Configuring System Message Logging

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

This chapter contains the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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.

System message logging is based on RFC 3164. 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
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.

Binary Tech Support

Binary tech support is a log-collecting framework that collects logs internally from all Cisco NX-OS processes that are running on the device. Enter the **show tech-support all binary** *uri* command to collect logs from across the entire device, including virtual device contexts (VDCs), and linecards. The logs are saved under one tarball that can be easily transferred for later analysis. If a line card fails during the log collection, binary tech support continues to collect logs from all remaining line cards and VDCs.

Virtualization Support

A virtual device context (VDC) is a logical representation of a set of system resources. System message logging applies only to the VDC where commands are entered.

For information about configuring VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide.*

Guidelines and Limitations for System Message Logging

System messages are logged to the console and the log file by default.

For the secure syslog server(s) to be reachable over in-band (non-management) interface, the CoPP profile may need tweaks especially when multiple logging servers are configured, and when lot of syslogs get generated in a short time (such as boot up, configuration application, and so on).

Platform related syslogs would be showing up only in the log file of the admin VDC or VDC 1 (default VDC) if the admin VDC is not in use. However, these events may impact the functionality of other VDCs (such as fabric CRC errors generated from specific modules, and so on). Hence it is required to configure syslog server in this VDC as well as have the IP reachability to syslog server in the admin VDC or VDC 1 (default VDC) in order to capture and monitor platform related syslog events.

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
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.

Step 3	[**no**] **logging console** [*severity-level*] **Example:** `switch(config)# logging console 3`	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: • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging 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.
Step 4	(Optional) **show logging console** **Example:** `switch(config)# show logging console`	Displays the console logging configuration.

	Command or Action	Purpose
Step 5	[**no**] **logging monitor** [*severity-level*] **Example:** `switch(config)# logging monitor 3`	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: • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging The configuration applies to Telnet and SSH sessions. 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.

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 log:messages.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **logging logfile** *logfile-name severity-level* [**size** *bytes*] **Example:** `switch(config)# logging logfile my_log 6`	Configures the name of the log file used to store system messages and the minimum severity level to log. When you configure a new logfile without specifying the size, the existing/previously specified logfile size is assigned and the default file size is not considered. A lower number indicates a higher severity level. Severity levels range from 0 to 7: • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging You can optionally specify a maximum file size. The default severity level is 5, and the file size is 10485760. The file size is from 4096 to 4194304 bytes.

Step 3	**logging event** {**link-status** | **trunk-status**} {**enable** | **default**}
	Example:
	`switch# logging event link-status default`
	`switch(config)#`
		Logs interface events.
		• **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 not explicitly configured.

	Command or Action	Purpose
Step 4	(Optional) **show logging info** **Example:** `switch(config)# show logging info`	Displays the logging 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 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:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **logging module** [*severity-level*] **Example:** `switch(config)# logging module 3`	Enables module log messages that have the specified severity level or higher. Severity levels range from 0 to 7: • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging If the severity level is not specified, the default of 5 is used. The **no** option disables module log messages.
Step 3	(Optional) **show logging module** **Example:** `switch(config)# show logging module`	Displays the module logging configuration.

	Command or Action	Purpose
Step 4	[**no**] **logging level** *facility severity-level* **Example:** `switch(config)# logging level aaa 2`	Enables logging messages from the specified facility that have the specified severity level or higher. Severity levels range from 0 to 7: • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging To apply the same severity level to all facilities, use the **all** facility. For defaults, see the **show logging level** command. 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.
Step 5	(Optional) **show logging level** [*facility*] **Example:** `switch(config)# show logging level aaa`	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	[**no**] **logging timestamp** {**microseconds** | **milliseconds** | **seconds**} **Example:** `switch(config)# logging timestamp milliseconds`	Sets the logging time-stamp units. By default, the units are seconds. **Note** This command applies to logs that are kept in the switch. It does not apply to the external logging server.
Step 7	(Optional) **show logging timestamp** **Example:** `switch(config)# show logging timestamp`	Displays the logging time-stamp units configured.
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 Syslog Servers

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

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 the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **logging server** *host* [*severity-level* [**use-vrf** *vrf-name*]]
	Example:
	`switch(config)# logging server 192.0.2.253`
	Example:
	`switch(config)# logging server 2001:db8::3 5 use-vrf red`
		Configures a syslog server at the specified hostname or IPv4 or IPv6 address. You can limit logging of messages to a particular VRF by using the **use-vrf** keyword. Severity levels range from 0 to 7:
		• 0 – emergency
		• 1 – alert
		• 2 – critical
		• 3 – error
		• 4 – warning
		• 5 – notification
		• 6 – informational
		• 7 – debugging
		The default outgoing facility is local7.
		The **no** option removes the logging server for the specified host.
		The first example forwards all messages on facility local 7. The second example forwards messages with severity level 5 or lower for VRF red.

Step 3	Required: **logging source-interface loopback** *virtual-interface* **Example:**	Enables a source interface for the remote syslog server. The range for the *virtual-interface* argument is from 0 to 1023.

	Command or Action	Purpose
	`switch(config)# logging source-interface loopback 5`	
Step 4	**logging source-interface** *interface* **Example:** `switch(config)# logging source-interface loopback 5`	Sets the source interface whose IP address is displayed in the log messages. This static configuration ensures that same IP address appears in all log messages that are sent from an individual Cisco NX-OS device.
Step 5	(Optional) **show logging server** **Example:** `switch(config)# show logging server`	Displays the syslog server configuration. **Note** The output of this command will display the syslog server configuration details along with a message stating This server is temporarily unreachable." Please ignore this message.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Example

This example shows how to configure a syslog server along with a verification command showing the syslog server details:

```
switch# configure terminal
switch(config)# logging server 1.1.1.1 use-vrf management

switch# show logging server
ogging server:                 enabled
{1.1.1.1}
        This server is temporarily unreachable  //Please note that this does not indicate
that IP address 1.1.1.1 is unreachable.
        server severity:        notifications
        server facility:        local7
        server VRF:             management
        server port:            514
```

In the **show logging server** command output displayed above, the message stating "This server is temporarily unreachable" is displayed for 15 seconds. Please note that this does not indicate that IP address 1.1.1.1 is unreachable. After the syslog server is configured, the switch will buffer any syslog message that is received in the initial 15 seconds. A maximum of 100 syslog messages are buffered in the initial 15 seconds.

If a new syslog message is generated after 15 seconds, address resolution is triggered. If address resolution is successful, the message stating that the server is temporarily unreachable is removed. The subsequent syslog messages are sent to the server along with the previously buffered syslog message logs. The **show logging server** command output for a scenario in which address resolution is successful is as given below.

```
switch# show logging server
Logging server:                 enabled
{1.1.1.1}
        server severity:        notifications
        server facility:        local7
        server VRF:             management
        server port:            514
```

If a DNS name is specified as the logging server, the switch discards all syslog messages that are generated after the initial 15 seconds until address resolution succeeds. If an IPv4/IPv6 address is specified as the logging server, only the first syslog message that is generated after the initial 15 seconds is discarded.

Configuring Destination Port for Forwarding Syslogs

You can specify the destination port to be used while forwarding the system messages to the remote server where they will be logged.

Note You will need to change the remote server syslog configuration file to listen to the specified user-defined port. By default, system messages are sent as a UDP payload over port number 514 to the remote server for logging.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **logging server** *host* [*severity-level* [**use-vrf** *vrf-name*]]
	Example:
	`switch(config)# logging server 192.0.2.253 port 600`
	Example:
	`switch(config)# logging server 192.0.2.253 5 port 600`
		Specifies the destination port on which the syslogs are forwarded to remote server. The port numbers range from 1 to 65535.
		The default destination port number is 514.
		Note To remove the custom destination port or to reset it to its default value, use the **logging server** command without specifying any port number. Optionally, you can specify the port number as 514.
		The first example forwards all messages on user-defined port number 600. The second example forwards messages with severity level 5 or lower on user-defined port number 600.

Step 3	(Optional) **show logging server** **Example:**	Displays the syslog server configuration.

	Command or Action	Purpose
	`switch(config)# show logging server`	
Step 4	(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.
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** *number-lines* **Example:** `switch# show logging last 40`	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** [**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 3	**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 4	**clear logging logfile** **Example:** `switch# clear logging logfile`	Clears the contents of the log file.
Step 5	**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 [**start-time** *yyyy mmm dd hh:mm:ss*] [**end-time** *yyyy mmm dd hh:mm:ss*]	Displays the messages 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 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 CLI commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*
System messages	*Cisco NX-OS System Messages Reference*

Feature History for System Message Logging

The table below summarizes the new and changed features for this document and shows the releases in which each feature is supported. Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 4: Feature History for System Message Logging

Feature Name	Releases	Feature Information
System message logging	7.2(0)D1(1)	This feature was introduced.
System message logging	5.2(1)	Added the ability to add the description for physical Ethernet interfaces and subinterfaces in the system message log.
Syslog servers	5.1(1)	Increased the number of supported syslog servers from three to eight.
IPv6 support	4.2(1)	Added support for IPv6 syslog hosts..
System message logging	4.0(1)	This feature was introduced.