



## Implementing Logging Services

This module describes the new and revised tasks you need to implement logging services on the router.

The Cisco IOS XR Software provides basic logging services. Logging services provide a means to gather logging information for monitoring and troubleshooting, to select the type of logging information captured, and to specify the destinations of captured system logging (syslog) messages.



**Note** For more information about logging services on the Cisco IOS XR Software and complete descriptions of the logging commands listed in this module, see the [Related Documents, on page 29](#) section of this module.

### Feature History for Implementing Logging Services

| Release       | Modification                                                                                   |
|---------------|------------------------------------------------------------------------------------------------|
| Release 5.0.0 | This feature was introduced.                                                                   |
| Release 6.1.2 | Platform Automated Monitoring (PAM) tool was introduced for all Cisco IOS XR 64-bit platforms. |

- [Prerequisites for Implementing Logging Services, on page 1](#)
- [Information About Implementing Logging Services, on page 2](#)
- [How to Implement Logging Services, on page 10](#)
- [Configuration Examples for Implementing Logging Services, on page 27](#)
- [Where to Go Next, on page 29](#)
- [Additional References, on page 29](#)

## Prerequisites for Implementing Logging Services

These prerequisites are required to implement logging services in your network operating center (NOC):

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

- You must have connectivity with syslog servers to configure syslog server hosts as the recipients for syslog messages.

## Information About Implementing Logging Services

### System Logging Process

By default, routers are configured to send syslog messages to a syslog process. The syslog process controls the distribution of messages to the destination of syslog messages such as the logging buffer, terminal lines, or a syslog server. The syslog process also sends messages to the console terminal by default.



**Note** For more information about how the syslog process functions within the Alarms and Debugging Event Management System (ALDEMS) infrastructure on Cisco IOS XR software, see *Implementing and Monitoring Alarms and Alarm Log Correlation on Cisco IOS XR Software*.

### Format of System Logging Messages

By default, the general format of syslog messages generated by the syslog process on the Cisco IOS XR software is as follows:

*node-id* : *timestamp* : *process-name* [*pid*] : % *message category* -*group* -*severity* -*message* -*code* : *message-text*

This is a sample syslog message:

```
RP/0/RP0/CPU0:router:Nov 28 23:56:53.826 : config[65710]: %SYS-5-CONFIG_I : Configured from console by console
```

This table describes the general format of syslog messages on Cisco IOS XR software.

**Table 1: General Syslog Message Format**

| Field                                                            | Description                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>node-id</i>                                                   | Node from which the syslog message originated.                                                                                                                                                                                                                                       |
| <i>timestamp</i>                                                 | Time stamp in the form <i>month day HH:MM:SS</i> , indicating when the message was generated.<br><br><b>Note</b> The time-stamp format can be modified using the <b>service timestamps</b> command. See the <a href="#">Modifying the Format of Time Stamps, on page 15</a> section. |
| <i>process-name</i>                                              | Process that generated the syslog message.                                                                                                                                                                                                                                           |
| [ <i>pid</i> ]                                                   | Process ID (pid) of the process that generated the syslog message.                                                                                                                                                                                                                   |
| % <i>category</i> - <i>group</i> - <i>severity</i> - <i>code</i> | Message category, group name, severity, and message code associated with the syslog message.                                                                                                                                                                                         |

| Field               | Description                                |
|---------------------|--------------------------------------------|
| <i>message-text</i> | Text string describing the syslog message. |

## Duplicate Message Suppression

Suppressing duplicate messages, especially in a large network, can reduce message clutter and simplify the task of interpreting the log. The duplicate message suppression feature substantially reduces the number of duplicate event messages in both the logging history and the syslog file. The suppression and logging process is the same for logging history and for external syslog servers.

When duplicate message suppression is enabled, two types of events are handled differently:

- New messages  
New messages are always logged immediately.
- Repeated messages  
Repeated messages are subject to suppression. The suppression of repeated messages is interrupted when a new message occurs.

For information about configuring this feature, see the [Suppressing Duplicate Syslog Messages, on page 17](#).

## Message Suppression

The first occurrence of an event is always logged immediately, but subsequent identical messages are suppressed during three different time intervals. Initially, duplicate messages are suppressed for 30 seconds after the first event, then for 120 seconds, and finally every 600 seconds (10 minutes). At the end of each interval, the next identical event triggers the “last message repeated *nm* times” message, and resets the count of duplicate messages. The end of the interval does not automatically trigger a message, so the summary message can be delayed well beyond the suppression interval.

For example, this syslog excerpt shows the log entries for repeated Telnet failures when the suppress duplicate feature `s` is enabled. In this case, Telnet failures occur at the rate of four per minute:

```
Jul 24 09:39:10 [10.1.1.1.2.2] 326: ROUTER-TEST TELNETD_[65778]: %IP-TELNETD-3-ERR_CONNECT
: Failed to obtain a VTY for a session: 'tty-server' detected the 'resource not available'
condition 'There are no TTYS available'
Jul 24 09:39:45 [10.1.1.1.2.2] 333: ROUTER-TEST last message repeated 2 times
Jul 24 09:41:50 [10.1.1.1.2.2] 358: ROUTER-TEST last message repeated 8 times
Jul 24 09:52:04 [10.1.1.1.2.2] 391: ROUTER-TEST last message repeated 40 times
Jul 24 10:02:35 [10.1.1.1.2.2] 412: ROUTER-TEST last message repeated 40 times
```

The first Telnet failure was logged at 9:39 as a normal error message. Thirty seconds later, a summary message reports two repetitions. Then after another 120 seconds, another message reports eight more repetitions. Finally, two more messages report the 40 repetitions that occurred in two consecutive 600-second intervals. Because the errors are occurring at regular 15-second intervals, a new error triggers a summary message just after the end of a suppression interval. The end of a suppression interval itself does not trigger a message.

## Logging History and Syslog Comparison

The logging process with suppression is the same for logging history and for external syslog servers. Both suppress duplicate messages using a sequence of suppression intervals. This example shows an excerpt from the `show logging history` command.

```

TELNETD_[65778]: %IP-TELNETD-3-ERR_CONNECT : ...
last message repeated 2 times
last message repeated 8 times
last message repeated 7 times
config[65677]: %MGBL-CONFIG-6-DB_COMMIT : ...
TELNETD_[65778]: %IP-TELNETD-3-ERR_CONNECT : ...

```

The logging history and syslog entries are the same in this case, but they can be different under other conditions. They can differ because of the severity level configured for each type of log and because of the timing of the log messages. Also, if there are just a few repeated messages that occur in less than 30 seconds, the reporting of duplicates can seem to be suppressed altogether. These duplicates ultimately are reported however, just before the next new event is logged.

## Syslog Message Destinations

Syslog message logging to the console terminal is enabled by default. To disable logging to the console terminal, use the **logging console disable** command in XR Config mode. To reenble logging to the console terminal, use the **logging console** command in XR Config mode.

Syslog messages can be sent to destinations other than the console, such as the logging buffer, syslog servers, and terminal lines other than the console (such as vtys).

This table lists the commands used to specify syslog destinations.

**Table 2: Commands Used to Set Syslog Destinations**

| Command                                | Description                                                                                       |
|----------------------------------------|---------------------------------------------------------------------------------------------------|
| <b>logging buffered</b>                | Specifies the logging buffer as a destination for syslog messages.                                |
| <b>logging</b> {hostname   ip-address} | Specifies a syslog server host as a destination for syslog messages. IPv4 and IPv6 are supported. |
| <b>logging monitor</b>                 | Specifies terminal lines other than the console as destinations for syslog messages.              |

The **logging buffered** command copies logging messages to the logging buffer. The buffer is circular, so newer messages overwrite older messages after the buffer is full. To display the syslog messages that are logged in the logging buffer, use the **show logging** command. The first message displayed is the oldest message in the buffer. To clear the current contents of the logging buffer, use the **clear logging** command. To disable logging to the logging buffer, use the **no logging buffered** command in XR Config mode.

The **logging** command identifies a syslog server host to receive logging messages. By issuing this command more than once, you build a list of syslog servers that receive logging messages. To delete the syslog server with the specified IP address (IPv4 and IPv6 are supported) or hostname from the list of available syslog servers, use the **no logging** command in XR Config mode.

The **logging monitor** command globally enables the logging of syslog messages to terminal lines other than the console, such as vtys. To disable logging to terminal lines other than the console, use the **no logging monitor** command in XR Config mode.

## Guidelines for Sending Syslog Messages to Destinations Other Than the Console

The logging process sends syslog messages to destinations other than the console terminal and the process is enabled by default. Logging is enabled to the logging buffer, terminal lines and syslog servers.

## Logging for the Current Terminal Session

The **logging monitor** command globally enables the logging of syslog messages to terminal lines other than console terminal. Once the **logging monitor** command is enabled, use the **terminal monitor** command to display syslog messages during a terminal session.

To disable the logging of syslog messages to a terminal during a terminal session, use the **terminal monitor disable** command in XR EXEC mode. The **terminal monitor disable** command disables logging for only the current terminal session.

To reenables the logging of syslog messages for the current terminal session, use the **terminal monitor** command in XR EXEC mode.




---

**Note** The **terminal monitor** and **terminal monitor disable** commands are set locally and will not remain in effect after the terminal session is ended.

---

## Syslog Messages Sent to Syslog Servers

The Cisco IOS XR Software provides these features to help manage syslog messages sent to syslog servers:

- UNIX system facilities
- Hostname prefix logging
- Source interface logging

## UNIX System Logging Facilities

You can configure the syslog facility in which syslog messages are sent by using the **logging facility** command. Consult the operator manual for your UNIX operating system for more information about these UNIX system facilities. The syslog format is compatible with Berkeley Standard Distribution (BSD) UNIX version 4.3.

This table describes the facility type keywords that can be supplied for the *type* argument.

**Table 3: Logging Facility Type Keywords**

| Facility Type Keyword | Description                            |
|-----------------------|----------------------------------------|
| auth                  | Indicates the authorization system.    |
| cron                  | Indicates the cron facility.           |
| daemon                | Indicates the system daemon.           |
| kern                  | Indicates the Kernel.                  |
| local0–7              | Reserved for locally defined messages. |
| lpr                   | Indicates line printer system.         |
| mail                  | Indicates mail system.                 |

| Facility Type Keyword | Description                         |
|-----------------------|-------------------------------------|
| news                  | Indicates USENET news.              |
| sys9                  | Indicates system use.               |
| sys10                 | Indicates system use.               |
| sys11                 | Indicates system use.               |
| sys12                 | Indicates system use.               |
| sys13                 | Indicates system use.               |
| sys14                 | Indicates system use.               |
| syslog                | Indicates the system log.           |
| user                  | Indicates user process.             |
| uucp                  | Indicates UNIX-to-UNIX copy system. |

## Hostname Prefix Logging

To help manage system logging messages sent to syslog servers, Cisco IOS XR Software supports hostname prefix logging. When enabled, hostname prefix logging appends a hostname prefix to syslog messages being sent from the router to syslog servers. You can use hostname prefixes to sort the messages being sent to a given syslog server from different networking devices.

To append a hostname prefix to syslog messages sent to syslog servers, use the **logging hostname** command in XR Config mode.

## Syslog Source Address Logging

By default, a syslog message contains the IP address (IPv4 and IPv6 are supported) of the interface it uses to leave the router when sent to syslog servers. To set all syslog messages to contain the same IP address, regardless of which interface the syslog message uses to exit the router, use the **logging source-interface** command in XR Config mode.

## UNIX Syslog Daemon Configuration

To configure the syslog daemon on a 4.3 BSD UNIX system, include a line such as the following in the `/etc/syslog.conf` file:

```
local7.debug /usr/adm/logs/cisco.log
```

The **debugging** keyword specifies the syslog level; see [Table 7: Syslog Message Severity Levels, on page 9](#) for a general description of other keywords. The **local7** keyword specifies the logging facility to be used; see [Table 7: Syslog Message Severity Levels, on page 9](#) for a general description of other keywords.

The syslog daemon sends messages at this level or at a more severe level to the file specified in the next field. The file must already exist, and the syslog daemon must have permission to write to it.

## Archiving Logging Messages on a Local Storage Device

Syslog messages can also be saved to an archive on a local storage device, such as the hard disk or a flash disk. Messages can be saved based on severity level, and you can specify attributes such as the size of the archive, how often messages are added (daily or weekly), and how many total weeks of messages the archive will hold.

### Setting Archive Attributes

To create a logging archive and specify how the logging messages will be collected and stored, use the **logging archive** command in XR Config mode. The **logging archive** command enters the logging archive submode where you can configure the attributes for archiving syslogs.

This table lists the commands used to specify the archive attributes once you are in the logging archive submode.

*Table 4: Commands Used to Set Syslog Archive Attributes*

| Command                                                         | Description                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>archive-length</b> <i>weeks</i>                              | Specifies the maximum number of weeks that the archive logs are maintained in the archive. Any logs older than this number are automatically removed from the archive.                                                                                                                                                                  |
| <b>archive-size</b> <i>size</i>                                 | Specifies the maximum total size of the syslog archives on a storage device. If the size is exceeded then the oldest file in the archive is deleted to make space for new logs.                                                                                                                                                         |
| <b>device</b> { <b>disk0</b>   <b>disk1</b>   <b>harddisk</b> } | Specifies the local storage device where syslogs are archived. By default, the logs are created under the directory <device>/var/log. If the device is not configured, then all other logging archive configurations are rejected. We recommend that syslogs be archived to the harddisk because it has more capacity than flash disks. |
| <b>file-size</b> <i>size</i>                                    | Specifies the maximum file size (in megabytes) that a single log file in the archive can grow to. Once this limit is reached, a new file is automatically created with an increasing serial number.                                                                                                                                     |
| <b>frequency</b> { <b>daily</b>   <b>weekly</b> }               | Specifies if logs are collected on a daily or weekly basis.                                                                                                                                                                                                                                                                             |
| <b>severity</b> <i>severity</i>                                 | Specifies the minimum severity of log messages to archive. All syslog messages greater than or equal to this configured level are archived while those lesser than this are filtered out. See the <a href="#">Severity Levels, on page 8</a> for more information.                                                                      |
| <b>threshold</b>                                                | Specifies the threshold percentage for archive logs.                                                                                                                                                                                                                                                                                    |

### Archive Storage Directories

By default, syslog archives are stored in the directory <device>/var/log. Individual archive files are saved to sub directories based on the year, month, and day the archive was created. For example, archive files created on February 26, 2006 are stored in this directory:

```
harddisk:/var/log/2006/02/26
```

## Severity Levels

You can limit the number of messages sent to the console, monitor and trap logging destinations by specifying the severity level of syslog messages sent to that destination (see [Table 7: Syslog Message Severity Levels, on page 9](#) for severity level definitions). However, for the logging buffer destination, syslog messages of all severity will be sent to it.

This table lists the commands used to control the severity level of syslog messages.

**Table 5: Commands Used to Control the Severity Level of Syslog Messages**

| Command                                     | Description                                                                                                                                                                        |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>logging buffered</b> [ <i>severity</i> ] | Limits the syslog messages that are displayed in the output of <b>show logging</b> based on severity. However, syslog messages of all severity will be sent to the logging buffer. |
| <b>logging console</b> [ <i>severity</i> ]  | Limits the syslog messages sent to the console terminal based on severity.                                                                                                         |
| <b>logging monitor</b> [ <i>severity</i> ]  | Limits the syslog messages sent to terminal lines based on severity.                                                                                                               |
| <b>logging trap</b> [ <i>severity</i> ]     | Limits the syslog messages sent to syslog servers based on severity.                                                                                                               |
| <b>severity</b> <i>severity</i>             | Limits the syslog messages sent to a syslog archive based on severity.                                                                                                             |

The **logging console**, **logging monitor**, and **logging traps** commands limit syslog messages sent to their respective destinations to messages with a level number at or below the specified severity level, which is specified with the *severity* argument. However, in the case of the **logging buffered** command, messages of all severity will continue to be sent to the logging buffer. This command only limits the syslog messages displayed in the output of **show logging** to messages with a level number at or below the specified *severity* argument.




---

**Note** Syslog messages of lower severity level indicate events of higher importance. See [Table 7: Syslog Message Severity Levels, on page 9](#) for severity level definitions.

---

## Logging History Table

If you have enabled syslog messages traps to be sent to a Simple Network Management Protocol (SNMP) network management station (NMS) with the **snmp-server enable traps syslog** command, you can change the level of messages sent and stored in a history table on the router. You can also change the number of messages that get stored in the history table.

Messages are stored in the history table, because SNMP traps are not guaranteed to reach their destination. By default, one message of the level warning and above (see [Table 7: Syslog Message Severity Levels, on page 9](#)) is stored in the history table even if syslog traps are not enabled.

This table lists the commands used to change the severity level and table size defaults of the logging history table



Table 6: Logging History Table Commands

| Command                                   | Description                                                                                                   |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| <b>logging history</b> <i>severity</i>    | Changes the default severity level of syslog messages stored in the history file and sent to the SNMP server. |
| <b>logging history size</b> <i>number</i> | Changes the number of syslog messages that can be stored in the history table.                                |



**Note** Table 7: Syslog Message Severity Levels, on page 9 lists the level keywords and severity level. For SNMP usage, the severity level values use +1. For example, **emergency** equals 1 not 0 and **critical** equals 3 not 2.

## Syslog Message Severity Level Definitions

This table lists the severity level keywords that can be supplied for the *severity* argument and corresponding UNIX syslog definitions in order from the most severe level to the least severe level.

Table 7: Syslog Message Severity Levels

| Severity Keyword | Level | Description                      | Syslog Definition |
|------------------|-------|----------------------------------|-------------------|
| emergencies      | 0     | System unusable                  | LOG_EMERG         |
| alerts           | 1     | Immediate action needed          | LOG_ALERT         |
| critical         | 2     | Critical conditions              | LOG_CRIT          |
| errors           | 3     | Error conditions                 | LOG_ERR           |
| warnings         | 4     | Warning conditions               | LOG_WARNING       |
| notifications    | 5     | Normal but significant condition | LOG_NOTICE        |
| informational    | 6     | Informational messages only      | LOG_INFO          |
| debugging        | 7     | Debugging messages               | LOG_DEBUG         |

## Syslog Severity Level Command Defaults

This table lists the default severity level settings for the commands that support the *severity* argument.

Table 8: Severity Level Command Defaults

| Command                 | Default Severity Keyword | Level |
|-------------------------|--------------------------|-------|
| <b>logging buffered</b> | debugging                | 7     |
| <b>logging console</b>  | informational            | 6     |

| Command                      | Default Severity Keyword | Level |
|------------------------------|--------------------------|-------|
| <code>logging history</code> | warnings                 | 4     |
| <code>logging monitor</code> | debugging                | 7     |
| <code>logging trap</code>    | informational            | 6     |

# How to Implement Logging Services

## Setting Up Destinations for System Logging Messages

This task explains how to configure logging to destinations other than the console terminal.

For conceptual information, see the [Syslog Message Destinations, on page 4](#) section.

### SUMMARY STEPS

1. `configure`
2. `logging buffered` [*size* | *severity*]
3. `logging monitor` [*severity*]
4. Use the `commit` or `end` command.
5. `terminal monitor`

### DETAILED STEPS

|               | Command or Action                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <p><code>configure</code></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router# configure</pre>                                                                         | Enters XR Config mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Step 2</b> | <p><code>logging buffered</code> [<i>size</i>   <i>severity</i>]</p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config)# logging buffered severity warnings</pre> | <p>Specifies the logging buffer as a destination for syslog messages, sets the size of the logging buffer, and limits syslog messages displayed in the output of <b>show logging</b> based on severity.</p> <ul style="list-style-type: none"> <li>• The default value for the <i>size</i> argument is 4096 bytes.</li> <li>• The default value for the <i>severity</i> argument is <b>debugging</b>.</li> <li>• Keyword options for the <i>severity</i> argument are <b>emergencies</b>, <b>alerts</b>, <b>critical</b>, <b>errors</b>, <b>warnings</b>, <b>notifications</b>, <b>informational</b>, and <b>debugging</b>.</li> <li>• By default, entering this command without specifying a severity level for the <i>severity</i> argument or specifying the size of the buffer for the <i>size</i> argument sets the</li> </ul> |

|               | Command or Action                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                                                                                                            | severity level to <b>debugging</b> and the buffer size to 4096 bytes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 3</b> | <p><b>logging monitor</b> [ <i>severity</i> ]</p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config)# logging monitor critical</pre> | <p>Specifies terminal lines other than console terminal as destinations for syslog messages and limits the number of messages sent to terminal lines based on severity.</p> <ul style="list-style-type: none"> <li>• Keyword options for the <i>severity</i> argument are <b>emergencies, alerts, critical, errors, warnings, notifications, informational, and debugging.</b></li> <li>• By default, entering this command without specifying a severity level for the <i>severity</i> argument sets the severity level to <b>debugging.</b></li> </ul>                                                                                 |
| <b>Step 4</b> | Use the <b>commit</b> or <b>end</b> command.                                                                                               | <p><b>commit</b> —Saves the configuration changes and remains within the configuration session.</p> <p><b>end</b> —Prompts user to take one of these actions:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b> — Saves configuration changes and exits the configuration session.</li> <li>• <b>No</b> —Exits the configuration session without committing the configuration changes.</li> <li>• <b>Cancel</b> —Remains in the configuration session, without committing the configuration changes.</li> </ul>                                                                                                                    |
| <b>Step 5</b> | <p><b>terminal monitor</b></p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router# terminal monitor</pre>                                    | <p>Enables the display of syslog messages for the current terminal session.</p> <p><b>Note</b> The logging of syslog message for the current terminal can be disabled with the <b>terminal monitor disable</b> command.</p> <ul style="list-style-type: none"> <li>• Use this command to reenble the display of syslog messages for the current session if the logging of messages for the current session was disabled with <b>terminal monitor disable</b> command.</li> </ul> <p><b>Note</b> Because this command is an XR EXEC mode command, it is set locally and will not remain in effect after the current session is ended.</p> |

## Configuring Logging to a Remote Server

You must have connectivity with syslog servers and snmp servers to configure them as the recipients for syslog messages.

### Configuration Example for Logging to Syslog Server

This example shows the configuration for sending syslog messages to an external syslog server. The ip address 209.165.201.1 is configured as the syslog server.

```
Router# configure
Router(config)# logging 209.165.201.1 vrf default
Router(config)# logging facility kern (optional)
Router(config)# logging hostnameprefix 203.0.113.1 (optional)
Router(config)# logging source-interface HundredGigE 0/0/0/0 (optional)
Router(config)# commit
```

Amongst other options, **all** and **none** are provided under the **logging severity** command form. If you enable **all** or **none**, all or no severity logs are logged to the syslog server, respectively. This configuration persists even when you enable a specific operator type.

### Configuration Example for Logging to SNMP Server

This example shows the configuration for sending syslog messages to an SNMP server. The logging trap command is used to limit the logging of messages sent to the snmp servers based on severity.

```
Router# configure
Router(config)# snmp-server traps syslog
Router(config)# logging trap warnings
Router(config)# commit
```

For more information on SNMP server configurations, see the *Configuring Simple Network Management Protocol* chapter in the *System Management Configuration Guide for Cisco NCS 6000 Series Routers*

## Configuring the Settings for the Logging History Table

This task explains how to configure the settings for the logging history table.

For conceptual information, see the [Severity Levels, on page 8](#) section.

### Before you begin

Logging of messages to an SNMP NMS is enabled by the **snmp-server enable traps syslog** command. For more information about SNMP, see the [Related Documents, on page 29](#) section.

### SUMMARY STEPS

1. **configure**
2. **logging history severity**
3. **logging history size number**
4. Use the **commit** or **end** command.
5. **show logging history**

### DETAILED STEPS

|        | Command or Action                                                              | Purpose                |
|--------|--------------------------------------------------------------------------------|------------------------|
| Step 1 | <b>configure</b><br><br><b>Example:</b><br><br>RP/0/RP0/CPU0:router# configure | Enters XR Config mode. |

|               | Command or Action                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 2</b> | <b>logging history severity</b><br><b>Example:</b><br><pre>RP/0/RP0/CPU0:router(config)# logging history errors</pre>      | Changes the default severity level of syslog messages stored in the history file and sent to the SNMP server. <ul style="list-style-type: none"> <li>• By default, syslog messages at or below the <b>warnings</b> severity level are stored in the history file and sent to the SNMP server.</li> </ul>                                                                                                                                                                                                              |
| <b>Step 3</b> | <b>logging history size number</b><br><b>Example:</b><br><pre>RP/0/RP0/CPU0:router(config)# logging history size 200</pre> | Changes the number of syslog messages that can be stored in the history table. <ul style="list-style-type: none"> <li>• By default, one syslog message is stored in the history table.</li> </ul> <p><b>Note</b> When the history table is full (that is, when it contains the maximum number of messages specified with this command), the oldest message is deleted from the table to allow the new message to be stored.</p>                                                                                       |
| <b>Step 4</b> | Use the <b>commit</b> or <b>end</b> command.                                                                               | <p><b>commit</b> —Saves the configuration changes and remains within the configuration session.</p> <p><b>end</b> —Prompts user to take one of these actions:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b> — Saves configuration changes and exits the configuration session.</li> <li>• <b>No</b> —Exits the configuration session without committing the configuration changes.</li> <li>• <b>Cancel</b> —Remains in the configuration session, without committing the configuration changes.</li> </ul> |
| <b>Step 5</b> | <b>show logging history</b><br><b>Example:</b><br><pre>RP/0/RP0/CPU0:router# show logging history</pre>                    | (Optional) Displays information about the state of the syslog history table.                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## Modifying Logging to the Console Terminal and the Logging Buffer

This task explains how to modify logging configuration for the console terminal and the logging buffer.



**Note** Logging is enabled by default.

### SUMMARY STEPS

1. **configure**

2. **logging buffered** [*size* | *severity*]
3. **logging console** [*severity*]
4. Use the **commit** or **end** command.

## DETAILED STEPS

|               | Command or Action                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure</b><br><b>Example:</b><br><pre>RP/0/RP0/CPU0:router# configure</pre>                                                                    | Enters XR Config mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Step 2</b> | <b>logging buffered</b> [ <i>size</i>   <i>severity</i> ]<br><b>Example:</b><br><pre>RP/0/RP0/CPU0:router(config)# logging buffered size 60000</pre> | <p>Specifies the logging buffer as a destination for syslog messages, sets the size of the logging buffer, and limits the syslog messages displayed in the output of <b>show logging</b> based on severity.</p> <ul style="list-style-type: none"> <li>• The default for the <i>size</i> argument is 4096 bytes.</li> <li>• The default for the <i>severity</i> argument is <b>debugging</b>.</li> <li>• Keyword options for the <i>severity</i> argument are <b>emergencies</b>, <b>alerts</b>, <b>critical</b>, <b>errors</b>, <b>warnings</b>, <b>notifications</b>, <b>informational</b>, and <b>debugging</b>.</li> <li>• By default, entering this command without specifying a severity level for the <i>severity</i> argument or specifying the size of the buffer for the <i>size</i> argument sets the severity level to <b>debugging</b> and the buffer size to 4096 bytes.</li> </ul> |
| <b>Step 3</b> | <b>logging console</b> [ <i>severity</i> ]<br><b>Example:</b><br><pre>RP/0/RP0/CPU0:router(config)# logging console alerts</pre>                     | <p>Limits messages sent to the console terminal based on severity.</p> <ul style="list-style-type: none"> <li>• Syslog messages are logged to the console terminal at the <b>informational</b> severity level by default.</li> <li>• Keyword options for the <i>severity</i> argument are <b>emergencies</b>, <b>alerts</b>, <b>critical</b>, <b>errors</b>, <b>warnings</b>, <b>notifications</b>, <b>informational</b>, and <b>debugging</b>.</li> <li>• Entering this command without specifying a severity level for the <i>severity</i> argument sets the severity level to <b>informational</b>.</li> </ul> <p><b>Note</b> Use this command to reenable logging to the console terminal if it was disabled with the <b>logging console disable</b> command.</p>                                                                                                                             |
| <b>Step 4</b> | Use the <b>commit</b> or <b>end</b> command.                                                                                                         | <p><b>commit</b> —Saves the configuration changes and remains within the configuration session.</p> <p><b>end</b> —Prompts user to take one of these actions:</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

|  | Command or Action | Purpose                                                                                                                                                                                                                                                                                                                                               |
|--|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |                   | <ul style="list-style-type: none"> <li>• <b>Yes</b> — Saves configuration changes and exits the configuration session.</li> <li>• <b>No</b> — Exits the configuration session without committing the configuration changes.</li> <li>• <b>Cancel</b> — Remains in the configuration session, without committing the configuration changes.</li> </ul> |

## Modifying the Format of Time Stamps

This task explains how to modify the time-stamp format for syslog and debugging messages.

### SUMMARY STEPS

1. **configure**
2. Do one of the following:
  - **service timestamps log datetime [localtime] [msec] [show-timezone]**
  - **service timestamps log uptime**
3. Do one of the following:
  - **service timestamps debug datetime [localtime] [msec] [show-timezone]**
  - **service timestamps debug uptime**
4. Use the **commit** or **end** command.

### DETAILED STEPS

|               | Command or Action                                                                                                                                                                                                                                                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure</b><br><b>Example:</b><br><pre>RP/0/RP0/CPU0:router# configure</pre>                                                                                                                                                                                                                                                                                                              | Enters XR Config mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Step 2</b> | Do one of the following: <ul style="list-style-type: none"> <li>• <b>service timestamps log datetime [localtime] [msec] [show-timezone]</b></li> <li>• <b>service timestamps log uptime</b></li> </ul> <b>Example:</b><br><pre>RP/0/RP0/CPU0:router(config)# service timestamps log datetime localtime msec</pre> or<br><pre>RP/0/RP0/CPU0:router(config)# service timestamps log uptime</pre> | Modifies the time-stamp format for syslog messages. <ul style="list-style-type: none"> <li>• By default, time stamps are enabled. The default time-stamp format is month day HH:MM:SS.</li> <li>• Issuing the <b>service timestamps log datetime</b> command configures syslog messages to be time-stamped with the date and time.               <ul style="list-style-type: none"> <li>• The optional <b>localtime</b> keyword includes the local time zone in time stamps.</li> <li>• The optional <b>msec</b> keyword includes milliseconds in time stamps.</li> </ul> </li> </ul> |

|               | Command or Action                                                                                                                                                                                                                                                                                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                                                                                                                                                                                                                                                                                                                                                                                           | <ul style="list-style-type: none"> <li>• The optional <b>show-timezone</b> keyword includes time zone information in time stamps.</li> <li>• Issuing the <b>service timestamps log uptime</b> command configures syslog messages to be time-stamped with the time that has elapsed since the router last rebooted.</li> <li>• The <b>service timestamps log uptime</b> command configures time-stamps to be configured in HHHH:MM:SS, indicating the time since the router last rebooted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Step 3</b> | <p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• <b>service timestamps debug datetime [localtime] [msec] [show-timezone]</b></li> <li>• <b>service timestamps debug uptime</b></li> </ul> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config)# service timestamps debug datetime msec show-timezone</pre> <p>or</p> <pre>RP/0/RP0/CPU0:router(config)# service timestamps debug uptime</pre> | <p>Modifies the time-stamp format for debugging messages.</p> <ul style="list-style-type: none"> <li>• By default, time-stamps are enabled. The default time stamp format is month day HH:MM:SS.</li> <li>• Issuing the <b>service timestamps log datetime</b> command configures debugging messages to be time-stamped with the date and time. <ul style="list-style-type: none"> <li>• The optional <b>localtime</b> keyword includes the local time zone in time stamps.</li> <li>• The optional <b>msec</b> keyword includes milliseconds in time stamps.</li> <li>• The optional <b>show-timezone</b> keyword includes time zone information in time stamps.</li> </ul> </li> <li>• Issuing the <b>service timestamps log uptime</b> command configures debugging messages to be time-stamped with the time that has elapsed since the networking device last rebooted.</li> </ul> <p><b>Tip</b>      Entering the <b>service timestamps</b> command without any keywords or arguments is equivalent to entering the <b>service timestamps debug uptime</b> command.</p> |
| <b>Step 4</b> | Use the <b>commit</b> or <b>end</b> command.                                                                                                                                                                                                                                                                                                                                                                              | <p><b>commit</b> —Saves the configuration changes and remains within the configuration session.</p> <p><b>end</b> —Prompts user to take one of these actions:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b> — Saves configuration changes and exits the configuration session.</li> <li>• <b>No</b> —Exits the configuration session without committing the configuration changes.</li> <li>• <b>Cancel</b> —Remains in the configuration session, without committing the configuration changes.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |



## Disabling Time Stamps

This task explains how to disable the inclusion of time stamps in syslog messages.

### SUMMARY STEPS

1. **configure**
2. Do one of the following:
  - **service timestamps disable**
  - **no service timestamps [debug | log] [datetime [localtime] [msec] [show-timezone]] | uptime**
3. Use the **commit** or **end** command.

### DETAILED STEPS

|               | Command or Action                                                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure</b><br><b>Example:</b><br><br>RP/0/RP0/CPU0:router# <code>configure</code>                                                                                                                                     | Enters XR Config mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Step 2</b> | Do one of the following: <ul style="list-style-type: none"> <li>• <b>service timestamps disable</b></li> <li>• <b>no service timestamps [debug   log] [datetime [localtime] [msec] [show-timezone]]   uptime</b></li> </ul> | Disables the inclusion of time stamps in syslog messages.<br><br><b>Note</b> Both commands disable the inclusion of time stamps in syslog messages; however, specifying the <b>service timestamps disable</b> command saves the command to the configuration, whereas specifying the <b>no</b> form of the <b>service timestamps</b> command removes the command from the configuration.                                                                                                                       |
| <b>Step 3</b> | Use the <b>commit</b> or <b>end</b> command.                                                                                                                                                                                | <b>commit</b> —Saves the configuration changes and remains within the configuration session.<br><br><b>end</b> —Prompts user to take one of these actions: <ul style="list-style-type: none"> <li>• <b>Yes</b> — Saves configuration changes and exits the configuration session.</li> <li>• <b>No</b> —Exits the configuration session without committing the configuration changes.</li> <li>• <b>Cancel</b> —Remains in the configuration session, without committing the configuration changes.</li> </ul> |

## Suppressing Duplicate Syslog Messages

This task explains how to suppress the consecutive logging of duplicate syslog messages.

**SUMMARY STEPS**

1. **configure**
2. **logging suppress duplicates**
3. Use the **commit** or **end** command.

**DETAILED STEPS**

|               | <b>Command or Action</b>                                                                                           | <b>Purpose</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|--------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure</b><br><b>Example:</b><br>RP/0/RP0/CPU0:router# configure                                             | Enters XR Config mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Step 2</b> | <b>logging suppress duplicates</b><br><b>Example:</b><br>RP/0/RP0/CPU0:router(config)# logging suppress duplicates | Prevents the consecutive logging of duplicate syslog messages.<br><br><b>Caution</b> If this command is enabled during debugging sessions, you could miss important information related to problems that you are attempting to isolate and resolve. In such a case, you might consider disabling this command.                                                                                                                                                                                                 |
| <b>Step 3</b> | Use the <b>commit</b> or <b>end</b> command.                                                                       | <b>commit</b> —Saves the configuration changes and remains within the configuration session.<br><br><b>end</b> —Prompts user to take one of these actions: <ul style="list-style-type: none"> <li>• <b>Yes</b> — Saves configuration changes and exits the configuration session.</li> <li>• <b>No</b> —Exits the configuration session without committing the configuration changes.</li> <li>• <b>Cancel</b> —Remains in the configuration session, without committing the configuration changes.</li> </ul> |

**Disabling the Logging of Link-Status Syslog Messages**

This task explains how to disable the logging of link-status syslog messages for logical and physical links.

When the logging of link-status messages is enabled, the router can generate a high volume of link-status updown syslog messages. Disabling the logging of link-status syslog messages reduces the number of messages logged.

**SUMMARY STEPS**

1. **configure**
2. **logging events link-status disable**
3. Use the **commit** or **end** command.

## DETAILED STEPS

|        | Command or Action                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>configure</b><br><b>Example:</b><br><pre>RP/0/RP0/CPU0:router# configure</pre>                                                           | Enters XR Config mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 2 | <b>logging events link-status disable</b><br><b>Example:</b><br><pre>RP/0/RP0/CPU0:router(config)# logging events link-status disable</pre> | Disables the logging of link-status syslog messages for software (logical) and physical links. <ul style="list-style-type: none"> <li>• The logging of link-status syslog messages is enabled by default for physical links.</li> <li>• To enable link-status syslog messages for both physical and logical links, use the <b>logging events link-status software-interfaces</b> command.</li> <li>• Use the <b>no logging events link-status</b> command to enable link-status syslog messages on physical links only.</li> </ul> |
| Step 3 | Use the <b>commit</b> or <b>end</b> command.                                                                                                | <b>commit</b> —Saves the configuration changes and remains within the configuration session.<br><b>end</b> —Prompts user to take one of these actions: <ul style="list-style-type: none"> <li>• <b>Yes</b> — Saves configuration changes and exits the configuration session.</li> <li>• <b>No</b> —Exits the configuration session without committing the configuration changes.</li> <li>• <b>Cancel</b> —Remains in the configuration session, without committing the configuration changes.</li> </ul>                         |

## Displaying System Logging Messages

This task explains how to display the syslog messages stored in the logging buffer.



**Note** The commands can be entered in any order.

## SUMMARY STEPS

1. **show logging**
2. **show logging location** *node-id*
3. **show logging process** *name*
4. **show logging string** *string*
5. **show logging start** *month day hh:mm:ss*

## 6. show logging end *month day hh:mm:ss*

### DETAILED STEPS

|               | Command or Action                                                                                                                         | Purpose                                                                                                      |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>show logging</b><br><b>Example:</b><br>RP/0/RP0/CPU0:router# show logging                                                              | Displays all syslog messages stored in the buffer.                                                           |
| <b>Step 2</b> | <b>show logging location <i>node-id</i></b><br><b>Example:</b><br>RP/0/RP0/CPU0:router# show logging location<br>0/1/CPU0                 | Displays syslog messages that have originated from the designated node.                                      |
| <b>Step 3</b> | <b>show logging process <i>name</i></b><br><b>Example:</b><br>RP/0/RP0/CPU0:router# show logging process init                             | Displays syslog messages that are related to the specified process.                                          |
| <b>Step 4</b> | <b>show logging string <i>string</i></b><br><b>Example:</b><br>RP/0/RP0/CPU0:router# show logging string install                          | Displays syslog messages that contain the specified string.                                                  |
| <b>Step 5</b> | <b>show logging start <i>month day hh:mm:ss</i></b><br><b>Example:</b><br>RP/0/RP0/CPU0:router# show logging start december<br>1 10:30:00 | Displays syslog messages in the logging buffer that were generated on or after the specified date and time.  |
| <b>Step 6</b> | <b>show logging end <i>month day hh:mm:ss</i></b><br><b>Example:</b><br>RP/0/RP0/CPU0:router# show logging end december 2<br>22:16:00     | Displays syslog messages in the logging buffer that were generated on or before the specified date and time. |

## Archiving System Logging Messages to a Local Storage Device

This task explains how to display save syslog messages to an archive on a local storage device.

### Before you begin



**Note** The local storage device must have enough space available to store the archive files. We recommend that syslogs be archived to the harddisk because it has more capacity than flash disks.

## SUMMARY STEPS

1. **configure**
2. **logging archive**
3. **device** {**disk0** | **disk1** | **harddisk**}
4. **frequency** {**daily** | **weekly**}
5. **severity** *severity*
6. **archive-length** *weeks*
7. **archive-size** *size*
8. **file-size** *size*
9. Use the **commit** or **end** command.

## DETAILED STEPS

|               | Command or Action                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                        |
|---------------|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure</b><br><b>Example:</b><br><pre>RP/0/RP0/CPU0:router# configure</pre>                     | Enters XR Config mode.                                                                                                                                                                                                                                                                                                                                                         |
| <b>Step 2</b> | <b>logging archive</b><br><b>Example:</b><br><pre>RP/0/RP0/CPU0:router(config)# logging archive</pre> | Enters logging archive configuration mode.                                                                                                                                                                                                                                                                                                                                     |
| <b>Step 3</b> | <b>device</b> { <b>disk0</b>   <b>disk1</b>   <b>harddisk</b> }                                       | Specify the device to be used for logging syslogs.                                                                                                                                                                                                                                                                                                                             |
|               | <b>Example:</b><br><pre>RP/0/RP0/CPU0:router(config-logging-arch)# device disk1</pre>                 | <ul style="list-style-type: none"> <li>• This step is required. If the device is not configured, then all other logging archive configurations are rejected.</li> <li>• We recommend that syslogs be archived to the harddisk because it has more capacity than flash disks.</li> <li>• By default, the logs are created under the directory &lt;device&gt;/var/log</li> </ul> |
| <b>Step 4</b> | <b>frequency</b> { <b>daily</b>   <b>weekly</b> }                                                     | (Optional) Specifies if logs are collected on a daily or weekly basis. Logs are collected daily by default.                                                                                                                                                                                                                                                                    |
|               | <b>Example:</b><br><pre>RP/0/RP0/CPU0:router(config-logging-arch)# frequency weekly</pre>             |                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Step 5</b> | <b>severity</b> <i>severity</i>                                                                       | (Optional) Specifies the minimum severity of log messages to archive. All syslog messages greater than or equal to this configured level are archived while those lesser than this are filtered out. The severity levels are:                                                                                                                                                  |
|               | <b>Example:</b><br><pre>RP/0/RP0/CPU0:router(config-logging-arch)# severity warnings</pre>            | <ul style="list-style-type: none"> <li>• emergencies</li> <li>• alerts</li> </ul>                                                                                                                                                                                                                                                                                              |

|               | Command or Action                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                                                                                                 | <ul style="list-style-type: none"> <li>• critical</li> <li>• errors</li> <li>• warnings</li> <li>• notifications</li> <li>• informational</li> <li>• debugging</li> </ul> <p>See the <a href="#">Syslog Message Severity Level Definitions, on page 9</a> section for information.</p>                                                                                                                                                                                                                         |
| <b>Step 6</b> | <b>archive-length</b> <i>weeks</i><br><b>Example:</b><br><pre>RP/0/RP0/CPU0:router(config-logging-arch)# archive-length 6</pre> | (Optional) Specifies the maximum number of weeks that the archive logs are maintained in the archive. Any logs older than this number are automatically removed from the archive.<br><br>By default, archive logs are stored for 4 weeks.                                                                                                                                                                                                                                                                      |
| <b>Step 7</b> | <b>archive-size</b> <i>size</i><br><b>Example:</b><br><pre>RP/0/RP0/CPU0:router(config-logging-arch)# archive-size 50</pre>     | (Optional) Specifies the maximum total size of the syslog archives on a storage device. If the size is exceeded then the oldest file in the archive is deleted to make space for new logs.<br><br>The default archive size is 20 MB.                                                                                                                                                                                                                                                                           |
| <b>Step 8</b> | <b>file-size</b> <i>size</i><br><b>Example:</b><br><pre>RP/0/RP0/CPU0:router(config-logging-arch)# file-size 10</pre>           | (Optional) Specifies the maximum file size (in megabytes) that a single log file in the archive can grow to. Once this limit is reached, a new file is automatically created with an increasing serial number.<br><br>By default, the maximum file size is 1 megabyte.                                                                                                                                                                                                                                         |
| <b>Step 9</b> | Use the <b>commit</b> or <b>end</b> command.                                                                                    | <b>commit</b> —Saves the configuration changes and remains within the configuration session.<br><br><b>end</b> —Prompts user to take one of these actions: <ul style="list-style-type: none"> <li>• <b>Yes</b> — Saves configuration changes and exits the configuration session.</li> <li>• <b>No</b> —Exits the configuration session without committing the configuration changes.</li> <li>• <b>Cancel</b> —Remains in the configuration session, without committing the configuration changes.</li> </ul> |

## Platform Automated Monitoring

Platform Automated Monitoring (PAM) is a system monitoring tool integrated into Cisco IOS XR software image to monitor the following issues:

- process crashes
- memory leaks
- CPU hogs
- tracebacks
- disk usage

PAM is enabled by default. When the PAM tool detects any of these system issues, it collects the required data to troubleshoot the issue, and generates a syslog message stating the issue. The auto-collected troubleshooting information is then stored as a separate file in `harddisk:/cisco_support/` or in `/misc/disk1/cisco_support/` directory.

## PAM Events

When PAM detects a process crash, traceback, potential memory leak, CPU hog, a full file system, , it automatically collects logs and saves these logs (along with the core file in applicable cases) as a `.tgz` file in `harddisk:/cisco_support/` or in `/misc/disk1/cisco_support/` directory. PAM also generates a syslog message with severity level as warning, mentioning the respective issue.

The format of the `.tgz` file is: `PAM-<platform>-<PAM event>-<node-name>-<PAM process>-<YYYYMMDD>-<checksum>.tgz`. For example, `PAM--crash-xr_0_RP0_CPU0-ipv4_rib-2016Aug16-210405.tgz` is the file collected when PAM detects a process crash.

Because PAM assumes that core files are saved to the default archive folder (`harddisk:/` or `/misc/disk1/`), you must not modify the location of core archive (by configuring exception filepath) or remove the core files generated after PAM detects an event. Else, PAM does not detect the process crash. Also, once reported, the PAM does not report the same issue for the same process in the same node again.

For the list of commands used while collecting logs, refer [Files Collected by PAM Tool, on page 25](#).

The sections below describe the main PAM events:

### Crash Monitoring

The PAM monitors process crash for all nodes, in real time. This is a sample syslog generated when the PAM detects a process crash:

```
RP/0/RP0/CPU0:Aug 16 21:04:06.442 : logger[69324]: %OS-SYSLOG-4-LOG_WARNING : PAM detected
  crash for ipv4_rib on 0_RP0_CPU0.
All necessary files for debug have been collected and saved at
0/RP0/CPU0 :
harddisk:/cisco_support/PAM-ncs6k-crash-xr_0_RP0_CPU0-ipv4_rib-2016Aug16-210405.tgz
Please copy tgz file out of the router and send to Cisco support. This tgz file will be
removed after 14 days.)
```

### Traceback Monitoring

The PAM monitors tracebacks for all nodes, in real time. This is a sample syslog generated when the PAM detects a traceback:

```
RP/0/RP0/CPU0:Aug 16 21:42:42.320 : logger[66139]: %OS-SYSLOG-4-LOG_WARNING : PAM detected
  traceback for ipv4_rib on 0_RP0_CPU0.
```

```
All necessary files for debug have been collected and saved at
0/RP0/CPU0 :
harddisk:/cisco_support/PAM-ncs6k-traceback-xr_0_RP0_CPU0-ipv4_rib-2016Aug16-214242.tgz
Please copy tgz file out of the router and send to Cisco support. This tgz file will be
removed after 14 days.)
```

### Memory Usage Monitoring

The PAM monitors the process memory usage for all nodes. The PAM detects potential memory leaks by monitoring the memory usage trend and by applying a proprietary algorithm to the collected data. By default, it collects top output on all nodes periodically at an interval of 30 minutes.

This is a sample syslog generated when the PAM detects a potential memory leak:

```
RP/0/RP0/CPU0:Aug 17 05:13:32.684 : logger[67772]: %OS-SYSLOG-4-LOG_WARNING : PAM detected
significant memory increase
(from 13.00MB at 2016/Aug/16/20:42:41 to 28.00MB at 2016/Aug/17/04:12:55) for
pam_memory_leaker on 0_RP0_CPU0.
All necessary files for debug have been collected and saved at
0/RP0/CPU0 :
harddisk:/cisco_support/PAM-ncs6k-memory_leak-xr_0_RP0_CPU0-pam_memory_leaker-2016Aug17-051332.tgz

(Please copy tgz file out of the router and send to Cisco support. This tgz file will be
removed after 14 days.)
```

### CPU Monitoring

The PAM monitors CPU usage on all nodes periodically at an interval of 30 minutes. The PAM reports a CPU hog in either of these scenarios:

- When a process constantly consumes high CPU (that is, more than the threshold of 90 percentage)
- When high CPU usage lasts for more than 60 minutes

This is a sample syslog generated when the PAM detects a CPU hog:

```
RP/0/RP0/CPU0:Aug 16 00:56:00.819 : logger[68245]: %OS-SYSLOG-4-LOG_WARNING : PAM detected
CPU hog for cpu_hogger on 0_RP0_CPU0.
All necessary files for debug have been collected and saved at 0/RP0/CPU0 :
harddisk:/cisco_support/PAM-ncs6k-cpu_hog-xr_0_RP0_CPU0-cpu_hogger-2016Aug16-005600.tgz
(Please copy tgz file out of the router and send to Cisco support. This tgz file will be
removed after 14 days.)
RP/0/RP0/CPU0:Jun 21 15:33:54.517 : logger[69042]: %OS-SYSLOG-1-LOG_ALERT : PAM detected
ifmgr is hogging CPU on 0_RP0_CPU0!
```

### File System Monitoring

The PAM monitors disk usage on all nodes periodically at an interval of 30 minutes. This is a sample syslog generated when the PAM detects that a file system is full:

```
RP/0/RP0/CPU0:Jun 20 13:59:04.986 : logger[66125]: %OS-SYSLOG-4-LOG_WARNING : PAM detected
/misc/config is full on 0_1_CPU0
(please clean up to avoid any fault caused by this). All necessary files for debug have
been collected and saved at
0/RP0/CPU0 : harddisk:/cisco_support/PAM-ncs6k-disk_usage-xr_0_1_CPU0-2016Jun20-135904.tgz
```



(Please copy tgz file out of the router and send to Cisco support. This tgz file will be removed after 14 days.)

## Disable and Re-enable PAM

The PAM tool consists of three monitoring processes—`monitor_cpu.pl`, `monitor_crash.pl`, and `monitor_show_logging.pl`.

Before disabling or re-enabling the PAM, use these options to check if the PAM is installed in the router:

- From Cisco IOS XR Command Line Interface:

```
Router# show pam status
Tue Jun 14 17:58:42.791 UTC
PAM is enabled
```

- From router shell prompt:

```
Router# run ps auxw|egrep perl

root      12559  0.0  0.0  57836 17992 ?        S    Apr24   0:00 /usr/bin/perl
/pkg/opt/cisco/pam//pam_plugin.pl
```

### Disable PAM

To disable PAM agent systemwide, execute the following command from XR EXEC mode:

```
Router# disable-pam
```

### Re-enable PAM

To re-enable PAM agent systemwide, execute the following command from XR EXEC mode:

```
Router# enable-pam
```

## Data Archiving in PAM

At any given point of time, PAM does not occupy more than 200 MB of harddisk: space. If more than 200 MB is needed, then PAM archives old files and rotates the logs automatically.

The PAM collects CPU or memory usage (using `top -b -n1` command) periodically at an interval of 30 minutes. The files are saved under `harddisk:/cisco_support/` directory with the filename as `<node name>.log` (for example, `harddisk:/cisco_support/xr-0_RP0_CPU0.log`). When the file size exceeds the limit of 15MB, the file is archived (compressed) into `.tgz` file, and then rotated for a maximum of two counts (that is, it retains only two `.tgz` files). The maximum rotation count of `.tgz` files is three. Also, the old file (ASCII data) is archived and rotated if a node is reloaded. For example, `xr-0_RP0_CPU0.log` is archived if RP0 is reloaded.

You must not manually delete the core file generated by the PAM. The core file is named as `<process name>_pid.by_user.<yyyymmdd>-<hhmmss>.<node>.<checksum>.core.gz`.

## Files Collected by PAM Tool

The table below lists the various PAM events and the respective commands and files collected by the PAM for each event.

You can attach the respective `.tgz` file when you raise a service request (SR) with Cisco Technical Support.

| Event Name         | Commands and Files Collected by PAM                                                                                                                                                                                                              |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process crash      | <ul style="list-style-type: none"> <li>• <b>show install active</b></li> <li>• <b>show platform</b></li> <li>• <b>show version</b></li> <li>• core (gz) file</li> <li>• core.txt file</li> </ul>                                                 |
| Process traceback  | <ul style="list-style-type: none"> <li>• <b>show dll</b></li> <li>• <b>show install active</b></li> <li>• <b>show logging</b></li> <li>• <b>show platform</b></li> <li>• <b>show version</b></li> </ul>                                          |
| Memory leak        | <ul style="list-style-type: none"> <li>• <b>show install active</b></li> <li>• <b>show platform</b></li> <li>• <b>show version</b></li> <li>• core (gz) file</li> <li>• dumpcore running</li> <li>• continuous memory usage snapshots</li> </ul> |
| Show logging event | <ul style="list-style-type: none"> <li>• <b>show install active</b></li> <li>• <b>show logging</b></li> <li>• <b>show platform</b></li> <li>• <b>show version</b></li> <li>• core (gz) file</li> <li>• core.txt file</li> </ul>                  |

| Event Name | Commands and Files Collected by PAM                                                                                                                                                                                                                                                                                  |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPU hog    | <ul style="list-style-type: none"> <li>• <b>follow process</b></li> <li>• <b>pstack</b></li> <li>• <b>show dll</b></li> <li>• <b>show install active</b></li> <li>• <b>show platform</b></li> <li>• <b>show version</b></li> <li>• <b>top -H</b></li> <li>• core (gz) file</li> <li>• CPU usage snapshots</li> </ul> |
| Disk usage | <ul style="list-style-type: none"> <li>• <b>show install active</b></li> <li>• <b>show platform</b></li> <li>• <b>show version</b></li> <li>• console log</li> <li>• core (gz) file</li> <li>• Disk usage snapshots</li> </ul>                                                                                       |

## Configuration Examples for Implementing Logging Services

This section provides these configuration examples:

### Configuring Logging to the Console Terminal and the Logging Buffer: Example

This example shows a logging configuration where logging to the logging buffer is enabled, the severity level of syslog messages sent to the console terminal is limited to syslog messages at or below the **critical** severity level, and the size of the logging buffer is set to 60,000 bytes.

```
!
logging console critical
logging buffered 60000
!
```

### Setting Up Destinations for Syslog Messages: Example

This example shows a logging configuration where logging is configured to destinations other than the console terminal. In this configuration, the following is configured:

- Logging is enabled to destinations other than the console terminal.

- Syslog messages at or below the **warnings** severity level are sent to syslog server hosts.
- Syslog messages at or below the **critical** severity level are sent to terminal lines.
- The size of the logging buffer is set to 60,000 bytes.
- The syslog server host at IP addresses 172.19.72.224 (IPv4) and 2001:DB8:A00:1::1/64 (IPv6) are configured as recipients for syslog messages.

```
!
logging trap warnings
logging monitor critical
logging buffered 60000
logging 172.19.72.224
logging 2001:DB8:A00:1::1/64
!
```

## Configuring the Settings for the Logging History Table: Example

This example shows a logging configuration in which the size of the logging history table is 200 entries and the severity of level of syslog messages sent to the logging history table is limited to messages at or below the **errors** severity level:

```
logging history size 200
logging history errors
```

## Modifying Time Stamps: Example

This example shows a time-stamp configuration in which time stamps are configured to follow the format month date HH:MM:SS time zone:

```
service timestamps log datetime show-timezone
```

This example shows a time-stamp configuration in which time stamps are configured to follow the format month date HH:MM:SS.milliseconds time zone:

```
service timestamps log datetime msec show-timezone
```

## Configuring a Logging Archive: Example

This example shows how to configure a logging archive, and define the archive attributes:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# logging archive
RP/0/RP0/CPU0:router(config-logging-arch)# device disk1
RP/0/RP0/CPU0:router(config-logging-arch)# frequency weekly
RP/0/RP0/CPU0:router(config-logging-arch)# severity warnings
RP/0/RP0/CPU0:router(config-logging-arch)# archive-length 6
RP/0/RP0/CPU0:router(config-logging-arch)# archive-size 50
RP/0/RP0/CPU0:router(config-logging-arch)# file-size 10
```

## Where to Go Next

To configure alarm log correlation, see the *Implementing and Monitoring Alarms and Logging Correlation* module in the *System Monitoring Configuration Guide for Cisco NCS 6000 Series Routers*.

## Additional References

The following sections provide references related to implementing logging services on Cisco IOS XR software.

### Related Documents

| Related Topic                                                    | Document Title                                                                                                                                                     |
|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Logging services command reference                               | <i>Logging Services Commands</i> module in the <i>System Monitoring Command Reference for Cisco NCS 6000 Series Routers</i>                                        |
| Onboard Failure Logging (OBFL) configuration                     | <i>Onboard Failure Logging Commands</i> module in the <i>System Monitoring Configuration Guide for Cisco NCS 6000 Series Routers</i> .                             |
| Onboard Failure Logging (OBFL) commands                          | <i>Onboard Failure Logging Commands</i> module in the <i>System Monitoring Command Reference for Cisco NCS 6000 Series Routers</i> .                               |
| Alarm and logging correlation commands                           | <i>Alarm Management and Logging Correlation Commands</i> module in the <i>System Monitoring Command Reference for Cisco NCS 6000 Series Routers</i> .              |
| Alarm and logging correlation configuration and monitoring tasks | <i>Implementing and Monitoring Alarms and Alarm Log Correlation</i> module in the <i>System Monitoring Configuration Guide for Cisco NCS 6000 Series Routers</i> . |
| SNMP commands                                                    | <i>SNMP Commands</i> module in the <i>System Monitoring Command Reference for Cisco NCS 6000 Series Routers</i> .                                                  |
| SNMP configuration tasks                                         | <i>Implementing SNMP</i> module in the <i>System Monitoring Configuration Guide for Cisco NCS 6000 Series Routers</i>                                              |
| Information about user groups and task IDs                       | <i>Configuring AAA Services</i> module in the <i>System Security Command Reference for Cisco NCS 6000 Series Routers</i> .                                         |

### Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

**MIBs**

| MIBs                                                                                                                                             | MIBs Link                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| To locate and download MIBs for Cisco IOS XR software, use the <i>Cisco Feature Navigator MIB Locator</i> and click on the IOS XR software type. | <a href="#">Cisco Feature Navigator MIB Locator</a> |

**RFCs**

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

**Technical Assistance**

| Description                                                                                                                                                                                                                                                         | Link                                                                                                              |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a> |