



# Alarm Management and Logging Correlation Commands

---

This module describes the commands used to manage alarms and configure logging correlation rules for system monitoring on the router.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

For detailed information about alarm management and logging correlation concepts, configuration tasks, and examples, see the *Implementing and Monitoring Alarms and Logging Correlation* module in the *System Monitoring Configuration Guide for Cisco CRS Routers*.

For system logging commands, see the *Logging Services Commands* module.

For system logging concepts, see the *Implementing Logging Services* module in the *System Monitoring Configuration Guide for Cisco CRS Routers*.

- [alarm](#), on page 3
- [all-alarms](#), on page 4
- [all-of-router](#), on page 5
- [clear logging correlator delete](#), on page 6
- [clear logging events delete](#), on page 7
- [clear logging events reset](#), on page 11
- [context-correlation](#), on page 12
- [logging correlator apply rule](#), on page 13
- [logging correlator apply ruleset](#), on page 15
- [logging correlator buffer-size](#), on page 17
- [logging correlator rule](#), on page 18
- [logging correlator ruleset](#), on page 21
- [logging events buffer-size](#), on page 22
- [logging events display-location](#), on page 24
- [logging events level](#), on page 26
- [logging events threshold](#), on page 28
- [logging suppress apply rule](#), on page 29
- [logging suppress rule](#), on page 30
- [nonrootcause](#), on page 31

- [reissue-nonbistate](#), on page 33
- [reparent](#), on page 34
- [rootcause](#), on page 36
- [show logging correlator buffer](#), on page 38
- [show logging correlator info](#), on page 40
- [show logging correlator rule](#), on page 41
- [show logging correlator ruleset](#), on page 44
- [show logging events buffer](#), on page 46
- [show logging events info](#), on page 50
- [show logging suppress rule](#), on page 52
- [show snmp correlator buffer](#), on page 54
- [show snmp correlator info](#), on page 55
- [show snmp correlator rule](#), on page 56
- [show snmp correlator ruleset](#), on page 57
- [source](#), on page 58
- [timeout](#), on page 59
- [timeout-rootcause](#), on page 61

# alarm

To specify a type of alarm to be suppressed by a logging suppression rule, use the **alarm** command in logging suppression rule configuration mode.

```
alarm msg-category group-name msg-code
```

## Syntax Description

*msg-category* Message category of the root message.

*group-name* Group name of the root message.

*msg-code* Message code of the root message.

## Command Default

No alarm types are configured by default.

## Command Modes

Logging suppression rule configuration

## Command History

Release	Modification
Release 3.8.0	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operations
logging	read, write

## Examples

This example shows how to configure the logging suppression rule “commit” to suppress alarms whose root message are “MBGL”, with group name “commit” and message code “succeeded”:

```
RP/0/RP0/CPU0:router(config)# logging suppress rule commit
RP/0/RP0/CPU0:router(config-suppr-rule)# alarm MBGL COMMIT SUCCEDED
```

## Related Commands

Command	Description
<a href="#">logging suppress rule, on page 30</a>	Creates a logging suppression rule.

# all-alarms

To configure a logging suppression rule to suppress all types of alarms, use the **all-alarms** command in logging suppression rule configuration mode.

## all-alarms

**Syntax Description** This command has no keywords or arguments.

**Command Default** No alarm types are configured by default.

**Command Modes** Logging suppression rule configuration

Command History	Release	Modification
	Release 3.8.0	This command was introduced.

**Usage Guidelines** No specific guidelines impact the use of this command.

Task ID	Task	Operations
	logging	read, write

**Examples** This example shows how to configure the logging suppression rule commit to suppress all alarms:

```
RP/0/RP0/CPU0:router(config)# logging suppress rule commit
RP/0/RP0/CPU0:router(config-suppr-rule)# all-alarms
```

Related Commands	Command	Description
	<a href="#">logging suppress rule, on page 30</a>	Creates a logging suppression rule.

# all-of-router

To apply a logging suppression rule to alarms originating from all locations on the router, use the **all-of-router** command in logging suppression apply rule configuration mode.

## all-of-router

**Syntax Description** This command has no keywords or arguments.

**Command Default** No scope is configured by default.

**Command Modes** Logging suppression apply rule configuration

Command History	Release	Modification
	Release 3.8.0	This command was introduced.

**Usage Guidelines** No specific guidelines impact the use of this command.

Task ID	Task ID	Operations
	logging	execute

**Examples** This example shows how to apply the logging suppression rule “commit” to all locations on the router:

```
RP/0/RP0/CPU0:router(config)# logging suppress apply rule commit
RP/0/RP0/CPU0:router(config-suppr-apply-rule)# all-of-router
```

Related Commands	Command	Description
	<a href="#">logging suppress apply rule, on page 29</a>	Applies and activates a logging suppression rule.

# clear logging correlator delete

To delete all messages or messages specified by a correlation ID from the logging correlator buffer, use the **clear logging correlator delete** command in EXEC mode.

```
clear logging correlator delete {all-in-buffer correlation-id}
```

## Syntax Description

**all-in-buffer** Clears all messages in the logging correlator buffer.

*correlation-id* Correlation event record ID. Up to 14 correlation IDs can be specified, separated by a space. Range is 0 to 4294967294.

## Command Default

No messages are automatically deleted unless buffer capacity is reached.

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 2.0	This command was introduced.

## Usage Guidelines

Use the [show logging correlator buffer, on page 38](#) command to confirm that records have been cleared.

Use the [logging correlator buffer-size, on page 17](#) command to configure the capacity of the logging correlator buffer.

## Task ID

Task ID	Operations
logging	execute

## Examples

This example shows how to clear all records from the logging correlator buffer:

```
RP/0/RP0/CPU0:router# clear logging correlator delete all-in-buffer
```

## Related Commands

Command	Description
<a href="#">show logging correlator buffer, on page 38</a>	Displays messages in the logging correlator buffer.

## clear logging events delete

To delete messages from the logging events buffer, use the **clear logging events delete** command in EXEC mode.

**clear logging events delete**

Syntax	Description
<b>admin-level-only</b>	Deletes only events at the administrative level.
<b>all-in-buffer</b>	Deletes all event IDs from the logging events buffer.
<b>bistate-alarms-set</b>	Deletes bi-state alarms in the SET state.
<b>category</b> <i>name</i>	Deletes events from a specified category.
<b>context</b> <i>name</i>	Deletes events from a specified context.
<b>event-hi-limit</b> <i>event-id</i>	Deletes events with an event ID equal to or lower than the event ID specified with the <i>event-id</i> argument. Range is 0 to 4294967294.
<b>event-lo-limit</b> <i>event-id</i>	Deletes events with an event ID equal to or higher than the event ID specified with the <i>event-id</i> argument. Range is 0 to 4294967294.
<b>first</b> <i>event-count</i>	Deletes events, beginning with the first event in the logging events buffer. For the <i>event-count</i> argument, enter the number of events to be deleted.
<b>group</b> <i>message-group</i>	Deletes events from a specified message group.
<b>last</b> <i>event-count</i>	Deletes events, beginning with the last event in the logging events buffer. For the <i>event-count</i> argument, enter the number of events to be deleted.
<b>location</b> <i>node-id</i>	Deletes messages from the logging events buffer for the specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<b>message</b> <i>message-code</i>	Deletes events with the specified message code.
<b>severity-hi-limit</b>	Deletes events with a severity level equal to or lower than the severity level specified with the <i>severity</i> argument.

---

<b>severity</b>	Severity level. Valid values are: <ul style="list-style-type: none"><li>• <b>alerts</b></li><li>• <b>critical</b></li><li>• <b>emergencies</b></li><li>• <b>errors</b></li><li>• <b>informational</b></li><li>• <b>notifications</b></li><li>• <b>warnings</b></li></ul> <p><b>Note</b> Settings for the severity levels and their respective system conditions are listed under the “Usage Guidelines” section for the <b>logging events level</b> command. Events of lower severity level represent events of higher importance.</p>
<b>severity-lo-limit</b>	Deletes events with a severity level equal to or higher than the severity level specified with the <i>severity</i> argument.
<b>timestamp-hi-limit</b>	Deletes events with a time stamp equal to or lower than the specified time stamp.

---



*hh : mm : ss [month] [day] [year]* Time stamp for the **timestamp-hi-limit** or **timestamp-lo-limit** keyword. The *month*, *day*, and *year* arguments default to the current month, day, and year, if not specified.

Ranges for the *hh : mm : ss month day year* arguments are as follows:

- *hh* :—Hours. Range is 00 to 23. You must insert a colon after the *hh* argument.
- *mm* :—Minutes. Range is 00 to 59. You must insert a colon after the *mm* argument.
- *ss*—Seconds. Range is 00 to 59.
- *month*—(Optional) The month of the year. The values for the *month* argument are:
  - january
  - february
  - march
  - april
  - may
  - june
  - july
  - august
  - september
  - october
  - november
  - december
- *day*—(Optional) Day of the month. Range is 01 to 31.
- *year*—(Optional) Year. Enter the last two digits of the year (for example, **04** for 2004). Range is 01 to 37.

---

<b>timestamp-lo-limit</b>	Deletes events with a time stamp equal to or higher than the specified time stamp.
---------------------------	--

---



---

**Command Default**

No messages are automatically deleted unless buffer capacity is reached.

---

**Command Modes**

EXEC mode

---

**Command History**

Release	Modification
---------	--------------

---

Release 2.0	This command was introduced.
-------------	------------------------------

---

Release 3.2	Support was introduced for the <b>admin-level-only</b> keyword option.
-------------	--

---

**clear logging events delete****Usage Guidelines**

This command is used to delete messages from the logging events buffer that match the keywords and arguments that you specify. The description is matched if all of the conditions are met.

Use the [show logging events buffer, on page 46](#) command to verify that events have been cleared from the logging events buffer.

Use the [logging events buffer-size, on page 22](#) command to configure the capacity of the logging events buffer.

**Task ID**

Task ID	Operations
	logging execute

**Examples**

This example shows how to delete all messages from the logging events buffer:

```
RP/0/RP0/CPU0:router# clear logging events delete all-in-buffer
```

**Related Commands**

Command	Description
<a href="#">clear logging events reset, on page 11</a>	Resets bi-state alarms.
<a href="#">show logging events buffer, on page 46</a>	Displays messages in the logging events buffer.

# clear logging events reset

To reset bi-state alarms, use the **clear logging events reset** command in EXEC mode.

```
clear logging events reset {all-in-buffer event-id}
```

## Syntax Description

**all-in-buffer** Resets all bi-state alarm messages in the event logging buffer.

*event-id* Event ID. Resets the bi-state alarm for an event or events. Up to 32 event IDs can be specified, separated by a space. Range is 0 to 4294967294.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 2.0	This command was introduced.

## Usage Guidelines

This command clears bi-state alarms messages from the logging events buffer. Bi-state alarms are generated by state changes associated with system hardware, such as a change of interface state from active to inactive, or the online insertion and removal (OIR) of a Modular Service Card (MSC), or a change in component temperature.

Use the [show logging events buffer, on page 46](#) command to display messages in the logging events buffer.

## Task ID

Task ID	Operations
logging	execute

## Examples

This example shows how to reset all bi-alarms in the logging events buffer:

```
RP/0/RP0/CPU0:router# clear logging events reset all-in-buffer
```

## Related Commands

Command	Description
<a href="#">clear logging events delete, on page 7</a>	Deletes all bi-state alarm messages, or messages specified by correlation ID, from the logging events buffer.
<a href="#">show logging events buffer, on page 46</a>	Displays messages in the logging events buffer.

# context-correlation

To enable context-specific correlation, use the **context-correlation** command in either stateful or nonstateful correlation rule configuration mode. To disable correlation on context, use the **no** form of this command.

**context-correlation**  
**no context-correlation**

**Syntax Description** This command has no keywords or arguments.

**Command Default** Correlation on context is not enabled.

**Command Modes** Stateful correlation rule configuration  
 Nonstateful correlation rule configuration

Command History	Release	Modification
	Release 3.6.0	This command was introduced.

**Usage Guidelines** This command enables context-specific correlation for each of the contexts in which a given rule is applied. For example, if the rule is applied to two contexts (context1 and context2), messages that have context “context1” are correlated separately from those messages with context “context2”.

Use the [show logging correlator rule, on page 41](#) command to show the current setting for the context-correlation flag.

Task ID	Task ID	Operations
	logging	read, write

**Examples** This example shows how to enable correlation on context for a stateful correlation rule:

```
RP/0/RP0/CPU0:router(config)# logging correlator rule stateful_rule type stateful
RP/0/RP0/CPU0:router(config-corr-rule-st)# context-correlation
```

Related Commands	Command	Description
	<a href="#">logging correlator rule, on page 18</a>	Defines the rules for correlating messages.
	<a href="#">show logging correlator rule, on page 41</a>	Displays one or more predefined logging correlator rules.

# logging correlator apply rule

To apply and activate a correlation rule and enter correlation apply rule configuration mode, use the **logging correlator apply rule** command in Global Configuration mode. To deactivate a correlation rule, use the **no** form of this command.

```
logging correlator apply rule correlation-rule [{all-of-router|context name|location node-id}]
no logging correlator apply rule correlation-rule [{all-of-router|context name|location node-id}]
```

## Syntax Description

<i>correlation-rule</i>	Name of the correlation rule to be applied.
<b>all-of-router</b>	(Optional) Applies the correlation rule to the entire router.
<b>context name</b>	(Optional) Applies the correlation rule to the specified context. Unlimited number of contexts. The <i>name</i> string is limited to 32 characters.
<b>location node-id</b>	(Optional) Applies the correlation rule to the specified node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation. Unlimited number of locations.

## Command Default

No correlation rules are applied.

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.6.0	This command was introduced.

## Usage Guidelines

The **logging correlator apply rule** command is used to either add or remove apply settings for a given rule. These settings then determine which messages are correlated for the affected rules.

If the rule is applied to **all-of-router**, then correlation occurs for only those messages that match the configured cause values for the rule to be correlated, regardless of the context or location setting of that message.

If a rule is applied to a specific set of contexts or locations, then correlation occurs for only those messages that match both the configured cause values for the rule and at least one of those contexts or locations.

Use the [show logging correlator rule, on page 41](#) command to show the current apply settings for a given rule.



### Tip

When a rule is applied (or if a rule set that contains this rule is applied), then the rule definition cannot be modified through the configuration until the rule or rule set is once again unapplied.



### Tip

It is possible to configure apply settings at the same time for both a rule and zero or more rule sets that contain the rule. In this case, the apply settings for the rule are the union of all the apply configurations.

The **logging correlator apply rule** command allows you to enter submode (config-corr-apply-rule) to apply and activate rules:

```
RP/0/RP0/CPU0:router(config)# logging correlator apply rule statefull
RP/0/RP0/CPU0:router(config-corr-apply-rule)#?

all-of-router  Apply the rule to all of the router
clear          Clear the uncommitted configuration
clear         Clear the configuration
commit        Commit the configuration changes to running
context       Apply rule to specified context
describe      Describe a command without taking real actions
do           Run an exec command
exit         Exit from this submode
location      Apply rule to specified location
no           Negate a command or set its defaults
pwd          Commands used to reach current submode
root         Exit to the global configuration mode
show         Show contents of configuration
RP/0/RP0/CPU0:router(config-corr-apply-rule)#
```

While in the submode, you can negate keyword options:

```
RP/0/RP0/CPU0:router(config-corr-apply-rule)# no all-of-router
RP/0/RP0/CPU0:router(config-corr-apply-rule)# no context
RP/0/RP0/CPU0:router(config-corr-apply-rule)# no location
```

#### Task ID

Task ID	Operations
logging	read, write

#### Examples

This example shows how to apply a predefined correlator rule to a location:

```
RP/0/RP0/CPU0:router(config)# logging correlator apply rule rule1
RP/0/RP0/CPU0:router(config-corr-apply-rule)# location 0/2/CPU0
```

#### Related Commands

Command	Description
<a href="#">logging correlator rule, on page 18</a>	Defines the rules for correlating messages.
<a href="#">show logging correlator rule, on page 41</a>	Displays one or more predefined logging correlator rules.
<a href="#">show logging correlator ruleset, on page 44</a>	Displays one or more predefined logging correlator rule sets.

# logging correlator apply ruleset

To apply and activate a correlation rule set and enter correlation apply rule set configuration mode, use the **logging correlator apply ruleset** command in Global Configuration mode. To deactivate a correlation rule set, use the **no** form of this command.

```
logging correlator apply ruleset correlation-ruleset [{all-of-router|context name|location node-id}]
no logging correlator apply ruleset correlation-ruleset [{all-of-router|context name|location
node-id}]
```

## Syntax Description

<i>correlation-ruleset</i>	Name of the correlation rule set to be applied.
<b>all-of-router</b>	(Optional) Applies the correlation rule set to the entire router.
<b>context name</b>	(Optional) Applies the correlation rule set to the specified context. Unlimited number of contexts. The <i>name</i> string is limited to 32 characters.
<b>location node-id</b>	(Optional) Applies the correlation rule to the specified node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation. Unlimited number of locations.

## Command Default

No correlation rule sets are applied.

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.6.0	This command was introduced.

## Usage Guidelines

The **logging correlator apply ruleset** command is used to either add or remove apply settings for a given rule set. These settings then determine which messages are correlated for the affected rules.

If the rule set is applied to **all-of-router**, then correlation occurs for only those messages that match the configured cause values for the rule to be correlated, regardless of the context or location setting of that message.

If a rule set is applied to a specific set of contexts or locations, then correlation occurs for only those messages that match both the configured cause values for the rule and at least one of those contexts or locations.

Use the [show logging correlator ruleset, on page 44](#) command to show the current apply settings for a given rule set.



**Tip** When a rule is applied (or if a rule set that contains this rule is applied), then the rule definition cannot be modified through the configuration until the rule or rule set is once again unapplied.



**Tip** It is possible to configure apply settings at the same time for both a rule and zero or more rule sets that contain the rule. In this case, the apply settings for the rule are the union of all the apply configurations.

The **logging correlator apply ruleset** command allows you to enter the submode (config-corr-apply-ruleset) to apply and activate rule sets:

```
RP/0/RP0/CPU0:router(config)# logging correlator apply ruleset ruleset1
RP/0/RP0/CPU0:router(config-corr-apply-ruleset)#?
  all-of-router  Apply the rule to all of the router
  clear         Clear the uncommitted configuration
  clear         Clear the configuration
  commit        Commit the configuration changes to running
  context       Apply rule to specified context
  describe      Describe a command without taking real actions
  do            Run an exec command
  exit          Exit from this submode
  location      Apply rule to specified location
  no            Negate a command or set its defaults
  pwd           Commands used to reach current submode
  root          Exit to the global configuration mode
  show          Show contents of configuration
RP/0/RP0/CPU0:router(config-corr-apply-ruleset)#
```

While in the submode, you can negate keyword options:

```
RP/0/RP0/CPU0:router(config-corr-apply-ruleset)# no all-of-router
RP/0/RP0/CPU0:router(config-corr-apply-ruleset)# no context
RP/0/RP0/CPU0:router(config-corr-apply-ruleset)# no location
```

Task ID	Task ID	Operations
	logging	read, write

### Examples

This example shows how to apply a predefined correlator rule set to the entire router:

```
RP/0/RP0/CPU0:router(config)# logging correlator apply ruleset ruleset1
RP/0/RP0/CPU0:router(config-corr-apply-rule)# all-of-router
```

### Related Commands

Command	Description
<a href="#">show logging correlator ruleset, on page 44</a>	Displays one or more predefined logging correlator rule sets.



# logging correlator buffer-size

To configure the logging correlator buffer size, use the **logging correlator buffer-size** command in Global Configuration mode. To return the buffer size to its default setting, use the **no** form of this command.

**logging correlator buffer-size** *bytes*  
**no logging correlator buffer-size** *bytes*

<b>Syntax Description</b>	<i>bytes</i> The size, in bytes, of the logging correlator buffer. Range is 1024 to 52428800 bytes.
---------------------------	---

<b>Command Default</b>	<i>bytes</i> : 81920 bytes
------------------------	----------------------------

<b>Command Modes</b>	Global Configuration mode
----------------------	---------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 2.0	This command was introduced.

**Usage Guidelines** The **logging correlator buffer-size** command configures the size of the correlation buffer. This buffer holds all the correlation records as well as the associated correlated messages. When the size of this buffer is exceeded, older correlations in the buffer are replaced with the newer incoming correlations. The criteria that are used to recycle these buffers are:

- First, remove the oldest nonstateful correlation records from the buffer.
- Then, if there are no more nonstateful correlations present; remove the oldest stateful correlation records.

Use the [show logging correlator info, on page 40](#) command to confirm the size of the buffer and the percentage of buffer space that is currently used. The [show logging events buffer, on page 46](#) **all-in-buffer** command can be used to show the details of the buffer contents.

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	logging	read, write

**Examples** This example shows how to set the logging correlator buffer size to 90000 bytes:

```
RP/0/RP0/CPU0:router(config)# logging correlator buffer-size 90000
```

Related Commands	Command	Description
	<a href="#">show logging correlator info, on page 40</a>	Displays the logging correlator buffer size and the percentage of the buffer occupied by correlated messages.

# logging correlator rule

To define the rules for correlating messages, use the **logging correlator rule** command in Global Configuration mode. To delete the correlation rule, use the **no** form of this command.

```
logging correlator rule correlation-rule type {stateful|nonstateful}
no logging correlator rule correlation-rule
```

## Syntax Description

<i>correlation-rule</i>	Name of the correlation rule to be applied.
<b>type</b>	Specifies the type of rule.
<b>stateful</b>	Enters stateful correlation rule configuration mode.
<b>nonstateful</b>	Enters nonstateful correlation rule configuration mode.

## Command Default

No rules are defined.

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 3.6.0	This command was introduced.

## Usage Guidelines

The **logging correlator rule** command defines the correlation rules used by the correlator to store messages in the logging correlator buffer. A rule must, at a minimum, consist of three elements: a root-cause message, one or more non-root-cause messages, and a timeout.

When the root-cause message, or a non-root-cause message is received, the timer is started. Any non-root-cause messages are temporarily held, while the root-cause is sent to syslog. If, after the timer has expired, the root-cause and at least one non-root-cause message was received, a correlation is created and stored in the correlation buffer.

A rule can be of type stateful or nonstateful. Stateful rules allow non-root-cause messages to be sent from the correlation buffer if the bi-state root-cause alarm clears at a later time. Nonstateful rules result in correlations that are fixed and immutable after the correlation occurs.

Below are the rule parameters that are available while in stateful correlation rule configuration mode:

```
RP/0/RP0/CPU0:router(config-corr-rule-st)# ?
context-correlation Specify enable correlation on context
nonrootcause        nonrootcause alarm
reissue-nonbistate  Specify reissue of non-bistate alarms on parent clear
reparent            Specify reparent of alarm on parent clear
rootcause           Specify root cause alarm: Category/Group/Code combos
timeout             Specify timeout
timeout-rootcause   Specify timeout for root-cause
```

```
RP/0/RP0/CPU0:router(config-corr-rule-st)#
```

Below are the rule parameters that are available while in nonstateful correlation rule configuration mode:

```
RP/0/RP0/CPU0:router(config-corr-rule-nonst)# ?
context-correlation Specify enable correlation on context
nonrootcause        nonrootcause alarm
rootcause           Specify root cause alarm: Category/Group/Code combos
timeout             Specify timeout
timeout-rootcause   Specify timeout for root-cause
RP/0/RP0/CPU0:router(config-corr-rule-nonst)#
```



**Note** A rule cannot be deleted or modified while it is applied, so the **no logging correlator apply** command must be used to unapply the rule before it can be changed.



**Note** The name of the correlation rule must be unique across all rule types and is limited to a maximum length of 32 characters.

Use the [show logging correlator buffer, on page 38](#) to display messages stored in the logging correlator buffer.

Use the [show logging correlator rule, on page 41](#) command to verify correlation rule settings.

#### Task ID

#### Task Operations

logging read,  
write

#### Examples

This example shows how to enter stateful correlation rule configuration mode to specify a collection duration period time for correlator messages sent to the logging events buffer:

```
RP/0/RP0/CPU0:router(config)# logging correlator rule state_rule type stateful
RP/0/RP0/CPU0:router(config-corr-rule-st)# timeout 50000
```

#### Related Commands

Command	Description
<a href="#">logging correlator apply rule, on page 13</a>	Applies and activates correlation rules.
<a href="#">nonrootcause, on page 31</a>	Enters non-root-cause configuration mode and specifies a non-root-cause alarm.
<a href="#">reissue-nonbistate, on page 33</a>	Reissues non-bistate alarm messages (events) from the correlator log after its root-cause alarm clears.
<a href="#">reparent, on page 34</a>	Reparents non-root-cause messages to the next highest active root-cause in a hierarchical correlation when their immediate parent clears.
<a href="#">rootcause, on page 36</a>	Specifies a root-cause message alarm.

Command	Description
<a href="#">show logging correlator buffer, on page 38</a>	Displays messages in the logging correlator buffer.
<a href="#">show logging correlator rule, on page 41</a>	Displays one or more predefined logging correlator rules.
<a href="#">timeout, on page 59</a>	Specifies the collection period duration time for the logging correlator rule message.
<a href="#">timeout-rootcause, on page 61</a>	Specifies an optional parameter for an applied correlation rule.

# logging correlator ruleset

To enter correlation rule set configuration mode and define a correlation rule set, use the **logging correlator ruleset** command in Global Configuration mode. To delete the correlation rule set, use the **no** form of this command.

**logging correlator ruleset** *correlation-ruleset* **rulename** *correlation-rulename*  
**no logging correlator ruleset** *correlation-ruleset*

Syntax Description	
	<i>correlation-ruleset</i> Name of the correlation rule set to be applied.
	<b>rulename</b> Specifies the correlation rule name.
	<i>correlation-rulename</i> Name of the correlation rule name to be applied.

**Command Default** No rule sets are defined.

**Command Modes** Global Configuration mode

Command History	Release	Modification
	Release 3.6.0	This command was introduced.

**Usage Guidelines** The **logging correlator ruleset** command defines a specific correlation rule set. A rule set name must be unique and is limited to a maximum length of 32 characters.

To apply a logging correlator rule set, use the [logging correlator apply ruleset, on page 15](#) command.

## Examples

This example shows how to specify a logging correlator rule set:

```
RP/0/RP0/CPU0:router(config)# logging correlator ruleset ruleset_1
RP/0/RP0/CPU0:router(config-corr-ruleset)# rulename state_rule
RP/0/RP0/CPU0:router(config-corr-ruleset)# rulename state_rule2
```

Related Commands	Command	Description
	<a href="#">logging correlator apply ruleset, on page 15</a>	Applies and activates a correlation rule set and enters correlation apply rule set configuration mode.
	<a href="#">show logging correlator buffer, on page 38</a>	Displays messages in the logging correlator buffer.
	<a href="#">show logging correlator ruleset, on page 44</a>	Displays defined correlation rule set names.

# logging events buffer-size

To configure the size of the logging events buffer, use the **logging events buffer-size** command in Global Configuration mode. To restore the buffer size to the default value, use the **no** form of this command.

**logging events buffer-size** *bytes*  
**no logging events buffer-size** *bytes*

<b>Syntax Description</b>	<i>bytes</i> The size, in bytes, of the logging events buffer. Range is 1024 to 1024000 bytes. The default is 43200 bytes.
---------------------------	--

<b>Command Default</b>	<i>bytes</i> : 43200
------------------------	----------------------

<b>Command Modes</b>	Global Configuration mode
----------------------	---------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 2.0	This command was introduced.

## Usage Guidelines



**Note** The logging events buffer automatically adjusts to a multiple of the record size that is lower than or equal to the value configured for the *bytes* argument.

Use the [show logging events info, on page 50](#) command to confirm the size of the logging events buffer.

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	logging read, write	

## Examples

This example shows how to increase the logging events buffer size to 50000 bytes:

```
RP/0/RP0/CPU0:router(config)# logging events buffer-size 50000
```

## Related Commands

Command	Description
<a href="#">logging events level, on page 26</a>	Specifies a severity level for logging alarm messages.
<a href="#">logging events threshold, on page 28</a>	Specifies the event logging buffer capacity threshold that, when surpassed, will generate an alarm.
<a href="#">show logging correlator info, on page 40</a>	Displays information about the size of the logging correlator buffer and available capacity.

Command	Description
<a href="#">show logging events buffer, on page 46</a>	Displays messages in the logging events buffer.
<a href="#">show logging events info, on page 50</a>	Displays configuration and operational messages about the logging events buffer.

# logging events display-location

To enable the alarm source location display field for bistate alarms in the output of the **show logging** and **show logging events buffer** command, use the **logging events display-location** command in Global Configuration mode.

**logging events display-location**  
**no logging events display-location**

<b>Syntax Description</b>	This command has no keywords or arguments.				
<b>Command Default</b>	The alarm source location display field in <b>show logging</b> output is not enabled.				
<b>Command Modes</b>	Global Configuration mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Release 3.8.0</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Release 3.8.0	This command was introduced.
Release	Modification				
Release 3.8.0	This command was introduced.				

**Usage Guidelines**

The output of the **show logging** command for bistate alarms has been enhanced. Previously, the alarm source field in the output displayed the location of the process that logged the alarm. Use the **logging events display-location** command to configure the output of the **show logging** command to include an additional source field that displays the actual source of the alarm. The alarm source is displayed in a format that is consistent with alarm source identification in other platforms and equipment. The new alarm source display field aids accurate identification and isolation of the source of a fault.

By default, the output of the **show logging** command does not include the new alarm source identification field. If you enable the alarm source location display field in the **show logging** output, the same naming conventions are also used to display hardware locations in the **show diag** and **show inventory** command output.



**Note** Customer OSS tools may rely on the default output to parse and interpret the alarm output.

Task ID	Task	Operations
	logging	read, write

## Examples

This example shows the **show logging** command output for bistate alarms before and after enabling the alarm source location display field:

```
RP/0/RP0/CPU0:router# show logging | inc Interface

Wed Aug 13 01:30:58.461 UTC
LC/0/2/CPU0:Aug 12 01:20:54.073 : ifmgr[159]: %PKT_INFRA-LINK-5-CHANGED : Interface
```



```

GigabitEthernet0/2/0/0, changed state to Administratively Down
LC/0/2/CPU0:Aug 12 01:20:59.450 : ifmgr[159]: %PKT_INFRA-LINK-3-UPDOWN : Interface
GigabitEthernet0/2/0/0, changed state to Down
LC/0/2/CPU0:Aug 12 01:20:59.451 : ifmgr[159]: %PKT_INFRA-LINEPROTO-5-UPDOWN : Line protocol
  on Interface GigabitEthernet0/2/0/0, changed state to Down
RP/0/5/CPU0:Aug 12 01:22:11.496 : ifmgr[202]: %PKT_INFRA-LINK-5-CHANGED : Interface
MgmtEth0/5/CPU0/0, changed state to Administratively Down
RP/0/5/CPU0:Aug 12 01:23:23.842 : ifmgr[202]: %PKT_INFRA-LINK-3-UPDOWN : Interface
MgmtEth0/5/CPU0/0, changed state to Down
RP/0/5/CPU0:Aug 12 01:23:23.843 : ifmgr[202]: %PKT_INFRA-LINEPROTO-5-UPDOWN : Line protocol
  on Interface MgmtEth0/5/CPU0/0, changed state to Down
RP/0/5/CPU0:Aug 12 01:23:23.850 : ifmgr[202]: %PKT_INFRA-LINK-3-UPDOWN : Interface
MgmtEth0/5/CPU0/0, changed state to Up
RP/0/5/CPU0:Aug 12 01:23:23.856 : ifmgr[202]: %PKT_INFRA-LINEPROTO-5-UPDOWN : Line protocol
  on Interface MgmtEth0/5/CPU0/0, changed state to Up

RP/0/RP0/CPU0:router# config
Wed Aug 13 01:31:32.517 UTC

RP/0/RP0/CPU0:router(config)# logging events display-location

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

RP/0/RP0/CPU0:router(config)# exit

RP/0/RP0/CPU0:router# show logging | inc Interface

Wed Aug 13 01:31:48.141 UTC
LC/0/2/CPU0:Aug 12 01:20:54.073 : ifmgr[159]: %PKT_INFRA-LINK-5-CHANGED : Interface
GigabitEthernet0/2/0/0, changed state to Administratively Down
LC/0/2/CPU0:Aug 12 01:20:59.450 : ifmgr[159]: %PKT_INFRA-LINK-3-UPDOWN : interface
GigabitEthernet0/2/0/0: Interface GigabitEthernet0/2/0/0, changed state to Down
LC/0/2/CPU0:Aug 12 01:20:59.451 : ifmgr[159]: %PKT_INFRA-LINEPROTO-5-UPDOWN : interface
GigabitEthernet0/2/0/0: Line protocol on Interface GigabitEthernet0/2/0/0, changed state
to Down
RP/0/5/CPU0:Aug 12 01:22:11.496 : ifmgr[202]: %PKT_INFRA-LINK-5-CHANGED : Interface
MgmtEth0/5/CPU0/0, changed state to Administratively Down
RP/0/5/CPU0:Aug 12 01:23:23.842 : ifmgr[202]: %PKT_INFRA-LINK-3-UPDOWN : interface
MgmtEth0/5/CPU0/0: Interface MgmtEth0/5/CPU0/0, changed state to Down
RP/0/5/CPU0:Aug 12 01:23:23.843 : ifmgr[202]: %PKT_INFRA-LINEPROTO-5-UPDOWN : interface
MgmtEth0/5/CPU0/0: Line protocol on Interface MgmtEth0/5/CPU0/0, changed state to Down
RP/0/5/CPU0:Aug 12 01:23:23.850 : ifmgr[202]: %PKT_INFRA-LINK-3-UPDOWN : interface
MgmtEth0/5/CPU0/0: Interface MgmtEth0/5/CPU0/0, changed state to Up
RP/0/5/CPU0:Aug 12 01:23:23.856 : ifmgr[202]: %PKT_INFRA-LINEPROTO-5-UPDOWN : interface
MgmtEth0/5/CPU0/0: Line protocol on Interface MgmtEth0/5/CPU0/0, changed state to Up

```

**Related Commands**

Command	Description
<a href="#">show logging events buffer, on page 46</a>	Displays messages in the logging events buffer.

# logging events level

To specify a severity level for logging alarm messages, use the **logging events level** command in Global Configuration mode. To return to the default value, use the **no** form of this command.

**logging events level** *severity*  
**no logging events level**

## Syntax Description

*severity* Severity level of events to be logged in the logging events buffer, including events of a higher severity level (numerically lower). [Table 1: Alarm Severity Levels for Event Logging, on page 26](#) lists severity levels and their respective system conditions.

## Command Default

All severity levels (from 0 to 6) are logged.

## Command Modes

Global Configuration mode

## Command History

Release	Modification
Release 2.0	This command was introduced.

## Usage Guidelines

This command specifies the event severity necessary for alarm messages to be logged. Severity levels can be specified by the severity level description (for example, **warnings**). When a severity level is specified, events of equal or lower severity level are also written to the logging events buffer.



**Note** Events of lower severity level represent events of higher importance.

This table lists the system severity levels and their corresponding numeric values, and describes the corresponding system condition.

**Table 1: Alarm Severity Levels for Event Logging**

Severity Level Keyword	Numeric Value	Logged System Messages
emergencies	0	System is unusable.
alerts	1	Critical system condition exists requiring immediate action.
critical	2	Critical system condition exists.
errors	3	Noncritical errors.
warnings	4	Warning conditions.
notifications	5	Notifications of changes to system configuration.
informational	6	Information about changes to system state.

Task ID	Task ID	Operations
	logging	read, write

**Examples**

This example shows how to set the severity level for notification to warnings (level 4):

```
RP/0/RP0/CPU0:router(config)# logging events level warnings
```

**Related Commands**

Command	Description
<a href="#">logging events buffer-size, on page 22</a>	Specifies the logging events buffer size.
<a href="#">logging events threshold, on page 28</a>	Specifies the logging events buffer capacity threshold that, when surpassed, will generate an alarm.

# logging events threshold

To specify the logging events buffer threshold that, when surpassed, generates an alarm, use the **logging events threshold** command in Global Configuration mode. To return to the default value, use the **no** form of this command.

**logging events threshold** *percent*  
**no logging events threshold**

<b>Syntax Description</b>	<i>percent</i> Minimum percentage of buffer capacity that must be allocated to messages before an alarm is generated. Range is 10 to 100. The default is 80 percent.
---------------------------	--

<b>Command Default</b>	<i>percent</i> : 80 percent
------------------------	-----------------------------

<b>Command Modes</b>	Global Configuration mode
----------------------	---------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 2.0	This command was introduced.

<b>Usage Guidelines</b>	This command can be configured to generate an alarm when 10 percent or more of the event buffer capacity is available.
-------------------------	--

The logging events buffer is circular; that is, when full it overwrites the oldest messages in the buffer. Once the logging events buffer reaches full capacity, the next threshold alarm is generated when the number of overwritten events surpasses the percentage of buffer capacity allocated to messages.

Use the [show logging events info, on page 50](#) command to display the current threshold setting.

<b>Task ID</b>	<b>Task</b>	<b>Operations</b>
	logging	read, write

<b>Examples</b>	This example shows how to configure the threshold setting to 95 percent of buffer capacity:
-----------------	---

```
RP/0/RP0/CPU0:router (config) # logging events threshold 95
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">logging events buffer-size, on page 22</a>	Specifies the logging correlator buffer size.
	<a href="#">logging events level, on page 26</a>	Specifies a severity level for logging alarm messages.
	<a href="#">show logging events info, on page 50</a>	Displays configuration and operational messages about the logging events buffer.

# logging suppress apply rule

To apply and activate a logging suppression rule, use the **logging suppress apply rule** command in Global Configuration mode. To deactivate a logging suppression rule, use the **no** form of this command.

```
logging suppress apply rule rule-name [{all-of-router|source location node-id}]
no logging suppress apply rule rule-name [{all-of-router|source location node-id}]
```

Syntax Description		
	<i>rule-name</i>	Name of the logging suppression rule to activate.
	<b>all-of-router</b>	(Optional) Applies the specified logging suppression rule to alarms originating from all locations on the router.
	<b>source location</b> <i>node-id</i>	(Optional) Applies the specified logging suppression rule to alarms originating from the specified node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.

**Command Default** No logging suppression rules are applied.

**Command Modes** Global Configuration mode

Command History	Release	Modification
	Release 3.8.0	This command was introduced.

**Usage Guidelines** No specific guidelines impact the use of this command.

Task ID	Task ID	Operations
	logging read, write	

**Examples** This example shows how to apply a predefined logging suppression rule to the entire router:

```
RP/0/RP0/CPU0:router(config)#logging suppress apply rule infobistate
RP/0/RP0/CPU0:router(config-suppr-apply-rule)# all-of-router
```

Related Commands	Command	Description
	<a href="#">all-of-router, on page 5</a>	Applies a logging suppression rule to suppress alarms originating from all sources on the router.
	<a href="#">source, on page 58</a>	Applies a logging suppression rule to alarms originating from a specific node on the router.

# logging suppress rule

To create a logging suppression rule and enter the configuration mode for the rule, use the **logging suppress rule** command in the Global Configuration mode. To remove a logging suppression rule, use the **no** form of this command.

```
logging suppress rule rule-name [{alarm msg-category group-name msg-code|all-alarms}]
no logging suppress rule rule-name
```

Syntax Description	
<i>rule-name</i>	Name of the rule.
<b>alarm</b>	(Optional) Specifies a type of alarm to be suppressed by the logging suppression rule.
<i>msg-category</i>	Message category of the root message.
<i>group-name</i>	Group name of the root message.
<i>msg-code</i>	Message code of the root message.
<b>all-alarms</b>	(Optional) Specifies that the logging suppression rule suppresses all types of alarms.

**Command Default** No logging suppression rules exist by default.

**Command Modes** Global Configuration mode

Command History	Release	Modification
	Release 3.8.0	This command was introduced.

**Usage Guidelines** If you use the **logging suppress rule** command without specifying a non-root-cause alarm, you can do so afterwards, by entering the **alarm** keyword at the prompt.

Task ID	Task	Operations
	logging	read, write

**Examples** This example shows how to create a logging suppression rule called infobistate:

```
RP/0/RP0/CPU0:router (config) # logging suppress rule infobistate
RP/0/RP0/CPU0:router (config-suppr-rule) #
```

Related Commands	Command	Description
	<a href="#">alarm, on page 3</a>	Specifies a type of alarm to be suppressed by a logging suppression rule.
	<a href="#">all-alarms, on page 4</a>	Configures a logging suppression rule to suppress all types of alarms.

## nonrootcause

To enter the non-root-cause configuration mode and specify a non-root-cause alarm, use the **nonrootcause** command in stateful or nonstateful correlation rule configuration modes.

```
nonrootcause alarm msg-category group-name msg-code
no nonrootcause
```

Syntax Description	alarm	Non-root-cause alarm.
	<i>msg-category</i>	(Optional) Message category assigned to the message. Unlimited messages (identified by message category, group, and code) can be specified, separated by a space.
	<i>group-name</i>	(Optional) Message group assigned to the message. Unlimited messages (identified by message category, group, and code) can be specified, separated by a space.
	<i>msg-code</i>	(Optional) Message code assigned to the message. Unlimited messages (identified by message category, group, and code) can be specified, separated by a space.

**Command Default** Non-root-cause configuration mode and alarm are not specified.

**Command Modes** Stateful correlation rule configuration  
Nonstateful correlation rule configuration

Command History	Release	Modification
	Release 3.6.0	This command was introduced.

**Usage Guidelines** This command is used to enter the non-root-cause configuration mode to configure one or more non-root-cause alarms associated with a particular correlation rule.

Use the [show logging events info, on page 50](#) command to display the current threshold setting.

If you use the **nonrootcause** command without specifying a non-root-cause alarm, you can do so afterwards, by entering the **alarm** keyword at the prompt.

Task ID	Task ID	Operations
	logging	read, write

### Examples

This example shows how to enter non-root-cause configuration mode and display the commands that are available under this mode:

```
RP/0/RP0/CPU0:router(config)# logging correlator rule state_rule type stateful
RP/0/RP0/CPU0:router(config-corr-rule-st)# nonrootcause
RP/0/RP0/CPU0:router(config-corr-rule-st-nonrc)# ?
```

```

alarm      Specify non-root cause alarm: Category/Group/Code combos
clear      Clear the uncommitted configuration
clear      Clear the configuration
commit     Commit the configuration changes to running
describe   Describe a command without taking real actions
do         Run an exec command
exit       Exit from this submode
no         Negate a command or set its defaults
pwd        Commands used to reach current submode
root       Exit to the global configuration mode
show       Show contents of configuration

```

This example shows how to specify a non-root-cause alarm for Layer 2 local SONET messages with an alarm severity of 4. The non-root-cause alarm is associated with the correlation rule named `state_rule`.

```
RP/0/RP0/CPU0:router(config-corr-rule-st-nonrc)# alarm L2 SONET_LOCAL ALARM
```

### Related Commands

Command	Description
<a href="#">logging events buffer-size, on page 22</a>	Specifies the logging correlator buffer size.
<a href="#">logging events level, on page 26</a>	Specifies a severity level for logging alarm messages.
<a href="#">logging events threshold, on page 28</a>	Specifies the logging events buffer capacity threshold that, when surpassed, will generate an alarm.
<a href="#">show logging events info, on page 50</a>	Displays configuration and operational messages about the logging events buffer.



## reissue-nonbistate

To reissue non-bistate alarm messages (events) from the correlator log after the root-cause alarm of a stateful rule clears, use the **reissue-nonbistate** command in stateful or nonstateful correlation rule configuration modes. To disable the reissue-nonbistate flag, use the **no** form of this command.

```
reissue-nonbistate
no reissue-nonbistate
```

<b>Syntax Description</b>	This command has no keywords or arguments.				
<b>Command Default</b>	Non-bistate alarm messages are not reissued after their root-cause alarm clears.				
<b>Command Modes</b>	Stateful correlation rule configuration Nonstateful correlation rule configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Release 3.6.0</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Release 3.6.0	This command was introduced.
Release	Modification				
Release 3.6.0	This command was introduced.				

**Usage Guidelines** By default, when the root-cause alarm of a stateful correlation is cleared, any non-root-cause, bistate messages being held for that correlation are silently deleted and are not sent to syslog. If the non-bistate messages should be sent, use the **reissue-nonbistate** command for the rules where this behavior is required.

Task ID	Task ID	Operations
	logging	read, write

**Examples** This example shows how to reissue nonbistate alarm messages:

```
RP/0/RP0/CPU0:router(config)# logging correlator rule state_rule type stateful
RP/0/RP0/CPU0:router(config-corr-rule-st)# reissue-nonbistate
```

Related Commands	Command	Description
	<a href="#">show logging correlator buffer, on page 38</a>	Displays messages in the logging correlator buffer.
	<a href="#">show logging events buffer, on page 46</a>	Displays messages in the logging events buffer.

# reparent

To reparent non-root-cause messages to the next highest active rootcause in a hierarchical correlation when their immediate parent clears, use the **reparent** command in stateful correlation rule configuration mode. To disable the reparent flag, use the **no** form of this command.

**reparent**  
**no reparent**

**Syntax Description** This command has no keywords or arguments.

**Command Default** A non-root-cause alarm is sent to syslog after a root-cause parent clears.

**Command Modes** Stateful correlation rule configuration

Command History	Release	Modification
	Release 3.6.0	This command was introduced.

**Usage Guidelines** Use the **reparent** command to specify what happens to non-root-cause alarms in a hierarchical correlation after their root-cause alarm clears. The following scenario illustrates why you may want to set the reparent flag.

Rule 1 with rootcause A and non-rootcause B

Rule 2 with rootcause B and non-rootcause C

(Alarm B is a non-rootcause for Rule 1 and a rootcause for Rule 2. For the purpose of this example, all the messages are bistate alarms.)

If both Rule 1 and Rule 2 each trigger a successful correlation, then a hierarchy is constructed that links these two correlations. When alarm B clears, alarm C would normally be sent to syslog, but the operator may choose to continue suppression of alarm C (hold it in the correlation buffer); because the rootcause that is higher in the hierarchy (alarm A) is still active.

The reparent flag allows you to specify non-root-cause behavior—if the flag is set, then alarm C becomes a child of rootcause alarm A; otherwise, alarm C is sent to syslog.



**Note** Stateful behavior, such as reparenting, is supported only for bistate alarms. Bistate alarms are associated with system hardware, such as a change of interface state from active to inactive.

Task ID	Task ID	Operations
	logging	read, write

**Examples** This example shows how to set the reparent flag for a stateful rule:

```
RP/0/RP0/CPU0:router(config)# logging correlator rule state_rule type stateful
RP/0/RP0/CPU0:router(config-corr-rule-st)# reparent
```

**Related Commands**

Command	Description
<a href="#">logging correlator rule, on page 18</a>	Defines the rules for correlating messages.
<a href="#">show logging correlator buffer, on page 38</a>	Displays messages in the logging correlator buffer.
<a href="#">show logging events info, on page 50</a>	Displays configuration and operational messages about the logging events buffer.

## rootcause

To specify the root-cause alarm message, use the **rootcause** command in stateful or nonstateful correlation rule configuration modes.

```
rootcause msg-category group-name msg-code
no rootcause
```

### Syntax Description

*msg-category* Message category of the root message.

*group-name* Group name of the root message.

*msg-code* Message code of the root message.

### Command Default

Root-cause alarm is not specified.

### Command Modes

Stateful correlation rule configuration

Nonstateful correlation rule configuration

### Command History

Release	Modification
Release 3.6.0	This command was introduced.

### Usage Guidelines

This command is used to configure the root-cause message for a particular correlation rule. Messages are identified by their message category, group, and code. The category, group, and code each can contain up to 32 characters. The root-cause message for a stateful correlation rule should be a bi-state alarm.

Use the [show logging events info, on page 50](#) command to display the root-cause and non-root-cause alarms for a correlation rule.

### Task ID

Task ID	Operations
logging	read, write

### Examples

This example shows how to configure a root-cause alarm for a stateful correlation rule:

```
RP/0/RP0/CPU0:router(config)# logging correlator rule state_rule type stateful
RP/0/RP0/CPU0:router(config-corr-rule-st)# rootcause L2 SONET_LOCAL ALARM
```

### Related Commands

Command	Description
<a href="#">logging events buffer-size, on page 22</a>	Specifies the logging correlator buffer size.
<a href="#">logging events level, on page 26</a>	Specifies a severity level for logging alarm messages.

Command	Description
<a href="#">logging events threshold, on page 28</a>	Specifies the logging events buffer capacity threshold that, when surpassed, will generate an alarm.
<a href="#">timeout-rootcause, on page 61</a>	Specifies an optional parameter for an applied correlation rule.
<a href="#">show logging events info, on page 50</a>	Displays configuration and operational messages about the logging events buffer.

# show logging correlator buffer

To display messages in the logging correlator buffer, use the **show logging correlator buffer** command in EXEC mode.

```
show logging correlator buffer {all-in-buffer [ruletype [{nonstateful|stateful}]}][rulesource
[{internal|user}]}][rule-name correlation-rule1 . . . correlation-rule14][correlationID correlation-id1
. . . correlation-id14}
```

Syntax Description	Parameter	Description
	<b>all-in-buffer</b>	Displays all messages in the correlation buffer.
	<b>ruletype</b>	(Optional) Displays the ruletype filter.
	<b>nonstateful</b>	(Optional) Displays the nonstateful rules.
	<b>stateful</b>	(Optional) Displays the stateful rules.
	<b>rulesource</b>	(Optional) Displays the rulesource filter.
	<b>internal</b>	(Optional) Displays the internally defined rules from the rulesource filter.
	<b>user</b>	(Optional) Displays the user-defined rules from the rulesource filter.
	<b>rule-name</b>	Displays a messages associated with a correlation rule name. Up to <i>correlation-rule1...correlation-rule14</i> 14 correlation rules can be specified, separated by a space.
	<b>correlationID</b>	Displays a message identified by correlation ID. Up to 14 correlation IDs can be specified, separated by a space. Range is 0 to 4294967294.

**Command Default** None

**Command Modes** EXEC mode

Command History	Release	Modification
	Release 2.0	This command was introduced.
	Release 3.2	The output was modified to include message category information.
	Release 3.6.0	The following keywords were added: <ul style="list-style-type: none"> <li>• <b>internal</b></li> <li>• <b>nonstateful</b></li> <li>• <b>rulesource</b></li> <li>• <b>ruletype</b></li> <li>• <b>stateful</b></li> <li>• <b>user</b></li> </ul>
		Range changed from 32 to 14 for <b>correlationID</b> and <b>rule-name</b> keywords.

**Usage Guidelines**

This command displays messages from the logging correlator buffer that match the correlation ID or correlation rule name specified. When the **all-in-buffer** keyword is entered, all messages in the logging correlator buffer are displayed.

If the ruletype is not specified, then both stateful and nonstateful rules are displayed.

if the rulesource is not specified, then both user and internal rules are displayed.

**Task ID****Task Operations ID**

logging read

**Examples**

This is the sample output from the **show logging correlator buffer** command:

```
RP/0/RP0/CPU0:router# show logging correlator buffer all-in-buffer

#C_id.id:Rule Name:Source :Context: Time : Text
#14.1 :Rule1:RP/0/5/CPU0: :Aug 22 13:39:13.693 2007:ifmgr[196]: %PKT_INFRA-LINK-3-UPDOWN :
  Interface MgmtEth0/5/CPU0/0, changed state to Down
#14.2 :Rule1:RP/0/5/CPU0: :Aug 22 13:39:13.693 2007:ifmgr[196]: %PKT_INFRA-LINEPROTO-3-UPDOWN
  : Line protocol on Interface MgmtEth0/5/CPU0/0, changed state to Down
```

This table describes the significant fields shown in the display.

**Table 2: show logging correlator buffer Field Descriptions**

Field	Description
C_id.	Correlation ID assigned to a event that matches a logging correlation rule.
id	An ID number assigned to each event matching a particular correlation rule. This event number serves as index to identify each individual event that has been matched for a logging correlation rule.
Rule Name	Name of the logging correlation rule that filters messages defined in a logging correlation rule to the logging correlator buffer.
Source	Node from which the event is generated.
Time	Date and time at which the event occurred.
Text	Message string that delineates the event.

**Related Commands**

Command	Description
<a href="#">show logging correlator info, on page 40</a>	Displays the logging correlator buffer size and the percentage of the buffer occupied by correlated messages.
<a href="#">show logging correlator rule, on page 41</a>	Displays one or more predefined logging correlator rules.

# show logging correlator info

To display the logging correlator buffer size and the percentage of the buffer occupied by correlated messages, use the **show correlator info** command in EXEC mode.

## show logging correlator info

**Syntax Description** This command has no keywords or arguments.

**Command Default** None

**Command Modes** EXEC mode

Command History	Release	Modification
	Release 2.0	This command was introduced.
	Release 3.2	The output was modified to include message category information.

**Usage Guidelines** This command displays the size of the logging correlator buffer and the percentage of the buffer allocated to correlated messages.

Use the [logging correlator buffer-size, on page 17](#) command to set the size of the buffer.

Task ID	Task ID	Operations
	logging	read

## Examples

In this example, the **show logging correlator info** command is used to display remaining buffer size and percentage allocated to correlated messages:

```
RP/0/RP0/CPU0:router# show logging correlator info

Buffer-Size      Percentage-Occupied
      81920                0.00
```

Related Commands	Command	Description
	<a href="#">logging correlator buffer-size, on page 17</a>	Specifies the logging correlator buffer size.
	<a href="#">show logging correlator buffer, on page 38</a>	Displays messages in the logging correlator buffer.
	<a href="#">show logging correlator rule, on page 41</a>	Displays one or more predefined logging correlator rules.



# show logging correlator rule

To display defined correlation rules, use the **show logging correlator rule** command in EXEC mode.

```
show logging correlator rule {all|correlation-rule1...correlation-rule14} [context
context1...context 6] [location node-id1...node-id6] [rulesource {internal|user}] [ruletype
{nonstateful|stateful}] [{summary|detail}]
```

Syntax	Description
<b>all</b>	Displays all rule sets.
<i>correlation-rule1...correlation-rule14</i>	Rule set name to be displayed. Up to 14 predefined correlation rules can be specified, separated by a space.
<b>context</b> <i>context1...context 6</i>	(Optional) Displays a list of context rules.
<b>location</b> <i>node-id1...node-id6</i>	(Optional) Displays the location of the list of rules filter from the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<b>rulesource</b>	(Optional) Displays the rulesource filter.
<b>internal</b>	(Optional) Displays the internally defined rules from the rulesource filter.
<b>user</b>	(Optional) Displays the user defined rules from the rulesource filter.
<b>ruletype</b>	(Optional) Displays the ruletype filter.
<b>nonstateful</b>	(Optional) Displays the nonstateful rules.
<b>stateful</b>	(Optional) Displays the stateful rules.
<b>summary</b>	(Optional) Displays the summary information.
<b>detail</b>	(Optional) Displays detailed information.

**Command Default** None

**Command Modes** EXEC mode

Command History	Release	Modification
	Release 2.0	This command was introduced.
	Release 3.2	The output was modified to include message category information.

Release	Modification
Release 3.6.0	The following keyword and argument pairs were added: <ul style="list-style-type: none"> <li>• <b>context</b> <i>context</i></li> <li>• <b>detail</b></li> <li>• <b>location</b> <i>node-id</i></li> <li>• <b>rulesource</b> { <i>internal</i>   <i>user</i> }</li> <li>• <b>ruletype</b> { <i>nonstateful</i>   <i>stateful</i> }</li> <li>• <b>summary</b></li> </ul>

**Usage Guidelines**

If the ruletype is not specified, then both stateful and nonstateful rules are displayed as the default.

If the rulesource is not specified, then both user and internally defined rules are displayed as the default.

If the summary or detail keywords are not specified, then detailed information is displayed as the default.

**Task ID**

Task ID	Task Operations
	logging read

**Examples**

This is sample output from the **show logging correlator rule** command:

```
RP/0/RP0/CPU0:router# show logging correlator rule test

Rule Name : test
Type : Non Stateful
Source : User
Timeout : 30000 Rule State: RULE_APPLIED_ALL
Rootcause Timeout : None
Context Correlation : disabled
Reissue Non Bistate : N/A
Reparent : N/A
Alarms :
Code Type: Category Group Message
Root: MGBL CONFIG DB_COMMIT
Leaf: L2 SONET ALARM
Apply Locations: None
Apply Contexts: None
Number of buffered alarms : 0
```

This table describes the significant fields shown in the display.

**Table 3: show logging correlator rule Field Descriptions**

Field	Description
Rule Name	Name of defined correlation rule.
Time out	Configured timeout for the correlation rule.
Rule State	Indicates whether or not the rule has been applied. If the rule applies to the entire router, this field will display “RULE_APPLIED_ALL.”

Field	Description
Code Type	Message category, group, and code.
Root	Message category, group and code of the root message configured in the logging correlation rule.
Leaf	Message category, group and code of a non-root-cause message configured in the logging correlation rule.
Apply Locations	Node or nodes where the rule is applied. If the logging correlation rule applies to the entire router, this field will display “None.”
Apply Contexts	Context or contexts to which the rule is applied. If the logging correlation rule is not configured to apply to a context, this field will display “None.”

**Related Commands**

Command	Description
<a href="#">logging correlator apply rule, on page 13</a>	Applies and activates correlation rules.
<a href="#">logging correlator rule, on page 18</a>	Defines the rules for correlating messages.
<a href="#">show logging correlator buffer, on page 38</a>	Displays messages in the logging correlator buffer.
<a href="#">show logging correlator info, on page 40</a>	Displays the logging correlator buffer size and the percentage of the buffer occupied by correlated messages

# show logging correlator ruleset

To display defined correlation rule set names, use the **show logging correlator ruleset** command in EXEC mode.

```
show logging correlator ruleset {all|correlation-ruleset1 . . . correlation-ruleset14}
[{detail|summary}]
```

Syntax Description	all	Displays all rule set names.
	<i>correlation-rule1</i> ... <i>correlation-rule14</i>	Rule set name to be displayed. Up to 14 predefined rule set names can be specified, separated by a space.
	<b>detail</b>	(Optional) Displays detailed information.
	<b>summary</b>	(Optional) Displays the summary information.

**Command Default** Detail is the default, if nothing is specified.

**Command Modes** EXEC mode

Command History	Release	Modification
	Release 3.6.0	This command was introduced.

**Usage Guidelines**

- If the ruletype is not specified, then both stateful and nonstateful rules are displayed as the default.
- If the rulesource is not specified, then both user and internally defined rules are displayed as the default.
- If the summary or detail options are not specified, then detailed information is displayed as the default.

Task ID	Task ID	Operations
	logging	read

## Examples

This is the sample output from the **show logging correlator ruleset** command:

```
RP/0/RP0/CPU0:router# show logging correlator RuleSetOne RuleSetTwo

Rule Set Name : RuleSetOne
Rules: Rule1 : Applied
Rule2 : Applied
Rule3 : Applied
Rule Set Name : RuleSetTwo
Rules: Rule1 : Applied
Rule5 : Not Applied
```

This is the sample output from the **show logging correlator ruleset** command when the **all** option is specified:

```
RP/0/RP0/CPU0:router# show logging correlator ruleset all
```

```
Rule Set Name : RuleSetOne
Rules: Rule1 : Applied
Rule2 : Applied
Rule3 : Applied
Rule Set Name : RuleSetTwo
Rules: Rule1 : Applied
Rule5 : Not Applied
Rule Set Name : RuleSetThree
Rules: Rule2 : Applied
Rule3 : Applied
```

This is sample output from the **show logging correlator ruleset** command when the **all** and **summary** options are specified:

```
RP/0/RP0/CPU0:router# show logging correlator ruleset all summary
RuleSetOne
RuleSetTwo
RuleSetThree
```

This table describes the significant fields shown in the display.

**Table 4: show logging correlator ruleset Field Descriptions**

Field	Description
Rule Set Name	Name of the ruleset.
Rules	All rules contained in the ruleset are listed.
Applied	The rule is applied.
Not Applied	The rule is not applied.

#### Related Commands

Command	Description
<a href="#">logging correlator apply rule, on page 13</a>	Applies and activates correlation rules.
<a href="#">logging correlator rule, on page 18</a>	Defines the rules for correlating messages.
<a href="#">show logging correlator buffer, on page 38</a>	Displays messages in the logging correlator buffer.
<a href="#">show logging correlator info, on page 40</a>	Displays the logging correlator buffer size and the percentage of the buffer occupied by correlated messages.
<a href="#">show logging correlator rule, on page 41</a>	Displays defined correlation rules.

## show logging events buffer

To display messages in the logging events buffer, use the **show logging events buffer** command in EXEC mode.

```
show logging events buffer [admin-level-only] [all-in-buffer] [bistate-alarms-set] [category name]
[context name] [event-hi-limit event-id] [event-lo-limit event-id] [first event-count] [group
message-group] [last event-count] [location node-id] [message message-code] [severity-hi-limit
severity] [severity-lo-limit severity] [timestamp-hi-limit hh:mm:ss [month] [day] [year]
timestamp-lo-limit hh:mm:ss [month] [day] [year]]
```

### Syntax Description

<b>admin-level-only</b>	Displays only the events that are at the administrative level.
<b>all-in-buffer</b>	Displays all event IDs in the events buffer.
<b>bistate-alarms-set</b>	Displays bi-state alarms in the SET state.
<b>category name</b>	Displays events from a specified category.
<b>context name</b>	Displays events from a specified context.
<b>event-hi-limit event-id</b>	Displays events with an event ID equal to or lower than the event ID specified with the <i>event-id</i> argument. Range is 0 to 4294967294.
<b>event-lo-limit event-id</b>	Displays events with an event ID equal to or higher than the event ID specified with <i>event-id</i> argument. Range is 0 to 4294967294.
<b>first event-count</b>	Displays events in the logging events buffer, beginning with the first event. For the <i>event-count</i> argument, enter the number of events to be displayed.
<b>group message-group</b>	Displays events from a specified message group.
<b>last event-count</b>	Displays events, beginning with the last event in the logging events buffer. For the <i>event-count</i> argument, enter the number of events to be displayed.
<b>location node-id</b>	Displays events for the specified location. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
<b>message message-code</b>	Displays events with the specified message code.
<b>severity-hi-limit</b>	Displays events with a severity level equal to or lower than the specified severity level.

---

<b>severity</b>	Severity level. Valid values are: <ul style="list-style-type: none"><li>• <b>emergencies</b></li><li>• <b>alerts</b></li><li>• <b>critical</b></li><li>• <b>errors</b></li><li>• <b>warnings</b></li><li>• <b>notifications</b></li><li>• <b>informational</b></li></ul> <p><b>Note</b> Settings for the severity levels and their respective system conditions are listed under the “Usage Guidelines” section for the <b>logging events level</b> command. Events of lower severity level represent events of higher importance.</p>
<b>severity-lo-limit</b>	Displays events with a severity level equal to or higher than the specified severity level.
<b>timestamp-hi-limit</b>	Displays events with a time stamp equal to or lower than the specified time stamp.

---

*hh : mm : ss [month] [day] [year]* Time stamp for the **timestamp-hi-limit** or **timestamp-lo-limit** keyword. The *month*, *day*, and *year* arguments default to the current month, day, and year if not specified.

Ranges for the *hh : mm : ss month day year* arguments are as follows:

- *hh* :—Hours. Range is 00 to 23. You must insert a colon after the *hh* argument.
- *mm* :—Minutes. Range is 00 to 59. You must insert a colon after the *mm* argument.
- *ss*—Seconds. Range is 00 to 59.
- *month*—(Optional) The month of the year. The values for the *month* argument are:
  - january
  - february
  - march
  - april
  - may
  - june
  - july
  - august
  - september
  - october
  - november
  - december
- *day*—(Optional) Day of the month. Range is 01 to 31.
- *year*—(Optional) Year. Enter the last two digits of the year (for example, **04** for 2004). Range is 01 to 37.

---

**timestamp-lo-limit** Displays events with a time stamp equal to or higher than the specified time stamp.

---



---

**Command Default** None

---

**Command Modes** EXEC mode

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 2.0	This command was introduced.
	Release 3.2	The output was modified to include message category information. The <b>admin-level-only</b> optional keyword was introduced.

---



**Usage Guidelines**

This command displays messages from the logging events buffer matching the description. The description is matched when all of the conditions are met.

**Task ID****Task Operations ID**

logging read

**Examples**

This is the sample output from the **show logging events buffer all-in-buffer** command:

```
RP/0/RP0/CPU0:router# show logging events buffer all-in-buffer
```

```
#ID      :C_id:Source      :Time                :%CATEGORY-GROUP-SEVERITY-MESSAGECODE: Text

#1       :      :RP/0/RP0/CPU0:Jan  9 08:57:54 2004:nvram[66]: %MEDIA-NVRAM_PLATFORM-3-BAD_N
VRAM_VAR : ROMMON variable-value pair: '^'[19~CONFIG_FILE = disk0:config/startup, contains
illegal (non-printable) characters
#2       :      :RP/0/RP0/CPU0:Jan  9 08:58:21 2004:psarb[238]: %PLATFORM-PSARB-5-GO_BID : Card
is going to bid state.
#3       :      :RP/0/RP0/CPU0:Jan  9 08:58:22 2004:psarb[238]: %PLATFORM-PSARB-5-GO_ACTIVE :
Card is becoming active.
#4       :      :RP/0/RP0/CPU0:Jan  9 08:58:22 2004:psarb[238]: %PLATFORM-PSARB-6-RESET_ALL_LC_
CARDS : RP going active; resetting all linecards in chassis
#5       :      :RP/0/RP0/CPU0:Jan  9 08:58:22 2004:redcon[245]: %HA-REDCON-6-GO_ACTIVE : this
card going active
#6       :      :RP/0/RP0/CPU0:Jan  9 08:58:22 2004:redcon[245]: %HA-REDCON-6-FAILOVER_ENABLED
: Failover has been enabled by config
```

This table describes the significant fields shown in the display.

**Table 5: show logging correlator buffer Field Descriptions**

Field	Description
#ID	Integer assigned to each event in the logging events buffer.
C_id.	Correlation ID assigned to a event that has matched a logging correlation rule.
Source	Node from which the event is generated.
Time	Date and time at which the event occurred.
%CATEGORY-GROUP-SEVERITY-MESSAGECODE	The category, group name, severity level, and message code associated with the event.
Text	Message string that delineates the event.

**Related Commands**

Command	Description
<a href="#">show logging events info, on page 50</a>	Displays configuration and operational messages about the logging events buffer.

# show logging events info

To display configuration and operational information about the logging events buffer, use the **show logging events info** command in EXEC mode.

## show logging events info

**Syntax Description** This command has no keywords or arguments.

**Command Default** None

**Command Modes** EXEC mode

**Command History**

Release	Modification
Release 2.0	This command was introduced.

**Usage Guidelines** This command displays information about the size of the logging events buffer, the maximum size of the buffer, the number of records being stored, the maximum allowable number of records threshold for circular filing, and message filtering.

**Task ID**

Task ID	Operations
logging	read

## Examples

This is the sample output from the **show logging events info** command:

```
RP/0/RP0/CPU0:router# show logging events info

Size (Current/Max)      #Records      Thresh      Filter
16960      /42400      37          90          Not Set
```

This table describes the significant fields shown in the display.

**Table 6: show logging events info Field Descriptions**

Field	Description
Size (Current/Max)	The current and maximum size of the logging events buffer. The maximum size of the buffer is controlled by the <a href="#">logging events buffer-size, on page 22</a> command.
#Records	The number of event records stored in the logging events buffer.
Thresh	The configured logging events threshold value. This field is controlled by the <a href="#">logging events threshold, on page 28</a> command.
Filter	The lowest severity level for events that will be displayed. This field is controlled by the <a href="#">logging events level, on page 26</a> command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">logging events buffer-size, on page 22</a>	Specifies the logging correlator buffer size.
<a href="#">logging events level, on page 26</a>	Specifies a severity level for logging alarm messages.
<a href="#">logging events threshold, on page 28</a>	Specifies the logging events buffer capacity threshold that, when surpassed, will generate an alarm.
<a href="#">show logging events buffer, on page 46</a>	Displays information about messages in the logging events buffer according to type, time, or severity level.

# show logging suppress rule

To display defined logging suppression rules, use the **show logging suppression rule** command in EXEC mode.

**show logging suppress rule** [{*rule-name1* [...] [*rule-name14*]}] **all** [**detail**] [**summary**] [**source location** *node-id*]

## Syntax Description

*rule-name1* [...] [*rule-name14*] Specifies up to 14 logging suppression rules to display.

**all** Displays all logging suppression rules.

**source location** *node-id* (Optional) Displays the location of the list of rules filter from the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.

**detail** (Optional) Displays detailed information.

**summary** (Optional) Displays the summary information.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.8.0	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operations
logging	read

## Examples

This example displays information about a logging suppression rule that has been configured but has not been activated:

```
RP/0/RP0/CPU0:router# show logging suppression rule test_suppression

Rule Name : test_suppression
Rule State: RULE_UNAPPLIED
Severities : informational, critical
Alarms :
  Category      Group           Message
  CAT_C         GROUP_C        CODE_C
  CAT_D         GROUP_D        CODE_D

Apply Alarm-Locations: PLIM-0/2, PowerSupply-0/A/A0
Apply Sources:        0/RP0/CPU0, 1/6/SP
```

Number of suppressed alarms : 0

This example displays information about all logging suppression rules applied to a specific source location on the router:

```
RP/0/RP0/CPU0:router# show logging suppress rule all source location 0/RP0/CPU0
```

```
Rule Name : test_suppression
Rule State: RULE_APPLIED_ALL
Severities : N/A
Alarms :
  Category      Group      Message
  CAT_E         GROUP_F    CODE_G
```

```
Apply Alarm-Locations: None
Apply Sources:        0/RP0/CPU0
```

Number of suppressed alarms : 0

This example shows summary information about all logging suppression rules:

```
RP/0/RP0/CPU0:router# show logging suppression rule all summary
Rule Name                                     :Number of Suppressed Alarms
Mike1                                         0
Mike2                                         0
Mike3                                         0
Reall                                         4
```

#### Related Commands

Command	Description
<a href="#">logging suppress apply rule, on page 29</a>	Applies and activates a logging suppression rule.
<a href="#">logging suppress rule, on page 30</a>	Creates a logging suppression rule.

# show snmp correlator buffer

To display messages in SNMP correlator buffer, use the **show snmp correlator buffer** in EXEC mode.

**show snmp correlator buffer** [{**all**|**correlation ID** |**rule-name name**}]

<b>Syntax Description</b>	<b>all</b>	Displays all messages in the correlator buffer.
	<b>correlation id</b>	Displays a message identified by correlation ID. Range is 0 to 4294967294. Up to 14 correlation rules can be specified, separated by a space.
	<b>rule-name name</b>	Displays a messages associated with a SNMP correlation rule name. Up to 14 correlation rules can be specified, separated by a space.
<b>Command Default</b>	None	
<b>Command Modes</b>	EXEC mode	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 3.8.0	This command was introduced.
<b>Usage Guidelines</b>	No specific guidelines impact the use of this command.	
<b>Task ID</b>	<b>Task ID</b>	<b>Operation</b>
	snmp	read

The sample shows an output from the **show snmp correlator buffer** command:

```
RP/0/RP0/CPU0:router# show snmp correlator buffer correlationID 10
Correlation ID : 10
Rule : ospf-trap-rule
Rootcause: 1.3.6.1.6.3.1.1.5.3
Time : Dec 14 02:32:05
Varbind(s):
  ifIndex.17 = 17
  ifDescr.17 = POS0/7/0/0
  ifType.17 = other(1)
  cieIfStateChangeReason.17 = down

Nonroot : 1.3.6.1.2.1.14.16.2.2
Time: Dec 14 02:32:04
Varbind(s):
  ospfRouterId = 1.1.1.1
  ospfNbrIpAddr = 30.0.28.2
  ospfNbrAddressLessIndex = 0
  ospfNbrRtrId = 3.3.3.3
  ospfNbrState = down(1)
```

## show snmp correlator info

To display the SNMP correlator buffer size and the percentage of the buffer occupied by correlated messages, use the **show snmp correlator info** command in EXEC mode.

**show snmp correlator info**

**Syntax Description** This command has no keywords or arguments.

**Command Default** None

**Command Modes** EXEC mode

Command History	Release	Modification
	Release 3.8.0	This command was introduced.

**Usage Guidelines** No specific guidelines impact the use of this command.

Task ID	Task ID	Operation
	snmp	read

The sample shows an output that contains remaining buffer size and percentage allocated to correlated messages from the **show snmp correlator info** command:

```
RP/0/RP0/CPU0:router# show snmp correlator info

  Buffer-Size      Percentage-Occupied
    85720                0.00
```

# show snmp correlator rule

To display defined SNMP correlation rules, use the **show snmp correlator rule** command in EXEC mode.

**show snmp correlator rule** [{*allrule-name*}]

## Syntax Description

**all** Displays all rule sets.

*rule-name* Specifies the name of a rule. Up to 14 predefined SNMP correlation rules can be specified, separated by a space.

## Command Default

None

## Command Modes

EXEC mode

## Command History

Release	Modification
Release 3.8.0	This command was introduced.

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

Task ID	Operation
snmp	read

This sample shows an output from the **show snmp correlator rule** command:

```
RP/0/RP0/CPU0:router# show snmp correlator rule rule_1
Rule Name : rule_1
  Time out : 888                               Rule State: RULE_APPLIED_ALL
  Root:    OID : 1.3.6.1.2.1.11.0.2
          vbind : 1.3.6.1.2.1.2.2.1.2 value /3\3\.\d{1,3}\.\d{1,3}/
          vbind : 1.3.6.1.2.1.5.8.3   index val
  Nonroot: OID : 1.3.6.1.2.1.11.3.3
```



# show snmp correlator ruleset

To display defined SNMP correlation rule set names, use the **show snmp correlator ruleset** command in EXEC mode.

```
show snmp correlator ruleset [{all/ruleset-name}]
```

<b>Syntax Description</b>	<b>all</b> Displays all rule set names.				
	<i>ruleset-name</i> Specifies the name of a rule set. Up to 14 predefined rule set names can be specified, separated by a space.				
<b>Command Default</b>	None				
<b>Command Modes</b>	EXEC mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Release 3.8.0</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Release 3.8.0	This command was introduced.
Release	Modification				
Release 3.8.0	This command was introduced.				
<b>Usage Guidelines</b>	No specific guidelines impact the use of this command.				
<b>Task ID</b>	<table border="1"> <thead> <tr> <th>Task ID</th> <th>Operation</th> </tr> </thead> <tbody> <tr> <td>snmp</td> <td>read</td> </tr> </tbody> </table>	Task ID	Operation	snmp	read
Task ID	Operation				
snmp	read				

This sample shows an output from the **show snmp correlator ruleset** command:

```
RP/0/RP0/CPU0:router# show snmp correlator ruleset test
Rule Set Name : test
Rules: chris1           : Not Applied
      chris2           : Applied
```

## source

To apply a logging suppression rule to alarms originating from a specific node on the router, use the **source** command in logging suppression apply rule configuration mode.

```
source location node-id
no source location node-id
```

<b>Syntax Description</b>	<b>location</b> <i>node-id</i> Specifies a node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.
---------------------------	--

<b>Command Default</b>	No scope is configured by default.
------------------------	------------------------------------

<b>Command Modes</b>	Logging suppression apply rule configuration
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 3.8.0	This command was introduced.

<b>Usage Guidelines</b>	No specific guidelines impact the use of this command.
-------------------------	--

<b>Task ID</b>	<b>Task</b>	<b>Operations</b>
	logging	execute

**Examples**

This example shows how to configure the logging suppression rule `infobistate` to suppress alarms from `0/RP0/CPU0`:

```
RP/0/RP0/CPU0:router(config)# logging suppress apply rule infobistate
RP/0/RP0/CPU0:router(config-suppr-apply-rule)# source location 0/RP0/CPU0
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">logging suppress apply rule, on page 29</a>	Applies and activates a logging suppression rule.

# timeout

To specify the collection period duration time for the logging correlator rule message, use the **timeout** command in stateful or nonstateful correlation rule configuration modes. To remove the timeout period, use the **no** form of this command.

```
timeout [milliseconds]  
no timeout
```

<b>Syntax Description</b>	<i>milliseconds</i> Range is 1 to 600000 milliseconds.
---------------------------	--

<b>Command Default</b>	Timeout period is not specified.
------------------------	----------------------------------

<b>Command Modes</b>	Stateful correlation rule configuration Nonstateful correlation rule configuration
----------------------	---

<b>Command History</b>	<b>Release</b> <b>Modification</b>
	Release 3.6.0 This command was introduced.

<b>Usage Guidelines</b>	Each correlation rule that is applied must have a timeout value, and only those messages captured within this timeout period can be correlated together.
-------------------------	--

The timeout begins when the first matching message for a correlation rule is received. If the root-cause message is received, it is immediately sent to syslog, while any non-root-cause messages are held.

When the timeout expires and the rootcause message has not been received, then all the non-root-cause messages captured during the timeout period are reported to syslog. If the root-cause message was received during the timeout period, then a correlation is created and placed in the correlation buffer.



<b>Note</b>	The root-cause alarm does not have to appear first. It can appear at any time within the correlation time period.
-------------	---

<b>Task ID</b>	<b>Task ID</b> <b>Operations</b>
	logging read, write

## Examples

This example shows how to define a logging correlation rule with a timeout period of 60,000 milliseconds (one minute):

```
RP/0/RP0/CPU0:router(config)# logging correlator rule state_rule type stateful  
RP/0/RP0/CPU0:router(config-corr-rule-st)# timeout 60000
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">logging correlator rule, on page 18</a>	Defines the rules by which the correlator logs messages to the logging events buffer.
<a href="#">timeout-rootcause, on page 61</a>	Specifies an optional parameter for an applied correlation rule.

# timeout-rootcause

To specify an optional parameter for an applied correlation rule, use the **timeout-rootcause** command in stateful or nonstateful correlation rule configuration modes. To remove the timeout period, use the **no** form of this command.

**timeout-rootcause** [*milliseconds*]  
**no timeout-rootcause**

**Syntax Description**      *milliseconds* Range is 1 to 600000 milliseconds.

**Command Default**      Root-cause alarm timeout period is not specified.

**Command Modes**      Stateful correlation rule configuration  
 Nonstateful correlation rule configuration

**Command History**

Release	Modification
Release 3.6.0	This command was introduced.

**Usage Guidelines**      When a root-cause timeout is configured and a non-root-cause message is received first, the following occurs:

- When a root-cause timeout is configured and a non-root-cause message is received first, the following occurs:
  - When the root-cause message arrives before the root-cause timeout expires, then the correlation continues as normal using the remainder of the main rule timeout.
- When the root-cause message is not received before the root-cause timeout expires, then all the non-root-cause messages held during the root-cause timeout period are sent to syslog and the correlation is terminated.

**Task ID**

Task ID	Operations
logging	read, write

## Examples

This example shows how to configure a timeout period for a root cause alarm:

```
RP/0/RP0/CPU0:router(config)# logging correlator rule state_rule type stateful
RP/0/RP0/CPU0:router(config-corr-rule-st)# timeout-rootcause 50000
```

Related Commands	Command	Description
	<a href="#">logging correlator rule, on page 18</a>	Defines the rules by which the correlator logs messages to the logging events buffer.

■ timeout-rootcause