

Logging Services Commands

This module describes the Cisco IOS XR7 Software commands to configure system logging (syslog) for system monitoring on the router.

For detailed information about logging concepts, configuration tasks, and examples, see the *Implementing Logging Services* chapter in the *System Monitoring Configuration Guide for Cisco 8000 Series Routers*.

- logging, on page 2
- logging archive, on page 4
- logging buffered, on page 5
- logging console, on page 7
- logging console disable, on page 8
- logging container all, on page 9
- logging events link-status, on page 10
- logging events link-status (interface), on page 11
- logging facility, on page 13
- logging file, on page 15
- logging format bsd, on page 16
- logging format rfc5424, on page 17
- logging history, on page 18
- logging history size, on page 19
- logging hostnameprefix, on page 20
- logging ipv4/ipv6, on page 21
- logging localfilesize, on page 24
- logging monitor, on page 24
- logging source-interface, on page 25
- logging suppress deprecated, on page 26
- logging suppress duplicates, on page 27
- logging trap, on page 28
- login-history, on page 28
- service timestamps, on page 29
- severity (logging), on page 31
- show logging, on page 31
- show logging history, on page 35
- terminal monitor, on page 36
- enable-pam process-monitoring, on page 37

- disable-pam process-monitoring, on page 38
- show pam process-monitoring-status, on page 38
- show syslog persistent status, on page 39

logging

To specify a system logging (syslog) server host as the recipient of syslog messages, use the **logging** command in XR Config mode. To remove the **logging** command from the configuration file and delete a syslog server from the list of syslog server hosts, use the **no** form of this command.

logging { *ip-address hostname* | { **vrf** *vrf_name* } } { **archive** | **buffered** | **console** | **correlator** | **disable** | **events** | **facility** *type* | **format** **rfc5424** | **history** | **hostnameprefix** | **localfilesize** | **monitor** | **operator** | **port** | **severity** | **source-address** | **source-interface** *ipv4 address* | **suppress** | **trap** }

Syntax Description

ip-address | *hostname*	IP address or hostname of the host to be used as a syslog server.
vrf *vrf-name*	Name of the VRF. Maximum length is 32 alphanumeric characters.
archive	Specifies logging to a persistent device(disk/harddisk).
buffered	Sets buffered logging parameters.
console	Sets console logging.
correlator	Configures properties of the event correlator
disable	Disables console logging.
events	Configures event monitoring parameters.
facility *type*	Modifies message logging facilities.
format	Configures the syslog message format to send to the server.
rfc5424	Sets the syslog message format according to RFC 5424.
history	Sets history logging.
hostnameprefix	Adds the hostname prefix to messages on servers.
localfilesize	Sets size of the local log file.
monitor	Sets monitor logging
operator	Sets severity operator of messages for anparticular remote host/vrf.
port	Sets UDP port for this remote host/vrf.

severity	Sets severity of messages for particular remote host/vrf
source-address *ipv4 address*	Specifies source address of the logging host.
source-interface	Specifies interface for source address in logging transactions.
suppress	Configures properties for the event suppression.
trap	Sets trap logging.

Command Default

No syslog server hosts are configured as recipients of syslog messages.

Command Modes

XR Config mode

Command History

Release	Modification
Release 24.2.1	The **facility** and **source-address** options per remote syslog server were introduced.
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **logging** command to identify a syslog server host to receive messages. By issuing this command more than once, you build a list of syslog servers that receive messages.

When syslog messages are sent to a syslog server, the Cisco IOS XR software includes a numerical message identifier in syslog messages. The message identifier is cumulative and sequential. The numerical identifier included in syslog messages sent to syslog servers provides a means to determine if any messages have been lost.

Use the logging trap, on page 28 command to limit the messages sent to snmp server.

The configurations for **facility** and **source-address** per remote syslog server takes priority over global configuration.

Task ID

Task ID	Operations
logging	read, write

This example shows how to log messages to a host named host1:

```
Router(config)#logging host1
```

```
Router(config)#logging A.B.C.D
facility        Modify message logging facilities
operator        Set severity operator of  messages for particular remote host/vrf
port            Set UDP port for this remote host/vrf
severity        Set severity of  messages for particular remote host/vrf
source-address  Specify source address of the logging host
vrf             Set VRF option
```

```
Router(config)#logging A.B.C.D
Router(config)#commit
Wed Nov 14 03:47:58.976 PST

Router(config)#do show run logging
Wed Nov 14 03:48:10.816 PST
logging A.B.C.D vrf default severity info
```

Note Default level is severity info.

Configuration Example for Facility and Source-address Per Remote Syslog Server

This example shows how to configure **facility** and **source-address** per remote syslog server:

```
Router#configure
Router(config)#
Router(config)#logging 209.165.201.1 source-address 209.165.201.2
Router(config)#logging 209.165.201.1 facility local2
Router(config)#commit
```

logging archive

To configure attributes for archiving syslogs, use the **logging archive** command in XR Config mode. To exit the **logging archive** submode, use the **no** form of this command.

logging archive
no logging archive

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines Use the **logging archive** command to configure attributes for archiving syslogs. This command enters logging archive configuration mode and allows you to configure the commands in the table:

Note The configuration attributes must be explicitly configured in order to use the logging archive feature.

Table 1: Configuring Command Attributes For Archiving Syslogs

Command	Range	Description	Recommended Setting
archive-length	<0-4294967295>	Number of weeks	4 weeks
archive-size	<1-2047>	Size in MB	20 MB
device	<disk0 | disk1 | harddisk>	Use configured devices as the archive device.	harddisk
file-size	<1-2047>	Size in MB	1 MB
frequency	<daily | weekly>		daily
severity	<alerts | critical | debugging | emergencies | errors | informational | notifications | warnings>		informational

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to enter logging archive configuration mode and change the device to be used for logging syslogs to disk1:

```
RP/0/RP0/CPU0:router(config)# logging archive
RP/0/RP0/CPU0:router(config-logging-arch)# device disk1
```

logging buffered

To send system logging (syslog) messages to logging buffer, use the **logging buffered** command in XR Config mode. To return to the default, use the **no** form of the **logging buffered** command.

logging buffered { *buffer-size* | **alerts** | **critical** | **debugging** | **discriminator** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** | **entries-count** *count* | **backup-period** }

Syntax Description

buffer-size	Size of the buffer, in bytes. Range is 2097152-125000000 bytes. The default is 2097152 bytes.
entries-count *count*	Specifies the buffer entries-count of syslog messages you want to see. The default value is 2545. The range is 2545-151699.
alerts	Specifies if any immediate action is needed
critical	Specifies critical conditions

debugging	Specifies debugging messages
discriminator	Sets logging buffer discriminator
emergencies	Specifies system is unusable
informational	Specifies informational messages
notifications	Specifies normal but significant conditions
warnings	Specifies warning conditions
backup-period	Sets how often the system flushes buffered syslog messages to persistent storage

Command Default

None

Command Modes

XR Config mode

XR Config Mode

Command History

Release	Modification
Release 26.3.1	A new keyword, **backup-period**, was added to the command.
Release 7.11.1	This command was modified to include **entries-count** option.
Release 6.0	This command was introduced.

Usage Guidelines

Use the **logging buffered** command to copy messages to the logging buffer. The logging buffer is circular, so newer messages overwrite older messages after the buffer is filled. This command is related to the **show logging buffer** command, which means that when you execute a **logging buffered warnings** command, it enables the logging for all the levels below the configured level, including log for LOG_ERR, LOG_CRIT, LOG_ALERT, LOG_EMERG, and LOG_WARNING messages. Use the **logging buffer***size* to specify the size of the buffer. Use the **logging buffer entries-count** command to specify the count of syslog entries.

If both the **logging buffered** *bytes* and **logging buffered entries-count** commands are present, then the maximum configured value is taken to display the number of system log messages.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows the configuration for sending syslog messages to the logging buffer:

```
RP/0/RP0/CPU0:router(config)# logging buffered 3000000
```

This example shows how to specify the count of syslog entries.

```
Router# configure
Router(config)# logging buffered entries-count 3000
Router(config)# commit
```

This example shows how often the system flushes buffered syslog messages to persistent storage based on the specified backup period.

```
Router(config)# logging buffered backup-period 30
Router(config)# commit
```

logging console

To enable logging of system logging (syslog) messages logged to the console by severity level, use the **logging console** command in XR Config mode. To return console logging to the default setting, use the **no** form of this command.

logging console {*severity* | **disable**}
no logging console

Syntax Description

severity	Severity level of messages logged to the console, including events of a higher severity level (numerically lower). The default is **informational**. Settings for the severity levels and their respective system conditions are listed in the table under the "Usage Guidelines" section.
disable	Removes the **logging console** command from the configuration file and disables logging to the console terminal.

Command Default

By default, logging to the console is enabled.

severity: **informational**

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **logging console** command to prevent debugging messages from flooding your screen.

The **logging console** is for the console terminal. The value specified for the *severity* argument causes messages at that level and at numerically lower levels (higher severity levels) to be displayed on the console.

Use the **logging console disable** command to disable console logging completely.

Use the **no logging console** command to return the configuration to the default setting.

Use the **show logging** command to display syslog messages stored in the logging buffer.

The value specified for the *severity* argument causes messages at that level and at numerically lower levels to be displayed on the console terminal. See the table for a list of the possible severity level keywords for the *severity* argument.

This table describes the acceptable severity levels for the *severity* argument.

Table 2: Severity Levels for Messages

Level Keywords	Level	Description	Syslog Definition
emergencies	0	Unusable system	LOG_EMERG
alerts	1	Need for immediate action	LOG_ALERT
critical	2	Critical condition	LOG_CRIT
errors	3	Error condition	LOG_ERR
warnings	4	Warning condition	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational message only	LOG_INFO
debugging	7	Debugging message	LOG_DEBUG

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to change the level of messages displayed on the console terminal to **alerts** (1), which means that **alerts** (1) and **emergencies** (0) are displayed:

```
RP/0/RP0/CPU0:router(config)# logging console alerts
```

This example shows how to disable console logging:

```
RP/0/RP0/CPU0:router(config)# logging console disable
```

This example shows how to return console logging to the default setting (the console is enabled, *severity*: **informational**):

```
RP/0/RP0/CPU0:router# no logging console
```

logging console disable

To disable logging of system logging (syslog) messages logged to the console, use the **logging console disable** command in XR Config mode. To return logging to the default setting, use the **no** form of this command.

logging console disable
no logging consoledisable

Syntax Description This command has no keywords or arguments.

Command Default By default, logging is enabled.

Command Modes XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines Use the **logging console disable** command to disable console logging completely.

Use the **no logging console disable** command to return the configuration to the default setting.

Task ID

Task ID	Operations
logging	read, write

Examples This example shows how to disable syslog messages:

```
RP/0/RP0/CPU0:router(config)# logging console disable
```

logging container all

To enable logging of messages from third-party software containers, use the **logging container all** command in XR Config mode. To disable logging messages from third-party containers, use the **no** form of this command.

logging container all

Syntax Description

container	Enables the logging of messages from third-party software containers.
all	Specifies all running containers in the device.

Command Default By default, logging is disabled.

Command Modes XR Config mode

Command History

Release	Modification
Release 7.3.15	This command was introduced.

Usage Guidelines None.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to enable third-party software container logging and how to view the logs for the third-party software container named DOCKER:

```
Router# configure
Router(config)# logging container all
Router(config)# commit


Router# show logging | inc DOCKER
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level warnings, 5 messages logged
    Monitor logging: level debugging, 0 messages logged
    Trap logging: level informational, 0 messages logged
    Buffer logging: level debugging, 148 messages logged

Log Buffer (2097152 bytes):

RP/0/RP0/CPU0:Mar  5 06:56:11.913 UTC: exec[66927]: %SECURITY-LOGIN-6-AUTHEN_SUCCESS :
Successfully authenticated user 'lab' from 'console' on 'con0_RP0_CPU0'
RP/0/RP0/CPU0:Mar  5 06:58:13.053 UTC: config[66985]: %MGBL-SYS-5-CONFIG_I : Configured
from console by lab
RP/0/RP0/CPU0:Mar  5 06:59:04.775 UTC: ubuntu-1[67232]: %OS-SYSLOG-6-DOCKER_APP :
^[]0;root@c382b2e7bed6: /^Groot@c382b2e7bed6:/# testlog
RP/0/RP0/CPU0:Mar  5 06:59:04.830 UTC: config[67139]: %MGBL-CONFIG-6-DB_COMMIT : Configuration
 committed by user 'lab'. Use 'show configuration commit changes 1000000012' to view the
changes.
RP/0/RP0/CPU0:Mar  5 06:59:45.028 UTC: config[67139]: %MGBL-SYS-5-CONFIG_I : Configured
from console by lab
RP/0/RP0/CPU0:Mar  5 06:59:48.552 UTC: run_cmd[67780]: %INFRA-INFRA_MSG-5-RUN_LOGIN : User
 lab logged into shell from con0/RP0/CPU0
RP/0/RP0/CPU0:Mar  5 06:59:56.073 UTC: ubuntu-1[67976]: %OS-SYSLOG-6-DOCKER_APP : testlog-123

RP/0/RP0/CPU0:Mar  5 07:00:12.471 UTC: ubuntu-1[68099]: %OS-SYSLOG-6-DOCKER_APP : testlog-new1

RP/0/RP0/CPU0:Mar  5 07:01:55.747 UTC: ubuntu-1[68245]: %OS-SYSLOG-6-DOCKER_APP : testlog-new1

RP/0/RP0/CPU0:Mar  5 07:02:02.869 UTC: run_cmd[67780]: %INFRA-INFRA_MSG-5-RUN_LOGOUT : User
 lab logged out of shell from con0/RP0/CPU0
```

logging events link-status

To enable the logging of link-status system logging (syslog) messages for logical and physical links, use the **logging events link-status** command in XR Config mode. To disable the logging of link status messages, use the **no** form of this command.

logging events link-status {**disable** | **software-interfaces**}
no logging events link-status [**disable** | **software-interfaces**]

Syntax Description

disable	Disables the logging of link-status messages for all interfaces, including physical links.
software-interfaces	Enables the logging of link-status messages for logical links as well as physical links.

Command Default

The logging of link-status messages is enabled for physical links.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

When the logging of link-status messages is enabled, the router can generate a high volume of link-status up and down system logging messages.

Use the **no logging events link-status** command to enable the logging of link-status messages for physical links only, which is the default behavior.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to disable the logging of physical and logical link-status messages:

```
RP/0/RP0/CPU0:router(config)# logging events link-status disable
```

logging events link-status (interface)

To enable the logging of link-status system logging (syslog) messages on a specific interface for virtual interfaces and subinterfaces, use the **logging events link-status** command in the appropriate interface or subinterface mode. To disable the logging of link status messages, use the **no** form of this command.

logging events link-status
no logging events link-status

Syntax Description

This command has no keywords or arguments.

Command Default

The logging of link-status messages is disabled for virtual interfaces and subinterfaces.

Command Modes

Interface configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

When the logging of link-status messages is enabled, the router can generate a high volume of link-status up and down system logging messages. The **logging events link-status** command enables messages for virtual interfaces and subinterfaces only.

The **logging events link-status** command allows you to enable and disable logging on a specific interface for bundles, tunnels, and VLANs.

Use the **no logging events link-status** command to disable the logging of link-status messages.



Note Enabling the **logging events link-status** command on a specific interface overrides the global configuration set using the **logging events link-status** command described in this section.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows the results of turning on logging for a bundle interface:

```
RP/0/RP0/CPU0:router(config)# int bundle-ether1
RP/0/RP0/CPU0:router(config-if)# logging events link-status
RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# commit

LC/0/4/CPU0:Jun 29 12:51:26.887 : ifmgr[142]:
%PKT_INFRA-LINK-3-UPDOWN : Interface HundredGigE0/0/0/0, changed state to Up

LC/0/4/CPU0:Jun 29 12:51:26.897 : ifmgr[142]:
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface HundredGigE0/0/0/0, changed state
 to Up

RP/0/RP0/CPU0:router(config-if)# shutdown
RP/0/RP0/CPU0:router(config-if)# commit

LC/0/4/CPU0:Jun 29 12:51:32.375 : ifmgr[142]:
%PKT_INFRA-LINK-3-UPDOWN : Interface HundredGigE0/0/0/0, changed state to Down

LC/0/4/CPU0:Jun 29 12:51:32.376 : ifmgr[142]:
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface HundredGigE0/0/0/0, changed state
 to Down
```

This example shows a sequence of commands for a tunnel interface with and without logging turned on:

```
RP/0/RP0/CPU0:router(config)# int tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# commit
RP/0/RP0/CPU0:router(config-if)# shutdown
RP/0/RP0/CPU0:router(config-if)# commit
RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# commit
RP/0/RP0/CPU0:router(config-if)# logging events link-status
RP/0/RP0/CPU0:router(config-if)# commit
```

```
RP/0/RP0/CPU0:router(config-if)# shutdown
RP/0/RP0/CPU0:router(config-if)# commit

RP/0/RP0/CPU0:Jun 29 14:05:57.732 : ifmgr[176]:
%PKT_INFRA-LINK-3-UPDOWN : Interface tunnel-te1, changed state to Administratively Down

RP/0/RP0/CPU0:Jun 29 14:05:57.733 : ifmgr[176]:
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface tunnel-te1, changed state to
Administratively Down

RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# commit

RP/0/RP0/CPU0:Jun 29 14:06:02.104 : ifmgr[176]:
%PKT_INFRA-LINK-3-UPDOWN : Interface tunnel-te1, changed state to Down

RP/0/RP0/CPU0:Jun 29 14:06:02.109 : ifmgr[176]:
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface tunnel-te1, changed state to
Down
```

This example shows the same process for a subinterface:

```
RP/0/RP0/CPU0:router(config)# int HundredGigE 0/0/0/0.1
RP/0/RP0/CPU0:router(config-subif)# commit
RP/0/RP0/CPU0:router(config-subif)# shutdown
RP/0/RP0/CPU0:router(config-subif)# commit
RP/0/RP0/CPU0:router(config-subif)# no shutdown
RP/0/RP0/CPU0:router(config-subif)# commit
RP/0/RP0/CPU0:router(config-subif)# logging events link-status
RP/0/RP0/CPU0:router(config-subif)# commit
RP/0/RP0/CPU0:router(config-subif)# shutdown
RP/0/RP0/CPU0:router(config-subif)# commit

LC/0/5/CPU0:Jun 29 14:06:46.710 : ifmgr[142]:
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface HundredGigE0/0/0/0.1, changed
state to Administratively Down

LC/0/5/CPU0:Jun 29 14:06:46.726 : ifmgr[142]:
%PKT_INFRA-LINK-3-UPDOWN : Interface HundredGigE0/0/0/0.1, changed state to Administratively
 Down

RP/0/RP0/CPU0:router(config-subif)# no shutdown
RP/0/RP0/CPU0:router(config-subif)# commit

LC/0/5/CPU0:Jun 29 14:06:52.229 : ifmgr[142]:
%PKT_INFRA-LINK-3-UPDOWN : Interface HundredGigE0/0/0/0.1, changed state to Up


LC/0/5/CPU0:Jun 29 14:06:52.244 : ifmgr[142]:
%PKT_INFRA-LINEPROTO-6-UPDOWN : Line protocol on Interface HundredGigE0/0/0/0.1, changed
state to Down
```

logging facility

To configure the type of syslog facility in which system logging (syslog) messages are sent to syslog servers, use the **logging facility** command in XR Config mode. To remove the **logging facility** command from the configuration file and disable the logging of messages to any facility type, use the **no** form of this command.

logging facility [*type*]
no logging facility

Syntax Description

type (Optional) Syslog facility type. The default is **local7**. Possible values are listed under Table 1 in the "Usage Guidelines" section.

Command Default

type: **local7**

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This table describes the acceptable options for the *type* argument.

Table 3: Facility Type Descriptions

Facility Type	Description
auth	Authorization system
cron	Cron/at facility
daemon	System daemon
kern	Kernel
local0	Reserved for locally defined messages
local1	Reserved for locally defined messages
local2	Reserved for locally defined messages
local3	Reserved for locally defined messages
local4	Reserved for locally defined messages
local5	Reserved for locally defined messages
local6	Reserved for locally defined messages
local7	Reserved for locally defined messages
lpr	Line printer system
mail	Mail system
news	USENET news
sys9	System use

Facility Type	Description
sys10	System use
sys11	System use
sys12	System use
sys13	System use
sys14	System use
syslog	System log
user	User process
uucp	UNIX-to-UNIX copy system

Use the logging, on page 2command to specify a syslog server host as a destination for syslog messages.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to configure the syslog facility to the **kern** facility type:

```
RP/0/RP0/CPU0:router(config)# logging facility kern
```

logging file

To specify the file logging destination, use the **logging file** command in XR Config mode. To remove the file logging destination, use the **no** form of this command.

logging file *filename* [**discriminator** {**match** | **nomatch**}] [**path** *pathname* {**maxfilesize** | **severity**}]
no logging file

Syntax Description

filename	Specifies the filename of the file to display.
discriminator	Specifies the match or nomatch syslog discriminator.
path *pathname*	Specifies the location to save the logging file.
maxfilesize	(optional) Specifies the maximum file size of the logging file in bytes. Range is from 1 to 2097152 (in KB). Default is 2 GB.

severity	(optional) Specifies the severity level for the logging file. Default is informational. • alerts Immediate action needed (severity=1) • critical Critical conditions (severity=2) • debugging Debugging messages (severity=7) • emergencies System is unusable (severity=0) • errors Error conditions (severity=3) • informational Informational messages (severity=6) • notifications Normal but significant conditions (severity=5) • warnings Warning conditions (severity=4)

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **logging file** command to set the logging file destination. To set the logging file discriminator you have to specify the file name. If it exceeds the maximum file size, then a wrap occurs.

Task ID

Task ID	Operation
logging	read, write

Example

This example shows how to set the maximum file size for the defined file destination:

```
RP/0/RP0/CPU0:router(config)# logging file file1 path /harddisk:/logfiles/ maxfilesize 2048
```

logging format bsd

To send system logging messages to a remote server in Berkeley Software Distribution (BSD) format, use the **logging format bsd** command in XR Config mode. To return console logging to the default setting, use the **no** form of this command.

logging format bsd

Syntax Description

format	Specifies the format of the syslog messages sent to the server.
bsd	Configures the format of the syslog messages according to the BSD format.

Command Default

By default, this feature is disabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.1.2	This command was introduced.

Usage Guidelines

None.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to log messages to a server, in the BSD format:

```
Router(config)#logging 209.165.200.225 vrf default severity info
Router(config)#logging format bsd
Router(config)#commit

Router(config)#do show run logging
logging format bsd
logging 209.165.200.225 vrf default severity info
```

logging format rfc5424

To configure the format of the system logging (syslog) messages according to the one outlined in RFC 5424, use the **logging format rfc5424** command in XR Config mode. To return console logging to the default setting, use the **no** form of this command.

logging format rfc5424

Syntax Description

format	Specifies the format of the syslog messages sent to the server.
rfc5424	Configures the format of the syslog messages according to the one outlined in RFC 5424.

Command Default

By default, this feature is disabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

None.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to log messages to a server, in the format specified in RFC 5424:

```
Router(config)#logging 209.165.200.225 vrf default severity info
Router(config)#logging format rfc5424
Router(config)#commit

Router(config)#do show run logging
logging format rfc5424
logging 209.165.200.225 vrf default severity info
```

logging history

To change the severity level of system logging (syslog) messages sent to the history table on the router and a Simple Network Management Protocol (SNMP) network management station (NMS), use the **logging history** command in XR Config mode. To remove the **logging history** command from the configuration and return the logging of messages to the default level, use the **no** form of this command.

logging history *severity*
no logging history

Syntax Description

severity	Severity level of messages sent to the history table on the router and an SNMP NMS, including events of a higher severity level (numerically lower). Settings for the severity levels and their respective system conditions are listed under the Usage Guidelines section for the **logging console** command.

Command Default

severity: **warnings**

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Logging of messages to an SNMP NMS is enabled by the **snmp-server enable traps** command. Because SNMP traps are inherently unreliable and much too important to lose, at least one syslog message, the most recent message, is stored in a history table on the router.

Use the **logging history** command to reflect the history of last 500 syslog messages. For example, when this command is issued, the last 500 syslog messages with severity less than warning message are displayed in the output of **show logging history** command.

Use the show logging history command to display the history table, which contains table size, message status, and message text data.

Use the logging history size command to change the number of messages stored in the history table.

The value specified for the *severity* argument causes messages at that severity level and at numerically lower levels to be stored in the history table of the router and sent to the SNMP NMS. Severity levels are numbered 0 to 7, with 1 being the most important message and 7 being the least important message (that is, the lower the number, the more critical the message). For example, specifying the level critical with the **critical** keyword causes messages at the severity level of **critical** (2), **alerts** (1), and **emergencies** (0) to be stored in the history table and sent to the SNMP NMS.

The **no logging history** command resets the history level to the default.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to change the level of messages sent to the history table and to the SNMP server to **alerts** (1), which means that messages at the severity level of **alerts** (1) and **emergencies** (0) are sent:

```
RP/0/RP0/CPU0:router(config)# logging history alerts
```

logging history size

To change the number of system logging (syslog) messages that can be stored in the history table, use the **logging history size** command in XR Config mode. To remove the **logging history size** command from the configuration and return the number of messages to the default value, use the **no** form of this command.

logging history size *number*
no logging history *number*

Syntax Description

number	Number from 1 to 500 indicating the maximum number of messages that can be stored in the history table. The default is 1 message.

Command Default

number: 1 message

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **logging history size** command to change the number of messages that can be stored in this history table. When the history table is full (that is, when it contains the maximum number of messages specified with the command), the oldest message is deleted from the table to allow the new message to be stored.

Use the logging history command to change the severity level of syslog messages stored in the history file and sent to the SNMP server.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to set the number of messages stored in the history table to 20:

```
RP/0/RP0/CPU0:router(config)# logging history size 20
```

logging hostnameprefix

To append a hostname prefix to system logging (syslog) messages logged to syslog servers, use the **logging hostnameprefix** command in XR Config mode. To remove the **logging hostnameprefix** command from the configuration file and disable the logging host name prefix definition, use the **no** form of this command.

logging hostnameprefix *hostname*
no logging hostnameprefix

Syntax Description

hostname	Hostname that appears in messages sent to syslog servers.

Command Default

No hostname prefix is added to the messages logged to the syslog servers.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **logging hostnameprefix** command to append a hostname prefix to messages sent to syslog servers from the router. You can use these prefixes to sort the messages being sent to a given syslog server from different networking devices.

Use the **logging** command to specify a syslog server host as a destination for syslog messages.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to add the hostname prefix host1 to messages sent to the syslog servers from the router:

```
RP/0/RP0/CPU0:router(config)# logging hostnameprefix host1
```

logging ipv4/ipv6

To configure the differentiated services code point (DSCP) or the precedence value for the IPv4 or IPv6 header of the syslog packet in the egress direction, use the **logging** {**ipv4** | **ipv6**} command in XR EXEC mode. To remove the configured DSCP or precedence value, use the **no** form of this command.

logging {**ipv4** | **ipv6**} {**dscp** *dscp-value* | **precedence** {*numbername*}}
no logging {**ipv4** | **ipv6**} {**dscp** *dscp-value* | **precedence** {*numbername*}}

Syntax Description

ipv4 / **ipv6**	Sets the DSCP or precedence bit for IPv4 or IPv6 packets.
dscp *dscp-value*	Specifies differentiated services code point value or per hop behavior values (PHB). For more information on PHB values, see Usage Guideline section below. The range is from 0 to 63. The default value is 0.
precedence {*number* | *name*}	Sets Type of Service (TOS) precedence value. You can specify either a precedence number or name. The range of argument *number* is between 0 to 7. The *name* argument has following keywords: • routine—Match packets with routine precedence (0) • priority—Match packets with priority precedence (1) • immediate—Match packets with immediate precedence (2) • flash—Match packets with flash precedence (3) • flash-override—Match packets with flash override precedence (4) • critical—Match packets with critical precedence (5) • internet—Match packets with internetwork control precedence (6) • network—Match packets with network control precedence (7)

Command Default

None.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

By specifying PHB values you can further control the format of locally generated syslog traffic on the network.

You may provide these PHB values:

- af11—Match packets with AF11 DSCP (001010)
- af12—Match packets with AF12 dscp (001100)
- af13—Match packets with AF13 dscp (001110)
- af21— Match packets with AF21 dscp (010010)
- af22—Match packets with AF22 dscp (010100)
- af23—Match packets with AF23 dscp (010110)
- af31—Match packets with AF31 dscp (011010)
- af32—Match packets with AF32 dscp (011100)
- af33—Match packets with AF33 dscp (011110)
- af41—Match packets with AF41 dscp (100010)
- af42—Match packets with AF42 dscp (100100)
- af43— Match packets with AF43 dscp (100110)
- cs1—Match packets with CS1(precedence 1) dscp (001000)
- cs2—Match packets with CS2(precedence 2) dscp (010000)
- cs3—Match packets with CS3(precedence 3) dscp (011000)
- cs4—Match packets with CS4(precedence 4) dscp (100000)
- cs5—Match packets with CS5(precedence 5) dscp (101000)
- cs6—Match packets with CS6(precedence 6) dscp (110000)
- cs7—Match packets with CS7(precedence 7) dscp (111000)
- default—Match packets with default dscp (000000)
- ef—Match packets with EF dscp (10111)

Assured Forwarding (AF) PHB group is a means for a provider DS domain to offer different levels of forwarding assurances for IP packets. The Assured Forwarding PHB guarantees an assured amount of bandwidth to an AF class and allows access to additional bandwidth, if obtainable.

For example AF PHB value af11 - Match packets with AF11 DSCP (001010), displays the DSCP values as 10 and 11. The DSCP bits are shown as 001010 and 001011 .

AF11 stands for:

- Assured forwarding class 1 (001)
- Drop priority 100 (1)
- Dropped last in AF1 class

Similarly AF PHB value af12 - Match packets with AF12 dscp (001100), displays the DSCP values as 12 and 13. The DSCP bits are shown as 001100 and 001101.

AF12 stands for:

- Assured forwarding class 1 (001)
- Drop priority 100 (2)
- Dropped second in AF1 class

Class Selector (CS) provides backward compatibility bits,

CS PHB value cs1 - Match packets with CS1(precedence 1) dscp (001000)

CS1 stands for:

- CS1 DSCP bits are displayed as 001000 and 001001
- priority stated as 1

Expedited Forwarding (EF) PHB is defined as a forwarding treatment to build a low loss, low latency, assured bandwidth, end-to-end service. These characteristics are suitable for voice, video and other realtime services.

EF PHB Value ef - Match packets with EF dscp (101110) - this example states the recommended EF value (used for voice traffic).

Task ID

Task ID	Operation
logging	read, write

Example

This example shows how to configure DSCP value as 1 for IPv4 header of syslog packet.

```
RP/0/RP0/CPU0:router(config)#logging ipv4 dscp 1
```

This example shows how to configure DSCP value as 21 for IPv6 header of syslog packet.

```
RP/0/RP0/CPU0:router(config)#logging ipv6 dscp 21
```

This example shows how to configure precedence value as 5 for IPv6 header of syslog packet.

```
RP/0/RP0/CPU0:router(config)#logging ipv6 precedence 5
```

logging localfilesize

To specify the size of the local logging file, use the **logging localfilesize** command in XR Config mode. To remove the **logging localfilesize** command from the configuration file and restore the system to the default condition, use the **no** form of this command.

logging localfilesize *bytes*
no logging localfilesize *bytes*

Syntax Description

bytes	Size of the local logging file in bytes. Range is 0 to 4294967295. Default is 32000 bytes.

Command Default

bytes: 32000 bytes

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **logging localfilesize** command to set the size of the local logging file.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to set the local logging file to 90000 bytes:

```
RP/0/RP0/CPU0:router(config)# logging localfilesize 90000
```

logging monitor

To specify terminal lines other than the console terminal as destinations for system logging (syslog) messages and limit the number of messages sent to terminal lines based on severity, use the **logging monitor** command in XR Config mode. To remove the **logging monitor** command from the configuration file and disable logging to terminal lines other than the console line, use the **no** form of this command.

logging monitor [*severity*]
no logging monitor

Syntax Description

severity	(Optional) Severity level of messages logged to the terminal lines, including events of a higher severity level (numerically lower). The default is **debugging**.

Command Default *severity*: **debugging**

Command Modes XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines The **logging monitor** is for the terminal monitoring. Use the **logging monitor** command to restrict the messages displayed on terminal lines other than the console line (such as virtual terminals). The value set for the *severity* argument causes messages at that level and at numerically lower levels to be displayed on the monitor.

Use the **terminal monitor** command to enable the display of syslog messages for the current terminal session.

Task ID

Task ID	Operations
logging	read, write

Examples This example shows how to set the severity level of messages logged to terminal lines to errors:

```
RP/0/RP0/CPU0:router(config)# logging monitor errors
```

logging source-interface

To set all system logging (syslog) messages being sent to syslog servers 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. To remove the **logging source-interface** command from the configuration file and remove the source designation, use the **no** form of this command.

logging source-interface *type interface-path-id*
no logging source-interface

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default No source IP address is specified.

Command Modes XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines Normally, a syslog message contains the IP address of the interface it uses to leave the networking device. Use the **logging source-interface** command to specify that syslog packets contain the IP address of a particular interface, regardless of which interface the packet uses to exit the networking device.

Use the logging, on page 2 command to specify a syslog server host as a destination for syslog messages.

Task ID

Task ID	Operations
logging	read, write

Examples This example shows how to specify that the IP address for HundredGigE interface 0/1/0/0 be set as the source IP address for all messages:

```
RP/0/RP0/CPU0:router(config)# logging source-interface HundredGigE interface 0/1/0/0
```

logging suppress deprecated

To prevent the logging of messages to the console to indicate that commands are deprecated, use the **logging suppress deprecated** command in XR Config mode. To remove the **logging suppress deprecated** command from the configuration file, use the **no** form of this command.

logging suppress deprecated
no logging suppress deprecated

Syntax Description This command has no keywords or arguments.

Command Default Console messages are displayed when deprecated commands are used.

Command Modes XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines The **logging suppress deprecated** command affects messages to the console only.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to suppress the consecutive logging of deprecated messages:

```
RP/0/RP0/CPU0:router(config)# logging suppress deprecated
```

logging suppress duplicates

To prevent the consecutive logging of more than one copy of the same system logging (syslog) message, use the **logging suppress duplicates** command in XR Config mode. To remove the **logging suppress duplicates** command from the configuration file and disable the filtering process, use the **no** form of this command.

logging suppress duplicates
no logging suppress duplicates

Syntax Description

This command has no keywords or arguments.

Command Default

Duplicate messages are logged.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

If you use the **logging suppress duplicates** command during debugging sessions, you might not see all the repeated messages and could miss important information related to problems that you are attempting to isolate and resolve. In such a situation, you might consider disabling this command.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to suppress the consecutive logging of duplicate messages:

```
RP/0/RP0/CPU0:router(config)# logging suppress duplicates
```

logging trap

To specify the severity level of messages logged to snmp server, use the **logging trap** command in XR Config mode. To restore the default behavior, use the **no** form of this command.

logging trap [*severity*]
no logging trap

Syntax Description

severity	(Optional) Severity level of messages logged to the snmp server, including events of a higher severity level (numerically lower). The default is **informational**. Settings for the severity levels and their respective system conditions are listed under Table 1 in the "Usage Guidelines" section for the **logging console** command.

Command Default

severity: **informational**

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **logging trap** command to limit the logging of messages sent to snmp servers to only those messages at the specified level.

The "Usage Guidelines" section for the logging console command lists the syslog definitions that correspond to the debugging message levels.

Use the logging, on page 2 command to specify a syslog server host as a destination for syslog messages.

The **logging trap disable** will disable the logging of messages to both snmp server and syslog servers.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to restrict messages to **notifications** (5) and numerically lower levels.

```
RP/0/RP0/CPU0:router(config)# logging trap notifications
```

login-history

To enable the display of the login banner in compliance with US DoD login notification requirements, use the **login-history enable** command in the XR Config mode. To disable the display of the login banner, use the **login-history enable** command in the XR Config mode.

login-history { **enable** | **disable** }

Command Default

The display of the login banner is not enabled.

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to enable and disable the display of the login banner in compliance with the US DoD login notification requirements:

```
Router(config)# login-history enable
Router(config-un)# login-history disable
```

If you enable the login banner, you can display the login notification banner that conforms to the US (DOD) requirements:

```
Username: user1
Password:
User root : login failed 2 time(s) successful 5 time(s).
Most recent Failure Thu Mar 19 2020 21:12:00 UTC
to con0_RP0_CPU0 from console

User user1 last logged in successfully Thu Mar 19 2020 21:11:50 UTC
to con0_RP0_CPU0 from console
```

service timestamps

To modify the time-stamp format for system logging (syslog) and debug messages, use the **service timestamps** command in XR Config mode. To revert to the default timestamp format, use the **no** form of this command.

service timestamps [[**debug** | **log**] {**datetime** [**localtime**] [**msec**] [**show-timezone**] | **disable** | **uptime**}]
no service timestamps [[**debug** | **log**] {**datetime** [**localtime**] [**msec**] [**show-timezone**] | **disable** | **uptime**}]

Syntax Description

debug	(Optional) Specifies the time-stamp format for debugging messages.
log	(Optional) Specifies the time-stamp format for syslog messages.
datetime	(Optional) Specifies that syslog messages are time-stamped with date and time.
localtime	(Optional) When used with the **datetime** keyword, includes the local time zone in time stamps.
msec	(Optional) When used with the **datetime** keyword, includes milliseconds in the time stamp.

show-timezone	(Optional) When used with the **datetime** keyword, includes time zone information in the time stamp.
disable	(Optional) Causes messages to be time-stamped in the default format.
uptime	(Optional) Specifies that syslog messages are time-stamped with the time that has elapsed since the networking device last rebooted.

Command Default

Messages are time-stamped in the month day hh:mm:ss by default.

The default for the **service timestamps log datetime localtime** and **service timestamps debug datetime localtime** forms of the command with no additional keywords is to format the time in the local time zone, without milliseconds and time zone information.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Time stamps can be added to either debugging or syslog messages independently. The **uptime** keyword adds time stamps in the format hhhh:mm:ss, indicating the elapsed time in hours:minutes:seconds since the networking device last rebooted. The **datetime** keyword adds time stamps in the format mmm dd hh:mm:ss, indicating the date and time according to the system clock. If the system clock has not been set, the date and time are preceded by an asterisk (*), which indicates that the date and time have not been set and should be verified.

The **no** form of the **service timestamps** command causes messages to be time-stamped in the default format.

Entering the **service timestamps** form of this command without any keywords or arguments is equivalent to issuing the **service timestamps debug uptime** form of this command.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to enable time stamps on debugging messages, which show the elapsed time since the networking device last rebooted:

```
RP/0/RP0/CPU0:router(config)# service timestamps debug uptime
```

This example shows how to enable time stamps on syslog messages, which show the current time and date relative to the local time zone, with the time zone name included:

```
RP/0/RP0/CPU0:router(config)# service timestamps log datetime localtime show-timezone
```

severity (logging)

To specify the filter level for logs, use the **severity** command in logging archive configuration mode. To return to the default, use the **no** form of this command.

severity {*severity*}
no severity

Syntax Description

severity	Severity level for determining which messages are logged to the archive. Possible severity levels and their respective system conditions are listed in the "Usage Guidelines" section for the **logging console** command. The default is **informational**.

Command Default

Informational

Command Modes

Logging archive configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **severity** command to specify the filter level for syslog messages. All syslog messages higher in severity or the same as the configured value are logged to the archive.

The "Usage Guidelines" section for the logging console command describes the acceptable severity levels for the *severity* argument.

Task ID

Task ID	Operations
logging	read, write

Examples

This example shows how to specify that warning conditions and higher-severity messages are logged to the archive:

```
Router(config)# logging archive
Router(config-logging-arch)# severity warnings
```

show logging

To display the contents of the logging buffer, use the **show logging** command in XR EXEC mode.

show logging [[**alarm-location location** *location*] | [**correlator** *options*] | **local location** *node-id* | [**location** *node-id*] [**start** *month day hh* **:** *mm* **:** *ss*] [**process** *name*] [**string** *string*] [**end** *month day hh* **:** *mm* **:ss**][**events** *options*][**history**][**last** *entries*][**suppress rule** {*rule_name* | **all**}]]

Syntax Description

alarm-location trace *location*	(Optional) Displays alarm-location information. The **trace** option shows trace data for the alarm location components.
correlator*options*	(Optional) Displays content and information about correlation buffer. Options available are: • buffer: Displays content of the correlation buffer. • info: Displays information about event correlation. • trace: Displays trace data for the alarm_logger component.
end *month day hh* **:** *mm* **:** *ss*	(Optional) Displays syslog messages with a time stamp equal to or lower than the time stamp specified with the *monthday hh* **:** *mm* **:** *ss* argument. The ranges for the *month day hh* **:** *mm* **:** *ss* arguments are: • *month*—The month of the year. The values for the *month* argument are the names of the twelve months. • *day*—Day of the month. Range is from 01 to 31. • *hh* **:**—Hours. Range is from 00 to 23. You must insert a colon after the *hh* argument. • *mm* **:**—Minutes. Range is from 00 to 59. You must insert a colon after the *mm* argument. • *ss*—Seconds. Range is from 00 to 59.
events *options*	Displays content and information about the event buffer.The various options available are: • buffer: Displays content of the event buffer. • info: Displays information about events buffer. • rule: Displays specified rules. • ruleset: Displays rulesets. • trace: Displays trace data for the correlation component.
history	Displays contents of logging history.
last *entries*	Displays last <n> entries. The number of entries can range from 1 to 500.
local location *node-id*	(Optional) Displays system logging (syslog) messages from the specified local buffer. The *node-id* argument is entered in the *rack/slot/modul e* notation.
location *node-id*	(Optional) Displays syslog messages from the designated node. The *node-id* argument is entered in the *rack/slot/modul e* notation.

start *month day hh* **:** *mm* **:** *ss*	(Optional) Displays syslog messages with a time stamp equal to or higher than the time stamp specified with the *month day mm* **:** *hh* **:** *ss* argument. The ranges for the *month day hh* **:** *mm* **:** *ss* arguments are as follows: • *month*—The month of the year. The values for the *month* argument are the names of the twelve months. • *day*—Day of the month. Range is from 01 to 31. • *hh* **:**—Hours. Range is from 00 to 23. You must insert a colon after the *hh* argument. • *mm* **:**—Minutes. Range is from 00 to 59. You must insert a colon after the *mm* argument. • *ss*—Seconds. Range is from 00 to 59.
process *name*	(Optional) Displays syslog messages related to the specified process.
string *string*	(Optional) Displays syslog messages that contain the specified string.
suppress rule{*rule_name*|**all**}	Displays content and information about log suppression. The **rule** option shows specified rules.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **show logging** command to display the state of syslog error and event logging on the processor console. The information from the command includes the types of logging enabled and the size of the buffer.

Task ID

Task ID	Operations
logging	read

Examples

This is the sample output from the **show logging** command with the **process** keyword and *name* argument. Syslog messages related to the init process are displayed in the sample output.

```
RP/0/RP0/CPU0:router# show logging process init

Syslog logging: enabled (24 messages dropped, 0 flushes, 0 overruns)
Console logging: level, 59 messages logged
Monitor logging: level debugging, 0 messages logged
```

```
Trap logging: level informational, 0 messages logged
Buffer logging: level debugging, 75 messages logged

Log Buffer (16384 bytes):

LC/0/1/CPU0:May 24 22:20:13.043 : init[65540]: %INIT-7-INSTALL_READY : total time 47.522
seconds
SP/0/1/SP:May 24 22:18:54.925 : init[65541]: %INIT-7-MBI_STARTED : total time 7.159 seconds

SP/0/1/SP:May 24 22:20:16.737 : init[65541]: %INIT-7-INSTALL_READY : total time 88.984
seconds
SP/0/SM1/SP:May 24 22:18:40.993 : init[65541]: %INIT-7-MBI_STARTED : total time 7.194 seconds

SP/0/SM1/SP:May 24 22:20:17.195 : init[65541]: %INIT-7-INSTALL_READY : total time 103.415
seconds
SP/0/2/SP:May 24 22:18:55.946 : init[65541]: %INIT-7-MBI_STARTED : total time 7.152 seconds

SP/0/2/SP:May 24 22:20:18.252 : init[65541]: %INIT-7-INSTALL_READY : total time 89.473
seconds
```

This is the sample output from the **show logging** command using both the **process** *name* keyword argument pair and **location** *node-id* keyword argument pair. Syslog messages related to the “init” process emitted from node 0/RP0/CPU0 are displayed in the sample output.

```
RP/0/RP0/CPU0:router# show logging process init location 0/RP0/CPU0

Syslog logging: enabled (24 messages dropped, 0 flushes, 0 overruns)
Console logging: level, 59 messages logged
Monitor logging: level debugging, 0 messages logged
Trap logging: level informational, 0 messages logged
Buffer logging: level debugging, 75 messages logged

Log Buffer (16384 bytes):
LC/0/1/CPU0:May 24 22:20:13.043 : init[65540]: %INIT-7-INSTALL_READY : total time 47.522
seconds
```

This table describes the significant fields shown in the display.

Table 4: show logging Field Descriptions

Field	Description
Syslog logging	If enabled, system logging messages are sent to a UNIX host that acts as a syslog server; that is, the host captures and saves the messages.
Console logging	If enabled, the level and the number of messages logged to the console are stated; otherwise, this field displays “disabled.”
Monitor logging	If enabled, the minimum level of severity required for a log message to be sent to the monitor terminal (not the console) and the number of messages logged to the monitor terminal are stated; otherwise, this field displays “disabled.”
Trap logging	If enabled, the minimum level of severity required for a log message to be sent to the syslog server and the number of messages logged to the syslog server are stated; otherwise, this field displays “disabled.”
Buffer logging	If enabled, the level and the number of messages logged to the buffer are stated; otherwise, this field displays “disabled.”

To find out OOR state of a router's hardware and Software Development Kit (SDK) resources, you can view the sample output from the **show logging** command with the output modifier as OOR. You can configure the threshold value at which a router reaches the **OOR State Red** or **Yellow** by using the `oor hw threshold` command. For more information, see `oor hw threshold` command in the chapter *Logging Services Commands* of *System Monitoring Command Reference for Cisco 8000 Series Routers*.

```
Router# show logging | inc OOR
Wed Jan 6 23:36:34.138 EST
LC/0/0/CPU0:Jan 6 23:01:09.609 EST: npu_drvr[278]: %PLATFORM-OFA-4-OOR_YELLOW : NPU 1, Table
 nhgroup, Resource stage2_lb_group
LC/0/0/CPU0:Jan 6 23:01:29.655 EST: npu_drvr[278]: %PLATFORM-OFA-4-OOR_YELLOW : NPU 1, Table
 nhgroup, Resource stage2_lb_member
LC/0/0/CPU0:Jan 6 23:01:38.938 EST: npu_drvr[278]: %PLATFORM-OFA-1-OOR_RED : NPU 3, Table
nhgroup, Resource stage2_lb_group
```

show logging history

To display information about the state of the system logging (syslog) history table, use the **show logging history** command in XR EXEC mode mode.

show logging history

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **show logging history** command to display information about the syslog history table, such as the table size, the status of messages, and the text of messages stored in the table. Simple Network Management Protocol (SNMP) configuration parameters and protocol activity also are displayed.

Use the logging history command to change the severity level of syslog messages stored in the history file and sent to the SNMP server.

Use the logging history size to change the number of syslog messages that can be stored in the history table.

Task ID

Task ID	Operations
logging	read

Examples

This is the sample output from the **show logging history** command:

```
RP/0/RP0/CPU0:router# show logging history
```

```
Syslog History Table: '1' maximum table entries
saving level 'warnings' or higher
137 messages ignored, 0 dropped, 29 table entries flushed
SNMP notifications disabled
```

This table describes the significant fields shown in the display.

Table 5: show logging history Field Descriptions

Field	Description
maximum table entries	Number of messages that can be stored in the history table. Set with the **logging history size** command.
saving level	Level of messages that are stored in the history table and sent to the SNMP server (if SNMP notifications are enabled). Set with the **logging history** command.
messages ignored	Number of messages not stored in the history table because the severity level is greater than that specified with the **logging history** command.
SNMP notifications	Status of whether syslog traps of the appropriate level are sent to the SNMP server. Syslog traps are either enabled or disabled through the **snmp-server enable** command.

terminal monitor

To enable the display of debug command output and system logging (syslog) messages for the current terminal session, use the **terminal monitor** command in XR EXEC mode.

terminal monitor [**disable**]

Syntax Description

disable	(Optional) Disables the display of syslog messages for the current terminal session.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Use the **terminal monitor** command to enable the display of syslog messages for the current terminal session.

Note Syslog messages are not sent to terminal lines unless the **logging monitor** is enabled.

Use the **terminal monitor disable** command to disable the display of logging messages for the current terminal session. If the display of logging messages has been disabled, use the **terminal monitor** command to re-enable the display of logging messages for the current terminal session.

The **terminal monitor** command is set locally, and does not remain in effect after a terminal session has ended; therefore, you must explicitly enable or disable the **terminal monitor** command each time that you would like to monitor a terminal session.

Task ID

Task ID	Operations
logging	execute

Examples

This example shows how to enable the display syslog messages for the current terminal session:

```
RP/0/RP0/CPU0:router# terminal monitor
```

enable-pam process-monitoring

To detect the blocked processes on all nodes in the system, use the **enable-pam process-monitoring** command in EXEC mode to enable the Platform Automated Monitoring process blockage monitoring feature.

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.5.2	This command was introduced.

Usage Guidelines

This command generates tech-support information that is useful for Cisco Technical Support representatives when troubleshooting a router. When PAM detects a process crash, traceback, potential memory leak, CPU hog, a full file system or blocked process on any node, 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 system log message with severity level as warning, mentioning the respective issue.

For Cisco Technical Support contact information, see the 'Obtaining Documentation and Submitting a Service Request' section in the Preface.

Task ID

Task ID	Operations
monitor	read
basic-services or cisco-support	read

Examples

```
Router# enable-pam process-monitoring
PAM "Monitoring Process Blockage" Feature is enabled
```

disable-pam process-monitoring

To disable the Platform Automated Monitoring process blockage monitoring feature, use the **disable-pam process-monitoring** command in EXEC mode. To re-enable the feature, use the **enable** form of this command.

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes EXEC mode

Command History

Release	Modification
Release 7.5.2	This command was introduced.

Usage Guidelines This command generates tech-support information that is useful for Cisco Technical Support representatives when troubleshooting a router. When PAM detects a process crash, traceback, potential memory leak, CPU hog, a full file system or blocked process on any node, 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 system log message with severity level as warning, mentioning the respective issue.

For Cisco Technical Support contact information, see the 'Obtaining Documentation and Submitting a Service Request' section in the Preface.

Task ID

Task ID	Operations
monitor	read
basic-services or cisco-support	read

Examples

```
Router# disable-pam process-monitoring
PAM "Monitoring Process Blockage" Feature has been disabled
```

show pam process-monitoring-status

To see if the Platform Automated Monitoring (PAM) process blockage monitoring is enabled or disabled, use the **show pam process-monitoring-status** command in EXEC mode.

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes EXEC mode

Command History

Release	Modification
Release 7.5.2	This command was introduced.

Usage Guidelines

This command generates tech-support information that is useful for Cisco Technical Support representatives when troubleshooting a router. When PAM detects a process crash, traceback, potential memory leak, CPU hog, a full file system or blocked process on any node, 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 system log message with severity level as warning, mentioning the respective issue.

For Cisco Technical Support contact information, see the 'Obtaining Documentation and Submitting a Service Request' section in the Preface.

Task ID

Task ID	Operations
monitor	read
basic-services or cisco-support	read

Examples

```
Router# show pam process-monitoring-status
PAM "Monitoring Process Blockage" Feature is disabled
```

show syslog persistent status

To display the status of persistent logging buffers, use the **show syslog persistent status** command in EXEC mode.

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 26.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read
basic-services or cisco-support	read

Examples

This example shows the status of persistent logging file details.

```
Router# show syslog persistent status
Thu Aug 6 11:14:32.464 UTC
node: node0_RP0_CPU0
Persistent file details:
Filename: /var/log/xr_syslog/persistent/messages.log
Maximum Size: 2731 messages (2097432 bytes)
Message Write Index: 260 messages (199704 bytes)
Dropped Messages: 0
Invalid Messages: 14
No of Wraps: 0
Backup Period: 10000 milliseconds
```