Contents

EAA commands

action cli

Use **action cli** to add a CLI action to a monitor policy.

Use **undo action** to remove an action.

Syntax

action *number* **cli** *command-line*

undo action *number*

Default

A monitor policy does not contain any actions.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

number: Specifies an action ID in the range of 0 to 231.

cli *command-line*: Specifies the command line to be executed when the event occurs. You can enter abbreviated forms of command keywords, but you must make sure the forms can uniquely identify the command keywords. For example, you can enter **int loop 1** for the **interface loopback 1** command.

Usage guidelines

You can configure a series of actions to be executed in response to the event specified in a monitor policy. EAA executes the actions in ascending order of action IDs. When you add actions to a policy, you must make sure the execution order is correct. If two actions have the same ID, the most recent one takes effect.

To execute a command in a view other than user view, you must define actions required for accessing the target view before defining the command execution action. In addition, you must number the actions in the order they should be executed, starting with entering system view.

For example, to shut down an interface, you must create the following actions in order:

1. Action to enter system view.
2. Action to enter interface view.
3. Action to shut down the interface.

When you define an action, you can specify a value or specify a variable name for an argument. For more information about using EAA environment variables, see "rtm environment."

Examples

# Configure a CLI action for the CLI-defined policy **test** to shut down GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] action 1 cli system-view
[Sysname-rtm-test] action 2 cli interface gigabitethernet 1/0/1
[Sysname-rtm-test] action 3 cli shutdown
```

action reboot

Use **action reboot** to add a reboot action to a monitor policy.

Use **undo action** to remove an action.

Syntax

action *number* **reboot** [**slot** *slot-number*]

undo action *number*

Default

A monitor policy does not contain any actions.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

number: Specifies an action ID in the range of 0 to 231.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, the command reboots the IRF fabric.

Usage guidelines

The reboot action configured with this command reboots devices or cards without saving the running configuration. If you want to save the running configuration, use the **action cli** command to configure reboot actions.

You can configure a series of actions to be executed in response to the event specified in a monitor policy. EAA executes the actions in ascending order of action IDs. When you add actions to a policy, you must make sure the execution order is correct. If two actions have the same ID, the most recent one takes effect.

When you define an action, you can specify a value or specify a variable name for an argument. For more information about using EAA environment variables, see "rtm environment."

Examples

# Configure an action for the CLI-defined policy **test** to reboot the specified slot.

<Sysname> system-view

```
[Sysname] rtm cli-policy test
[Sysname-rtm-test] action 3 reboot slot 1
```

action switchover

Use **action switchover** to add an active/standby switchover action to a monitor policy.

Use **undo action** to remove an action.

Syntax

action *number* **switchover**

undo action *number*

Default

A monitor policy does not contain any actions.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

number: Specifies an action ID in the range of 0 to 231.

Usage guidelines

You can configure a series of actions to be executed in response to the event specified in a monitor policy. EAA executes the actions in ascending order of action IDs. When you add actions to a policy, you must make sure the execution order is correct. If two actions have the same ID, the most recent one takes effect.

This command does not trigger a master/subordinate switchover in either of the following situations:

- No subordinate device is configured.
- The subordinate device is not in up state.

Examples

# Configure an action for the CLI-defined policy **test** to perform an active/standby switchover.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] action 3 switchover
```

action syslog

Use **action syslog** to add a Syslog action to a monitor policy.

Use **undo action** to remove an action.

Syntax

action *number* **syslog priority** *priority* **facility** *local-number* **msg** *msg-body*

undo action *number*

Default

A monitor policy does not contain any actions.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

number: Specifies an action ID in the range of 0 to 231.

priority *priority*: Specifies the log severity level in the range of 0 to 7. A lower value represents a higher severity level.

facility *local-number*: Specifies a logging facility by its facility number in the range of local0 to local7. Facility numbers are used by a log host to identify log creation facilities for filtering log messages.

msg *msg-body*: Configures the log message body.

Usage guidelines

EAA sends log messages to the information center. You can configure the information center to output these messages to certain destinations. For more information about the information center, see "Configuring the information center."

You can configure a series of actions to be executed in response to the event specified in a monitor policy. EAA executes the actions in ascending order of action IDs. When you add actions to a policy, you must make sure the execution order is correct. If two actions have the same ID, the most recent one takes effect.

When you define an action, you can specify a value or specify a variable name for an argument. For more information about using EAA environment variables, see "rtm environment."

Examples

# Configure an action for the CLI-defined policy **test** to send a log message "hello" with a severity of 7 from the facility device **local3**.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] action 3 syslog priority 7 facility local3 msg hello
```

commit

Use **commit** to enable a CLI-defined monitor policy.

Syntax

commit

Default

No CLI-defined monitor policies are enabled.

Views

CLI-defined policy view

Predefined user roles

network-admin

Usage guidelines

You must execute this command for a CLI-defined monitor policy to take effect.

After changing the settings in a policy that has been enabled, you must re-execute this command for the changes to take effect.

Examples

# Enable CLI-defined monitor policy **test**.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] commit
```

display rtm environment

Use **display rtm environment** to display user-defined EAA environment variables and their values.

Syntax

display rtm environment [*var-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

var-name: Specifies a user-defined EAA environment variable by its name, a case-sensitive string of 1 to 63 characters. The name can contain digits, letters, and the underscore sign (_), but its leading character cannot be the underscore sign. If you do not specify a variable, this command displays all user-defined EAA environment variables.

Examples

# Display all user-defined EAA environment variables.

```
<Sysname> display rtm environment
Name             Value
save_cmd         save main force
show_run_cmd     display current-configuration
```

Table 1 Command output

Field	Description
Name	Name of a user-defined EAA environment variable. This field displays a maximum of 30 characters. To display a user-defined EAA environment variable name of more than 30 characters, use the **display current-configuration** command.
Value	Value of the user-defined EAA environment variable. This field displays a maximum of 30 characters. To display a user-defined EAA environment variable value of more than 30 characters, use the **display current-configuration** command.

display rtm policy

Use **display rtm policy** to display information about EAA monitor policies.

Syntax

display rtm policy { **active** | **registered** [**verbose**] } [*policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

active: Specifies policies that are executing the actions.

registered: Specifies policies that have been created.

verbose: Displays detailed information about monitor policies.

policy-name: Specifies a policy by its name, a case-sensitive string of 1 to 63 characters. If you do not specify a policy, the command displays information about all monitor policies.

Usage guidelines

To display the running configuration of CLI-defined monitor policies, execute the **`display current-configuration`** command in any view or execute the **`display this`** command in CLI-defined monitor policy view.

Examples

# Display monitor policies that are executing the actions.

```
<Sysname> display rtm policy active
JID   Type  Event      TimeActive           PolicyName
507   CLI   INTERFACE  Aug 29 14:55:55 2013 test
```

Table 2 Command output

Field	Description
JID	Job ID, displayed only when you specify the **`active`** keyword.
Type	Policy creation method: • **TCL**—The policy was configured by using Tcl. • **CLI**—The policy was configured from the CLI.
Event	Event type, including CLI, hotplug, interface, process, SNMP, SNMP-Notification, Syslog, and track.
TimeActive	Time when the monitor policy was triggered.
PolicyName	Name of the monitor policy.

# Display brief information about all created monitor policies.

```
<Sysname> display rtm policy registered
Total number: 1
Type  Event      TimeRegistered       PolicyName
CLI              Aug 29 14:54:50 2013 test
```

Table 3 Command output

Field	Description
Total number	Total number of the monitor policies.
Type	Policy creation method: • **TCL**—The policy was configured by using Tcl. • **CLI**—The policy was configured from the CLI.
Event	Event type, including CLI, hotplug, interface, process, SNMP, SNMP-Notification, Syslog, and track.
TimeRegistered	Time when the monitor policy was created.
PolicyName	Name of the monitor policy.

# Display detailed information about all monitor policies.

```
<Sysname> display rtm policy registered verbose
  Total number: 1

   Policy Name: test
   Policy Type: CLI
    Event Type:
TimeRegistered: Aug 29 14:54:50 2013
```

```
User-role: network-operator
           network-admin
```

Table 4 Command output

Field	Description
Total number	Total number of the monitor polices.
PolicyName	Name of the monitor policy.
Policy Type	Policy creation method: • **TCL**—The policy was configured by using Tcl. • **CLI**—The policy was configured from the CLI.
Event Type	Event type, including CLI, hotplug, interface, process, SNMP, SNMP-Notification, Syslog, and track.
TimeRegistered	Time when the policy was created.
User-role	User roles for executing the monitor policy. To execute the monitor policy, an administrator must have a minimum of one of the displayed user roles.

event cli

Use **event cli** to configure a CLI event for a CLI-defined monitor policy.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event cli { **async** [**skip**] | **sync** } **mode** { **execute** | **help** | **tab** } **pattern** *regular-exp*

undo event

Default

No CLI event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

async [**skip**]: Enables or disables the system to execute the command that triggers the policy. If you specify the **skip** keyword, the system executes the actions in the policy without executing the command that triggers the policy. If you do not specify the **skip** keyword, the system executes both the actions in the policy and the command entered at the CLI.

sync: Enables the system to execute the command that triggers the event only if the policy has been executed successfully.

mode { **execute** | **help** | **tab** }: Specifies the CLI operation to monitor:

- **execute**: Triggers the policy when a matching command is entered.
- **help**: Triggers the policy when a question mark (?) is entered at a matching command line.
- **tab**: Triggers the policy when the **Tab** key is pressed to complete a parameter in a matching command line.

pattern *regular-exp*: Specifies a regular expression for matching commands that trigger the policy. For more information about using regular expressions, see CLI in *Fundamentals Configuration Guide*.

Usage guidelines

Use CLI event monitor policies to monitor operations performed at the CLI.

You can configure only one event for a monitor policy. If the monitor policy already contains an event, the new event replaces the old event.

Examples

# Configure a CLI-defined policy to monitor execution of commands that contain the **display interface brief** string. Enable the system to execute the actions in the policy without executing the command that triggers the policy.

```
<Sysname>system-view
[Sysname] rtm cli-policy test
[Sysname-rmt-test] event cli async skip mode execute pattern display interface brief
```

# Configure a CLI-defined policy to monitor the use of the **Tab** key at command lines that contain the **display interface brief** string. Enable the system to execute the actions in the policy and display the complete parameter when **Tab** is pressed at a policy-matching command line.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rmt-test] event cli async mode tab pattern display interface brief
```

# Configure a CLI-defined policy to monitor the use of the question mark (?) at command lines that contain the **display interface brief** string. Enable the system to execute a policy-matching command line only if the actions in the policy are executed successfully when a question mark is entered at the command line.

```
<Sysname>system-view
[Sysname] rtm cli-policy test
[Sysname-rmt-test] event cli sync mode help pattern display interface brief
```

event hotplug

Use **event hotplug** to configure a hot-swapping event.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event hotplug [**insert** | **remove**] **slot** *slot-number*

undo event

Default

No hotplug event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

insert: Specifies the IRF member device join event.

remove: Specifies the IRF member device leave event.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

After you configure the event, the monitor policy is triggered when the member device joins or leaves the IRF fabric. If you do not specify the **insert** or **remove** keyword, EAA monitors the member device for joining or leaving the IRF fabric.

You can configure only one event entry for a monitor policy. If the monitor policy already contains an event entry, the new event entry replaces the old event entry.

Examples

# Configure a CLI-defined policy to monitor the member device for joining or leaving the IRF fabric.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event hotplug slot 1
```

event interface

Use **event interface** to configure an interface event for a CLI-defined monitor policy.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event interface *interface-list* **monitor-obj** *monitor-obj* **start-op** *start-op* **start-val** *start-val* **restart-op** *restart-op* **restart-val** *restart-val* [**interval** *interval*]

undo event

Default

No interface event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

interface-list: Specifies a space-separated list of up to eight interface items. An item specifies an interface or specifies a range of interfaces in the form of *interface-type interface-number* **to** *interface-type interface-number*. The interfaces in an interface range must be same type. The start interface number must be smaller than the end interface number.

monitor-obj *monitor-obj*: Specifies the traffic statistic to be monitored on the interface. For keywords available for the *monitor-obj* argument, see Table 5.

start-op *start-op*: Specifies the operator for comparing the monitored traffic statistic with the start threshold. The start threshold is crossed if the comparison result meets the condition. For keywords available for the *start-op* argument, see Table 6.

start-val *start-val*: Specifies the start threshold to be compared with the monitored traffic statistic. The value range is 0 to 4294967295.

restart-op *restart-op*: Specifies the operator for comparing the monitored traffic statistic with the restart threshold. The restart threshold is crossed if the comparison result meets the condition. For keywords available for the *restart-op* argument, see Table 6.

restart-val *restart-val*: Specifies the restart threshold to be compared with the monitored traffic statistic. The value range is 0 to 4294967295.

interval *interval*: Specifies the interval to sample the monitored traffic statistic for a comparison. The value range is 1 to 4294967295, in seconds. The default value is 300.

Table 5 Monitored objects

Monitored traffic statistic	Description
input-drops	Number of discarded incoming packets during the sampling interval
input-errors	Number of incoming error packets during the sampling interval
output-drops	Number of discarded outgoing packets during the sampling interval
output-errors	Number of outgoing error packets during the sampling interval
rcv-bps	Receive rate, in bps during the sampling interval
rcv-broadcasts	Number of incoming broadcasts during the sampling interval
rcv-kbps	Receive rate, in kilobytes per second
rcv-kpps	Receive rate, in kilopackets per second
rcv-pps	Receive rate, in packets per second
tx-bps	Transmit rate, in bps
tx-kbps	Transmit rate, in kilobytes per second
tx-kpps	Transmit rate, in kilopackets per second
tx-pps	Transmit rate, in packets per second

Table 6 Comparison operators

Comparison operator	Description
eq	Equal to
ge	Greater than or equal to
gt	Greater than
le	Less than or equal to
lt	Less than
ne	Not equal to

Usage guidelines

Use interface event monitor policies to monitor traffic statistics on an interface.

You can configure only one event for a monitor policy. If the monitor policy already contains an event, the new event replaces the old event.

EAA executes an interface event policy when the monitored interface traffic statistic crosses the start threshold in the following situations:

- The statistic crosses the start threshold for the first time.
- The statistic crosses the start threshold each time after it crosses the restart threshold.

The following is the interface event monitor process of EAA:

1. Compares the traffic statistic sample with the start threshold at sampling intervals until the start threshold is crossed.
2. Executes the policy.

3. Compares the traffic statistic sample with the restart threshold at sampling intervals until the restart threshold is crossed.
4. Compares the traffic statistic sample with the start threshold at sampling intervals until the start threshold is crossed.
5. Executes the policy again.

This process cycles for the monitor policy to be executed and re-executed.

Examples

# Configure a CLI-defined policy to monitor the incoming error packet statistic on GigabitEthernet 1/0/1 every 60 seconds. Set the start threshold to 1000 and the restart threshold to 50. Enable EAA to execute the policy when the statistic exceeds 1000 for the first time. Enable EAA to re-execute the policy if the statistic exceeds 1000 each time after the statistic has dropped below 50.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event interface gigabitethernet 1/0/1 monitor-obj input-errors
start-op gt start-val 1000 restart-op lt restart-val 50 interval 60
```

event process

Use **event process** to configure a process event for a CLI-defined monitor policy.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event process { **exception** | **restart** | **shutdown** | **start** } [**name** *process-name* [**instance** *instance-id*]] [**slot** *slot-number*]

undo event

Default

No process event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

exception: Monitors the specified process for exceptional events. EAA executes the policy when an exception occurs to the monitored process.

restart: Monitors the specified process for restart events. EAA executes the policy when the monitored process restarts.

shutdown: Monitors the specified process for shutdown events. EAA executes the policy when the monitored process is shut down.

start: Monitors the specified process for start events. EAA executes the policy when the monitored process starts.

name *process-name*: Specifies a user-mode process by its name. The process can be one that is running or not running. If you do not specify a name, this command monitors all use-mode processes.

instance *instance-id*: Specifies a process instance ID in the range of 0 to 4294967295. The instance ID can be one that has not been created yet. If you do not specify an instance, EAA monitors all instances of the process.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command applies to the IRF fabric.

Usage guidelines

Use process event monitor policies to monitor process state changes. These changes can result from manual operations or automatic system operations.

You can configure only one event for a monitor policy. If the monitor policy already contains an event, the new event replaces the old event.

Examples

# Configure a CLI-defined policy to monitor all instances of the process **snmpd** for restart events.

```
<Sysname>system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event process restart name snmpd
```

event snmp oid

Use **event snmp oid** to configure an SNMP event for a CLI-defined monitor policy.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event snmp oid *oid* **monitor-obj** { **get** | **next** } **start-op** *start-op* **start-val** *start-val* **restart-op** *restart-op* **restart-val** *restart-val* [**interval** *interval*]

undo event

Default

No SNMP event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

oid *oid*: Specifies the OID of the monitored MIB variable, a string of 1 to 256 characters.

monitor-obj { **get** | **next** }: Specifies the SNMP operation used for sampling variable values. The **get** keyword represents the SNMP get operation, and the **next** keyword represents the SNMP getNext operation.

start-op *start-op*: Specifies the operator for comparing the sampled value with the start threshold. The start threshold is crossed if the comparison result meets the condition. For keywords available for the *start-op* argument, see Table 6.

start-val *start-val*: Specifies the start threshold to be compared with the sampled value. The *start-val* argument can be any data type supported by SNMP, including numerals and character strings. The value range for the *start-val* argument is a string of 1 to 512 characters. If the threshold value contains spaces, you must enclose the value in quotation marks (" ").

restart-op *op*: Specifies the operator for comparing the sampled value with the restart threshold. The restart threshold is crossed if the comparison result meets the condition. For keywords available for the *start-op* argument, see Table 6.

restart-op *restart-val*: Specifies the restart threshold to be compared with the sampled value. The *restart-val* argument can be any data type supported by SNMP, including numerals and character strings. The value range for the *restart-val* argument is a string of 1 to 512 characters. If the threshold value contains spaces, you must enclose the value in quotation marks (" ").

interval *interval*: Specifies the sampling interval in the range of 1 to 4294967295, in seconds. The default value is 300.

Usage guidelines

Use SNMP event monitor policy to monitor value changes of MIB variables.

You can configure only one event for a monitor policy. If the monitor policy already contains an event, the new event replaces the old event.

EAA executes an SNMP event policy when the monitored MIB variable's value crosses the start threshold in the following situations:

- The monitored variable's value crosses the start threshold for the first time.
- The monitored variable's value crosses the start threshold each time after it crosses the restart threshold.

The following is the SNMP event monitor process of EAA:

1. Compares the variable sample with the start threshold at sampling intervals until the start threshold is crossed.
2. Executes the policy.
3. Compares the variable sample with the restart threshold at sampling intervals until the restart threshold is crossed.
4. Compares the variable sample with the start threshold at sampling intervals until the start threshold is crossed.
5. Executes the policy again.

This process cycles for the monitor policy to be executed and re-executed.

For the command to take effect, enable SNMP before you execute this command.

Examples

# Configure a CLI-defined policy to get the value of the MIB variable **1.3.6.4.9.9.42.1.2.1.6.4** every five seconds. Set the start threshold to 1 and the restart threshold to 2. Enable EAA to execute the policy when the value changes to 1 for the first time. Enable EAA to re-execute the policy if the value changes to 1 each time after the value has changed to 2.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event snmp oid 1.3.6.4.9.9.42.1.2.1.6.4 monitor-obj get start-op eq
start-val 1 restart-op eq restart-val 2 interval 5
```

event snmp-notification

Use **event snmp-notification** to configure an SNMP-Notification event for a CLI-defined policy.

Use **undo event** to remove the event in a CLI-defined policy.

Syntax

event snmp-notification oid *oid* **oid-val** *oid-val* **op** *op* [**drop**]

undo event

Default

No SNMP-Notification event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

oid *oid*: Specifies the OID of the monitored MIB variable, a string of 1 to 256 characters.

oid-val *oid-val*: Specifies the threshold to be compared with the sampled value. The *oid-val* argument can be any data type supported by SNMP, including numerals and character strings. The value range for the *oid-val* argument is a string of 1 to 512 characters. If the threshold value contains spaces, you must enclose the value in quotation marks (" ").

op *op*: Specifies the operator for comparing the sampled value with the threshold. The policy is executed if the comparison result meets the condition. For keywords available for the *start-op* argument, see Table 6.

drop: Drops the notification if the comparison result meets the condition. If you do not specify this keyword, the system sends the notification.

Usage guidelines

Use SNMP-Notification event monitor policies to monitor variables in SNMP notifications.

EAA executes an SNMP-Notification event monitor policy when the value of the monitored variable in an SNMP notification meets the specified condition.

You can configure only one event for a monitor policy. If the monitor policy already contains an event, the new event replaces the old event.

For the command to take effect, enable SNMP before you execute this command.

Examples

# Configure a CLI-defined policy to monitor SNMP notifications that contain the use name variable **1.3.6.1.4.1.25506.2.2.1.1.2.1.0**. Enable the system to execute the policy and drop the SNMP notification if the use name variable value is **admin**.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event snmp-notification oid 1.3.6.1.4.1.25506.2.2.1.1.2.1.0 oid-val
admin op eq drop
```

event syslog

Use **event syslog** to configure a Syslog event for a CLI-defined monitor policy.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event syslog priority { *priority* | **all** } **msg** *msg* **occurs** *times* **period** *period*

undo event

Default

No Syslog event is configured.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

priority { *priority* | **all** }: Specifies the severity level for matching log messages.

- *priority*: Specifies the lowest severity level for matching log messages. It is an integer in the range of 0 to 7. A lower number represents higher severity level. For example, specify a severity level of 3 to match log messages from level 3 to level 0.
- **all:** Represents any severity level from 0 to 7.

msg msg: Specifies a regular expression to match the logs. The *msg* argument represents a regular expression, a string of 1 to 255 characters.

occurs *times* **period** *period*: Executes the policy if the number of log matches over an interval exceeds the limit. The *times* argument specifies the maximum number of log matches in the range of 1 to 32. The *period* argument specifies an interval in the range of 1 to 4294967295 seconds.

Usage guidelines

Use Syslog event monitor policies to monitor log messages.

EAA executes a Syslog event monitor policy when the number of matching logs over an interval reaches the limit.

NOTE:

EAA does not count log messages generated by the RTM module when it counts log matches.

You can configure only one event for a monitor policy. If the monitor policy already contains an event, the new event replaces the old event.

A regular expression can contain the special characters described in Table 7.

Table 7 Special characters supported in a regular expression

Characters	Meaning	Examples
^	Matches the beginning of a line.	"^u" matches all lines beginning with "u". A line beginning with "Au" is not matched.
$	Matches the end of a line.	"u$" matches all lines ending with "u". A line ending with "uA" is not matched.
. (period)	Matches any single character.	".s" matches "as" and "bs".
*	Matches the preceding character or string zero, one, or multiple times.	"zo*" matches "z" and "zoo", and "(zo)*" matches "zo" and "zozo".
+	Matches the preceding character or string one or multiple times.	"zo+" matches "zo" and "zoo", but not "z".
|	Matches the preceding or succeeding string.	"def|int" matches a line containing "def" or "int".
( )	Matches the string in the parentheses, usually used together with the plus sign (+) or asterisk sign (*).	"(123A)" matches "123A". "408(12)+" matches "40812" and "408121212", but not "408".
\N	Matches the preceding strings in	"(string)\1" matches a string containing

Characters	Meaning	Examples
	parentheses, with the *Nth* string repeated once.	"stringstring". "(string1)(string2)\2" matches a string containing "string1string2string2". "(string1)(string2)\1\2" matches a string containing " string1string2string1string2".
[ ]	Matches a single character in the brackets.	"[16A]" matches a string containing 1, 6, or A; "[1-36A]" matches a string containing 1, 2, 3, 6, or A (- is a hyphen). To match the character "]", put it immediately after "[", for example, []abc]. There is no such limit on "[".
[^]	Matches a single character that is not in the brackets.	"[^16A]" matches a string that contains one or more characters except for 1, 6, or A, such as "abc". A match can also contain 1, 6, or A (such as "m16"), but it cannot contain these three characters only (such as 1, 16, or 16A).
{n}	Matches the preceding character *n* times. The number *n* must be a nonnegative integer.	"o{2}" matches "food", but not "Bob".
{n,}	Matches the preceding character *n* times or more. The number *n* must be a nonnegative integer.	"o{2,}" matches "foooood", but not "Bob".
{n,m}	Matches the preceding character *n* to *m* times or more. The numbers *n* and *m* must be nonnegative integers and *n* cannot be greater than *m*.	" o{1,3}" matches "fod", "food", and "foooood", but not "fd".
\<	Matches a string that starts with the pattern following \<. A string that contains the pattern is also a match if the characters preceding the pattern are not digits, letters, or underscores.	"\<do" matches "domain" and "doa".
\>	Matches a string that ends with the pattern preceding \>. A string that contains the pattern is also a match if the characters following the pattern are not digits, letters, or underscores.	"do\>" matches "undo" and "cdo".
\b	Matches a word that starts with the pattern following \b or ends with the pattern preceding \b.	"er\b" matches "never", but not "verb" or "erase". "\ber" matches "erase", but not "verb" or "never".
\B	Matches a word that contains the pattern but does not start or end with the pattern.	"er\B" matches "verb", but not "never" or "erase".
\w	Same as [A-Za-z0-9_], matches a digit, letter, or underscore.	"v\w" matches "vlan" and "service".
\W	Same as [^A-Za-z0-9_], matches a character that is not a digit, letter, or underscore.	"\Wa" matches "-a", but not "2a" or "ba".
\	Escape character. If a special character listed in this table follows \, the specific meaning of the character is removed.	"\\" matches a string containing "\", "\^" matches a string containing "^", and "\\b" matches a string containing "\b".

Examples

# Configure a CLI-defined policy to monitor Syslog messages for level 3 to level 0 messages that contain the **down** string. Enable the policy to execute when five log matches are found within 6 seconds.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event syslog priority 3 msg down occurs 5 period 6
```

event track

Use **event track** to configure a track event for a CLI-defined monitor policy.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event track *track-list* **state** { **negative** | **positive** } [**suppress-time** *suppress-time*]

undo event

Default

A CLI-defined policy does not contain a track event.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

track-list: Specifies a space-separated list of up to 16 track items. Each item specifies a track entry number or a range of track entry numbers in the form of *track-entry-number* **to** *track-entry-number*. The value range for the *track-entry-number* argument is 1 to 1024.

state { **negative** | **positive** }: Monitors state change of the track entries.

- **negative**: Triggers the policy when the states of the track entries change from Positive to Negative.
- **positive**: Triggers the policy when the states of the track entries change from Negative to Positive.

suppress-time *suppress-time*: Sets a suppress time in the range of 1 to 4294967295, in seconds. The default value is 0.

Usage guidelines

Use track event monitor policies to monitor state change of track entries. If you specify one track entry for a policy, EAA triggers the policy when the state of the track entry changes from Positive to Negative or from Negative to Positive. If you specify multiple track entries for a policy, EAA triggers the policy only when the state of all the track entries changes from Positive to Negative or Negative to Positive.

If you set a suppress time for a track event monitor policy, the timer starts when the policy is triggered. The system does not process the messages that report the track entry positive-to-negative or negative-to-positive state change until the timer times out.

For example, to automatically disconnect the sessions between the local device and its down link BGP peers when the sessions between the local device and its uplink BGP peers are disconnected, you can configure a track event monitor policy as follows:

- Configure a track event for the policy and specify track entries to monitor the links between the local device and its uplink BGP peers.
- Add the CLI action **`peer ignore`** to the policy to disable BGP session establishment between the local device and its downlink BGP peers.

You can configure only one event entry for a monitor policy. If the monitor policy already contains an event entry, the new event entry replaces the old event entry.

Examples

# Create CLI-defined monitor policy **test**. Configure a track event for the policy that occurs when the states of track entry 1 to track entry 8 change from Positive to Negative. Set the suppress time to 180 seconds for the policy.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event track 1 to 8 state negative suppress-time 180
```

rtm cli-policy

Use **`rtm cli-policy`** to create a CLI-defined EAA monitor policy and enter its view, or enter the view of an existing CLI-defined EAA monitor policy.

Use **`undo rtm cli-policy`** to delete a CLI-defined monitor policy.

Syntax

`rtm cli-policy` *`policy-name`*

`undo rtm cli-policy` *`policy-name`*

Default

No CLI-defined monitor policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

`policy-name`: Specifies the name of a CLI-defined monitor policy, a case-sensitive string of 1 to 63 characters.

Usage guidelines

You must create a CLI-defined monitor policy before you can use the CLI to configure settings in the policy.

For a CLI-defined monitor policy to take effect, you must execute the **`commit`** command after you complete configuring the policy.

You can execute this command multiple times to create multiple CLI-defined monitor policies. Make sure the CLI-defined monitor policies that are executed at the same time do not have conflicting actions. If the actions conflict, the system executes the actions randomly.

You can assign the same name to a CLI-defined policy and a Tcl-defined policy.

Examples

# Create a CLI-defined policy and enter its view.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
```

Related commands

commit

rtm environment

Use **rtm environment** to configure an EAA environment variable.

Use **undo rtm environment** to delete a user-defined EAA environment variable.

Syntax

rtm environment *var-name var-value*

undo rtm environment *var-name*

Default

No user-defined EAA environment variables exist.

The system provides the variables in Table 8. You cannot create, delete, or modify these system-defined variables.

Table 8 System-defined EAA environment variables by event type

Event	Variable name and description
Any event	_event_id: Event ID _event_type: Event type _event_type_string: Event type description _event_time: Time when the event occurs _event_severity: Severity level of an event
CLI	_cmd: Commands that are matched
Syslog	_syslog_pattern: Log message content
Hotplug	_slot: ID of the member device that joins or leaves the IRF fabric
Interface	_ifname: Interface name
SNMP	_oid: OID of the MIB variable where an SNMP operation is performed _oid_value: Value of the MIB variable
SNMP-Notification	_oid: OID that is included in the SNMP notification.
Process	_process_name: Process name

Views

System view

Predefined user roles

network-admin

Parameters

var-name: Specifies a user-defined EAA environment variable by its name, a case-sensitive string of 1 to 63 characters. The name can contain digits, letters, and the underscore sign (_), but its leading character cannot be the underscore sign.

var-value: Specifies the variable value.

Usage guidelines

When you define an action, you can enter a variable name with a leading dollar sign (**$***variable_name*) instead of entering a value for an argument. EAA will replace the variable name with the variable value when it performs the action.

For an action argument, you can specify a list of variable names in the form of **$***variable_name1***$***variable_name2...***$***variable_nameN.*

Examples

# Create an environment variable: set its name to **if** and set its value to **interface**.

```
<Sysname> system-view
[Sysname] rtm environment if interface
```

rtm event syslog buffer-size

Use **rtm event syslog buffer-size** to set the size for the EAA-monitored log buffer.

Use **undo rtm event syslog buffer-size** to restore the default.

Syntax

rtm event syslog buffer-size *buffer-size*

undo rtm event syslog buffer-size

Default

The size of the EAA-monitored log buffer is 50000.

Views

System view

Predefined user roles

network-admin

Parameters

buffer-size: Specifies the size for the EAA-monitored log buffer, in the range of 1 to 500000.

Usage guidelines

After you execute a Syslog event monitor policy, the system saves a copy of the logs to the EAA-monitored log buffer. When the logs in the buffer match the Syslog event, EAA executes the monitor policy actions.

Typically, the default EAA-monitored log buffer size is sufficient. However, when a feature malfunctions or the user enables multiple debugging functions, a large number of logs are generated. Some logs might be discarded before the matching is performed. You can set the EAA-monitored log buffer to a large size based on the memory usage.

Examples

# Set the size of the EAA-monitored log buffer to 1000.

```
<Sysname> system-view
[Sysname] rtm event syslog buffer-size 1000
```

Related commands

event syslog

rtm scheduler suspend

Use **rtm scheduler suspend** to suspend all monitor policies, including CLI monitor policies and Tcl monitor policies.

Use **undo rtm scheduler suspend** to resume monitor policies.

Syntax

rtm scheduler suspend

undo rtm scheduler suspend

Views

System view

Predefined user roles

network-admin

Usage guidelines

You need to suspend the monitor policies under the following circumstances:

- The monitor policies are triggered frequently, affecting the system services and performance.
- The Tcl script of a policy needs to be revised.

After you execute this command, EAA will not execute the policies even if the trigger conditions are met.

This command does not suspend a running monitor policy until all its actions are executed.

Examples

# Suspend monitor policies.

```
<Sysname> system-view
[Sysname] rtm scheduler suspend
```

rtm tcl-policy

Use **rtm tcl-policy** to create a Tcl-defined policy and bind it to a Tcl script file.

Use **undo rtm tcl-policy** to delete a Tcl policy.

Syntax

rtm tcl-policy *policy-name tcl-filename*

undo rtm tcl-policy *policy-name*

Default

No Tcl policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a policy name, a case-sensitive string of 1 to 63 characters.

tcl-filename: Specifies a .tcl script file name. The file name is case sensitive. You must ensure that the file is available on a storage medium of the device.

Usage guidelines

When you use this command to create a Tcl-defined policy, follow these guidelines:

Make sure the script file is saved on all IRF member devices. This practice ensures that the policy can run correctly after a master/subordinate switchover occurs or the member device where the script file resides leaves the IRF.

This command both creates and enables the specified Tcl-defined monitor policy. To revise the Tcl script of a Tcl-defined policy, you must suspend all monitor policies first, and then resume the policies after you finish revising the script. The system cannot execute a Tcl-defined policy if you edit its Tcl script without suspending all monitor policies.

To bind a Tcl-defined policy to a different Tcl script file:

1. Execute the **undo rtm tcl-policy** command to delete the Tcl policy.
2. Create the Tcl policy again, and then bind it to the new Tcl script file.

You can assign the same policy name to a CLI-defined policy and a Tcl-defined policy. However, you cannot assign the same name to policies that are the same type.

Examples

# Create a Tcl policy and bind it to a Tcl script file.

```
<Sysname> system-view
[Sysname] rtm tcl-policy test test.tcl
```

running-time

Use **running-time** to configure the action runtime of a CLI-defined policy.

Use **undo running-time** to restore the default.

Syntax

running-time *time*

undo running-time

Default

The action runtime of a CLI-defined policy is 20 seconds.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

time: Specifies the action runtime in the range of 0 to 31536000 seconds. If you specify 0, the policy runs its actions forever once the policy is triggered.

Usage guidelines

The action runtime limits the amount of time that the monitor policy runs its actions from the time it is triggered. When the runtime is reached, the system stops executing the actions even if the execution is not finished.

This setting prevents an incorrectly defined policy from running its actions permanently to occupy resources.

Examples

# Set the action runtime to **60** seconds for CLI-defined policy **test**.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] running-time 60
```

user-role

Use **`user-role`** to assign a user role to a CLI-defined policy.

Use **`undo user-role`** to remove a user role from a CLI-defined policy.

Syntax

`user-role` *`role-name`*

`undo user-role` *`role-name`*

Default

A monitor policy contains user roles that its creator had at the time of policy creation.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

`role-name`: Specifies a user role by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

For EAA to execute an action in a monitor policy, you must assign the policy the user role that has access to the action-specific commands and resources. If EAA lacks access to an action-specific command or resource, EAA does not perform the action and all the subsequent actions.

For example, a monitor policy has four actions numbered from 1 to 4. The policy has user roles that are required for performing actions 1, 3, and 4, but it does not have the user role required for performing action 2. When the policy is triggered, EAA executes only action 1.

A monitor policy supports a maximum of 64 valid user roles. User roles added after this limit is reached do not take effect.

An EAA policy cannot have both the **security-audit** user role and any other user roles. Any previously assigned user roles are automatically removed when you assign the **security-audit** user role to the policy. The previously assigned **security-audit** user role is automatically removed when you assign any other user roles to the policy.

Examples

# Assign user roles to a CLI-defined policy.

```
<Sysname> system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] user-role network-admin
[Sysname-rtm-test] user-role admin
```