CHAPTER 11

Monitoring Alarms

An ***alarm*** is a Prime Infrastructure response to one or more related events. If an event is considered of high enough severity (critical, major, minor, or warning), Prime Infrastructure raises an alarm until the resulting condition no longer occurs.

What is an Event?

An *event* is an occurrence or detection of some condition in and around the network. An event is a distinct incident that occurs at a specific point in time. Examples of events include:

- Port status change
- Device reset
- Device becomes unreachable by the management station

An event can also be a:

- Possible symptom of a fault that is an error, failure, or exceptional condition in the network. For example, when a device becomes unreachable, an unreachable event is triggered.
- Possible symptom of a fault clearing. For example, when a device state changes from unreachable to reachable, a reachable event is triggered.

One or more events may generate an abnormal state or alarm. The alarm can be cleared, but the event remains. You can view the list of events using the Event Browser.

Choose **Operate > Alarms & Events**, then click Events to access the Events Browser page.

Event Creation

Prime Infrastructure maintains an event catalog and decides how and when an event is created and whether to associate an alarm with the event. Multiple events can be associated to the same alarm.

Prime Infrastructure discovers events in the following ways:

- By receiving notification events and analyzing them; for example, syslog and traps.
- By automatically polling devices and discovering changes; for example, device unreachable.
- By receiving events when a significant change occurs in the Prime Infrastructure server; for example, rebooting the server.
- By receiving events when the status of the alarm is changed; for example when the user acknowledges or clears an alarm.

Incoming event notifications (traps and syslogs) are identified by matching the event data to predefined patterns. A trap or syslog is considered supported by Prime Infrastructure if it has matching patterns and can be properly identified. If the event data does not match with predefined patterns, the event is considered as unsupported and it is dropped.

Faults are discovered by Prime Infrastructure through polling, traps, or syslog messages. Prime Infrastructure maintains the context of all faults and ensures that duplicate events or alarms are not maintained in the Prime Infrastructure database.

The following table provides examples of when Prime Infrastructure creates an event.

Time	Event	Prime Infrastructure Behavior
10:00AM PDT December 1, 2011	Device A becomes unreachable.	Creates a new unreachable event on device A.
10:30AM PDT December 1, 2011	Device A continues to be unreachable.	No change in the event status.
10:45AM PDT December 1, 2011	Device A becomes reachable.	Creates a new reachable event on device A.
11:00AM PDT December 1, 2011	Device A stays reachable.	No change in the event status.
12:00AM PDT December 1, 2011	Device A becomes unreachable.	Creates a new unreachable event on device A.

What is an Alarm?

An *alarm* is a Prime Infrastructure response to one or more related events. If an event is considered of high enough severity (critical, major, minor, or warning), Prime Infrastructure raises an alarm until the resulting condition no longer occurs.

One or more events can result in a single alarm being raised. An alarm is created in the following sequence:

1. A notification is triggered when a fault occurs in the network.
2. An event is created, based on the notification.
3. An alarm is created after checking if there is no active alarm corresponding to this event.

An alarm is associated with two types of events:

- Active events: Events that have not been cleared. An alarm remains in this state until the fault is resolved in a network.
- Historical events: Events that have been cleared. An event changes its state to an historical event when the fault is resolved in a network.

After an alarm is cleared, it indicates the end of an alarm life cycle. A cleared alarm can be revived if the same fault reoccurs within a preset period of time. The present period is set to 5 minutes in Prime Infrastructure.

Event and Alarm Association

Prime Infrastructure maintains a catalog of events and alarms. The catalog contains the list of events managed by Prime Infrastructure, and the relationship among the events and alarms. Events of different types can be attached to the same alarm type.

When a notification is received:

1. Prime Infrastructure compares an incoming notification against the event and alarm catalog.
2. Prime Infrastructure decides whether an event has to be raised.

3. If an event is raised, Prime Infrastructure decides whether the event triggers a new alarm or associates it to an existing alarm.

A new event is associated with an existing alarm, if the new event triggered is of the same type and occurs on the same source.

For example, an active interface error alarm. The interface error events that occur at the same interface, are all associated to the same alarm.

Alarm Status

Table 11-1 describes the alarm statuses.

Table 11-1 Alarm Status Descriptions

Alarm Status	Description
New	When an event triggers a new alarm or an event is associated with an existing alarm.
Acknowledged	When you acknowledge an alarm, the status changes from New to Acknowledged.
Cleared	An alarm can be in these statuses: • Auto-clear from the device—The fault is resolved on the device and an event is triggered for the same. For example, a device-reachable event clears the device-unreachable event. This in-turn, clears the device-unreachable alarm. • Manual-clear from Prime Infrastructure users: You can manually clear an active alarm without resolving the fault in the network. A clearing event is triggered and this event clears the alarm. • If the fault continues to exist in the network, a new event and alarm are created subsequently based on the event notification (traps/syslogs).

Event and Alarm Severity

Each event has an assigned severity. Events fall broadly into the following severity categories, each with their associated color in Prime Infrastructure:

- Flagging—Indicates a fault: Critical (red), Major (orange), Minor (yellow), or Warning (sky blue).
- Informational—Info (blue). Some of the Informational events clear the flagging events.

For example, a Link Down event might be assigned a Critical severity, while its corresponding Link Up event will be an Informational severity.

In a sequence of events, the event with the highest severity determines the severity of the alarm.

Where to Find Alarms

Table 11-2 lists the places where you can find alarms.

Table 11-2 Where to Find Alarms

Location in GUI	Description
Operate > Alarms & Events	Displays a new page listing all alarms with details such as severity, status, source, timestamp. You can change the status of alarms, assign, annotate, delete, and specify email notifications from this page.
Rest your cursor on **Alarm Summary**	Displays a table listing the critical, major, and minor alarms currently detected by Prime Infrastructure.
Alarm Browser	Opens a window that displays the same information as in the **Operate > Alarms & Events** but does not take you to a new page.
From device 360° view	Click the Alarms tab to view alarms on the device, their status and category, or click the Alarm Browser icon to launch the Alarm Browser.
Operate > Monitoring Dashboard > Incidents	Displays dashlets that contain alarm summary information, top sites with the most alarms, top alarm types, top events, and top interfaces with issues.

Defining Thresholds

You use monitoring templates to define thresholds. When the thresholds you specify are reached, Prime Infrastructure issues an alarm.

To define thresholds:

Step 1 Choose **Design > Monitoring Templates**.

Step 2 Under Features, choose **Threshold**.

Step 3 Complete the basic template fields.

Step 4 Under Feature Category, choose one of the following metrics:

- Device Health—allows you to change threshold values for CPU utilization, memory pool utilization, and environment temperature
- Interface Health—allows you to change threshold values for the number of outbound units that are discarded, inbound and outbound utilization, and other health parameters.

Step 5 Under Metric Parameters, choose the threshold setting you want to change, then click **Edit Threshold Setting**.

Step 6 Enter a new value and choose the alarm severity when the threshold is met or exceeded.

Step 7 Click **Done**.

Step 8 Click **Save as New Template**.

Step 9 Under the My Templates folder, navigate to the template you created and select it.

Step 10 Click **Go to Deployment**.

Step 11 Choose the template you created, then click **Deploy**.

Getting Help for Alarms

Prime Infrastructure provides helpful tools for network operators to connect to Cisco experts to diagnose and resolve problems. If you receive an alarm for which you need help troubleshooting, Prime Infrastructure allows you to:

- Connect with the Cisco Support Community to view and participate in discussion forums. See Launching Cisco Support Community.
- Open a support case Cisco Technical Support. See Opening a Support Case.

Launching Cisco Support Community

If you receive an alarm in **Operate > Alarms & Events**, you can use Prime Infrastructure to view discussion forums on the Cisco Support Community. By viewing and participating in the Cisco Support Community forums, you can find information that can help you diagnose and resolve problems. You must enter your Cisco.com username and password to view and participate in the Cisco Support Community forums.

Step 1 Chose **Operate > Alarms & Events**, then rest your mouse over the IP address of the device on which the alarm occurred.

Step 2 From the device 360° view, click the **Support Community** icon.

Step 3 On the Cisco Support Community Forum page, enter additional search parameters to refine the discussions that are displayed.

Opening a Support Case

If you receive an alarm in **Operate > Alarms & Events** for which you cannot find a resolution in the Cisco Support Community (see Launching Cisco Support Community), you can use Prime Infrastructure to open a support request and to help you gather critical information to be attached to the support case. You must enter your Cisco.com username and password to open a support case.

Note You must have a direct internet connection on the Prime Infrastructure server in order to access the Cisco Support Community and to open a support case.

Step 1 To open a support case, click **TAC Service Requests** in the lower right corner of the Prime Infrastructure window.

Step 2 Enter your Cisco.com username and password.

Step 3 Click Create New Case.

Prime Infrastructure gathers information about the device and populates the fields for which it can retrieve information. You can enter a Tracking Number that corresponds to your own organization's trouble ticket system.

Step 4 Click **Next** to enter a description of the problem.

By default, Prime Infrastructure enters information that it can retrieve from the device. Prime Infrastructure automatically generates the necessary supporting documents such as the technical information for the device, configuration changes, and all device events over the last 24 hours.You can also upload files from your local machine.

Step 5 Click **Create Service Request**.

Changing Alarm Status

You can remove an alarm from the list of alarms by changing its status to acknowledged or cleared. No e-mails will be generated for these alarms.

Step 1 Choose **Operate > Alarms & Events**.

Step 2 Click the expand icon next to an alarm.

Step 3 Choose **Change Status > Acknowledge** or **Clear**.

When to Acknowledge Alarms

You may want certain alarms to be removed from the Alarms List. For example, if you are continuously receiving an interference alarm from a certain device, you may want to stop that device from being counted as an active alarm on the Alarm Summary page or any alarms list. In this scenario, you can find the alarm for the device in the Alarms list, select the check box, and choose **Acknowledge** from the Select a command drop-down list.

Now if the device generates a new violation on the same interface, Prime Infrastructure will not create a new alarm, and the Alarm Summary page shows no new alarms. However, if the interference violation is created on another interface, a new alarm is created.

By default, acknowledged alarms are not displayed in either the Alarm Summary page or any alarm list page. Also, no emails are generated for these alarms after you have marked them as acknowledged. By default, acknowledged alarms are not included for any search criteria. To change this default, go to the **Administration > System Settings > Alarms and Events** page and disable the **Hide Acknowledged Alarms** preference.

When you acknowledge an alarm, the following warning appears as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled.

Note When you acknowledge an alarm, a warning displays as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled. Use the **Administration > User Preferences** page to disable this warning message.

You can also search for all previously acknowledged alarms to reveal the alarms that were acknowledged during the last seven days. Prime Infrastructure automatically deletes cleared alerts that are more than seven days old so your results can only show activity for the last seven days. Until an existing alarm is deleted, a new alarm cannot be generated for any managed entity for which Prime Infrastructure has already generated an alarm.

Including Acknowledged and Cleared Alarms in Searches

By default, acknowledged and cleared alarms are not included for any search criteria. To change this default, choose **Administration > System > Alarms and Events** and disable the Hide Acknowledged Alarms or Hide Cleared Alarms preference.

Cleared alarms remain in the Prime Infrastructure database, but in the Clear state. You clear an alarm when the condition that caused it no longer exists.

Changing Alarm and Event Options

To change alarm and event options such as when alarms are deleted, which alarm severities are displayed, and alarm email options:

Step 1 Choose **Administration > System Settings > Alarms and Events**.

Step 2 Change the necessary settings for the alarms.

Step 3 Click **Save**.

Configuring Alarm Severity Levels

To configure the severity level for newly generated alarms:

Step 1 Choose **Administration > System Settings**.

Step 2 From the left sidebar menu, choose **Severity Configuration**.

Step 3 Select the check box of the alarm condition whose severity level you want to change.

Step 4 From the Configure Security Level drop-down list, choose a severity level, then click **Go**.

Step 5 Click **OK** to confirm the changes.