Configuring System Message Logging

This chapter describes how to configure system message logging on the Cisco MDS 9000 Family switches.

This chapter contains the following topics:

About System Message Logging

The system message logging software saves messages in a log file or directs the messages to other devices. 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 of 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 logged system messages using the CLI or by saving them to a properly configured syslog server. The switch software saves syslog messages in a file that can be configured to save up to 4 MB. You can monitor system messages remotely by accessing the switch through Telnet, SSH, or the console port, or by viewing the logs on a syslog server.

When the switch first initializes, the network is not connected until initialization completes. Therefore, messages are not redirected to a syslog 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 28-1 describes the facilities supported by the system message logs.

Table 28-1 Facilities Supported by the System Message Logs

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 syslog messages	Standard
sysmgr	System manager	Cisco MDS 9000 Family specific
tlport	TL port	Cisco MDS 9000 Family specific

Table 28-1 Facilities Supported by the System Message Logs (continued)

Facility Keyword	Description	Standard or Cisco MDS Specific
user	User process	Standard
uucp	Unix-to-Unix copy system	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 syslog	Cisco MDS 9000 Family specific
vshd	vshd	Cisco MDS 9000 Family specific
wwn	WWN manager	Cisco MDS 9000 Family specific
xbar	Xbar syslog	Cisco MDS 9000 Family specific
zone	Zone server	Cisco MDS 9000 Family specific

Table 28-2 describes the severity levels supported by the system message logs.

Table 28-2 Error Message Severity Levels

Level Keyword	Level	Description	Syslog 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

Refer to the *Cisco MDS 9000 Family System Messages Guide* for details on the error log message format.

Configuring System Message Logging

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

Enabling Message Logging

You can disable logging to the console or enable logging to a given 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.

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).

Tip 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. T o increase the logging level (above critical), you must change the console baud speed to 38400 baud.

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 Log Files

Logging messages 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. You can rename this file. The file name can have up to 200 characters and the file size ranges from 4096 bytes to 4194304 bytes.

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

You can display the log file and copy the logfile to a different location.

Configuring the Syslog Daemon

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

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

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

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 syslog daemon reads the new changes by entering this command:

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

Outgoing Syslog Server Logging Facilities

All syslog 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 syslog 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 28-3.

Table 28-3 Internal 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 syslog messages	Standard
user	User process	Standard
uucp	Unix-to-Unix copy system	Standard

Configuring Syslog Servers

To configure syslog servers, follow these steps:

Step 1 Choose **Events > Syslog** from the Fabric Manager menu tree, and then click the **Servers** tab. The Information pane displays syslog information for multiple switches.

From the Device Manager, choose **Events > Syslog**, and then click the **Servers** tab. The Syslog dialog box with the Servers tab selected displays syslog information for a single switch.

Step 2 Configure the server attributes for the syslog.

Step 3 To add a syslog server, click **Create**. You see the Create Syslog Server dialog box.

Step 4 Complete the fields on this dialog box and click **OK**.

Configuring Syslog Attributes

To configure syslog attributes, follow these steps:

Step 1 From the Fabric Manager, choose **Events > Syslog** on the menu tree and click the **General** tab. The Information pane displays syslog information for multiple switches.

From the Device Manager, choose **Events > Syslog** and click the **General** tab. The General tab of the Syslog dialog box displays syslog information for a single switch.

Step 2 Configure the general attributes for the syslog.

Configuring Syslog Priorities

To configure syslog priorities, follow these steps:

Step 1 From the Fabric Manager, choose **Events > Syslog** on the menu tree, and then click the **Priorities** tab. The Information pane displays syslog information for multiple switches.

From the Device Manager, choose **Events > Syslog**, and then click the **Priorities** tab. The Syslog dialog box with the Servers tab selected displays syslog information for a single switch.

Step 2 Configure the priorities for the syslog.

Default Settings

Table 28-4 lists the default settings for system message logging.

Table 28-4 Default System Message Log Setting

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 (can be changed to any name with up to 200 characters).
Logging server	Disabled.
Syslog server IP address	Non configured.
No. of servers	3 servers.
Server facility	Local 7.

About SNMP Events

SNMP is an application layer protocol that facilitates the exchange of management information between network devices. Cisco MDS 9000 Family switches, like other SNMP-enabled devices, send events (traps and informs) to configurable destinations, called trap receivers in SNMPv2.

Viewing the Events Log

To view the events log from the Device Manager, choose **SNMP Log** from the Events menu. The Events Log dialog box displays a log of events for a single switch

To manage the SNMP log, choose **SNMP Log** from the Events menu and click the **Controls** tab. The Controls tab provides summary statistics about the SNMP log and allows you to change the default settings for the log.

Caution Changing these values from different Fabric Manager workstations at the same time may cause unpredictable results.

Configuring Event Destinations

To configure event destinations, follow these steps:

Step 1 Choose **Events > Notifications/Traps** from the Fabric Manager the menu tree and click the **Destinations** tab, or choose **Events > Destinations** from the Device Manager.

The Fabric Manager Information pane from the Fabric Manager shows event destination information for multiple switches. The Device Manager dialog shows event destinations for a single switch.

Step 2 To create an event destination, click **Create** in the Device Manager dialog box or click the **Create Row** icon on the Fabric Manager toolbar. You see the Create Event Destinations dialog box. (The dialog box from the Fabric Manager allows you to choose a switch.)

Step 3 Complete the fields and click **Apply** to create the event destination, or click **OK** to create the destination and close the dialog box.

Configuring Event Security

Caution This is an advanced function that should only be used by administrators having experience with SNMPv3.

To configure event security from the Fabric Manager, choose **Events > Notifications/Traps** on the menu tree, and click the **Security** tab.

To configure event security from the Device Manager, choose **Destinations** from the Events menu and click the **Security** tab.

The Information pane from the Fabric Manager displays event security information for multiple switches. The dialog box from Device Manager displays event security for a single switch.

Configuring Event Filters

To configure event filters from the Fabric Manager, choose **Events > Filters** on the menu tree, and click the **FC or Other** tab.

To configure event filters from the Device Manager, choose **Filters** from the Events menu.

The Event Filters dialog box displays event filters for a single switch. The Information pane in Fabric Manager displays two different views, which list the same event filters for multiple switches, in different order.

To configure event filters, check the check box next to the appropriate filter name.

About RMON Facilities

Remote Monitoring (RMON) allows you to specify thresholds and monitor alarms on SNMP variables.

Enabling RMON Alarms by Port

To enable alarm notifications by port from the Device Manager, choose **Events > Threshold Manager** and click the **Ports** tab.

To configure an RMON alarm for one or more ports, follow these steps:

Step 1 Click the **Selected** radio button.

Step 2 Click the button to the right of the Selected field to display all ports.

Step 3 Choose the ports you want to monitor.

Step 4 Click **OK** to accept the selection.

Alternatively, click the appropriate radio button to select ports by type (All ports, xE ports, or Fx port).

Step 5 Check the check box for each variable that you want to monitor.

Step 6 Enter the threshold value in the Value column.

Step 7 Enter the sampling period in seconds.

Step 8 Choose one of the following severity levels to assign to the alarm:

- Fatal
- Warning
- Critical
- Error
- Information

Step 9 Click **Create**.

Step 10 Confirm the operation to define an alarm and a log event when the system prompts you to define a severity event.

If you do not confirm the operation, the system only defines a log event.

Enabling RMON Alarms for VSANs

To manage RMON alarm service attributes for selected VSANs from the Device Manager, choose **Events > Threshold Manager** and click the **Services** tab. You see the Threshold Manager dialog box with the Services tab selected.

To enable an RMON alarm for one or more VSANs, follow these steps:

Step 1 Enter one or more VSANs to monitor in the VSAN Id(s) field.

Step 2 Check the check box for each variable that you want to monitor.

Step 3 Enter the threshold value in the Value column.

Step 4 Enter the sampling period in seconds.

Step 5 Select a severity level to assign to the alarm:

Step 6 Click **Create**.

Step 7 Confirm the operation to define an alarm and a log event when the system prompts you to define a severity event.

If you do not confirm the operation, the system only defines a log event.

Enabling RMON Alarms for Physical Components

To configure RMON alarm physical attributes from the Device Manager, choose **Events > Threshold Manager** and click the **Physical** tab. You see the Create RMON Alarms dialog box with the Physical tab selected.

To configure an RMON alarm for a physical component, follow these steps:

Step 1 Check the check box for each variable that you want to monitor.

Step 2 Enter the threshold value in the Value column.

Step 3 Enter the sampling period in seconds.

Step 4 Select one of the following severity levels to assign to the alarm:

- Fatal
- Warning
- Critical
- Error
- Information

Step 5 Click **Create**.

Step 6 Confirm the operation to define an alarm and a log event when the system prompts you to define a severity event.

If you do not confirm the operation, the system only defines a log event.

Configuring RMON Controls

To change the default controls for RMON alarms, choose **Threshold Manager** from the Device Manager menu. You see the Threshold Manager window.

Click More on the Threshold Manager window. You see the second Threshold Manager dialog box.

Managing RMON Alarms

To view the alarms that have already been enabled, follow these steps:

Step 1 Choose **Events > Threshold Manager**, and then click **More** in the Threshold Manager dialog box.

Step 2 Click the **Alarms** tab. You see the RMON Alarms dialog box.

Step 3 To create a customized threshold entry, click **Create**. You see the Create RMON Alarms dialog box.

Managing RMON Event Severity Levels

To define customized RMON event severity levels, follow these steps:

Step 1 Choose **Event s> Threshold Manager**, and then click **More** in the Threshold Manager dialog box.

Step 2 Click the **Events** tab on the RMON Thresholds dialog box. You see the RMON Events dialog box.

Step 3 To create a new threshold entry, click **Create**. You see the Create Threshold Entry dialog box.

Step 4 Configure the RMON event threshold attributes.

Viewing the RMON Log

To view the RMON log from the Device Manager, follow these steps:

Step 1 Choose **Events** > **Threshold Manager**, and then click **More** in the Threshold Manager dialog box.

Step 2 Click the **Log** tab on the RMON Thresholds dialog box. You see the RMON Log dialog box.