



System Management Overview

You can use the system management features to monitor and manage a switch using Cisco MDS NX-OS software. These features include Call Home, SNMP, RMON, SPAN, and the Embedded Event Manager (EEM).

- [Cisco Fabric Services, on page 1](#)
- [System Messages, on page 1](#)
- [Call Home, on page 2](#)
- [Scheduler, on page 2](#)
- [System Processes and Logs, on page 2](#)
- [Embedded Event Manager, on page 2](#)
- [SNMP, on page 3](#)
- [RMON, on page 3](#)
- [Pathtrace, on page 3](#)
- [Domain Parameters, on page 3](#)
- [SPAN, on page 3](#)
- [Fabric Configuration Server, on page 4](#)
- [Uniform Timestamps, on page 4](#)

Cisco Fabric Services

The Cisco MDS NX-OS software uses the Cisco Fabric Services (CFS) infrastructure to enable efficient database distribution and to promote device flexibility. CFS simplifies SAN provisioning by automatically distributing configuration information to all switches in a fabric.

For information on configuring CFS, see [Using the CFS Infrastructure](#).

System Messages

System messages are monitored remotely by accessing the switch through Telnet, SSH, or the console port, or by viewing the logs on a system message logging server. Log messages are not saved across system reboots.

For information about configuring system messages, see [Configuring System Message Logging](#).

Call Home

Call Home provides email-based notification of critical system events. A versatile range of message formats are available for optimal compatibility with pager services, standard email, or XML-based automated parsing applications. Common uses of this feature may include direct paging of a network support engineer, email notification to a Network Operations Center, and utilization of Cisco Smart Call Home services for direct case generation with the Technical Assistance Center.

For information about configuring Call Home, see [Configuring Call Home](#).

Scheduler

The Cisco MDS command scheduler feature helps you schedule configuration and maintenance jobs in any switch in the Cisco MDS 9000 Family switches. You can use this feature to schedule jobs on a one-time basis or periodically. The Cisco NX-OS command scheduler provides a facility to schedule a job (set of CLI commands) or multiple jobs at a specified time in the future. The jobs can be executed once at a specified time in the future or at periodic intervals.

For information on configuring the Cisco MDS command scheduler feature, see [Scheduling Maintenance Jobs](#).

System Processes and Logs

The health of a switch can be monitored by various system processes and logs. The Online Health Management System (system health) is a hardware fault detection and recovery feature. This Health Management System ensures the general health of switching, services, and supervisor modules in any switch in the Cisco MDS 9000 Family.

For information on monitoring the health of the switch, see [System Status Monitoring](#).

Embedded Event Manager

Embedded Event Manager (EEM) monitors events that occur on your device and takes action to recover or troubleshoot these events, based on your configuration. EEM consists of three major components:

- Event statements—Events to monitor from another Cisco NX-OS component that may require some action, workaround, or notification.
- Action statements —An action that EEM can take, such as sending an email or disabling an interface, to recover from an event.
- Policies—An event paired with one or more actions to troubleshoot or recover from the event.

For information on configuring EEM, see [About Embedded Event Manager](#).

SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. In all Cisco MDS 9000 Family switches, three SNMP versions are available: SNMPv1, SNMPv2c, and SNMPv3. The CLI and SNMP use common roles in all switches in the Cisco MDS 9000 Family. You can use SNMP to modify a role that was created using the CLI and vice versa.

Users, passwords, and roles for all CLI and SNMP users are the same. A user configured through the CLI can access the switch using SNMP (for example, the DCNM-SAN or the Device Manager) and vice versa.

For information on configuring SNMP, see [Configuring SNMP](#).

RMON

RMON is an Internet Engineering Task Force (IETF) standard monitoring specification that allows various network agents and console systems to exchange network monitoring data. You can use the RMON alarms and events to monitor Cisco MDS 9000 Family switches running the Cisco SAN-OS Release 2.0(1b) or later or Cisco Release NX-OS 4.1(3) or later software.

For information on configuring RMON, see [Configuring RMON](#).

Pathtrace

The Pathtrace feature builds on the Traceroute feature to provide information about interfaces, such as ingress and egress interface names and the number of transmitted and received frames and errors, at each hop in the path between 2 devices in a fabric. Pathtrace provides an end-to-end view of the shortest path without the need to connect to individual switches and check the Fabric Shortest Path First (FSPF) topology hop by hop.

For information on using the Pathtrace feature, see [Using Pathtrace](#).

Domain Parameters

The Fibre Channel domain (fcdomain) feature performs principal switch selection, domain ID distribution, FC ID allocation, and fabric reconfiguration functions as described in the FC-SW-2 standards. The domains are configured on a per-VSAN basis. If you do not configure a domain ID, the local switch uses a random ID.

For information on configuring the Fibre Channel domain feature, see [Configuring Domain Parameters](#).

SPAN

The Switched Port Analyzer (SPAN) feature is specific to switches in the Cisco MDS 9000 Family. It monitors network traffic through a Fibre Channel interface. Traffic through any Fibre Channel interface can be replicated to a special port called the SPAN destination port (SD port). Any Fibre Channel port in a switch can be

configured as an SD port. Once an interface is in SD port mode, it cannot be used for normal data traffic. You can attach a Fibre Channel analyzer to the SD port to monitor SPAN traffic.

For information on SPAN feature, see [Monitoring Network Traffic Using SPAN](#).

Fabric Configuration Server

The Fabric Configuration Server (FCS) provides discovery of topology attributes and maintains a repository of configuration information of fabric elements. A management application is usually connected to the FCS on the switch through an N port. In the Cisco MDS 9000 Family switch environment, multiple VSANs constitute a fabric, where one instance of the FCS is present per VSAN.

For information on configuring FCS, see [Configuring Fabric Configuration Server](#).

Uniform Timestamps

While debugging issues on a switch, it is critical to arrange logs in chronological order to understand the sequence of events that resulted in the issue. MDS logs use different time formats and it is tedious to merge and sort them to understand the timeline of events. The Uniform Timestamps feature allows onboard syslogs, accounting logs, and logs of various MDS software components to use a uniform timestamp format. This allows quick merging and sorting of multiple logs together to build a complex timeline onboard the switch. Logs can also be exported from the switch (by using the **show tech-support** command and so on) and processed easily by hand, scripts, or data-mining applications.

This feature enables RFC 5424 format timestamps. This format is supported by many other devices and vendors so that logs can also be merged with other products to build an end to end timeline through a fabric. Ensure that clocks on all the devices are synchronized before attempting this.

This feature does not change the format of syslogs that are exported to an external syslog server via the syslog protocol.

For more information, see the **system timestamp format** command in the [Cisco MDS 9000 Series Command Reference, Release 8.x](#).

Configuring Uniform Timestamps

To enable RFC 5424 compliant timestamping in logs, perform the step below:

Procedure

- Step 1** Enter global configuration mode:
- ```
switch# configure terminal
```
- Step 2** Enable RFC 5424 compliant timestamping in logs:
- ```
switch# system timestamp format rfc5424
```
-