



Configuring System Message Logging

This chapter describes how to configure system message logging on Cisco NX-OS devices.

This chapter contains the following sections:

- [About System Message Logging, on page 1](#)
- [Guidelines and Limitations for System Message Logging, on page 2](#)
- [Default Settings for System Message Logging, on page 2](#)
- [Configuring System Message Logging, on page 3](#)
- [Verifying the System Message Logging Configuration, on page 13](#)
- [Configuration Example for System Message Logging, on page 14](#)
- [Additional References, on page 14](#)

About System Message Logging

You can use system message logging to control the destination and to filter the severity level of messages that system processes generate. You can configure logging to terminal sessions, a log file, and syslog servers on remote systems.

For more information about the system message format and the messages that the device generates, see the [Cisco NX-OS System Messages Reference](#).

By default, the device outputs messages to terminal sessions and logs system messages to a log file.

The following table describes the severity levels used in system messages. When you configure the severity level, the system outputs messages at that level and lower.

Table 1: System Message Severity Levels

Level	Description
0 – emergency	System unusable
1 – alert	Immediate action needed
2 – critical	Critical condition
3 – error	Error condition
4 – warning	Warning condition

Level	Description
5 – notification	Normal but significant condition
6 – informational	Informational message only
7 – debugging	Appears during debugging only

The device logs the most recent 100 messages of severity 0, 1, or 2 to the NVRAM log. You cannot configure logging to the NVRAM.

You can configure which system messages should be logged based on the facility that generated the message and its severity level.

Syslog Servers

The syslog servers run on remote systems that log system messages based on the syslog protocol. You can configure up to eight IPv4 or IPv6 syslog servers.

To support the same configuration of syslog servers on all switches in a fabric, you can use Cisco Fabric Services (CFS) to distribute the syslog server configuration.



Note When the device first initializes, messages are sent to syslog servers only after the network is initialized.

Guidelines and Limitations for System Message Logging

System message logging has the following configuration guidelines and limitations:

- System messages are logged to the console and the log file by default.
- Any system messages that are printed before the syslog server is reachable (such as supervisor active or online messages) cannot be sent to the syslog server.
- Generally, the syslogs display the local time zone. However, few components such as NGINX display the logs in UTC time zone.

Default Settings for System Message Logging

The following table lists the default settings for the system message logging parameters.

Table 2: Default System Message Logging Parameters

Parameters	Default
Console logging	Enabled at severity level 2
Monitor logging	Enabled at severity level 5

Parameters	Default
Log file logging	Enabled to log messages at severity level 5
Module logging	Enabled at severity level 5
Facility logging	Enabled
Time-stamp units	Seconds
Syslog server logging	Disabled
Syslog server configuration distribution	Disabled

Configuring System Message Logging



Note Be aware that the Cisco NX-OS commands for this feature might differ from those commands used in Cisco IOS.

Configuring System Message Logging to Terminal Sessions

You can configure the device to log messages by their severity level to console, Telnet, and SSH sessions.

By default, logging is enabled for terminal sessions.



Note 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 will generate an error message. To increase the logging level (above critical), you must change the console baud speed to 38400 baud.

Procedure

	Command or Action	Purpose
Step 1	terminal monitor Example: switch# terminal monitor	Enables the device to log messages to the console.
Step 2	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<p>[no] logging console [<i>severity-level</i>]</p> <p>Example:</p> <pre>switch(config)# logging console 3</pre>	<p>Configures the device to log messages to the console session based on a specified severity level or higher. A lower number indicates a higher severity level. Severity levels range from 0 to 7:</p> <ul style="list-style-type: none"> • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging <p>If the severity level is not specified, the default of 2 is used. The no option disables the device's ability to log messages to the console.</p>
Step 4	<p>(Optional) show logging console</p> <p>Example:</p> <pre>switch(config)# show logging console</pre>	Displays the console logging configuration.
Step 5	<p>[no] logging monitor [<i>severity-level</i>]</p> <p>Example:</p> <pre>switch(config)# logging monitor 3</pre>	<p>Enables the device to log messages to the monitor based on a specified severity level or higher. A lower number indicates a higher severity level. Severity levels range from 0 to 7:</p> <ul style="list-style-type: none"> • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging <p>The configuration applies to Telnet and SSH sessions.</p>

	Command or Action	Purpose
		If the severity level is not specified, the default of 2 is used. The no option disables the device's ability to log messages to the Telnet and SSH sessions.
Step 6	(Optional) show logging monitor Example: switch(config)# show logging monitor	Displays the monitor logging configuration.
Step 7	[no] logging message interface type ethernet description Example: switch(config)# logging message interface type ethernet description	Enables you to add the description for physical Ethernet interfaces and subinterfaces in the system message log. The description is the same description that was configured on the interface. The no option disables the printing of the interface description in the system message log for physical Ethernet interfaces.
Step 8	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Configuring the Origin ID for Syslog Messages

You can configure Cisco NX-OS to append the hostname, an IP address, or a text string to syslog messages that are sent to remote syslog servers.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	Required: logging origin-id {hostname ip ip-address string text-string} Example: switch(config)# logging origin-id string n9k-switch-abc	Specifies the hostname, IP address, or text string to be appended to syslog messages that are sent to remote syslog servers.
Step 3	(Optional) show logging origin-id Example: switch(config)# show logging origin-id Logging origin_id : enabled (string: n9k-switch-abc)	Displays the configured hostname, IP address, or text string that is appended to syslog messages that are sent to remote syslog servers.

	Command or Action	Purpose
Step 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Logging System Messages to a File

You can configure the device to log system messages to a file. By default, system messages are logged to the file `/logflash/log/logfilename`.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	[no] logging logfile logfile-name severity-level [size bytes] Example: <pre>switch(config)# logging logfile my_log 6</pre>	Configures the nonpersistent log file parameters. <i>logfile-name</i> : Configures the name of the log file that is used to store system messages. Default filename is "message". <i>severity-level</i> : Configures the minimum severity level to log. A lower number indicates a higher severity level. Default is 5. Range is from 0 through 7: <ul style="list-style-type: none"> • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging size bytes : Optionally specify maximum file size. Range is from 4096 through 4194304 bytes.

	Command or Action	Purpose
Step 3	logging event {link-status trunk-status} {enable default} Example: <pre>switch(config)# logging event link-status default</pre>	Logs interface events. <ul style="list-style-type: none"> • link-status—Logs all UP/DOWN and CHANGE messages. • trunk-status—Logs all TRUNK status messages. • enable—Specifies to enable logging to override the port level configuration. • default—Specifies that the default logging configuration is used by interfaces that are not explicitly configured.
Step 4	(Optional) show logging info Example: <pre>switch(config)# show logging info</pre>	Displays the logging configuration.
Step 5	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Configuring Module and Facility Messages Logging

You can configure the severity level and time-stamp units of messages logged by modules and facilities.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	[no] logging module [<i>severity-level</i>] Example: <pre>switch(config)# logging module 3</pre>	Enables module log messages that have the specified severity level or higher. Severity levels range from 0 to 7: <ul style="list-style-type: none"> • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning

	Command or Action	Purpose
		<ul style="list-style-type: none"> • 5 – notification • 6 – informational • 7 – debugging <p>If the severity level is not specified, the default of 5 is used. The no option disables module log messages.</p>
Step 3	(Optional) show logging module Example: <pre>switch(config)# show logging module</pre>	Displays the module logging configuration.
Step 4	[no] logging level <i>facility severity-level</i> Example: <pre>switch(config)# logging level aaa 2</pre>	<p>Enables logging messages from the specified facility that have the specified severity level or higher. Severity levels range from 0 to 7:</p> <ul style="list-style-type: none"> • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging <p>To apply the same severity level to all facilities, use the all facility. For defaults, see the show logging level command.</p> <p>The no option resets the logging severity level for the specified facility to its default level. If you do not specify a facility and severity level, the device resets all facilities to their default levels.</p>
Step 5	(Optional) show logging level [<i>facility</i>] Example: <pre>switch(config)# show logging level aaa</pre>	Displays the logging level configuration and the system default level by facility. If you do not specify a facility, the device displays levels for all facilities.
Step 6	(Optional) [no] logging level <i>ethpm</i> Example: <pre>switch(config)# logging level ethpm ? <0-7></pre>	<p>Enables logging of the Ethernet Port Manager link-up/link-down syslog messages at level 3.</p> <p>Use the no option to use the default logging level for Ethernet Port Manager syslog messages.</p>

	Command or Action	Purpose
	<pre> 0-err;1-let;2-crit;3-err;4-warn;5-notif;6-inform;7-debug link-down Configure logging level for link down syslog messages link-up Configure logging level for link up syslog messages switch(config)#logging level ethpm link-down ? error ERRORS notif NOTICE (config)# logging level ethpm link-down error ? <CR> (config)# logging level ethpm link-down notif ? <CR> switch(config)#logging level ethpm link-up ? error ERRORS notif NOTICE (config)# logging level ethpm link-up error ? <CR> (config)# logging level ethpm link-up notif ? <CR> </pre>	
Step 7	<p>[no] logging timestamp {microseconds milliseconds seconds}</p> <p>Example:</p> <pre>switch(config)# logging timestamp milliseconds</pre>	<p>Sets the logging time-stamp units. By default, the units are seconds.</p> <p>Note This command applies to logs that are kept in the switch. It does not apply to the external logging server.</p>
Step 8	<p>(Optional) show logging timestamp</p> <p>Example:</p> <pre>switch(config)# show logging timestamp</pre>	<p>Displays the logging time-stamp units configured.</p>
Step 9	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch(config)# copy running-config startup-config</pre>	<p>Copies the running configuration to the startup configuration.</p>

Configuring Syslog Servers



Note Cisco recommends that you configure the syslog server to use the management virtual routing and forwarding (VRF) instance. For more information on VRFs, see Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide.

You can configure up to eight syslog servers that reference remote systems where you want to log system messages.

Procedure

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	<p>[no] logging server host [severity-level [use-vrf vrf-name]]</p> <p>Example:</p> <pre>switch(config)# logging server 192.0.2.253</pre> <p>Example:</p> <pre>switch(config)# logging server 2001::3 5 use-vrf red</pre>	<p>Configures a syslog server at the specified hostname, IPv4, or IPv6 address. You can specify logging of messages to a particular syslog server in a VRF by using the use-vrf keyword. The use-vrf vrf-name keyword identifies the default or management values for the VRF name. The default VRF is the management VRF, by default. However, the show-running command will not list the default VRF. Severity levels range from 0 to 7:</p> <ul style="list-style-type: none"> • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging <p>The default outgoing facility is local7.</p> <p>The no option removes the logging server for the specified host.</p> <p>The first example forwards all messages on facility local 7. The second example forwards</p>

	Command or Action	Purpose
		messages with severity level 5 or lower to the specified IPv6 address in VRF red.
Step 3	Required: logging source-interface loopback virtual-interface Example: switch(config)# logging source-interface loopback 5	Enables a source interface for the remote syslog server. The range for the <i>virtual-interface</i> argument is from 0 to 1023.
Step 4	(Optional) show logging server Example: switch(config)# show logging server	Displays the syslog server configuration.
Step 5	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Configuring Syslog Servers on a UNIX or Linux System

You can configure a syslog server on a UNIX or Linux system by adding the following line to the `/etc/syslog.conf` file:

```
facility.level <five tab characters> action
```

The following table describes the syslog fields that you can configure.

Table 3: Syslog fields in `syslog.conf`

Field	Description
Facility	Creator of the message, which can be auth, authpriv, cron, daemon, kern, lpr, mail, mark, news, syslog, user, local0 through local7, or an asterisk (*) for all. These facility designators allow you to control the destination of messages based on their origin. Note Check your configuration before using a local facility.
Level	Minimum severity level at which messages are logged, which can be debug, info, notice, warning, err, crit, alert, emerg, or an asterisk (*) for all. You can use none to disable a facility.

Field	Description
Action	Destination for messages, which can be a filename, a hostname preceded by the at sign (@), a comma-separated list of users, or an asterisk (*) for all logged-in users.

Procedure

Step 1 Log debug messages with the local7 facility in the file `/var/log/myfile.log` by adding the following line to the `/etc/syslog.conf` file:

Example:

```
debug.local7 var/log/myfile.log
```

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

Example:

```
$ 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 checking `myfile.log` after entering this command:

Example:

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

Displaying and Clearing Log Files

You can display or clear messages in the log file and the NVRAM.

Procedure

	Command or Action	Purpose
Step 1	Required: show logging last <i>number-lines</i> Example: <code>switch# show logging last 40</code>	Displays the last number of lines in the logging file. You can specify from 1 to 9999 for the last number of lines.
Step 2	show logging logfile duration <i>hh:mm:ss</i> Example: <code>switch# show logging logfile duration 15:10:0</code>	Displays the messages in the log file that have occurred within the duration entered.
Step 3	show logging logfile last-index Example:	Displays the sequence number of the last message in the log file.

	Command or Action	Purpose
	switch# show logging logfile last-index	
Step 4	show logging logfile [start-time yyyy mmm dd hh:mm:ss] [end-time yyyy mmm dd hh:mm:ss] Example: switch# show logging logfile start-time 2013 oct 1 15:10:0	Displays the messages in the log file that have a timestamp within the span entered. If you do not enter an end time, the current time is used. You enter three characters for the month time field and digits for the year and day time fields.
Step 5	show logging logfile [start-seqn number] [end-seqn number] Example: switch# show logging logfile start-seqn 100 end-seqn 400	Displays messages occurring within a range of sequence numbers. If you do not include an end sequence number, the system displays messages from the start number to the last message in the log file.
Step 6	show logging nvram [last number-lines] Example: switch# show logging nvram last 10	Displays the messages in the NVRAM. To limit the number of lines displayed, you can enter the last number of lines to display. You can specify from 1 to 100 for the last number of lines.
Step 7	clear logging logfile [persistent] Example: switch# clear logging logfile	Clears the contents of the log file. persistent: Clears the contents of the log file from the persistent location.
Step 8	clear logging nvram Example: switch# clear logging nvram	Clears the logged messages in NVRAM.

Verifying the System Message Logging Configuration

To display system message logging configuration information, perform one of the following tasks:

Command	Purpose
show logging console	Displays the console logging configuration.
show logging info	Displays the logging configuration.
show logging last number-lines	Displays the last number of lines of the log file.
show logging level [facility]	Displays the facility logging severity level configuration.
show logging logfile duration hh:mm:ss	Displays the messages in the log file that have occurred within the duration entered.
show logging logfile last-index	Displays the sequence number of the last message in the log file.

Command	Purpose
show logging logfile [start-time yyyy mmm dd hh:mm:ss] [end-time yyyy mmm dd hh:mm:ss]	Displays the messages in the log file based on a start and end date/time.
show logging logfile [start-seqn number] [end-seqn number]	Displays messages occurring within a range of sequence numbers. If you do not include an end sequence number, the system displays messages from the start number to the last message in the log file.
show logging module	Displays the module logging configuration.
show logging monitor	Displays the monitor logging configuration.
show logging nvram [last number-lines]	Displays the messages in the NVRAM log.
show logging origin-id	Displays the configured hostname, IP address, or text string that is appended to syslog messages that are sent to remote syslog servers.
show logging server	Displays the syslog server configuration.
show logging timestamp	Displays the logging time-stamp units configuration.

Configuration Example for System Message Logging

This example shows how to configure system message logging:

```
configure terminal
logging console 3
logging monitor 3
logging logfile my_log 6
logging module 3
logging level aaa 2
logging timestamp milliseconds
logging server 172.28.254.253
logging server 172.28.254.254 5 facility local3
copy running-config startup-config
```

Additional References

Related Documents

Related Topic	Document Title
System messages	<i>Cisco NX-OS System Messages Reference</i>