Configuring System Message Logging

This chapter contains the following sections:

Information 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 Cisco Nexus device outputs messages to terminal sessions.

By default, the switch 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

Level	Description
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 switch 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

Syslog servers run on remote systems that are configured to log system messages based on the syslog protocol. You can configure the Cisco Nexus Series switch to sends logs to up to eight 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 switch first initializes, messages are sent to syslog servers only after the network is initialized.

Licensing Requirements for System Message Logging

Product	License Requirement
Cisco NX-OS	System message logging requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

Guidelines and Limitations for System Message Logging

System messages are logged to the console and the logfile by default.

Default Settings for System Message Logging

The following table lists the default settings for 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 2
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

Configuring System Message Logging to Terminal Sessions

You can configure the switch to log messages by their severity level to console, Telnet, and Secure Shell sessions.

By default, logging is enabled for terminal sessions.

Procedure

	Command or Action	Purpose
Step 1	switch# **terminal monitor**	Copies syslog messages from the console to the current terminal session.

	Command or Action	Purpose
Step 2	switch# **configure terminal**	Enters global configuration mode.
Step 3	switch(config)# **logging console** [*severity-level*]	Enables the switch to log messages to the console session based on a specified severity level or higher (a lower number value 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.
Step 4	switch(config)# **no logging console** [*severity-level*]	(Optional) Disables logging messages to the console.
Step 5	switch(config)# **logging monitor** [*severity-level*]	Enables the switch to log messages to the monitor based on a specified severity level or higher (a lower number value 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 configuration applies to Telnet and SSH sessions.
Step 6	switch(config)# **no logging monitor** [*severity-level*]	(Optional) Disables logging messages to Telnet and SSH sessions.

	Command or Action	Purpose
Step 7	switch# **show logging console**	(Optional) Displays the console logging configuration.
Step 8	switch# **show logging monitor**	(Optional) Displays the monitor logging configuration.
Step 9	switch# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure a logging level of 3 for the console:

```
switch# configure terminal
switch(config)# logging console 3
```

The following example shows how to display the console logging configuration:

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

The following example shows how to disable logging for the console:

```
switch# configure terminal
switch(config)# no logging console
```

The following example shows how to configure a logging level of 4 for the terminal session:

```
switch# terminal monitor
switch# configure terminal
switch(config)# logging monitor 4
```

The following example shows how to display the terminal session logging configuration:

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

The following example shows how to disable logging for the terminal session:

```
switch# configure terminal
switch(config)# no logging monitor
```

Configuring System Message Logging to a File

You can configure the switch 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	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **logging logfile** *logfile-name severity-level* [**size** *bytes*]	Configures the name of the log file used to store system messages and the minimum severity level to log. You can

	Command or Action	Purpose
		optionally specify a maximum file size. The default severity level is 5 and the file size is 4194304. Severity levels range from 0 to 7: • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging The file size is from 4096 to 10485760 bytes.
Step 3	switch(config)# **no logging logfile** [*logfile-name severity-level* [**size** *bytes*]]	(Optional) Disables logging to the log file. You can optionally specify a maximum file size. The default severity level is 5 and the file size is 4194304.
Step 4	switch# **show logging info**	(Optional) Displays the logging configuration. You can optionally specify a maximum file size. The default severity level is 5 and the file size is 4194304.
Step 5	switch# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure a switch to log system messages to a file:

```
switch# configure terminal
switch(config)# logging logfile my_log 6 size 4194304
```

The following example shows how to display the logging configuration (some of the output has been removed for brevity):

```
switch# show logging info
Logging console:                 enabled (Severity: debugging)
Logging monitor:                 enabled (Severity: debugging)
Logging linecard:                enabled (Severity: notifications)
Logging fex:                     enabled (Severity: notifications)
Logging timestamp:               Seconds
Logging server:                  disabled
Logging logfile:                 enabled
        Name - my_log: Severity - informational Size - 4194304
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     3                       3
aclmgr                        3                             3
afm                     3                       3
```

```
altos                3                3
auth                 0                0
authpriv             3                3
bootvar              5                5
callhome             2                2
capability           2                2
cdp                  2                2
cert_enroll          2                2
...
```

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	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **logging module** [*severity-level*]	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.
Step 3	switch(config)# **logging level** *facility severity-level*	Enables logging messages from the specified facility that have the specified severity level or higher. Severity levels from 0 to 7: • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging

	Command or Action	Purpose
		To apply the same severity level to all facilities, use the all facility. For defaults, see the **show logging level** command. **Note** If the default severity and current session severity of a component is the same, then the logging level for the component will not be displayed in the running configuration.
Step 4	switch(config)# **no logging module** [*severity-level*]	(Optional) Disables module log messages.
Step 5	switch(config)# **no logging level** [*facility severity-level*]	(Optional) Resets the logging severity level for the specified facility to its default level. If you do not specify a facility and severity level, the switch resets all facilities to their default levels.
Step 6	switch# **show logging module**	(Optional) Displays the module logging configuration.
Step 7	switch# **show logging level** [*facility*]	(Optional) Displays the logging level configuration and the system default level by facility. If you do not specify a facility, the switch displays levels for all facilities.
Step 8	switch# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure the severity level of module and specific facility messages:

```
switch# configure terminal
switch(config)# logging module 3
switch(config)# logging level aaa 2
```

Configuring Logging Timestamps

You can configure the time-stamp units of messages logged by the Cisco Nexus Series switch.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **logging timestamp** {**microseconds** | **milliseconds** | **seconds**}	Sets the logging time-stamp units. By default, the units are seconds.

	Command or Action	Purpose
Step 3	switch(config)# **no logging timestamp** {**microseconds** | **milliseconds** | **seconds**}	(Optional) Resets the logging time-stamp units to the default of seconds.
Step 4	switch# **show logging timestamp**	(Optional) Displays the logging time-stamp units configured.
Step 5	switch# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure the time-stamp units of messages:

```
switch# configure terminal
switch(config)# logging timestamp milliseconds
switch(config)# exit
switch# show logging timestamp
Logging timestamp:              Milliseconds
```

Configuring Syslog Servers

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

Step 2	**logging server** *host* [*severity-level* [**use-vrf** *vrf-name* [**facility** *facility*]]] **Example:** `switch(config)# logging server 172.28.254.254 5 use-vrf default facility local3`	Configures a host to receive syslog messages. • The *host* argument identifies the hostname or the IPv4 or IPv6 address of the syslog server host. • The *severity-level* argument limits the logging of messages to the syslog server to a specified level. Severity levels range from 0 to 7. See Table 1: System Message Severity Levels , on page 1. • The **use vrf** *vrf-name* keyword and argument identify the *default* or *management* values for the virtual routing and forwarding (VRF) name. If a specific VRF is not identified, management is the default. However, if management is configured, it will not be listed in the output of the **show-running** command because it is the default. If a

	Command or Action	Purpose
		specific VRF is configured, the **show-running** command output will list the VRF for each server. **Note** The current Cisco Fabric Services (CFS) distribution does not support VRF. If CFS distribution is enabled, the logging server configured with the default VRF is distributed as the management VRF. • The facility argument names the syslog facility type. The default outgoing facility is local7. The facilities are listed in the command reference for the Cisco Nexus Series software that you are using. **Note** Debugging is a CLI facility but the debug syslogs are not sent to the server.
Step 3	**no logging server** *host* **Example:** `switch(config)# no logging server 172.28.254.254 5`	(Optional) Removes the logging server for the specified host.
Step 4	**show logging server** **Example:** `switch# show logging server`	(Optional) Displays the syslog server configuration.
Step 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following examples show how to configure a syslog server:

```
switch# configure terminal
switch(config)# logging server 172.28.254.254 5
use-vrf default facility local3

switch# configure terminal
switch(config)# logging server 172.28.254.254 5 use-vrf management facility local3
```

Configuring syslog 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 (@), or 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:

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

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

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

Step 3 Make sure that the system message logging daemon reads the new changes by checking myfile.log after entering this command:

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

Configuring syslog Server Configuration Distribution

You can distribute the syslog server configuration to other switches in the network by using the Cisco Fabric Services (CFS) infrastructure.

After you enable syslog server configuration distribution, you can modify the syslog server configuration and view the pending changes before committing the configuration for distribution. As long as distribution is enabled, the switch maintains pending changes to the syslog server configuration.

Note If the switch is restarted, the syslog server configuration changes that are kept in volatile memory might get lost.

Before You Begin

You must have configured one or more syslog servers.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **logging distribute**	Enables distribution of the syslog server configuration to network switches using the CFS infrastructure. By default, distribution is disabled.
Step 3	switch(config)# **logging commit**	Commits the pending changes to the syslog server configuration for distribution to the switches in the fabric.
Step 4	switch(config)# **logging abort**	Cancels the pending changes to the syslog server configuration.
Step 5	switch(config)# **no logging distribute**	(Optional) Disables the distribution of the syslog server configuration to network switches using the CFS infrastructure. You cannot disable distribution when configuration changes are pending. See the **logging commit** and **logging abort** commands. By default, distribution is disabled.
Step 6	switch# **show logging pending**	(Optional) Displays the pending changes to the syslog server configuration.
Step 7	switch# **show logging pending-diff**	(Optional) Displays the differences from the current syslog server configuration to the pending changes of the syslog server configuration.
Step 8	switch# **show logging internal info**	(Optional) Displays information about the current state of the syslog server distribution and the last action taken.
Step 9	switch# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

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	switch# **show logging last** *number-lines*	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	switch# **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 that have a time stamp 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	switch# **show logging nvram** [**last** *number-lines*]	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	switch# **clear logging logfile**	Clears the contents of the log file.
Step 5	switch# **clear logging nvram**	Clears the logged messages in NVRAM.

The following example shows how to display messages in a log file:

```
switch# show logging last 40
switch# show logging logfile start-time 2007 nov 1 15:10:0
switch# show logging nvram last 10
```

The following example shows how to clear messages in a log file:

```
switch# clear logging logfile
switch# clear logging nvram
```

Verifying the System Message Logging Configuration

Use these commands to verify system message logging configuration information:

Command	Purpose
show logging console	Displays the console logging configuration.
show logging info	Displays the logging configuration.
show logging internal info	Displays the syslog distribution information.
show logging ip access-list cache	Displays the IP access list cache.

Command	Purpose
show logging ip access-list cache detail	Displays detailed information about the IP access list cache.
show logging ip access-list status	Displays the status of the IP access list cache.
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 pending	Displays the syslog server pending distribution configuration.
show logging pending-diff	Displays the syslog server pending distribution configuration differences.
show logging server	Displays the syslog server configuration.
show logging session	Displays the logging session status.
show logging status	Displays the logging status.
show logging timestamp	Displays the logging time-stamp units configuration.
show running-config acllog	Displays the running configuration for the ACL log file.

Configuring ACL Logging

Information About ACL Logging

The Access Control List (ACL) logging feature allows the logging of the packets which hit the IPv4 ACLs. The log message is displayed on a flow basis. The flow is identified using the combination of IP source address, destination address, Layer 4 protocol, and the Layer 4 source/destination ports on an interface. The log message is generated based on the following conditions:

- When a new flow is created (INFO message)
- When the flow's packet threshold is reached (WARNING message)
- At the end of a periodic interval (default five minutes) with the information about how many packets hit the flow (INFO message - configurable)

Along with the above, when the number of flows exceeds a threshold in a given interval, a warning message is logged and the flow is not added to the logging cache.

The following table describes the limitation in the Cisco Nexus device.

Except for the VTY ACL, all other ACLs support ACL logging for only the "deny" ACE entries. However, since the same ACL can be applied for both vty ACL and other features, "permit <> log" CLI cannot be blocked. However, applying such an ACL to any of the interfaces/vlans can be prevented. Mgmt0 supports permit logging.

In the Cisco Nexus device, CTS is not supported, therefore RBACL is not supported.

ACL logging is not supported for IPv6 and MAC ACLs. It is supported on all interfaces where PACL, RACL, VACL and VTY can be applied, including FEX HIF interfaces.

The ACL logging is rate-limited. All the packets that hit the ACL are not sent to the sup. The rate limiter function is per switch and is applied across all ASIC and TCAM regions. The following CLIs will be provided to configure the rate.

Configuring the ACL Logging Cache

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **logging ip access-list cache entries** *num_entries*	Sets the maximum number of log entries cached in software. The range is from 0 to 1000000 entries. The default value is 8000 entries.
Step 3	switch(config)# **logging ip access-list cache interval** *seconds*	Sets the number of seconds between log updates. Also if an entry is inactive for this duration, it is removed from the cache. The range is from 5 to 86400 seconds. The default value is 300 seconds.
Step 4	switch(config)# **logging ip access-list cache threshold** *num_packets*	Sets the number of packet matches before an entry is logged. The range is from 0 to 1000000 packets. The default value is 0 packets, which means that logging is not triggered by the number of packet matches.
Step 5	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example show how to set the maximum number of log entries to 5000, the interval to 120 seconds, and the threshold to 500000:

```
switch# configure terminal
switch(config)# logging ip access-list cache entries 5000
switch(config)# logging ip access-list cache interval 120
switch(config)# logging ip access-list cache threshold 500000
switch(config)# copy running-config startup-config
```

Applying ACL Logging to an Interface

Before You Begin

- Create an IP access list with at least one access control entry (ACE) configured for logging.
- Configure the ACL logging cache.
- Configure the ACL log match level.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface mgmt0**	Specifies the mgmt0 interface.
Step 3	switch(config-if)# **ip access-group** *name* **in**	Enables ACL logging on ingress traffic for the specified interface.
Step 4	switch(config-if)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

The following example shows how to apply the mgmt0 interface with the logging specified in acl1 for all ingress traffic:

```
switch# configure terminal
switch(config)# interface mgmt0
switch(config-if)# ip access-group acl1 in
switch(config-if)# copy running-config startup-config
```

Configuring VLAN Access Map with Logging

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **vlan access-map** *map-name*	Enters access map configuration mode for the access map specified.
Step 3	switch(config-access-map)# **match ip address** *ip-access-list*	Specifies an IPv4 and IPv6 ACL for the map.
Step 4	switch(config-access-map)# **action drop log**	Specifies the action that the switch applies to traffic that matches the ACL.
Step 5	switch(config-access-map)# **exit**	Exits access map configuration mode.

This example shows how to create a VLAN access map for logging.

```
switch# configure terminal
switch(config)# vlan access-map vacl1
switch(config-access-map)# match ip address pacl1
switch(config-access-map)# action drop log
switch(config-access-map)# exit
switch(config)#
```

Configuring the ACL Log Match Level

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **acllog match-log-level** *number*	Specifies the logging level to match for entries to be logged in the ACL log (acllog). The *number* is a value from 0 to 7. The default is 6. **Note** For log messages to be entered in the logs, the logging level for the ACL log facility (acllog) and the logging severity level for the logfile must be greater than or equal to the ACL log match log level setting. For more information, see Configuring Module and Facility Messages Logging, on page 7 and Configuring System Message Logging to a File, on page 5.

	Command or Action	Purpose
Step 3	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Configuring Rate Limiter for ACL Logging

You can limit the number of logged packets that are sent to the supervisor (CPU) to be logged to the cache.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	**hardware rate-limiter access-list-log packets** *num-packets*	*num-packets*—Value in packets per second. Valid range is 50 to 600000. The default is 100 packets per second.

This example shows how to set the rate limiter to 1000 packets per second.

```
switch# configure terminal
switch(config)# hardware rate-limiter access-list-log packets 1000
```

Clearing ACL Logs

You can clear the ACL logs.

Procedure

	Command or Action	Purpose
Step 1	switch# **clear logging ip access-list cache**	Clears the IP configuration access list cache.

Verifying ACL Logging

Use one of the following commands to verify the configuration:

Command	Purpose
show logging ip access-list status	Displays the ACLLOG status.

Command	Purpose
show logging ip access-list cache [**detail**]	Displays the entries in cache and optionally additional details.
show acllog status	Displays flow counts and rate limits
show acllog flows	Displays the currently active logged flows.