C H A P T E R 6

Configuring SME Disks

This chapter contains information about managing disks using SME, referred to as SME Disk management.

Note Read all of the Cautions carefully while configuring SME Disks.

This chapter includes the following topics:

Information About SME Disk Management

SME Disk management includes the following topics:

SME Disk Architecture

The SME Disk feature encrypts the data contained in a disk.

The software architecture for the SME Disk is similar to the existing SME infrastructure that supports the SME tape. Disk support has been added to the existing SME architecture from MDS NX-OS Release 5.2.1. Figure 6-1 depicts a typical dual-fabric production data center. The SME disk functionality is provided on the following Cisco MDS hardware:

- 16-Port Storage Services Node (SSN-16) Module
- 18/4 Multiservice Module (MSM-18/4)
- 9222i Switch

Figure 6-1 shows the SME Disk architecture.

Figure 6-1   SME Disk Architecture
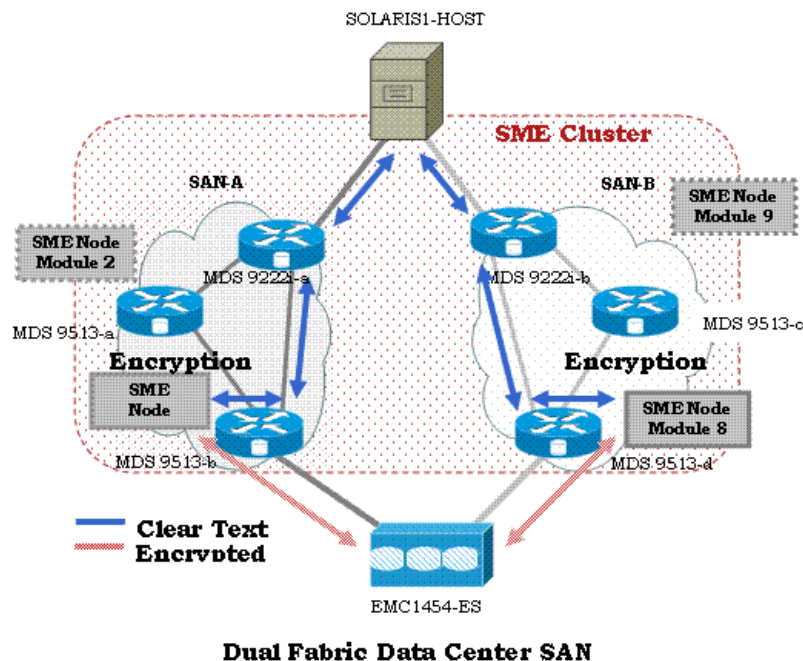
In the figure, a switch is termed as an SME node. A module has one or more interfaces that support SME. The SME nodes encrypt and decrypt the traffic flowing between the host and the storage. The Fibre Channel traffic to be encrypted or decrypted is directed to the SME node through the FC-Redirect feature of the SAN. For example, the SSN-16 can support 4 SME interfaces and the MSM-18/4 supports 1 SME interface.

SME Disk functionality works in the dual-fabric topology, where it performs encryption and decryption on all the paths present between the host and the storage.

⚠
Caution   SME Disk does not support thin provisioning of disks.

SME Disk needs to manage all the paths to the disk in both the fabrics. An SME cluster provides this functionality. An SME cluster consists of a collection of SME nodes. Any SME node that fails in a cluster triggers another node in the same cluster to take control of the encryption and/or decryption activity.

The disk on which the SME Disk provides the encryption and/or decryption functionality can be the one without any existing data or the one with existing data. If the disk has existing data, the existing data needs to be encrypted. The process of converting the existing clear data to encrypted data is termed as data preparation.

Data preparation can be performed in offline mode. In the offline data preparation mode, the application on the host accessing the disk is quiesced and no I/Os are sent to the disk. SME Disk functionality also ensures that if any host tries to read or write the data from or into the disk, the particular I/O is failed back to the host.

In the Online Mode, the application on the host can continue to perform I/O on the disk while SME is converting the existing data on the disk from clear text to encrypted text.

The disk is uniquely identified in configuration by the cluster name, disk group name, and disk name.

For the purpose of encryption or decryption, the SME Disk requires encryption keys. For every encrypted disk, a key is generated. The SME's existing Key Management Center (KMC) infrastructure is used for SME disk key management. Keys for each disk are generated by the Storage Media Encryption coprocessor and are stored in the SME Key Management Center.

⚠️

Caution   SME Disk does not allow dynamic resizing of LUN.

For Release 5.2.1, the maximum supported disk size is one block less than two terabyte (TB). The maximum LBA is 0xFFFFFFFE.

From Release 5.2.6, the supported disk size for signature and nonsignature mode clusters is greater than two TB.

SME Disk only supports disk block size of 512 bytes.

For Release 5.2.1, SME Disk does not support online conversion of existing clear data on the disk to encrypted data.

Replication

There are two kinds of replication:

- Mirrors or Clones—When the data for the source disk is duplicated by the disk array into another disk in the same storage system, the destination disk is called a mirror or clone of the source disk. This is called local replication.

- Remote Replication—When the data for the source disk is being duplicated by the disk array into another disk in a remote storage system, then the source disk and the remote disk are in a replication relationship. Based on the distance and bandwidth availability between local and the remote site, remote replication is categorised under the following types:

  - Synchronous—The local disk array does not respond to the write command on the local LUN until the data is also written to the remote LUN.

- Asynchronous—The local disk array does not immediately write the data to the remote LUN. The changes to the local LUN are batched into a delta dataset and periodically sent to the remote LUN.

Snapshot

Snapshots are point-in-time copies that can be created instantly for a source disk. Once a snapshot is created any writes to the source disk will result in the previous data to be saved elsewhere before modification. This allows the disk array to present a specific point-in-time copy of the data of the source disk.

Managing Replication with SME

SME supports replication through Disk key replication (DKR). DKR simplifies the key management of the source and destination disk by automating the propagation of the source disk key to destination disk. SME Disk Clusters are of two modes:

- Non-signature cluster
- Signature cluster

Replication management is the same for both the cluster modes. Replication management consists of following steps:

- Extraction of replication relationship using array vendor specific technology. The output of this step results in identifying the source and destination disk relationship based on the SCSI properties of the vendor, product. and device identifiers.

- Importing the replication relationship information into SME through DKR using DCNM.

> **Note** Ensure you manage all SME configuration operations on the disks in a DKR relationship through DCNM only.

Manage Key Change Operations in DCNM for DKR

Key change operations involve the following:

- No data preparation—Any local key changes will result in DKR suspending host access to the remote disk. Once the local key change is verified for data integrity and the data replication to the remote end is synchronized, the admin can select the corresponding relationship and perform the sync operation in DKR. This operation will synchronized the source and destination keys and resume the host access to the remote disk.

- Data preparation—Ensure you disable DKR relationship and the replication between the source and destination disk before you start data preparation on the source disk. This is a disk array vendor specific operation. Once you complete data preparation and have verified for data integrity, follow the procedure below:.

  - Enable the data replication between the source and destination using disk array vendor specific operation.

  - Once data is synchronized between the source and destination disk, enable the DKR relationship. This operation will synchronize the source and estination keys.

> **Note** Host access on the destination disk should be quiesced until the above two steps are completed.

Managing Snapshots in SME

This section describes how to manage snapshots of crypto disks. Snapshot management is different for signature and non-signature clusters.

To manage crypto snapshots that are discovered by a same host through the same SME cluster as the source disk, then follow the below procedure:

Step 1   Start a discovery in SME for configuring the snapshot disks.

Step 2   If SME finds a valid SME metadata on the disk media with no corresponding active key in the Key management center (KMC) then the disk is put in a failed state by SME.

Step 3   The administrator has the option to recover the disk using recovery from- metadata option.

Step 4   Once the above recovery is performed, the snapshot comes up as a crypto disk and it can be accessed by the host.

To manage snapshots that are being discovered by a different host through a differnt SME cluster from the source, use DKR and follow the below procedure:

Step 1   tart a discovery in SME for configuring the snapshot disks.

Step 2   Once the snapshot disks are configured into SME, create a DKR relationship between the source and snapshot disk.

Step 3   Enable the DKR relationship to synchronize the source and snapshot key.

Step 4   Destroy the DKR relationship between the source and snapshot.

Step 5   Host can now have access to the snapshot disk.

> **Note** Ensure you destroy the DKR relationship between the source and snapshot after key synchronization. If the source key is rekeyed, it may result in data integrity issues on the snapshot.

Cluster Support

For Release 5.2.1, the switch can support up to two SME clusters. The following prerequisites must be met for supporting multiple clusters. If these prerequisites are not met data loss can occur.

- For SME disks, the SME cluster must be set as disk capable.
- SME Tape and SME Disk cannot co-exist in the same SME cluster. Use different clusters for SME Disk and SME Tape.
- Multiple SME clusters can be supported on the same MDS chassis with the following requirements :
  - SME tape cluster node is on one Cisco MSM18/4 switching module.

- SME disk cluster node is on another Cisco MSM 18/4 switching module.

- For the SSN-16, SME Tape and Disk belong to different crypto nodes and belong to different clusters.

- Do not use the same target ports in different clusters.

- The same disk cannot be part of more than one SME cluster otherwise data loss occurs.

- Do not add the same SME interfaces in two different clusters.

From MDS Release 5.2(6), SME Disk can write a signature to the media to identify the disk as a crypto disk. These SME clusters are called signature clusters. Nonsignature clusters are SME Disks that do not write a signature on the media to identify crypto on the disk.

Data Preparation

Data preparation is a process that converts the clear data on the disk to encrypted data and vice versa. When the SME Disk feature is enabled on an existing disk containing clear data, the existing clear data needs to be converted to encrypted data. The process can be done in two ways:

- With the host accessing the data. This is called as the online data preparation mode.

- With the disk that is inaccessible to the host. This is called as the offline data preparation mode.

Note   Only offline data preparation mode is supported.

When the SME Disk feature is enabled on a new disk that does not contain prior data, the host I/Os read/write is decrypted or encrypted using a key. This encryption process is transparent to the application. For these disks, the data preparation process is not required.

Note   Ensure you do not change the cluster configuration while data preparation is under progress and do not remove node or add a new node while data preparation is in progress.

For disks requiring data preparation, the user must have backed up data before starting conversion of clear data to encrypted data.

In an SME cluster, there can be multiple SME nodes handling the ITLs associated with a particular crypto disk. The multiple SME nodes encrypt or decrypt data written to or read from the crypto disk. However, the responsibility of the data preparation or rekeying for a crypto disk is assigned to one SME node which is the data preparation node. The cluster master handles the data preparation node based on the following:

- LUN visibility (report LUN, INQ, and so on) or accessibility (reservations)

- Target port affinity

- Load factor of the SME nodes

For signature mode, when converting a clear disk to crypto disk, the administrator must ensure that the reserved space of 64 MB at the end of the disk is available on the SME disk.

Note   Disk Key Replication (DKR) must be disabled when performing data preparation on the source disk.

Recovering SME Disk when Data Preparation Fails

When data preparation fails, SME Disk puts the disk in a failed state. The disk is not accessible to hosts and all paths of the disk are put in I/O reject state (reject all host I/Os state). To recover the disk from the failed state, follow these steps:

Step 1   Because the disk is not accessible from the host, restore the contents of the failed disk on the backend storage.

Step 2   Enter the **recover** command with appropriate arguments to recover the disk to the proper crypto state based on the backup data. For more information on the **recover** command syntax using CLI, see "Recovering the SME Disk" section on page 6-27 and through the GUI, see "Recovering SME Disks" section on page 6-41.

In the Signature mode, the disk can be recovered by using the signature information on the media.

Offline Data Preparation

Offline data preparation is performed when the applications running on the host is not accessing data from the disk that is undergoing data preparation.

Figure 6-2 shows the SME Disk offline data preparation architecture.

Figure 6-2   SME Disk Offline Data Preparation Architecture
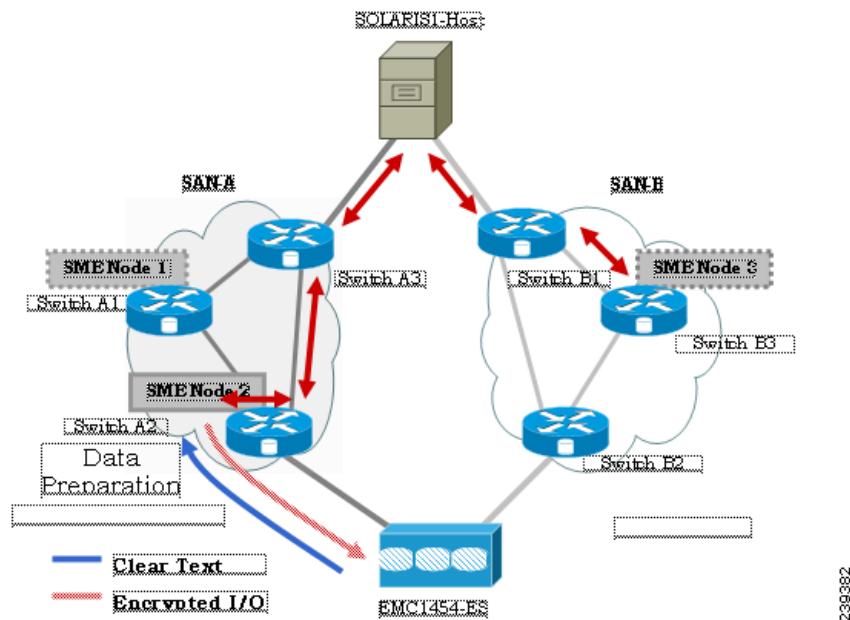
The offline data preparation involves the following actions:

- Quiescing the host applications by stopping the host I/O traffic.

- Backing up the clear data in the targeted disk. The backup can be to another disk or to an external tape. This backup is used to recover from errors.

- Server I/Os during the duration of the offline data preparation are rejected by the SME node.

> ⚠
> **Caution** While host I/Os are blocked the host paths must be online during offline data preparation since the identity of the host port is used by the crypto engine. All DKR relationships that involves disk must be in disable state. Disk Key Replication (DKR) is used to manage remote replication relationships. For more information, see Configuring DKR, page 6-48.

> ⚠
> **Caution** Disable all replication links of that disk before starting data preparation on the disk.

> ⚠
> **Caution** Destroy older snapshots once the rekey is successful. The old snapshot can be kept as a backup to recover in case data preparation or rekey fails. Once successful, SME Disk does not support reading from older snapshots using previous keys.

- The offline data preparation is done by one SME node that uses the host identity of the selected path on which data preparation related I/Os are issued to the disk. During this process, I/Os to the targeted disk are failed back to the host with a SCSI check condition **not ready**. Server I/Os during the duration of the offline data preparation are sent back to the host as an SCSI check condition.

- Unquiescing the host applications. After the data preparation is completed, the applications running on the host are brought online to start access data from the encrypted crypto disk.

Online Data Preparation

Online data preparation is performed when the applications on the host are accessing the data on the crypto disk. The server read or write I/Os are decrypted or encrypted by the SME nodes while the data preparation process is going on.

> ✎
> **Note** For this release, only offline data preparation mode is supported.

Rekeying

Once the data on the disk is encrypted, the key associated with the encrypted data has to be changed for security reasons. The change policy is organization specific. The process of changing the key associated with the encrypted data for a disk from an old key to a new key is referred to as the rekey process.

Rekeying is a special function of the data preparation operation where the currently encrypted contents of the disk is read, decrypted using the current (old) key, encrypted with a new key, and written back to the disk.

> ✎
> **Note** You cannot change the quorum or the master node during a Master key rekey.

Replacing an SME Enabled MDS Switch

The steps to replace an MDS Switch acting as a node in one or more SME clusters depends on your current topology and configuration.

Multi-node Cluster

If the MDS switch you want to replace is the master node in one or more SME Clusters, you must first fail the master node and then remove the failed master node.

If the MDS switch you want to replace is a non-master node in a multi-node SME cluster, you must remove the SME interfaces (if any) and the node from the clusters using the DCNM SME management UI. For more infomation, see "Removing (Unbinding) SME Interfaces from a SME Cluster" section on page 3-8 and "Deleting Switches From a SME Cluster" section on page 3-8.

Single-node Cluster

If the MDS switch you want replace is the only node in an SME Cluster, the operation is completely destructive to the SME Cluster. Follow the procedure under Appendix M, "Disaster Recovery in SME." to build a new SME Cluster on the new switch.

Turning Off Encryption

If you disable encryption in the signature mode, the host can view the exact size of the disk. The exact size of the disk is 64 MB more than the size of the disk seen during encryption.

Snapshot Support

There are two types of snapshot supported:

- Nonsignature mode—In the nonsignature mode, when a snapshot is first discovered, SME does not detect it as a snapshot of a crypto LUN. The administrator must use the key of the source LUN and enable encryption without data preparation on the new LUN.

- Signature mode—In the signature mode, the SME disk detects snapshots during discovery. The SME disk discovers the signature of the media and moves these disks to a failed state with the explanation that they may be possible crypto snapshots. To enable encryption on crypto snapshots, you can use the recover-from-metadata option.

SME Disk Key Management

SME disk uses a two-level key hierarchy. An SME cluster consists of various disks that are grouped functionally into disk groups. The following is the key hierarchy:

- Master Key—Generated when a SME cluster is created. A master key is used to wrap the disk keys in the cluster. A master key is always wrapped with a password. The three security modes to store the master key are Basic, Standard, and Advanced. For more information on SME key details and the security modes, see "Configuring SME Key Management" section on page 7-1.

- Disk Key—Generated only when the encryption is enabled. Only when it is enabled, the disk status is Crypto. Disk keys are always wrapped with the master key.

Keys are identified using a Globally Unique Identifier (GUID) and disk keys are stored in the Cisco Key Management Center (KMC). These disk keys are encrypted using the master key.

Key Generation

The secure keys are generated for each SME disk in the cluster in the SME node in a cryptographic way. Random key numbers are generated with the FIPS random-number generation. The key size used is 256 bits.

A new key can be generated for each SME disk that is enabled. Keys also can be imported from a key file. Keys can also be replicated using the disk key replication feature.

Disk States

These types of disk states are available:

- Clear—The disk is online and encryption is disabled.
- Crypto—The disk is online and encryption is enabled.
- Suspend—The disk has been suspended and the host I/O access is suspended.
- Data-preparing—The data on the disk is currently being converted by SME Disk.
- Failed—The disk data needs to be restored due to the failed data preparation.
- Failed—Fails due to a mismatch between the signature and KMC.
- Pending enable no-dataprepare (Wait SME enable)—When there is a disk state mismatch between switch persistent data and CKMC. This state occurs when a customer does not copy the running configuration to saved configuration before rebooting the switch.

MKR fails when the disks are in the following states:

- Failure—MKR fails when there is a mismatch between the metadata and KMC.
- Failure—MKR fails when the metadata exists but there is no key in the KMC.
- Failure—MKR fails when the metadata write fails.
- Preparing (progress 2%, remainin…...)—MKR displays the status preparing and fails.
- Configured path status
- Offline—MKR fails if the disk itl discovery is pending.
- Is online—MKRfails when the disk itl is in a fault I/O state and is configured.
- Crypto—MKR fails when the KMC verification is still pending.
- MKR fails if the metadata update is pending.
- Crypto—MKR fails if the FSM update is pending.

Note   Ensure all paths to the disk are discovered and are online.

Cisco KMC

The Cisco KMC is the centralized key management system that stores the key database for active and archived keys required for the encryption and decryption in the SME disk.

Each SME disk can have zero or one active key and zero or more archived keys.

Each key entry consists of the following:

- Cluster name, disk group name and disk name needed to identify the configured disk in sme configuration
- Vendor ID, Product ID, and Device Identifier needed to identify the corresponding physical disk in SAN
- Active or archived state
- Creation and archived timestamp

SME cluster will contact and verify and update the CKMC during configuration changes.

CKMC provides the following features:

- Centralized key management to archive, purge, recover, and distribute disk keys.
- Integration into the DCNM-SAN Server depending on the deployment requirements.
- Integrated access controls using AAA mechanisms.

For more information on the security modes and key management settings, see the "Configuring SME Key Management" section on page 7-1

Cisco KMC supports SME disk-related operations. KMC operations include the following topics:

- Archiving Clusters, page 6-11
- Purging Disks or Disk Groups, page 6-11
- Rekeying, page 6-11
- Accounting, page 6-12

Archiving Clusters

Archiving deletes the cluster from the switch and it retains the keys in the Cisco KMC.

Purging Disks or Disk Groups

When storage arrays are decommissioned either due to lease expiration or upgrade, the keys associated with the disks can be purged. Purging keys can be done either at the disk level or at the disk group level. By deleting an active disk group, all the keys are archived. By deleting an archived disk group, all the keys are purged.

⚠️
Caution   Purging the key is an unrecoverable operation. Unless there are exported backups of the key database, the key that is purged cannot be retrieved forever.

Rekeying

Data in the disk and disk group can be rekeyed either periodically for better security or on-demand when the key security has been compromised.

✎
Note   From Release 5.2.6, master key rekey is supported.

The rekey operation at an individual disk level generates a new key for the disk and archives the old key. A data preparation operation is triggered to decrypt the data using old key, encrypt the data with the new key, and write it back to the disk.

The rekey operation performed at a disk group level on all the disks or a subset of disks in the disk group. KMC maintains a history of keys for all of the disks.

Accounting

Cisco KMC maintains an accounting log to record all the key-related operations, their results, and other related information. The view provides support to filter the log records based on the patterns. For more information, see .

Quorum Disk

A quorum has to be present for a cluster to be functional as a cluster is a group of servers. A quorum is defined as N/2 + 1 servers in the cluster are up and running. N is the total number of servers in the cluster. To avoid a split-brain scenario for a cluster with an even number of servers, in the case where half of the members of the cluster lose communication with the other half of the members of the cluster, a quorum disk is used to determine which partition has the quorum for remaining in the cluster.

Because a server cluster has to be functional even when an SME cluster fails, it is important that the quorum disk not be configured as a crypto disk.

Data Replication

Replication is a disk array based technology where the disk array automatically duplicates data from one LUN to another.

Data replication relationship is of two types:

- Synchronous mode
- Asynchronous mode

Remote replication involves in moving of data on primary storage arrays over WAN links to secondary storage arrays on secondary sites. Remote replication protects data loss in case of primary site failure or a geographical disaster.

SME does not perform data replication. SME is designed to support other third-party data replication solutions.

SME Disk Key Replication

The SME Disk Key Replication (DKR) feature manages key replication in support of third-party data mirroring solutions. The DKR feature supports the following:

- Mirrors or clones—A copy of the data in the source disk is duplicated by the disk array into another disk (mirror or clone) in the same storage system.
- Replication—The data in the source disk is duplicated by the disk array into another disk in a remote storage system. Two types of replication are available: Synchronous and Asynchronous.

Note Disk Key Replication only takes care of key replication. The user needs to ensure data replication.

Note DKR relationships are only allowed between the same SME Disk Clusters of the same type. For example, a Signature SME Disk cluster cannot be used in DKR with a nonsignature SME Disk cluster.

The source and the destination disk can be in three stable states: clear, crypto, and failed. When a disk key replication relationship is synchronized, both the state and the active crypto key of the source disk are replicated to the destination disk.

The DKR feature is maintained by DCNM-SAN and all SME key modification operations for disks using DKR must be done through DCNM-SAN.

Caution The key replication must be disabled when a disk is undergoing data preparation or rekey. The combination is not supported.

Note To ensure appropriate key associations, you must ensure that the same KMC (database) manages all the disks that are involved in a replication or snapshot relationship.

Note DKR must be disabled when converting a nonsignature SME disk cluster to a signature SME disk cluster.

Prerequisites for DKR

DKR has the following prerequisites:

- The CKMC must be the same for the DKR feature to connect and transfer data. The same KMC should be used for source and destination disks that are managed for disk replication.

- Disk replication takes care of key replication only and not the data replication as it is done by the storage vendor. Proper steps should be followed while syncing the keys.

Caution Once a disk is added to an DKR relationship all SME operations on that disk must be done only through DCNM-SAN. SME Disk configuration must not be done through CLI for disks involved in DKR relationship. Using the CLI results in unpredictable results and can put data on the disk at risk.

Guidelines and Limitations for DKR

The following are the guidelines and limitations for disk replication support:

- The Recover Point I/O journal snapshots are not supported across key change operations.

- Any type of snapshot is not supported when encryption is enabled, encryption is disabled, or on a rekey operation.

⚠

Caution   For non-signature clusters, we recommend that the snapshots be destroyed once the above operation is successfully completed. For signature clusters, snapshots can be supported across rekey operations.FR

Replication or Mirroring Requirements

The following are the requirements for replication or mirroring:

- A key update on the source disk must result in a key update on the destination disk that is in a current replication relationship with the source disk.

- A source disk can be the source disk for multiple destination disks.

- A destination disk in a replication relationship can be the destination of only one replication relationship.

DKR Features

DKR provides the following key features:

- DKR map file—Contains the XML-formatted information that allows you to input information about the replication relationships into DCNM-SAN.

- DKR database—DCNM-SAN processes the DKR map file and stores the relationships in a database in the *source disk*:*destination disk*:*type of relationship*:*state of relationship* format.

- Management of SME disk key change operations—All of the key change operations on the source disk need to be replicated on the destination disk.

DKR Relationships

DKR relationships are created through the DKR map file. Specify the source and destination disks that are in a DKR relationship, which allows you to input a large number of entries in a single operation. DKR relationships can be set up in two ways:

- Remote Replication relationship—The destination disk might be exported to the host and can be visible to the SME disk through device discovery.

DKR Mapping File

You can populate the DKR database by giving DCNM-SAN a map file that contains the replication and snapshot relationships. Each DKR relationship consists of a source and destination disk.

The disk can be identified in the following format:

```
<?xml version="1.0" encoding="UTF-8"?>
<SME_DKR xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="DKR.xsd">
<Version>Version</Version>
<Options>SME_DKR_NONE</Options>
<Relations>
<Type>SME_DKR_MIRROR</Type>
<Source>
<Label>grp-1</Label>
<Cluster_Name>source-1</Cluster_Name>
<Disk_Group_Name>primary-cx400</Disk_Group_Name>
<Disk_Name>pry0</Disk_Name>
<Identifier>
```

```
<VPW>
<Vendor>DGC     </Vendor>
<Product>VRAID          </Product>
<WWN>600601609bc12a008ca7298a9c44e011</WWN>
</VPW>
</Identifier>
</Source>
<Destination>
<Label>grp-2emote</Label>
<Cluster_Name>destination-1</Cluster_Name>
<Disk_Group_Name>secondary-cx400</Disk_Group_Name>
<Disk_Name>sec0</Disk_Name>
<Identifier>
<VPW>
<Vendor>DGC     </Vendor>
<Product>VRAID          </Product>
<WWN>600601600e602a00b461b7289b44e011</WWN>
</VPW>
</Identifier>
</Destination>
</Relations>
</SME_DKR>
```

Note The administrator has to configure and discover the destination disk explicitly because DCNM-SAN does not configure the destination disk in the destination cluster.

ISSU with SME Disk

In-Service Software Upgrade (ISSU) has the following requirements:

- No SME configuration changes must be in progress or initiated while an ISSU is in progress.

- Ensure that no data preparation operations are underway before you schedule ISSU.

- ISSU causes the crypto nodes (DPP) to become offline during the firmware upgrade causing host I/O traffic to be disrupted.

- The IT-nexus that are bound to that crypto node can end up migrating to a different crypto which can cause an imbalanced load distribution.

Note For SME disk, the ISSU from Cisco NX-OS Release prior to 5.2(1) is not supported and the SME Disk configuration will be rejected.

When upgrading from Release 5.2.1 to Release 5.2.6, the clusters have to be in the nonsignature mode and when downgrading from Release 5.2.6 to Release 5.2.1, signature clusters have to be deleted.

Managing Key Change Operations in Cisco DCNM for DKR

The following are the two key change operations:

- No data preparation—Any local key changes result in DKR suspending host access to the remote disk. Once the local key change is verified for data integrity and the data replication to the remote end is synchronized, the administrator can select the required relationship and perform the synchronization operation in DKR. This operation synchronizes the source and destination keys and resumes the host access to the remote disk.

- **Data preparation**—Ensure that you complete the following before starting the data preparation on the source disk:

    – Disable DKR relationship.

    – Disable the replication between source and destination disk. This is a disk array vendor-specific operation.

    Once data preparation is complete and verified for data integrity, perform the following:

    – Enable the data replication between the source and destination using the disk array vendor-specific operation.

    – Once data is synchronized between the source and destination disk, enable the DKR relationship. This operation synchronizes the source and destination keys.

⚠
Caution   Stop accessing the host on the destination disk until the data preparation is complete. Accessing the host during data preparation results in data loss.

Read-Only Disks

Read-only disks allows the host to read the contents of a disk in a failed state by specifying an encryption key. This is a solution to recover the contents of a disk. When there is an situation where the possible set of keys to a disk is known, this mode can be used to try each of the possible keys to find the correct key to read the contents of the disk. This mode is not expected to be used in the normal configuration or normal recovery procedures that have been discussed in this document.

To recover the data using the read-only mode, perform the following steps:

Step 1   In the **Manage Disk Encryption:Settings** page, select **Make Read-Only**.

Once you get the correct key, you can recover the disk using the recovery wizard.

Step 2   For more information in recovering disks, see Recovering SME Disks, page 6-41.

Write Signature

You can use this feature on the signature cluster mode. When a disk has not been converted to signature mode, you can write the signature to the disk manually. You can do this through the disk details page or in batch mode through the cluster details page.

✎
Note   Use this command for converting a non-signature disk cluster to a signature disk cluster.

Configuring SME Disk Management Using the CLI

⚠
Caution   Cisco KMC must be online at all times during configuration changes.

> **Note** In order to create or configure an SME Disk-capable cluster, you need to define the cluster as disk capable. For more information on how to configure this definition, refer to the "Creating the SME Cluster" section on page 4-6.

> **Note** SME Disk cluster is not compatible with the following FCIP configurations:
>
> - FCIP with IP compression enabled
> - FCIP with IPsec and WA

This section includes the following topics:

Discovering IT-Nexus

> **Caution** All IT-nexuses that host paths between the server and storage must be added to the configuration or else the data integrity is at risk.

To discover the IT-nexus disk, follow these steps:

	Command	Purpose
Step 1	switch# **config t**	Enters configuration mode.
Step 2	switch(config)# **sme cluster** *clustername*	Specifies the cluster and enters SME cluster configuration submode.
Step 3	switch(config-sme-cl)# [**no**] **discover host** *wwn1* **target** *wwn2* **vsan** *vsanid* **fabric** *fabricname*	Specifies the IT-nexus that needs to be discovered.

The discovery of Initiator-Target-LUN nexus (ITL) will involve querying the CKMC to determine the crypto state and if appropriate the active key of the disk. For more information on crypto disk states, see "Disk States" section on page 6-10.

> **Note** Disks and multiple paths to each disk are identified through SCSI Inquiry data of Vendor ID, Product ID, and Device Identifier (VPD).

Note In a scripted environment where multiple IT-nexuses discovery is issued simultaneously, the resulting situation can cause too many queries to CKMC. This can sometimes result in some queries timing out. The workaround is to rediscover the IT-nexus. To prevent this scenario in a scripted environment, its always good to give a delay of one minute between each discovery command.

Displaying IT-Nexus

To display all IT-nexuses that are added to a cluster, enter this command:

```
switch(config-sme-cl)# show sme cluster c52 it-nexus
----------------------------------------------------------------------------
    Host WWN,              VSAN    Status    Switch         Interface
    Target WWN
----------------------------------------------------------------------------
21:00:00:1b:32:84:ca:4a,
20:04:00:a0:b8:1f:4a:c6   5       online    172.23.146.52sme10/1
```

Note The switch and the crypto node where the IT-nexus is bound to is also shown. In the above example, the IT-nexus is being hosted by the following:

- Switch with IP address 172.23.146.52
- On the control path processor (CPP) in the line card on module 10
- I/O traffic is being hosted by the data path processor (DPP) 1 on line card in module 10

Adding SME Nodes to the Cluster

Detailed Steps

To add an SME node to the cluster, follow these steps:

	Command	Purpose
Step 1	switch# **config t**	Enters configuration mode.
Step 2	switch(config)# **sme cluster** *clustername*	Specifies the disk name to be created.
Step 3	switch(config-sme-cl)# **node local**	Specifies the local node that will be added to the cluster.
Step 4	switch(config-sme-cl)# **node** *remote node ID*	Specifies the IP address or name of the remote node that will be added to the cluster.

Adding SME Encryption Engine to the Cluster

Detailed Steps

To add an SME encryption engine to the cluster when the encryption engine is local to the master node, follow these steps:

	Command	Purpose
Step 1	switch# **config t**	Enters configuration mode.
Step 2	switch(config)# **sme cluster** *clustername*	Specifies the disk name to be created.
Step 3	switch(config-sme-cl)# **node local**	Specifies the local node that will be added to the cluster.
Step 4	switch(config-sme-cl-node)# **fabric-membership** *fabricname*	Specifies the local switch fabric name.
Step 5	switch(config-sme-cl-node)# **interface sme 1/1 force**	Specifies adding encryption engine to the cluster.

To add a encryption engine that resides on the non-master node, go to the mater node and create an SME interface and follow these steps:

	Command	Purpose
Step 1	switch# **config t**	Enters configuration mode.
Step 2	switch(config)# **sme cluster enable**	Enables the cluster feature.
Step 3	switch(config)# **sme enable**	Enables the SME feature.
Step 4	switch(config-sme-cl-node)# **interface sme 1/1 force**	Specifies adding encryption engine to the cluster.

On the master node, add the remote crypto engine to the cluster as follows:

	Command	Purpose
Step 1	switch# **config t**	Enters configuration mode.
Step 2	switch(config)# **sme cluster** *clustername*	Specifies the disk name to be created.
Step 3	switch(config)# node *<node alias>* ip-address *<ip address of remote switch>*	Adds remote node to the cluster.
Step 4	switch(config)# fabric-membership *<name of fabric>*	Specifies the remote switch fabric name.
Step 5	switch(config-sme-cl-node)# **interface sme 1/1 force**	Specifies adding encryption engine to the cluster.

Configuring a Disk Group

The disks in an SME cluster can be grouped functionally into disk groups.

Detailed Steps

To configure a disk group, follow these steps:

Send documentation comments to mdsfeedback-doc@cisco.com

	Command	Purpose
Step 1	switch# **config t**	Enters configuration mode.
Step 2	switch(config)# [**no**] **sme cluster** *clustername*	Specifies the cluster and enters SME cluster configuration submode.
Step 3	switch(config-sme-cl)# [**no**] **disk-group** *dg-name*	Configures a disk group.

Adding a Disk to the Disk Group

A disk is specified as part of a disk group and is identified using a name as an alias.

Detailed Steps

To add a disk to the disk group, follow these steps:

	Command	Purpose
Step 1	switch# **config t**	Enters configuration mode.
Step 2	switch(config)# [**no**] **sme cluster** *clustername*	Specifies the cluster and enters SME cluster configuration submode.
Step 3	switch(config-sme-cl)# [**no**] **disk-group** *dg-name*	Configures a disk group.
Step 4	switch(config-sme-cl-dg)# [**no**] **disk** *disk-name*	Specifies the disk name to be created.

Adding Paths to the Disk

⚠

Caution   All paths (ITLs) of a host to the target LUN must be in the same disk to prevent data corruption.

A disk is specified as part of a disk group and is identified using a name as an alias. All the paths to the disk in the cluster must be specified using the host, target, LUN, VSAN, and fabric.

Detailed Steps

To add a disk, follow these steps:

	Command	Purpose
Step 1	switch# **config t**	Enters configuration mode.
Step 2	switch(config)# [**no**] **sme cluster** *clustername*	Specifies the cluster and enters SME cluster configuration submode.
Step 3	switch(config-sme-cl)# [**no**] **disk-group** *dg-name*	Configures a disk group.

	Command	Purpose
Step 4	`switch(config-sme-cl-dg)# [`**`no`**`] disk disk-name`	Specifies the disk name to be created.
Step 5	`switch(config-sme-cl-dg-disk)# [`**`no`**`]` **`host`** `wwn1` **`target`** `wwn2` **`lun`** `11` **`vsan`** `v1` **`fabric`** `f1`	Specifies the path to the disk in the cluster.

> **Note** If the IT-nexus specified in the path above is not configured in SME, SME will also trigger a discovery of the IT-nexus along with adding the configured path to the specified disk. In a scripted environment, when adding paths, it is always advisable to give a delay of one minute to allow the IT-nexus discovery to complete.

Displaying ITL-Nexus

To see the list of paths discovered on SUP, enter this command:

```
switch(config-sme-cl)# show sme cluster c52 disk detail
Disk 1 is crypto
    Model is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0b80001f4ac4000032454a3a69ce
    ASL ID is 581688B7
    Is configured as disk device d1 in disk group dg1
    Paths
      Host 21:00:00:1b:32:84:ca:4a Target 20:04:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5
         Is online (SUCCESS), configured
```

To see the list of paths discovered on CPP where IT-nexus is bound, enter this command:

```
switch# attach module 10
Attaching to module 10 ...
To exit type 'exit', to abort type '$.'
module-10# show sme internal info crypto-node 1 itl brief
---------------------------------------------------------------------------------------------
    if-ndx            host                    tgt            vsan lun  type
sme    locking event        state
---------------------------------------------------------------------------------------------
   0x12480000  21:00:00:1b:32:84:ca:4a  20:04:00:a0:b8:1f:4a:c6    5  0x0000
1  1          Unlocked  SMED_ISAPI_ITL_ST_UP_CRYPTO
```

Managing Disks

This section includes the following topics:

- Enabling Encryption on the SME Disk with Data Preparation, page 6-22
- Modifying the SME Disk Key, page 6-26
- Recovering the SME Disk, page 6-27

Send documentation comments to mdsfeedback-doc@cisco.com

Enabling Encryption on the SME Disk with Data Preparation

When SME encryption is enabled on a set of disks that have existing data, the existing data on the disks must be converted from clear to crypto. This process is called data preparation.

This operation involves reading data from the disk, encrypting the data, and writing back to the disk. The crypto engine takes on the host port identifier to perform the above operation.

The action to perform data prepare is **enable offline**.

⚠️

Caution   The Initiator-Target-LUN(ITL) path that is undergoing data preparation must be online until the data preparation is complete. Any host port or target port flap results in the failure of data preparation.

✎

Note   Currently, offline data preparation is supported.

⚠️

Caution   During the data preparation process, we do not recommend that you manually enter the GUID of the key. The SME should generate the key automatically.

Detailed Steps

To perform data preparation on a disk, follow these steps:

	Command	Purpose
Step 1	switch# **config t**	Enters configuration mode.
Step 2	switch(config)# **sme cluster** *clustername* switch(config-sme-cl)#	Specifies the cluster and enters SME cluster configuration submode.
Step 3	switch(config-sme-cl)# **disk-group** *dg-name* switch(config-sme-cl)#	Creates a disk group.
Step 4	switch(config-sme-cl-dg)# **disk** *disk-name*	Specifies the disk name to be created.
Step 5	switch(config-sme-cl-dg-disk)# **enable offline**	Performs offline data preparation on an SME disk to convert clear data to encrypted data.
Step 6	switch(config-sme-cl-dg-disk)# **no enable offline**	Performs offline data preparation on an SME disk to convert encrypted data to clear data.

⚠️

Caution   When an enable or a disable encryption operation is performed on a disk, you must execute the **copy running-config startup-config** command on all the switches. Failure to do so results in Persistent Storage Service (PSS) on the switch which is inconsistent with the state of the disk as recorded in the CKMC.

⚠️

Caution   When an enable operation is performed on a signature mode cluster for the first time, ensure that there is sufficient LUN size for a 64 MB SME disk reserved space at the end of the disk. Failure to do so can result in data loss.

Rekeying the SME Disk

Data in the disk under a disk group can be rekeyed on demand. For example, when the key security has been compromised.

The rekey operation at an individual disk level generates a new key for the disk and archives the old key. A data preparation operation is triggered to decrypt the data using old key, encrypt the data with the new key, and write it back to the disk.

The rekey operation can be performed on all subsets of disks in the disk group. KMC maintains a history of keys for all of the disks.

Detailed Steps

To rekey the SME disk, follow these steps:

	Command	Purpose
Step 1	switch# **config t**	Enters configuration mode.
Step 2	switch(config)# **sme cluster** *clustername*	Specifies the cluster and enters SME cluster configuration submode.
Step 3	switch(config-sme-cl)# **disk-group** *dg-name*	Creates a disk group.
Step 4	switch(config-sme-cl-dg)# **disk** *disk-name*	Specifies the disk name to be created.
Step 5	switch(config-sme-cl-dg-disk)# **rekey offline**	Performs offline rekey on the SME disk.

Monitoring Data Preparation

To monitor progress of the data preparation, enter the following command:

```
switch# show sme cluster c52 disk-group dg1 disk d1
Disk d1 is data-preparing (progress 0%, remaining time d:0 h:0 m:0 s:26)
 Description is LSI INF-01-00
 Vendor ID is LSI
 Product ID is INF-01-00
 Device ID is 600a0b80001f4ac4000032454a3a69ce
 Encryption is Enabled
 Key guid is 5b2a0bb9c3ea2428-961579da480ed56f
 Paths
  Host 21:00:00:1b:32:84:ca:4a Target 20:04:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5
  [f52]
   Is online (disk itl in IO reject state), configured, data prepare
```

Enabling Encryption on the SME Disk without Data Preparation

When SME encryption is enabled on a set of new disks that have no existing data, SME can be enabled without data preparation.

SME can be enabled only for a specified disk. Once SME is enabled, any host I/Os to the disks in the disk group are encrypted or decrypted.

Note Enabling SME at disk group level is not supported.

Note For signature mode clusters, enabling encryption is possible only if there is at least one I/O capable path available to the disk.

Note For asymmetric devices, an I/O capable path implies an Active Optimized (AO) path.

Caution All paths to the disk must be added to the SME prior to enabling encryption or else the data integrity is at risk.

Use the optional keyword **no-dataprepare** to enable encryption on the disk.

Caution Enabling encryption on a disk that has paths that are discovered but not configured results in host I/Os issued on these paths to fail. To allow host I/Os, these paths must be configured on the disk.

Caution Enabling encryption without data preparation operation must only be done on disks with no existing data or data loss can occur.

Detailed Steps

To perform encryption on a disk, follow these steps:

	Command	Purpose
Step 1	switch# **config t**	Enters configuration mode.
Step 2	switch(config)# **sme cluster** *clustername* switch(config-sme-cl)#	Specifies the cluster and enters SME cluster configuration submode.
Step 3	switch(config-sme-cl)# **disk-group** *dg-name* switch(config-sme-cl)#	Creates a disk group.
Step 4	switch(config-sme-cl-dg)# **disk** *disk-name*	Specifies the disk name to be created.
Step 5	switch(config-sme-cl-dg-disk)# **enable no-dataprepare**	Enables encryption on a disk.
Step 6	switch(config-sme-cl-dg-disk)# **no enable no-dataprepare**	Disables encryption on a disk.

Displaying the Configured Disk

To display the configured disk, enter this command:

```
switch# show sme cluster c52 disk-group dg1 disk d1
  Disk d1 is crypto
    Description is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0b80001f4ac4000032454a3a69ce
    Encryption is Enabled
    Key guid is 1f09c7425d706a2e-6e00de45a53aa68
    Paths
```

```
Host 21:00:00:1b:32:84:ca:4a Target 20:04:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5 [f52]
    Is online (SUCCESS), configured
```

Path States

The types of path states that are available as follows:

- Online—Path is discovered and is online.

  - Path that is configured, discovered, and available for host I/O access.

    ```
    Host 21:00:00:1b:32:84:ca:4a Target 20:04:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5
    [f52]
    Is online (success), configured
    ```

    Note   The above output is the expected state of a path that is configured correctly and successfully discovered.

  - Path that is configured, discovered, but not available for host I/O access.

    ```
    Host 21:00:00:1b:32:84:ca:4a Target 20:04:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5
    [f52]
    Is online (disk itl in IO reject state), configured
    ```

    Note   If the I/O reject state continues to persist even after a successful configuration and discovery, try to rediscover IT-nexus.

  - Path that is not configured is discovered, and is also available for host I/O access (encryption is not enabled on the disk).

    ```
    Host 21:00:00:1b:32:84:ca:4a Target 20:04:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5
    [f52]
    Is online (success), NOT configured
    ```

  - Path that is not configured, discovered, and not available for host I/O access (encryption is enabled on the disk or disk is suspended)

    ```
    Host 21:00:00:1b:32:84:ca:4a Target 20:04:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5
    [f52]
    Is online (disk itl in IO reject state), NOT configured
    ```

    Caution   All paths are expected to be online and available for host I/O access when a disk is completely and correctly configured.

- Offline—Configured path is not yet discovered.

  ```
  Host 21:01:00:1b:32:a4:ca:4a Target 20:05:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5
  [f52]
  Is offline (disk itl discovery pending), configured
  ```

- Failed—Path has been taken down to prevent host I/Os because the disk is in a failed state.

  ```
  Host 21:00:00:1b:32:84:ca:4a Target 20:04:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5
  [f52]
  Is failed (disk itl dp fail), configured
  ```

- Misconfigured path—Path being added to this disk belongs to another disk.

  - Misconfigured paths are marked as authentication failed and host I/Os are not allowed.

- To recover, these paths must be deleted first followed by rediscovery and proper reconfiguration.

```
Host 21:00:00:1b:32:84:ca:4a Target 20:05:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5
[f52]
          Is failed (disk itl auth fail vpd mismatch), configured
```

- Unconfigured path—Path is discovered but not yet added to this disk by the user. Shown as "Not configured" in output.

  - If configured disk does not have encryption enabled, these paths allow host I/Os.

  - If configured disk has encryption enabled, these paths do not allow host I/Os.

Modifying the SME Disk Key

This procedure allows the user to modify the crypto key of a disk manually.

✎
Note Manual modification of the crypto key of a disk is only allowed when the disk is in suspended state. In the suspended state, the host I/O access to a disk is not allowed.

Detailed Steps

To modify the SME disk key, follow these steps:

	Command	Purpose
Step 1	switch# **config t**	Enters configuration mode.
Step 2	switch(config)# **sme cluster** *clustername*	Specifies the cluster and enters SME cluster configuration submode.
Step 3	switch(config-sme-cl)# **disk-group** *dg-name*	Specifies a disk group.
Step 4	switch(config-sme-cl-dg)# **disk** *disk-name*	Specifies the disk name to be created.
Step 5	switch(config-sme-cl-dg-disk)# **suspend**	Suspends the SME disk.
Step 6	switch(config-sme-cl-dg-disk)# **modify-key guid** *guid*	Modifies the SME disk key. Provides the key GUID as input that needs to be the new active key of the disk.
Step 7	switch(config-sme-cl-dg-disk)# **no suspend**	Resumes the SME disk.

⚠
Caution This configuration is not expected to be provided directly by the administrator through the CLI. The DNCM-SAN Replication Key Context (DKR) takes advantage of the modify key feature to manage disk key replication relationships.

Displaying Suspended Disk

To display information on a suspended disk, enter this command:

```
switch(config-sme-cl-dg-disk)# show sme cluster c52 disk-group dg1 disk d1
  Disk d1 is suspend
    Description is LSI INF-01-00
    Vendor ID is LSI
```

```
Product ID is INF-01-00
Device ID is 600a0b80001f4ac4000032454a3a69ce
Encryption is Enabled
Key guid is 1f09c7425d706a2e-6e00de45a53aa68c
Paths
Host 21:00:00:1b:32:84:ca:4a Target 20:04:00:a0:b8:1f:4a:c6 Lun 0x0000 vsan 5 [f52]
    Is online (disk itl in IO reject state), configured
```

Recovering the SME Disk

In order to perform the recovery on a failed disk, the administrator needs to first restore the contents of the disk from the backup, which is a storage operation. The administrator then needs to update the state of the failed disk in SME configuration with the **recover** command.

Recovery can be done in two ways:

⚠

Caution   The SME **recover** CLI command is used only for recovery of encryption key and not for data.

Recovering SME Disk to Clear State

If the disk was recovered from a backup that contains clear data then the administrator need to recover the SME Disk to clear state.

✎

Note   For signature mode clusters, there must be at least one I/O-capable path for recovery to succeed. As part of the recovery, SME disk clears the signature from the signature portion of the disk.

Detailed Steps

To recover the SME disk to clear state, follow these steps:

	Command	Purpose
Step 1	switch# **config t**	Enters configuration mode.
Step 2	switch(config)# **sme cluster** *clustername* switch(config-sme-cl)#	Specifies the cluster and enters SME cluster configuration submode.
Step 3	switch(config-sme-cl)# **disk-group** *dg-name* switch(config-sme-cl)#	Specifies a disk group.
Step 4	switch(config-sme-cl-dg)# **disk** *disk-name*	Specifies the disk name to be created.
Step 5	switch(config-sme-cl-dg-disk)# **recover**	Resets the crypto state of the disk to a clear state. That is, no encryption is performed on the host I/Os issued on the disk.

Recovering SME Disk to Crypto State

If the disk was recovered from a backup that contains encrypted data then the administrator should recover the SME disk to crypto state.

> **Note** For signature mode clusters, there must be atleast one I/O- capable path for recover to succeed. As part of the recovery, SME disk writes the signature to the signature portion of the disk.

Detailed Steps

To recover the SME Disk to crypto state, follow these steps:

	Command	Purpose
Step 1	switch# **config t**	Enters configuration mode.
Step 2	switch(config)# **sme cluster** *clustername* switch(config-sme-cl)#	Specifies the cluster and enters SME cluster configuration submode.
Step 3	switch(config-sme-cl)# **disk-group** *dg-name* switch(config-sme-cl)#	Specifies a disk group.
Step 4	switch(config-sme-cl-dg)# **disk** *disk-name*	Specifies the disk name to be created.
Step 5	switch(config-sme-cl-dg-disk)# **recover guid** *guid*	Sets the encryption status of the disk to be a crypto disk and use the key specified by the GUI as encryption key for the disk.

> **Caution** The **Recover** command does not recover the contents of the disk. Its recovers the crypto-state of the disk based on the data recovered into the disk. The data on the disk must first be restored before using the **recover** command.

Recovering SME Disk from KMC

> **Note** This is applicable only for signature mode clusters.

To recover SME Disk from KMC, SME Disk looks for an active key in KMC. After the active key is found, the active key is used to generate the signature written on the disk as the disk recovers to a crypto state.

> **Note** The encryption key is the active key recorded in KMC.

> **Note** If the KMC does not have an active key for the disk, then the disk recovers to a clear state and the signature in the reserved area is cleared.

To recover the SME Disk from KMC, follow these steps:

	Command	Purpose
Step 1	switch# **config t**	Enters configuration mode.
Step 2	switch(config)# **sme cluster** *clustername* switch(config-sme-cl)#	Specifies the cluster and enters SME cluster configuration submode.

	Command	Purpose
Step 3	`switch(config-sme-cl)# disk-group dg-name` `switch(config-sme-cl)#`	Specifies a disk group.
Step 4	`switch(config-sme-cl-dg)# disk disk-name`	Specifies the disk name to be created.
Step 5	`switch(config-sme-cl-dg-disk)# recover from` `-kmc`	Sets the encryption status of the disk to be a crypto disk.

Recovering SME Disk from Signature on Disk

Note This option is available only for signature mode clusters.

SME Disk gets the signature from the reserved area of the disk. If the signature is valid, SME Disk searches in the KMC using the GUID from the signature. If the KMC search succeeds, the disk recovers to a crypto state.

Note When the KMC search fails, the recover operation fails and the disk remains in failed state.

Note When there are no signatures found on the disk, the disk recovers to a clear state.

To recover SME Disk from the signature mode cluster, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# sme cluster clustername` `switch(config-sme-cl)#`	Specifies the cluster and enters SME cluster configuration submode.
Step 3	`switch(config-sme-cl)# disk-group dg-name` `switch(config-sme-cl)#`	Specifies a disk group.
Step 4	`switch(config-sme-cl-dg)# disk disk-name`	Specifies the disk name to be created.
Step 5	`switch(config-sme-cl-dg-disk)# recover from` `-metadata`	Sets the encryption status of the disk to be a crypto disk.

Configuring SME Disk Management Using the GUI

This section includes the following topics:

- Configuring Disk Groups, page 6-30
- Configuring Disks, page 6-31
- Configuring Disk Paths, page 6-33
- Suspending and Resuming the Configured Disk, page 6-35
- Managing Disk Encryption on SME Disks, page 6-36
- Recovering SME Disks, page 6-41

Configuring Disk Groups

This section includes the following topics:

Creating Disk Groups

Detailed Steps

To create a disk group, follow these steps:

Step 1   Open DCNM-SAN Web Client. Log in with the user name and password.

For login information, refer to the *Cisco DCNM-SAN Fundamentals Guide.*

Step 2   In the DCNM-SAN Web Client, click the **SME** tab.

Step 3   Create a disk-capable cluster. For more information, see "Creating a SME Cluster Using the SME Wizard" section on page 4-10.

Step 4   Select **Disk Groups**. Click **Add**.

The disks in an SME cluster can be grouped functionally into disk groups.

✎

Note   The Disk Group tab is displayed only when a disk-capable cluster is created.

Step 5   Enter a name for the disk group. Click **Next**.

✎

Note   The disk group wizard allows you to create an empty disk group when you click **Finish.** If you click **Finish**, an empty disk group is created that can be used for pre-provisioning. The series of filters allows you to add the disks to a disk group from the **Fabric > VSAN > Zones > Select Disks** menu option.

Step 6   Select specific VSANs for the disk group. Click **Next**.

VSANs are displayed for single as well as dual fabrics. You can select the VSANs for each fabric that you would like to discover the path for.

Step 7   Select specific zones for the disk group. Click **Next**.

Step 8   Select the hosts for the disk group. You can select single or multiple hosts. Click **Next**.

Step 9   Select the disk targets for the disk group. You can select single or multiple disk targets. Click **Next**.

Step 10   Select the disks to create the disk group. Click **Next**.

⚠

Caution   Failure to add all of the paths from the host to storage can result in data loss or data corruption.

The select disk path screen shows the Disk Name that you can modify, Vendor ID (VID), Product ID (PID), Device ID (DID), and number of paths for the disk. Along with this information when you click on the zoom icon, you can see the Initiator PWWN, Target PWWN, and the number of LUNs for the corresponding disk.

Step 11   Verify the information shown on the confirmation screen. Click **Confirm** to save and activate the changes.

Step 12   View the disk group that is successfully added to a cluster.

Deleting Disk Groups

Prerequisites

Before deleting a disk group, ensure that the configured disks are deleted from the disk groups.

Detailed Steps

To delete a disk group, follow these steps:

Step 1   Select **Disk Groups** to display the disk groups that are part of the cluster.

Step 2   Select a disk group and click **Remove**.

Step 3   Click **OK** to delete the disk group.

Step 4   View the notification that the disk group has been removed.

Configuring Disks

This section includes the following topics:

Adding Disks

> ✎
>
> **Note**   When you add disks to a signature mode cluster and if the volume contains data, you have to resize the disk to reserve at least 64MB of space for Cisco SME signature information at the end of the volume.

Detailed Steps

To add disks to an existing disk group, follow these steps:

Step 1   Select the configured **Disk Group**.

Step 2   Select the **Disks** under the configured Disk Group and click **Add**.

Step 3   Select the VSANs that you would like to discover paths from. Click **Next**.

Step 4   Select specific zones for the disk. Click **Next**.

Step 5   Select the hosts for the disk. You can select single or multiple hosts. Click **Next**.

Step 6   Select the disk targets. You can select single or multiple targets. Click **Next**.

Step 7   Select the paths that SME would use for encrypted data between the host and the disk. Click **Next**.

Step 8   Click **Confirm** to add the new disk to the disk group.

Step 9   View the disks successfully added to the disk group.

Deleting Disks

Detailed Steps

To delete a disk from an existing disk group, follow these steps:

Step 1   Select the disk from a disk group that you want to remove.

Step 2   Click **Remove**.

Step 3   Click **OK** to delete the disk.

Step 4   View the notification that the disk has been removed.

> **Note**   If there are any errors in performing the required action, the error is shown in red text with a red border so that it is highlighted.

Configuring Signature Mode

> **Note**   Converting a SME Disk cluster from a non-signature mode to signature mode will result in writing signatures to all the configured crypto disks. Once the conversion is complete, verify if all the crypto disks and their paths are in online state and verify the signature of the disks.

To convert a cluster to signature mode, follow these steps:

Step 1   In DCNM-SAN Web Client, click the **SME** tab.

Step 2   Select **Clusters** in the navigation pane. Click and expand on the desired destination clusters.

The Cluster Details screen is displayed.

Step 3   Click **Convert to Signature Mode**.

> **Note**   You will not see this option for disks that are already in signature mode.

The Signature Mode Conversion screen is displayed.

Step 4   Click **Next**.

The Convert Cluster screen is displayed.

Once the conversion is complete, ensure there are no failed disks and verify the signature for crypto disks to ensure the signature is correct. For failed disks, see Recovering SME Disks, page 6-41.

Converting Disks to Signature Mode

To convert a cluster to signature mode, follow these steps:

Step 1   In DCNM-SAN Web Client, click the **SME** tab.

Step 2   Select **Clusters** in the navigation pane. Click and expand on the desired destination clusters.

The Cluster Details screen is displayed.

Step 3   Click **Convert Disks to Signature Mode**.

The Signature Mode Conversion screen is displayed.

Step 4   Click **Next**.

The Convert Cluster screen is displayed.

Verifying Signatures for Disks

To verify signatures on disks, follow these steps:

Step 1   In the DCNM-SAN web client, click the **SME** tab.

Step 2   Under **Disk Groups**, select the disk for signature verification.

The **Disk Details** screen is displayed.

Step 3   Under **Disk Signature**, click **Verify Signature**.

The signature is verifies and the signature verification is successful message is displayed.

Configuring Disk Paths

This section includes the following topics:

- Configuring and Discovering Disk Paths, page 6-34
- Adding Discovered Path, page 6-34
- Removing Disk Paths, page 6-34

Configuring and Discovering Disk Paths

Launch the Add Disk Path Wizard to add the disk paths to the disk by clicking **Configure/Discover**.

Detailed Steps

To configure and discover a disk path to a disk, follow these steps:

Step 1   Select the disk to which the new disk path has to be added. In the Discovered Paths section, click **Configure/Discover** to configure and discover the disk path corresponding to the disk path.

Step 2   Select the VSANs that you want to discover paths from. Click **Next**.

Step 3   Select specific zones for the disk. Click **Next**.

Step 4   Select the disk path that you want to add to the disk. Click **Next**.

Step 5   Click **Confirm** to add the disk path.

Step 6   Verify that the selected disk path is successfully added to the disk. The disk paths are shown in the Configure Paths area under the disk section.

Adding Discovered Path

During the disk discovery, the disk paths that are corresponding to the disk also get discovered. The corresponding disk paths for a disk get discovered and are displayed in the Discovered Paths area under the disk section.

⚠

Caution   All the paths for a disk must be configured. Writing to an encrypted disk using an unconfigured path will results in corruption or loss of data.

Detailed Steps

Step 1   To add the discovered path to a disk, select the discovered path. Click **Configure/Discover**.

Step 2   Click **OK** to continue. This configures and adds the selected disk displayed under the Discovered Paths area to the Configured Paths area.

Step 3   Verify that the selected Discovered Path is successfully added to the Configured Paths under the disk section.

Removing Disk Paths

Detailed Steps

To delete a disk path from a disk, follow these steps:

Step 1   Click a disk name to display the disk details and configured paths.

Step 2   Select a disk path and click **Remove**.

Step 3   Click **OK** to delete the disk path.

Step 4   Verify that the selected disk path is removed successfully.

Suspending and Resuming the Configured Disk

Restore operation mainly requires suspend and resume operations.

These operations are used in Disk Key Replication. There are some limitations for Disk Key Replication. For more information see, .

⚠️

Caution   Suspending a disk results in SME rejecting all the I/Os issued by the host. If you suspend a disk that is being actively used by a host, application I/O failures can occur. We recommend that the applications using this disk be quiesced, or failover to an alternate disk before suspending the disk.

Suspending the Configured Disk

✎

Note   You can suspend the disk that is in either crypto state or clear state.

To suspend an encrypted disk, follow these steps:

Step 1   Select the required disks from the Disk group.

Step 2   Click **Suspend/Resume**. The drop-down list displays Suspend Disks and Resume Disks.

Step 3   Select **Suspend Disks**. Click **OK** to suspend the selected disks.

The Disk suspended successfully message is displayed in the top of the screen.

Resuming the Configured Disk

✎

Note   For resuming, the disk should be in the suspended state.

To resume the suspended disk, follow these steps:

Step 1   Select the required Disks from the Disk group.

Step 2   Click **Suspend/Resume**. The drop-down list displays Suspend Disks and Resume Disks.

Step 3   Select **Resume Disks**. Click **OK** to resume the selected disks.

The Disk resumed successfully message is displayed in the top of the screen.

Managing Disk Encryption on SME Disks

Managing data encryption on SME disks contains the following topics:

- Performing Data Preparation on the Disk for Converting Clear Data to Encrypted Data, page 6-36
- Performing Data Preparation on the Disk for Converting Encrypted Data to Clear Data, page 6-40
- Rekeying on an Encrypted Disk, page 6-41
- Recovering SME Disks, page 6-41
- Performing Disk Encryption to Convert the Disk Status from Clear to Crypto, page 6-43
- Performing Disk Encryption to Convert the Disk Status from Crypto to Clear, page 6-45
- Exporting and Importing Keys, page 6-45

⚠
Caution   When the enable or disable operation is performed on the disk in signature mode, ensure that there is a minimum of one I/O path to the disk. If there are no I/O paths, enable fails. During disable, if there are no I/O paths, the media continues using stored signatures which results in failure during discovery.

⚠
Caution   When the enable or disable operation is performed on a disk, you must save running-config to startup-config on all the switches. Failure to do so results in Persistent Storage Service (PSS) on the switch inconsistent with the state of the disk as recorded in the CKMC. During the disable operation, if there are no I/O paths, the key for the disk in the KMC is archived and the disk state is set to clear. However, the signature on the media is not cleared by SME since there is no I/O access to the disk. This results in the disk going to a failed state because of the inconsistency in the state of the disk between KMC and the information in the disk signature.

Performing Data Preparation on the Disk for Converting Clear Data to Encrypted Data

⚠
Caution   During the data preparation process, we do not recommend manually entering the GUID of the key. We recommended that SME generates the key automatically.

You can convert clear data to encrypted data by performing offline data preparation on a clear disk using the following options:

- Using Select New Key, page 6-37
- Using Select Key, page 6-38
- Using Input GUID, page 6-39

✎
Note   Manage Encryption page view is different for the different operations.

If you click on the Manage Encryption button without selecting any disk, only the Import Operation button is enabled and only the Import option can be performed.

However, if you click on the Manage Encryption button after selecting multiple disks that are in the same

state (clear or crypto or suspend), you can perform multiple disk operations such as Import, Export, and so on.

If you click on the Manage Encryption button after selecting multiple disks that are in different states (clear, crypto, and suspend), you only can perform Import and Export operations.

Using Select New Key

You can perform data preparation by selecting the New Key button. This operation converts clear data on a disk to encrypted data by generating a new disk key.

Detailed Steps

To perform data preparation on a clear disk using the New Key option, follow these steps:

Step 1   Select the disk and click **Manage Disk Encryption**.

Step 2   In the Manage Disk Encryption: Settings window, click **Change disk encryption status**.

The Current Status will be Clear. Select the required action **Encrypt** from the **Action** drop-down list.

For data preparation, ensure that the **Prepare Data** check box is checked.

Click **New Key** and click **Next.**
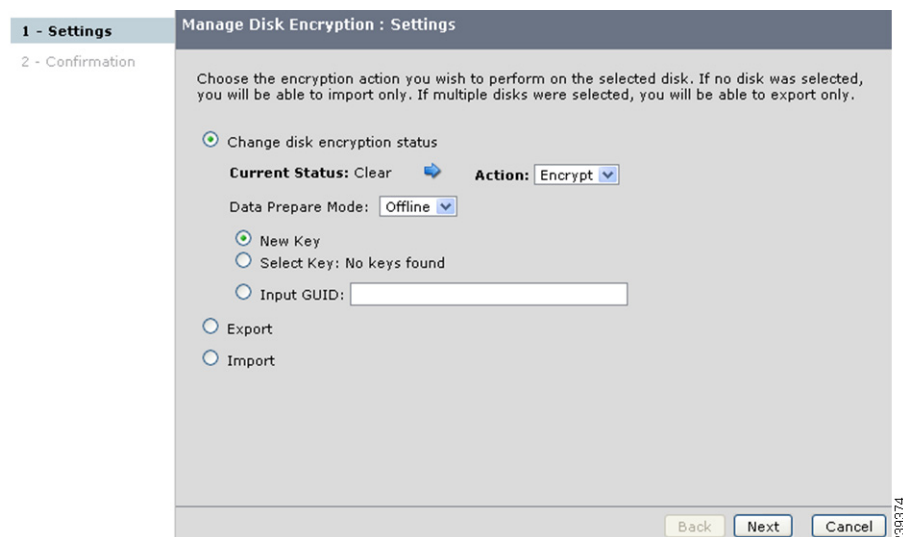
Step 3   Click **Confirm** in the next screen.

The percentage of the disk preparation is displayed. Wait until the disk status changes to crypto.

When the data preparation is completed successfully, the disk status turns to Crypto.

> **Note**   There is no automatic refresh to display the status. The disk preparation status can be monitored only by refreshing the page manually.

> **Caution**   Aborting the data preparation results in losing the contents of the disk.

> **Note**   You can choose to abort the data preparation process by clicking the **Abort** button. The Abort button is available under **Disk Level** when the data preparation is happening.
>
> We do not recommend aborting the data preparation as it will result in losing the contents. However, when you abort the data preparation operation, you need to recover the disk data from the backup. The recover state also should be consistent with the data in the backup.

Using Select Key

You can perform data preparation by using the Select Key button. This operation converts clear data on a disk to encrypted data by using an existing disk key.

Detailed Steps

To perform data preparation on a clear disk using an existing key option, follow these steps:

Step 1   Select the disk and click **Manage Disk Encryption**.

    a.   In the Manage Disk Encryption: Settings screen, click **Change disk encryption status**.

    b.   The Current Status will be Clear. Select the required action **Encrypt** from the **Action** drop-down list.

    c.   For data preparation, ensure that the **Prepare Data** check box is checked.

    d.   Click **Select Key** and select a key from the drop-down list.

    e.   Click **Next.**

Step 2   Click **Confirm** in the next screen.

The percentage of the disk preparation is displayed. Wait until the status shows 100%.

When the data preparation is completed successfully, the disk status turns to Crypto.

Using Input GUID

You can perform data preparation by using the Input GUID option. This operation converts clear data on a disk to encrypted data by generating a new disk key.

To perform data preparation on a clear disk by providing the GUID, follow these steps:

Step 1   Select the disk and click **Manage Disk Encryption**.

a.   In the Manage Disk Encryption: Settings screen, click **Change disk encryption status**.

b.   The Current Status will be Clear. Select the required action **Encrypt** from the **Action** drop-down list.

c.   For data preparation, ensure that the **Prepare Data** check box is checked.

d.   Click the **Input GUID** option and provide the GUID of the key that is in the KMC database.

e.   Click **Next.**

Step 2   Click **Confirm** in the next screen.
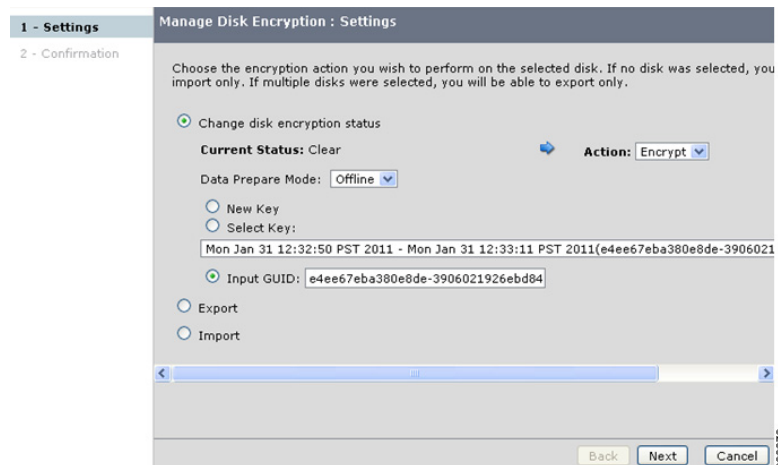
The percentage of completion of disk preparation is displayed. Wait until the status shows 100% and the disk state changes to crypto.

When the data preparation is completed successfully, the disk status turns to Crypto.

Performing Data Preparation on the Disk for Converting Encrypted Data to Clear Data

You can convert encrypted data to clear data on a disk by performing data preparation on an encrypted disk.

Detailed Steps

To convert encrypted data on a disk to clear state, follow these steps:

Step 1   Select the disk and click **Manage Disk Encryption**.

    a.   In the Manage Disk Encryption: Settings screen, click **Change disk encryption status**.

    b.   The Current Status is Encrypted. Select the required action **Clear** from the **Action** drop-down list.

    c.   For data preparation, ensure that the **Prepare Data** check box is checked.

    d.   Click **Next**.

Step 2   Click **Confirm** in the next screen.

Step 3   The percentage of the disk preparation is displayed. Wait until the status shows 100% and the disk state changes to clear.

Step 4   When the data preparation is completed successfully, the disk status turns to Clear.

Rekeying on an Encrypted Disk

Detailed Steps

To rekey an encrypted disk, follow these steps:

Step 1   Select the disk and click **Manage Disk Encryption**.

    a.   In the Manage Disk Encryption: Settings screen, click **Change disk encryption status**.

    b.   The Current Status is Encrypted. Select the required action **Rekey** from the **Action** drop-down list.
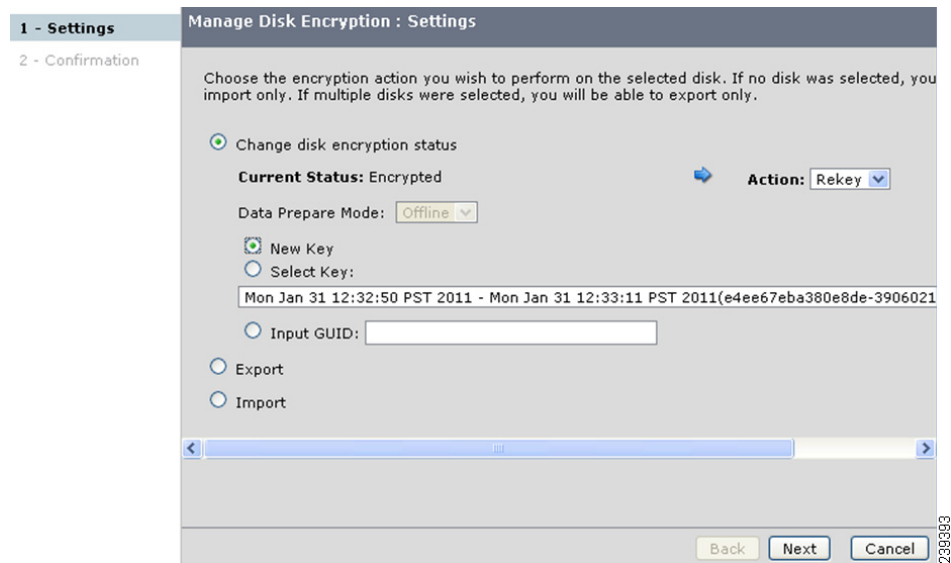
    c.   Click **Next**.

Step 2   Click **Confirm** in the next screen.

The percentage of the disk preparation is displayed. Wait until the disk status changes to crypto.

When the data preparation is completed successfully, the disk status turns to Crypto.

Recovering SME Disks

During data preparation if there are any failures, the data preparation process is aborted. If a failure occurs, the disk is put in a failed state and all host I/Os to the disk fails. This section describes the procedure to follow to recover the disk back to the state before the data preparation.

In signature mode, SME verifiesthe signature on the disk by comparing the disk information in the KMC. Any mismatch between the information in KMC and the signature results in disk failure.

⚠️

Caution   The **Recover** command does not recover the contents of the disk. This command recovers the crypto-state of the disk based on the data recovered into the disk. The data on the disk must first be restored before using the **recover** command.

✎

Note   Restoration of the contents of the disk is done by a backend storage operation that copies the backup data from a mirror or snapshot in the disk array. This restoration does not require the failed disk to be accessible from host. This is important because SME does not allow any host access to the failed disk.

Recovering a Disk to Clear Status

Detailed Steps

To recover a failure disk to a clear disk, follow these steps:

Step 1   Click the disk that is in failed (Failure) state.

Step 2   Click the **Recover** option that is available in the **Disk Details** area.

Step 3   Select **Recover to clear snapshot** and click **Next**.

Step 4   Click **Confirm** to perform the recover operation on the Recover Disk : Confirmation screen.

The disk recovered successful message is displayed in the top of the screen showing the disk status as Clear.

Recovering a Disk to Encrypted Status

Detailed Steps

To recover a failure disk to a crypto disk, follow these steps:

Step 1   Click the disk that is in failed state.

Step 2   Click the **Recover** option that is available in the **Disk Details** area.

Step 3   Select **Recover to crypto snapshot** by providing the key GUID and click **Next**.

Step 4   Click **Confirm** to perform the recover operation on the Recover Disk: Confirmation screen.

The Disk recovered successful message is displayed in the top of the screen showing the disk status as **Crypto**.

Recovering a Disk Using Metadata Signature

✎

Note   You can only recover signature disks.

Detailed Steps

To recover the failure disk using the metadata, follow these steps:

Step 1   Click the disk that is in failed state.

Step 2   Click the **Recover** option that is available in the **Disk Details** area.

Step 3   Select **Recover from metadata** by providing the key GUID and click **Next**.

Step 4   Click **Confirm** to perform the recover operation on the Recover Disk: Confirmation screen.

The Disk recovered successful message is displayed in the top of the screen.

Recovering a Disk from Key Manager

Step 1   Click the disk that is in failed state.

Step 2   Click the **Recover** option that is available in the **Disk Details** area.

Step 3   Select **Recover from key manager** by providing the key GUID and click **Next**.

Step 4   Click **Confirm** to perform the recover operation on the Recover Disk: Confirmation screen.

The Disk recovered successful message is displayed in the top of the screen.

Performing Disk Encryption to Convert the Disk Status from Clear to Crypto

You can perform disk encryption operation to convert the disk status from clear to crypto using the following options:

- Using Select New Key, page 6-43
- Using Input GUID, page 6-44
- Using Input GUID, page 6-44

Using Select New Key

You can perform disk encryption by selecting the New Key button. This operation converts the disk status from clear to crypto by using new disk key.

Detailed Steps

To perform disk encryption using the New Key option, follow these steps:

Step 1   Select the disk and click **Manage Disk Encryption**.

    a.   In the Manage Disk Encryption: Settings screen, click **Change disk encryption status**.

    b.   The Current Status will be Clear. Select the required action **Encrypt** from the **Action** drop-down list.

    c.   For disk encryption, ensure that the **Prepare Data** check box is not checked.

     d. Select **New Key** and click **Next.**

Step 2   Click **Confirm** in the next screen.

     The percentage of the disk encryption is displayed. Wait until the status shows 100%.

     When the disk encryption is completed successfully, the disk status turns to Crypto.

Using Select Key

You can perform disk encryption by using the Select Key option. This operation converts the disk status from clear to crypto by using an existing disk key.

Detailed Steps

To perform disk encryption using an existing key option, follow these steps:

Step 1   Select the disk and click **Manage Disk Encryption**.

     a. In the Manage Disk Encryption: Settings screen, click **Change disk encryption status**.

     b. The Current Status will be Clear. Select the required action **Encrypt** from the **Action** drop-down list.

     c. For disk encryption, ensure that the **Prepare Data** check box is not checked.

     d. Click **Select Key** and select a key from the drop-down list. Click **Next.**

Step 2   Click **Confirm** in the next screen.

     The percentage of the disk preparation is displayed. Wait until the status shows 100%.

     When the disk encryption is completed successfully, the disk status turns to Crypto.

Using Input GUID

You can perform disk encryption by using the Input GUID option. This operation converts the disk status from clear to crypto by using Input GUID.

Detailed Steps

To perform disk encryption using the Input GUID, follow these steps:

Step 1   Select the disk and click **Manage Disk Encryption**.

     a. In the Manage Disk Encryption: Settings screen, click **Change disk encryption status**.

     b. The Current Status will be Clear. Select the required action **Encrypt** from the **Action** drop-down list.

     c. For disk encryption, ensure that the **Prepare Data** check box is not checked.

     d. Select the **Input GUID** option and provide the GUID of the key that is in the KMC database. Click **Next.**

Step 2   Click **Confirm** in the next screen.

The percentage of the disk preparation is displayed. Wait until the status shows 100%.

When the disk encryption is completed successfully, the disk status turns to Crypto.

Performing Disk Encryption to Convert the Disk Status from Crypto to Clear

Detailed Steps

To perform disk encryption operation for converting the disk status from crypto to clear, follow these steps:

Step 1   Select the disk and click **Manage Disk Encryption**.

   a.   In the Manage Disk Encryption: Settings screen, click **Change disk encryption status**.

   b.   The Current Status is Encrypted. Select the required action **Clear** from the **Action** drop-down list.

   c.   For disk encryption, ensure that the **Prepare Data** check box is not checked.

   d.   Click **Next**.

Step 2   Click **Confirm** in the next screen.

The percentage of the disk preparation is displayed. Wait until the status shows 100%.

When the disk encryption is completed successfully, the disk status turns to Clear.

Exporting and Importing Keys

You can explicitly export the keys that are generated during the key generation process or encryption process, and save the keys in a password-protected file.

Note   The disk keys are not protected by the master key. However, they are protected by the password generated key.

This section includes these exporting and importing tasks:

Exporting Keys for Single Disk

You can export keys for a single disk by selecting a particular disk.

Detailed Steps

To export keys for a single disk, follow these steps:

Step 1	Select a single disk from a disk group and click **Manage Encryption**.
Step 2	In the Manage Disk Encryption: Settings screen, click **Export**.
	a. Provide data for Password and Confirm Password in the appropriate fields.
	b. Click **Next**.
Step 3	The keys for the selected disk are exported to a file. Click **Download** in the next screen to begin the download.
Step 4	When the download activity is completed, click **Close** to close the wizard.

Exporting Keys for Multiple Disks

You can export keys for multiple disks by selecting multiple disks.

Detailed Steps

To export keys for multiple disks, follow these steps:

Step 1	Select multiple disks from a disk group and click **Manage Encryption**.
Step 2	In the Manage Disk Encryption: Settings screen, click **Export**.
	a. Provide data for Password and Confirm Password in the appropriate fields.
	b. Click **Next**.
Step 3	The keys for the selected disks are exported to a file. Click **Download** in the next screen to begin the download.
Step 4	When the download activity is completed, click **Close** to close the wizard.

Importing Keys to a Single Disk or to a Disk Set

You can import keys to a single disk or import the disk keys to a defined disk set.

Detailed Steps

To import keys to a single disk or to a defined disk set, follow these steps:

Step 1	Do not select any disk. Click **Manage Encryption**.
Step 2	In the Manage Disk Encryption: Settings screen, click **Import**.
	a. Browse to the single or multiple keys file from where the key or keys file was exported earlier. Provide the password for the corresponding file in the field provided to perform import operation.
	b. Click **Next**.

Step 3   Provide the disk name or the disk set name on to which the key or the keys file should be imported to. Click **Next** to begin the import.

Step 4   Click **Confirm** to close the wizard.

The Import Successful message is displayed in the top of the screen.

Restoring an Encrypted Disk from a Deactivated Key

You can restore an encrypted disk from the deactivated key as follows:

- Restoring a Deactivated Key Using the Select Key Option, page 6-47
- Restoring a Deactivated Key Using the Input GUID Option, page 6-48

Restoring a Deactivated Key Using the Select Key Option

Detailed Steps

To restore an encrypted disk from a deactivated key using the Select Key option, follow these steps:

Step 1   Select a suspended disk from a disk group. Click **Manage Encryption**.

Step 2   In the Manage Disk Encryption: Settings screen, click **Change disk encryption status**.

   a.   The Current Status is Suspended. Select **Restore from deactivated key** from the **Action** drop-down list.

   b.   Click **Select Key**. Select the required key from the list of keys.

   c.   Click **Next**. The Encryption Action is displayed as Restore from deactivated key.

Step 3   Click **Confirm** to close the wizard.

The disk modified successful message is displayed.

Step 4 To resume disks, select **Resume Disks** from the **Suspend/Resume** drop-down list option.

Step 5 Click **OK** to resume the selected disks.

Step 6 The status of the selected disk is resumed back to the status before Suspend.

Restoring a Deactivated Key Using the Input GUID Option

Detailed Steps

To restore an encrypted disk from a deactivated key using the Input GUID, follow these steps:

Step 1 Select a suspended disk. Click **Manage Encryption**.

Step 2 In the Manage Disk Encryption: Settings screen, click **Change disk encryption status**.

    a. The Current Status is Suspended. Select the required action **Restore from deactivated key** from the **Action** drop-down list.

    b. Click **Input GUID**. Provide the key GUID.

    c. Click **Next**. The Encryption Action is displayed as Restore from deactivated key.

Step 3 Click **Confirm** to close the wizard.

The Resume Successful message is displayed in the top of the screen.

Configuring DKR

⚠️
Caution All SME operations for disks involved in DKR relationships (either active or disabled state) must be done through DCNM-SAN. Operation through CLI is not supported and data loss can occur.

This section includes the following topics:

Creating Disk Key Replication

✎
Note   Only the disk keys using DKR are replicated. Data is replicated by third- party software.

Detailed Steps

To create disk key replication, follow these steps:

Step 1   In DCNM-SAN Web Client, click the **SME** tab.

Step 2   Select **Clusters** in the navigation pane. Click and expand on the desired source and destination clusters.

Figure 6-3   Clusters
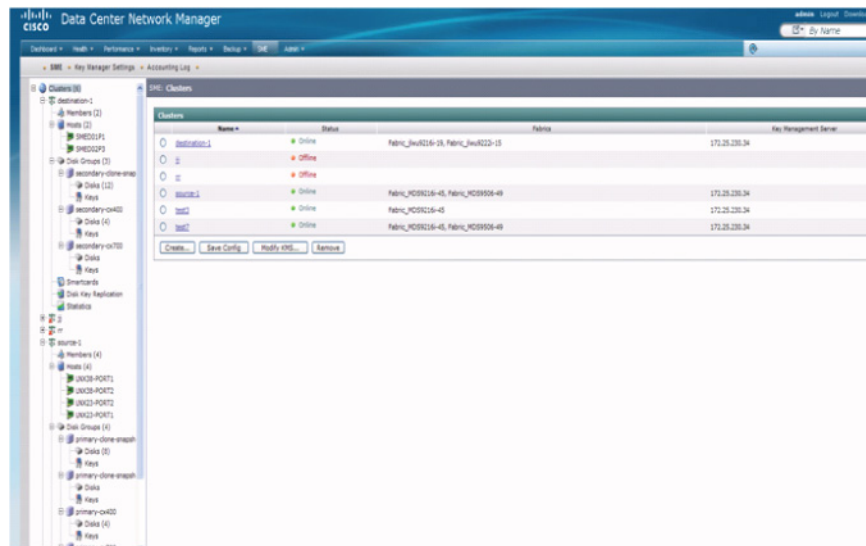
Step 3   Click **Disk Replication** in the information pane. The create wizard is displayed.

Figure 6-4   Disk Replication Creation
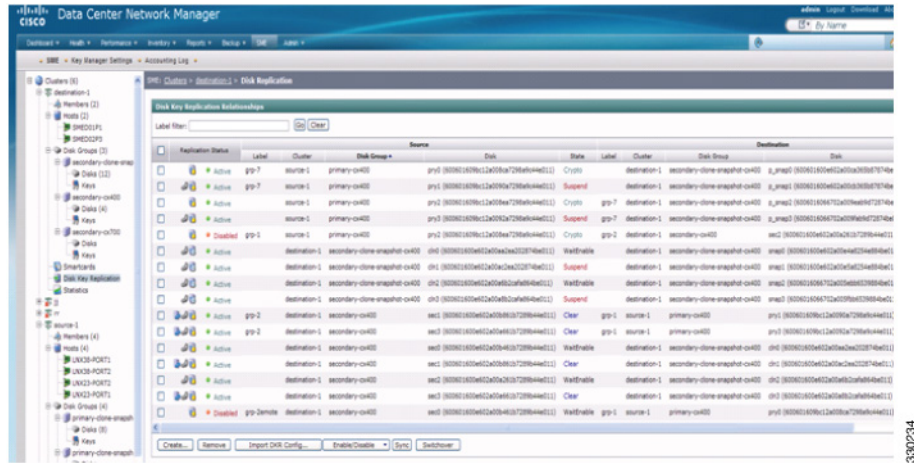
Step 4   Click **Create**. The Disk Key Relationship screen is displayed.

Step 5   Select the type of replication relationship **Mirror** or **Snapshot**. Select the source and the destination disk. Click **Next**.

Figure 6-5   DKR Disk Selection

![Create Disk Key Replication Relationship: Select Disks screen]
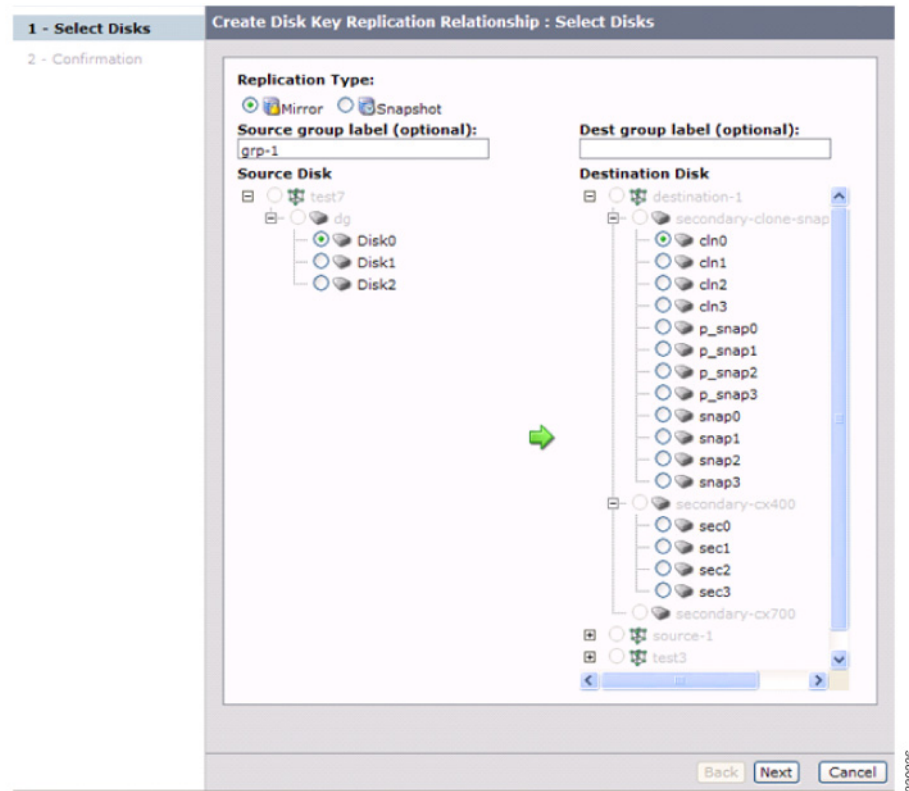
> **Note**   The source disks and the destination disks are displayed based on the cluster that is selected.

Step 6   Click **Next**. The Confirmation screen is displayed.

Figure 6-6   *DKR Confirmation*
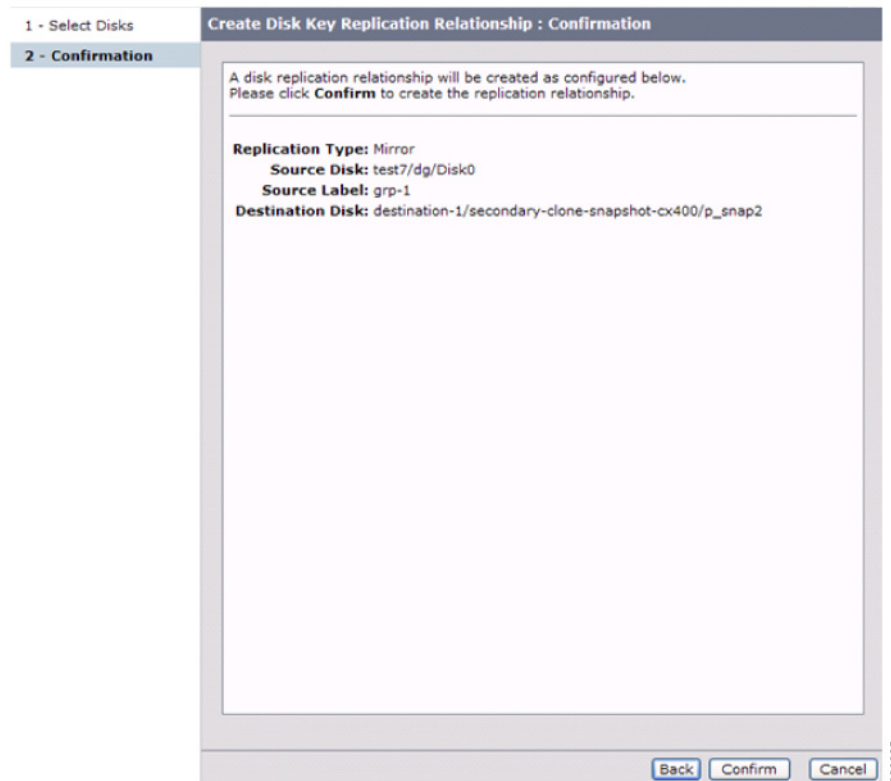
The disk replication successful message is displayed showing the Replication Status as Disabled.

Note   Whenever a disk key replication is created, by default the disk key replication status is always Disabled.

All the relationships are stored in the KMC database. If the KMC database is down, you will not be able to see any relationships.

Enabling or Disabling Disk Key Replication

Detailed Steps

To enable disk key replication, follow these steps:

Step 1   Select the disks for which you need to enable the relationship. Click **Enable/Disable**.

Step 2   Select **Enable Relationship** option from the drop-down list box.

Step 3   You are prompted with a dialog box asking if you are sure and want to do this. Click **OK** to continue.

The disk replication enable successful message is displayed at the top of the screen. The enabled disk's Replication Status is displayed as Active.

Step 4 Perform disk encryption on the replicated disk.

✎

Note The source and destination disk can either be in the same cluster or be in a different cluster; however, they should be using the same KMC.

A source disk can be a source disk for multiple relationships. However, the destination disk can be the destination disk for only one relationship.

A source disk must be discovered and configured in the source cluster before an DKR relationship is established.

✎

Note If the source disk or the destination disk is not in either CLEAR, CRYPTO, or FAILED states, DCNM-SAN displays an error and does not process the entry. The state of the source disk or the destination disk must be obtained from the switch.

To disable disk key replications, follow these steps:

Step 1 Select the disks for which you need to disable the relationship. Click **Enable/Disable**.

Step 2 Select **Disable Relationship**.

Step 3 The prompt appears asking you are sure you want to do this. Click **OK** to continue.

The disk replication disable successful message is displayed at the top of the screen. The disabled disk's Replication Status is displayed as Disabled.

Removing or Deleting Replication Relationships

Detailed Steps

To remove or delete replication relationships, follow these steps:

Step 1 Select the disks for which you need to remove or delete the relationship. Click **Remove**.

Step 2 You are prompted a question if you are sure to remove replication relationships. Click **OK** to continue.

The replication relationships are removed or deleted.

Importing DKR Configurations

To import an DKR relationship configuration file, follow these steps:

Step 1 Click **Import DKR Config..**.The Import DKR config file: Provide file screen is displayed. Click **Browse** and select the required DKR Config File.

Step 2 Click **Next**. The confirmation screen is displayed asking you to confirm to begin import of the DKR Config file. Click **Confirm** to continue.

The import file operation is processed and the DKR Config file is imported and successful import message is displayed.

Performing the Switchover Operation

Detailed Steps

You can perform a switchover operation to swap the source and destination in a disk key replication relationship. A switchover can only be performed on a DKR relationship in a Disabled state. To perform the switchover operation, follow these steps:

Step 1 Select the disabled relationships on which you want to perform the switchover operation. Click **Switchover**.

Step 2 You are prompted a question if you are sure you want to do this. Click **OK** to continue.

The relationships will have their source and destinations swapped. The relationships will still be in a disabled state.

Labels & Filtering

Labels can be associated with both sides of a disk key replication relationship. The DKR view provides the ability to filter based on these labels.

Performing the Sync Operation

You can perform the Sync operation on multiple relationships. To do this, follow these steps:

Step 1 Select the relationships on which you want to perform the Sync operation. Click **Sync**.

Step 2 You are prompted a question if you are sure you want to do this. Click **OK** to continue.

The relationships are replicated and are made similar and in sync with each other.

Configuring Key Management Operations

This section includes the following topics:

- Replacing Smart Cards, page 6-55
- Configuring Master Key Rekey, page 6-56

Replacing Smart Cards

This section describes how to replace smart cards for clusters.

Detailed Steps

To replace a smart card (Advanced security mode), follow these steps:

Step 1   Under **Data Center Network Manager**, click **SME**. The cluster list is displayed.

Step 2   Click **Smartcards**. The Recovery shares details along with the associated list of smart cards is displayed.

Step 3   Select the smart card that you would want to replace and click **Replace Smartcard and Rekey Master Key**.

The smart card replacement wizard is displayed.

Step 4   Insert the new smart card. Click **Next**.

The SME Recovery Officer who owns the replacement smart card is prompted to log in and to insert the smart card to download the master key.

Step 5   Enter the switch login information and the smart card PIN and label. Click **Next**.

Each member of the Cisco Recovery Officer quorum is requested to log in and present their smart card to authorize and authenticate the operation.

Step 6   Insert one of the smart cards that stores the master key. Click **Next**.

Step 7   Enter the switch login information and the smart card PIN and Label. Click **Next**. Do this for each of the smart cards.

Step 8   Insert the smart cards belonging to each recovery officer in any order.

To store the new master keyshares, follow these steps:

a.   Enter the switch login information, the PIN number for the smart card, and a label that will identify the smart card. Click **Next**.

A notification is shown that the first keyshare is successfully stored.

b.   Enter the switch credentials and PIN information for the second recovery officer. Click **Next**.

A notification is shown that the second keyshare is successfully stored.

c.   Enter the switch credentials and PIN information for the third recovery officer. Click **Next.**

A notification is shown that the third keyshare is successfully stored.

d.   Enter the switch credentials and PIN information for the fourth recovery officer. Click **Next**.

A notification is shown that the fourth keyshare is successfully stored.

e.   Enter the switch credentials and PIN information for the fifth recovery officer. Click **Next**.

A notification is shown that the fifth keyshare is successfully stored. Click **Next** to begin the automatic synchronization of volume groups.

Step 9   The smart card replacement is completed. Click **Close** to return to the DCNM-SAN Web Client and to view the smart card information.

Step 10   Select **Smartcards** to view the new smart card information. The smart card details display the old recovery shares and the new recovery shares.

Configuring Master Key Rekey

You can initiate the master key rekey operation using one of the following methods:

- Under **Data Center Network Manager**, click **SME**. The cluster list is displayed. Click on the required cluster. Under **Cluster Details > Security Mode**, click **Rekey Master Key**.

- Under **Data Center Network Manager**, click **SME**. The cluster list is displayed. Click **Smartcards**. The Recovery shares details along with the associated list of smart cards is displayed. Under **Recovery Shares**, click **Rekey Master Key**.

Prerequisites

- Ensure you install the smartcard drivers on the web client where MKR is initiated.

- Ensure there is IP communication between the Cisco DCNM server, primary server, secondary server, CKMC, and switches.

- Ensure Cisco DCNM-SAN services are running.

- Ensure the clusters are online throughout the MKR process.

- Ensure you export the keys before starting MKR.

- Ensure there is free space for new shares on the smart cards.

- Always start MKR on a fresh browser and ensure there are no instances of DCNM client running.

- Ensure you do not start MKR if the disk is in one of the following states:
  - DP error
  - DP in-progress
  - Pending KMC update
  - ITL Offline
  - Crypto state with no paths (VPD not known)
  - Suspend state with no paths (VPD not known)
  - Data Prepare (discovery pending)
  - Wait enabled

Detailed Steps

Step 1 Once you initiate the rekey master key operation, you will receive a confirmation dialog box. Click **OK**

The Get Keyshares dialog box is displayed.

Note All nodes that are part of the cluster should remain online until the rekey master key operation is complete.

Step 2 Insert the Smart Card.

To rekey the master keyshares, follow these steps:

a. Enter the switch login information, the PIN number for the smart card, and a label that will identify the smart card. Click **Next**.

A notification is shown that the first keyshare is successfully stored.

b. Enter the switch credentials and PIN information for the second recovery officer. Click **Next**.

A notification is shown that the second keyshare is successfully stored.

c. Enter the switch credentials and PIN information for the third recovery officer. Click **Next.**

A notification is shown that the third keyshare is successfully stored.

d. Enter the switch credentials and PIN information for the fourth recovery officer. Click **Next**.

A notification is shown that the fourth keyshare is successfully stored.

e. Enter the switch credentials and PIN information for the fifth recovery officer. Click **Next**.

A notification is shown that the fifth keyshare is successfully stored. Click **Next** to begin the rekeying process.

Step 3 You will see an indication that the operation is in progress and to wait until the rekeying of master keys is completed. Click **Next**.

The Rekey Master Key configuration is successful.

Resume Sync

When you have all the shares stored in the smart card and when there are discrepancies in the fabric and when MKR fails, click Resume Sync to resume the MKR operation.

Verifying the SME Disk Management Configuration

To display the SME disk management configuration information, perform one of the following tasks:

Command	Purpose
show sme cluster	Displays detailed information about the clusters.
show sme cluster detail	Displays detailed information about the clusters.
show sme cluster *clustername*	Displays detailed information about a particular cluster.
show sme cluster *clustername* **detail**	Displays detailed information about a particular cluster.
show sme cluster summary	Displays summary information about the clusters.
show sme cluster *clustername* **summary**	Displays detailed information about a particular cluster.
show sme cluster *clustername* **it-nexus**	Displays detailed information about the IT-nexuses in a particular cluster.
show sme cluster *clustername* **disk-group**	Displays the summary and total number of disks in a disk group.
show sme cluster *clustername* **disk-group** *diskgroup-name*	Displays the detailed information about the disks in a particular disk group.
show sme cluster *clustername* **disk-group** *diskgroup-name* **disk**	Displays the detailed information about the disks in a particular disk group.

Command	Purpose
show sme cluster *clustername* **disk-group** *diskgroup-name* **disk** *diskname*	Displays the detailed information about the disks in a particular disk group and shows the status of ITLs.
show sme cluster *clustername* **disk detail**	Displays the detailed information about the disk in a cluster.
show sme cluster *clustername* **disk summary**	Displays the summary information about the disk in a cluster.
show sme cluster *clustername* **disk-data prepare detail**	Displays the detailed information about the disks that are undergoing data preparation in a cluster. ✎ **Note** This is currently not supported.
show sme cluster *clustername* **disk-data prepare summary**	Displays the summary information about the disks that are undergoing data preparation in a cluster. ✎ **Note** This is currently not supported.
show sme cluster *clustername* **interface detail**	Displays the detailed information about the SME interfaces in a cluster.
show sme cluster *clustername* **interface summary**	Displays the summary information about the SME interfaces in a cluster.
show sme cluster *clustername* **interface sme** *sme-interface*	Displays the information about a particular SME interface in a cluster.
show sme cluster *clustername* **interface node** *remote-switch*	Displays the information about the SME interfaces for a remote node in a cluster.
show sme cluster *clustername* **key database**	Displays the information about the keys in a cluster.
show sme cluster *clustername* **key database detail**	Displays the detailed information about the keys in a cluster.
show sme cluster *clustername* **key database summary**	Displays the summary information about the keys in a cluster.
show sme cluster *clustername* **key database guid** *guid*	Displays the key information in a cluster for the particular GUID.
show sme cluster *clustername* **load-balancing**	Displays the load-balancing status for the cluster.
show sme cluster *clustername* **lun crypto-status**	Displays the crypto status for the LUNs in a cluster.
show sme cluster *clustername* **node**	Displays information about the nodes in a cluster.
show sme cluster *clustername* **node summary**	Displays summary information about the nodes in a cluster.
show sme cluster *clustername* **node** *remote-switch*	Displays information about a particular remote node in a cluster.
show sme cluster *clustername* **recovery officer**	Displays information about SME cluster recovery officer.

Command	Purpose
show sme cluster *clustername* **recovery officer** *recovery-index*	Displays information about a particular SME cluster recovery officer.
show sme cluster *clustername* **recovery officer detail**	Displays detail information about SME cluster recovery officer.
show sme cluster *clustername* **recovery officer summary**	Displays summary information about SME cluster recovery officer.
show sme cluster *clustername* **recovery officer summary** *recovery-index*	Displays summary information about a particular SME cluster recovery officer.

For detailed information about the fields in the output from these commands, refer to the *Cisco MDS 9000 Family NX-OS Command Reference*.

Monitoring SME Disk Management

This section includes the following topics:

Viewing Host Details

You can view detailed information about hosts in a SME cluster. Information for a specific host includes the disk group membership, paths from the host to the target, VSAN, fabric, status, and the disk device.

To view the host details, select a host in the navigation pane.

Viewing Disk Group Details

You can view detailed information about disk groups in a SME cluster. Information for a specific disk includes the disk group membership, device description, serial number, and the host and target PWWN.

To view the disk group details, select a disk group in the navigation pane.

Viewing Disk Details

You can view details and information about the disks in a disk group in an SME cluster. Information for a specific disk includes the path information and the disk status.

To view the disk details, select a disk from the navigation pane.

Viewing Disk Path Details

You can view the disk path details of a disk in a disk group in an SME cluster. Information for a specific disk includes the path information and the disk status.

To view the disk path details, select a disk from the navigation pane. The details are displayed in the Disk Details and Configured Paths section.

Viewing Signature Mode Clusters

You can view the detailed information of SME clusters that are in signature mode. To view the cluster details, click clusters from the navigation pane.

Viewing SME Disk Information Using the CLI

Use the **show sme cluster** command to view information about a cluster.

```
switch# show sme cluster
SME Cluster is dest1
  Cluster ID is 0x29ab000dec3f1402
  Cluster status is online
  Security mode is basic
  Total Nodes are 2
  Recovery Scheme is 1 out of 1
  Fabric[0] is Fabric_jlwu9216i-19
  Fabric[1] is Fabric_jlwu9222i-15
  Primary KMC server 172.25.230.33:8800 is provisioned, connection state is none
  Secondary KMC server has not been provisioned
  Master Key GUID is b020829d0f009fa2-4d496531313d981e, Version: 0
  Shared Key Mode is Not Enabled
  Auto Vol Group is Not Enabled
  Tape Compression is Enabled
  Tape Key Recycle Policy is Enabled
  Key On Tape is Not Enabled
  Cluster Infra Status : Operational
  Cluster is Administratively Up
  Cluster Config Version : 2445
  SSL for KMC : Not Configured
  SSL for ICN : Not Configured
  Cluster is Disk capable
  Cluster Metadata On Disk is Set: 64 megabytes <!---64 megabytes indicates a signature
mode cluster>
```

Note   The cluster config version specifies the version of the saved configuration on the switch. In scenarios when a cluster information must be retrieved or a cluster must be revived the switch with the highest configuration version must be used.

Use the **show sme cluster detail** command to view detail information about a cluster.

```
switch# show sme cluster detail
SME Cluster is dest1
  Cluster ID is 0x29ab000dec3f1402
  Cluster status is online
  Security mode is basic
  Total Nodes are 2
  Recovery Scheme is 1 out of 1
  Fabric[0] is Fabric_jlwu9216i-19
  Fabric[1] is Fabric_jlwu9222i-15
  Primary KMC server 172.25.230.33:8800 is provisioned, connection state is none
  Secondary KMC server has not been provisioned
  Master Key GUID is b020829d0f009fa2-4d496531313d981e, Version: 0
  Shared Key Mode is Not Enabled
  Auto Vol Group is Not Enabled
  Tape Compression is Enabled
  Tape Key Recycle Policy is Enabled
  Key On Tape is Not Enabled
  Cluster Infra Status : Operational
  Cluster is Administratively Up
  Cluster Config Version : 2445
  SSL for KMC : Not Configured
  SSL for ICN : Not Configured
  Cluster is Disk capable
  Cluster Metadata On Disk is Set: 64 Megabytes
```

Use the **show sme cluster summary** command to view summary information about the cluster.

```
switch# show sme cluster summary
-------------------------------------------------------------------------------
Cluster         ID                    Security Mode    Status
-------------------------------------------------------------------------------
C               0x20eb000dec3f45c2    basic            online
-------------------------------------------------------------------------------
```

Use the **show sme cluster** *clustername* command to view information about a particular cluster.

```
switch# show sme cluster c
SME Cluster is C
  Cluster ID is 0x29ab000dec3f1402
  Cluster status is online
  Security mode is basic
  Total Nodes are 2
  Recovery Scheme is 1 out of 1
  Fabric[0] is Fabric_jlwu9216i-19
  Fabric[1] is Fabric_jlwu9222i-15
  Primary KMC server 172.25.230.33:8800 is provisioned, connection state is none
  Secondary KMC server has not been provisioned
  Master Key GUID is b020829d0f009fa2-4d496531313d981e, Version: 0
  Shared Key Mode is Not Enabled
  Auto Vol Group is Not Enabled
  Tape Compression is Enabled
  Tape Key Recycle Policy is Enabled
  Key On Tape is Not Enabled
  Cluster Infra Status : Operational
  Cluster is Administratively Up
  Cluster Config Version : 2445
  SSL for KMC : Not Configured
  SSL for ICN : Not Configured
  Cluster is Disk capable
  Cluster Metadata On Disk is Set: 64 Megabytes
```

Use the **show sme cluster** *clustername* **detail** command to view detail information about a particular cluster.

```
switch# show sme cluster c detail
SME Cluster is C
  Cluster ID is 0x29ab000dec3f1402
  Cluster status is online
  Security mode is basic
  Total Nodes are 2
  Recovery Scheme is 1 out of 1
  Fabric[0] is Fabric_jlwu9216i-19
  Fabric[1] is Fabric_jlwu9222i-15
  Primary KMC server 172.25.230.33:8800 is provisioned, connection state is none
  Secondary KMC server has not been provisioned
  Master Key GUID is b020829d0f009fa2-4d496531313d981e, Version: 0
  Shared Key Mode is Not Enabled
  Auto Vol Group is Not Enabled
  Tape Compression is Enabled
  Tape Key Recycle Policy is Enabled
  Key On Tape is Not Enabled
  Cluster Infra Status : Operational
  Cluster is Administratively Up
  Cluster Config Version : 2445
  SSL for KMC : Not Configured
  SSL for ICN : Not Configured
  Cluster is Disk capable
  Cluster Metadata On Disk is Set: 64 Megabytes
```

Use the **show sme cluster** *clustername* **summary** command to view summary information about a particular cluster.

```
switch# show sme cluster c summary
-------------------------------------------------------------------------------
Cluster         ID                    Security Mode    Status
-------------------------------------------------------------------------------
C               0x20eb000dec3f45c2    basic            online
-------------------------------------------------------------------------------
```

Use the **show sme cluster** *clustername* **disk group** command to view the disk group information in particular cluster.

```
switch# show sme cluster c disk-group
-----------------------------------
Disk Group Name        Total Disks
-----------------------------------
DG                     8
```

Use the **show sme cluster** *clustername* **disk-group DG** command to view information about a disk group in a cluster.

```
switch# show sme cluster scluster20 disk-group dg1
Disk group dg1
  Number of disks is 16

Disk group dg1
  Number of disks is 16

  Disk Disk0 is clear
    Description is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000005006218003813000
    Encryption is Not Enabled

  Disk Disk1 is clear
    Description is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000015006218003813000
    Encryption is Not Enabled

  Disk Disk10 is clear
    Description is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000a5006218003813000
    Encryption is Not Enabled

  Disk Disk11 is clear
    Description is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000b5006218003813000
    Encryption is Not Enabled

  Disk Disk12 is clear
    Description is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000c5006218003813000
```

```
    Encryption is Not Enabled

Disk Disk13 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb00000000d5006218003813000
  Encryption is Not Enabled

Disk Disk14 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb00000000e5006218003813000
  Encryption is Not Enabled

Disk Disk15 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb00000000f5006218003813000
  Encryption is Not Enabled

Disk Disk2 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb00000000025006218003813000
  Encryption is Not Enabled

Disk Disk3 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb00000000035006218003813000
  Encryption is Not Enabled

Disk Disk4 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb00000000045006218003813000
  Encryption is Not Enabled

Disk Disk5 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb00000000055006218003813000
  Encryption is Not Enabled

Disk Disk6 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb00000000065006218003813000
  Encryption is Not Enabled

Disk Disk7 is clear
  Description is LSI INF-01-00
  Vendor ID is LSI
  Product ID is INF-01-00
  Device ID is 600a0bb00000000075006218003813000
  Encryption is Not Enabled
```

```
  Disk Disk8 is clear
    Description is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000085006218003813000
    Encryption is Not Enabled

  Disk Disk9 is clear
    Description is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000095006218003813000
    Encryption is Not Enabled
```

Use the **show sme cluster** *clustername* **disk-group** *disk-group name* **DG disk** command to view information about a disk in the disk group.

```
switch# show sme cluster scluster20 disk-group dg1 disk
Disk group dg1
  Number of disks is 16

Disk group dg1
  Number of disks is 16

  Disk Disk0 is clear
    Description is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000005006218003813000
    Encryption is Not Enabled

  Disk Disk1 is clear
    Description is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000015006218003813000
    Encryption is Not Enabled

  Disk Disk10 is clear
    Description is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000a5006218003813000
    Encryption is Not Enabled

  Disk Disk11 is clear
    Description is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000b5006218003813000
    Encryption is Not Enabled

  Disk Disk12 is clear
    Description is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000c5006218003813000
    Encryption is Not Enabled

  Disk Disk13 is clear
    Description is LSI INF-01-00
    Vendor ID is LSI
```

```
       Product ID is INF-01-00
       Device ID is 600a0bb00000000d5006218003813000
       Encryption is Not Enabled

  Disk Disk14 is clear
       Description is LSI INF-01-00
       Vendor ID is LSI
       Product ID is INF-01-00
       Device ID is 600a0bb00000000e5006218003813000
       Encryption is Not Enabled

  Disk Disk15 is clear
       Description is LSI INF-01-00
       Vendor ID is LSI
       Product ID is INF-01-00
       Device ID is 600a0bb00000000f5006218003813000
       Encryption is Not Enabled

  Disk Disk2 is clear
       Description is LSI INF-01-00
       Vendor ID is LSI
       Product ID is INF-01-00
       Device ID is 600a0bb00000000025006218003813000
       Encryption is Not Enabled

  Disk Disk3 is clear
       Description is LSI INF-01-00
       Vendor ID is LSI
       Product ID is INF-01-00
       Device ID is 600a0bb00000000035006218003813000
       Encryption is Not Enabled

  Disk Disk4 is clear
       Description is LSI INF-01-00
       Vendor ID is LSI
       Product ID is INF-01-00
       Device ID is 600a0bb00000000045006218003813000
       Encryption is Not Enabled

  Disk Disk5 is clear
       Description is LSI INF-01-00
       Vendor ID is LSI
       Product ID is INF-01-00
       Device ID is 600a0bb00000000055006218003813000
       Encryption is Not Enabled

  Disk Disk6 is clear
       Description is LSI INF-01-00
       Vendor ID is LSI
       Product ID is INF-01-00
       Device ID is 600a0bb00000000065006218003813000
       Encryption is Not Enabled

  Disk Disk7 is clear
       Description is LSI INF-01-00
       Vendor ID is LSI
       Product ID is INF-01-00
       Device ID is 600a0bb00000000075006218003813000
       Encryption is Not Enabled

  Disk Disk8 is clear
       Description is LSI INF-01-00
       Vendor ID is LSI
       Product ID is INF-01-00
```

```
    Device ID is 600a0bb00000000085006218003813000
    Encryption is Not Enabled


  Disk Disk9 is clear
    Description is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000095006218003813000
    Encryption is Not Enabled
```

Use the **show sme cluster** *clustername* **disk-group** *disk-group name* **disk** *disk name* command to view information about a disk in the disk group.

```
switch# show sme cluster scluster20 disk-group dg1 disk Disk 0
Disk Disk0 is clear
    Description is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000005006218003813000
    Encryption is Not Enabled
    Paths
      Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0000 vsan 100
        [Fabric_sw-A-9222i-95]
          Is online (SUCCESS), configured
```

Use the **show sme cluster** *clustername* **disk detail** command to view detail information about a disk in a cluster.

```
switch# show sme cluster scluster20 disk detail
Disk 1 is clear
    Model is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000095006218003813000
    Is configured as disk device Disk9 in disk group dg1
    Paths
      Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0009 vsan 100
        Is online (SUCCESS), configured

Disk 2 is clear
    Model is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000005006218003813000
    Is configured as disk device Disk0 in disk group dg1
    Paths
      Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0000 vsan 100
        Is online (SUCCESS), configured

Disk 3 is clear
    Model is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000f5006218003813000
    Is configured as disk device Disk15 in disk group dg1
    Paths
      Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x000f vsan 100
        Is online (SUCCESS), configured

Disk 4 is clear
    Model is LSI INF-01-00
    Vendor ID is LSI
```

```
                   Product ID is INF-01-00
                   Device ID is 600a0bb0000000025006218003813000
                   Is configured as disk device Disk2 in disk group dg1
                   Paths
                      Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0002 vsan 100
                         Is online (SUCCESS), configured


              Disk 5 is clear
                   Model is LSI INF-01-00
                   Vendor ID is LSI
                   Product ID is INF-01-00
                   Device ID is 600a0bb0000000085006218003813000
                   Is configured as disk device Disk8 in disk group dg1
                   Paths
                      Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0008 vsan 100
                         Is online (SUCCESS), configured


              Disk 6 is clear
                   Model is LSI INF-01-00
                   Vendor ID is LSI
                   Product ID is INF-01-00
                   Device ID is 600a0bb00000000b5006218003813000
                   Is configured as disk device Disk11 in disk group dg1
                   Paths
                      Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x000b vsan 100
                         Is online (SUCCESS), configured


              Disk 7 is clear
                   Model is LSI INF-01-00
                   Vendor ID is LSI
                   Product ID is INF-01-00
                   Device ID is 600a0bb0000000065006218003813000
                   Is configured as disk device Disk6 in disk group dg1
                   Paths
                      Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0006 vsan 100
                         Is online (SUCCESS), configured


              Disk 8 is clear
                   Model is LSI INF-01-00
                   Vendor ID is LSI
                   Product ID is INF-01-00
                   Device ID is 600a0bb0000000055006218003813000
                   Is configured as disk device Disk5 in disk group dg1
                   Paths
                      Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0005 vsan 100
                         Is online (SUCCESS), configured


              Disk 9 is clear
                   Model is LSI INF-01-00
                   Vendor ID is LSI
                   Product ID is INF-01-00
                   Device ID is 600a0bb0000000075006218003813000
                   Is configured as disk device Disk7 in disk group dg1
                   Paths
                      Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0007 vsan 100
                         Is online (SUCCESS), configured


              Disk 10 is clear
                   Model is LSI INF-01-00
                   Vendor ID is LSI
                   Product ID is INF-01-00
                   Device ID is 600a0bb0000000035006218003813000
                   Is configured as disk device Disk3 in disk group dg1
                   Paths
```

```
      Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0003 vsan 100
          Is online (SUCCESS), configured


Disk 11 is clear
    Model is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb0000000045006218003813000
    Is configured as disk device Disk4 in disk group dg1
    Paths
      Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0004 vsan 100
          Is online (SUCCESS), configured


Disk 12 is clear
    Model is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb0000000015006218003813000
    Is configured as disk device Disk1 in disk group dg1
    Paths
      Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x0001 vsan 100
          Is online (SUCCESS), configured


Disk 13 is clear
    Model is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000d5006218003813000
    Is configured as disk device Disk13 in disk group dg1
    Paths
      Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x000d vsan 100
          Is online (SUCCESS), configured


Disk 14 is clear
    Model is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000c5006218003813000
    Is configured as disk device Disk12 in disk group dg1
    Paths
      Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x000c vsan 100
          Is online (SUCCESS), configured


Disk 15 is clear
    Model is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000a5006218003813000
    Is configured as disk device Disk10 in disk group dg1
    Paths
      Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x000a vsan 100
          Is online (SUCCESS), configured


Disk 16 is clear
    Model is LSI INF-01-00
    Vendor ID is LSI
    Product ID is INF-01-00
    Device ID is 600a0bb00000000e5006218003813000
    Is configured as disk device Disk14 in disk group dg1
    Paths
      Host 10:00:0e:91:c3:76:5c:00 Target 50:06:21:80:03:81:30:00 Lun 0x000e vsan 100
          Is online (SUCCESS), configured
```

Use the **show sme cluster** *clustername* **disk summary** command to view summary information about a particular disk in a cluster.

```
switch# show sme cluster c disk summary
--------------------------------------------------------------------------------
Target WWN               Lun      Description          Crypto-Disk        Status
--------------------------------------------------------------------------------
50:06:01:6b:30:60:06:d6  0x0002   DGC DISK             Disk7              clear
50:06:01:6b:30:60:06:d6  0x0000   DGC DISK             Disk5              clear
50:06:01:6b:30:60:06:d6  0x0001   DGC DISK             Disk6              clear
50:06:01:63:30:60:06:d6  0x0003   DGC RAID 5           Disk3              clear
50:06:01:63:30:60:06:d6  0x0004   DGC RAID 5           Disk4              clear
50:06:01:63:30:60:06:d6  0x0001   DGC RAID 5           Disk1              clear
50:06:01:63:30:60:06:d6  0x0002   DGC RAID 5           Disk2              clear
50:06:01:63:30:60:06:d6  0x0000   DGC RAID 5           Disk0              clear
```

Use the **show sme cluster** *clustername* **it-nexus** command to view detail information about the IT-nexuses in a particular cluster.

```
switch# show sme cluster c it-nexus
--------------------------------------------------------------------------------
    Host WWN,           VSAN     Status    Switch         Interface
    Target WWN
--------------------------------------------------------------------------------


21:00:00:1b:32:8a:1d:4c,
50:06:01:63:30:60:06:d6   2       online    172.28.234.68 sme1/1


21:01:00:1b:32:aa:49:4c,
50:06:01:6b:30:60:06:d6   2       online    172.28.234.68 sme1/1


21:02:00:1b:32:ca:49:4c,
50:06:01:6b:30:60:06:d6   2       online    172.28.234.68 sme1/1
```

Use the **show sme cluster** *clustername* **interface detail** command to view detail information about the SME interfaces in a cluster.

```
Interface sme1/1 belongs to local switch
  Status is up
    RSA Certificate is (len 247 fingerprint SHA1::
87:2f:16:6d:91:ec:8f:cb:95:3a:df:6b:c6:49:c3:67:c4:a9:39:6f:)
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAMJGt4JoIhfV3KU6eJPdfmzIjYLqbZ2mA3VdJ7T86btzyMhpZZI4x76O
uCvLxEIuKW+p/XRqhpV4AN7YQDVCw0OB3dacXfRQjM8EdoC6lMXDGsKCzYzti51H
ZqQvAKCMydz/P3CSbVx3MsoOeDuvv/Hj6wvIngtDGfvHkWms9b1lAgED
-----END RSA PUBLIC KEY-----
```

Use the **show sme cluster** *clustername* **interface summary** command to view summary information about the SME interfaces in a cluster.

```
switch# show sme cluster c interface summary
--------------------------------------------------------------------------------
Switch               Interface      Status
--------------------------------------------------------------------------------
local switch         sme1/1         up
```

Use the **show sme cluster** *clustername* **interface sme** *sme-interface* command to view information about a particular SME interface in a cluster.

```
switch# show sme cluster c interface sme 1/1
Interface sme1/1 belongs to local switch
```

```
        Status is up
```

Use the **show sme cluster** *clustername* **lun crypto-status** command to view crypto status of the LUNs in a cluster.

```
switch# show sme cluster c lun crypto-status
LUN (Serial Number)                                             Encryption
--------------------------------------------------------------------------------
LUN
---
  cpp_lun_ndx            0x29
  sme_enabled            0
  vendor_id              DGC
  product_id             DISK
  device_id              10493CF4
  prod_rev_level         0216
  vendor_specific        860000AB71CL
  cluster_name           C
  dg_name                DG
  device_name            Disk7
  max_lba                0x27fffff
  blk_sz                 0x200
  disk_state             0x1
  current disk fsm state SMED_CPP_DISK_ST_CLEAR_DISK
  cur_key_guid           0000000000000000-0000000000000000
  new_key_guid           0000000000000000-0000000000000000
  cur_key_obj            (nil)
  new_key_obj            (nil)
  dp                     (nil)
  total itl count        2
  active itl count       2
  lun hold count         0
  Not locked
    I 21:01:00:1b:32:aa:49:4c T 50:06:01:6b:30:60:06:d6 L 0x0002
        (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])
    I 21:02:00:1b:32:ca:49:4c T 50:06:01:6b:30:60:06:d6 L 0x0002
        (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])
LUN
---
  cpp_lun_ndx            0x27
  sme_enabled            0
  vendor_id              DGC
  product_id             DISK
  device_id              93B1508B
  prod_rev_level         0216
  vendor_specific        8000009529CL
  cluster_name           C
  dg_name                DG
  device_name            Disk5
  max_lba                0x27fffff
  blk_sz                 0x200
  disk_state             0x1
  current disk fsm state SMED_CPP_DISK_ST_CLEAR_DISK
  cur_key_guid           0000000000000000-0000000000000000
  new_key_guid           0000000000000000-0000000000000000
  cur_key_obj            (nil)
  new_key_obj            (nil)
  dp                     (nil)
  total itl count        2
  active itl count       2
  lun hold count         0
  Not locked
    I 21:01:00:1b:32:aa:49:4c T 50:06:01:6b:30:60:06:d6 L 0x0000
```

```
                       (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])
          I 21:02:00:1b:32:ca:49:4c T 50:06:01:6b:30:60:06:d6 L 0x0000
                       (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])
     LUN
     ---
       cpp_lun_ndx              0x28
       sme_enabled              0
       vendor_id                DGC
       product_id               DISK
       device_id                F074E188
       prod_rev_level           0216
       vendor_specific          850000AA73CL
       cluster_name             C
       dg_name                  DG
       device_name              Disk6
       max_lba                  0x27fffff
       blk_sz                   0x200
       disk_state               0x1
       current disk fsm state   SMED_CPP_DISK_ST_CLEAR_DISK
       cur_key_guid             0000000000000000-0000000000000000
       new_key_guid             0000000000000000-0000000000000000
       cur_key_obj              (nil)
       new_key_obj              (nil)
       dp                       (nil)
       total itl count          2
       active itl count         2
       lun hold count           0
       Not locked
         I 21:01:00:1b:32:aa:49:4c T 50:06:01:6b:30:60:06:d6 L 0x0001
                       (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])
         I 21:02:00:1b:32:ca:49:4c T 50:06:01:6b:30:60:06:d6 L 0x0001
                       (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])
     LUN
     ---
       cpp_lun_ndx              0x25
       sme_enabled              0
       vendor_id                DGC
       product_id               RAID 5
       device_id                3C2590FB
       prod_rev_level           0216
       vendor_specific          39000061BDCL
       cluster_name             C
       dg_name                  DG
       device_name              Disk3
       max_lba                  0x9fffff
       blk_sz                   0x200
       disk_state               0x1
       current disk fsm state   SMED_CPP_DISK_ST_CLEAR_DISK
       cur_key_guid             0000000000000000-0000000000000000
       new_key_guid             0000000000000000-0000000000000000
       cur_key_obj              (nil)
       new_key_obj              (nil)
       dp                       (nil)
       total itl count          1
       active itl count         1
       lun hold count           0
       Not locked
         I 21:00:00:1b:32:8a:1d:4c T 50:06:01:63:30:60:06:d6 L 0x0003
                       (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])
     LUN
     ---
       cpp_lun_ndx              0x26
       sme_enabled              0
       vendor_id                DGC
```

```
      product_id               RAID 5
      device_id                8B09E6E9
      prod_rev_level           0216
      vendor_specific          3A000061D3CL
      cluster_name             C
      dg_name                  DG
      device_name              Disk4
      max_lba                  0x9fffff
      blk_sz                   0x200
      disk_state               0x1
      current disk fsm state   SMED_CPP_DISK_ST_CLEAR_DISK
      cur_key_guid             0000000000000000-0000000000000000
      new_key_guid             0000000000000000-0000000000000000
      cur_key_obj              (nil)
      new_key_obj              (nil)
      dp                       (nil)
      total itl count          1
      active itl count         1
      lun hold count           0
      Not locked
       I 21:00:00:1b:32:8a:1d:4c T 50:06:01:63:30:60:06:d6 L 0x0004
          (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])
  LUN
  ---
      cpp_lun_ndx              0x23
      sme_enabled              0
      vendor_id                DGC
      product_id               RAID 5
      device_id                90D80D94
      prod_rev_level           0216
      vendor_specific          3700006182CL
      cluster_name             C
      dg_name                  DG
      device_name              Disk1
      max_lba                  0x9fffff
      blk_sz                   0x200
      disk_state               0x1
      current disk fsm state   SMED_CPP_DISK_ST_CLEAR_DISK
      cur_key_guid             0000000000000000-0000000000000000
      new_key_guid             0000000000000000-0000000000000000
      cur_key_obj              (nil)
      new_key_obj              (nil)
      dp                       (nil)
      total itl count          1
      active itl count         1
      lun hold count           0
      Not locked
       I 21:00:00:1b:32:8a:1d:4c T 50:06:01:63:30:60:06:d6 L 0x0001
          (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])
  LUN
  ---
      cpp_lun_ndx              0x24
      sme_enabled              0
      vendor_id                DGC
      product_id               RAID 5
      device_id                930ED44F
      prod_rev_level           0216
      vendor_specific          38000061A5CL
      cluster_name             C
      dg_name                  DG
      device_name              Disk2
      max_lba                  0x9fffff
      blk_sz                   0x200
      disk_state               0x1
```

```
      current disk fsm state    SMED_CPP_DISK_ST_CLEAR_DISK
      cur_key_guid              0000000000000000-0000000000000000
      new_key_guid              0000000000000000-0000000000000000
      cur_key_obj               (nil)
      new_key_obj               (nil)
      dp                        (nil)
      total itl count           1
      active itl count          1
      lun hold count            0
      Not locked
       I 21:00:00:1b:32:8a:1d:4c T 50:06:01:63:30:60:06:d6 L 0x0002
           (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])
LUN
---
      cpp_lun_ndx               0x22
      sme_enabled               0
      vendor_id                 DGC
      product_id                RAID 5
      device_id                 CC1BCB3A
      prod_rev_level            0216
      vendor_specific           360000616BCL
      cluster_name              C
      dg_name                   DG
      device_name               Disk0
      max_lba                   0x9fffff
      blk_sz                    0x200
      disk_state                0x1
      current disk fsm state    SMED_CPP_DISK_ST_CLEAR_DISK
      cur_key_guid              0000000000000000-0000000000000000
      new_key_guid              0000000000000000-0000000000000000
      cur_key_obj               (nil)
      new_key_obj               (nil)
      dp                        (nil)
      total itl count           1
      active itl count          1
      lun hold count            0
      Not locked
       I 21:00:00:1b:32:8a:1d:4c T 50:06:01:63:30:60:06:d6 L 0x0000
           (SMED_ISAPI_ITL_ST_UP_CLEAR [lock event=NONE])
```

Use the **show sme cluster** *clustername* **load-balancing** command to view the load-balancing status of the cluster.

```
switch# show sme cluster c load-balancing
Load balancing status is enabled for cluster C
```

Use the **show sme cluster** *clustername* **node** command to view information about the nodes in a cluster.

```
switch# show sme cluster c node
Node 172.28.234.54 is remote switch
  Node ID is 2
  Status is online
  Node is not master switch
  Fabric is Fabric_sw-sme-9513-54
Node 172.28.234.68 is local switch
  Node ID is 1
  Status is online
  Node is the master switch
  Fabric is Fabric_sw-sme-9513-54
```

Use the **show sme cluster** *clustername* **node** *remote-switch* command to view information about a particular remote node in a cluster.

```
switch# show sme cluster c node 172.28.234.54
Node 172.28.234.54 is remote switch
  Node ID is 2
  Status is online
  Node is not master switch
  Fabric is Fabric_sw-sme-9513-54
```

Use the **show sme cluster** *clustername* **node summary** command to view summary information about the nodes in a cluster.

```
switch# show sme cluster c node summary
-------------------------------------------------------------------------------
Switch                 Status          Master     Node ID
-------------------------------------------------------------------------------
172.28.234.54          online          no         2
local switch           online          yes        1
```

Use the **show sme cluster** *clustername* **key database** command to view information about the keys in a cluster.

```
switch# show sme cluster c key database
Key Type is master key
  GUID is 2ebddb1dbf180660-c0e4add77be8e8a0
    Cluster is C, Master Key Version is 0

Key Type is disk key
  GUID is 5a8adb8aca98106f-dd61016f5fb8b543
    Cluster is C, Crypto disk group is DG
    Crypto disk is Disk1

Key Type is disk key
  GUID is dc203fa33cd267ad-dd2e7513e307521f
    Cluster is C, Crypto disk group is DG
    Crypto disk is Disk0
```

Use the **show sme cluster** *clustername* **key database detail** command to view detail information about the keys in a cluster.

```
switch# show sme cluster c key database detail
Key Type is master key
  GUID is 2ebddb1dbf180660-c0e4add77be8e8a0
    Cluster is C, Master Key Version is 0
  Key status is active
  Key was created at Mon Oct 04 13:38:41 UTC 2010
  Key length is 32

Key Type is disk key
  GUID is 5a8adb8aca98106f-dd61016f5fb8b543
    Cluster is C, Crypto disk group is DG
    Crypto disk is Disk1
  Key status is active
  Key was created at Mon Oct 04 13:58:23 UTC 2010
  Key length is 32
  Key data type is symmetric key wrap
  Symmetric key wrapping version is 0
  Symmetric crypto algorithm is aes-cbc
  Authentication algorithm used is sha-256 and value
    G5UvNvtQC67CGfbJBWV1xs+zUKF4CIOIrk+tfG+dPQY=
```

```
    IV length is 16 and value
      jAMWrbbqtDou2DmSmlddmQAAAAAAAAAAAAAAAAAAAAA=
    Key Object is wrapped by 2ebddb1dbf180660-c0e4add77be8e8a0
    Key data length is 80
    Encrypted data is
      qLOTc/pr9NvMcRTgwePgzwpJaBoDxzLevYXh1gw9c+fbZlp4
      kabTYUM7QGTrZKFkkJPOPO/XPSn9VVKVYvNSCguQV0teq6Vo
      vdUqeDyht9g=

Key Type is disk key
  GUID is dc203fa33cd267ad-dd2e7513e307521f
    Cluster is C, Crypto disk group is DG
    Crypto disk is Disk0
  Key status is active
  Key was created at Mon Oct 04 13:57:56 UTC 2010
  Key length is 32
  Key data type is symmetric key wrap
  Symmetric key wrapping version is 0
  Symmetric crypto algorithm is aes-cbc
  Authentication algorithm used is sha-256 and value
    8isr/LRaHdqQmlGPagCq9reDOYLQiFdImmQfmIRsu9s=
  IV length is 16 and value
    gJfKQqKTsU8iJ5HrGQR3GwAAAAAAAAAAAAAAAAAAAAA=
  Key Object is wrapped by 2ebddb1dbf180660-c0e4add77be8e8a0
  Key data length is 80
  Encrypted data is
    zL+syhPqSQfXy8zAwLfrntbIcjIux+dIjPQWQ0Jk/zpVTmRD
    KT6RlzFmkN3ibXaqzba6yrfCXUGMmWX/KK7CdEQtkWk1ecUz
    k+zvbYtdq50=
```

Use the **show sme cluster** *clustername* **key database summary** command to view summary information about the keys in a cluster.

```
switch# show sme cluster c key database summary
-----------------------------------------------------------------------------
Key Type                      GUID
-----------------------------------------------------------------------------
master key                    2ebddb1dbf180660-c0e4add77be8e8a0
disk key                      5a8adb8aca98106f-dd61016f5fb8b543
disk key                      dc203fa33cd267ad-dd2e7513e307521f
```

Use the **show sme cluster** *clustername* **key database guid** *GUID* command to view key information in a cluster for a particular GUID.

```
switch# show sme cluster c key database guid 2ebddb1dbf180660-c0e4add77be8e8a0
Key Type is master key
  GUID is 2ebddb1dbf180660-c0e4add77be8e8a0
    Cluster is C, Master Key Version is 0
```

Use the **show sme cluster** *clustername* **key database guid** *GUID* **summary** command to view summary information about the key in a cluster for GUID.

```
switch# show sme cluster C key database guid 2ebddb1dbf180660-c0e4add77be8e8a0 summary
-----------------------------------------------------------------------------
Key Type                      GUID
-----------------------------------------------------------------------------
master key                    2ebddb1dbf180660-c0e4add77be8e8a0
```

Use the **show sme cluster** *clustername* **key database guid** *GUID* **detail** command to view detail information about the key in a cluster for a particular GUID.

```
switch# show sme cluster c key database guid 2ebddb1dbf180660-c0e4add77be8e8a0 detail
Key Type is master key
  GUID is 2ebddb1dbf180660-c0e4add77be8e8a0
    Cluster is C, Master Key Version is 0
  Key status is active
  Key was created at Mon Oct 04 13:38:41 UTC 2010
  Key length is 32
```

Use the **show sme cluster** *clustername* **recovery officer** command to view information about the SME cluster recovery officer.

```
switch# show sme cluster c recovery officer
Recovery Officer 1 is set
  Master Key Version is 0
  Recovery Share Version is 0
  Recovery Share Index is 1
  Recovery Scheme is 1 out of 1
  Recovery Officer Label is
  Recovery share protected by a password


Key Type is master key share
    Cluster is C, Master Key Version is 0
    Recovery Share Version is 0, Share Index is 1
```

Use the **show sme cluster** *clustername* **recovery officer detail** command to view detail information about the SME cluster recovery officer.

```
switch# show sme cluster c recovery officer detail
Recovery Officer 1 is set
  Master Key Version is 0
  Recovery Share Version is 0
  Recovery Share Index is 1
  Recovery Scheme is 1 out of 1
  Recovery Officer Label is
  Recovery share protected by a password

Key Type is master key share
    Cluster is C, Master Key Version is 0
    Recovery Share Version is 0, Share Index is 1
  Key status is active
  Key was created at Mon Oct 04 13:44:45 UTC 2010
  Key length is 81
  Key data type is password key wrap
  Password key wrapping version is 0
  Password scheme used is pkcs5_2
  Password scheme digest algorithm used by password scheme is sha-1
  Authentication algorithm used is sha-256, key length is 32 and value
    58 63 71 59 69 6a 6d 44 50 74 2f 6e 63 77 46 30 38 41 59 31 74 55 54 6e 72 58 37 4d
50 4b 41 6b 55 56 7a 53 6b 6e
52 44 6a 50 45 3d 00 00 00 00

  Salt length is 8 and value
    54 65 79 45 32 65 39 46 33 64 77 3d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00

  IV length is 16
  Iteration count is 2048
```

```
Key data length is 96
Encrypted data is
    69 76 77 4d 52 66 37 44 7a 79 45 30 4f 38 58 34 77 77 69 32 43 34 79 6a 68 54 74 6a
50 77 50 6e 62 71 4e 69 48 77
39 62 57 37 4a 4b 45 37 47 30
    4c 41 46 33 54 6d 6f 31 69 78 4a 39 62 47 65 55 36 4c 67 43 74 5a 49 61 30 49 6a 49
41 66 6c 74 2f 6c 46 57 37 41
38 77 44 75 64 63 32 50 77 45
    4d 68 63 54 54 45 33 4f 4f 48 4f 41 74 4f 66 6a 59 47 32 6d 5a 49 35 34 45 6c 30 30
37 37 77 76 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00
```

Use the **show sme cluster** *clustername* **recovery officer summary** command to view summary information about the SME cluster recovery officer.

```
switch# show sme cluster c recovery officer summary
--------------------------------------------------------------------------------
Share    Status   Label        Smartcard   Serial No
--------------------------------------------------------------------------------
1        Set                   No
```

Use the **show sme cluster** *clustername* **recovery officer** *recovery-index* command to view information about a particular SME cluster recovery officer.

```
switch# show sme cluster c recovery officer 1
Recovery Officer 1 is set
  Master Key Version is 0
  Recovery Share Version is 0
  Recovery Share Index is 1
  Recovery Scheme is 1 out of 1
  Recovery Officer Label is
  Recovery share protected by a password

Key Type is master key share
    Cluster is C, Master Key Version is 0
    Recovery Share Version is 0, Share Index is 1
```

Use the **show sme cluster** *clustername* **recovery officer detail** *recovery-index* command to view detail information about a particular SME cluster recovery officer.

```
switch# show sme cluster c recovery officer detail 1
Recovery Officer 1 is set
  Master Key Version is 0
  Recovery Share Version is 0
  Recovery Share Index is 1
  Recovery Scheme is 1 out of 1
  Recovery Officer Label is
  Recovery share protected by a password

Key Type is master key share
    Cluster is C, Master Key Version is 0
    Recovery Share Version is 0, Share Index is 1
  Key status is active
  Key was created at Mon Oct 04 13:44:45 UTC 2010
  Key length is 81
  Key data type is password key wrap
  Password key wrapping version is 0
  Password scheme used is pkcs5_2
  Password scheme digest algorithm used by password scheme is sha-1
  Authentication algorithm used is sha-256, key length is 32 and value
```

```
        58 63 71 59 69 6a 6d 44 50 74 2f 6e 63 77 46 30 38 41 59 31 74 55 54 6e 72 58 37 4d
50 4b 41 6b 55 56 7a 53 6b 6e
52 44 6a 50 45 3d 00 00 00 00

  Salt length is 8 and value
        54 65 79 45 32 65 39 46 33 64 77 3d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00

  IV length is 16
  Iteration count is 2048
  Key data length is 96
  Encrypted data is
        69 76 77 4d 52 66 37 44 7a 79 45 30 4f 38 58 34 77 77 69 32 43 34 79 6a 68 54 74 6a
50 77 50 6e 62 71 4e 69 48 77
39 62 57 37 4a 4b 45 37 47 30
        4c 41 46 33 54 6d 6f 31 69 78 4a 39 62 47 65 55 36 4c 67 43 74 5a 49 61 30 49 6a 49
41 66 6c 74 2f 6c 46 57 37 41
38 77 44 75 64 63 32 50 77 45
        4d 68 63 54 54 45 33 4f 4f 48 4f 41 74 4f 66 6a 59 47 32 6d 5a 49 35 34 45 6c 30 30
37 37 77 76 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00
```

Use the **show sme cluster <clustername> recovery officer summary <recovery-index>** command to view summary information about a particular SME cluster recovery officer.

```
switch# show sme cluster c recovery officer summary 1
--------------------------------------------------------------------------------
Share     Status    Label        Smartcard    Serial No
--------------------------------------------------------------------------------
1         Set                     No
```

Feature History for SME Disk Management

Table 6-1 lists the release history for this feature.

Table 6-1   Feature History for SME Disk Configuration

Feature Name	Releases	Feature Information
Master Key Rekeying	5.2(6)	A master key is used to wrap the disk keys in the cluster.
Signature and Non-signature Mode Clusters	5.2(6)	Two modes to configure clusters.
SME disk configuration	5.2(1)	SME disk is a new feature that is introduced in Release 5.2(1).

Send documentation comments to mdsfeedback-doc@cisco.com