CHAPTER 5

Understanding Events

Fault management is the process of locating, diagnosing, and reporting network problems. This is important for increasing network reliability and effectiveness, and for increasing the productivity of network users. Fault management is more than just handling emergencies. It provides functions for managing problems with services and handling customer-facing service problems.

Efficient fault management can:

- Save repair costs through efficient fault detection, location, and correction
- Improve customer care through efficient trouble administration
- Improve service availability and equipment reliability through proactive maintenance and through measurement, review, and corrective action

One responsibility of fault management is to detect faults. A piece of equipment, a transmission medium, a software module, or a database is said to be in a fault state if it cannot perform its intended function and meet all of the requirements placed on that function. The onset of a fault is called a *failure event* and is usually signaled by one or more event reports. The termination of a fault state is called a *clear event*.

Fault management is responsible for determining, from a variety of information sources, the root cause of a fault, and for its repair. In certain cases, the root cause of a fault might be in a connecting network. In such cases, fault management is responsible for reporting the problem through appropriate channels.

The steps for successful fault management are:

1. Identify a problem by gathering data about the state of the network (polling and trap generation).
2. Restore any services that have been lost.
3. Isolate the cause, and decide if the fault should be managed.
4. Correct the fault.

In Prime Central for HCS 9.2.1, events sent by the CUCDM servers are also processed. To enable this feature, configure the CUCDM servers SNMP destination to send the traps to the Event Collector IP of the Prime Central for HCS deployment.

Note As of now only the Event Collector receives the traps from CUCDM, processes and makes it available in all the event's browsers and in the Prime Central for HCS BNI interface. Enrichment, RCA, and SIA are not performed for the CUCDM events.

A fault in Prime Central for HCS parlance is called an event. Prime Central for HCS processes all events reported by domain managers and performs service assurance functions such as event enrichment, event normalization, root-cause analysis, and service impact analysis. The events are reported in Alarm Browser - All Events portlet. Prime Central for HCS supports all events from the following domain managers:

- CUOM/CUSM (multi-tenant CUOM)
- UCS Manager
- DCNM SAN
- DCNM LAN

Note DCNM is an optional component in Prime Central for HCS 9.2.1. If you are not using DCNM in your deployment, skip tasks and sections related to DCNM.

This chapter contains the following sections:

Understanding the Lifecycle of an Event

The managed domain managers receive events (syslogs and traps) from network elements and perform the first level of event correlation. Prime Central for HCS receives correlated events from the domain managers and performs second-level, cross-domain event correlation and deduplication. It then provides an aggregated view of correlated and deduplicated event to network operation center (NOC) operators.

Prime Central for HCS performs the following main functions:

- Receives events from domain managers.
- Normalizes the events to a common events representation to perform aggregation, deduplication, correlation, and enrichment.

Events entering Prime Central for HCS are first classified and marked with EventTypeID, which is used as identifier of these event classes. Sets of events can be processed using the same rules and have the same kind of service impact. EventTypeID groups all supported events in event categories of events that can each be handled in the same way. Events having the same EventTypeID receive synthetic events that are generated for EventTypeID. Correlation rules will be written only among these synthetic events.

When an event gets generated, Prime Central for HCS first classifies the event based on several parameters, such as the domain manager, event type, device. Later, based on the inference, it either passes on the events not supported to the Northbound interface or performs the next stages of processing.

The events that are supported are enriched with more data, such as customer details and are again classified.

The events are then analyzed for root cause of the issue, or the service impact of the event is analyzed.

In Prime Central for HCS, events are of various types:

- Normalized-only events—Events that Prime Central for HCS receives and normalizes. These events are not enriched further. It passes on the events directly to northbound system without additional processing. These events are marked with EventTypeID=default.

- Enriched events—After normalization, some events are enriched with additional information. For example, CUOM events are enriched with the CustomerName, the VM Name in which the UC application is running, and others. Some of the enriched events are used to determine its impact on customer services by overlaying them on the service impact tree.
- Root-cause events—Synthetic events that were determined to be root-cause of the failure.
- Symptomatic events—Synthetic events that were part of event correlation but were determined not to be root-cause of the failure.
- Synthetic Events—These are events generated internally to indicate a category of events. For example, all Service Down events on a CUCM node, which indicate that services running on the CUCM node are down, are grouped under the Synthetic event named OM_CUCM_Processes. Synthetic events are used to build the correlation tree used for root cause analysis. For more information on synthetic events, see *Cisco Prime Central for Hosted Collaboration Solution Programmer Guide*.
- Service-impact events—Service-impact events describe the state of services; this is an event generated to notify the state of the top node in the service impact tree.

The events that are reported from the underlying domain managers are presented in the Alarm Browser - All Events portlet.

The following sections explain the various stages of event processing:

From the Alarm Browser, click on **Event Details > Description** to view the description of the event as provided by the Domain Manager. After selecting an event, you can also right-click and click on **Event Details > Next steps** to view the Recommended Actions as provided by the Domain Manager.

Event Normalization and Enrichment

All events reported from the domain managers are normalized to a common format. Alarm Browser - All Events portlet presents the events, and the associated details, in a common format. Based on the event type, Prime Central for HCS enriches the reported events with additional data. The level of detail that Prime Central for HCS presents in the Alarm Browser - All Events portlet depends on various parameters.

After Prime Central for HCS identifies an event that is supported, it enriches the event with the following information:

- DeviceId— IP or hostname of the device that originated the event and sent it to the domain manager. For example, CUCM hostname, Router management IP/hostname.
- Component—The component for which the event is raised. It can be a device or its sub-component.
- Original Severity—Original severity of the raw event received from domain manager. Prime Central for HCS later maps the event to an equivalent severity that is common across all events. Table 5-2 explains the mapping of severity between domain managers and Prime Central for HCS
- Summary—A brief event description that helps you to interpret the event.
- Prime Central for HCS Severity—Prime Central for HCS maps the severity of the event with an equivalent severity level. Severity of the synthetic event will be the severity of the first event that creates the synthetic event. For synthetic root cause events, severity is marked as Critical.

Prime Central for HCS enriches all events that originate from a device that is dedicated to a single customer with the following:

- CustomerName—Identifies customer that components belongs to. Value of this field is obtained from the event itself for CUOM events and from the SDR for some IM events (primarily VM related events).
- CustomerextName—External customer name.

Table 5-1 Level of Event Enrichment Based on Various Parameters

Field Name	Normalized-Only Events	Enriched-Only Events	Root-Cause Events	Symptomatic Events	Service Impact Events
EventIdentifier	Yes	Yes	Yes	Yes	Yes
EventName	Yes (only for CUOM, UCSM, Infrastructure Monitoring)	Yes (only for CUOM, UCSM, Infrastructure Monitoring)	—	—	—
Summary	Yes	Yes	Yes	Yes	Yes
ComponentId	Yes (only for CUOM, UCSM, Infrastructure Monitoring)	Yes (only for CUOM, UCSM, Infrastructure Monitoring)	—	—	—
DeviceId	Yes	Yes	Yes	Yes	—
DomainManagerID	Yes	Yes	No	—	—
Customer[1]	—	Yes (Only CUOM and Infrastructure Monitoring VM events)	Yes (Only CUOM and Infrastructure Monitoring VM events)	Yes (Only CUOM and Infrastructure Monitoring VM events)	Yes
CustomerExtName [2]	—	Yes (Only CUOM and Infrastructure MonitoringVM events)	Yes (Only CUOM and Infrastructure MonitoringVM events)	Yes (Only CUOM and Infrastructure Monitoring VM events)	Yes
CauseType	Yes (set to Unknown)	Yes (set to Unknown)	Yes (set to Rootcause)	Yes (set to Symptom)	—
ParentEventId	—	—	Yes	Yes	—
Severity	Yes	Yes	Yes	Yes	Yes
OriginalSeverity	Yes	Yes	—	—	—
EventTypeId	—	Yes	Yes	Yes	—

Table 5-1 Level of Event Enrichment Based on Various Parameters (continued)

Field Name	Normalized-Only Events	Enriched-Only Events	Root-Cause Events	Symptomatic Events	Service Impact Events
ProblemeventID	Yes	Yes	Yes	Yes	Yes
ServiceName (for service events only)	—	—	—	—	Yes
ServiceImpactType (for service events only)	—	—	—	—	Yes
OperationalDataPointer	Yes (only for CUOM, UCSM, Infrastructure Monitoring)	Yes (only for CUOM, UCSM, Infrastructure Monitoring)	—	—	—

1. The Customer field is not part of the CUBE-SP event's (subclassification of OM events) field names.
2. CustomerExtName field is not part of the CUBE-SP event's field names.

Event Deduplication

When the same event occurs multiple times, Prime Central for HCS reports the event only once. The Alarm Browser - All Events portlet specifies the number of times the event has occurred with the level of severity. Every time an event is deduplicated, the Count field in the event that indicates the number of times the event has occurred, is incremented.

- Performance event. CPU threshold violation occurs 5 times in 15 minutes then update the same CPU high event with count and increase the severity.
- Location BW violation occurs 5 times in 15 minutes then update the same Location BW event with count and increase the severity.
- Service Quality Event. MOS score below a defined threshold occurs 10 times in 30 minutes; update the same quality degradation event with count and increase the severity.

Event Suppression

You can configure Prime Central for HCS to discard certain events that are not of interest to you. The Event Suppression feature discards certain incoming events from the underlying domain managers. These discarded events are not seen in the Alarm Browser - All Events portlet and not notified to northbound systems.

Event Suppression script creates a procedure after reading inputs from a filter specification file and installs the procedure on to the Event Collector database. Incoming events that match the filter conditions are not inserted into the database. These events are also not forwarded to the Northbound OSS systems.

The following options are supported:

The directory where the load-event-suppression-filters.pl is located:

cd <*prime_installation_directory*>**/prime-hcs/scripts**

Usage: **load-event-suppression-filters.pl -f <*filter-xml*> | -r**

Where,

- -f <*filter-xml*>: is an XML file that configures the perl load-event suppression filter
- -r: Remove suppression filter

Example Usage:

```
load-event-suppression-filters.pl -f filters.xml
```

To Configure Event Suppression Filter

You can configure Event Suppression filter by following the procedure explained below. This command generates a SQL procedure and remotely installs the procedure on EC server database.

Step 1 Log into the Prime Central server as **primeusr**.

Step 2 Execute the following command.
cd <*prime_installation_directory***>/prime-hcs/scripts**

```
perl load-event-suppression-filters.pl -f file-name
```

To Remove Event Suppression Filter:

Step 1 Log into the Prime Central server as **primeusr**.

Step 2 Create a filter specifications XML file (format described below). For example, cuom-filter.xml.

Step 3 Execute the following command:

```
perl load-event-suppression-filters.pl -r
```

Filter File Format:

The XML file format is self-explanatory. The suppression filters have to be grouped together within <*suppression filter*> element. Each <*suppression filter*> represents the Filter expression. Each element within the <*suppression filter*> element is the name of the column in alarm browser; the element is matched against the specified value. It is not mandatory for all filter elements to be present in a filter expression. Following columns are supported:

- CustomerName
- EventTypeId
- DeviceId
- ComponentId

A special element WhereCondition is supported, in which you can specify an ANSI SQL-compliant WhereCondition similar to NBI Gateway filter.

The supported list of filterable columns and types, which can be specified in the <*WhereCondition*> is available in *Cisco Prime Central for Hosted Collaboration Solution Programmer Guide*.

Follow the guidelines mentioned below when specifying a filter:

- Within a specific filter, the filter elements are applied with 'AND'
- When there are multiple filters defined, all filter conditions are applied with 'OR'

An example of the file contents:

```
<suppressionFilters>
  <!--
 <suppressionFilter>
  <CustomerName>hello_1</CustomerName>
  <EventTypeId>event_type_1</EventTypeId>
  <DeviceId>node_001</DeviceId>
  <ComponentId>fe1/1</ComponentId>
  <WhereCondition>EventTypeId LIKE 'OM_CUCM%'</WhereCondition>
 </suppressionFilter>
 -->
 <suppressionFilter>
  <EventTypeId>OM_CUCM_SIP_Trunks</EventTypeId>
  <DeviceId>HCM-SA-CUCM-1</DeviceId>
 </suppressionFilter>
 <suppressionFilter>
  <EventTypeId>OM_CUCM_Connectivity</EventTypeId>
  <ComponentId>HCM-SA-CUCM-1</ComponentId>
 </suppressionFilter>
</suppressionFilters>
```

Event Filtering

The Filter option allows you to narrow down the displayed data in the Alarm Browser - All Events portlet. Filtering provides a quick and easy way to identify a specific record that matches the given criteria, provided by you.

The events can also be filtered using APIs. For more information on filtering, see *Cisco Prime Central for Hosted Collaboration Solution Programmer Guide*.

Event Flapping

Prime Central for HCS marks an event as Flapping when an event occurs *x* times in *y* seconds. The values *x* and *y* are called FlappingThreshold and FlappingInterval. These values are configured in the custom.flappingproperties database table in the Event Collector. You are allowed to change the FlappingInterval and FlappingThreshold values.

To change the values, do the following:

Step 1 Log into the Event Collector as **netcool**.

Step 2 Connect to Objectserver using **nco_sql**:

```
nco_sql -user <user_name> -password <password>
```

Step 3 Run the following SQL query to update the FlappingInterval and FlappingThreshold:

update custom.flappingproperties Set FlappingInterval=<*time_in_seconds*>, FlappingThreshold=<*No_of_occurences*> where EventName=*'default'*;

go

When Prime Central for HCS detects flapping, the EventDescription field collects the flapping details where the Grade field represents the flapping count.

Event Clearing

Prime Central for HCS clears events from the domain managers, based on the following strategy:

It ensures that a problem event in the Alarm Browser - All Events portlet is automatically cleared when the underlying fault in the network is fixed. For example, if a service in a UC node is shut down, a Service down event is raised. Later if the service is restarted, the Service down event is automatically cleared in the Alarm Browser - All Events portlet.

Prime Central for HCS does not support clearing of problem events from DCNM LAN and DCNM SAN That is, when the underlying fault is fixed, the problem event is not cleared immediately. You can configure the clearing time for these problem events and the default value is 60 minutes.

Note DCNM is an optional component in Prime Central for HCS 9.2.1. If you are not using DCNM in your deployment, skip tasks and sections related to DCNM.

A synthetic event acts as a container for one or more events. A synthetic event is cleared only if all of its contained events are cleared.

For events that participate in the correlation tree, when a clearing event arrives for a parent event, but not for its active child event, Prime Central for HCS adopts the following approach:

1. Prime Central for HCS clears the parent event after it receives the clearing event.
2. A transient state timer starts.
3. If child clearing event arrives during the transient state, Prime Central for HCS clears the active child event. If Prime Central for HCS does not receive a clearing event before the expiry of the transient state period, the state of the child event moves from Active to Undetermined - Uncleared.
4. Such 'Undetermined - Uncleared' events can be viewed in the Alarm Browser - Undetermined events portlet.

If you prefer to clear the event, log into Prime Central for HCS, and clear the event manually. The following table lists the default period (in seconds) at the expiry of which an event is automatically cleared from the dashboard. The events are categorized based on EventTypeIDs. You cannot customize the values.

Table 5-2 Event Type IDs

EventTypeID	Cleared in... (in seconds)
VC_VM_VMOTION	172800
VC_VM_Restored	172800
VC_Host_Resources	259200

Table 5-2 Event Type IDs

EventTypeID	Cleared in... (in seconds)
VC_VM_Resources	259200
VC_Cluster_Resources	259200
If EventType ID is Empty	259200
Non-critical DCNM LAN events	3600

There is no clearing support for the pure events from vCenter and these events remain in the Infrastructure Monitoring until the clearing time. The events are cleared from the Infrasture Monitoring but they are available in Prime Central for HCS. The following is the list of pure events from vCenter that are cleared after the expiry time:

Table 5-3 vCenter Event Type IDs

EventTypeID	Cleared in... (in minutes)
KVM_ESX_Server_Connected_Cisco	15–30
KVM_ESX_Server_Disconnected	15–30
KVM_VM_Connected_Cisco_HCM	15–30
KVM_VM_RestartOnAlt_Host_Cisco	15–30
KVM_VM_Powered_On_Cisco_HCM	15–30
KVM_VM_Powered_Off_Cisco_HCM	15–30
KVM_VM_Disconnected_Cisco_HCM	15–30
KVM_VM_Disk_Latency_Critical	15–30
KVM_VM_Disk_Latency_Warning	15–30
KVM_VM_Disk_Latency_Cleared	15–30

Event Persistence

Prime Central for HCS retains all events reported by domain managers in a relational database. The events can be filtered and searched using the API listed in the section Event Filtering. You can configure Prime Central for HCS to automatically delete events that are older than the configured time period. The default period is 14 days. To change the default value, follow the procedure below:

Step 1 Login as **primeusr.**

Step 2 Go to **cd** <*prime_installation_directory*>**/prime_integrator/DMIntegrator/lib**

Step 3 Unzip the faultmgmtutils-1.0.0.jar file.

Step 4 Edit the **history.size.in.days** property in partitioning.properties file.

Step 5 After you edit the files, archive it back to the jar file format and remove the extracted files.

Step 6 Login to primed database using sqlplus.

`SQL>` **select to_char(lastmodified) from reporter_status where lastmodified < current_date - 1** ;

SQL> select to_char(lastmodified) from reporter_status where lastmodified < current_date - 1 .

Assuming that the paritioning.properties is set with 1 day, the operator can open Active Event List and sort the events in ascending order of first occurrence. Events older than 1 day are not be displayed.

All active events that are still not cleared are stored in the object server. All events including cleared events are persisted in the oracle database (within prime database). Therefore, the event clean-up process essentially cleans up events from the oracle database that are older than X number of days.

The events that are listed in the Alarm Browser is a view of the active events from object server. When you clean up events from the archive database does not affect Alarm Browser view. The clean up process runs every hour and the changes reflect after the process is complete. The log file is available on the Prime Central for HCS server at /AlarmPartitioning.log.

Root Cause Analysis

When a significant fault happens in the HCS system (for example a VM that hosts an UC application fails or a UCS blade fails), numerous events are generated. The Root Cause Analysis feature attempts to determine the root cause event from the numerous events that are seen during this fault condition. For the VM failure scenario, Prime Central for HCS receives several events about the VM and the UC application. It then determines that the VM down event is the root cause for the numerous events seen from the UC application

The root cause events can be displayed by choosing Alarm Browser - Root Cause Events portlet from the Assurance menu.

Once Prime Central for HCS determines the event to be processed for RCA, it enriches the event with the following additional data:

- Prime Central for HCS Severity.
- Operational Data—Troubleshooting and next steps for root-cause event.
- ParentEvent—Indicates the event that is the root cause for this event.
- CauseType—Identifies whether this event was determined to be one of possible root-cause events.

Service Impact Analysis

While root-cause analysis helps differentiate between possible root-cause events and symptomatic events; service impact analysis helps identify whether services were impacted by failure or perhaps failure was not in the path of the service or was protected by redundancy. For more information, see Chapter 7, “Understanding Services”.

Using the Alarm Browser to View Affected Services and Customers

Prime Central provides an Alarm Browser portlet that displays aggregated, deduplicated, and correlated active alarms. Users with the appropriate role can use the Alarm Browser to monitor and manage data about faults in the network. The events that are reported from the underlying domain managers are

presented in the Alarm Browser - All Events portlet. The Alarm Browser - All Events portlet displays the details of the event, including the node details, a summary of the issue, and the number of times the event has occurred.

The colors and the mapping of severity of events are explained in Table 5-4:

Information about alarms is displayed in the portlet according to filters and views:

- Filters let you display a subset of alerts based on specific criteria.
- Views let you choose which alert fields to display.

Table 5-4 Prime Central for HCS and Domain Manager Severity Mapping

Prime Central for HCS Severity	CUOM Severity	UCSM Severity	DCSM-SAN Severity	DCNM-LAN Severity	Infrastructure Monitoring Severity
0—Clear, Green	N/A	0—Clear	—	—	—
1—Indeterminate, Purple	N/A	1—Info	Debugging	Debugging	Informational
2—Warning, Blue	Informational	3—Warning	Info, Notification	Info, Notification	Harmless
3—Minor, Yellow	Warning	4—Minor	Warning	Warning	Warning
4—Major, Orange	N/A	5—Major	Alert, Emergencies	Alert, Emergencies	—
5—Critical, Red	Critical	6—Critical	Error, Critical	Error, Critical	Critical

To open the Alarm Browser - All Events portlet:

Step 1 From the Prime Central menu, choose **Assure > Alarm Browser - All Events**.

Step 2 The first time you launch the Alarm Browser, you must accept the self-signed and untrusted security certificates.

To accept the security certificates in Mozilla Firefox, do the following:

a. At the security prompt, click **I Understand the Risks**.

b. Click **Add Exception**.

c. In the Add Security Exception dialog box, make sure the **Permanently store this exception** check box is checked. (If you leave it unchecked, you will have to reaccept the security certificates the next time you launch the Alarm Browser.) Then, click **Confirm Security Exception**.

d. In the Warning - Security dialog box, check the **Always trust content from this publisher** check box. (If you leave it unchecked, you will have to reaccept the security certificates the next time you launch the Alarm Browser.) Then, click **Yes** to the following message:

```
The web site's certificate cannot be verified. Do you want to continue?
```

Note If you click No, the security certificate is denied, and the Alarm Browser displays the error "The application failed to run."

To accept the security certificates in Microsoft Internet Explorer, do the following:

a. At the security prompt, click **Continue to this website**.

b. In the Internet Explorer Information Bar, choose **Display Blocked Content**.

c. In the Warning - Security dialog box, check the **Always trust content from this publisher** check box. (If you leave it unchecked, you will have to reaccept the security certificates the next time you launch the Alarm Browser.) Then, click **Yes**.

The table displays the following information by default.

Table 5-5 Field Descriptions for the Alarm Browser Portlet

Field	Description	
Severity	Severity of the selected event:	
		Critical event (red)
		Major event (orange)
		Minor event (amber)
		Warning event (sky blue)
		Indeterminate event (dark blue)
		Cleared, normal, or OK (green)
DeviceID	Hostname or IP address of the device where the selected event occurred.	
CauseType	Indicates the type of event—Root Cause, Symptomatic, or Unknown.	
EventTypeID	Indicates the categorization of the event. For example, VC_VM_Avlblty indicates that the event belongs to the category VM Availability.	
Summary	Error message or condition that is associated with the selected event.	
ComponentId	Indicates the component inside the entity in which the event occurred. For example, if the event is a 'Service Down' event, the field is set to the name of the CUCM service that is down.	
Class	Indicates the origin of the event—from one of the following: CUCM, CUCxN, Infrastructure Monitoring, or UCS Manager.	
Last Occurrence	Time stamp when the event last occurred.	
Count	Number of times the event occurred.	
Customer	Name of the customer affected by the event.	

Table 5-5 Field Descriptions for the Alarm Browser Portlet (continued)

Field	Description
CustomerExtName	An alternative CustomerID provided by the customer/service provider for a customer. This field, for example, can be the customer ID assigned to this customer in the SP's northbound OSS system.
Grade	Indicates flapping status—0 indicates no flapping; 1 indicates flapping.
OriginalSeverity	The original severity of the event that was received from the underlying domain manager (CUOM, Infrastructure Monitoring, or UCSM).
EventName	The name of the Event. Event Names are assigned for events from UCS Manager, CUOM and Infrastructure Monitoring. Events from DCNM LAN and DCNM SAN do not have the EventName.
DomainManagerID	The domain manager's IP address from which the event was received.
EsxiHostName	Indicates the ESXi server on which the VM or the application is running (if applicable).
Type	Indicates if this is a 'Problem' event or a 'Resolution' event.
EventIdentifier	The unique Identifier for the event.
ExpireTime	The time at which the event will automatically be cleared. This is set for events that do not have clearing support (for example, events from DCNM LAN and DCNM SAN).
FabAIPAddress	For UCS Manager events, indicates the Fabric A IP address.
FabBIPAddress	For UCS Manager events, indicates the Fabric B IP address.
ProblemEventId	Indicates the 'Problem' Event Identifier for a a 'Resolution' event.
UCSObjectDn	The UCS DN (Distinguished name) such as **sys/chassis/blade-1** for the entity on which the event occurred. Only for UCS Manager events.
OperationalDataPointer	Contains a URL that can be used to fetch more details about the event.
ParentEventID	When this event participates in the correlation tree (for Root Cause Analysis), this field indicates the parent event for this event.

Step 3 To view additional details about a specific event in the Alarm Browser table, double-click the event, or right-click the event and choose **Information**. The Alarm Status dialog box opens.

a. Use the tabs in the event Status dialog box to manage that specific event:

- Fields—Additional fields that are parsed from the event.
- Journal—Enter a journal entry with notes about the event. See Adding Journal Notes to an Event, page 5-16.

b. Click **Close**.

Step 4 You could do one of the following by right-clicking an event:

- If an event is a synthetic event and has CauseType value **Symptom,** right-click the event in the table, and choose **ShowRootCause** to view the root cause of this event.
- If an event is a synthetic event and has CauseType value **RootCause,** right-click the event in the table, and choose **ShowSymptoms** to view the symptoms of this event.
- If an event is a synthetic event, right click the event in the table and choose **ShowContainment** to view the underlying raw events the event contains. For example, for the VC_VM_Avlblty synthetic event, the contained raw events could be VC_VM_Powered_Off and VC_VM_Disconnected.

- Right click an event (a CUOM, UCS Manager or Infrastructure Monitoring event) in the table, and choose **EventDetails > Event_Details** to show the documentation or description of what the event represents.
- Right click on an event (a CUOM, UCS Manager or Infrastructure Monitoring event) in the table and choose **EventDetails > Operations_Data** to show the Next Step that can be adopted to resolve this event.

Prime Central identifies the relationship between a root cause event and its consequent events. It automatically correlates the consequent events as children of the root event. The Alarm Browser displays the root cause event and the severity of the root cause event. In addition, the Alarm Browser displays the time at which the original event was detected.

Working with the Alarm Browser - All Events Table

The various events that arise from the domain managers are listed in the Alarm Browser - All Events table. As an administrator or operator, you can select an event listed on the table and perform various activities such as prioritizing an event, deleting an event. This section contains the following topics:

Acknowledging and Deacknowledging Events

You can acknowledge and deacknowledge event within Prime Central for HCS. The acknowledgement or deacknowledgement does not propagate back to the domain managers.

Step 1 To acknowledge an event, right-click an event in the Alarm Browser and choose **Acknowledge**.

Step 2 To deacknowledge a previously acknowledged event, right-click the event and choose **De-acknowledge**.

Prioritizing an Event

You can change the default priority that Prime Central for HCS assigns to an event. You can change the severity of events only if you have permission to do so, and you can change only the severity of events assigned to you, your group, or the *nobody* user.

Select an event from Active Event List browser, and double-click to see Event information. Scroll down to OwnerUID field to determine if the event has been assigned.

Priority change is permanent until it is manually updated again, or the same event is received from the domain managers with a different severity.

Step 1 To change the priority of an event, right-click an event in the Alarm Browser and choose **Prioritize**.

Step 2 Change the severity to a priority of your preference.

The severity column reflects the updated severity.

Suppressing or Escalating an Event

You can change the default priority that Prime Central for HCS assigns to an event. A parameter is used in Active Event List to assign a level of importance to the events. Escalation is to attach more importance to an event, while suppression is to attach less importance.

Step 1 To change the priority of an event, right-click an event in the Alarm Browser and choose **Suppress/Escalate**.

Step 2 Change the severity to a priority of your preference.

The severity column reflects the updated severity.

Deleting an Event

Using this option, you can remove events from the event list. To delete one or more events in the event list, select the events, right-click, and click **Delete**.

Note If you delete many events from the Alarm Browser - All Events, the pie and bar graphs will go out of synch.

Viewing the Information of an Event

This options helps you view complete information related to one or more events that are selected in the event list.

To view information related to an event, right-click an event in the Alarm Browser and choose **Information**.

A dialog box, **Alert Status for Serial Number** opens. The following tabs are available:

- Fields—Click this tab to view a list of all the columns and their corresponding values for a selected event.
- Details— Click this tab to view alert details of the event.
- Journal—Click this tab to view the journal entries for the event. To create journal entries, see Adding Journal Notes to an Event, page 5-16.

The following are the other options available:

- Previous— If you selected multiple events from the event list, click this button to display detailed information for the previous event in your selection. This action can fail if events have been deleted elsewhere in the system.
- Next— If you selected multiple events from the event list, click this button to display detailed information for the next event in your selection. This action can fail if events have been deleted elsewhere in the system.
- Close—Click this button to close this window.

Adding Journal Notes to an Event

You can add and save your own event history information. You can maintain a journal for any event.

Step 1 Right-click an event in the Alarm Browser and choose **Journal**. The Journal dialog box opens.

Step 2 The upper list box is display only and shows the existing journal history text. Each entry shows the name of the user who entered the information, and the time stamp. You can use the Alerts menu while within this dialog box by right-clicking within this list box.

Step 3 Use the lower list box to add a text entry of up to 4096 characters. Click **Apply** to save the text within the upper list box. The new text is saved as the last entry, and your username and a time stamp are added automatically.

Step 4 (Optional) Check the **Apply to all selected** check box if you want to add the newly-entered text to all events that are selected in the event list, and not just to the event whose serial number is displayed at the top of the dialog box. To save the text entry to the journal for each selected event, click **Apply**.

Step 5 Do one of the following:

- If you selected multiple events in the event list, click **Previous** to move to the journal entry for the previous event in your selection.
- If you selected multiple events in the event list, click **Next** to move to the journal entry for the next event in your selection.
- Click **Apply** to save newly-entered text to the journal. The Journal dialog box remains open for more entries. This option is useful if you have selected multiple events and want to add different journal entries for them.
- Click **OK** to save the newly-entered text and close the dialog box.
- Click **Close** to close the dialog box. You are prompted to save any unsaved changes.

Sorting Columns

You can sort the columns in the Alarm Browser in ascending or descending order.

Step 1 To sort a column in the Alarm Browser, click the column header once. The rows are sorted in ascending order.

Step 2 To sort in descending order, click the column header again.

Step 3 To unsort the column, click the column header a third time.

Step 4 To sort multiple columns, press **Crtl** and click the required column headers. The sorting importance of the columns is indicated in square brackets ([]) in the column header. To alternate the sorting of individual columns within the selection between ascending and descending order, keep **Ctrl** pressed and click the column headers. To unsort the columns, release **Crtl** and click any header from among the sorted columns. The previously-sorted columns are unsorted; the column that you clicked is sorted in ascending order.

Step 5 To lock a column, right-click the column header and click **Lock Column**. The column is moved to the left side of the portlet, and remains visible when you scroll horizontally. To unlock the column, right-click the column header and click **Lock Column** again.

Refreshing Data

The event list refreshes automatically at regular intervals to show all incoming alerts from the integration layer. You can choose to refresh the event list manually between the configured intervals to view all the latest alerts at the current point in time.

To refresh the Alarm Browser manually between automatic refresh updates, click the **Refresh** icon in the toolbar.

Finding Data

Use the Find dialog box to search for specific text within the data in the Alarm Browser.

Step 1 In the Alarm Browser toolbar, click the **Find** icon.

Step 2 In the Find dialog box, do the following:

a. In the Column list, select the column to search.

b. In the Value field, enter the search value that you want to match. You can enter an exact value to search for or a regular expression.

c. In the Options area, specify the type of match required by selecting one of the following:

- Exact Match—To find rows where the data in the selected column exactly matches the specified search value.
- Regular Expression—To find rows where the data in the selected column matches the specified regular expression.
- Sub String—To find rows where the data in the selected column contains the specified value somewhere within it.

d. Click **Find** to find the first matching occurrence. If a matching row is found in the Alarm Browser, any currently-selected rows are deselected, and the matching row is selected. The Find dialog box remains open so that you can view any additional matching occurrences.

e. Click **Next** to show the next match, and subsequent matches, in the Alarm Browser.

f. Click **Close** to close the Find dialog box.

Changing the Event Information Displayed

You can set what event information is displayed from the available data by editing the list view, or by selecting and applying a different view. You can also edit the filter criteria used by the current event list, or select a different filter to apply to the event list.

From the Alarm Browser, do any of the following:

- To edit the current view and change the columns displayed, click **Edit Views**. The View Builder opens and you can make the updates. See Creating and Editing Views, page 5-21.
- To select a different view to apply to the event list, click the view drop-down list on the toolbar and select from the list of available views. The properties pane updates according to the view settings.
- To edit the current filter, click **Edit Filters**. The Filter Builder opens. See Using the Filter Builder, page 5-19.
- To select a different filter to apply to the event list, select a filter from the Filter list. The properties pane updates with the filter settings.

Using the Quick Filter

You can use the quick filtering facility as a fast way of displaying events that match a selected criteria. You can filter for event data and display events that correspond to the value of a specific cell. For example, you can quickly display only those events that occurred at the same time as the selected event, or before the selected event.

To use the quick filter:

Step 1 In the Alarm Browser portlet, right-click a cell that contains a value on which to base the quick filter.

Step 2 From the right-click menu, choose **Quick Filter** and select one of the following submenu options:

- Equals—Shows all rows with the same field value as the selected cell.
- Not Equals—Shows all rows with a field value different from the selected cell.
- Greater Than—Shows all rows with a greater field value than the selected cell.
- Greater Than or Equals—Shows all rows with a field value greater than or equal to the selected cell.
- Less Than—Shows all rows with a lesser field value than the selected cell.
- Less Than or Equals—Shows all rows with a field value less than or equal to the selected cell.
- Like—Shows all rows that contain the same string as the selected cell.
- Not Like—Shows all rows that do not contain the same string as the selected cell.

The event list refreshes to display only those events that match the specified filter criteria.

Step 3 To remove quick filtering and restore the portlet to its original view of all events, right-click a cell again and choose **Quick Filter > Off**.

In the event of Quick Filter showing no results, to restore the original frame, follow the procedure given below:

Step 1 Pick the **Refresh** icon.

Step 2 Change the filter criterion to **All Events.** Once the table is populated, right-click a cell again and choose **Quick Filter > Off**.

Using the Filter Builder

Network events typically create many alerts that are not of immediate importance to the personnel monitoring the system. Use advanced filters to control the event information that is displayed.

In the Alarm Browser, use the Filter drop-down list to filter event data by specific fields, such as Cleared Events.

Note We recommend that you either use predefined filters or create new filters. If you wish to edit a predefined filter, copy the filter, and then edit it. Do not edit existing filters.

Do the following to create and edit the filters for event data:

Step 1 In the Alarm Browser toolbar, click the **Edit Filters** icon.

The Filter Builder opens.

You can use the following modes to create filters; the Filter Builder displays a tab for each mode.

- Basic—Provides a set of lists and text fields that you use to specify the filter conditions. To build the conditions, select a field from the specified data source or data sources, select a comparator, and enter a numeric data type or string data type value. The data type value is used as the filtering criteria used against the field. If you use basic mode to construct your filter, you can view the resulting SQL in the text field on the Advanced tab. Use the fields mentioned in Table 5-5 to create filters.
- Advanced—Provides a text field into which you can enter an SQL syntax. If you create a filter in advanced mode, it might not be possible to express the SQL syntax in the fields on the Basic tab. After you have saved a filter created in advanced mode, the Basic tab is removed for that filter.
- Dependent—This tab is displayed only for dependent filters. On this tab, use the Search fields to identify the filters that you want to use for the dependencies. After you have identified the required filters, move the filters from the Available filters list to the Selected dependencies list. In a dependent filter, the SQL WHERE statements of each filter are concatenated by using OR statements.
- Metric—A metric is an aggregate statistic that can be derived from the alerts that match a filter to display a useful figure; for example, an average, count, or sum of all field values. If a filter is displayed using a monitor box linked to an Alarm Browser, the metric information obtained from the set of alerts that match this filter is used for this display.

Step 2 Do one of the following:

- To create and edit filters in basic mode, click **New Filter**.
- To edit an existing filter, select the list that contains the required filter. After the list has refreshed, click the filter.

  If you are editing an existing filter, skip the next step.

Note Do not delete the "Default" filter. Deleting the Default filter generates an error.

Step 3 Select the users you want to grant access to the filter and click **OK**.

Step 4 Specify the general properties for the filter:

- Filter Name—Enter a name for the filter. The name cannot contain the following characters:

  $! £ % ^ & * () + = ¬ ` ~ # @ ' : ; < > { } [ ] ? / \ | , "
- Default View—Select the view with which you want to associate the filter, or select the view that is associated with the filter. The default view is applied when you launch an Alarm Browser with the filter but do not specify a view.
- Collection—(For global filters and system filters only) Select the filter collection or collections to which you want to add the filter.
- Description—Enter a description that explains the purpose of the filter.
- Data Source—Select the data source or data sources that contain the fields against which you want to run queries. Click **Show Data Sources** to display a list of available data sources.

Step 5 Click the **Basic** tab and, in the first row, create a filter condition as follows:

a. From the Field list, select a field from the specified data source.

b. From the Comparator list, select a comparator.

c. In the Value field, enter a numeric data type value, or a string data type value. The data types must correspond to those in the ObjectServer field. String data type entries in the Value field must be contained in single quotes.

d. (Optional) Use **like** and **not like** comparators for regular expression pattern-matching metacharacters against the entry in the Value field.

Note Do not use the getdate expression in the Value field.

Step 6 To add additional filter conditions, click **+**. You can add as many filter conditions as required.

Step 7 Use the match options to specify how the filter conditions combine in aggregate:

- Click **All** to trigger the filter only if all the conditions are met.
- Click **Advanced** to trigger the filter if any of the conditions are met.

Step 8 Enter the filter conditions to the new filter.

Step 9 (Optional) To preview the literal SQL WHERE clause output, click **Advanced**.

Step 10 (Optional) Click **Metric** and use the following fields to set the metric value:

- Label—Enter a title for the metric.
- Function—Select one of the following functions to perform on the field data:
  - Average—Returns the average value of the selected field for all records that match the filter.

  - Count—Returns a count of all the records that match the filter. The selected field is not used for this calculation.
  - Maximum—Returns the highest value of the selected field in records that match the filter.
  - Minimum—Returns the lowest value of the selected field in records that match the filter.
  - Sum—Returns the sum of the selected field for all records that match the filter.
- Field—Select a field on which to perform the chosen function.

Step 11 Click **Save and Close**.

Advanced Mode

Provides a text field into which you can enter an SQL syntax. If you create a filter in advanced mode, it might not be possible to express the SQL syntax in the fields on the Basic tab. After you have saved a filter created in advanced mode, the Basic tab is removed for that filter.

Dependent Mode (Optional)

This tab is displayed only for dependent filters. On this tab, use the Search fields to identify the filters that you want to use for the dependencies. After you have identified the required filters, move the filters from the Available filters list to the Selected dependencies list. In a dependent filter, the SQL WHERE statements of each filter are concatenated by using OR statements.

Creating and Editing Views

Use the View Builder to create and edit views that are dynamically applied to Alarm Browser data. The views determine what information is displayed from the available event data.

Note We recommend that you either use predefined views or create new views. If you wish to edit a predefined view, copy the view, and then edit it. Do not edit existing views.

Step 1 In the Alarm Browser toolbar, click the **Edit Views** icon. The View Builder opens.

Step 2 Do one of the following:

- To create a new view, click **New View**.
- To edit an existing view, select the desired view from the View list. The page updates with the view properties.

  If you are editing an existing view, skip the next step.

Step 3 Select the users you want to grant access to the view and click **OK**.

Step 4 Use the following fields to set the general properties for the view:

- Name—Enter a name for the view. The name cannot contain the following characters:

  $! £ % ^ & * () + = ¬ ` ~ # @ ’ : ; < > { } [ ] ? / \ | , "

  By default, the following characters cannot be used as the initial character of a view name:

  / \ * ? " < > | & .
- Data Source—Select the data source or data sources that contain the fields that you want to be displayed in the view. Click **Show Data Sources** to display a list of available data sources.

Step 5 You can set the horizontal left-to-right order of the columns in the Alarm Browser, and change which columns are visible. You can build views to reflect one or more columns as specified in Table 5-5Field Descriptions for the Alarm Browser Portlet, page 5-12.

a. Use the **>** and **<** arrows to move fields between lists. Only those fields in the Event list view list are visible as columns in the Alarm Browser.

b. In the Event list view list, select a field.

c. Use the arrow buttons to the right of the list to change the display order of the columns in the view:

- Click **Top** to move the field to the top of the list. In the Alarm Browser, the field is displayed as the column furthest to the left.
- Click **Up** to move the selected field up one position in the list.
- Click **Down** to move the selected field down one position in the list.
- Click **Bottom** to move the selected field to the bottom of the list. In the Alarm Browser, the field is displayed as the column furthest to the right.

Step 6 (Optional) Check the **Lock column** check box to lock the selected column at the far left of the Alarm Browser in the view, so that the column is always displayed when you scroll horizontally.

Step 7 Click **Save and Close**.

Freezing and Unfreezing the Alarm Browser

To take a snapshot of event information before it is changed by updates from the integration layer, you can freeze all the fields on the Alarm Browser.

Step 1 To freeze the fields, click the **Freeze/Unfreeze** icon in the Alarm Browser toolbar.

The updates from the integration layer are suppressed.

Step 2 To unfreeze the fields and obtain updates from the integration layer, click the **Freeze/Unfreeze** icon again.

Step 3 (Optional) To force a refresh of the fields independently of the refresh rate, click the **Refresh** icon.

Changing Preferences

Use the Preferences dialog box to configure preferences for the Alarm Browser.

Step 1 In the Alarm Browser toolbar, click the **Change preferences** icon. The Preferences dialog box opens.

Step 2 Use the Event List tab to set other event list preferences.

- Show Colors—Displays each row of the event list with a background color that corresponds to the severity of the event.
- Show Distribution Summary Bar—Displays the distribution summary bar, which shows the number of alerts that match each severity color.
- Show Toolbar—Makes the toolbar available on the event list.

- Font Name—Choose a font for your event list.
- Font Size—Choose a font size for your event list.
- Date Format—Choose the required date format. If you select Customize, enter a custom format. The correct format of the date is d/m/yy h:mm:ss.
- Time Zone—Choose a time zone from the available options.
- Event List Icons—Specify how you want the event severity to be depicted in the Severity column:
  - Show—Displays an icon to denote event severity.
  - Show With Text—Displays an icon and text to denote event severity.
  - Don't Show—Displays text to denote event severity.

Step 3 Click **Save**.

Step 4 Click **Close**.