APPENDIX F

Planning For Cisco SME Installation

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

- SAN Considerations, page F-1
- Interoperability Matrix, page F-2
- MSM-18/4 Modules, page F-2
- Key Management Center and Fabric Manager Server, page F-2
- Security, page F-3
- Communication, page F-3
- Preinstallation Requirements, page F-4
- Preconfiguration Tasks, page F-4
- Provisioning Cisco SME, page F-7

SAN Considerations

Collect the following information about the SAN before installing Cisco SME:

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

  Note It is suggested that you use version Cisco SAN-OS 3.1(1a) or later, or NX-OS 4.x.

- SAN switch vendors.

  Note Cisco 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 Cisco 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 Cisco 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 Cisco SME licenses.

Key Management Center and Fabric Manager 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 Chapter 6, "Cisco SME Key Management."

- Use basic or standard or advanced key security mode.

  To learn more about master key security modes, refer to Chapter 4, "Cisco 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 Cisco 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 Fabric Manager server and KMC.

  Refer to Chapter 1, "Product Overview" to learn about the server 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 Fabric Manager server 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 Cisco SME cluster communication
  - Ports 8800 and 8900 for Cisco KMC communication
  - Ports HTTP (80) and HTTPS (443) for Cisco 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 2-9 to learn about sme.useIP.

Preinstallation Requirements

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

- Install Java 1.5 or 1.6 on the Fabric Manager server.
- 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 Cisco SME licenses on the required set of switches.

Preconfiguration Tasks

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

- Installing Fabric Manager, page F-4
- Configuring CFS Regions For FC-Redirect, page F-5
- Enabling Cisco SME Services, page F-5
- Assigning Cisco SME Roles and Users, page F-6
- Creating Cisco SME Fabrics, page F-6
- Installing SSL Certificates, page F-6

Installing Fabric Manager

While installing the Fabric Manager, do the following tasks:

- Ensure that the Cisco Fabric Manager 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 Fabric Manager, refer to the "Installing Fabric Manager, Fabric Manager Client, and Enabling HTTPS" section on page 2-12 and the *Cisco Fabric Manager Fundamentals Configuration 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:

```
switch# config t
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. Refer to the "show fc-redirect peer-switches" section on page A-34.

Step 3 To migrate existing Cisco 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**. Refer to the "show fc-redirect configs" section on page A-33.

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.

Note For more information, refer to the "clear fc-redirect config" section on page A-3.

Enabling Cisco SME Services

To enable Cisco SME services, do the following tasks:

- Enable clustering on all the Cisco SME switches. For more information, refer to the "Enabling Clustering" section on page 2-3.
- Enable Cisco SME services using either Fabric Manager or Device Manager. For more information, refer to the "Enabling Cisco SME" section on page 2-6.

- Set the FC Redirect version to 2 (if you are using SAN-OS Release 3.1(1a) or later, or NX-OS 4.x). To learn more about enabling the version2 mode, refer to the "fc-redirect version2 enable" section on page A-12.

Note To learn about enabling these services, refer to Chapter 2, "Getting Started."

Assigning Cisco SME Roles and Users

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

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

- Create the appropriate Cisco 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 the Fabric Manager 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 know more about the roles and their responsibilities refer to the "Creating and Assigning Cisco SME Roles and Cisco SME Users" section on page 2-9. For detailed information on creating and assigning roles, refer to the *Cisco Fabric Manager Security Configuration Guide* and the *Cisco MDS 9000 Family NX-OS Security Configuration Guide.*

Creating Cisco SME Fabrics

When creating Cisco SME fabrics, note the following guidelines:

- Add the Cisco SME fabrics using the Fabric Manager 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 Cisco SME.

For more information, refer to the "Adding a Fabric and Changing the Fabric Name" section on page 2-13.

Installing SSL Certificates

To create SSL certificates, do the following tasks:

- Follow the procedure specified in Appendix C, "Provisioning Self-Sign 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 Fabric Manager server and KMC after installing the SSL certificates.

Provisioning Cisco SME

When provisioning and configuring Cisco SME, do the following tasks:

- Create a Cisco 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, "Cisco SME Interface Configuration."
- Follow the steps outlined in Chapter 4, "Cisco SME Cluster Management," including cluster creation and tape backup group configuration procedures.
- Save the running configuration to startup configuration.