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 supports IPv4 and IPv6 addresses.

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.

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.

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

Level	Description
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.

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

Syslog servers run on remote systems that are configured to log system messages based on the syslog protocol. You can configure up to three syslog servers.

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

System Message Logging Facilities

The following table lists the facilities that you can use in the system message logging configuration.

Facility	Description
aaa	AAA manager
aclmgr	ACL manager
adjmgr	Adjacency Manager
all	Keyword that represents all facilities
arbiter	Arbiter manager
arp	ARP manager
auth	Authorization system
authpriv	Private authorization system
bootvar	Bootvar
callhome	Call home manager
capability	MIG utilities daemon
cdp	CDP manager
cert-enroll	Certificate enroll daemon
cfs	CFS manager
clis	CLIS manager
cmpproxy	CMP proxy manager

Facility	Description
copp	CoPP manager
core	Core daemon
cron	Cron and at scheduling service
daemon	System daemons
dhcp	DHCP manager
diagclient	GOLD diagnostic client manager
diagmgr	GOLD diagnostic manager
eltm	ELTM manager
ethpm	Ethernet PM manager
evmc	EVMC manager
evms	EVMS manager
feature-mgr	Feature manager
fs-daemon	FS daemon
ftp	File transfer system
glbp	GLBP manager
hsrp	HSRP manager
im	IM manager
ipconf	IP configuration manager
ipfib	IP FIB manager
kernel	OS kernel
l2fm	L2 FM manager
l2nac	L2 NAC manager
l3vm	L3 VM manager
license	Licensing manager
local0	Local use daemon
local1	Local use daemon
local2	Local use daemon
local3	Local use daemon

Facility	Description
local4	Local use daemon
local5	Local use daemon
local6	Local use daemon
local7	Local use daemon
lpr	Line printer system
m6rib	M6RIB manager
mail	Mail system
mfdm	MFDM manager
module	Module manager
monitor	Ethernet SPAN manager
mrib	MRIB manager
mvsh	MVSH manager
news	USENET news
nf	NF manager
ntp	NTP manag
otm	GLBP manager
pblr	PBLR manager
pfstat	PFSTAT manager
pixm	PIXM manager
pixmc	PIXMC manager
pktmgr	Packet manager
platform	Platform manager
pltfm_config	PLTFM configuration manager
plugin	Plug-in manager
port-channel	Port channel manager
port_client	Port client manager
port_lb	Diagnostic port loopback test manager
qengine	Q engine manager

Facility	Description
radius	RADIUS manager
res_mgr	Resource manager
rpm	RPM manager
security	Security manager
session	Session manager
spanning-tree	Spanning tree manager
syslog	Internal syslog manager
sysmgr	System manager
tcpudp	TCP and UDP manager
u2	U2 manager
u6rib	U6RIB manager
ufdm	UFDM manager
urib	URIB manager
user	User process
uucp	Unix-to-Unix copy system
vdc_mgr	VDC manager
vlan_mgr	VLAN manager
vmm	VMM manager
vshd	VSHD manager
xbar	XBAR manager
xbar_client	XBAR client manager
xbar_driver	XBAR driver manager
xml	XML agent

Guidelines and Limitations for System Message Logging

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

Default System Message Logging Settings

Parameter	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

This section includes the following topics:

- Configuring System Message Logging to Terminal Sessions
- Restoring System Message Logging Defaults for Terminal Sessions
- Configuring System Message Logging for Modules
- Restoring System Message Logging Defaults for Modules
- Configuring System Message Logging for Facilities
- Restoring System Message Logging Defaults for Facilities
- Configuring syslog Servers
- Restoring System Message Logging Defaults for Servers
- Using a UNIX or Linux System to Configure Logging
- Displaying Log Files

Configuring System Message Logging to Terminal Sessions

You can log messages by severity level to console, Telnet, and Secure Shell (SSH) sessions. By default, logging is enabled for terminal sessions.

Procedure

	Command or Action	Purpose
Step 1	switch# **terminal monitor**	Enables the device to log messages to the console.
Step 2	switch# **configure terminal**	Enters global configuration mode.
Step 3	switch(config)# **logging console** [*severity-level*]	Configures the device to log messages to the console session based on a specified severity level or higher. The default severity level is 2.
Step 4	switch(config)# **show logging console**	(Optional) Displays the console logging configuration.
Step 5	switch(config)# **logging monitor** [*severity-level*]	Enables the device to log messages to the monitor based on a specified severity level or higher. The configuration applies to Telnet and SSH sessions. The default severity level is 2.
Step 6	switch(config)# **show logging monitor**	(Optional) Displays the monitor logging configuration.
Step 7	(Optional) switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to configure system messages:

```
switch# terminal monitor
switch# configure terminal
switch(config)# logging console 2
switch(config)# show logging console
Logging console: enabled (Severity: critical)
switch(config)# logging monitor 3
switch(config)# show logging monitor
Logging monitor: enabled (Severity: errors)
switch(config)# copy running-config startup-config
switch(config)#
```

Restoring System Message Logging Defaults for Terminal Sessions

You can use the following commands in global configuration mode to restore default settings for system message logging for terminal sessions.

Command	Description
no logging console [*severity-level*]	Disables the device from logging messages to the console.
no logging monitor [*severity-level*]	Disables logging messages to Telnet and SSH sessions.

Configuring System Message Logging for Modules

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

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. If the severity level is not specified, the default of 5 is used.
Step 3	switch(config)# **show logging module**	
Step 4	switch(config)# **logging timestamp** {**microseconds** | **milliseconds** | **seconds**}	(Optional) Sets the logging time-stamp units. The default unit is seconds.
Step 5	switch(config)# show logging timestamp	(Optional) Displays the logging time-stamp units configured.
Step 6	(Optional) switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to configure system message logging for modules:

```
switch# configure terminal
switch(config)# logging module 3
switch(config)# show logging module
Logging linecard: enabled (Severity: errors)
switch(config)# logging timestamp microseconds
switch(config)# show logging timestamp
Logging timestamp: Microseconds
switch(config)# copy running-config startup-config
switch(config)#
```

Restoring System Message Logging Defaults for Modules

You can use the following commands in the global configuration mode to restore default settings for system message logging for modules.

Command	Description
no logging module [*severity-level*]	Restores the default severity level for logging module system messages.
no logging timestamp {**microseconds** | **milliseconds** | **seconds**}	Resets the logging time-stamp unit to the default (seconds).

Configuring System Message Logging for Facilities

You can use this procedure to configure the severity level and time-stamp units of messages logged by 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. If the severity level is not specified, the default of 5 is used.
Step 3	switch(config)# **show logging module**	(Optional) Displays the module logging configuration.
Step 4	switch(config)# **logging timestamp** {**microseconds** | **milliseconds** | **seconds**}	Sets the logging time-stamp units. The default unit is seconds.
Step 5	switch(config)# **show logging timestamp**	(Optional) Copies the running configuration to the startup configuration.
Step 6	(Optional) switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to configure system message logging for modules:

```
switch# configure terminal
switch(config)# logging module 3
switch(config)# show logging module
Logging linecard: enabled (Severity: errors)
switch(config)# logging timestamp microseconds
switch(config)# show logging timestamp
Logging timestamp: Microseconds
switch(config)# copy running-config startup-config
switch(config)#
```

Restoring System Message Logging Defaults for Facilities

You can use the following commands to restore system message logging defaults for facilities.

Command	Description
no logging level [*facility severity-level*]	Restores the default logging severity level for the specified facility. If you do not specify a facility and severity level, the device resets all facilities to their default levels.

Command	Description
no logging timestamp {**microseconds** | **milliseconds** | **seconds**}	Resets the logging time-stamp unit to the default (seconds).

Configuring syslog Servers

You can configure syslog servers for system message logging.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **logging server** *host* [*severity-level* [**use-vrf** *vrf-name*]]	Configures a syslog server at the specified hostname or IPv4 or IPv6 address. You can limit logging of messages to a particular Virtual routing and forwarding (VRF) by using the use_vrf keyword. Severity levels range from 0 to 7. The default outgoing facility is local7.
Step 3	switch(config)# **show logging server**	(Optional) Displays the syslog server configuration.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to forward all messages on facility local7.

```
switch# configure terminal
switch(config)# logging server 10.10.2.2 7
switch(config)# show logging server
Logging server: enabled {10.10.2.2}
        server severity: debugging
        server facility: local7
switch(config)# copy running-config startup-config
switch(config)#
```

Restoring System Message Logging Defaults for Servers

You can use the following command to restore server system message logging default.

Command	Description
no logging server *host*	Removes the logging server for the specified host.

Using a UNIX or Linux System to Configure Logging

Before you begin

The following UNIX or Linux fields must be configured for syslog.

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 On the UNIX or Linux system, add the following line to the file, /var/log/myfile.log:

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

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~
```

Displaying Log Files

You can display messages in the log file.

Procedure

	Command or Action	Purpose
Step 1	**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.

Example

This example shows how to display the last five lines in the logging file:

```
switch# show logging last 5
2008 Aug 31 09:37:04 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
2008 Aug 31 09:37:04 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
2008 Aug 31 09:37:05 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
2008 Aug 31 09:37:05 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
2008 Aug 31 09:37:05 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
switch#
```

Verifying the System Message Logging Configuration

Use one of the following commands to verify the configuration:

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 logging level
show logging module	Displays the module logging configuration.
show logging monitor	Displays the monitor logging configuration.
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.

This example shows how to display the console logging configuration:

```
switch# show logging console
Logging console:                disabled
switch#
```

This example shows how to display the logging configuration:

```
switch# show logging info
Logging console:                enabled (Severity: critical)
Logging monitor:                enabled (Severity: notifications)
Logging linecard:               enabled (Severity: notifications)
Logging timestamp:              Seconds
Logging server:                 disabled
Logging logfile:                enabled
        Name - g/external/messages: Severity - notifications Size - 4194304

Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     2                       2
auth                    0                       0
authpriv                3                       3
bootvar                 5                       5
callhome                2                       2
cdp                     2                       2
cert_enroll             2                       2
cfs                     3                       3
confcheck               2                       2
cron                    3                       3
daemon                  3                       3
diagclient              2                       2
diagmgr                 2                       2
eth_port_channel        5                       5
ethpm                   5                       5
evmc                    5                       5
evms                    2                       2
feature-mgr             2                       2
ftp                     3                       3
ifmgr                   5                       5
igmp_1                  3                       3
ip                      2                       2
ipv6                    2                       2
kern                    6                       6
l2fm                    2                       2
licmgr                  6                       6
local0                  3                       3
local1                  3                       3
local2                  3                       3
local3                  3                       3
local4                  3                       3
local5                  3                       3
local6                  3                       3
local7                  3                       3
lpr                     3                       3
mail                    3                       3
mfdm                    2                       2
module                  5                       5
monitor                 7                       7
msp                     2                       2
mvsh                    2                       2
news                    3                       3
ntp                     2                       2
otm                     3                       3
pblr                    2                       2
pixm                    2                       2
pixmc                   2                       2
platform                5                       5
```

```
portprofile             5                       5
private-vlan            3                       3
radius                  2                       2
res_mgr                 2                       2
rpm                     2                       2
sal                     2                       2
securityd               2                       2
sksd                    3                       3
stp                     3                       3
syslog                  3                       3
sysmgr                  3                       3
ufdm                    2                       2
urib                    3                       3
user                    3                       3
uucp                    3                       3
vdc_mgr                 6                       6
vim                     5                       5
vlan_mgr                2                       2
vms                     5                       5
vshd                    5                       5
xmlma                   3                       3

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
switch#
```

This example shows how to display the last number of lines of the log file:

```
switch# show logging last 5
2008 Jul 29 17:52:42 S22-DCOS %ETHPORT-5-IF_UP: Interface Ethernet2/5 is up in mode access
2008 Jul 29 17:52:43 S22-DCOS %ETHPORT-5-IF_UP: Interface Ethernet2/2 is up in mode trunk
2008 Jul 29 17:52:43 S22-DCOS %ETHPORT-5-IF_UP: Interface Ethernet2/4 is up in mode access
2008 Jul 29 17:53:04 S22-DCOS %SYSMGR-3-BASIC_TRACE: process_cfg_write: PID 1858 with message
 rcvd cfg_action from
sap 0x545 for vdc 1 at time 1217353984 .
2008 Jul 29 17:53:04 S22-DCOS clis[2558]: CLI-3-NVDB: Batched send failed for component:
clic
switch#
```

This example shows how to display the logging levels:

```
switch# show logging level aaa
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     2                       2

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
switch#
```

This example shows how to display the module logging configuration:

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

This example shows how to display the monitor logging configuration:

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

This example shows how to display the syslog server configuration:

```
switch# show logging server
Logging server:                 enabled
{10.10.2.2}
        server severity:        debugging
        server facility:        local7
switch#
```

This example shows how to display the logging session status:

```
switch# show logging session status
Last Action Time Stamp     : Fri Nov 18 11:28:55 1910
Last Action                : Distribution Enable
Last Action Result         : Success
Last Action Failure Reason : none
switch#
```

This example shows how to display the logging status:

```
switch# show logging status
Fabric Distribute     : Enabled
Session State         : IDLE
switch#
```

This example shows how to display the logging session status:

```
switch# show logging timestamp
Logging timestamp:              Seconds
switch#
```

System MEssage Logging Example Configuration

The following example shows how to configure system message logging:

```
switch# configure terminal
switch(config)# logging console 3
switch(config)# logging monitor 3
switch(config)# logging logfile my_log 6
switch(config)# logging module 3
switch(config)# logging level aaa 2
switch(config)# logging timestamp milliseconds
switch(config)# logging distribute
switch(config)# logging server 172.28.254.253
switch(config)# logging server 172.28.254.254 5 local3
switch(config)# logging commit
switch(config)# copy running-config startup-config
switch(config)#
```

Feature History for System Message Logging

Feature Name	Releases	Feature Information
System Message Logging	4.0(4)SV1(1)	This feature was introduced.