Delete the aggregate on the SED to be destroyed:

```
storage aggregate delete -aggregate aggregate_name
```

For complete command syntax, see the man page.

Example

```
cluster1::> storage aggregate delete -aggregate aggr1
```

3. Identify the disk ID for the SED to be destroyed:

```
storage encryption disk show
```

For complete command syntax, see the man page.

Example

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
0.0.0    data F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1    data F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.2   data F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. Destroy the disk:

```
storage encryption disk destroy -disk disk_id
```

For complete command syntax, see the man page.

Note: You are prompted to enter a confirmation phrase before continuing. Enter the phrase exactly as shown on the screen.

Example

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or
broken
self-encrypting disks on 1 node.
You cannot reuse destroyed disks unless you revert
them to their original state using the PSID value.
To continue, enter
destroy disk
:destroy disk

Info: Starting destroy on 1 disk.
View the status of the operation by using the
"storage encryption disk show-status" command.
```

Emergency shredding of data on an SED

In case of a security emergency, you can instantly prevent access to SEDs, even if power is not available to the storage system or the KMIP server.

Before you begin

- You must be using a KMIP server, and the KMIP server must be configured with an easily destroyed authentication item (for example, a smart card or USB drive).
- You must be a cluster administrator to perform this task.

Step

1. Perform emergency shredding of data on an SED:

If...	Then...
Power is available to the storage system and you have time to take the storage system offline gracefully	<p>a. If the storage system is configured as an HA pair, disable takeover.</p> <p>b. Take all aggregates offline and delete them.</p> <p>c. Set the privilege level to advanced:</p> <pre>set -privilege advanced</pre> <p>d. If the SEDs are in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID:</p> <pre>storage encryption disk modify -disk * -fips-key-id 0x0</pre> <p>e. Halt the storage system.</p> <p>f. Boot into maintenance mode.</p> <p>g. Sanitize or destroy the disks:</p> <ul style="list-style-type: none"> • If you want to make the data on the disks inaccessible and still be able to reuse the disks, sanitize the disks: <pre>disk encrypt sanitize -all</pre> <ul style="list-style-type: none"> • If you want to make the data on the disks inaccessible and you do not need to save the disks, destroy the disks: <pre>disk encrypt destroy disk_id1 disk_id2 ...</pre> <p>Note: The <code>disk encrypt sanitize</code> and <code>disk encrypt destroy</code> commands are reserved for maintenance mode only. These commands must be run on each HA node, and are not available for broken disks.</p> <p>h. Repeat these steps for the partner node.</p> <p>This leaves the storage system in a permanently disabled state with all data erased. To use the system again, you must reconfigure it.</p>
Power is available to the storage system and you must shred the data immediately	<p>a. If the storage system is configured as an HA pair, disable takeover.</p> <p>b. Set the privilege level to advanced:</p> <pre>set -privilege advanced</pre> <p>c. Sanitize or destroy the disks:</p> <ul style="list-style-type: none"> • If you want to make the data on the disks inaccessible and still be able to reuse the disks, sanitize the disks: <pre>storage encryption disk sanitize -disk * -force-all-states true</pre> <ul style="list-style-type: none"> • If you want to make the data on the disks inaccessible and you do not need to save the disks, destroy the disks: <pre>storage encryption disk destroy -disk * -force-all-states true</pre> <p>The storage system panics, leaving the system in a permanently disabled state with all data erased. To use the system again, you must reconfigure it.</p>

If...	Then...
Power is available to the KMIP server but not to the storage system	<ul style="list-style-type: none"> <li data-bbox="651 254 1370 289">a. Log in to the KMIP server. <li data-bbox="651 296 1370 365">b. Destroy all keys associated with the SEDs containing the data you want to prevent access to. <p data-bbox="651 380 1370 415">This prevents access to disk encryption keys by the storage system.</p>
Power is not available to the KMIP server or the storage system	Destroy the authentication item for the KMIP server (for example, the smart card). This prevents access to disk encryption keys by the storage system.

For complete command syntax, see the man pages.

Returning SEDs to service when authentication keys are lost

The system treats an SED as broken if you lose the authentication keys for it permanently and cannot retrieve them from the KMIP server. Although you cannot access or recover the data on the disk, you can take steps to make the SED's unused space available again for data.

Before you begin

You must be a cluster administrator to perform this task.

About this task

You should use this process only if you are certain that the authentication keys for the SED are permanently lost and that you cannot recover them.

Step

1. Return SEDs to service:

If the SEDs are...	Use these steps...
Not in FIPS-compliance mode, or in FIPS-compliance mode and the FIPS key is available	<p>a. Sanitize the broken disk: <code>storage encryption disk sanitize -disk <i>disk_id</i></code></p> <p>b. Set the privilege level to advanced: <code>set -privilege advanced</code></p> <p>c. Unfail the sanitized disk: <code>storage disk unfail -spare true -disk <i>disk_id</i></code></p> <p>d. Check whether the disk has an owner: <code>storage disk show -disk <i>disk_id</i></code></p> <p>e. If the disk does not have an owner, assign one, then unfail the disk again: <code>storage disk assign -owner <i>node</i> -disk <i>disk_id</i></code> <code>storage disk unfail -spare true -disk <i>disk_id</i></code></p> <p>f. Verify that the SED is now a spare and ready to be reused in an aggregate: <code>storage disk show -disk <i>disk_id</i></code></p>
In FIPS-compliance mode, the FIPS key is not available, and the SEDs have a PSID printed on the label	<p>a. Obtain the SED's PSID from its disk label.</p> <p>b. Set the privilege level to advanced: <code>set -privilege advanced</code></p> <p>c. Reset the SED to its factory-configured settings: <code>storage encryption disk revert-to-original-state -disk <i>disk_id</i> -psid <i>disk_physical_secure_id</i></code></p> <p>d. Unfail the sanitized disk: <code>storage disk unfail -spare true -disk <i>disk_id</i></code></p> <p>e. Check whether the disk has an owner: <code>storage disk show -disk <i>disk_id</i></code></p> <p>f. If the disk does not have an owner, assign one, then unfail the disk again: <code>storage disk assign -owner <i>node</i> -disk <i>disk_id</i></code> <code>storage disk unfail -spare true -disk <i>disk_id</i></code></p> <p>g. Verify that the SED is now a spare and ready to be reused in an aggregate: <code>storage disk show -disk <i>disk_id</i></code></p>

For complete command syntax, see the man pages.

Returning SEDs to unprotected mode

An SED is protected from unauthorized access only if the authentication key ID for the node is set to a value other than the SED's default manufacturer secure ID (MSID), which the system evaluates to

0x0. You can return an SED to unprotected mode by using the `storage encryption disk modify` command to set the key ID to 0x0.

Before you begin

You must be a cluster administrator to perform this task.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. If the SED is running in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID:

```
storage encryption disk modify -disk disk_id -fips-key-id 0x0
```

You can use the `security key-manager query` command to view key IDs.

Example

```
cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id
0x0

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

3. Set the data authentication key ID for the node back to the default MSID:

```
storage encryption disk modify -disk disk_id -data-key-id 0x0
```

You can use the `security key-manager query` command to view key IDs.

Example

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id
0x0

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

Deleting an external key manager connection (9.3)

You can disconnect a KMIP server from a node when you no longer need the server. You might disconnect a KMIP server when you are transitioning to volume encryption, for example.

Before you begin

You must be a cluster administrator to perform this task.

About this task

When you disconnect a KMIP server from one node in an HA pair, the system automatically disconnects the server from all cluster nodes.

Note: If you plan to continue using external key management after disconnecting a KMIP server, make sure another KMIP server is available to serve authentication keys.

Step

1. Disconnect a KMIP server from the current node:

```
security key-manager delete -address key_management_server_ipaddress
```

Example

```
cluster1::> security key-manager delete -address 10.233.1.198
(security key-manager delete)
```

Deleting an external key manager connection (9.2 and earlier)

You can disconnect a KMIP server from a node when you no longer need the server. You might disconnect a KMIP server when you are transitioning to volume encryption, for example.

Before you begin

You must be a cluster administrator to perform this task.

About this task

When you disconnect a KMIP server from one node in an HA pair, the system automatically disconnects the server from the partner node.

Note: If you plan to continue using external key management after disconnecting a KMIP server, make sure another KMIP server is available to serve authentication keys.

Step

1. Disconnect a KMIP server from the current node:

```
security key-manager delete -address key_management_server_ipaddress
```

Example

```
cluster1::> security key-manager delete -address 10.233.1.198
(security key-manager delete)

Node: cluster1-01
Key manager 10.233.1.198 registration will be removed from service.
Key manager registration successfully removed.

Node: cluster1-02
Key manager 10.233.1.198 registration will be removed from service.
Key manager registration successfully removed.
```

Transitioning to external key management from onboard key management

If you want to switch to external key management from onboard key management, you must delete the onboard key management configuration before you can enable external key management.

Before you begin

- If you have been using NSE, you must have reset the authentication keys of all NSE disks to MSID (0x0).
[Returning SEDs to unprotected mode](#) on page 49
- If you have been using NVE, you must have unencrypted all volumes.
[Unencrypting volume data](#) on page 32
- You must be a cluster administrator to perform this task.

Step

1. Delete the onboard key management configuration for a cluster:

```
security key-manager delete-key-database
```

Example

The following command deletes the onboard key management configuration for **cluster1**:

```
cluster1::> security key-manager delete-key-database
```

Transitioning to onboard key management from external key management

If you want to switch to onboard key management from external key management, you must delete the external key management configuration before you can enable onboard key management.

Before you begin

- If you have been using NSE, you must have reset the authentication keys of all NSE disks to MSID (0x0).
[Returning SEDs to unprotected mode](#) on page 49
- You must have deleted all external key manager connections.
[Deleting an external key manager connection \(9.2 and earlier\)](#) on page 51
- You must be a cluster administrator to perform this task.

Step

1. Delete the external key management configuration for a cluster:

```
security key-manager delete-kmip-config
```

Example

The following command deletes the external key management configuration for **cluster1**:

```
cluster1::> security key-manager delete-kmip-config
```

What happens when key management servers are not reachable during the boot process

ONTAP takes certain precautions to avoid undesired behavior in the event that a storage system configured for NSE cannot reach any of the specified key management servers during the boot process.

If the storage system is configured for NSE, the SEDs are rekeyed and locked, and the SEDs are powered on, the storage system must retrieve the required authentication keys from the key management servers to authenticate itself to the SEDs before it can access the data.

The storage system attempts to contact the specified key management servers for up to three hours. If the storage system cannot reach any of them after that time, the boot process stops and the storage system halts.

If the storage system successfully contacts any specified key management server, it then attempts to establish an SSL connection for up to 15 minutes. If the storage system cannot establish an SSL connection with any specified key management server, the boot process stops and the storage system halts.

While the storage system attempts to contact and connect to key management servers, it displays detailed information about the failed contact attempts at the CLI. You can interrupt the contact attempts at any time by pressing Ctrl-C.

As a security measure, SEDs allow only a limited number of unauthorized access attempts, after which they disable access to the existing data. If the storage system cannot contact any specified key management servers to obtain the proper authentication keys, it can only attempt to authenticate with the default key which leads to a failed attempt and a panic. If the storage system is configured to automatically reboot in case of a panic, it enters a boot loop which results in continuous failed authentication attempts on the SEDs.

Halting the storage system in these scenarios is by design to prevent the storage system from entering a boot loop and possible unintended data loss as a result of the SEDs locked permanently due to exceeding the safety limit of a certain number of consecutive failed authentication attempts. The limit and the type of lockout protection depends on the manufacturing specifications and type of SED:

SED type	Number of consecutive failed authentication attempts resulting in lockout	Lockout protection type when safety limit is reached
HDD	1024	Permanent. Data cannot be recovered, even when the proper authentication key becomes available again.
X440_PHM2800MCTO 800GB NSE SSDs with firmware revisions NA00 or NA01	5	Temporary. Lockout is only in effect until disk is power-cycled.
X577_PHM2800MCTO 800GB NSE SSDs with firmware revisions NA00 or NA01	5	Temporary. Lockout is only in effect until disk is power-cycled.
X440_PHM2800MCTO 800GB NSE SSDs with higher firmware revisions	1024	Permanent. Data cannot be recovered, even when the proper authentication key becomes available again.

SED type	Number of consecutive failed authentication attempts resulting in lockout	Lockout protection type when safety limit is reached
X577_PHM2800MCTO 800GB NSE SSDs with higher firmware revisions	1024	Permanent. Data cannot be recovered, even when the proper authentication key becomes available again.
All other SSD models	1024	Permanent. Data cannot be recovered, even when the proper authentication key becomes available again.

For all SED types, a successful authentication resets the try count to zero.

If you encounter this scenario where the storage system is halted due to failure to reach any specified key management servers, you must first identify and correct the cause for the communication failure before you attempt to continue booting the storage system.

NVE APIs

You can use Zephyr APIs to integrate with NVE functionality in scripts or workflow automation. The APIs use XML messaging over HTTP, HTTPS, and Windows DCE/RPC.

security-key-manager-backup-get

Display the Onboard Key Manager backup information.

security-key-manager-delete-keys

Delete the Onboard Key Manager configuration.

security-key-manager-delete-kmip-config

Delete an external key manager configuration.

security-key-manager-key-get-iter

Display the IDs for the NSE authentication key, the NSE FIPS authentication key, and the SVM key encryption key. Each node should show the same sets of keys.

security-key-manager-setup

Enable key management.

security-key-manager-update-passphrase

Change the passphrase for the Onboard Key Manager.

volume-create

Create a volume and enable encryption on the volume.

volume-move-start

Move a volume and enable encryption on the volume. Also used to move an encrypted volume and unencrypt a volume.

Where to find additional information

You can learn more about the tasks described in this guide in NetApp's extensive documentation library.

- [*Disk and aggregate management*](#)
Describes how to manage physical storage in NetApp systems, including disks, aggregates, and RAID groups.
- [*Logical storage management*](#)
Describes how to manage logical storage in NetApp systems, including FlexVol volumes, FlexClone volumes, FlexCache volumes, files, and LUNs.
- [*ONTAP 9 commands*](#)
Describes encryption commands in reference format.
- [*NetApp Documentation: OnCommand Workflow Automation \(current releases\)*](#)
Describes how to use the OnCommand Workflow Automation scripting tool to perform encryption-related tasks.

Copyright information

Copyright © 2018 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

[*doccomments@netapp.com*](mailto:doccomments@netapp.com)

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

- 7-Mode Transition Tool
 - use with NetApp Volume Encryption [6](#)
 - use with NVE [6](#)

A

- about this guide
 - deciding whether to use [5](#)
- APIs
 - Data ONTAP [54](#)
 - descriptions [54](#)
 - NetApp Volume Encryption [54](#)
 - NVE [54](#)
- audience
 - for the guide [5](#)

C

- certificates
 - installing SSL, on cluster [10, 19](#)
- certificates, SSL
 - replacing before expiration [42](#)
- cluster security
 - configuring self-encrypting disks for FIPS 140-2 compliance [26, 31](#)
 - enabling cluster-wide FIPS-compliant mode [27](#)
- comments
 - how to send feedback about documentation [58](#)
- configurations, MetroCluster
 - support for Storage Encryption [17](#)
- configuring
 - self-encrypting disks for FIPS 140-2 compliance [26, 31](#)

D

- data
 - emergency shredding of on NetApp Storage Encryption disks [46](#)
 - methods for making it inaccessible on SEDs [43](#)
- destroying
 - NSE disks [45](#)
- disk, self-encrypting
 - information to collect before configuring with external key management servers [9, 18](#)
- disks
 - destroying NSEs [45](#)
- disks, NSE
 - emergency shredding of data on [46](#)
 - sanitizing [44](#)
- disks, self-encrypting
 - overview of managing [32](#)
 - replacing [41](#)
- documentation
 - additional information about NetApp encryption [55](#)
 - additional information about NSE [55](#)
 - additional information about NVE [55](#)

- how to receive automatic notification of changes to [58](#)
- how to send feedback about [58](#)

E

- enabling cluster-wide FIPS-compliant mode [27](#)
- encryption
 - changing the encryption key [34, 35](#)
 - deleting an encrypted volume [36](#)
 - encrypting data at rest [6](#)
 - moving an encrypted volume [33](#)
 - unencrypting data at rest [32](#)
- encryption keys
 - backing up [39](#)
- encryption, NetApp Volume Encryption
 - backing up key management information manually [39](#)
 - changing the encryption key [34, 35](#)
 - changing the key management passphrase [38](#)
 - delegating authority to run the volume move command [34](#)
 - deleting an encrypted volume [36](#)
 - encrypting a new volume [13](#)
 - encrypting an existing volume [14, 15](#)
 - moving an encrypted volume [33](#)
 - unencrypting volume data [32](#)
- encryption, NVE
 - backing up key management information manually [39](#)
 - changing the encryption key [34, 35](#)
 - changing the key management passphrase [38](#)
 - delegating authority to run the volume move command [34](#)
 - deleting an encrypted volume [36](#)
 - encrypting a new volume [13](#)
 - encrypting an existing volume [14, 15](#)
 - moving an encrypted volume [33](#)
 - unencrypting volume data [32](#)
- expiration, SSL certificates
 - replacing before [42](#)
- external key management server
 - disabling [52](#)
- external key management servers
 - assigning authentication keys to SEDs [25, 30](#)
 - creating authentication keys [23, 24](#)
 - deleting a connection [50, 51](#)
 - disconnecting [50, 51](#)
 - information to collect before configuring Storage Encryption with [9, 18](#)
 - restoring authentication keys [40](#)
 - setting up [11, 20, 21](#)
- external key management, NetApp Storage Encryption
 - deleting an onboard key management database configuration [52](#)

F

- feedback
 - how to send comments about documentation [58](#)
- FIPS 140-2 compliance
 - configuring self-encrypting disks for [26, 31](#)
- FIPS-compliant mode
 - enabling cluster-wide [27](#)
- FlexGroups
 - use with NetApp Volume Encryption [6](#)
 - use with NVE [6](#)

I

- information
 - how to send feedback about improving documentation [58](#)
- installing
 - SSL certificates on cluster [10, 19](#)

K

- key management passphrase
 - changing [38](#)
 - setting initially [12, 28](#)
- key management servers
 - precautions taken against unreachability during boot process [53](#)
- key management servers, external
 - assigning authentication keys to SEDs [25, 30](#)
 - creating authentication keys [23, 24](#)
 - restoring authentication keys [40](#)
 - setting up [11, 20, 21](#)
- key management setup
 - workflow [18](#)
- KMIP server
 - disabling [52](#)

L

- licenses, NetApp Volume Encryption
 - installing [8](#)
- licenses, NVE
 - installing [8](#)

M

- managing
 - self-encrypting disks, overview of [32](#)
- methods
 - for making data on SEDs inaccessible [43](#)
- MetroCluster
 - use with NetApp Volume Encryption [6](#)
 - use with NVE [6](#)
- MetroCluster configurations
 - support for Storage Encryption [17](#)
- MSIDs
 - rekeying SEDs to [49](#)

N

- NetApp encryption
 - where to find additional information about [55](#)
- NetApp Storage Encryption
 - onboard key management database [52](#)
 - viewing keys generated by the Onboard Key Manager [29](#)
- NetApp Storage Encryption disks
 - emergency shredding of data on [46](#)
- NetApp Volume Encryption
 - APIs [54](#)
 - backing up key management information manually [39](#)
 - changing the encryption key [34, 35](#)
 - changing the key management passphrase [38](#)
 - delegating authority to run the volume move command [34](#)
 - deleting an encrypted volume [36](#)
 - deleting an external key manager configuration [52](#)
 - determining the ONTAP version [8](#)
 - enabling onboard key management [12, 28](#)
 - encrypting a new volume [13](#)
 - encrypting an existing volume [14, 15](#)
 - installing the license [8](#)
 - moving an encrypted volume [33](#)
 - overview [6](#)
 - support details [6](#)
 - unencrypting volume data [32](#)
 - use with 7-Mode Transition Tool [6](#)
 - use with FlexGroups [5, 6](#)
 - use with MetroCluster [6](#)
 - use with SnapLock [6](#)
 - use with SnapLock configurations [5](#)
 - use with SnapMirror [6](#)
 - use with SnapVault [6](#)
 - workflow [7](#)
- NSE
 - deleting an onboard key management configuration [52](#)
 - viewing keys generated by the Onboard Key Manager [29](#)
 - where to find additional information about [55](#)
- NSE disks
 - sanitizing [44](#)
- NVE
 - APIs [54](#)
 - backing up key management information manually [39](#)
 - changing the encryption key [34, 35](#)
 - changing the key management passphrase [38](#)
 - delegating authority to run the volume move command [34](#)
 - deleting an encrypted volume [36](#)
 - deleting an external key manager configuration [52](#)
 - determining the ONTAP version [8](#)
 - enabling onboard key management [12, 28](#)
 - encrypting a new volume [13](#)
 - encrypting an existing volume [14, 15](#)
 - installing the license [8](#)
 - moving an encrypted volume [33](#)
 - overview [6](#)
 - support details [6](#)

- unencrypting volume data [32](#)
 - use with 7-Mode Transition Tool [6](#)
 - use with FlexGroups [5](#), [6](#)
 - use with MetroCluster [6](#)
 - use with SnapLock [6](#)
 - use with SnapLock configurations [5](#)
 - use with SnapMirror [6](#)
 - use with SnapVault [6](#)
 - where to find additional information about [55](#)
 - NVE Encryption
 - workflow [7](#)
- ## O
- Onboard Key Manager
 - disabling [52](#)
 - enabling [12](#), [28](#)
 - viewing keys generated by the Onboard Key Manager [29](#)
 - Onboard Key Manager, NetApp Storage Encryption
 - viewing keys generated by the Onboard Key Manager [29](#)
 - Onboard Key Manager, NetApp Volume Encryption
 - deleting an external key manager configuration [52](#)
 - enabling [12](#), [28](#)
 - Onboard Key Manager, NVE
 - deleting an external key manager configuration [52](#)
 - enabling [12](#), [28](#)
 - viewing generated keys [29](#)
- ## P
- power guides
 - key management setup workflow [18](#)
 - Power Guides
 - requirements for using this guide [5](#)
- ## R
- rekeying
 - SEDs to MSID [49](#)
 - replacing
 - self-encrypting disks [41](#)
 - SSL certificates before expiration [42](#)
 - returning SEDs to service
 - when authentication keys are no longer available [48](#)
- ## S
- sanitizing
 - NSE disks [44](#)
 - security
 - enabling cluster-wide FIPS-compliant mode [27](#)
 - SEDs
 - methods for making data inaccessible on [43](#)
 - returning to service when authentication keys are no longer available [48](#)
 - returning to unprotected mode [49](#)
 - self-encrypting disk
 - information to collect before configuring with external key management servers [9](#), [18](#)
 - self-encrypting disks
 - configuring for FIPS 140-2 compliance [26](#), [31](#)
 - overview of managing [32](#)
 - replacing [41](#)
 - returning to service when authentication keys are no longer available [48](#)
 - servers, external key management
 - assigning authentication keys to SEDs [25](#), [30](#)
 - creating authentication keys [23](#), [24](#)
 - deleting a connection [50](#), [51](#)
 - disconnecting [50](#), [51](#)
 - information to collect before configuring Storage Encryption with [9](#), [18](#)
 - restoring authentication keys [40](#)
 - setting up [11](#), [20](#), [21](#)
 - setting up
 - external key management servers [11](#), [20](#), [21](#), [23](#), [24](#)
 - setting up key management
 - workflow [18](#)
 - SnapLock
 - use with NetApp Volume Encryption [6](#)
 - use with NVE [6](#)
 - SnapMirror
 - use with NetApp Volume Encryption [6](#)
 - use with NVE [6](#)
 - SnapVault
 - use with NetApp Volume Encryption [6](#)
 - use with NVE [6](#)
 - SSL certificates
 - installing on cluster [10](#), [19](#)
 - replacing before expiration [42](#)
 - Storage Encryption
 - installing SSL certificates on the cluster for [10](#), [19](#)
 - support for [17](#)
 - Storage Encryption with external key management servers
 - information to collect before configuring [9](#), [18](#)
 - suggestions
 - how to send feedback about documentation [58](#)
 - support for
 - Storage Encryption [17](#)
- ## T
- Twitter
 - how to receive automatic notification of documentation changes [58](#)
- ## U
- unprotected mode
 - returning SEDs to [49](#)
 - unreachable key management servers
 - precautions taken in the event of during boot process [53](#)
- ## V
- versions, NetApp Volume Encryption
 - determining the ONTAP version [8](#)
 - versions, NVE
 - determining the ONTAP version [8](#)

W

workflows

key management setup [18](#)

NetApp Volume Encryption [7](#)

NVE [7](#)

X

XTS-AES-256 keys [6](#)