CHAPTER 1

Storage Media Encryption Overview

Encrypting storage media in the data center has become a critical issue. Numerous high profile incidents of lost or stolen tape and disk devices have underscored the risk and exposure companies face when sensitive information falls into the wrong hands. To satisfy the most demanding requirements, Cisco MDS 9000 Family Storage Media Encryption (SME) for the Cisco MDS 9000 family switches offers a highly scalable, reliable, and flexible solution that integrates encryption transparently as a fabric service for Fibre Channel SANs.

This chapter provides an overview of the SME and the hardware and software requirements for the product. It contains the following sections:

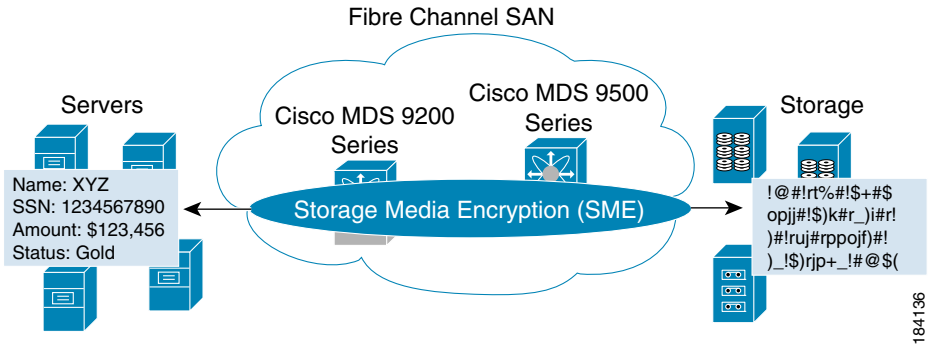
About SME

The SME solution is a comprehensive network-integrated encryption service with enterprise-class key management that works transparently with existing and new SANs. The innovative Cisco network-integrated solution has numerous advantages over competitive solutions available today:

- SME installation and provisioning are both simple and nondisruptive. Unlike other solutions, SME does not require rewiring or SAN reconfiguration.
- Encryption engines are integrated on the Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4), the Cisco MDS 9222i Multiservice Module Switch, and the 16-Port Gigabit Ethernet Storage Services Node (SSN-16), which eliminates the need to purchase and manage extra switch ports, cables, and appliances.
- Traffic from any virtual SAN (VSAN) can be encrypted using SME, enabling flexible, automated load balancing through network traffic management across multiple SANs.
- No additional software is required for provisioning, key, and user role management; SME is integrated into Cisco DCNM for SAN (DCNM-SAN), which reduces operating expenses.

Figure 1-1 shows the integration of SME with SAN fabrics to offer seamless management of data encryption.

Figure 1-1 SME



This section covers the following topics:

- SME Features, page 1-2
- SME Terminology, page 1-6
- Supported Topologies, page 1-7
- In-Service Software Upgrade in SME, page 1-9

SME Features

The Cisco MDS 9000 Family of intelligent directors and fabric switches provide an open, standards-based platform for hosting intelligent fabric applications and services. As a platform, the Cisco MDS 9000 family switches provide all essential features required to deliver secure, highly available, enterprise-class Fibre Channel storage area network (SAN) fabric services. Cisco has integrated encryption for data-at-rest as a transparent fabric service to take full advantage of this platform.

SME is a standards-based encryption solution for heterogeneous disks, tape libraries, and virtual tape libraries. SME is managed with Cisco DCNM-SAN and a command-line interface (CLI) for unified SAN management and security provisioning. SME includes the following comprehensive built-in key management features:

- Transparent Fabric Service, page 1-3
- Encryption, page 1-3
- SME Roles, page 1-3
- Key Management, page 1-4
- Clustering, page 1-5
- FC-Redirect, page 1-6
- Server-Based Discovery for Provisioning Disks and Tapes, page 1-6
- Target-Based Load Balancing, page 1-6

Transparent Fabric Service

Cisco employs a Fibre Channel redirect scheme that automatically redirects the traffic flow to an MSM-18/4 module, a MDS 9222i switch, or a SSN-16 module anywhere in the fabric. There are no appliances in-line in the data path and there is no SAN rewiring or reconfiguration.

Encryption

SME uses strong, IEEE-compliant AES 256 encryption algorithms to protect data at rest. Advanced Cisco MDS 9000 SAN-OS and NX-OS software security features, such as Secure Shell (SSH), Secure Sockets Layer (SSL), RADIUS, and Fibre Channel Security Protocol (FC-SP) provide the foundation for the secure architecture.

SME uses the NIST-approved random number standard to generate the keys for encryption.

Encryption and compression services are transparent to the hosts and storage devices.

Encryption Algorithms

The IEEE-approved standard for encryption of disk drives is IEEE 1619—Standard Architecture for Encrypted Shared Storage Media (1619.1 for tape drives). It specifies the XTS encryption mode commonly used for disk encryption. The IEEE Security in Storage Working Group (SISWG) was investigating the possibility of submitting the XTS mode to NIST for consideration as an Approved Mode of Operation for FIPS 140-2 certification. It uses a narrow-block encryption algorithm, and the standardization process for a wide-block algorithm is currently in progress as 1619.2. Other encryption algorithms for consideration are LRW-AES and AES-CBS. Draft versions of the IEEE 1619 standard had used LRW-AES, which was later replaced by XTS-AES.

SME Roles

SME services include the following four configuration and security roles:

- SME Administrator
- SME Storage Administrator
- SME Key Management Center (KMC) Administrator
- SME Recovery Officer

The SME Administrator configures and maintains SME. This role can be filled by multiple storage network administrators. The SME Storage Administrators are responsible for SME provisioning operations and the SME KMC Administrators are responsible for the SME KMC administration operations. The security officer may be assigned the SME KMC Administrator role in some scenarios.

Note SME Administrator role includes the SME Storage Administrator and the SME KMC Administrator roles.

The SME Recovery Officers are responsible for key recovery operations. During SME configuration, additional Recovery Officers can be added. SME Recovery Officers play a critical role in recovering the key database of a deactivated cluster and they are responsible for protecting the master key. The role of the SME Recovery Officer separates master key management from SME administrations and operations. In some organizations, a security officer may be assigned to this role.

At the advanced security level, a quorum of SME Recovery Officers is required to perform recovery procedures. The default is 2 out of 5. In this case 2 of the 5 recovery officers are required to unlock the master key.

For additional information on SME Administrator and SME Recovery Officer roles, see the "Creating and Assigning SME Roles and SME Users" section on page 2-19.

Key Management

Cisco Key Management Center (KMC) provides essential features such as key archival, secure export and import, and key shredding.

Key management features include the following:

- Master key resides in password protected file or in smart cards.
  - If the cluster security mode is set to Basic, the master key resides in the password protected file.
  - If the cluster security mode is set to Standard, the master key resides in only one smart card. And the same smart card is required to recover the master key.
  - If the cluster security mode is set to Advanced, the master key resides in multiple smart cards. Quorum (2 out of 3 or 2 out of 5 or 3 out of 5) of smart cards are required to recover the master key based on the user selection.
- Unique key per tape for an SME tape cluster.
- Unique key per LUN for an SME disk cluster.
- Keys reside in clear-text only inside a FIPS boundary.
- Tape keys and intermediate keys are wrapped by the master key and deactivated in the CKMC.
- Disk keys are wrapped by the cluster master key and deactivated in the CKMC.
- Option to store tape keys on tape media.

The centralized key lifecycle management includes the following:

- Archive, shred, recover, and distribute media keys.
  - Integrated into DCNM-SAN.
  - Secure transport of keys.
- End-to-end key management using HTTPS/SSL/SSH.
  - Access controls and accounting.
  - Use of existing AAA mechanisms.

The Cisco KMC provides dedicated key management for SME, with support for single and multisite deployments. The Cisco KMC performs key management operations.

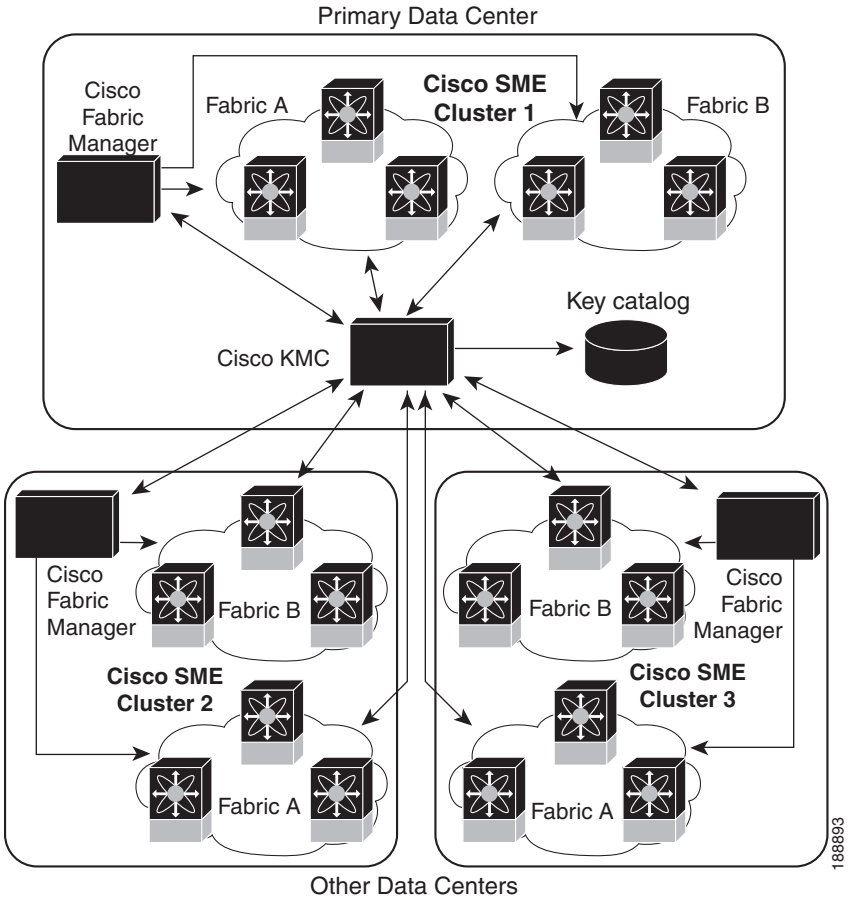
The Cisco KMC is either integrated or separated from DCNM-SAN depending on the deployment requirements.

Single site operations can be managed by the integration of the Cisco KMC in DCNM-SAN. In multisite deployments, the centralized Cisco KMC can be used together with the local DCNM-SAN servers that are used for fabric management. This separation provides robustness to the KMC and also supports the SME deployments in different locations sharing the same Cisco KMC.

Figure 1-2 shows how Cisco KMC is separated from DCNM-SAN for a multisite deployment.

A Cisco KMC is configured only in the primary data center and DCNM-SAN servers are installed in all the data centers to manage the local fabrics and provision SME. The SME provisioning is performed in each of the data centers and the tape devices and backup groups in each of the data centers are managed independently.

Figure 1-2 Multisite Setup in Cisco KMC



In the case of multisite deployments when the Cisco KMC is separated from DCNM-SAN, fabric discovery is not required on the Cisco KMC installation. The clusters that have connection to the Cisco KMC will be online and the clusters that are not connected, but are not deactivated, appear as offline. The SME clusters that are deleted from the fabric appear as deactivated.

The high availability Cisco KMC server consists of a primary server and a secondary server. When the primary server is unavailable, the cluster connects to the secondary server and fails over to the primary server once the primary server is available. The high availability KMC will be available after you configure the high availability settings in DCNM-SAN Web Client. For more information on the configuration, see the "Choosing High Availability Settings" section on page 7-9.

Clustering

Cluster technology provides reliability and availability, automated load balancing, failover capabilities, and a single point of management.

FC-Redirect

SME performance can easily be scaled up by adding more Cisco MDS 9000 Family switches or modules. The innovative Fibre Channel redirect capabilities in Cisco MDS 9000 NX-OS enable traffic from any switch port to be encrypted without SAN reconfiguration or rewiring.

Server-Based Discovery for Provisioning Disks and Tapes

SME provides discovery of backend targets using the identity of the host during a session establishment.

Target-Based Load Balancing

The SME cluster consists of a set of switches (in a dual-fabric environment) running the SME application. Clustering offers target-based load balancing of SME application services. The cluster infrastructure allows the SME application to communicate and coordinate to maintain consistency and high availability.

Load balancing is achieved by distributing ownership of the various metadata objects throughout the cluster. SME assigns hosts to the available SME interfaces using the following algorithm:

- All hosts for a given target port are always assigned to the same SME interface.
- If a target port is connected to one of the SME switches, an interface is selected based on the load from the target-connected switch. That is, the target locality is considered when choosing a SME interface for a target.
- If a target is connected to a switch that has no SME interface, then the target is assigned to the least loaded available interface in the SME cluster.

In target-based load balancing, the load on an interface refers to the number of targets assigned to that interface.

Caution SME provides a load balancing CLI that allows you to rebalance the targets assigned to the available SME interfaces in the cluster. However, the **load balancing** command is disruptive to the traffic. Ensure that you execute this command at a scheduled downtime, otherwise, the existing traffic will be affected.

SME Terminology

The following SME-related terms are used in this book:

- SME interface—The security engine in the MSM-18/4 module or fixed slot of a Cisco MDS 9222i fabric switch. Each MSM-18/4 module and MDS 9222i switch has one security engine.
- SME cluster—A network of MDS switches that are configured to provide the SME functionality; each switch includes one or more MSM-18/4 modules and each module includes a security engine. Includes one or more nodes or switches for high availability (HA) and load balancing.
- Fabric—A physical fabric topology in the SAN as seen by DCNM-SAN. There can be multiple VSANs (logical fabrics) within the physical fabric.
- Tape group—A backup environment in the SAN. This consists of all the tape backup servers and the tape libraries that they access.
- Tape device—A tape drive that is configured for encryption.
- Tape volumes—A physical tape cartridge identified by a barcode for a given use.

- Tape volume group—A logical set of tape volumes that are configured for a specific use, for example, a group of tape volumes used to backup a database.
- Disk group—The disks that are grouped functionally to form disk groups.
- Disk—Disk is a LUN. A LUN is a logical unit that is exported to the host by the storage controller.
- IT-NEXUS—Initiator or Target pWWNs that defines a host to target connection.
- SME node—Each switch in the cluster is called an SME node and plays a role in determining if the cluster has a quorum.
- Cisco Key Management Center (CKMC)—A component of DCNM-SAN that stores the encryption keys.
- Master key—An encryption key generated when an SME cluster is created. The master key encrypts the tape volume keys and tape keys and it is required to decrypt those keys in order to retrieve encrypted data.
- Media key—A key that is used for encrypting and authenticating the data on specific tapes.
- Disk key—A key that is used for encrypting and authenticating the data on specific disks.
- SmartCard—A card (approximately the size of a credit card) with a built-in microprocessor and memory used for authentication.
- SME Administrator—An administrator who configures SME. This role includes the Cisco Storage Administrator role where the administrator manages the SME operations and the SME KMC Administrator role where the administrator is responsible for the SME key management operations.
- Storage Administrator —An administrator who manages the SME operations.
- SME KMC Administrator—An administrator who is responsible for the SME key management operations.
- SME Recovery Officer—A data security officer entrusted with smart cards and the associated PINs. Each smart card stores a share of the cluster master key. Recovery officers must present their cards and PINs to recover the key database of a deactivated cluster. A quorum of recovery officers are required to execute this operation.

Supported Topologies

SME supports single-and dual-fabric topologies. The Cisco MSM-18/4 module, the MDS 9222i switch, and the SSN-16 provides the SME engines used by SME to encrypt and compress data-at-rest. Multiple modules can be deployed in a Fibre Channel fabric to easily scale-up performance, to enable simplified load balancing, and to increase availability. In a typical configuration, one MSM-18/4 module is required in each SME cluster.

SME clusters include designated backup servers, tape libraries, and one or more MDS switches running Cisco SAN-OS Release 3.2(2c) or later or NX-OS 4.x or later. One cluster switch must include an MSM-18/4 module. With easy-to-use provisioning, traffic between any host and tape on the fabric can utilize the SME services.

Required SME engines are included in the following Cisco products:

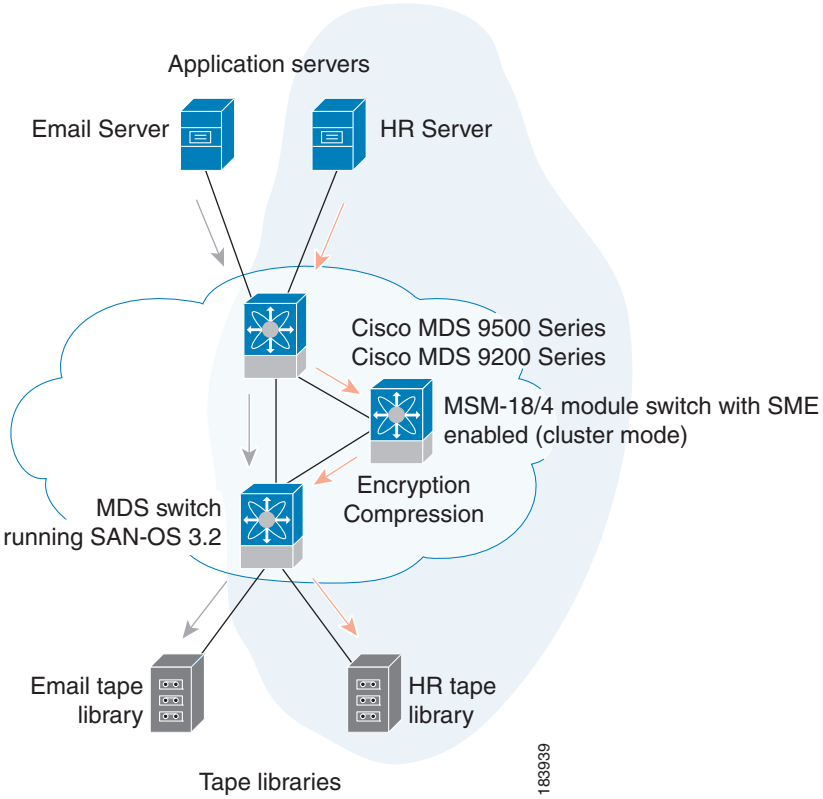
- Cisco MDS 9000 Family 18/4-Port Multiservice Module (MSM-18/4)
- Cisco MDS 9222i Multiservice Module Switch
- Cisco MDS 16-Port Storage Services Node (SSN-16)

Single-Fabric Topology for Tape

Figure 1-3 shows a single-fabric topology in which the data from the HR server is forwarded to the Cisco MSM-18/4 module. The Cisco MSM-18/4 module can be anywhere in the fabric. SME does a one-to-one mapping of the information from the host to the target and forwards the encrypted data to the dedicated HR tape. SME also tracks the barcodes on each encrypted tape and associates the barcodes with the host servers.

Figure 1-3 shows encrypted data from the HR server is compressed and stored in the HR tape library. Data from the email server is not encrypted when backed up to the dedicated email tape library.

Figure 1-3 SME: Single-Fabric Topology



Note Tape devices should be connected to core switches such as an MDS 9500 Series switch or MDS 9222i switch running Cisco SAN-OS Release 3.2(2c) or later or Cisco NX-OS Release 4.x or later.

Encryption and compression services are transparent to the hosts and storage devices. These services are available for devices in any virtual SANs (VSANs) in a physical fabric and can be used without rezoning.

Single-Fabric Topology for Disk

A single-fabric topology in which the data from the HR server is forwarded to the Cisco MSM-18/4 module, Cisco MDS 922i switch or SSN-16 module. The Cisco MSM-18/4 module, Cisco MDS 9222i switch or SSN-16 module can be anywhere in the fabric. SME does a one-to-one mapping of the information from the host to the target and forwards the encrypted data to the dedicated HR disk.

Note SME disk also supports dual-fabric topology with which the data can be encrypted on all the paths.

Disk devices should be connected to core switches, such as an MDS 9500 Series switch or an MDS 9222i switch, running on Cisco NX-OS Release 5.2(1) or later.

Encryptions are transparent to the hosts and storage devices. These services are available for devices in any virtual SANs (VSANs) in a physical fabric and can be used without rezoning.

In-Service Software Upgrade in SME

In-Service Software Upgrade (ISSU) is a comprehensive, transparent software upgrade capability that allows you to add new features and services without any disruption to the traffic.

In a cluster, which has the MDS 9222i switch as nodes, if the nodes are not able to communicate, then the node having the lowest node identifier (node ID) remains in the cluster while the other node leaves the cluster. However, when an ISSU is performed on a node having the lowest node identifier, a complete loss of the cluster results since both the nodes leave the cluster.

This undesirable situation is addressed in a two-node cluster as follows:

- The upgrading node sends a message to the other node of the intent to leave the cluster. The upgrading node can either be a master node or a slave node.
- The remaining node remains in the cluster and performs the role of the master node if it was a slave node. This node continues to remain in the cluster with the quorum intact.
- After the ISSU is completed and the switches boots up, the upgraded node rejoins the cluster as a slave node.

SME disk has disk-specific ISSU restrictions and limitations. For more information about these restrictions, see Chapter 6, “Configuring SME Disks.”

Note This feature is tied to the internals of ISSU logic and no additional command needs to be executed for this purpose.

About MIBs

The MIB module manages SME service. SME is an encryption service provided by an encryption node residing on a line card in a storage device. It receives clear-text data from the host, encrypts and then sends it to be written to tape or disk. It does the reverse in the opposite direction so the service is completely transparent to the host. The purpose of this service is to enhance data security in case the tape or disk is lost or stolen.

As with any services important the user requires that provides some level of fault tolerance in a graceful manner. SME provides fault tolerance by allowing encryption nodes to be grouped into a cluster. Nodes in the same cluster immediately take over the work of a failed node so that the user does not experience service disruption.

Software and Hardware Requirements

This section includes the following topics:

Software Requirements

All MDS switches in the SME cluster must be running the current release of Cisco SAN-OS Release 3.2(2c) or later, or Cisco NX-OS 4.x or later software for SME Tape. Cisco NX-OS Release 5.2(1) or later software is required for SME Disk. The software requirements include the following:

- DCNM-SAN must be running Cisco SAN-OS Release 3.2(2c) or later or Cisco NX-OS Release 4.x or later for SME Tape.
- The Cisco MDS switches attached to tape devices must be running Cisco SAN-OS Release 3.2(2c) or later or Cisco NX-OS Release 4.x or later for SME Tape.
- All switches that include MSM-18/4 modules must be running Cisco SAN-OS Release 3.2(2c) or later or Cisco NX-OS Release 4.x or later software for SME Tape.
- DCNM-SAN must be running Cisco NX-OS Release 5.2(1) for SME Disk.
- All Cisco MDS switches in the SME cluster enabled for disks must be running Cisco NX-OS Release 5.2(1).
- All switches that include MSM-18/4 modules, MDS 9222i switch or SSN-16 modules must be running Cisco NX-OS Release 5.2(1) for SME Disk.

Hardware Requirements

SME requires at least one encryption service engine in each cluster. The SME engines on the required modules provide the transparent encryption and compression services to the hosts and storage devices. To take full advantage of the standard and advanced security levels, a smart card reader is required.

For detailed information on required hardware and installing required hardware, refer to the specific installation guides. For information about ordering hardware, refer to http://www.cisco.com/en/US/ordering/index.shtml.

This section includes information about the following required hardware:

Cisco MDS 9000 Family 18/4-Port Multiservice Module

The Cisco MDS 9000 Family 18/4-Port Multiservice module (MSM-18/4) provides 18 autosensing 1-, 2-, and 4-Gbps Fibre Channel ports and four Gigabit Ethernet IP services ports. The MSM-18/4 module provides multiprotocol capabilities such as Fibre Channel, Fibre Channel over IP (FCIP), Small Computer System Interface over IP (iSCSI), IBM Fiber Connectivity (FICON), and FICON Control Unit Port (CUP) management.

The MSM-18/4 module provides 18 4-Gbps Fibre Channel interfaces for high-performance SAN and mainframe connectivity and four Gigabit Ethernet ports for FCIP and iSCSI storage services. Individual ports can be configured with hot-swappable shortwave, longwave, extended-reach, coarse wavelength-division multiplexing (CWDM) or dense wavelength-division multiplexing (DWDM) Small Form-Factor Pluggables (SFPs) for connectivity up to 125 miles (200 km).

The MSM-18/4 module can minimize latency for disk and tape through FCIP write acceleration and FCIP tape write and read acceleration. The MSM-18/4 module provides up to 16 virtual Inter-Switch Link (ISL) connections on the four 1-Gigabit Ethernet ports through tunneling, and provides up to 4095 buffer-to-buffer credits that can be assigned to a single Fibre Channel Port.

The MSM-18/4 provides intelligent diagnostics, protocol decoding, and network analysis tools with the integrated Call Home capability.

Note Cisco MDS 9000 Series switches running Cisco SAN-OS Release 3.2(2c) or later or Cisco NX-OS Release 4.x or later support the MSM-18/4 module for SME tape.

Cisco MDS 9000 Series switches running Cisco NX-OS Release 5.2(1) support the MSM-18/4 and SSN-16 modules for SME disk.

For additional information, refer to the *Cisco MDS 9500 Series Hardware Installation Guide*.

Cisco MDS 9222i Multiservice Modular Switch

The Cisco MDS 9222i Multiservice Modular switch includes an integrated supervisor module (in slot 1) that provides the control and management functions of the Cisco MDS 9222i switch and it provides an 18-Port Fibre Channel switching and 4-Port Gigabit Ethernet IP services module. The Cisco MDS 9222i built-in supervisor module provides multiple communication and control paths to avoid a single point of failure. The Cisco MDS 9222i supervisor module has a PowerPC PowerQUICC III class processor, 1 GB of DRAM, and an internal CompactFlash card that provides 1 GB of storage for software images.

The Cisco MDS 9222i switch includes a modular expansion slot to host Cisco MDS 9000 Family switching and services modules. For additional information, refer to the *Cisco MDS 9200 Series Hardware Installation Guide*.

Note The Cisco MDS 9222i switch requires Cisco SAN-OS Release 3.2(2c) or later or Cisco NX-OS Release 4.x or later for SME tape.

The Cisco MDS 9222i switch requires Cisco NX-OS Release 5.2(1) for SME disk.

Cisco MDS 16-Port Storage Services Node

The Cisco MDS 9000 Family 16-Port Storage Services Node (SSN-16) hosts four independent service engines which can be individually and incrementally enabled to scale as business requirements grow. The SSN-16 configuration is based on the single service engine of the Cisco MDS 9000 Family 18/4-Port Multiservice module and the four-to-one consolidation provides hardware savings and frees up slots in the MDS 9500 series chassis.

The SSN-16 seamlessly integrates into the Cisco MDS 9500 Series Multilayer directors and the Cisco MDS 9222i Multiservice Modular switch. Each of the four service engines supports four Gigabit Ethernet IP storage services ports for a total of 16 ports of Fibre Channel over IP (FCIP) connectivity. The traffic can be switched between an IP port and any Fibre Channel port on Cisco MDS 9000 Family switches.

The SSN-16 supports the full range of services available on other Cisco MDS 9000 Family modules including VSAN, security, and traffic management. Features such as I/O Accelerator (IOA), SME Disk and Tape, and FCIP can be configured in different octeons in a single SSN-16 module.

By running four separate, concurrent applications on one module, SSN-16 provides the following functions:

- Provides better disaster recovery and continuity solutions for mission critical applications.
- Minimizes the number of devices required, which improves the reliability.
- Consolidates the management with a single module, which provides end-to-end visibility.
- Facilitates solution-level performance optimization.

The SSN-16 module provides transparent services to any port in a fabric and does not require additional SAN reconfiguration and rewiring. The module does not require the host or target to be directly attached and is available with multimodule clustering and balancing.

The SSN-16 module supports up to four SME interfaces per module and provides higher scalability and improved performance of up to 20 percent on the MSM-18/4 module and 9222i switches.

Note Cisco MDS 9500 Series switches running Cisco NX-OS Release 4.2(1) or later support the SSN-16.

For additional information, refer to the *Cisco MDS 9500 Series Hardware Installation Guide*.

FC-Redirect-Capable Switches

Note In Cisco MDS NX-OS Release 5.2(x), you cannot install a FCoE module in a switch that is running DMM, SME, or IOA.

SME requires that each target switch be FC-Redirect capable. FC-Redirect is not supported on the following switches:

- Cisco MDS 9120 switch
- Cisco MDS 9140 switch
- Cisco MDS 9124 switch
- Cisco MDS 9134 switch
- Cisco MDS 9020 switch

Note SME does not support any FCoE connected devices including devices connected through the MDS FCoE linecard (DS-X9708-K9).

Note Disk devices, tape devices, and tape libraries are not supported in these edge switches. Disks and tapes cannot be connected to these switches.

Smart Card Readers

To employ standard and advanced security levels, SME requires the following:

- Smart Card Reader for SME (DS-SCR-K9)
- Smart Card for SME (DS-SC-K9)

The smart card reader is a USB device that is connected to a management workstation. The management workstation is used to configure the SME cluster. The smart card reader requires the smart card drivers that are included on the installation CD. These must be installed on the management workstation where the reader is attached.

Note The smart card reader is supported on Windows-only platforms. This support includes only the Windows 4 64-bit and Windows XP 32-bit platforms.

For the newly installed smart card drivers to work efficiently with the smart card readers, you must stop all Microsoft smart card services.

SME Prerequisites

This section describes the following requirements:

Java Cryptography Extension Requirement

SME requires Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 5C0 (for JRE 1.5). You will need to extract and copy the local_policy.jar and the US_export_policy.jar files to the <DCNM install path>\dcm\java\jre1.6\lib\security\. You can obtain these files from the DCNM-SAN Installation CD.

Zoning Requirement

Zoning requires internal virtual N ports that are created by SME in the default zone. The default zone must be set to deny and these virtual N ports must not be zoned with any other host or target.

For information on zoning, refer to the *Fabric Configuration Guide, Cisco DCNM for SAN* and the *Cisco MDS 9000 Family NX-OS Fabric Configuration Guide*.

FC-Redirect Requirements

FC-Redirect requirements include the following:

- The MDS switch with the MSM-18/4 module installed or the MDS 9222i switch needs to be running Cisco MDS SAN-OS Release 3.2(2c) or later, or Cisco NX-OS Release 4.x or later.
- The target must be connected to an MDS 95XX, 9216, or 9222i switch running Cisco MDS SAN-OS Release 3.2(2c) or later, or Cisco NX-OS Release 4.x or later.
- 32 targets per MSM-18/4 module can be FC-redirected.
- Each FC-redirected target can be zoned to 16 hosts or less.
- CFS should be enabled on all required switches for FC-Redirect.
- SME servers, disk targets, and tape devices should not be part of an IVR zone set.
- Advanced zoning capabilities such as quality of service (QoS), logical unit number (LUN) zoning, and read-only LUNs must not be used for FC-Redirect hosts and targets.

SME Security Overview

SME transparently encrypts and decrypts data inside the storage environment without slowing or disrupting business critical applications.

In SME Tape, SME generates a master key, tape volume keys, and tape keys. The keys are encrypted in a hierarchical order: the master key encrypts the tape volume keys and the tape keys.

In SME Disk, SME generates a master key and disk keys. The keys are encrypted in a hierarchical order: the master key encrypts the disk keys.

The keys are also copied to the key catalog on the Cisco KMC server for backup and archival. Eventually inactive keys are removed from the fabric, but they are retained in the Cisco KMC catalog. The keys can be retrieved automatically from the Cisco KMC by the SME services in the fabric if needed again.

A single Cisco KMC can be used as a centralized key repository for multiple fabrics with SME services if desired. Key catalog import and export capabilities are also provided to accommodate moving tape media to different fabrics in environments with multiple Cisco KMC servers. Backup applications can be used to archive the key catalogs for additional protection.

Note SME cluster can be configured either for SME Disk or for SME Tape. Both Tape and Disk configurations cannot be configured under a same cluster. A cluster can be configured only for one of them.

Additional Security Capabilities

Additional security capabilities offered by Cisco NX-OS complete the SME solution. For example, RADIUS and TACACS+ servers can be used to authenticate, authorize, and provide accounting (AAA) for SME administrators. Management of SME can be limited to authorized administrators using

role-based access controls (RBACs). When communication occurs from the DCNM-SAN to cluster nodes, the secure shell (SSHv2) protocol provides message integrity and privacy. PKI certificates can be configured in the CKMC and cluster nodes to enable trustpoint (SSL-protected transport).