CHAPTER 52

Configuring System Message Logging

This chapter describes how to configure system message logging on Cisco MDS 9000 Family switches. It includes the following sections:

- About System Message Logging, page 52-1
- System Message Logging Configuration, page 52-3
- System Message Logging Configuration Distribution, page 52-8
- Displaying System Message Logging Information, page 52-10
- Default Settings, page 52-15

About System Message Logging

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 52-1 describes some samples of the facilities supported by the system message logs.

Table 52-1 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

Table 52-1 Internal Logging Facilities (continued)

Facility Keyword	Description	Standard or Cisco MDS Specific
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
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

Table 52-1 Internal Logging Facilities (continued)

Facility Keyword	Description	Standard or Cisco MDS 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 52-2 describes the severity levels supported by the system message logs.

Table 52-2 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 System Messages Reference* for details on the error log message format.

System Message Logging Configuration

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:

- Message Logging Initiation, page 52-4
- Console Severity Level, page 52-4
- Monitor Severity Level, page 52-4
- Module Logging, page 52-5
- Facility Severity Levels, page 52-5
- Log Files, page 52-6
- System Message Logging Servers, page 52-6

Message Logging Initiation

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.

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

	Command	Purpose
Step 1	`switch# terminal monitor`	Enables logging for a Telnet or SSH session. **Note** A console session is enabled by default.
Step 2	`switch# terminal no monitor`	Disables logging for a Telnet or SSH session. **Note** A Telnet or SSH session is disabled by default.

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

See the "Configuring Console Port Settings" section on page 5-29.

To configure the severity level for the console session, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# logging console 3`	Configures console logging at level 3 (error). Logging messages with a severity level of 3 or above are displayed on the console.
	`switch(config)# no logging console`	Reverts console logging to the factory set default severity level of 2 (critical). Logging messages with a severity level of 2 or above are displayed on the console.

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).

To configure the severity level for a monitor session, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# logging monitor 3`	Configures monitor logging at level 3 (error). Logging messages with a severity level of 3 or above are displayed on the monitor.
	`switch(config)# no logging monitor`	Reverts monitor logging to the factory set default severity level of 5 (notifications). Logging messages with a severity level of 5 or above are displayed on the console.

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.

To enable or disable the logging for modules and configure the severity level, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# logging module 1`	Configures module logging at level 1 (alerts) for all modules.
	`switch(config)# logging module`	Configures module logging for all modules in the switch at the default level 5 (notifications).
	`switch(config)# no logging module`	Disables module logging.

Facility Severity Levels

To configure the severity level for a logging facility (see Table 52-1), follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# logging level kernel 4`	Configures Telnet or SSH logging for the kernel facility at level 4 (warning). As a result, logging messages with a severity level of 4 or above are displayed.
	`switch(config)# no logging level kernel 4`	Reverts to the default severity level 6 (informational) for the Telnet or SSH logging for the kernel facility. **Note** Use the **show logging info** command to display the default logging levels for the facilities listed in Table 52-1.

Log Files

Logging messages can 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.

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

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# logging logfile messages 3`	Configures logging of information for errors or events above with a severity level 3 or above to the default log file named messages.
	`switch(config)# logging logfile ManagerLog 3`	Configures logging of information for errors or events with a severity level 3 or above to a file named ManagerLog using the default size of 10,485,760 bytes.
	`switch(config)# logging logfile ManagerLog 3 size 3000000`	Configures logging information for errors or events with a severity level 3 or above to a file named ManagerLog. By configuring a size, you are restricting the file size to 3,000,000 bytes.
	`switch(config)# no logging logfile`	Disables logging messages to the logfile.

Note You can rename the log file using the **logging logfile** command.

The configured log file is saved in the /var/log/external directory. The location of the log file cannot be changed. You can use the **show logging logfile** and **clear logging logfile** commands to view and delete the contents of this file. You can use the **dir log:** command to view logging file statistics. You can use the **delete log:** command to remove the log file.

You can copy the logfile to a different location using the **copy log:** command using additional copy syntax (see the "Copying Configuration Files" section on page 9-5).

System Message Logging Servers

You can configure a maximum of three system message logging servers.

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~
```

To configure system message logging server IPv4 addresses, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch#`	Enters configuration mode.
Step 2	`switch(config)# logging server 172.22.00.00`	Configures the switch to forward log messages according to the specified facility types and severity levels to remote multiple servers specified by its hostname or IPv4 address (172.22.00.00).
	`switch(config)# logging server 172.22.00.00 facility local1`	Configures the switch to forward log messages according to the specified facility (local1) for the server IPv4 address (172.22.00.00). The default outgoing facility is local7.
	`switch(config)# no logging server 172.11.00.00`	Removes the specified server (172.11.00.00) and reverts to factory default.

To configure system message logging server IPv6 addresses, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch#`	Enters configuration mode.
Step 2	`switch(config)# logging server 2001::0db8:800:200c:417a`	Configures the switch to forward log messages according to the specified facility types and severity levels to a remote server specified by its IPv6 address.
	`switch(config)# logging server 2001::0db8:800:200c:417a facility local1`	Configures the switch to forward log messages according to the specified facility (local1) for the server IPv6 address. The default outgoing facility is local7.
	`switch(config)# no logging server 2001::0db8:800:200c:417a`	Removes the specified server and reverts to factory default.

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 52-1 and the outgoing logging facilities are listed in Table 52-3.

Table 52-3 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 Configuration Distribution

You can enable fabric distribution for all Cisco MDS 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 7, “Using the CFS Infrastructure” for more information on the CFS application.

To enable fabric distribution for system message logging server configurations, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# logging distribute`	Enables the system message logging server configuration to be distributed to all switches in the fabric, acquires a lock, and stores all future configuration changes in the pending database.
	`switch(config)# no logging distribute`	Disables (default) system message logging server configuration distribution to all switches in the fabric.

To commit the system message logging server configuration changes, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# logging commit`	Distributes the configuration changes to all switches in the fabric, releases the lock, and overwrites the effective database with the changes made to the pending database.

To discard the system message logging server configuration changes, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# logging abort`	Discards the system message logging server configuration changes in the pending database and releases the fabric lock.

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.

To use administrative privileges and release a locked system message logging session, use the **clear logging session** command.

```
switch# clear logging session
```

Database Merge Guidelines

See the "CFS Merge Support" section on page 7-9 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.

Displaying System Message Logging Information

Use the **show logging** command to display the current system message logging configuration. See Examples 52-1 to 52-10.

Note When using the **show logging** command, output is displayed only when the configured logging levels for the switch are different from the default levels.

Example 52-1 Displays Current System Message Logging

```
switch# show logging
Logging console:                 enabled (Severity: critical)
Logging monitor:                 enabled (Severity: debugging)
Logging linecard:                enabled (Severity: debugging)
Logging server:                  enabled
{172.20.102.34}
        server severity:         debugging
        server facility:         local7
{10.77.202.88}
        server severity:         debugging
        server facility:         local7
{10.77.202.149}
        server severity:         debugging
        server facility:         local7
Logging logfile:                 enabled
        Name - messages: Severity - debugging Size - 4194304
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
kern                    6                       6
user                    3                       3
mail                    3                       3
daemon                  7                       7
auth                    0                       7
syslog                  3                       3
lpr                     3                       3
news                    3                       3
uucp                    3                       3
cron                    3                       3
authpriv                3                       7
ftp                     3                       3
local0                  3                       3
local1                  3                       3
local2                  3                       3
```

```
local3                  3                       3
local4                  3                       3
local5                  3                       3
local6                  3                       3
local7                  3                       3
vsan                    2                       2
fspf                    3                       3
fcdomain                2                       2
module                  5                       5
sysmgr                  3                       3
zone                    2                       2
vni                     2                       2
ipconf                  2                       2
ipfc                    2                       2
xbar                    3                       3
fcns                    2                       2
fcs                     2                       2
acl                     2                       2
tlport                  2                       2
port                    5                       5
flogi                   2                       2
port_channel            5                       5
wwn                     3                       3
fcc                     2                       2
qos                     3                       3
vrrp_cfg                2                       2
ntp                     2                       2
platform                5                       5
vrrp_eng                2                       2
callhome                2                       2
mcast                   2                       2
rdl                     2                       2
rscn                    2                       2
bootvar                 5                       2
securityd               2                       2
vhbad                   2                       2
rib                     2                       2
vshd                    5                       5
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)

Feb 14 09:50:57 excal-113 %TTYD-6-TTYD_MISC: TTYD TTYD started
Feb 14 09:50:58 excal-113 %DAEMON-6-SYSTEM_MSG: precision = 8 usec
...
```

Use the **show logging nvram** command to view the log messages saved in NVRAM. Only log messages with a severity level of critical and below (levels 0, 1, and 2) are saved in NVRAM.

Example 52-2 Displays NVRM Log Contents

```
switch# show logging nvram
Jul 16 20:36:46 172.22.91.204 %KERN-2-SYSTEM_MSG: unable to alloc and fill in a
new mtsbuf (pid=2209, ret_val = -105)
Jul 16 20:36:46 172.22.91.204 %KERN-2-SYSTEM_MSG: unable to alloc and fill in a
new mtsbuf (pid=2199, ret_val = -105)
Jul 16 20:36:46 172.22.91.204 %KERN-2-SYSTEM_MSG: unable to alloc and fill in a
new mtsbuf (pid=2213, ret_val = -105)
Jul 16 20:36:46 172.22.91.204 %KERN-2-SYSTEM_MSG: unable to alloc and fill in a
new mtsbuf (pid=2213, ret_val = -105)
...
```

Example 52-3 Displays the Log File

```
switch# show logging logfile
Jul 16 21:06:50 %DAEMON-3-SYSTEM_MSG: Un-parsable frequency in /mnt/pss/ntp.drift
Jul 16 21:06:56 %DAEMON-3-SYSTEM_MSG: snmpd:snmp_open_debug_cfg: no snmp_saved_dbg_uri ;
Jul 16 21:06:58 172.22.91.204 %PORT-5-IF_UP: Interface mgmt0 is up
Jul 16 21:06:58 172.22.91.204 %MODULE-5-ACTIVE_SUP_OK: Supervisor 5 is active
...
```

Example 52-4 Displays Console Logging Status

```
switch# show logging console
Logging console:                enabled (Severity: notifications)
```

Example 52-5 Displays Logging Facility

```
switch# show logging level
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
kern                    6                       6
user                    3                       3
mail                    3                       3
daemon                  7                       7
auth                    0                       7
syslog                  3                       3
lpr                     3                       3
news                    3                       3
uucp                    3                       3
cron                    3                       3
authpriv                3                       7
ftp                     3                       3
local0                  3                       3
local1                  3                       3
local2                  3                       3
local3                  3                       3
local4                  3                       3
local5                  3                       3
local6                  3                       3
local7                  3                       3
vsan                    2                       2
fspf                    3                       3
fcdomain                2                       2
module                  5                       5
sysmgr                  3                       3
zone                    2                       2
vni                     2                       2
ipconf                  2                       2
ipfc                    2                       2
xbar                    3                       3
fcns                    2                       2
fcs                     2                       2
acl                     2                       2
tlport                  2                       2
port                    5                       5
flogi                   2                       2
port_channel            5                       5
wwn                     3                       3
fcc                     2                       2
qos                     3                       3
vrrp_cfg                2                       2
```

```
ntp                     2                       2
platform                5                       5
vrrp_eng                2                       2
callhome                2                       2
mcast                   2                       2
rdl                     2                       2
rscn                    2                       2
bootvar                 5                       2
securityd               2                       2
vhbad                   2                       2
rib                     2                       2
vshd                    5                       5
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
```

Example 52-6 Displays Logging Information

```
switch# show logging info
Logging console:                enabled (Severity: critical)
Logging monitor:                enabled (Severity: debugging)
Logging linecard:               enabled (Severity: debugging)
Logging server:                 enabled
{172.20.102.34}
        server severity:        debugging
        server facility:        local7
{10.77.202.88}
        server severity:        debugging
        server facility:        local7
{10.77.202.149}
        server severity:        debugging
        server facility:        local7
Logging logfile:                enabled
        Name - messages: Severity - debugging Size - 4194304
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
kern                    6                       6
user                    3                       3
mail                    3                       3
daemon                  7                       7
auth                    0                       7
syslog                  3                       3
lpr                     3                       3
news                    3                       3
uucp                    3                       3
cron                    3                       3
authpriv                3                       7
ftp                     3                       3
local0                  3                       3
local1                  3                       3
local2                  3                       3
local3                  3                       3
local4                  3                       3
local5                  3                       3
local6                  3                       3
local7                  3                       3
vsan                    2                       2
fspf                    3                       3
fcdomain                2                       2
module                  5                       5
sysmgr                  3                       3
zone                    2                       2
vni                     2                       2
```

```
ipconf                  2                       2
ipfc                    2                       2
xbar                    3                       3
fcns                    2                       2
fcs                     2                       2
acl                     2                       2
tlport                  2                       2
port                    5                       5
flogi                   2                       2
port_channel            5                       5
wwn                     3                       3
fcc                     2                       2
qos                     3                       3
vrrp_cfg                2                       2
ntp                     2                       2
platform                5                       5
vrrp_eng                2                       2
callhome                2                       2
mcast                   2                       2
rdl                     2                       2
rscn                    2                       2
bootvar                 5                       2
securityd               2                       2
vhbad                   2                       2
rib                     2                       2
vshd                    5                       5
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
```

Example 52-7 Displays Last Few Lines of a Log File

```
switch# show logging last 2
Nov 8 16:48:04 excal-113 %LOG_VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from pts/1
(171.71.58.56)
Nov 8 17:44:09 excal-113 %LOG_VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from pts/0
(171.71.58.72)
```

Example 52-8 Displays Switching Module Logging Status

```
switch# show logging module
Logging linecard:               enabled (Severity: debugging)
```

Example 52-9 Displays Monitor Logging Status

```
switch# show logging monitor
Logging monitor:                enabled (Severity: information)
```

Example 52-10 Displays Server Information

```
switch# show logging server
Logging server:                 enabled
{172.22.95.167}
        server severity:        debugging
        server facility:        local7
{172.22.92.58}
        server severity:        debugging
```

```
server facility:        local7
```

Default Settings

Table 52-4 lists the default settings for system message logging.

Table 52-4 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.