CHAPTER 3

Configuring System Message Logging

This chapter describes how to configure system message logging on Cisco DCNM-SAN. It includes the following sections:

Information About System Message Logging

With the system message logging software, you can save messages in a log file or direct the messages to other devices. By default, the switch logs normal but significant system messages to a log file and sends these messages to the system console. This feature provides you with the following capabilities:

- Provides logging information for monitoring and troubleshooting
- Allows you to select the types of captured logging information
- Allows you to select the destination server to forward the captured logging information properly configured system message logging server.

You can monitor system messages by clicking the Events tab on DCNM-SAN or by choosing **Logs > Events > Current** on Device Manager. You can also monitor system messages remotely by accessing the switch through Telnet, SSH, or the console port, or by viewing the logs on a system message logging server.

Note When the switch first initializes, the network is not connected until initialization completes. Therefore, messages are not redirected to a system message logging server for a few seconds.

Log messages are not saved across system reboots. However, a maximum of 100 log messages with a severity level of critical and below (levels 0, 1, and 2) are saved in NVRAM.

Table 3-1 describes some samples of the facilities supported by the system message logs.

Table 3-1 Internal Logging Facilities

Facility Keyword	Description	Standard or Cisco MDS Specific
acl	ACL manager	Cisco MDS 9000 Family specific
all	All facilities	Cisco MDS 9000 Family specific
auth	Authorization system	Standard
authpriv	Authorization (private) system	Standard
bootvar	Bootvar	Cisco MDS 9000 Family specific
callhome	Call Home	Cisco MDS 9000 Family specific
cron	Cron or at facility	Standard
daemon	System daemons	Standard
fcc	FCC	Cisco MDS 9000 Family specific
fcdomain	fcdomain	Cisco MDS 9000 Family specific
fcns	Name server	Cisco MDS 9000 Family specific
fcs	FCS	Cisco MDS 9000 Family specific
flogi	FLOGI	Cisco MDS 9000 Family specific
fspf	FSPF	Cisco MDS 9000 Family specific
ftp	File Transfer Protocol	Standard
ipconf	IP configuration	Cisco MDS 9000 Family specific
ipfc	IPFC	Cisco MDS 9000 Family specific
kernel	Kernel	Standard
local0 to local7	Locally defined messages	Standard
lpr	Line printer system	Standard
mail	Mail system	Standard
mcast	Multicast	Cisco MDS 9000 Family specific
module	Switching module	Cisco MDS 9000 Family specific
news	USENET news	Standard
ntp	NTP	Cisco MDS 9000 Family specific
platform	Platform manager	Cisco MDS 9000 Family specific
port	Port	Cisco MDS 9000 Family specific
port-channel	PortChannel	Cisco MDS 9000 Family specific
qos	QoS	Cisco MDS 9000 Family specific
rdl	RDL	Cisco MDS 9000 Family specific
rib	RIB	Cisco MDS 9000 Family specific
rscn	RSCN	Cisco MDS 9000 Family specific
securityd	Security	Cisco MDS 9000 Family specific
syslog	Internal system messages	Standard
sysmgr	System manager	Cisco MDS 9000 Family specific
tlport	TL port	Cisco MDS 9000 Family specific

Table 3-1 Internal Logging Facilities (continued)

Facility Keyword	Description	Standard or Cisco MDS Specific
user	User process	Standard
uucp	UNIX-to-UNIX Copy Program	Standard
vhbad	Virtual host base adapter daemon	Cisco MDS 9000 Family specific
vni	Virtual network interface	Cisco MDS 9000 Family specific
vrrp_cfg	VRRP configuration	Cisco MDS 9000 Family specific
vrrp_eng	VRRP engine	Cisco MDS 9000 Family specific
vsan	VSAN system messages	Cisco MDS 9000 Family specific
vshd	vshd	Cisco MDS 9000 Family specific
wwn	WWN manager	Cisco MDS 9000 Family specific
xbar	Xbar system messages	Cisco MDS 9000 Family specific
zone	Zone server	Cisco MDS 9000 Family specific

Table 3-2 describes the severity levels supported by the system message logs.

Table 3-2 Error Message Severity Levels

Level Keyword	Level	Description	System Message Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Note Refer to the *Cisco MDS 9000 Family and Nexus 7000 Series System Messages Reference* for details on the error log message format.

This section includes the following topics:

- Monitoring Syslog Server from DCNM-SAN, page 3-4
- System Message Logging, page 3-4
- SFP Diagnostics, page 3-4
- Outgoing System Message Logging Server Facilities, page 3-5
- System Message Logging Servers, page 3-5
- System Message Logging Configuration Distribution, page 3-6
- Fabric Lock Override, page 3-6

Monitoring Syslog Server from DCNM-SAN

Cisco DCNM-SAN registers itself as a logging server and receives syslog messages and stores them in separate files for each switch.

With Cisco NX-OS Release 5.0(1a) and later, the DCNM-SAN stores the syslog messages from all the switches in a fabric to a database, and displays only the aggregated syslog information from the web client. This feature can be enabled or disabled. The syslog stored in the database is filtered by a configurable severity level.

Once the DCNM-SAN receives the syslog messages through the syslog receiver, the raw messages are parsed and the flag for persisting the message in the database is checked. The severity carried by this message is checked from the parsed fields, and the syslog messages are sent to the database.

The raw syslog messages are parsed into the following fields: switch time, facility, severity, event, and Vsan Id. The description is stored in the database and filtered by the severity level.

The following fields are added to server.properties:

- syslog.dblog.enable = false

  This field is used to turn on the feature for storing the syslog messages into the database. By turning on this flag, the syslog messages are also written into the database.

- syslog.dblog.severity = warnings

  This field is used to filter the syslog messages based on the severity. By configuring this property, syslog messages are filtered on the severity level.

System Message Logging

The system message logging software saves the messages in a log file or directs the messages to other devices. This feature has the following capabilities:

- Provides logging information for monitoring and troubleshooting.
- Allows the user to select the types of captured logging information.
- Allows the user to select the destination server to forward the captured logging information.

By default, the switch logs normal but significant system messages to a log file and sends these messages to the system console. You can specify which system messages should be saved based on the type of facility and the severity level. Messages are time-stamped to enhance real-time debugging and management.

You can access the logged system messages using the CLI or by saving them to a correctly configured system message logging server. The switch software saves system messages in a file that can save up to 1200 entries. You can monitor system messages remotely by accessing the switch through Telnet, SSH, the console port, or by viewing the logs on a system message logging server.

SFP Diagnostics

The error message related to SFP failures is written to the syslog. You can listen to the syslog for events related to SFP failures. The values, low or high alarm, and the warning are checked for the following parameters:

- TX Power
- RX Power

- Temperature
- Voltage
- Current

The SFP notification trap indicates the current status of the alarm and warning monitoring parameters for all the sensors based on the digital diagnostic monitoring information. This notification is generated whenever there is a change in the status of at least one of the monitoring parameters of the sensors on the transceiver in an interface.

The CISCO-INTERFACE-XCVR-MONITOR-MIB contains the SFP notification trap information. Refer to the *Cisco MDS 9000 Family MIB Quick Reference* for more information on this MIB.

Outgoing System Message Logging Server Facilities

All system messages have a logging facility and a level. The logging facility can be thought of as *where* and the level can be thought of as *what*.

The single system message logging daemon (syslogd) sends the information based on the configured **facility** option. If no facility is specified, local7 is the default outgoing facility.

The internal facilities are listed in Table 3-1 and the outgoing logging facilities are listed in Table 3-3.

Table 3-3 Outgoing Logging Facilities

Facility Keyword	Description	Standard or Cisco MDS Specific
auth	Authorization system	Standard
authpriv	Authorization (private) system	Standard
cron	Cron or at facility	Standard
daemon	System daemons	Standard
ftp	File Transfer Protocol	Standard
kernel	Kernel	Standard
local0 to local7	Locally defined messages	Standard (local7 is the default)
lpr	Line printer system	Standard
mail	Mail system	Standard
news	USENET news	Standard
syslog	Internal system messages	Standard
user	User process	Standard
uucp	UNIX-to-UNIX Copy Program	Standard

System Message Logging Servers

Device Manager allows you to view event logs on your local PC as well as those on the switch. For a permanent record of all events that occur on the switch, you should store these messages off the switch. To do this the Cisco MDS 9000 Family switch must be configured to send syslog messages to your local PC and a syslog server must be running on that PC to receive those messages. These messages can be categorized into four classes:

- Hardware—Line card or power supply problems

- Link Incidents—FICON port condition changes
- Accounting—User change events
- Events—All other events

Note You should avoid using PCs that have IP addresses randomly assigned to them by DHCP. The switch continues to use the old IP address unless you manually change it; however, the Device Manager prompts you if it does detect this situation. UNIX workstations have a built-in syslog server. You must have root access (or run the Cisco syslog server as setuid to root) to stop the built-in syslog daemon and start the Cisco syslog server.

System Message Logging Configuration Distribution

You can enable fabric distribution for all Cisco MDS 9000 Family switches in the fabric. When you perform system message logging configurations, and distribution is enabled, that configuration is distributed to all the switches in the fabric.

You automatically acquire a fabric-wide lock when you issue the first configuration command after you enabled distribution in a switch. The system message logging server uses the effective and pending database model to store or commit the commands based on your configuration. When you commit the configuration changes, the effective database is overwritten by the configuration changes in the pending database and all the switches in the fabric receive the same configuration. After making the configuration changes, you can choose to discard the changes by aborting the changes instead of committing them. In either case, the lock is released. See Chapter 2, “Using the CFS Infrastructure” for more information on the CFS application.

Fabric Lock Override

If you have performed a system message logging task and have forgotten to release the lock by either committing or discarding the changes, an administrator can release the lock from any switch in the fabric. If the administrator performs this task, your changes to the pending database are discarded and the fabric lock is released.

Tip The changes are only available in the volatile directory and are subject to being discarded if the switch is restarted.

Guidelines and Limitations

See the “CFS Merge Support” section on page 2-6 for detailed concepts.

When merging two system message logging databases, follow these guidelines:

- Be aware that the merged database is a union of the existing and received database for each switch in the fabric.
- Verify that the merged database will only have a maximum of three system message logging servers.

Caution If the merged database contains more that three servers, the merge will fail.

Default Settings

Table 3-4 lists the default settings for system message logging.

Table 3-4 Default System Message Log Settings

Parameters	Default
System message logging to the console	Enabled for messages at the critical severity level.
System message logging to Telnet sessions	Disabled.
Logging file size	4194304.
Log file name	Message (change to a name with up to 200 characters).
Logging server	Disabled.
Syslog server IP address	Not configured.
Number of servers	Three servers.
Server facility	Local 7.

Configuring System Message Logging

System logging messages are sent to the console based on the default (or configured) logging facility and severity values.

This sections includes the following topics:

Task Flow for Configuring System Message Logging

Follow these steps to configure system message logging:

Step 1 Enable or disable message logging.

Step 2 Configure monitor severity level.

Step 3 Configure facility severity levels.

Step 4 Send log files.

Step 5 Configure system message logging servers.

Enabling or Disabling Message Logging

You can disable logging to the console or enable logging to a specific Telnet or SSH session.

- When you disable or enable logging to a console session, that state is applied to all future console sessions. If you exit and log in again to a new session, the state is preserved.
- When you enable or disable logging to a Telnet or SSH session, that state is applied only to that session. If you exit and log in again to a new session, the state is not preserved.

Detailed Steps

To enable or disable the logging state for a Telnet or SSH session, follow these steps:

Step 1 Select a switch in the Fabric pane.

Step 2 Expand **Events** and select **SysLog** in the Physical Attributes pane.

You see the SysLog information in the Information pane.

Step 3 Click the **Switch Logging** tab.

You see the switch information.

Step 4 Select a switch in the Information pane.

Step 5 Check (enable) or uncheck (disable) the **Console Enable** check box.

Step 6 Click the **Apply Changes** icon.

Configuring Console Severity Level

When logging is enabled for a console session (default), you can configure the severity levels of messages that appear on the console. The default severity for console logging is 2 (critical).

The current critical (default) logging level is maintained if the console baud speed is 9600 baud (default). All attempts to change the console logging level generates an error message. To increase the logging level (above critical), you must change the console baud speed to 38400 baud.

Configuring Monitor Severity Level

When logging is enabled for a monitor session (default), you can configure the severity levels of messages that appear on the monitor. The default severity for monitor logging is 5 (notifications).

Detailed Steps

To configure the severity level for a logging facility, follow these steps:

Step 1 Select a switch in the Fabric pane.

Step 2 Expand **Events** and select **SysLog** in the Physical Attributes pane.

You see the SysLog information in the Information pane.

Step 3 Click the **Switch Logging** tab.

You see the switch information.

Step 4 Select a switch in the Information pane.

Step 5 Select a severity level from the Console Severity drop-down list in the row for that switch.

Step 6 Click the **Apply Changes** icon.

Configuring Module Logging

By default, logging is enabled at level 7 for all modules. You can enable or disable logging for each module at a specified level.

Configuring Facility Severity Levels

Detailed Steps

To configure the severity level for a logging facility, follow these steps:

Step 1 Expand **Events** and select **SysLog** in the Physical Attributes pane.

In Device Manager, choose **Logs > Syslog > Setup** and click the **Switch Logging** tab in the Syslog dialog box.

You see the switch information.

Step 2 Check the check boxes where you want message logging to occur (**ConsoleEnable**, **TerminalEnable**, **LineCardEnable**).

Step 3 Choose the message severity threshold from the **Console Severity** drop-down box for each switch in DCNM-SAN or click the appropriate message severity level radio button in Device Manager.

Step 4 Click the **Apply Changes** icon in DCNM-SAN, or click **Apply** in Device Manager to save and apply your changes.

Sending Log Files

By default, the switch logs normal but significant system messages to a log file and sends these messages to the system console. Log messages are not saved across system reboots.The logging messages that are generated may be saved to a log file. You can configure the name of this file and restrict its size as required. The default log file name is messages.

The file name can have up to 80 characters and the file size ranges from 4096 bytes to 4194304 bytes.

Restrictions

The configured log file is saved in the /var/log/external directory. The location of the log file cannot be changed.

Detailed Steps

To send log messages to a file, follow these steps:

Step 1 Select a switch in the Fabric pane.

Step 2 Expand **Events** and select **SysLog** in the Physical Attributes pane.

You see the SysLog information in the Information pane.

Step 3 Select a switch in the Information pane.

Step 4 Click the **Switch Logging** tab.

Step 5 Enter the name of the log file in the LogFile Name column in the row for that switch.

Step 6 Click the **Apply Changes** icon.

Configuring System Message Logging Servers

You can configure a maximum of three system message logging servers. One of these syslog servers should be DCNM-SAN if you want to view system messages from the Event tab in DCNM-SAN.

To send log messages to a UNIX system message logging server, you must configure the system message logging daemon on a UNIX server. Log in as root, and follow these steps:

Step 1 Add the following line to the /etc/syslog.conf file.

```
local1.debug                    /var/log/myfile.log
```

Note Be sure to add five tab characters between **local1.debug** and **/var/log/*myfile*.log**. Refer to entries in the /etc/syslog.conf file for further examples.

The switch sends messages according to the specified facility types and severity levels. The **local1** keyword specifies the UNIX logging facility used. The messages from the switch are generated by user processes. The **debug** keyword specifies the severity level of the condition being logged. You can set UNIX systems to receive all messages from the switch.

Step 2 Create the log file by entering these commands at the UNIX shell prompt:

```
$ touch /var/log/myfile.log
$ chmod 666 /var/log/myfile.log
```

Step 3 Make sure the system message logging daemon reads the new changes by entering this command:

```
$ kill -HUP ~cat /etc/syslog.pid~
```

Note Most tabs in the Information pane for features using CFS are dimmed until you click the CFS tab. The CFS tab shows which switches have CFS enabled and shows the master switch for this feature. Once you click the CFS tab, the other tabs in the Information pane that use CFS are activated.

Detailed Steps

To configure system message logging servers, follow these steps:

Step 1 Expand **Events** and select **SysLog** in the Physical Attributes pane.

Step 2 Click the **Servers** tab in the Information pane.

In Device Manager, choose **Logs > Syslog > Setup** and click the **Servers** tab in the syslog dialog box.

Step 3 Click the **Create Row icon** in DCNM-SAN, or click **Create** in Device Manager to add a new syslog server.

Step 4 Enter the name or IP address in dotted decimal notation (for example, 192.168.2.12) of the syslog server in the Name or IP Address field.

Step 5 Set the message severity threshold by clicking the **MsgSeverity** radio button and set the facility by clicking the **Facility** radio button.

Step 6 Click the **Apply Changes** icon in DCNM-SAN, or click **Create** in Device Manager to save and apply your changes.

Verifying Log Configuration

This section describes how to display the system message logging configuration information.

Verifying Syslog Servers from DCNM-SAN Web Server

To verify the syslog servers remotely using DCNM-SAN Web Server, follow these steps:

Step 1 Point your browser at the DCNM-SAN Web Server.

Step 2 Choose **Events > Syslog** to view the syslog server information for each switch. The columns in the table are sortable.

Monitoring Logs

To section covers the following topics:

Viewing Logs from DCNM-SAN Web Server

To view system messages remotely using DCNM-SAN Web Server, follow these steps:

Step 1 Point your browser at the DCNM-SAN Web Server.

Step 2 Click the **Events tab** followed by the **Details** to view the system messages. The columns in the events table are sortable. In addition, you can use the Filter button to limit the scope of messages within the table.

Viewing Logs from Device Manager

You can view system messages from Device Manager if Device Manager is running from the same workstation as DCNM-SAN. Choose **Logs > Events > current** to view the system messages on Device Manager. The columns in the events table are sortable. In addition, you can use the Find button to locate text within the table.

You can view switch-resident logs even if you have not set up your local syslog server or your local PC is not in the switch's syslog server list. Due to memory constraints, these logs will wrap when they reach a certain size. The switch syslog has two logs: an NVRAM log that holds a limited number of critical and greater messages and a nonpersistent log that contains notice or greater severity messages. Hardware messages are part of these logs.

Additional References

For additional information related to implementing system message logging, see the following section:

- MIBs, page 3-12

MIBs

MIBs	MIBs Link
• CISCO-SYSLOG-EXT-MIB • CISCO-SYSLOG-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html

Feature History for System Message Logging

Table 3-5 lists the release history for this feature. Only features that were introduced or modified in Release 3.x or a later release appear in the table.

Table 3-5 Feature History for System Message Logging

Feature Name	Releases	Feature Information
Syslog Enhancements	5.0(1a)	Added Monitoring Syslog Server from DCNM-SAN. Added System Message Logging information.