Fault Management Overview

Cisco Prime Collaboration ensures near-real time quick and accurate fault detection. After identifying the event, Prime Collaboration groups related events, creates alarms, and performs fault analysis to determine the root cause of the fault in a network.

Prime Collaboration allows you to monitor the events that are of importance to you. You can customize the event severity and enable to receive notifications from Prime Collaboration, based on the severity. Prime Collaboration monitor events from the endpoints and service infrastructure devices.

This chapter explains the concepts that are key to the Prime Collaboration fault management framework.

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.
Alarms

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

An alarm:

- Is the Prime Collaboration 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.

Prime Collaboration 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, Prime Collaboration 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.

Event Creation

Prime Collaboration 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.

Prime Collaboration 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.

Prime Collaboration allows you to disable monitoring of events that may not be of importance to you. The events that are disabled will not be listed in the Alarms and Events browser. Also, Prime Collaboration will not trigger the 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 Prime Collaboration 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 Prime Collaboration behavior while it deals with event creation:
Alarm Creation

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

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, page 1-5 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 reoccurs within a preset period of time.

For Prime Collaboration, the preset period is 60 minutes.

Event and Alarm Association

Prime Collaboration maintains a catalog of events and alarms. The catalog contains the list of events managed by Prime Collaboration, 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. Prime Collaboration compares an incoming notification against the event and alarm catalog.
2. Prime Collaboration decides whether an event has to be raised.
3. If an event is raised, Prime Collaboration 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.

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Prime Collaboration Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:00AM PDT June 7, 2012</td>
<td>Device A becomes unreachable</td>
<td>Creates a new Unreachable event on device A.</td>
</tr>
<tr>
<td>10:30AM PDT June 7, 2012</td>
<td>Device A continues to be in the unreachable state.</td>
<td>No change in the event status.</td>
</tr>
<tr>
<td>10:45AM PDT June 7, 2012</td>
<td>Device A becomes reachable.</td>
<td>Creates a new Reachable event on device A.</td>
</tr>
<tr>
<td>11:00AM PDT June 7, 2012</td>
<td>Device A stays reachable</td>
<td>No change in the event status.</td>
</tr>
<tr>
<td>12:00AM PDT June 7, 2012</td>
<td>Device A becomes unreachable.</td>
<td>Creates a new Unreachable event on device A.</td>
</tr>
</tbody>
</table>
An active interface error alarm is an example. All interface error events that occur at 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 Prime Collaboration to create alarms for these events, you must change the severity of these events.

## Event and Alarm Correlation

Event correlation is the process of relating one event to other events.

Prime Collaboration distinguishes two event relationship types:

- An event sequence. Events that have the same type and the same source are considered part of an event sequence, or an alarm. An alarm represents the complete lifecycle of a fault.
- An event sequence hierarchy (alarms), representing causality.

Prime Collaboration associates a new event to an existing alarm if the existing alarm has the same event type and source as the new event.

Prime Collaboration raises an alarm, if the number of related events received (by fault management system) from the device element exceeds a specified threshold in a specified unit of time, based on predefined correlation rules. See [Alarm Correlation Rules](#).

Example use cases:

- Call Manager location goes out-of-resource for more than 5 times over the last one hour.
- CPU usage of a device is over 80% for last 15 minutes.

You can modify these rules and configure the number of event occurrences to set the trigger. This can vary from two to 100. You can also set the time interval. You can modify these rules at [Administration > Alarm & Event Configuration > Rules Settings](#). See [Modifying Alarm Correlation Rules](#) for details.

If an administrator does not specify a time interval, maximum time period, or a count for a specific alarm, the default values for the time interval, maximum time period, and count is attached on an alarm, device type, or device class basis.

## Event Aggregation

Prime Collaboration indicates by an alarm, if the number of same event received from a set of elements exceeds a specified threshold.

Example use cases:

- Number of unregistered phones on a device pool / Unified CM location crosses more than 5%.
- Number of service quality issues experienced on a device pool / Unified CM location crosses more than 5%
- Group all the call quality events raised against a single poor-quality call.
- Route group / site level utilization from the trunk associated to the site.
- Multiple TelePresence peripherals experiencing same error (For example, microphone / HDMI cable disconnected), generate one alarm for the device.
• Multiple endpoints of a conference experiencing degraded quality.

Event Masking

Using event masking (also known as topological masking) Prime Collaboration ignores events pertaining to systems that are downstream of a failed system.

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

Example use cases:
• When a Call Manager goes down, Prime Collaboration masks all its component (such as powersupply, interface, fan) events.
• When a switch card goes down, Prime Collaboration masks all the contained port level events.

Alarm Status

The following are the supported statuses for an alarm:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Acknowledged</td>
<td>When an event triggers a new alarm or an event is associated with an existing alarm.</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>When you acknowledge an alarm, the status changes from Not Acknowledged to Acknowledged</td>
</tr>
</tbody>
</table>
| 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 session because of packet loss, jitter, and latency. These alarms are auto-cleared after the session ends.  
                          • Manual-clear from Prime Collaboration 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 Prime Collaboration server—Prime Collaboration clears all session-related alarms, when the session ends.  
                          If there are no updates to an active alarm for 24 hours, Prime Collaboration automatically clears the alarm.  
| Note                 | Certain alarms might get cleared automatically before 24 hours. See Supported Alarms for Prime Collaboration and Supported Events for Prime Collaboration. |
Event Severity

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

Prime Collaboration allows you to customize the settings and severity of an event. The events that are of importance to you can be given higher severity. See Customizing Alarms and Events to know how to customize the event settings and severity.

The event settings and severity predefined in the Prime Collaboration 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 Prime Collaboration database. The relationships between the events are retained. The content of the database can be reviewed, using the Alarm and Event Browser. The purge interval for this data is four weeks.

Note

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

Alarm Notifications

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

See Configuring Alarm and Event Notification for details about how to configure for notifications.