Planning For SME Installation

This appendix outlines the steps and guidelines that you need to be follow to ensure a successful SME installation. Before installing the application, read the requirements and prerequisites for the following services and features:

SAN Considerations

Collect the following information about the SAN before installing SME:

- Version of the SAN or NX-OS operating system.

Note We suggest that you use version Cisco SAN-OS Release 3.1(1a) or later or NX-OS Release 4.x or later.

- SAN switch vendors.

Note SME is supported on Cisco-only SANs. However, SANs that have switches from other vendors may also be supported on a case-by-case basis.

- SAN topology, including the placement of hosts and targets and number of fabrics.
- Backup host operating system.

- Backup application type and version.
- HBA type and firmware version.
- Tape library and drive types.
- Number of hosts and tape drives.
- SAN topology diagram.
- Types of modules used for ISL connectivity (Generation 1 or Generation 2).

Note This information is required for large SME setups.

- Zoning of the hosts and tape drives and if all the drives are accessible to all the hosts. It is preferred that there is selective accessibility between the hosts and drives.

Interoperability Matrix

Verify the interoperability matrix to be used. If needed, submit an RPQ for new types and versions of SAN components such as tape libraries and drives, or new backup application software versions.

Refer to the Cisco MDS 9000 Family Interoperability Support Matrix.

MSM-18/4 Modules

Collect the following information about MSM-18/4 modules:

- Determine the total throughput requirement and the required number of MSM-18/4 modules. The throughput requirement can be based on either meeting the backup window or based on achieving the line rate throughput for each drive. Refer to the Cisco Storage Media Encryption Design Guide for details.
- Determine the placement of the MSM-18/4 modules. Consult the design guide for sample topology and recommendations.
- For large SME setups, determine if the line cards used for ISLs can scale for the FC Redirect configuration. Refer to the Cisco Storage Media Encryption Design Guide for details.

Note Generation 2 modules are recommended for ISL connectivity.

- Order the appropriate number of SME licenses.

Key Management Center and DCNM-SAN Server

Determine which of the following key management strategies and policies are appropriate for you:

- Use Cisco KMC or KMC with RSA Key Manager for the data center.
- Use PostgreSQL database or Oracle Express as the database.

We recommend that you use PostgreSQL as the database.

- Use shared key mode or unique key per tape.
- Configure key-on-tape mode.
- Use tape recycling.

Note For more information about key policies, refer to the Storage Media Encryption Key Management White Paper and and Chapter 7, "Configuring SME Key Management."

- Use basic or standard or advanced key security mode.

To learn more about master key security modes, refer to Chapter 4, "Configuring SME Cluster Management."

If you are using smart cards in the standard or advanced security mode, ensure that you do the following:

- Install the GemPlus smart card reader drivers on the host used for SME provisioning. These card reader drivers are included in the Cisco MDS 9000 Management Software and Documentation CD-ROM.
- Order the required number of smart cards and readers.
- Identify a host in the customer environment for setting up the DCNM-SAN and KMC.

Refer to Chapter 1, "Storage Media Encryption Overview" to learn about the requirements.

Security

Determine whether you will use SSL for switch-to-KMC communication. If you are using SSL, then do the following tasks:

- Identify whether a self-signed certificate is required or whether the customer will use their own certificate as the root certificate.
- List the names and IP addresses of the switches where the certificates will be installed.
- Install OpenSSL. This application could be installed on the server used for DCNM-SAN and KMC.
  - For the server running Windows operating system, download and install OpenSSL from the following locations:

http://gnuwin32.sourceforge.net/packages/openssl.htm

http://www.slproweb.com/products/Win32OpenSSL.html

The SSL installed should be used to generate keys.

- • Use the OpenSSL application installed at the following location:

C:\Program Files\GnuWin32\bin\openssl.exe

Note For a server running on Linux, the OpenSSL application should already be available on the server.

- Identify the authentication modes used in the SAN, that is local database, TACACS+, or RADIUS.

Communication

Verify that you do the following tasks:

- Allow the following ports on the firewall server:
  - Ports 9333 to 9339 for TCP and UDP for SME cluster communication
  - Ports 8800 and 8900 for Cisco KMC communication
  - Ports HTTP (80) and HTTPS (443) for SME web-client communication
- Use either DNS or IP address (not a mix) for the SAN and KMC communication

Note If you are using IP addresses, refer to the "sme.useIP for IP Address or Name Selection" section on page 2-32 to learn about sme.useIP.

Preinstallation Requirements

Before installing SME, ensure that you do the following tasks:

- Install Java 1.5 or 1.6 on the DCNM-SAN.
- If you are using SSL, install OpenSSL on the server to be used for SSL certificate generation.
- Ensure that essential ports are allowed through the firewall and on the management interface.
- If you are using DNS, ensure that all switches and the KMC server, are mutually reachable (through the ping command) using their DNS names.
- Synchronize the time between all the switches, the KMC and the server used for generating SSL certificates. Configure NTP if required.
- Ensure that the hosts and the tape drives are appropriately zoned.
- Ensure that there is CLI access to the switches.
- Install smart card reader drivers.
- Ensure that the required number of smart cards and readers are available.
- Install the MSM-18/4 modules and SME licenses on the required set of switches.

Preconfiguration Tasks

Before configuring SME, you need to install DCNM-SAN, enable the services, assign roles and users, create fabrics, install SSL certificates, and then provision SME. The following sections describe the steps that you need to follow:

Installing DCNM-SAN

While installing DCNM-SAN, do the following tasks:

- Ensure that the Cisco DCNM-SAN login name and password is the same as the switch login name and password.
- Select the appropriate database.
- Select the appropriate authentication mode.
- Select HTTPS during the installation.

Note To know more about installing DCNM-SAN, refer to the Cisco DCNM-SAN Fundamentals Guide.

Configuring CFS Regions For FC-Redirect

To configure the CFS regions for FC-Redirect, do the following tasks:

Step 1 Configure a switch in the CFS region as shown in the following example:

Example:

```
switch# configure terminal
switch# cfs region 2
switch# fc-redirect
switch# end
```

Repeat this step for all the switches that are included in the specified region.

Step 2 Confirm all the required switches are available in the CFS region by entering the **show fc-redirect peer-switches** command.

Step 3 To migrate existing SME installations to CFS regions for FC-Redirect, delete all the existing FC-Redirect configurations created by the switches in other regions from each switch. To remove the configurations, perform the following steps:

a) Obtain a list of all FC-Redirect configurations by entering the **show fc-redirect configs**.

b) Remove all configurations created by the switches in other regions by using the **clear fc-redirect configs** command. The configurations are removed from the switches but the switches remain active in the region in which they are created.

Enabling SME Services

To enable SME services, do the following tasks:

- Set the FC-Redirect version to 2 (if you are using SAN-OS Release 3.1(1a) or later or NX-OS Release 4.x).

Note To learn about enabling these services, refer to cisco_sme_getting_started.ditamap#map_FD48D7B73A974D59BE491B1598E630AD

Assigning SME Roles and Users

The SME feature provides two primary roles: SME Administrator (sme-admin) and the SME Recovery Officer (sme-recovery). The SME Administrator role also includes the SME Storage Administrator (sme-stg-admin) and SME KMC Administrator (sme-kmc-admin) roles.

To set up the roles and users, note the following guidelines:

- Create the appropriate SME roles, that is, sme-admin and/or sme-stg-admin and sme-kmc-admin, and sme-recovery in the Advanced Master Key Security mode.
- Choose separate users for the sme-kmc-admin role and the sme-stg-admin role to split the responsiblities of key management and SME provisioning. To combine these responsibilities into one role, choose the stg-admin role.
- Use DCNM-SAN to create users for sme-admin, sme-stg-admin, and sme-kmc-admin roles as appropriate.
- In the Advanced mode for the master key, create three or five users under the sme-recovery role.
- Create users on the switches for all of these roles.

To learn more about the roles and their responsibilities refer to the Creating and Assigning SME Roles Using the CLI. For detailed information on creating and assigning roles, refer to the *Security Configuration Guide, Cisco DCNM for SAN and the Cisco MDS 9000 Family NX-OS Security Configuration Guide.*

Creating SME Fabrics

When creating SME fabrics, note the following guidelines:

- Add the SME fabrics using the DCNM-SAN Web Client. Modify the names to exclude switch names from the fabric name.
- The fabric name must remain constant. You cannot change the fabric name after you have configured SME.

Installing SSL Certificates

To create SSL certificates, do the following tasks:

- Follow the procedure specified in Chapter 8Provisioning Certificates to install SSL certificates on the switches and the KMC.
- Use the same password at every step of the installation procedure to simplify the process.
- Restart the DCNM-SAN and KMC after installing the SSL certificates.

Provisioning SME

When provisioning and configuring SME, do the following tasks:

- Create a SME interface for each of the MSM-18/4 modules that will be used for storage media encryption. For more information, refer to Chapter 3 Configuring SME Interfaces
- Follow the steps outlined in Chapter 4 Configuring SME Cluster Management including cluster creation and tape backup group configuration procedures.
- Save the running configuration to startup configuration.

For more informaiton, see the solution guide to SME which contains additional details and requirements for installing SME Disk in specific configurations.

Migrating SME Database Table

Note Data migration is currently supported only for SME Tapes. It is not yet supported for SME Disks.

This appendix describes a database migration utility and also outlines the steps you need to follow to migrate SME tables from one database to another database.

The database migration utility transfers contents of database tables in Oracle Express installation or in PostgreSQL to an Oracle Enterprise installation.

This utility is packaged in the Cisco DCNM for SAN CD starting from NX-OS Software Release 4.1(3) and is available at /software/SMEdbmigrate.zip.

Note The DCNM-SAN application should be installed before the migration process by using the destination database so that DCNM-SAN tables gets created in the destination database.

To migrate database files from the source database to the destination database, follow these steps:

Step 1 Extract the contents of the SMEdbmigrate.zip file to your directory folder. The contents of the file will be as follows:

- SMEdbmigrate.jar
- ojdbc14.jar
- postgresql-8.1.jar
- smedbmigrate.bat
- smedbmigrate.sh
- smedbmigration.properties

Step 2 Right-click the smedbmigration.properties file to open in a text editor. Modify the existing database URL, type, and user name and the destination database URL, type, and user name.

Step 3 To migrate the data files, run the following shell script or batch file:

- sh smedbmigrate.sh (for Unix)
- smedbmigrate.bat (for Windows)

The shell script or the batch file can be executed from any server that has to access to both the source database and the destination database.

Step 4 Enter passwords for the source and destination database when prompted.

The sample output would be as follows:

Example:

```
[root@test-vm-236 SMEdbmigrate]#./smedbmigrate.sh
[INFO] File /root/download/SMEdbmigrate/smedbmigration.properties found
Please enter the passsword for user admin on source database jdbc:postgresql://172.28.233.186:5432/dcmdb
 **********

Please enter the passsword for user admin on destination database
jdbc:postgresql://172.28.255.110:5432/dcmdb **********
*[INFO] Migrating database from jdbc:postgresql://172.28.233.186:5432/dcmdb to
jdbc:postgresql://172.28.255.110:5432/dcmdb
[INFO] Migration Start for SME_SETTINGS
…
…
…
[INFO] Migration complete
[root@test-vm-236 SMEdbmigrate]#
```

Note Run a key retrieval operation to confirm that the migration has been successful.