Concepts

This section provides information on the following topics:

Concepts

This chapter explains the concepts that are key to Cisco Prime Collaboration Assurance.

Event

An event is a distinct incident that occurs at a specific point in time.

An event is 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, an event is triggered.

Examples of events include:

- Port status change
- Node reset
- Node becoming reachable for the management station
- Connectivity loss between routing protocol processes on peer routers

Events are derived from incoming traps and notifications, detected status changes (by polling), and user actions.

It is important to understand that an event, once it occurs, does not change its status even when the conditions that triggered the event are no longer present.

Choose **Monitor** > **Alarms & Events** to view the list of events.

Alarm

The life cycle of a fault scenario is called an alarm.

An alarm:

- Is a Cisco Prime Collaboration Assurance response to events it receives.
- Is a sequence of events, each representing a specific occurrence in the alarm life cycle (see below example). In a sequence of events, the event with the highest severity determines the severity of the alarm.
- Represents a series of correlated events that describe a fault occurring in the network.
- Describes the complete event life cycle, from the time that the alarm is raised (when the fault is first detected) until it is cleared and acknowledged.

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

Cisco Prime Collaboration Assurance constructs alarms from a sequence of correlated events. A complete event sequence for an alarm includes a minimum of two events:

- Alarm active (for example, an interface down event raises an alarm).
- Alarm clear (for example, an interface up event clears the alarm).

The lifecycle of an alarm can include any number of correlated events that are triggered by changes in severity, updates to services, and so on.

When a new related event occurs, Cisco Prime Collaboration Assurance correlates it to the alarm and updates the alarm severity and message text based on the new event. If you manually clear the alarm, the alarm severity changes to cleared.

You can view the events that form an alarm in the Alarms and Events browser.

Choose **Monitor** > **Alarms & Events** to view the list of alarms.

Event Creation

Cisco Prime Collaboration Assurance maintains an event catalog and decides how and when an event has to be created and whether to associate an event with an alarm. Multiple events can be associated to the same alarm.

Cisco Prime Collaboration Assurance 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 the status of the alarm is changed; for example, when the user clears an alarm.

Cisco Prime Collaboration Assurance allows you to disable monitoring of events that may not be of importance to you. The events that are disabled are not listed in the Alarms and Events browser. Also, Cisco Prime Collaboration Assurance does not trigger an alarm.

Incoming event notifications received as syslogs or traps are identified by matching the event data to predefined patterns. An event is considered supported by Cisco Prime Collaboration Assurance 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.

The following table illustrates the Cisco Prime Collaboration Assurance behavior while it deals with event creation:

Time	Event	Cisco Prime Collaboration Assurance Behavior
10:00AM PDT June 7, 2012	Device A becomes unreachable	Creates a new Unreachable event on device A.
10:30AM PDT June 7, 2012	Device A continues to be in the unreachable state.	No change in the event status.
10:45AM PDT June 7, 2012	Device A becomes reachable.	Creates a new Reachable event on device A.
11:00AM PDT June 7, 2012	Device A stays reachable	No change in the event status.
12:00AM PDT June 7, 2012	Device A becomes unreachable.	Creates a new Unreachable event on device A.

Alarm Creation

An alarm represents the life cycle of a fault in a network. Multiple events can be associated with a single alarm.

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 cleared. See Alarm Status to know how an alarm is cleared.

The alarm life cycle ends after an alarm is cleared. A cleared alarm can be revived if the same fault recurs within a preset period of time.

For Cisco Prime Collaboration Assurance, the preset period is 60 minutes.

Event and Alarm Association

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

When a notification is received:

1. Cisco Prime Collaboration Assurance compares an incoming notification against the event and alarm catalog.
2. Cisco Prime Collaboration Assurance decides whether an event has to be raised.
3. If an event is raised, Cisco Prime Collaboration Assurance decides whether the event should trigger a new alarm or associate 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.

An active interface error alarm is an example. All interface error events that occur on the same interface, are associated to the same alarm.

If any event is cleared, its severity changes to informational.

Note Some events have default severity as informational. For these events, alarms will not be created. If you want Cisco Prime Collaboration Assurance to create alarms for these events, you must change the severity of these events.

Event Aggregation

If the number of same event received from a set of elements exceeds a specified threshold, Cisco Prime Collaboration Assurance creates an alarm.

Example use cases:

- Number of unregistered phones on a device pool / Unified CM location is more than 5%.
- Number of service quality issues experienced on a device pool / Unified CM location is more than 5%
- All the call quality events raised against a single poor-quality call are grouped.

Event Masking

Cisco Prime Collaboration Assurance automatically masks the hierarchy of events when the top-level component is the cause for the issue, and raises an alarm against the top level component while masking all the downstream events.

Example use cases:

- When a Unified CM goes down, Cisco Prime Collaboration Assurance masks all its component (such as powersupply, interface, fan) events.
- When a switch card goes down, Cisco Prime Collaboration Assurance masks all the contained port level events.

Alarm Status

The following are the supported statuses for an alarm:

Table 1: Alarm Status

Status	Description
Not Acknowledged	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 Not Acknowledged to Acknowledged
Cleared	• System-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 alarm. • Alarms are also triggered during the conference because of packet loss, jitter, and latency. These alarms are auto-cleared after the conference ends. • Manual-clear from Cisco Prime Collaboration Assurance 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 polling. • Auto-clear from the Cisco Prime Collaboration Assurance server—Cisco Prime Collaboration Assurance clears all conference-related alarms, when the conference ends. If there are no updates to an active alarm for 24 hours, Cisco Prime Collaboration Assurance automatically clears the alarm. **Note** Certain alarms might get cleared automatically before 24 hours. See Supported Events and Alarms for Prime Collaboration.

Event Severity

Each event has an assigned severity, and can be identified by its color in Cisco Prime Collaboration Assurance.

Events fall broadly into the following severity categories:

- 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.

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

Cisco Prime Collaboration Assurance allows you to customize the settings and severity of an event. The events that are of importance to you can be given higher severity.

The event settings and severity predefined in the Cisco Prime Collaboration Assurance application is used if you have not customized the event settings and severity.

Event and Alarm Database

All events and alarms, including active and cleared, are persisted in the Cisco Prime Collaboration Assurance database.

The relationships between the events are retained. The Alarm and Event Browser allows you to review the content of the database. The purge interval for this data is four weeks.

Note Events are stored in the form of the Cisco Prime Collaboration Assurance event object. The original notification structure of incoming event notifications (trap or syslog) is not maintained.

Alarm Notifications

Cisco Prime Collaboration Assurance allows you to subscribe to receive notifications for alarms. Cisco Prime Collaboration Assurance sends notifications based on user-configured alarm sets and notification criteria.