CHAPTER 9

Handling and Reporting Alarms and Events

Cisco E-DI uses events received from devices, and data collected during polling and inventory, to maintain an accurate representation of the state of the devices and the network.

This data gives you an up-to-date view of the health of the device, and alerts you to configuration changes that are likely to fail. All events received from the network are automatically archived in the database. See Event Handling for more information.

Cisco E-DI also monitors certain events and performs automatic actions such as data synchronization and local status update. Any Cisco E-DI command or perl script can generate an event action.

When there are error conditions on the Network Elements, Cisco E-DI raises alarms and events as appropriate. The events are generated in standard Syslog message format so that external clients can subscribe to receive and process these events.

Note The timestamps for alarms and events use Cisco E-DI time, not the device time.

When the color mode is enabled, the Cisco E-DI CLI prompt indicates the NE's alarm aggregate status. The color of the prompt indicates the highest alarm severity found in the devices within the scope of the CLI mode. See CLI Color Mode, page 1-14 for more details.

When there are no alarms are on the device, the CLI prompt is white.

If session-based device authentication is enabled, Cisco E-DI automatically sets the Syslog auto-subscription to Off. This means that you are notified that each managed device must be configured to forward the Syslog messages to Cisco E-DI either directly or through a Syslog relay agent.

You can configure one or more Syslog relays as valid Syslog generation sources. To do this, enter the configuration command **`relay-agent syslog`**.

Cisco E-DI automatically accepts messages from any preconfigured Syslog relay or directly from the NE. You do not have to choose one or the other.

This section includes the following information:

Alarms

An alarm is a fault condition which needs attention from an administrator. Cisco E-DI monitors the network and itself to report network or server related alarms to the user. Alarms are raised based on the analysis of data obtained through polling of status and performance parameters, and the events received from the network.

The alarms are triggered according to user-defined conditions and thresholds, or by using default settings. Cisco E-DI captures the state of all NE interfaces, and represents them as NE alarms (if necessary). The NE's alarm aggregate status is indicated by the color of the CLI prompt.

Alarms can belong to either the server domain or the network. Basic parameters can be configured in the server configuration mode.

Alarms will be cleared automatically if the relevant network or server conditions are resolved. Alarms can also be cleared manually using the **clear alarms** command. See Table A-1 for details of the options available with this command.

All alarm related commands are context sensitive in the network and server domains.

All alarms are stored in the alarm history. Where Cisco E-DI is managing many devices, a large number of alarms is possible because of the number of interfaces and other components in the devices that potentially have associated states.

To avoid any performance issues, a limit is defined for the alarm history. This indicates how many entries each alarm will have in its history.

Table 9-1 describes the commands used to manage the alarm history data.

Table 9-1 Commands to Manage the Alarm History

Action	Command
To define the size limit for the alarm history. The default is 20 entries per alarm.	`[SRV:/server](config)# [no] alarm-history size <10-100>`
To configure the amount by which the alarm history is truncated. Each time the number of alarms crosses the specified limit, the alarm history is truncated. The default value is 50%.	`[SRV:/server](config)# [no] alarm-history truncate <30-80>`

Alarm Parameters

Cisco E-DI alarms have the following parameters:

- Alarm condition—A network or server related qualitative or quantitative parameter that has a state or value, depending on which alarm is raised or cleared.
- State—Either **Active** or **Clear**.
- Default severity—Used when no thresholds are defined, or a pre-defined severity for an alarm has to be ignored.
- Alarm component—For a network, this is a sub-section of a device. For example, an interface or a module. For the server, it could be a module name.
- Alarm severity—A pre-defined state that signifies that level of severity. Alarms can be triggered with a specified severity based on a state value which can be Boolean or can be triggered with varying levels of severity based on the defined thresholds and the state value.

- Alarm thresholds—Specified by the you and associated to a condition value either as a percentage or a numerical value. Alarms that have thresholds can oscillate between different alarm severities according to the values associated to that condition.

Alarm Conditions

The alarm conditions are given in Table 9-2.

Table 9-2 Alarm Conditions

Alarm Condition	Unit	Threshold	Domain	Description
CPUOverloaded	%	Yes	Network	CPU utilization on the device is too high.
ConnectionFailed	No	No	Network	Failed to establish a Telnet/SSH connection to the device.
DBUnavailable	No	No	Server	Database connection unavailable on the server.
EDIDiskSpaceUsageHigh				Cisco E-DI disk space usage is high
FCSErrors	%	Yes	Network	Too high FCSError rate (FCS errors vs. throughput) on a Radio interface.
FailedToLoad	No	No	Server	Server module failed to load.
HighMemPoolUtil	%	Yes	Network	High memory pool utilization on the device, expressed as used memory vs. total memory.
IfAdminDown	No	No	Network	Device interface administratively down.
IfDown	No	No	Network	Device interface operationally down.
IfOverloaded	%	Yes	Network	Interface utilization high, expressed as through-put vs. total-bandwidth.
IfPacketErrors	%	Yes	Network	Too high Packet error rate (packet errors vs. total throughput) on an interface.
LineProtoDown	No	No	Network	Interface line protocol down.
LoggingHostMismatch	No	No	Network	Logging settings on the device does not have Cisco E-DI as a Syslog event recipient.
MemAllocFailure	No	No	Network	Memory allocation failure on the device.
MemoryDefragmented	%	Yes	Network	Largest contiguous memory segment available vs. total available free space.
PrimaryServerUnavailable				Primary server unavailable
RunningConfigUnavailable	No	No	Network	Running Config of the device is unavailable
SecondaryServerUnavailable				Secondary server unavailable
StartupConfigUnavailable	No	No	Network	Startup Config of the device is unavailable
SwPolicyViolation	No	No	Network	Software on device does not conform to the policy specified.
TftpServerNotstarted	No	No	Server	TftpServer on the server failed to start.
TxFailedAfterMaxRetries	%	Yes	Network	Tx failures relative to through-put after allowed re-transmission attempts exceeded threshold.
Unreachable	No	No	Server	Device is not reachable using SNMP.
Unsupported	No	No	Network	Device not a recognized type.

Table 9-2 Alarm Conditions (continued)

Alarm Condition	Unit	Threshold	Domain	Description
VtpConfigDigestErrors				VtpConfigDigestErrors
VTPConfigRevNumberErrors				VTPConfigRevNumberErrors

Table 9-3 gives the commands that you can use to display specific alarm conditions.

Table 9-3 Commands to View Alarms

Action	Command
To show all alarms in active and cleared state.	`[NET:/network]# show alarms all`
To show alarms that match the given condition.	`[NET:/network]# show alarms condition condition-name`
To show the detailed history for the active alarms.	`[NET:/network]# show alarms details`
To show alarms that are of given severity.	`[NET:/network]# show alarms severity alarm-severity`
To show all alarms that match the given severity.	`[NET:/network]# show alarms all severity alarm-severity`
To show all alarms that match the given condition.	`[NET:/network]# show alarms all condition condition-name`
To show the details of all alarms in the network.	`[NET:/network]# show alarms all details`
To show active alarms that match the criteria specified in the filter.	`[NET:/network]# show alarms filter text`
To show all alarms that match the criteria specified in the filter.	`[NET:/network]# show alarms all filter text`
To show active alarms for the entire network.	`[NET:/network]# show alarms network`
To show active alarms for the server.	`[NET:/network]# show alarms server`
To show alarms for a device.	`[NET:/network]# show alarms device ip_address [all| details | [condition condition-name] | [severity alarm-severity]]`
To show alarms for a group.	`[NET:/network]# show alarms group group-name [all | details | [condition condition-name] | [severity alarm-severity]]`
To show alarms with a specified id.	`[NET:/network]# show alarms id number`

Configuring an Alarm Policy

To configure an alarm policy:

Step 1 Login to the Cisco E-DI server with administrative privileges.

Step 2 Enter into the configure mode:

```
[SVR:/server]# config terminal
```

Step 3 Enter the following command to configure an alarm policy using the default alarm policy as a base:

```
[SVR:/server](config)# alarm-policy default
```

Step 4 Enter the following command to configure an alarm condition, for example CPUOverloaded:

```
[SVR:/server](conf-alarm-policy)# define alarm-condition CPUOverloaded
```

Step 5 Enter the following command to define the number of cycles to observe before the alarm is raised, for example 2:

```
[SVR:/server](def-cond-param)# cycles 2
```

Step 6 Enter the following command to define the severity and threshold value associated with that condition:

```
[SVR:/server](def-cond-param)# threshold P1 2
```

This example will raise an alarm with a severity of P1 when the CPU goes over 2% over a period of 2 cycles.

The following example shows two sample alarm configurations:

```
alarm-policy default
  notify severity P1 john@cisco.com support@cisco.com
  !
   define alarm-condition CPUOverloaded
   set default-severity P2
   threshold P1 50
   threshold P2 40
   poll-cycles 2
  !
  define alarm-condition IfPacketErrors
   threshold P1 5
  !
  define alarm-condition IfAdminDown
   set default-severity P4
   disable
  !
```

Events

All Syslog and SNMP trap events received by Cisco E-DI from the network are automatically archived in the database.

By default, the database has the capacity to store 1 million events. This limit can be increased up to 10 million events. See Configuring Event Size Restriction for more details. Events are also published by Cisco E-DI to northbound interfaces.

Cisco E-DI provides CLI commands to perform the following actions on the events:

- View all events by device or group
- Filter events based on a regular expression
- Delete events based on device or group or a time limit
- Attach a trigger to an event. The trigger action can be any Cisco E-DI command or perl script.

Cisco E-DI also listens for certain events, and performs automatic actions such as data synchronization or local status update.

To setup Cisco E-DI to listen for Syslog notifications from the NEs enter:

```
[SVR:/server} (config)# subscribe syslog
```

Note The behavior of this command changes when session-based device authentication is enabled. See Using Session-Based Device Authentication, page 2-7 for a full explanation of the command behavior.

Cisco E-DI also listens for Syslog notifications from Syslog servers on the network.

Note Cisco E-DI will receive and process Syslog messages corresponding to linkup and linkdown notifications. SNMP traps for linkup and linkdown are received, and archived, but not processed.

Events can be summarized, queried, and cleared based on a timestamp. Event triggers can be defined to look for a particular type of content in the events and implement any EXEC level command. Sophisticated regular expressions can be defined to filter events and take appropriate action.

Displaying Events

Table 9-3 gives the commands that you can use to display specific event conditions.

Table 9-4 Commands to Display Events

Action	Command
To show network events in network mode and server events in server mode. This is a context sensitive command. The results are formatted.	`[NET:/network]# show events`
To provide events in the original format as generated on the device or Cisco E-DI.	`[NET:/network]# show events raw-format`
To query the server for the required number of commands.	`[NET:/network]# show events last number`
To query the server for the events recorded in between the dates and times specified.	`[NET:/network]# show events between yyyy mm dd hh:mm:ss yyyy mm dd`
To specify the number of events in the original Syslog format as generated on the device or Cisco E-DI.	`[NET:/network]# show events raw-format last number`
To list events for a specific device	`[NET:/network]# show events device ip_address`
To list specified number of events for a specific device	`[NET:/network]# show events device ip_address last number`
To list events for a specific group	`[NET:/network]# show events group group-name`
To list specified number of events for a specific group	`[NET:/network]# show events group group-name last number`
To summarize all events for a device	`[NET:/network]# show events device ip_address summary`
To summarize all events for a group	`[NET:/network]# show events group group-name summary`
To summarize all events for a specific by the type of facility.	`[NET:/network]# show events summary`
To filter events by specifying a regular expression.	`[NET:/network]# show events filter regular-expression/text in event's message`
To filter events by specifying a regular expression.	`[NET:/network]# show events raw-format filter regular-expression/text in event's message`
To clear events for the current selection of devices or server. This is a context sensitive command.	`[NET:/network]# clear events`

Table 9-4 Commands to Display Events (continued)

Action	Command
To clear all events for the network or server. This is a context sensitive command.	`[NET:/network]# clear events all [network | server]`
To clear events for the network or server which are older than the specified time frame. This is a context sensitive command.	`[NET:/network]# clear events older-than [days | hours] [1-240]`

Configuring an Event Trigger

An event trigger can be defined to look for a particular type of content in the events. This allows you to perform an action upon detecting a specified pattern in the events received from the network or server.

Any EXEC level task can be performed as an action, including sending an e-mail or generating an alarm. Table 9-5 details the commands to configure an event trigger to perform a specified action.

Table 9-5 Commands to Configure an Event Trigger

Action	Command
To define an event trigger to perform a certain action upon detecting a network condition. **Note** If you choose a name which already exists for an event trigger, the existing event trigger will be overwritten by the new event-trigger. You can list event triggers and associated parameters.	`[SRV:/server](config)# event-trigger name`
To apply the trigger to events generated from the server or the specified device on the network.	`[SRV:/server](conf-evt-trig)# domain {network {ip_address1 ip_address2}| server}`
To specify a pattern to be matched. Option to match all or any of the regular expressions specified.	`[SRV:/server](conf-evt-trig)# pattern [match-all | match-any] regular-expression`
To implement the specified **exec** level commands when a successful match of the pattern occurs.	`[SRV:/server](conf-evt-trig)# execute [exec-level-command-1; exec-level-command-2…]`

To list all the configured event triggers and the associated parameters.	`[SRV:/server]# show server running-config module event-triggers`
	or
	`[SRV:/server]# show running-config`

To delete an event trigger.	`[SRV:/server](config)# no event-trigger name`

The following example shows a sample event trigger:

```
event-trigger MemoryTrigger
  pattern match-all MALLOC-FAIL
  execute show alarms | email john@cisco.com
```

Configuring Event Size Restriction

Events are stored in the Cisco E-DI database. The number of events stored can be configured. Once the number of events cross the specified size, 10% of the recent events are automatically deleted.

To configure the nuber of events to be stored:

Step 1 Login to the Cisco E-DI server with administrative privileges.

Step 2 Enter into the configure mode:

```
[SVR:/server]# config terminal
```

Step 3 Enter the following command to define the maximum number of events to be stored:

```
[SVR:/server](config)# events server | network max-size number
```

Step 4 Enter this command to verify that the running configuration shows the maximum number of events:

```
[SVR:/server]# show running-config | include event
```