Cisco UCS Performance Manager Administration Guide

First Published: December 2015

Release 2.0.0

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2014-2015 Cisco Systems, Inc. All rights reserved.

Contents

Chapter 1: Using Cisco UCS Performance Manager.....5

Interface and Navigation..... 5
Dashboard.....8
Navigating the Event Console.....14
Running a Command from the UI.....17
Working with Triggers and Notifications..... 18
LDAP Authentication.....31
Product Licensing.....36

Chapter 2: Adding, Discovering and Modeling Devices..... 38

Adding a Device.....38
Modeling Devices.....40
Debugging the Modeling Process.....41

Chapter 3: Working with Devices..... 42

Viewing the Device List..... 42
Working with Devices..... 43
Managing Devices and Device Attributes..... 54
Working with Host Groups..... 56
Working with Integrated Infrastructure..... 57
Working with Component Groups.....58

Chapter 4: Event Management..... 60

Basic Event Fields.....60
Other Fields.....62
Details..... 63
De-Duplication.....63
Auto-Clear Correlation.....64
Event Consoles.....65
Creating Events Manually.....70
Event Classes..... 71
Mapping and Transformation.....71
Event Life Cycle.....74

Chapter 5: Production States and Maintenance Windows.....77

Production States.....77
Maintenance Windows..... 78

Chapter 6: Organizers and Path Navigation.....81

Classes.....81

Chapter 7: Self Monitoring.....83

About Collectors.....84
About Hubs.....84
Navigating Collectors and Hubs.....84
Collector Data Storage.....86
Deleting Collectors.....87
Moving Devices Between Collectors.....87

Chapter 8: Managing Users.....88

Creating User Accounts.....88
Editing User Accounts.....89
User Groups.....91
Roles.....92
Device Access Control Lists.....92

Chapter 9: Reporting.....95

Scheduling Reports.....95
Cisco UCS Capacity Reports.....96
Cisco UCS Reports.....105
Enterprise Reports.....105
Performance Reports.....110
System Reports.....111
VMware vSphere Reports.....112

Chapter 10: General Administration and Settings.....113

Events Settings.....113
Thresholds.....115
Performance Data Retention.....122
Audit Logging.....122
Debug Logging.....127
Support Bundles.....128
Setting Portlet Permissions.....130
Backup and Restore.....131
Working with the Job Manager.....133
Host Name Changes.....135

Glossary of terms.....136

Using Cisco UCS Performance Manager 1

This guide provides an overview of Cisco UCS Performance Manager architecture and features, as well as procedures and examples to help use and configure the system.

Related publications

Title	Description
Cisco UCS Performance Manager Installation Guide	Provides detailed information and procedures for installing and upgrading Cisco UCS Performance Manager.
Cisco UCS Performance Manager Getting Started Guide	Provides instructions to get your system up and running quickly after the installation.
Cisco UCS Performance Manager Administration Guide	Provides an overview of Cisco UCS Performance Manager architecture and features, as well as procedures and examples to help use the system.
Cisco UCS Performance Manager User Guide	Provides specific instructions for using Cisco UCS Performance Manager in the UCS environnment.
Cisco UCS Performance Manager Migration Guide	Provides detailed information and procedures for migrating data from Cisco UCS Performance Manager version 1.1.x to version 2.0.
Cisco UCS Performance Manager Release Notes	Describes known issues, fixed issues, and late-breaking information not already provided in the published documentation set.

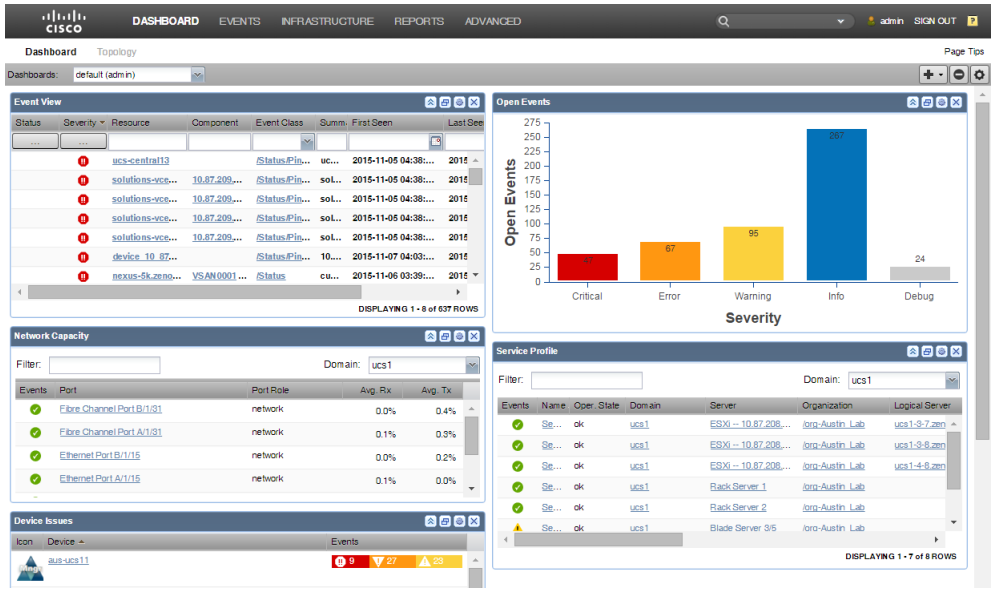
Documentation feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to `ucs-docfeedback@cisco.com`. We appreciate your feedback.

Interface and Navigation

After you install the system and navigate to the interface from your Web browser, the Dashboard appears. The Dashboard provides at-a-glance information about the status of your IT infrastructure. It is the primary window into devices and events that the system enables you to monitor.

Figure 1: Dashboard



Navigation

The Navigation menu lets you access major system features. In addition to the Dashboard, the menu is divided among several functional areas:

- **Events**- Guides you to the event management area, where you can monitor event status, triggers, and event transforms. You also can track changes made to events.
- **Infrastructure**- Offers access to all the devices that have been added to the system.
- **Reports**- Allows you access to pre-defined and configurable reports.
- **Advanced**- Provides access to monitoring templates, system settings, and licensing.

User Information Area

Figure 2: User Information Area

The User information area offers information and selections:

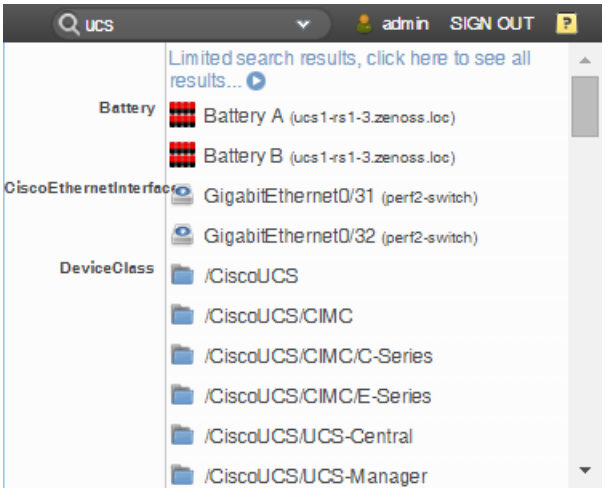
- **Search**- Search area to find information within the application. Click the down arrow in the search box to manage your saved searches.
- **Login ID**- The ID of the user currently logged in appears at the far left of this area. Click the ID to edit user settings, such as authentication information, roles, and groups. (You also can access user settings from the **Advanced > Settings > Users** page.)
- **Sign Out**- Click to log out of the system.
- **Help** icon - Click to access product documentation.

Search

The Cisco UCS Performance Manager search facility supports locating devices and other system objects, as well as events and services.

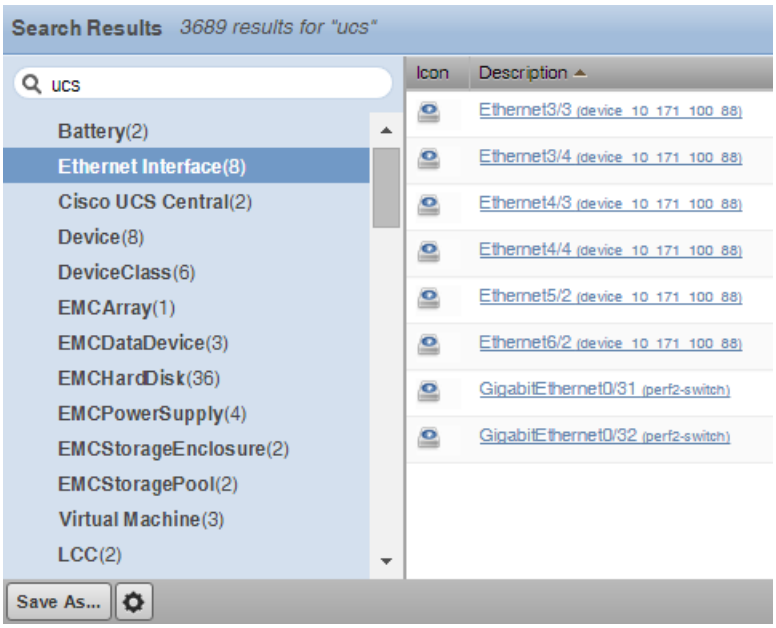
In the Cisco UCS Performance Manager interface, the search feature is part of the user information area. Enter part or all of a name in the search box at the top right of the interface. The system displays matches, categorized by type.

Figure 3: Search Results



To view all search results, click the indicator at the top of the list.

Figure 4: All Search Results



From here, you can display search results by category. Click in the left panel to filter search results by a selection.

You can save the search to access later.

1 Click **Save As** (at the bottom left of the Search Results page).

   The Save Search As dialog appears.

2 Enter a name for the search, and then click **Submit**.

You can access saved searches from:

- Action menu located at the bottom of the Search Results page.
- Search box located at the top of the interface. Click the arrow, and then select **Manage Saved Searches**.

Dashboard

The Dashboard contains two views to highlight different types of information about your UCS environment:

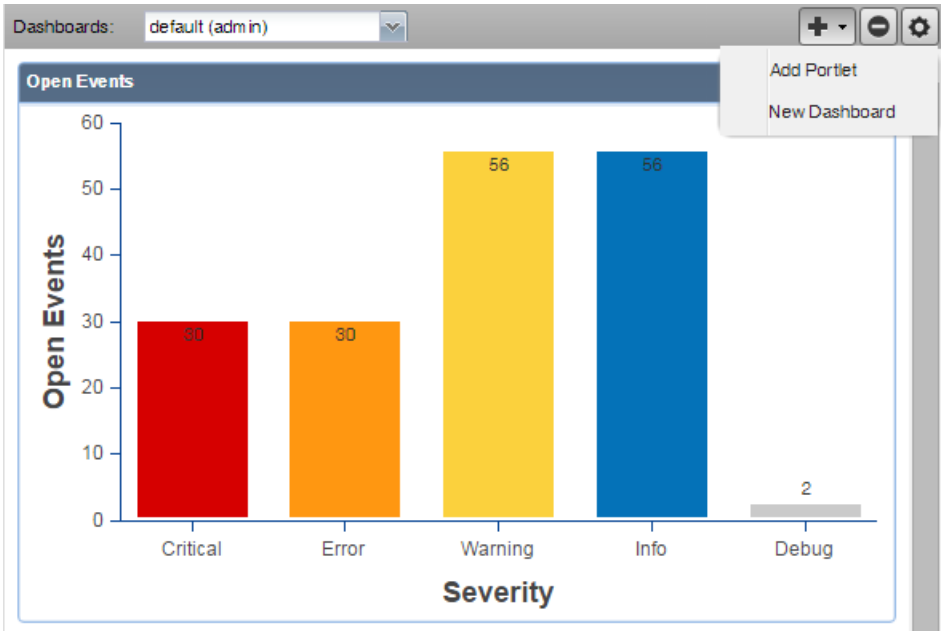
- Dashboard view
- Topology view

Customizing the Dashboard

You can customize the dashboard by:

- Creating multiple dashboards
- Selecting the portlets you want to view
- Arranging portlets
- Defining who can view the dashboard
- Changing the Dashboard column layout

The following screenshot of a sample dashboard shows the Add icon menu activated:



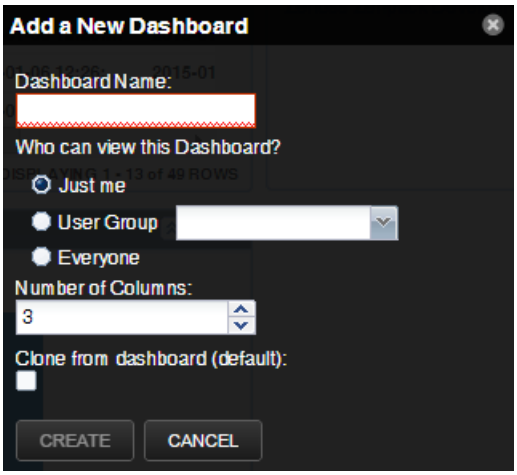
Adding a New Dashboard

A default admin dashboard is created when you launch the system. This dashboard can be customized by administrators, but you may want to create other dashboards that display distinctive information or are targeted to a specific type of user (including just yourself). You can create as many additional dashboards as you choose. You can customize them by selecting who can view the dashboard as well as selecting and customizing portlets to display the most important information. Users that are not administrators will initially see a read-only version of the default admin dashboard and can then create additional dashboards for their use.

Note You cannot delete the default admin dashboard.

To create an additional dashboard:

1 From the **Add** icon on the Dashboard controls, select **New Dashboard**. The Add a New Dashboard dialog appears.



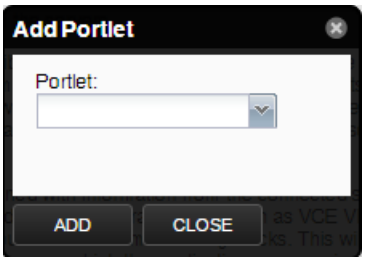
2 Enter a Dashboard Name. When this dashboard name is displayed in the Dashboards drop-down list, the user name who created it will be appended in parentheses as part of the name. This gives everyone who can see the dashboard an indication of who created it.
3 Select who can view this dashboard. If you want a User Group to view this dashboard, the group must already be created in the system and the user creating this new dashboard must be a member of the group. You cannot add a dashboard and assign it to a group you are not part of.
4 Select the number of columns to display in the dashboard. The default is 3.
5 If you want to clone the new dashboard from the previously viewed dashboard, select the check box. Otherwise, you will begin with a completely blank dashboard.
6 Click **Create**.

Adding Portlets

You can customize your dashboard by adding portlets that display information you are interested in. Your dashboard can display more than one of the same portlet type. For example, you could have several Device Chart portlets with each one showing a different device class.

To add portlets to the Dashboard view:

1 Click the **Add** icon and select **Add Portlet**. The Add Portlet dialog appears.



2 Click the name of the portlet you want to add from the drop-down list, then click **Add**. The Add Portlet dialog displays with a preview of the portlet along with configuration options. Click **Add** to display the portlet on the dashboard. If you want to add another portlet, repeat this procedure. The new portlet is displayed in the top left of the dashboard.
3 (optional) Move the portlet within the Dashboard view by clicking and dragging it to the desired location.

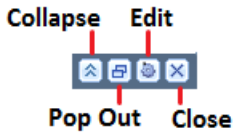
The following portlets are available for display on any dashboard. The default portlets on the default dashboard are indicated as such:

- Chassis Capacity
- Chassis Link Events
- Device Chart
- Device Issues
- Domain Overview (Default)
- Event View
- Fabric Extender Capacity
- HTML Portlet
- Integrated Infrastructure
- Network Capacity
- Network Map
- Open Events Chart (Default)
- Out Of Balance Events
- Past Events Line Chart
- Production States
- Service Profile (Default)
- Site Window
- Storage Capacity
- Top Level Organizers
- UCS Inventory (Default)
- Watch List
- Welcome to UCS Peformance Manager (Default)

Working with Portlets

There are several options to control the portlet display.

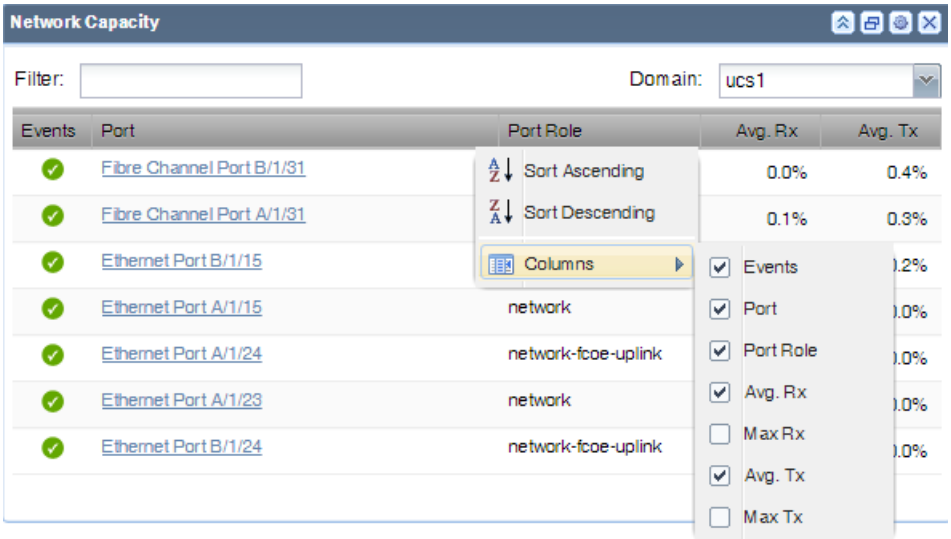
Figure 5: Dashboard Portlet Controls



- Click the **Collapse** icon to collapse the portlet so that only the title is displayed on the dashboard.
- Click the **Pop Out** icon to show the portlet in a full screen view. Click **Close** to return to the dashboard view.
- Click the **Edit** icon to edit the portlet settings. You can edit the title of the portlet, its height and how often it refreshes. Some portlets may have additional configuration options. A preview of the portlet is provided on the right side of the dialog box. Click **Save** to update the portlet configuration.
- Click the **Close** icon to remove the portlet from the dashboard.

In tabular portlets, you can control the display by sorting columns as well as adding and hiding columns.

- To sort based on a column, hover over the column header and click the arrow to display the sort and display options.
- To add or hide columns, hover over the **Columns** entry and check or clear the boxes of the columns to add or hide.



Arranging Portlets

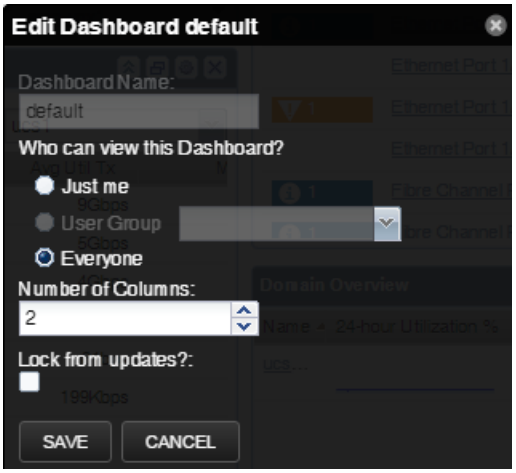
To arrange portlets, click the portlet header and drag the portlet to any location on the Dashboard. Other portlets rearrange depending on the location you drop it.

Editing the Dashboard Settings

You can customize your dashboard to display a different number of columns or limit access to the dashboard.

To edit the dashboard settings:

1 Click the Action icon in the upper-right side of the Dashboard. The Edit Dashboard window appears.



2 Change the value of the users who can view this dashboard, if needed. If you want a User Group to be able to view this dashboard, the group must already be defined in the system and the user editing the dashboard must be a member of the user group in order to see that group in the drop-down list.

3 Change the number of columns to use in this dashboard if needed.

4 Select the **Lock from updates?** check box to prevent editing of the dashboard.

5 Click **Save**.

Topology View

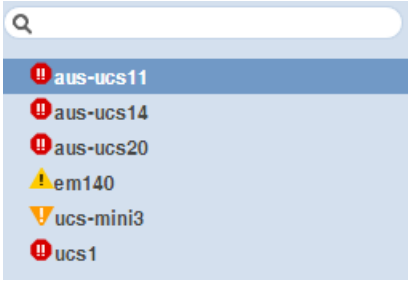
The main content of the Topology view of the dashboard contains portlets that provide information about the system and your infrastructure. These portlets display:

- **All Domains** - Displays the number of appearances of each color-coded severity level in all domains.

  Figure 6: All Domains Portlet

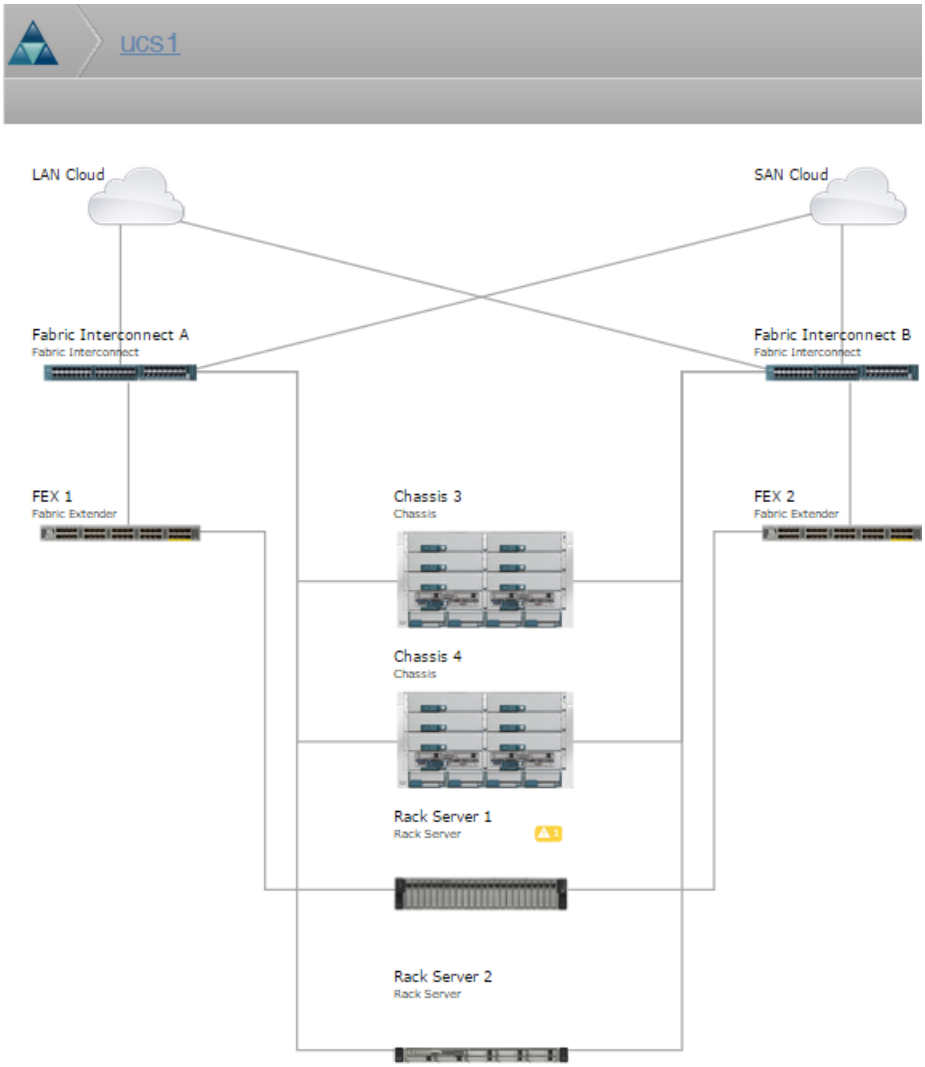
- **Devices** - Displays a list of devices along with any associated color-coded severity levels. Click on a device name to display its topology.

  Figure 7: Devices List

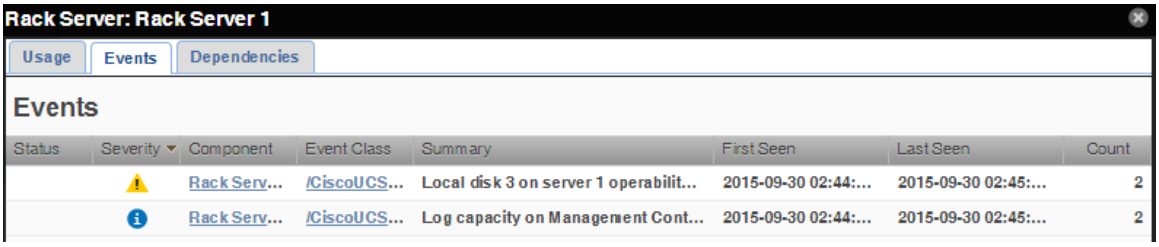
- **Overall Ethernet Bandwidth Utilization** - Indication of the total bandwidth utilization of all Cisco UCS Performance Manager domains. Shown as a percent.
- **Connected Ethernet Ports Bandwidth Utilization** - Indication of the total connected ports bandwidth utilization. Shown as a percent.
- **UCS Physical Topology** - Click a device name to view its physical topology diagram. Severity alerts are shown on the appropriate component. Rescale the topology view by using the mouse wheel to zoom in and out, or click and drag the view for better visibility. You can also use the mini-map in the lower-right corner to customize your view. When you click on the lines between modules the network links are displayed.

Figure 8: Device Topology



Click an event alert warning to show the Events detail page. You can also click the Usage or Dependencies tab for more information.

Figure 9: Events Detail



Click a link on the topology view to see the port mappings between the components. For example, clicking the link between Fabric Interconnect A and Chassis 3 will display the port mappings in addition to usage, event, and dependency information.

Figure 10: Port Mapping Detail

The Device Topology display is refreshed every 15 minutes by default. To perform a manual refresh, click the **Refresh** icon . To change the default setting, click the down arrow on the **Refresh** icon and select your setting.

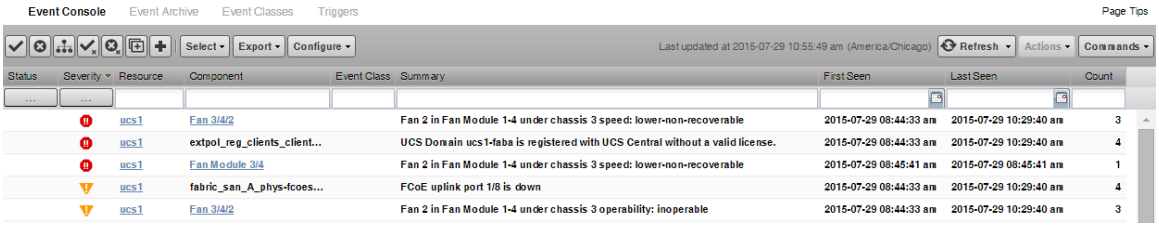
Click the **Export** button to generate a `.png` image of your topology view.

Navigating the Event Console

The event console is the system's central nervous system, enabling you to view and manage events. It displays the repository of all events that are detected by the system, whether they are device fault and status events, or performance threshold events.

To access the event console, click **Events** in the Navigation menu. The Event Console appears.

Figure 11: Event Console



Sorting and Filtering Events

You can sort and filter events that appear in the event console to customize your view.

You can sort events by any column that appears in the event console. To sort events, click a column header. Clicking the header toggles between ascending and descending sort order.

Filter options appear below each column header. A match value can be any full string or a subset of a string, optionally with the wildcard (*) contained in the values in that column. You can also use "`||`" (OR), or "`!!`" (NOT) expressions to further target your filters. For example, typing `!!status` in the Event Class filter will return all the non-status class events.

Figure 12: Event Console Filter Options

You can filter the events that appear in the list in several ways, depending on the field type:

- **Resource** - Enter a match value to limit the list.
- **Component** - Enter a match value to limit the list.
- **Event Class** - Enter a match value to limit the list.
- **Summary** - Enter a match value to limit the list.
- **First Seen** - Enter a value or use a date selection tool to limit the list.
- **Last Seen** - Enter a value or use a date selection tool to limit the list.
- **Count** - Enter a value to filter the list, as follows:
  - *N* - Displays events with a count equal to *N*.
  - *:N* - Displays events with a count less than or equal to *N*.
  - *M:N* - Displays events with a count between *M* and *N* (inclusive).
  - *M:* - Displays events with a count greater than or equal to *M*.

To clear filters, select **Configure > Clear filters**.

You also can re-arrange the display order of columns in the event console. Click-and-drag column headers to change their display.

Creating an Actionable View

For users that are not Administrators, there is an option that will filter the list of events to show only those that are not read-only for the user's permission level, and enable the action buttons above the event table header.

To turn on the actionable view, click **Configure** and select the **Only show actionable events** check box. The view is changed to show only events that can have an action performed on them based on the user's permission level. For more information, see *Managing Events* on page 17.

Saving a Custom View

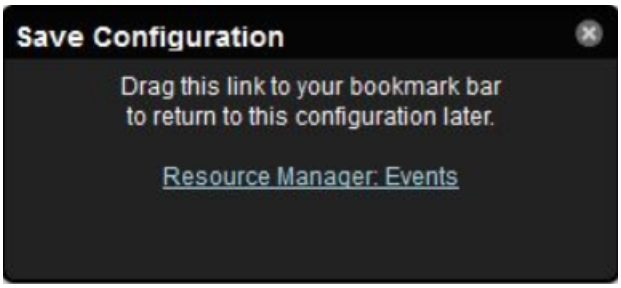
You can save your custom event console view by bookmarking it for quick access later. To do this:

1. Select **Configure > Save this configuration**.

   A dialog containing a link to the current view appears.
2. Click-and-drag the link to the bookmarks area on your browser's menu bar.

   The system adds a link titled "Cisco UCS Performance Manager: Events" to your bookmarks list.

Figure 13: Saving a Custom View (Bookmark)



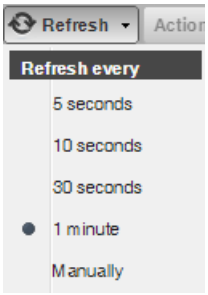
Note You may want to re-title the bookmark, particularly if you choose to save more than one event console view.

Refreshing the View

You can refresh the list of events manually or specify that they refresh automatically. To manually refresh the view, click **Refresh**. You can manually refresh at any time, even if you have an automatic refresh increment specified.

To configure automatic refresh, select one of the time increments from the Refresh list. By default, automatic refresh is enabled and set to refresh each minute.

Figure 14: Automatic Refresh Selections



Viewing Event Details

You can view details for any event in the system. To view details, double-click an event row.

Note Do not double-click on or near the device (resource) name, component, or event class in the row. Doing this displays details about that entity, rather than information about the event.

The Event Detail area appears.

Figure 15: Event Detail

To see more information about the event, click **Event Details**.

You can use the Log field (located at the bottom of the area) to add specific information about the event. Enter details, and then click **Add**.

Selecting Events

To select one or more events in the list, you can:

- Click a row to select a single event.
- Ctrl-click rows to select multiple events, or Shift-click to select a range of events.
- Click **Select > All** to select all events.

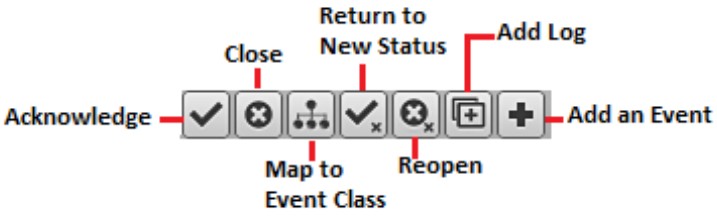
Managing Events

You can manage events from the event console. After making a selection by clicking on the row of the event, you can:

- Acknowledge the event
- Close the event
- Reclassify the event, associating it with a specific event class
- Return the event to New status (revoke its Acknowledged status)
- Reopen the event
- Add a note to the log

You also can add an event from the event console. This feature is useful for testing a specific condition by simulating an event.

Figure 16: Event Management Options



Running a Command from the UI

Cisco UCS Performance Manager allows commands to be run though the Web-based user interface (UI). You can run commands on a single device or on a group of devices.

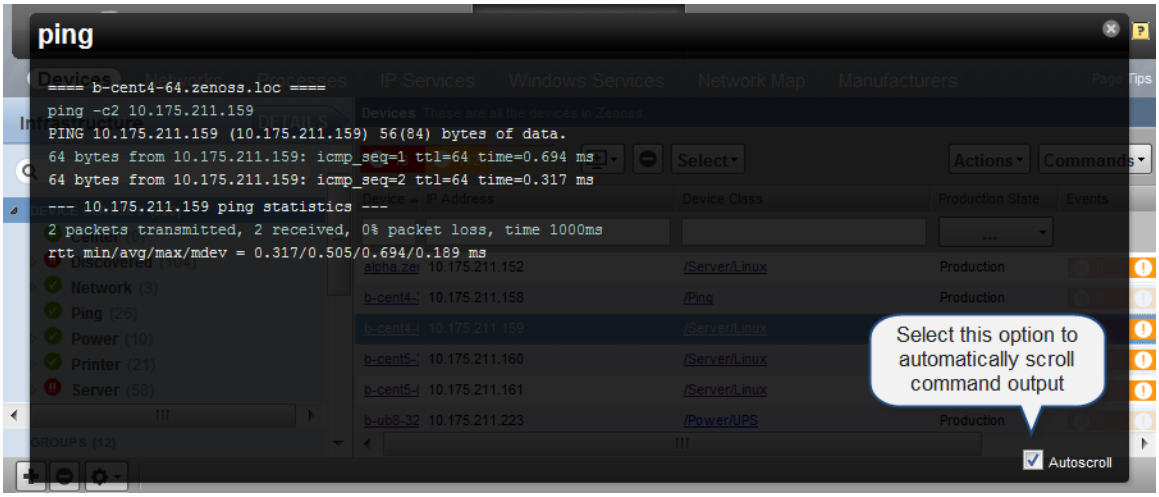
The system includes several built-in commands, such as `ping` and `traceroute`.

To run commands from the user interface:

1. Select one or more devices from the Devices list, which can be found under the **Infrastructure** menu. Do not click on a link within the row, just click anywhere else in the row to select the device.
2. Click **Commands** and select a command from the list.

   The system runs the command. Command output appears on the screen.

Figure 17: Command Output



You can resize the command output window. You also can stop automatic scrolling by de-selecting the Autoscroll option at the bottom right corner of the output window.

Working with Triggers and Notifications

You can create *notifications* to send email or pages, create SNMP traps, or execute arbitrary commands in response to an event. Notifications also can be used to notify other management systems, and to execute arbitrary commands to drive other types of integration. How and when a notification is sent is determined by a *trigger*, which specifies a rule comprising a series of one or more conditions.

To set up a notification, you must:

- Create a trigger, selecting the rules that define it
- Create a notification, selecting one or more triggers that cause it to run
- Choose appropriate options and subscribers, depending on the notification type

Read the following sections to learn about:

- Setting up triggers and trigger permissions
- Setting system SMTP settings for notifications
- Setting up notifications and notification permissions

Working with Triggers

Setting up a trigger involves:

- Creating the trigger and the rules that define it
- Setting trigger permissions

Creating a Trigger

To create a trigger:

1 Select **Events > Triggers** from the Navigation menu.

The Triggers page appears. It displays all existing triggers, indicating whether each is enabled.

2 Click the **Add** icon.

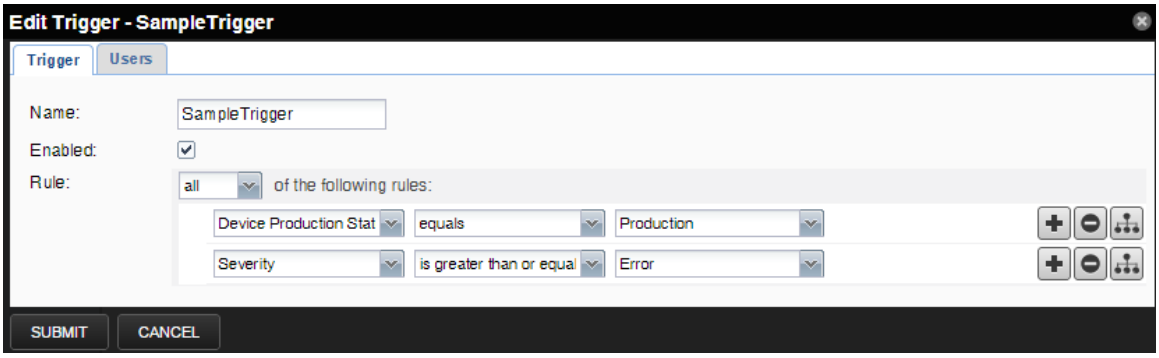
The Add Trigger dialog appears.

3 Enter a name for the trigger, and then click **Submit**. Be sure to only use letters, numbers, or the underscore character for the name. Do not use spaces or special characters.

The trigger is added to the list and is automatically enabled.

4 Double-click the trigger, or select the row of the trigger and click the **Action** icon to open the Edit Trigger dialog.

Figure 18: Edit Trigger



Enter information or make selections to define the trigger:

- **Enabled** - Select this option to enable the trigger.
- **Rule** - Define the rule comprising the trigger:
  - Select All or Any from the list to specify whether a notification will be triggered based on all, or any one, of the trigger rules.
  - Define the rule by making selections from each event field.

  To add a rule to the trigger, click the **Add** icon.

  Optionally, click the **Branch** icon to create a sub-branch of a given rule.

Note Be sure to take into account that a device production state may change during a maintenance window and if you haven't defined that a trigger should also fire during a production state of `Maintenance`, you may not get notification of a defined severity during the maintenance window.

Setting Global Trigger Permissions

You can set global permissions for viewing, editing, and managing triggers. Global permissions are given to any user with "manage" permission, which includes:

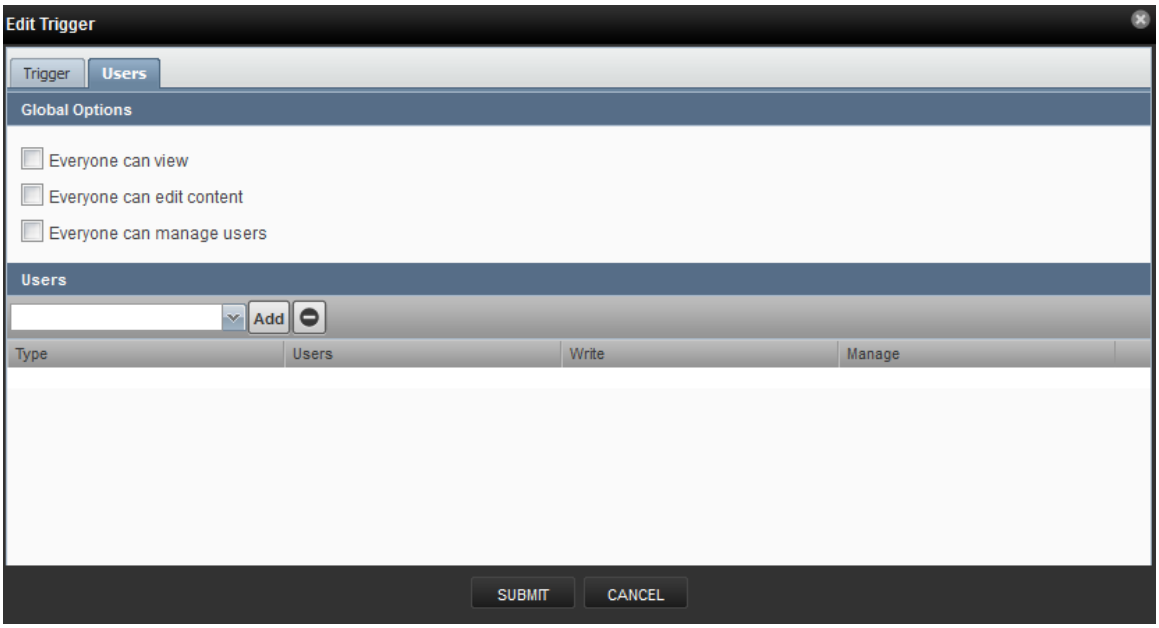
- Admin, Manager, and ZenManager roles
- Trigger owner

Edit global permissions from the Users tab on the Edit Trigger dialog.

Global options are:

- **Everyone can view** - Provides global view permission.
- **Everyone can edit content** - Provides global update permission.
- **Everyone can manage users** - Provides global manage permission.

Figure 19: Edit Trigger - Users Tab



Setting Individual Trigger Permissions

You can grant permissions to individual users. For each user added, you can select:

- **Write** - Select this option to grant the user permission to update the trigger
- **Manage** - Select this option to grant the user permission to manage the trigger.

To set an individual's trigger permissions:

1. Select a user from the drop-down list in the Users section of the Edit Trigger dialog.
2. Click **Add**. The user is added.
3. Assign permissions by selecting the appropriate check box(es).
4. Optionally, add additional user trigger permissions by repeating this procedure.
5. When you are finished, click **Submit**.

To remove an individual's trigger permissions:

1. Select the row of the user's permissions.
2. Click the **Remove** icon.
3. Optionally, remove other user trigger permissions by repeating this procedure.
4. When you are finished, click **Submit**.

Working with Notifications

Setting up a notification involves:

- Creating the notification
- Defining notification content (for email- or page-type notifications)
- Defining the SNMP trap host (for SNMP trap-type notifications)
- Defining commands to run (for command-type notifications)
- Setting notification permissions
- Setting up notification schedules

Creating or Editing a Notification

To create or edit a notification:

1 Select **Events > Triggers** from the Navigation menu.
2 Select **Notifications** in the left panel.

The Notifications page appears.

Figure 20: Notifications

The Notifications area lists all defined notifications. For each notification, the area indicates whether the notification is enabled (Yes or No), the Action associated with the notification, and the number of notification subscribers.

To edit a notification, double-click it; or select it, and then click the **Action** icon.

To create a notification:

a Click the **Add** icon.

The Add Notification dialog appears.

b Enter a name for the notification.

> **Note** Spaces are not allowed in a notification name.

c Select an Action associated with the notification:

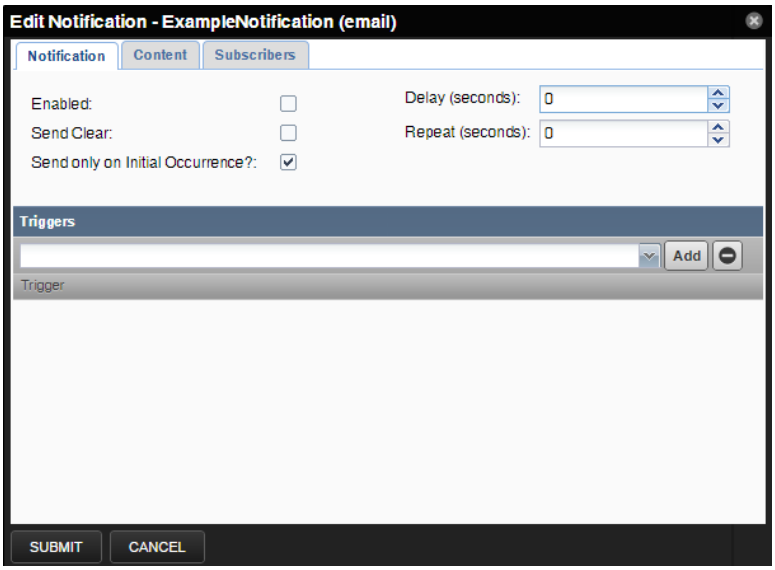
- **Command**- Allows the system to run arbitrary shell commands when events occur. Common uses of a Command notification include:
  - *Auto-remediation of events*. You can use SSH to remotely restart services on a UNIX system when they fail, or winexe to do the same for Windows services.
  - *Integration with external systems*. This includes opening tickets in your incident management system.
  - *Extending alerting mechanisms*. Cisco UCS Performance Manager supports email and pagers as alerting mechanisms "out of the box" through normal alerting rules.
- **Email** - Sends an HTML or text email message to authorized subscribers when an event matches a trigger rule.
- **Page** - Pages authorized subscribers when an event matches a trigger rule.
- **Syslog** - Sends a message to the syslog.
- **SNMP Trap** - Sends an SNMP trap when an event matches a trigger rule.

d Click **Submit**.

e Edit your newly created notification by double-click it or by selecting it and clicking the **Action** icon.

The Edit Notification dialog appears.

Figure 21: Edit Notification



On the Notification tab, you can select or set:

- **Enabled** - Select this option to enable the notification.
- **Send Clear** - Specify to send a notification when the problem has been resolved by a clear event.
- **Send only on Initial Occurrence** - Select this option to send the notification only on the first occurrence of the trigger.
- **Delay (seconds)** - Specify the minimum age (in seconds) of an event before the notification will be executed. You might want to set a delay to prevent notifications being sent for transient problems, or to prevent multiple notifications being sent for the same problem.

  For example, if you have five events that come in and match the trigger in 45 seconds, specifying a delay of 60 seconds will ensure that only one notification is sent. Additionally, if you have an event that matches the trigger at 15 seconds and is later cleared by another event at 45 seconds, a delay of 60 seconds will prevents notifications being sent.
- **Repeat (seconds)** - Specify how often to repeat the notification until the event that triggered it is resolved.

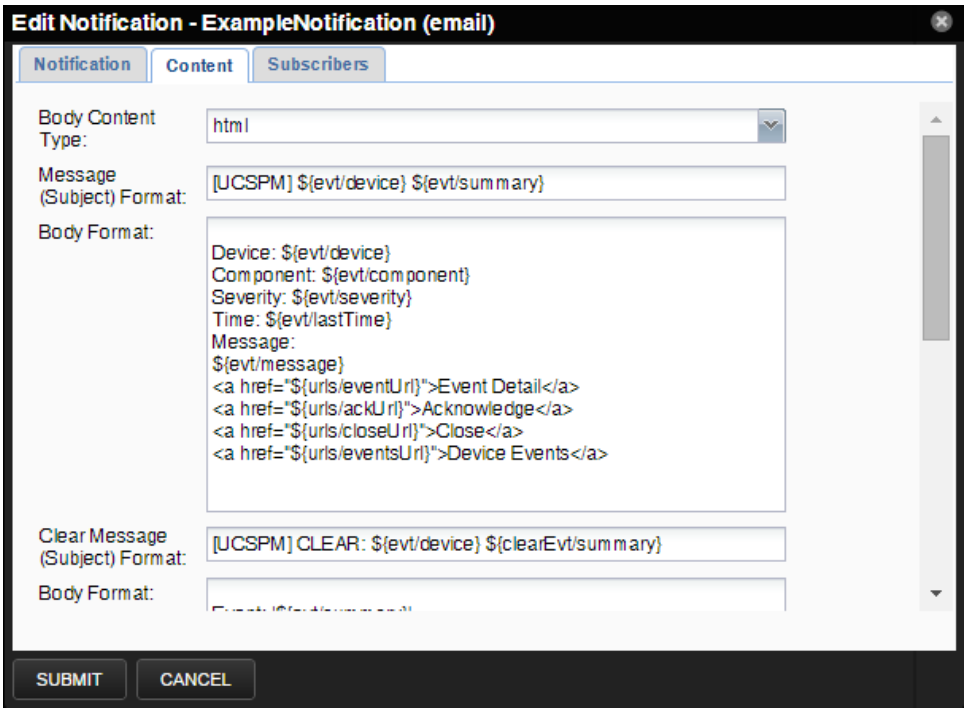
Defining Notification Content

To define notification content, click the **Content** tab of the notification.

For email-type notifications, you can use the default configuration for the following fields, or customize them to your needs:

- **Body Content Type** - Select HTML or text.
- **Message (Subject) Format** - Sent as the subject of the notification.
- **Body Format** - Sent in the notification.
- **Clear Message (Subject) Format** - Sent when a notification clears.
- **Body Format** - Sent when a notification clears.
- **From Address for Emails** - Sent as email address of sender
- **Various SMTP settings** - Used to define SMTP host, port, username, and password. To set these system-wide, go to the **Advanced > Settings** page.

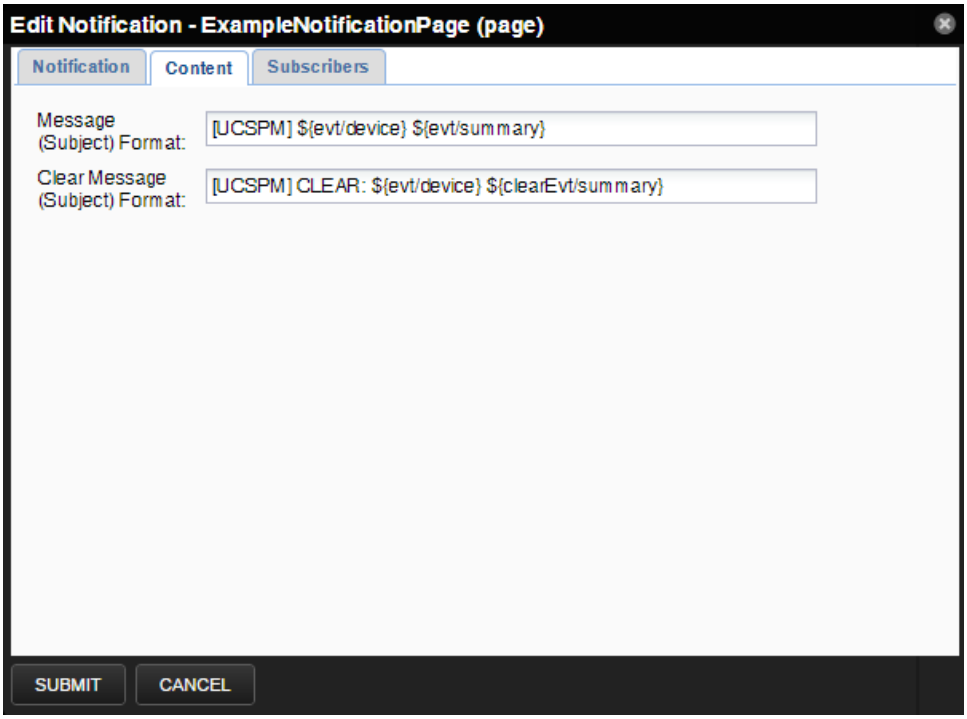
Figure 22: Define Notification Content (Email)



For page-type notifications, you can use the default configuration for the following fields, or customize them to your needs:

- **Message (Subject) Format** - Sent as the subject of the notification.
- **Clear Message (Subject) Format** - Sent when a notification clears.

Figure 23: Edit Notification Content (Page)



Notification Content Variables

Within the body of your email, page, and command notifications, you can specify information about the current event, in the form:

```
'${objectname/objectattribute}'
```

Note Do not escape event command messages and event summaries. For example, write this command as: `${evt/summary}` (rather than `echo '$evt/summary'`).

Object names may be evt, evtSummary, or urls; or for clearing event context, clearEvt and clearEventSummary. For each object name, the following lists show valid attributes (for example, '${evt/DevicePriority}'):
evt/ and clearEvt/

Table 1: evt/ and clearEvt/

Value	Description
DevicePriority	-
agent	Typically the name of the daemon that generated the event. For example, an SNMP threshold event has *zenperfsnmp* as its agent.
clearid	id of the event this clear event will clear
component	component this event is related to
count	how many times this event occurred
created	when the event was created
dedupid	dynamically generated fingerprint that allows the system to perform de-duplication on repeating events that share similar characteristics
device	device this event is related to
eventClass	class of this event
eventClassKey	Free-form text field that is used as the first step in mapping an unknown event into an event class.
eventGroup	Free-form text field that can be used to group similar types of events. This is primarily an extension point for customization. Currently not used in a standard system.
eventKey	Free-form text field that allows another specificity key to be used to drive the de-duplication and auto-clearing correlation process.
eventState	-
evid	unique id for the event
facility	the syslog facility
firstTime	UTC Time. First time that the event occurred.
ipAddress	-
lastTime	UTC time. Most recent time that the event occurred.

manager	-
message	a message communicated by the event
ntevid	windows event id
ownerid	ownerid
priority	syslog priority
prodState	production state of the device
severity	the severity of the event
stateChange .	last time that the event status changed
status	-
summary	a short message summarizing the event

eventSummary/ and **clearEventSummary/**

Note Some of the values in this table are direct duplicates of fields on *evt*. For example, *uuid -> evt.evid*.

Value	Description
uuid	evt.evid
occurrence	-
status	evt.eventState
first_seen_time	evt.firstTime
status_change_time	evt.stateChange
last_seen_time	evt.lastTime
count	evt.count
current_user_uuid .	UUID of the user who acknowledged this event
current_user_name	name of the user who acknowledged this event.
cleared_by_event_uuid	the UUID of the event that cleared this event (for events with status == CLEARED).
notes	event notes
audit_log	event audit log
update_time	last time a modification was made to the event
created_time	evt.lastTime
fingerprint	evt.dedupid
event_class	evt.eventClass
event_class	evt.eventClass
event_class_key	evt.eventClassKey
event_class_mapping_uuid	If this event was matched by one of the configured event class mappings, it contains the UUID of that mapping rule.

actor	-
summary	evt.summary
message	evt.message
severity	the severity of the event
event_key	evt.eventKey
event_group	evt.eventGroup
agent	evt.agent
syslog_priority	evt.priority
syslog_facility	evt.facility
nt_event_code	evt.ntevid
monitor	evt.monitor
tags	event tags

urls/

Value	Description
ackUrl	URL for acknowledging the event
closeUrl	URL for closing the event
reopenUrl	URL for reopening the event
eventUrl	URL for viewing the event
eventsUrl	URL for viewing events for the relevant device, or all events

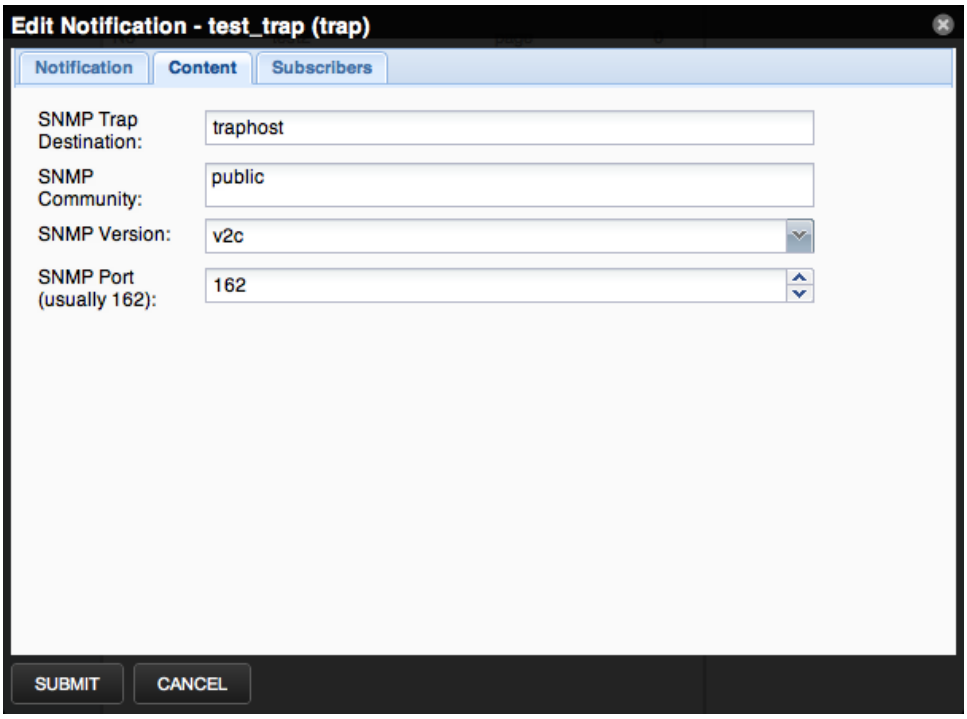
Defining the SNMP Trap Host

For SNMP trap-type notifications, enter information or make selections on the Content tab of the notification:

- **SNMP Trap Destination**- Specify the host name or IP address where the trap should be sent.
- **SNMP Community**- Specify the SNMP community. By default, this is public.
- **SNMP Version**- Select v2c (default) or v3.
- **SNMP Port**- Specify the SNMP port. Typically, this is 162.

SNMP traps sent as a result of this notification are defined in the `ZENOSS-MIB` file. You can find this MIB file on any Cisco UCS Performance Manager server at `$ZENHOME/share/mibs/site/ZENOSS-MIB.txt`.

Figure 24: Edit Notification Content (SNMP Trap)

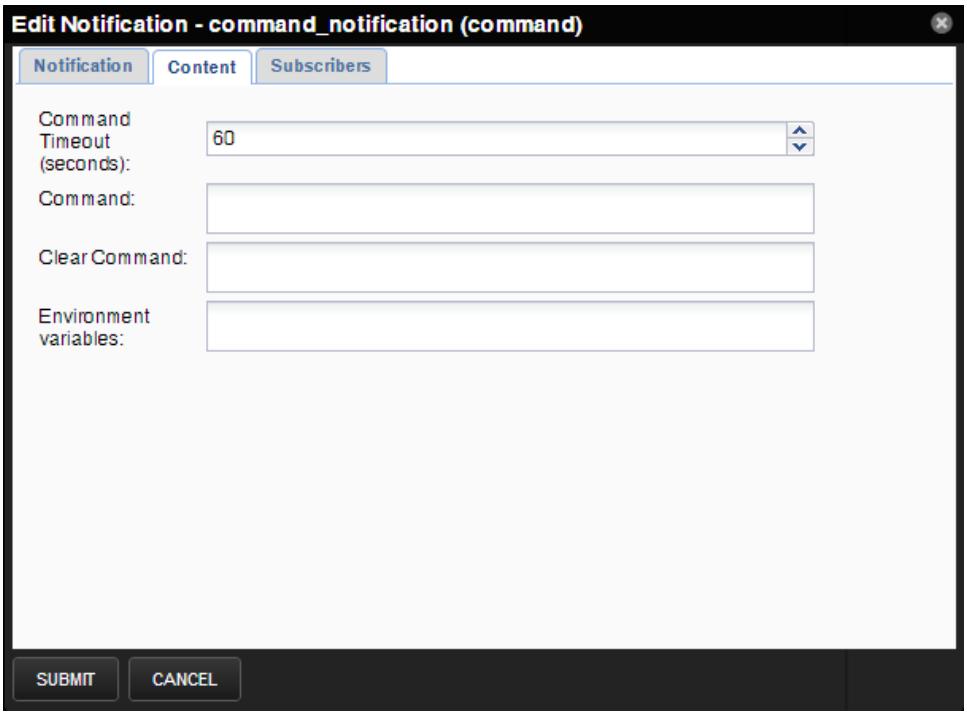


Defining Commands to Run

For Command-type notifications, you must specify the command to run when configured triggers are matched. Do this on the Content tab of the notification. Configure these fields:

- **Command Timeout** - By default, 60 seconds.
- **Command** - Command to run when a trigger is matched.
- **Clear Command** - Optional command to run when the triggering event clears.
- **Environment variables** -

Figure 25: Edit Notification Content (Command)



Global Notification Permissions

By establishing permissions, you can control which users have the ability to view, manage, and update notifications. Permissions are granted based on the user's assigned role. The following table lists account roles and their associated notification permissions:

Role	Permissions
Admin, Manager, ZenManager	Users assigned the Admin, Manager, or ZenManager roles can view, update, and manage any notification.
Notification owner	When a user creates a notification, he is designated the owner of that notification. During the life of the notification, the owner can view, update, and manage it.
All other users (including those assigned ZenUser and ZenOperator roles)	Must be specifically granted permissions through the interface to view, edit, or manage notifications.

You can set global permissions for viewing, updating and managing a notification. Global permissions are given to any user with "manage" permission, which includes:

- Admin, Manager, and ZenManager roles
- Notification owner

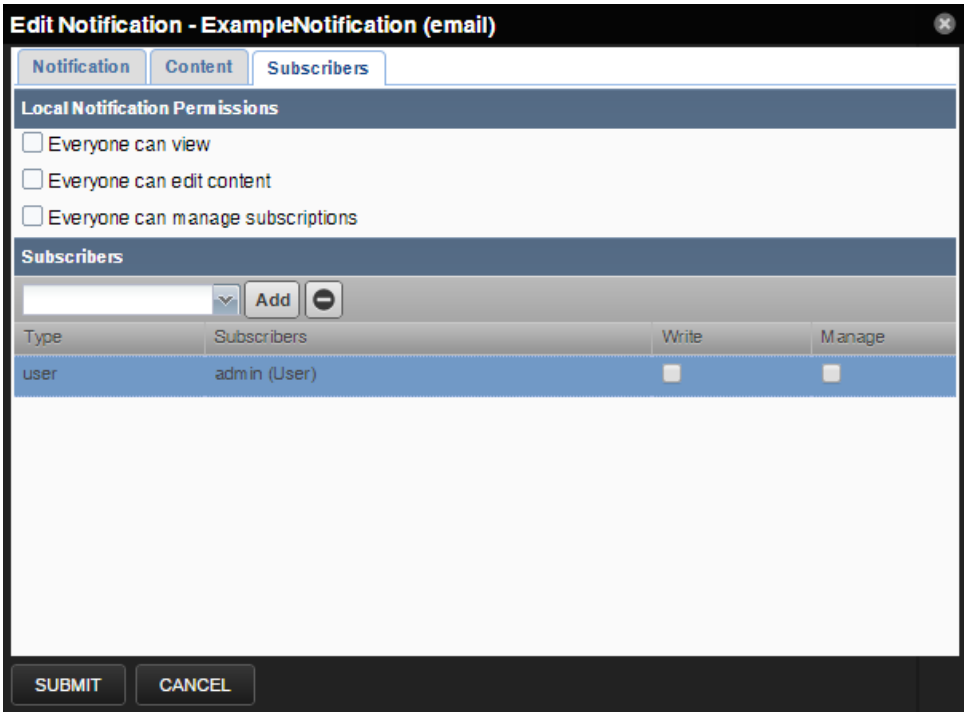
Edit global permissions from the Subscribers tab on the Edit Notification Subscription panel.

Global options are:

- **Everyone can view** - Provides global view permission.
- **Everyone can edit content** - Provides global update permission.
- **Everyone can manage subscriptions** - Provides global manage permission.

Permission checks occur when the data is sent to the browser and when any action occurs. To determine where a user can make modifications to a particular tab, permission checks are performed on global roles, then managerial roles, and then individual roles. Any role that provides the required permission will allow that permission's associated behavior.

Figure 26: Edit Notification



Setting Individual Notification Permissions

You can grant permissions to individual users or groups. For each user or group added, you can select:

- **Write** - Select this option to grant the user or group permission to update the notification.
- **Manage** - Select this option to grant the user or group permission to manage the notification.

You can manually enter in the name of a user or group, or select one from the list of options.

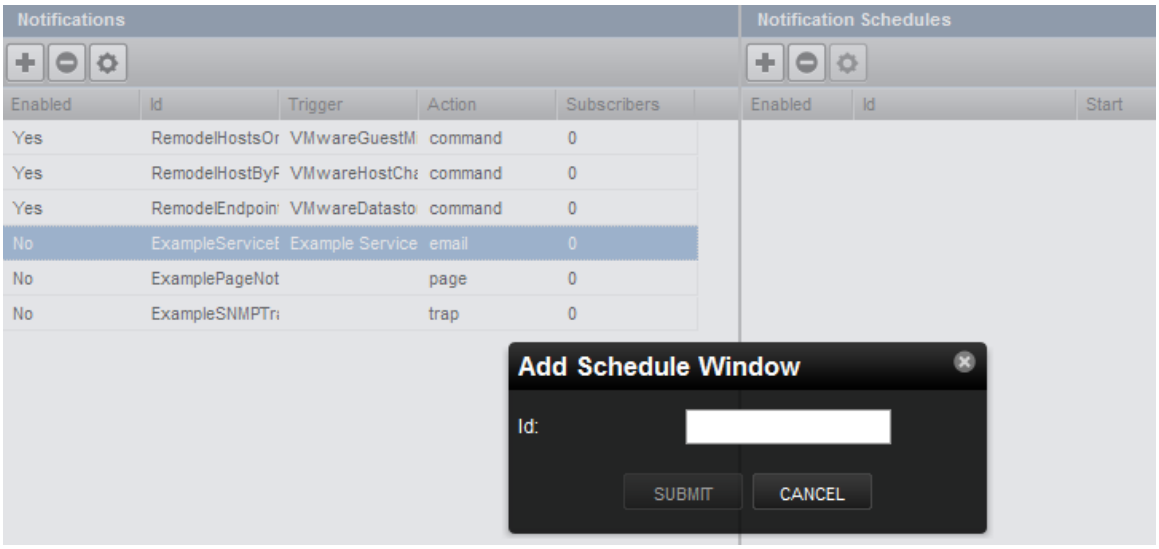
Setting Up Notification Schedules

You can establish one or more notification schedules for each defined notification. To set up a schedule:

1. Select the notification in the Notifications area.
2. Click Add in the Notification Schedules area.

   The Add Schedule Window dialog appears.

Figure 27: Add Notification Schedule



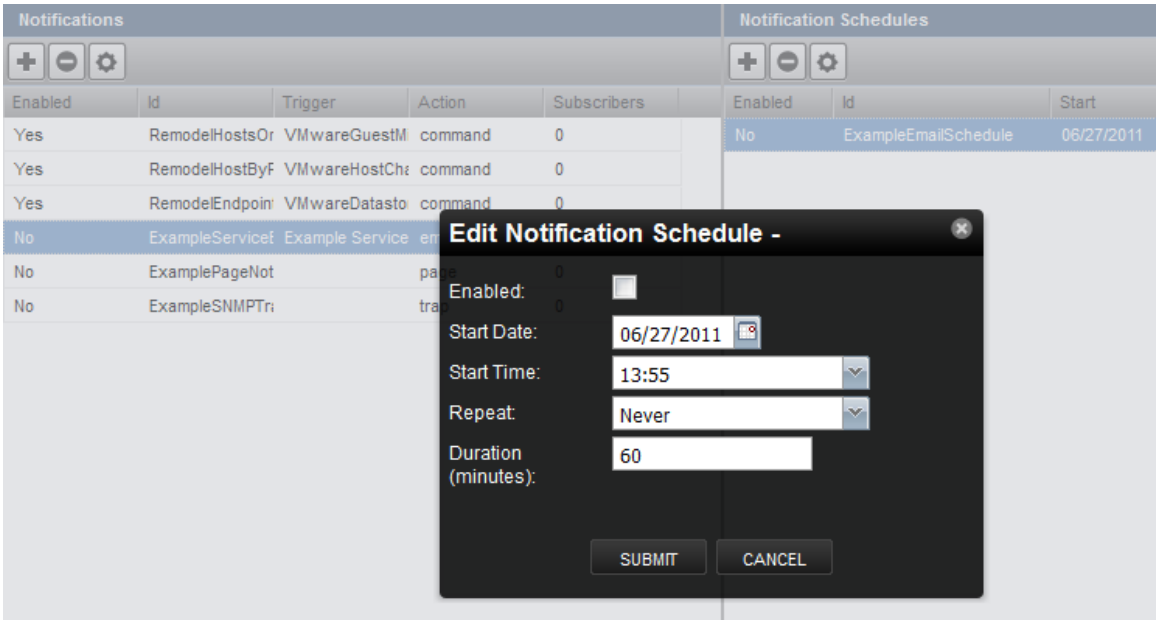
3 Enter a schedule ID, and then click **Submit**.

4 Double-click the newly added schedule to edit it. Select or enter values for the following fields:

- **Enabled**- Select to enable the schedule. By default, this schedule is not enabled.
- **Start Date**- Enter or select a start date for the schedule.
- **Start Time**- Enter or Select a start time for the schedule.
- **Repeat**- Select a schedule repeat value: Never, Daily, Every Weekday, Weekly, Monthly, or First Sunday of the Month.
- **Duration (Minutes)**- Enter a schedule duration, which is the period of time that the notification window is active. If a notification has notification windows specified, then notifications are sent only if one of the windows is active when the notification is received.

5 Click **Submit**.

Figure 28: Edit Notification Schedule



LDAP Authentication

You can use your existing LDAP authentication infrastructure, such as Active Directory or OpenLDAP, to enable single sign-on to the Cisco UCS Performance Manager interface. With this capability, you can use the user management tools with which you are familiar to enable your Windows users to use their Windows credentials to authenticate to the Cisco UCS Performance Manager interface. This saves you from having to manually create user accounts and separately maintain passwords.

For those LDAP properties that are mapped, changes you make in LDAP are updated in Cisco UCS Performance Manager. (You must clear your browser cache, or log out and back in, for properties changes to propagate immediately.)

LDAP Configuration Information

Before configuring LDAP authentication, you should gather the following information from your LDAP or Active Directory administrator:

- Host name or IP address of an Active Directory global catalog server (for Active Directory authentication)
- Host name or IP address of an LDAP server (for other LDAP server authentication)
- User's base distinguished name (DN)
- Manager DN
- Manager password
- Groups base DN
- Optionally, list of Active Directory groups to map to Cisco UCS Performance Manager roles

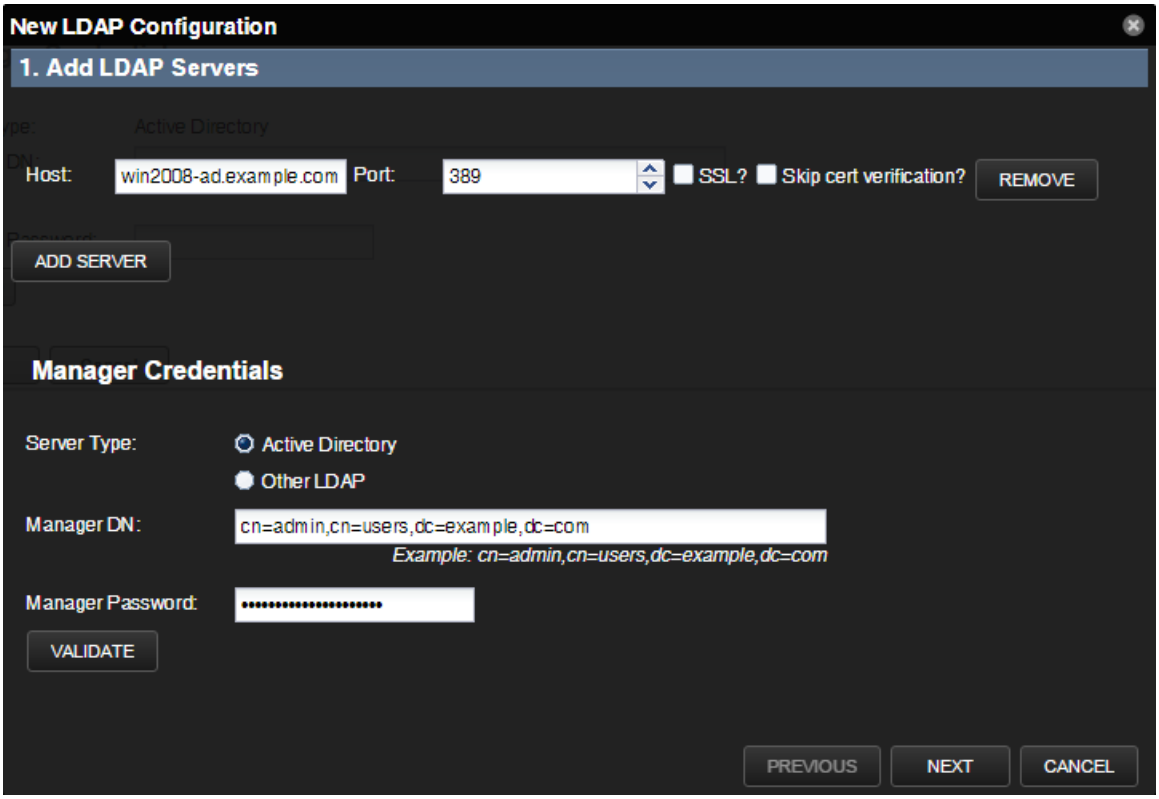
Configuring LDAP Authentication

You can configure LDAP authentication at initial setup, or from the Settings area of the interface:

- While in the setup wizard, at Step 2: Specify or Discover Devices to Monitor, click **LDAP Setup** (located at the bottom right of the wizard panel).
- From the interface, select **Advanced > LDAP** and click the **Add** icon.

The first panel (Add LDAP Servers) of the LDAP Configuration wizard appears.

Figure 29: LDAP Configuration Wizard (Add LDAP Servers)



1 Enter information and make selections:

- **Host**- Enter the host name or IP address of an Active Directory global catalog server (for Active Directory authentication) or the host name or IP address of an LDAP server (for Other LDAP server types).
- **Port**- Optionally, change the server port number. By default, the port number is 389.
- **SSL**- Select if using SSL. When you select this option, the default port number adjusts to 636.
- **Skip cert verification?**- If you are using a self-signed certificate, select this check box to skip its verification. Requires OpenLDAP 2.4 or higher.

2 Optionally, click **Add Server** to add another LDAP server. To remove a server from the list, click **Remove**.

3 Enter information and make selections in the Manager Credentials area:

- **Server Type**- Select a server type (Active Directory or Other LDAP).
- **Manager DN**- Enter the distinguished name of a user in the domain administrators group. An example that follows the user's base DN is:

```
cn=admin,cn=users,dc=example,dc=com
```

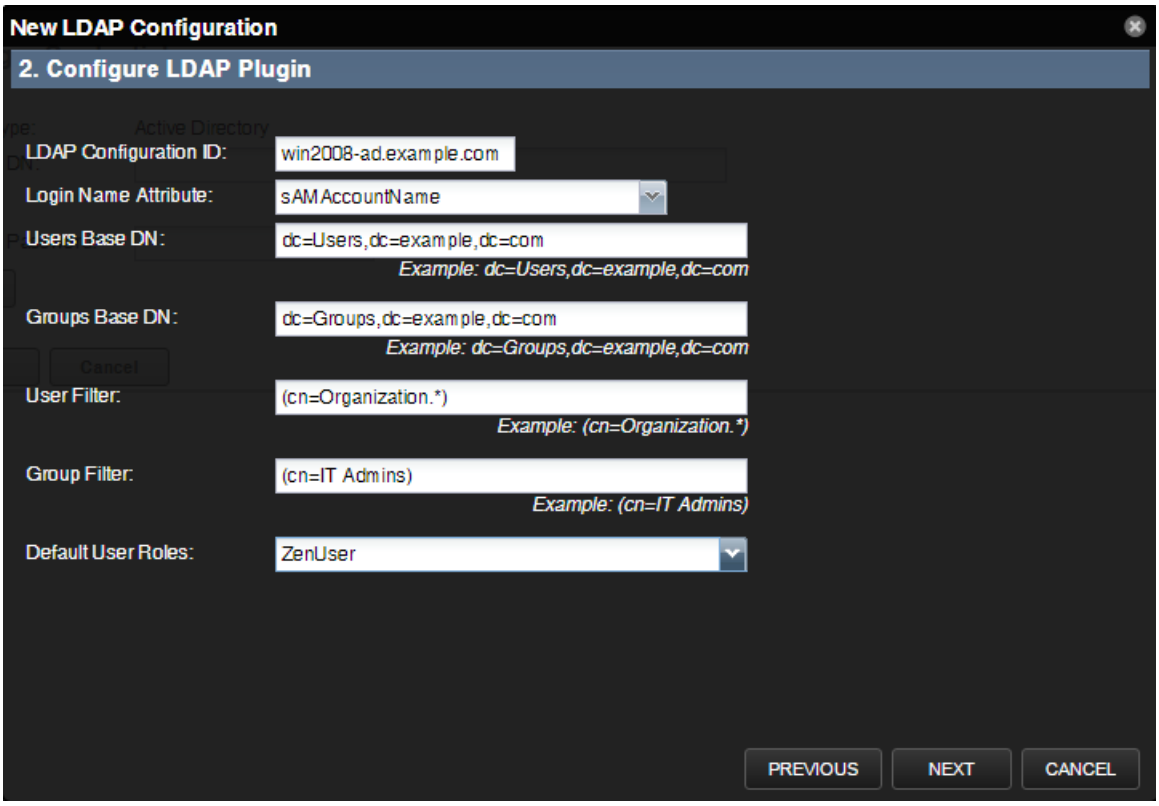
- **Manager Password**- Enter the password for the Manager DN.

4 Optionally, click **Validate** to ensure your setup is valid.

5 Click **Next**.

The second panel (Configure LDAP Plugin) of the LDAP Configuration wizard appears.

Figure 30: LDAP Configuration Wizard (Configure LDAP Plugin)



6 Enter information and make selections:

- **Login Name Attribute**- Select the LDAP record attribute used as the user name.

  Note You can edit the list of selections by adding attributes on the Mappings page of the LDAP configuration area (**Advanced > LDAP**).

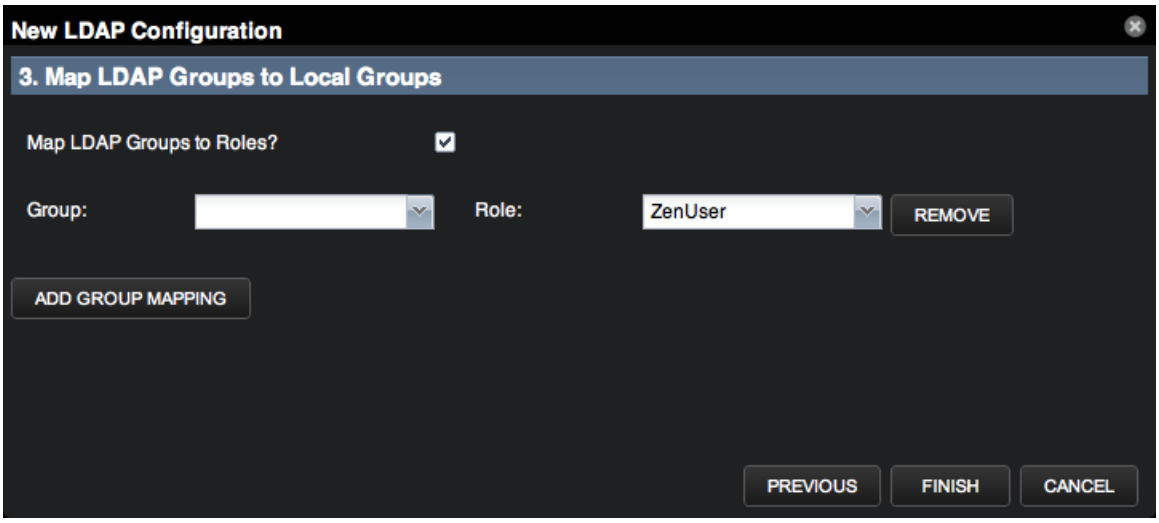
- **Users Base DN**- Enter the user's base distinguished name. For example, if your domain is ad.example.com, then your user's base DN might be:

  ```
  dc=Users,dc=example,dc=com
  ```

- **Groups Base DN**- Enter the DN for the branch of your LDAP database that contains group records. These group records are of the LDAP class "groupOfUniqueNames," and the entry CN attribute constitutes the group name.
- **User Filter**- Specify a free-form LDAP filter expression to be added to the default user search filter. The default user search filter and this additional search filter are combined as an AND expression. Records must satisfy both filters to be found using the various user searches. Any value specified in this field must follow correct LDAP search filter syntax.
- **Group Filter**- Specify a free-form LDAP filter expression to be added to the default group search filter. The default group search filter and this additional search filter are combined as an AND expression. Records must satisfy both filters to be found using the various group searches. Any value specified in this field must follow correct LDAP search filter syntax.
- **Default User Roles**- Specify one or more roles (by multi-selecting from the drop-down list) to be given to all users authenticated from your LDAP tree. Zope expects all users - anonymous as well as authenticated - to have the role Anonymous.

7 Click **Next**. The third panel (Map LDAP Groups to Local Groups) of the LDAP Configuration wizard appears.

Figure 31: LDAP Configuration Wizard (Map LDAP Groups to Local Groups)



8 Enter information and make selections:

- **Map LDAP Groups to Roles?**- Select this option if you want to control user roles within the Cisco UCS Performance Manager Web interface by using Active Directory groups, instead of controlling the roles directly from within the system.

  Note If you choose to use this option, then you should add the following groups to LDAP:

  - Cisco UCS Performance Manager Managers
  - Cisco UCS Performance Manager Users

- **Group**- Select the LDAP group to map to a Cisco UCS Performance Manager role.
- **Role**- Select the Cisco UCS Performance Manager role to map the LDAP group.

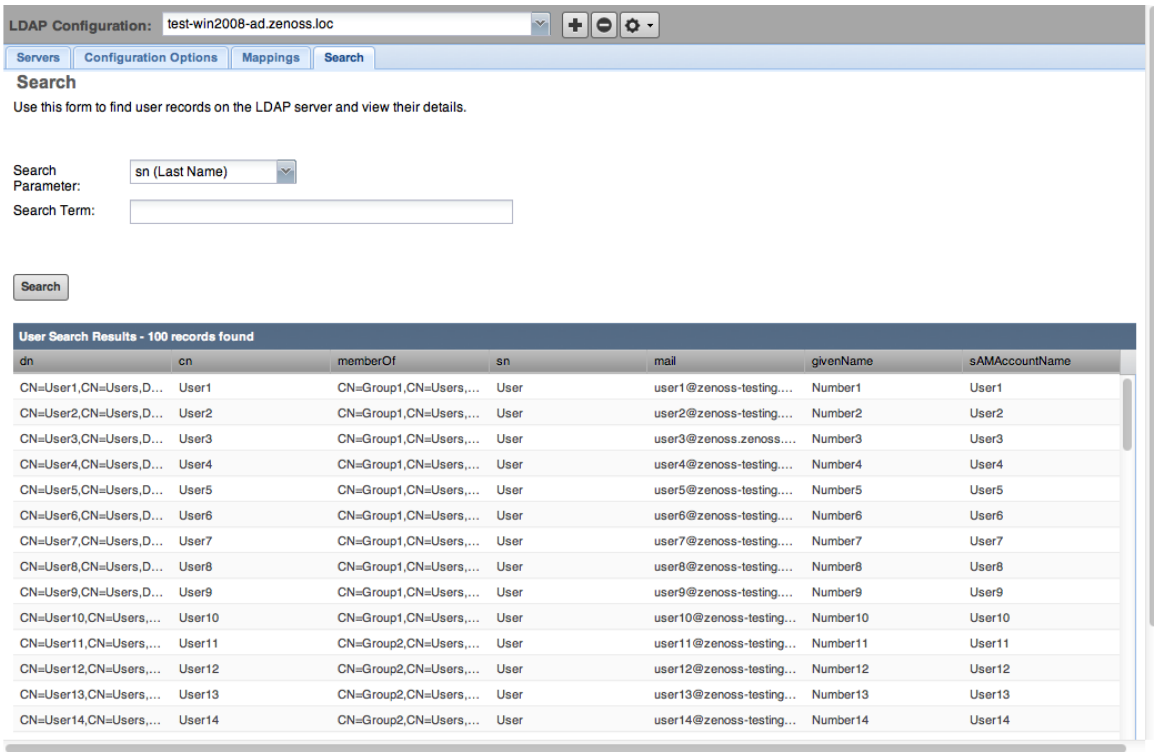
9 Optionally, click **Add Group Mapping** to map another group. To remove a mapped group, click **Remove**.

10 Click **Finish** to complete LDAP configuration.

After setup, you can edit your LDAP configuration settings from the Settings, Configuration Options, and Mappings tabs.

The Search tab allows you to locate user records on your LDAP server. Select from the list of search parameters, and optionally enter a search term, and then click **Search**. Search results return on the lower portion of the page.

Figure 32: LDAP Configuration - Search



Configuring Local Authentication as a Fallback

You can use local authentication as a fallback in the event that the LDAP server is unreachable. The local authentication plugin is called userManager.

1 Verify that the userManager plugin is available:

   a Go to the following URL to access the Zope Management Interface (ZMI):

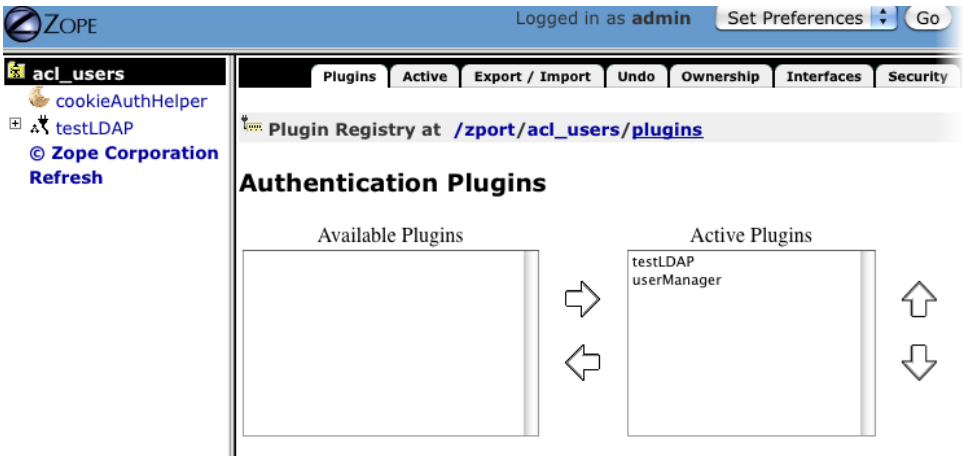
   `https://YourUCSPMSystem/zport/acl_users/manage`

   b In the Name column, click **plugins**.

   c Click **Authentication Plugins**.

   d Make sure that your LDAP plugin is first in the list of Active Plugins. (The userManager plugin must be below it.)

Figure 33: Authentication Plugins



2 Create a user with fallback capabilities. For example, to allow an LDAP user named `ucspm-user` to log in when the LDAP server is down:

   a In Cisco UCS Performance Manager, navigate to **Advanced > Users > Add New User**.

   b Create a user named `ucspm-user`.

   Note You must create this account before the user logs in with the LDAP credentials. The password defined when creating the account in Cisco UCS Performance Manager will be valid even when the LDAP server is down.

Product Licensing

Cisco UCS Performance Manager requires a license to be entered in order to use the user interface of the product. You typically enter your license file as part of the installation wizard, but if you do not enter a license at that time, you will be given a 30-day temporary license. Cisco UCS Performance Manager begins monitoring and collecting data as normal, even with the temporary license. The following sections describe how to manage and add licenses to the system. In the case that your license expires or you have exceeded the maximum number of servers for your license, Cisco UCS Performance Manager will continue to monitor and collect data, but you will be unable to access it through the user interface until you enter a valid license file. This ensures that you do not lose any data during a lapse in licensing.

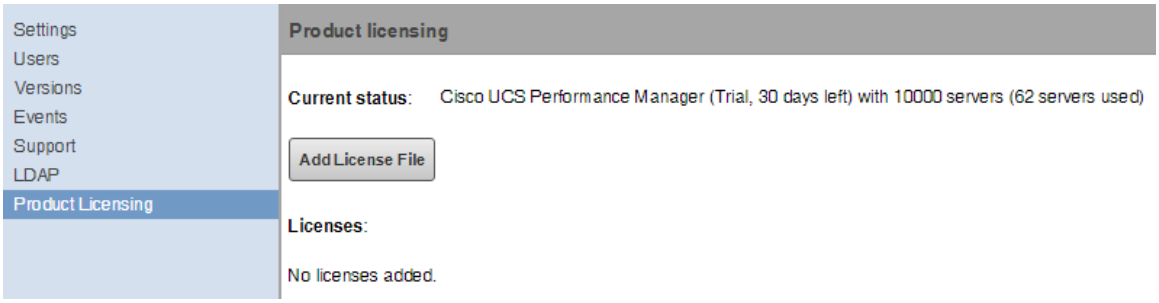
Managing Product Licenses

If you have your product license file(s) prior to installation, you can enter it as part of the installation wizard. However, if you don't enter it then or have to update your license, you can do so through the Cisco UCS Performance Manager user interface.

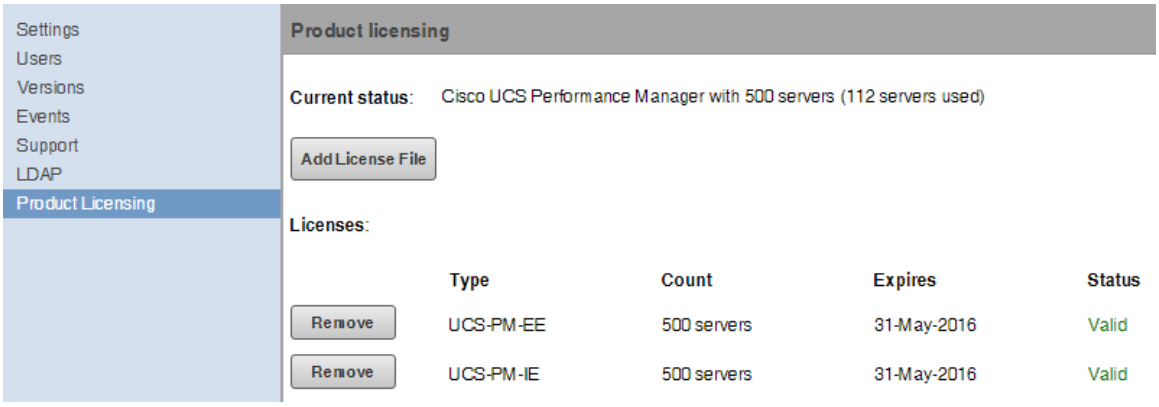
To manage your product license(s):

1 Select **Advanced > Product Licensing**. You will see the current status of your license(s). It will show whether you have a Cisco UCS Performance Manager or a Cisco UCS Performance Manager Express license along with an indication of the number of servers used and the total number of servers available with the licenses currently entered. Each license gives its type, count, expiration date, and status.

   The following image shows a system that is still using the trial license.



The following image shows a system with several valid licenses.



Note Cisco UCS Performance Manager licenses are indicated by the code `IE` in the type column, while Cisco UCS Performance Manager Express licenses are indicated by the code `EE`.

2. To add a license file, click **Add License File**. Then, select the file from your system and click **OK** to confirm. You can control-click to select multiple license files if needed.
3. To remove a license file, click **Remove** next to the license you wish to remove. Then, click **OK** to confirm.

Adding, Discovering and Modeling Devices 2

Modeling is the process by which the system:

- Populates the device database
- Collects information about the devices in the system (such as operating system type or file system capacity)

The system models devices when they are added to the database, either manually or through the discovery process.

Adding a Device

If you didn't add all your devices during the initial installation, you can add them post-installation using the Cisco UCS Performance Manager interface. Before you add any additional endpoints, network, storage, server, or hypervisor devices, follow the instructions in the *Cisco UCS Performance Manager Installation Guide* for preparing your device and for specific options you will be asked about on the appropriate wizard page.

Note Be aware of your naming convention when adding vSphere devices so that you don't add the same vSphere device with both its FQHN and its short hostname. Also, only add one vSphere device at a time and then perform initial modeling before adding another vSphere device.

To add a device from the Cisco UCS Performance Manager interface:

1. From the Navigation menu, select **Infrastructure**.

   The Devices page appears.
2. Click the **Add Devices** icon and make a selection:

   - Add Infrastructure
   - Add Cisco UCS
   - Add Cisco UCS Central Endpoint

   The appropriate dialog appears.
3. Enter information or make selections to add the device. For the Add Infrastructure dialog, you can add network, storage, server, and hypervisor devices. For the Add UCS Domains or Add UCS Central Endpoint dialog, you can enter credentials for your UCS domain or your UCS Central instance.
4. Click **Add**.

   Note You can view the Add Device job in progress. Click **View Job Log** in the notification that appears when you add the device.

When the job completes, the device is added in the selected device class.

5 Click **Done** when you have added all your devices.

Adding or Editing Information on a Device Record

You may want to add or edit details about a device.

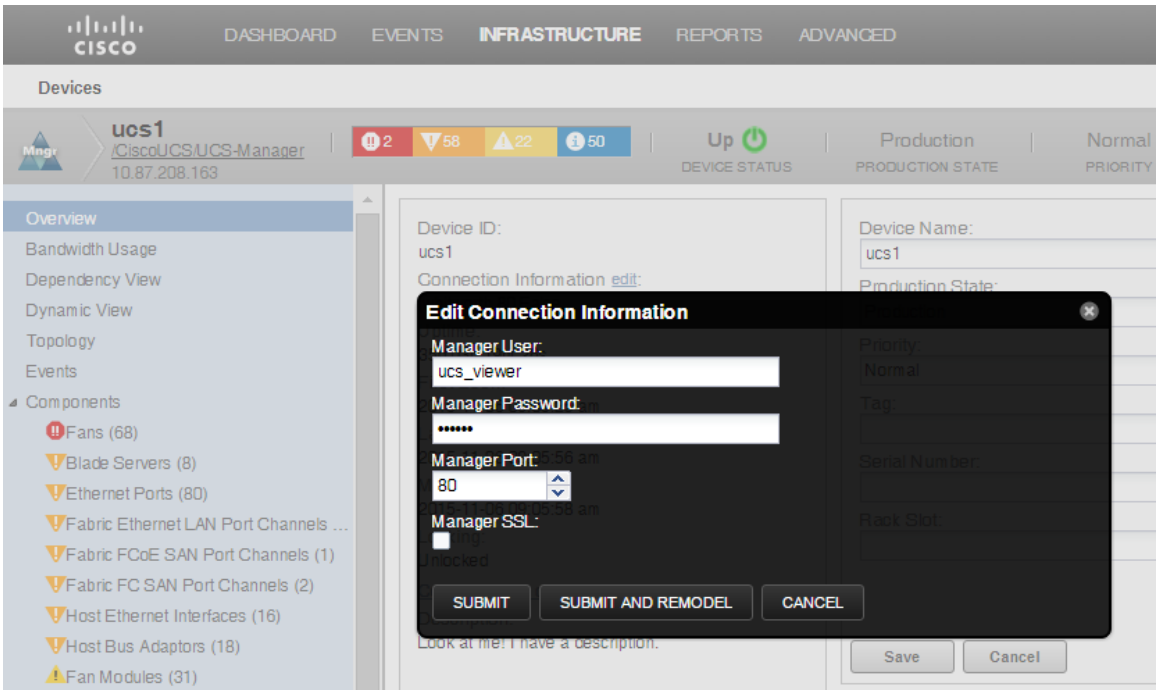
To add or edit information:

1 Click a device name in the devices list. The Device overview page appears.
2 You can select values to change, or click the "edit" link adjacent to a label to edit that value. Enter or change information in one or more areas, and then click **Save** to save your changes.

Editing Connection Information

To edit the connection information for an already monitored device:

1 Click a device name in the devices list. The Device overview page appears.
2 Click the Edit link next to Connection Information. The Edit Connection Information dialog appears.



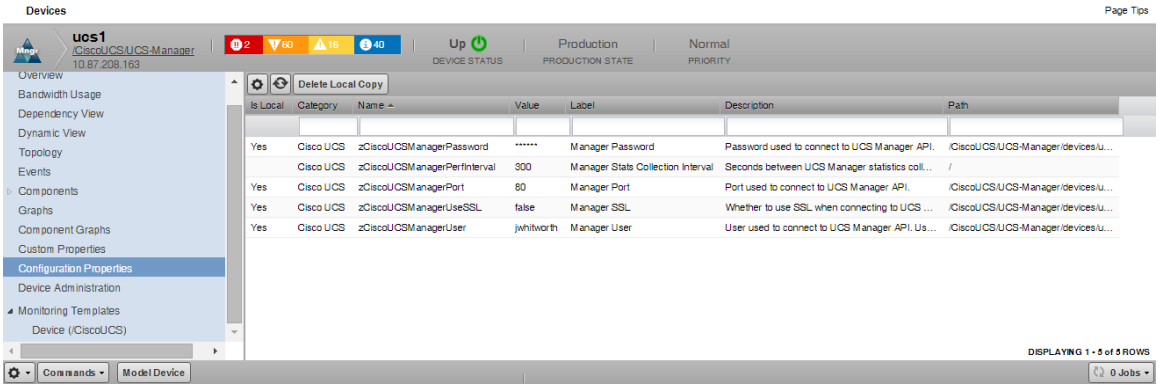
3 Edit the username, password, and/or port and select whether or not to use SSL.
4 Click **Submit** to submit the new connection information. The device will be remodeled at the next scheduled remodeling time.

   or

   Click **Submit and Remodel** to submit the new connection information and begin an immediate remodeling of the device.

Alternately, you can change the connection configuration properties one at a time from the devices Configuration Properties page. To view the device's configuration properties:

1 On the Device's details page, click **Configuration Properties**. The device-specific zProperties are displayed.



2 Double-click on the row of the property you want to change. For example, double-click `zCiscoUCSManagerPerfInterval` to edit the number of seconds between UCS Manager statistics collections. The Edit Config Property dialog appears.

3 Edit the appropriate field and click **Submit**. These changes will take effect during the next modeling cycle. To immediately remodel the device, click the **Model Device** button on the bottom of the Device Overview page.

Modeling Devices

To model devices, the system can use:

- SSH
- WinRM
- SNMP (legacy option)

Note SSH and WinRM are the recommended options.

The modeling method you select depends on your environment, and on the types of devices you want to model and monitor.

By default the system remodels each known device every 720 minutes (12 hours).

Note You can change the frequency with which devices are remodeled. Edit the value of the Modeler Cycle Interval in the collector's configuration.

For larger deployments, modeling frequency may impact performance. In such environments, you should stop the `zenmodeler` daemon and run the modeling process once daily from a cron job.

Testing to See if a Device is Running SNMP

To test whether a device is running SNMP, run this command:

```
$ snmpwalk -v1 -c
      communityString
      DeviceIDsystem
```

If this command does not time out, then SNMP is installed and working correctly.

You can set the version of SNMP to use by editing the zSnmpVer configuration property. Valid values include: v1, v2c, and v3. Click the **Configuration Properties** link on the device, and edit the zSnmpVer configuration property by double-clicking on it and selecting the SNMP version you want to use.

Configuring Windows Devices to Provide Data Through SNMP

By default, Windows may not have SNMP installed. To install SNMP on your particular version of Windows, please refer to the Microsoft documentation.

After setting up and configuring the SNMP service, you must set the zSnmpCommunity string in Cisco UCS Performance Manager to match, to obtain SNMP data.

If you want processor and memory monitoring, install SNMP-Informant on the device. Go to *http://www.snmp-informant.com* and download SNMP for Windows.

To collect Windows event logs or log files from a Windows box using syslog, you can use the SyslogAgent Windows add-on, available from:

http://syslogserver.com/syslogagent.html

Configuring Linux Devices to Provide Data Through SNMP

To configure a Linux machine for monitoring, it must have SNMP installed. A good Linux SNMP application is net-snmp. Download, install, and configure net-snmp to then use SNMP to monitor Linux devices.

Debugging the Modeling Process

You can run the modeler from the command line against a single device. This feature is useful when debugging issues with a plugin.

By passing the `--collect` command to the modeler, you can control which modeler plugins are used. For example, the following command runs only the interface plugin against the `build.zenoss.loc` device:

1. Log in to the Control Center host as a user with `serviced` CLI privileges.
2. Attach to the `zenmodeler` service.

```
serviced service attach zenmodeler
```

3. Change to the `zenoss` user.

```
su - zenoss
```

4. Run the `zenmodeler` command.

```
$ zenmodeler run -v10 --collect=IpInterface -d build.zenoss.loc
```

Working with Devices

3

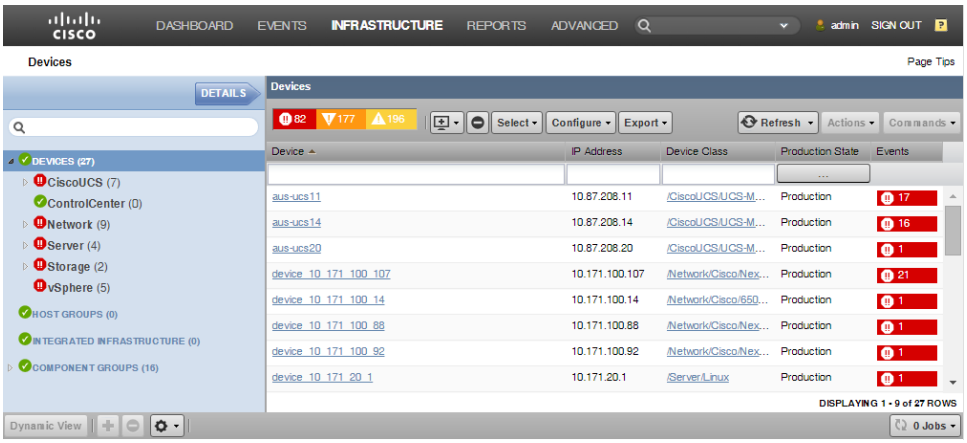
This chapter provides information and procedures for managing devices in the system.

Viewing the Device List

The device list shows all devices in the system. From this view, you can search for devices and perform a range of management tasks on all devices.

To access the device list, select **Infrastructure** from the Navigation menu.

Figure 34: Device List



Devices Hierarchy

Devices are organized in the tree view by:

- Devices
- Host Groups
- Integrated Infrastructure
- Component Groups

Click the indicator next to each category name to expand it and see included devices.

Managing Multiple Devices from the Device List

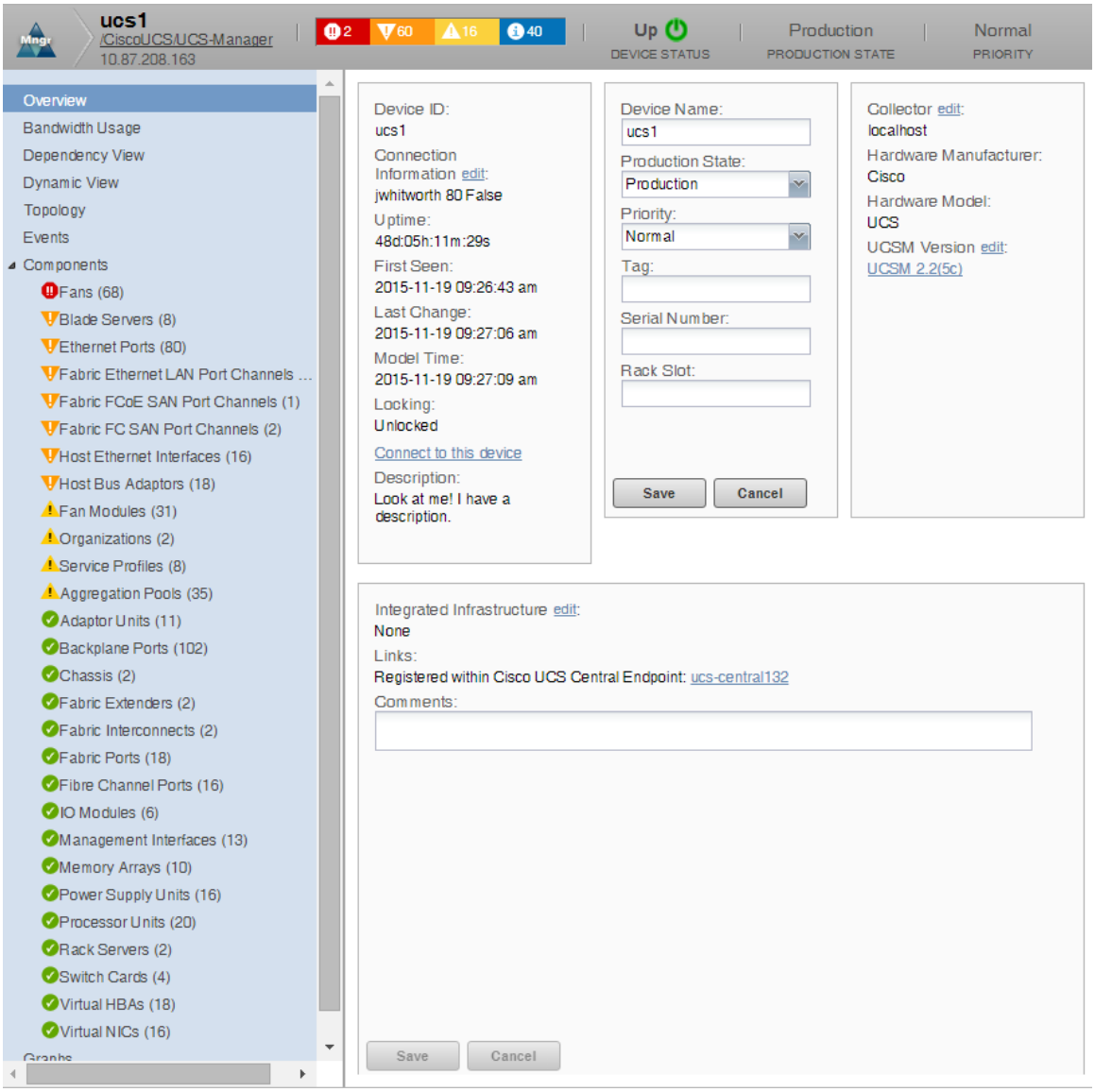
You can perform some management tasks for more than one device at a time. You can:

- Move devices to a different class (not available with Cisco UCS Performance Manager Express license)
- Assign devices to Host Groups and/or an Integrated Infrastructure
- Remove devices
- Perform actions such as assign priority and production state
- Lock devices

Working with Devices

To view details for a single device, click its name in the device list. The device overview page appears.

Figure 35: Device Overview



Event status is shown in the "event rainbow" at the top of the page. Other key information that appears at the top of the device overview page includes:

- Device name
- IP address used to communicate with the device
- Device status (shows the current results of a ping test)
- Production state (Pre-Production, Production, Test, Maintenance, or Decommissioned)
- Device description (taken from the UCS Manager System Description field and displayed in the UCS Inventory dashboard portlet)

When you open the page, device overview information displays. This view provides classification and status information. From here, you can edit device information (indicated by text fields or edit links). Editable fields include:

- Connection Information
- Device Name
- Production State
- Priority
- Tag
- Serial Number
- Rack Slot
- Collector
- Hardware and software manufacturer and model

Clicking **Connect to this device** will initiate direct access to the device. For a UCS device, it will lauch the UCS Manager. For ease of use, you may want to right-click the link and open the connection in another browser tab. For a Linux device, it will lauch an SSH window, etc.

The System area allows you to add or remove associated systems.

In vSphere and Servers, you also have the ability to add or remove associated groups.

The Links area displays links between the device and other external systems.

The left panel of the device overview page allows you to access other device management views depending on the device class:

- Bandwidth Usage
- Dependency View (new in 2.0)
- Dynamic View
- Topology
- Events
- Components
- Graphs
- Custom Properties (new in 2.0)
- Configuration Properties
- Device Administration (new in 2.0)
- Administration

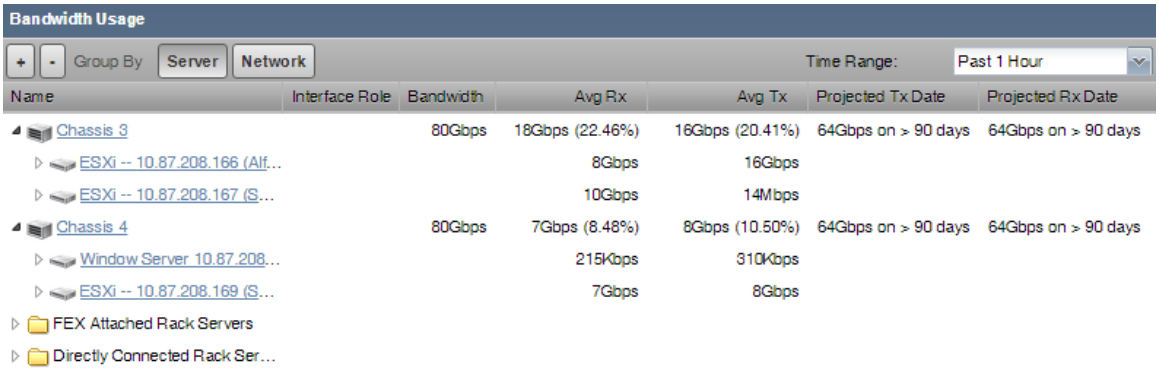
Information that appears here varies depending on device type.

Bandwidth Usage

The Bandwidth Usage view of a device shows different views of the network traffic as compared to its bandwidth. You can display the information grouped by server components or by network components for a specific time range (past 1 hour, past 6 hours, or past day).

To see the bandwidth usage on the various blades of each chassis:

1 From a device's Overview page, click **Bandwidth Usage**. The Bandwidth Usage page along with its associated graphs appears.
2 Ensure that the Group By **Server** button is activated and expand the menu items under the chassis you are interested in. Optionally, you can click **+** (Expand All) or **-** (Collapse All) to quickly open and close all the components.

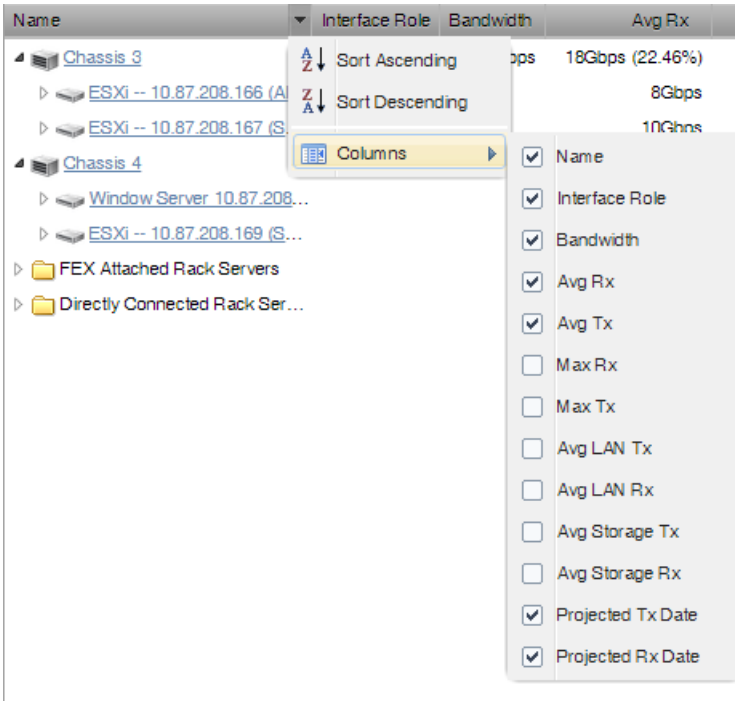


3 The bandwidth for the chassis appears along with the average transmitted and average received rates broken down by blade as well as projected exhaustion dates. You can also drill down on the chassis to view hypervisors (Hyper-V) and VMs.

Note The aggregation pool values (e.g., the top level chassis/fex) are calculated at an interval of 10 minutes which may result in some variance compared to the sum of the values of the underlying ports.

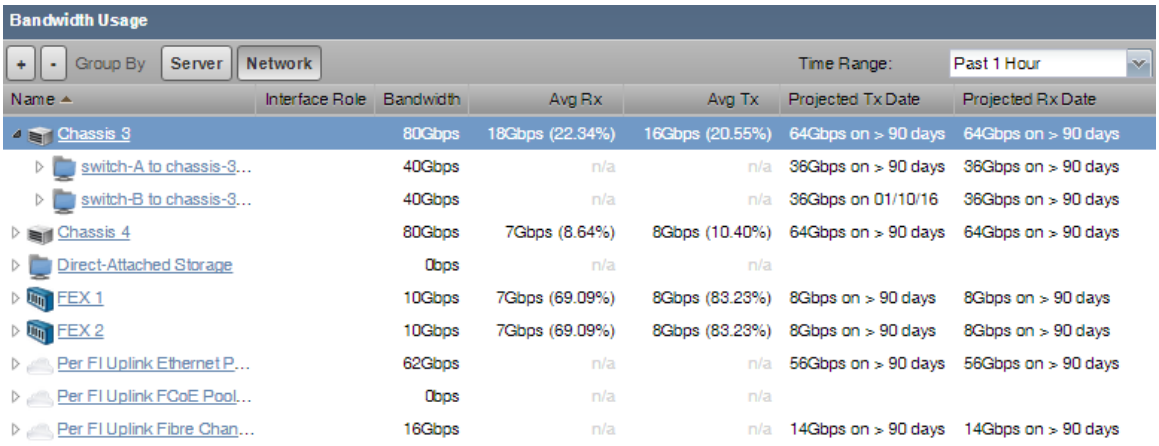
---

4 You can change the time range to either the past 6 hours or the past day by changing the value in the Time Range field.
5 You can add or remove columns from the display by clicking the arrow next to any column header, scrolling down to **Columns** and selecting the information you are interested in displaying from the flyout menu.



To see the bandwidth usage grouped by network:

1. From a device's Overview page, click **Bandwidth Usage**. The Bandwidth Usage page along with its associated graphs appears.
2. Click the Group By **Network** button and expand the menu items under the information you are interested in. You can drill down to the port level.

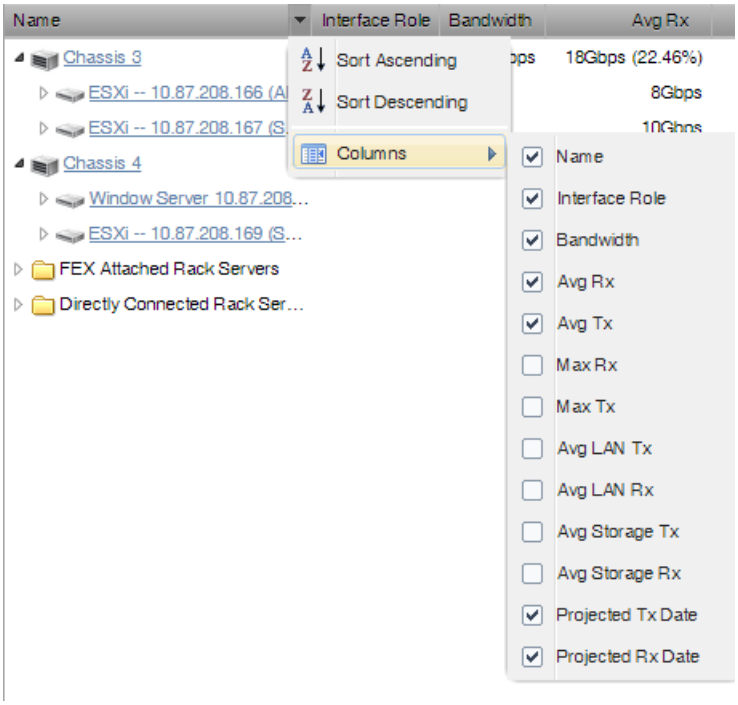


Name	Interface Role	Bandwidth	Avg Rx	Avg Tx	Projected Tx Date	Projected Rx Date
Chassis 3		80Gbps	18Gbps (22.34%)	16Gbps (20.55%)	64Gbps on > 90 days	64Gbps on > 90 days
switch-A to chassis-3...		40Gbps	n/a	n/a	36Gbps on > 90 days	36Gbps on > 90 days
switch-B to chassis-3...		40Gbps	n/a	n/a	36Gbps on 01/10/16	36Gbps on > 90 days
Chassis 4		80Gbps	7Gbps (8.64%)	8Gbps (10.40%)	64Gbps on > 90 days	64Gbps on > 90 days
Direct-Attached Storage		0bps	n/a	n/a		
FEX 1		10Gbps	7Gbps (69.09%)	8Gbps (83.23%)	8Gbps on > 90 days	8Gbps on > 90 days
FEX 2		10Gbps	7Gbps (69.09%)	8Gbps (83.23%)	8Gbps on > 90 days	8Gbps on > 90 days
Per FI Uplink Ethernet P...		62Gbps	n/a	n/a	56Gbps on > 90 days	56Gbps on > 90 days
Per FI Uplink FCoE Pool...		0bps	n/a	n/a		
Per FI Uplink Fibre Chan...		16Gbps	n/a	n/a	14Gbps on > 90 days	14Gbps on > 90 days

Note The aggregation pool values (e.g., the top level chassis/fex) are calculated at an interval of 10 minutes which may result in some variance compared to the sum of the values of the underlying ports.

Note You can also see fiber channels and ethernet port channels as groups in the aggregation pools.

3. You can change the time range to either the past 6 hours or the past day by changing the value in the Time Range field.
4. You can add or remove columns from the display by clicking the arrow next to any column header, scrolling down to **Columns** and selecting the information you are interested in displaying from the flyout menu.



Dependency View

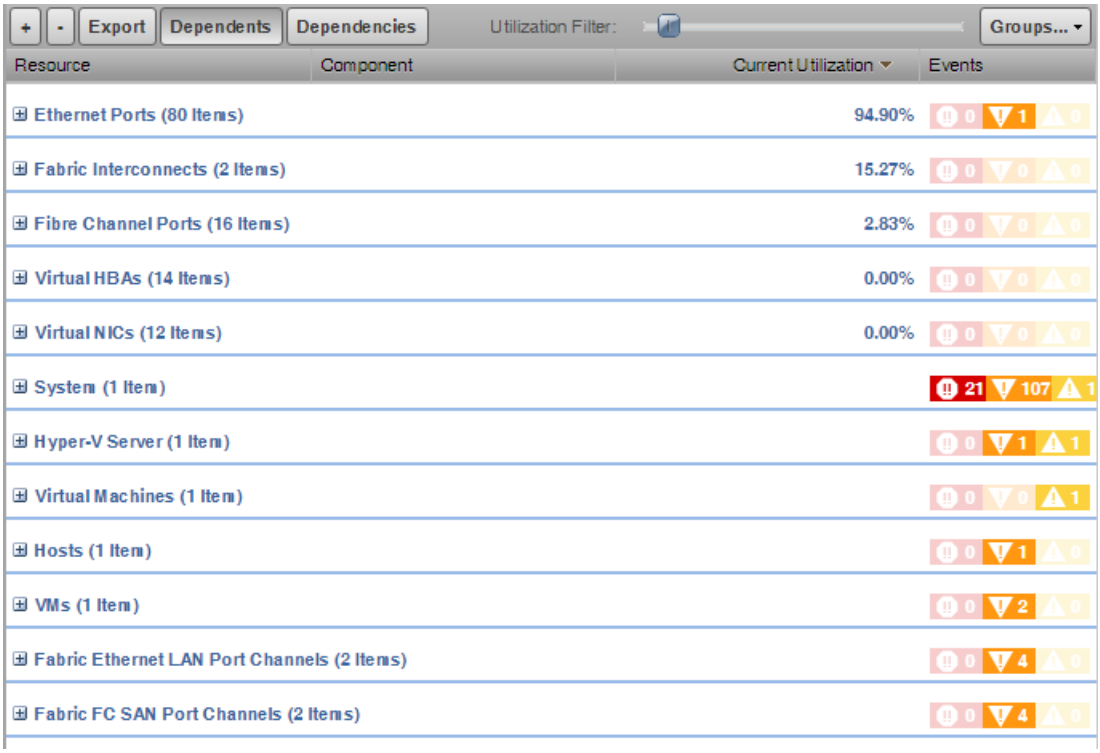
The dependency view of a device shows the resources that are dependent on the selected device as well as those resources that the device is dependent on. In this view, you can see the resource, associated component, current utilization and any events related to the component.

There are several places where you can see a dependency view:

- Device Overview page
  - Navigate to the device overview page and select **Dependency View**
- Device Component page
  - Navigate to the device overview page and select the component you are interested in. In the **Display** drop-down list, select **Dependencies**.
- Group Details page (including Host Groups, Integrated Infrastructure, and Component Groups)
  - Navigate to the Group or Integrated Infrastructure name and click **Details**. Then, select **Dependency View**.

Regardless of how you navigate to the Dependency View, the functionality remains the same. The following shows a sample Dependency View.

Figure 36: Dependency View



1. Click the **+** (Expand All) icon to see all the component under each listed resource. Click the **-** (Collapse All) icon, to return to the default view. You can also expand an individual
2. Export the data displayed by clicking the **Export** button. A `.csv` file is exported with the data as it is presented in the view.
3. Click **Dependents** to see the resources that are dependent on the selected device or component. Click **Dependencies** to see the resources that this device or component is dependent on. For example, if you click the Dependency View of a Hyper-V server, you will see that VMs, datastores, and other resources are dependent on the Hyper-V server, while the server itself is dependent on the Host CPUs, HDDs, and Network Adapters (seen after clicking **Dependencies**).
4. Slide the **Utilization Filter** slider bar to limit the display to resources that meet the utilization threshold selected on the slider bar. The default is to show components that are using zero percent or greater utililization. Move the slider bar to the right until the desired utilization filter is displayed. To show all the resources, slide the bar to the far left. Regardless of the percentage you choose on the **Utilization Filter** slider, you will always see components that have events logged against them, even though they do not meet the utilization criteria selected.
5. Expand the view of a particular resource by clicking the expand icon next to the resource.
6. Click **Groups** to select the resources that you want to display in the view.

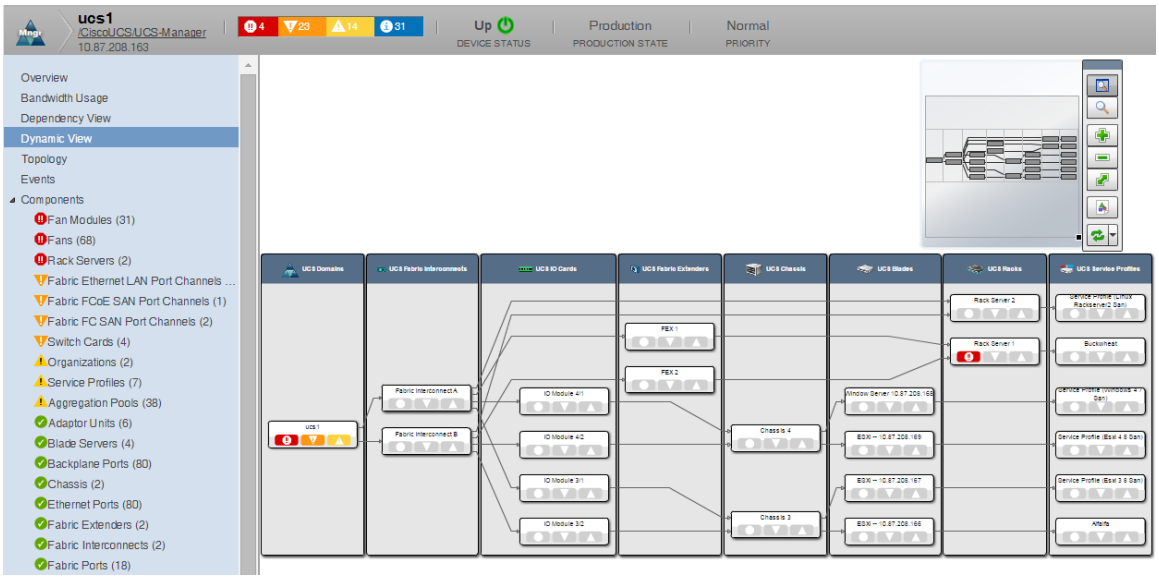
All selections made with respect to the display of the view will be saved so that when a particular user selects another dependency view, Cisco UCS Performance Manager renders the dependency view using the same parameters. This is only applicable for the same user. There is no global setting available for the dependency view.

Dynamic View

Cisco UCS Performance Manager provides a dynamic visualization of system objects and their relationships to other objects.

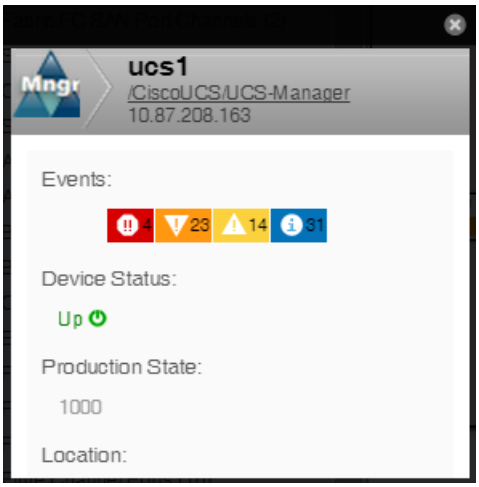
You can access a dynamic view from host groups, an integrated infrastructure, or server devices (registered OS). Depending on the object type, different relationships are illustrated. Each dynamic view shows related objects in a graph. Each object in that graph displays its associated event information.

Note For vSphere, the only dynamic view available is through a host group.



When you click an object in the graph, the "inspector" panel appears. This panel provides detailed information about the object and links directly to it. Information that appears in the inspector depends on the object type selected.

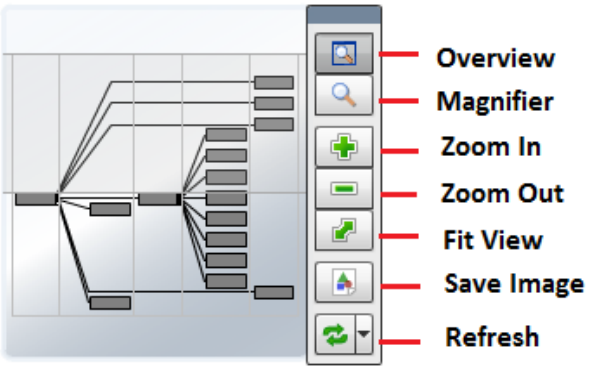
Figure 37: Dynamic View: Inspector Panel



View controls appear to the right of the graph. These allow you to adjust your view:

- **Overview** - Toggles display on and off of the graph overview illustration.
- **Magnifier** - Toggles on and off the magnifier, which allows you to magnify selected portions of the graph.
- **Zoom In** - Zooms in on the graph.
- **Zoom Out** - Zooms out on the graph.
- **Fit View** - Fits the graph to the browser page.
- **Save Image** - Saves the dynamic view as a `.png` image.
- **Refresh** - Refreshes the graph.

Figure 38: Dynamic View: View Controls



Dynamic View of Devices

The dynamic view of devices shows the relationship between a device and monitored components.

To access the dynamic view for a device:

1 From **Infrastructure > Devices**, click a device in the device list. The device overview page appears.
2 Select **Dynamic View** in the left panel.

Dynamic View of Cisco UCS Devices

On Cisco UCS devices, the dynamic view shows the components and relationships that make up a Cisco UCS domain. The following list describes the components that are listed in the Dynamic View for various types of UCS devices:

- UCS Classic
  - UCS Domains
  - UCS Fabric Interconnects
  - UCS Fabric Ports
  - UCS IO Cards
  - UCS Fabric Extenders
  - UCS Chassis
  - UCS Blades
  - UCS Racks
  - UCS Service Profiles (only those bound to servers)
- UCS Mini
  - UCS Domains
  - UCS FI-IO Modules
  - UCS Chassis
  - UCS Blades
  - UCS Service Profiles (only those bound to servers)

Dynamic View of Storage Devices

On storage devices, such as NetApp Filers, there are two dynamic views:

- **Physical Storage View** - Shows the device's storage enclosures and associated hard disks.
- **Logical Storage View** - Shows the logical storage arrangement that the storage device presents, such as file systems and raid groups.

Events

Detailed information about events, scoped to the device, appears in the Events view. From here, you can:

- Sort event and event archive information by a range of categories
- Classify and acknowledge events
- Filter events by severity, state, or by one of several categories

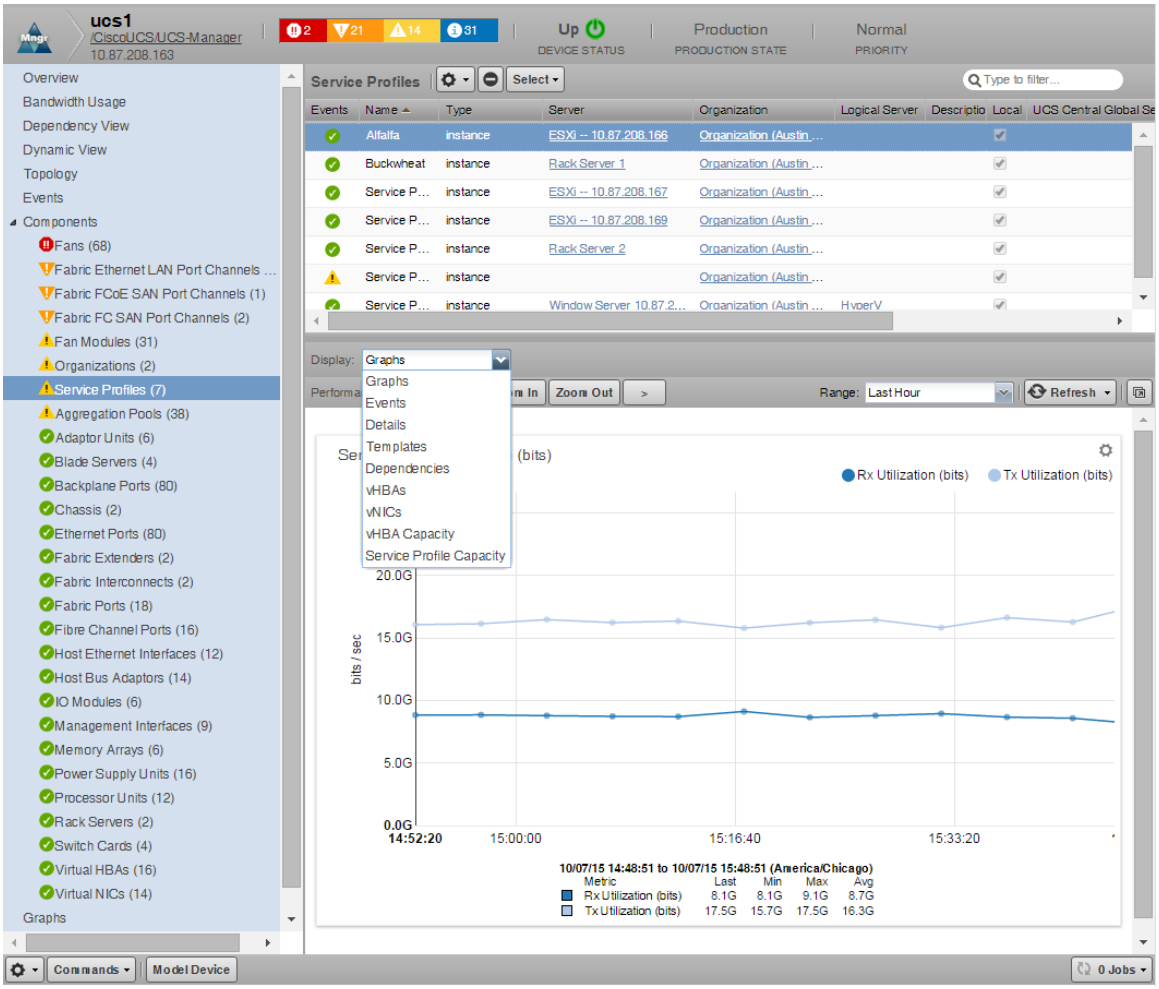
Components

The Components view provides information about the different types of device components, including:

- Adaptor Units
- Aggregation Pools
- Backplane Ports
- Chassis
- Ethernet Ports
- Fabric Extenders
- Fabric Interconnects
- Fabric Ports
- Fans
- Fan Modules
- Fibre Channel Ports
- Host Ethernet Interfaces
- Host Bus Adaptors
- IO Modules
- Management Interfaces
- Memory Arrays
- Organizations
- Power Supply Units
- Processor Units
- Rack Servers
- Server Blades
- Service Profiles
- Switch Cards
- Virtual HBAs
- Virtual NICs

To access components information, select Components in the left panel, and then select a component type.

Figure 39: Device (Components)



The status of each device component type, as shown by the color of its indicator, is determined by the collective status of the monitored components of the same type. For example, if the Ethernet Ports status is green, then all monitored Ethernet Ports are functioning normally. If there is an event related to a monitored Ethernet Port, then the highest severity event associated with that component is displayed.

Note If there is an event unrelated to a known component, then the system places it in the component type Other.

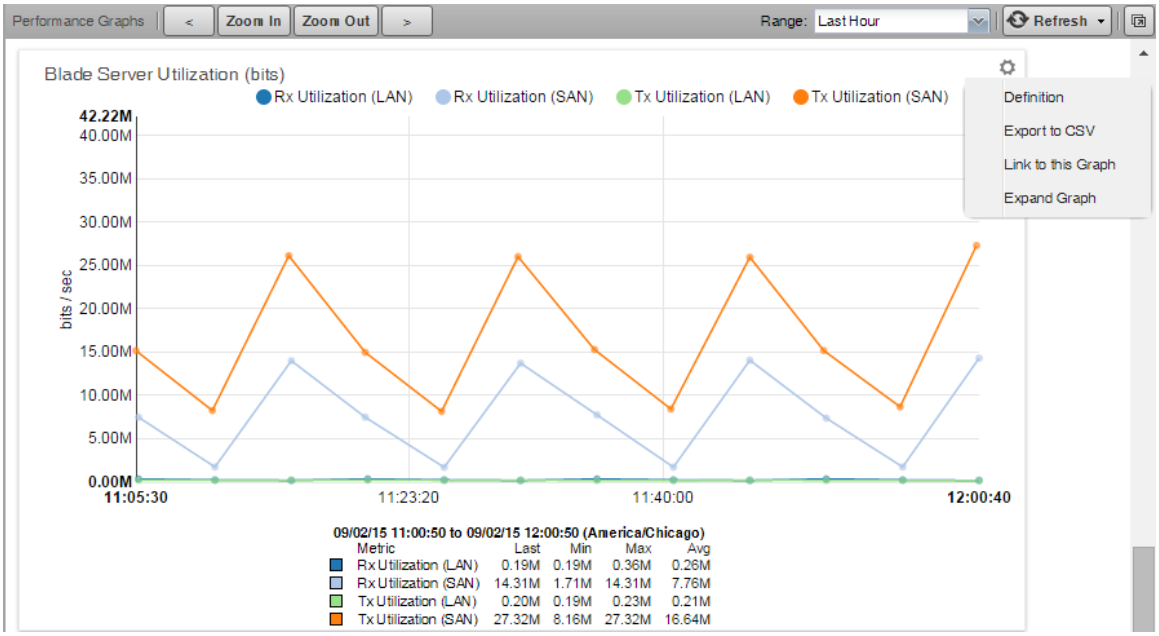
From this view, you can:

- Lock components
- Turn on or off component monitoring
- Delete components
- Display Graphs, Events, Details, Templates, and any other component-specific information.

Graphs

The Graphs view shows performance graphs defined for the device or component. To access graphs, select **Graphs** in the left panel. The following figure shows a performance graph for a blade server. The Action (gear) icon has been selected for illustrative purposes.

Figure 40: Performance Graphs



Note Hovering on the graph displays a vertical timeline with a popup displaying all values for that specific time.

You can control these performance graph options:

- **Zoom In/Zoom Out** - Click to narrow or expand the size of the time range for display. You can also click the forward and back arrowheads to scroll through time on the graph. Clicking any of these controls automatically puts you into a Custom time range. See below.
- **Range** - Select the span of time displayed in the graph. You can select:
  - Last Hour
  - Yesterday
  - Last Week
  - Last 30 days
  - Last Year
  - Custom - Select the Start and End time to display. Check **Now** to set the end time to the current time. Whenever you make a change to a custom range setting, click **Refresh** to update the graph.
- **Refresh** - Modify the refresh value (by default, 30 minutes) by clicking the drop-down list. Setting the refresh rate to manual requires you to click **Refresh** each time you want to update the graph.
- **Pop-out** - Click this icon to render the current graphs in full-screen mode.
- **Action (gear)** - Click this icon to open a submenu of actions including:
  - **Definition** - Select to view the graph's JSON definition.
  - **Export to CSV** - Select to export the graph data to a `.csv` file for further analysis. Only the data contained in the defined range will be included.
  - **Link to this Graph** - Select this option and drag the generated link to your browser's bookmark bar to link directly to this graph. The graph will be populated using the last set time range, however the end time will be the current time you click the link.
- **Table Legend** - Hovering over a legend description will highlight that particular data set. You can also click on a legend description to toggle its display. A solid dot indicates data will be displayed. A hollow dot indicates data will be hidden.

Managing Devices and Device Attributes

Read the information and procedures in this section to learn about specific device management tasks, including:

- Clearing heartbeat events
- Pushing configuration changes to the system
- Locking device configuration
- Renaming devices
- Remodeling devices
- Setting the device manage IP address

Clearing Heartbeat Events

If you have devices configured to send a recurring event that is mapped to a heartbeat class, you can clear stale heartbeat events.

To clear the heartbeat events associated with a device:

1. Navigate to Advanced > Settings.
2. In the left panel, select Events.
3. At the bottom of the Event Configuration page, click the **Clear** button in the Clear Event Heartbeats section.

   The system displays a brief message banner.

Locking Device Configuration

You can lock a device's configuration to prevent changes from being overwritten when remodeling the device. Two levels of locking are available. You can lock the configuration from deletion and updates, or solely from deletion.

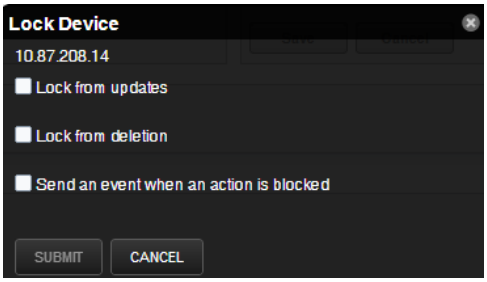
Note Device locking prevents changes and deletion due to remodeling. It does not prevent manual changes and deletion.

To edit lock selections for a device configuration:

1. Navigate to the device in the device list.
2. At the bottom of the device overview page, select **Locking** from the Action menu.

   The Lock Device dialog appears.

   Figure 41: Lock Device Dialog

3. Select the type of lock you want to implement or remove.
4. To send events when actions are blocked by a lock action, select the "Send an event..." option.

   The lock or unlock action is implemented on the device, and the system displays a confirmation message of the action.

Renaming a Device

Because the system uses the manage IP to monitor a device, the device name may be different than its fully qualified domain name (FQDN). The device name must always be unique in the system.

To rename a device:

1 Navigate to the device in the device list. Click the device name.
2 On the device overview page, edit the Device Name field with the new device name.
3 Click **Save**.

The system renames the device and displays a confirmation message of the action.

Remodeling a Device

Remodeling forces the system to re-collect all configuration information associated with a device. Normally, the system models devices every 720 minutes; however, if you want to remodel a device immediately, follow these steps:

1 Navigate to the device in the device list and click on the Device name.
2 At the bottom of the Device Overview page, click the **Model Device** button.

The system remodels the device. A dialog appears that shows progress of the action.

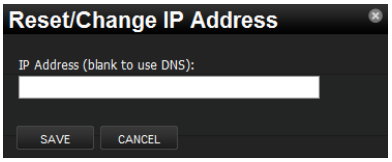
Resetting the Device Manage IP Address

You might want to reset the manage IP address if the IP address of a device has changed and you want to maintain the historical data at the original IP address. To reset the manage IP address of a device:

1 Navigate to the device in the device list.
2 At the bottom of the device overview page, select Reset/Change IP Address from the Action menu.

The Reset IP dialog appears.

Figure 42: Reset IP Dialog



3 Enter the new IP address for the device, or leave the field blank to allow the IP address to be set by DNS.
4 Click **Save**.

The IP address for the device is reset.

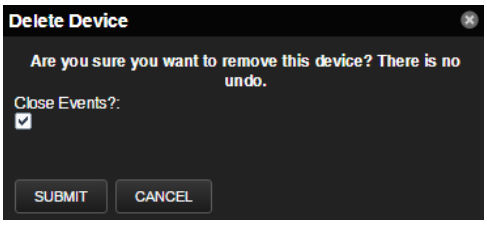
Deleting a Device

To delete a device from the system:

1 Navigate to the **Infrastructure** page.
2 Select the device you want to remove from the system by clicking on its row. You can select multiple devices by Ctrl-clicking or Shift-clicking the devices. Be sure to click on the row in an area that is not defined by a link.

The Delete Device dialog appears.

Figure 43: Delete Device



3 Optionally, change the selection to close current events for the device. By default, event data is removed.
4 Click **Submit**.

The system removes the device(s) and associated data (if selected), and displays a confirmation message of the action.

Working with Host Groups

Host groups consist of a number of UCS domains or VMs that are running on the hosts of UCS domains. These groups allow you to view the operating systems so that you can view events from the UCS resources that support the host group. In addition, you can quickly identify which of these operating systems are affected by capacity issues. Host groups can only be used for Linux and Windows targets. There are many different use cases for setting up host groups. One scenario would be to set up a host group for production devices and another for test devices. Another scenario might be to create a host group for devices supporting a particular business unit or location.

It is crucial to understand the importance of monitoring servers (bare metal and VM OS) so that you have a more meaningful dynamic view of all the tiers of an application stack with just one view.

Creating a Host Group

To create a host group using devices that are already being monitored:

1 Navigate to the **Infrastructure** page to view a list of the monitored devices.
2 Click **Host Groups** in the left column.
3 Click the **Add** icon in the lower-left portion of the window. The Add Group dialog appears.
4 Enter the name and a description of the host group (e.g., Production or Austin). Click **Submit**. The new host group name appears in the left column.
5 Click **Devices** or a device class to display a list of monitored devices.
6 Select the server (OS) device(s) you want to add to the host group by clicking or control-clicking on each row.

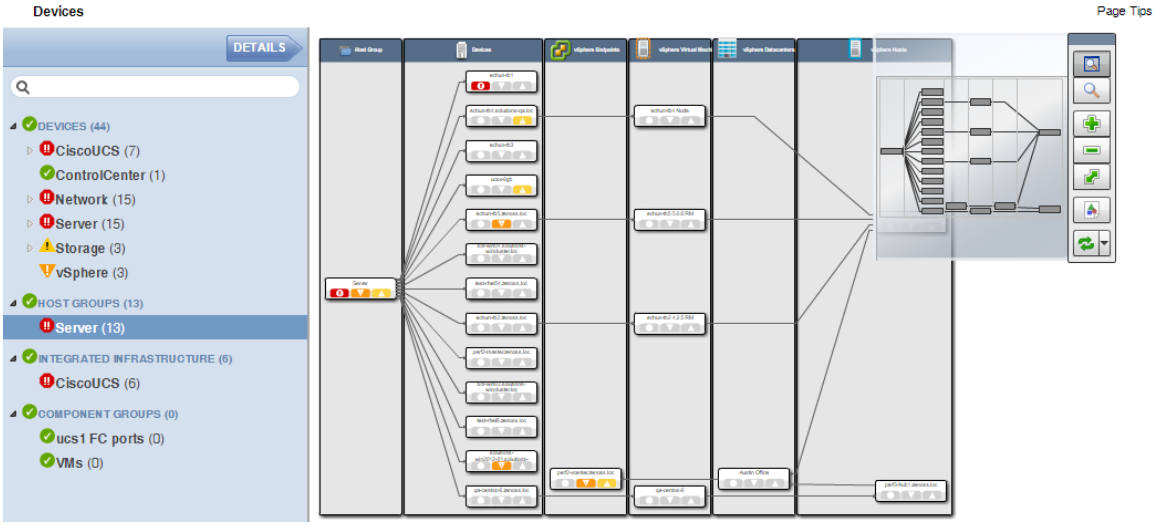
Note Be sure to click anywhere on the row that is not a hyperlink to select it. If you click a hyperlink, you will be taken to the specific details page.

7 Drag-and-drop the selected device(s) on the name of the host group and accept the move action.
8 At anytime, right-click on the name of the host group to refresh the tree or to display it in another window.

Viewing Host Group Dynamic View

The dynamic view of a host group shows all the integrated infrastructure components supporting the specific operating system servers in this application. To view a host group's dynamic view:

1 On the **Infrastructure** view, click the name of a host group.
2 Click the **Dynamic View** button in the lower-left corner of the window. The dynamic view for the host group appears.



Note Use the mouse wheel to zoom in or out of the dynamic view.

Working with Integrated Infrastructure

The integrated infrastructure view allows you to see compute, storage, network, and virtualization nodes together as an integrated infrastructure. Your UCS device is considered as a compute resource in an integrated infrastructure. Servers and VMs that run operating systems are not considered as a compute resource and as such cannot be added to an integrated infrastructure.

Creating an Integrated Infrastructure

To create an integrated infrastructure view using compute, storage, network, and virtualization components that are already being monitored:

1. Navigate to the **Infrastructure** page to view a list of the monitored devices.
2. Click **Integrated Infrastructure** in the left column.
3. Click the **Add** icon in the lower-left portion of the window.
4. Enter the name and a description of the integrated infrastructure. Click **Submit**. The new integrated infrastructure name appears in the left column.
5. Click **Devices** to display a list of monitored devices.
6. Select the various devices you want to add to the integrated infrastructure by control-clicking on each row.

   Note Be sure to click anywhere on the row that is not a hyperlink to select it. If you click a hyperlink, you will be taken to the specific details page.

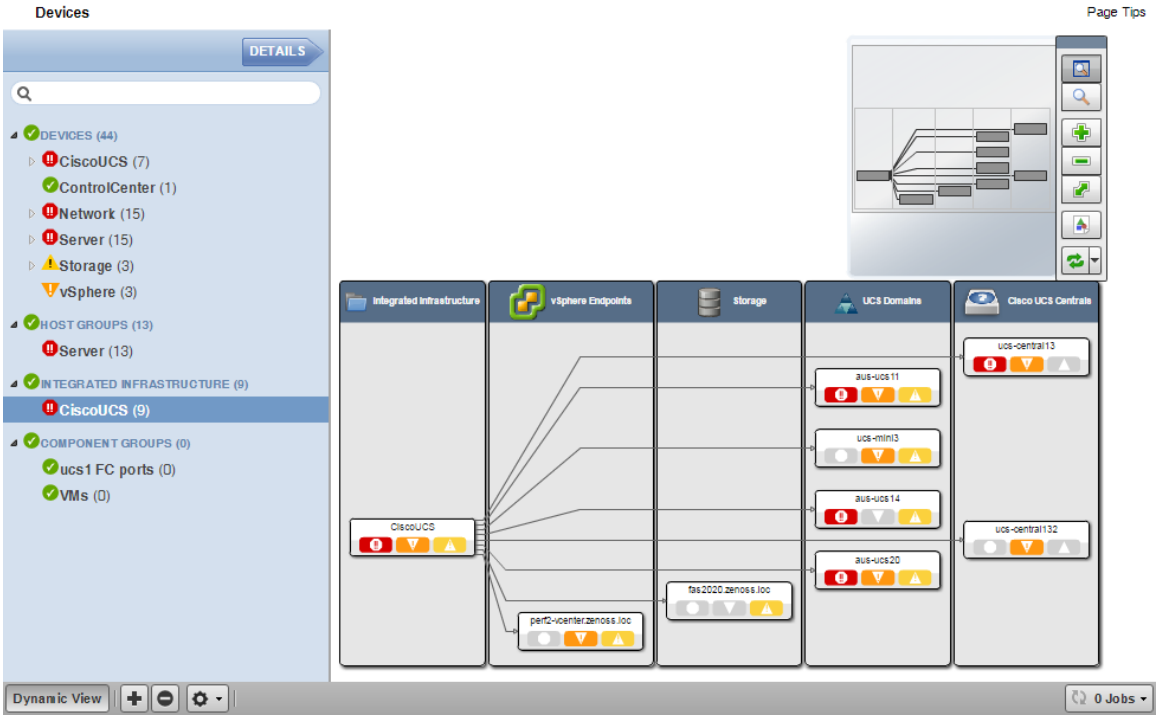
7. Drag-and-drop the devices on the name of the integrated infrastructure and accept the move action.
8. At anytime, right-click on the name of the integrated infrastructure to refresh the tree or to display it in another window.

Viewing Integrated Infrastructure Dynamic View

The dynamic view of an integrated infrastructure shows all the compute, storage, network, and virtualization nodes being monitored. To view an integrated infrastructure's dynamic view:

1. On the **Infrastructure** view, click the name of an integrated infrastructure.

2 Click the **Dynamic View** button in the lower-left corner of the window. The dynamic view for the integrated infrastructure appears.



Note Use the mouse wheel to zoom in or out of the dynamic view.

Working with Component Groups

Use Component Groups to view or manage component resources as a logical group. When you add components to a component group, you can view all of the events for the group in a single location, display component graphs with all of the components on the same graph, and use the Dynamic and Dependencies views to see the group's dependents and dependencies. You can also monitor or lock individual components in the group or the entire group itself.

Creating and Viewing Component Group Information

To create and view information about component groups:

1 Navigate to **Infrastructure > Devices**.
2 Select **Component Groups**, then click the **Add** icon at the bottom of the page.
The **Add Component Group** dialog is displayed.
3 Enter a suitable **Name**, and an optional **Description**, then click **Submit**.
The new component group appears under **Component Groups**.
4 Under **Component Groups** at the top of the page, click the **Add** icon to open the **Add to Component Group** dialog.
5 In the dialog's search field, enter a component type, such as Blade Servers for example.
A list of components is displayed in the **Search Results** table.
6 Select one or more components, then click **Add**.
7 Continue to search for and add components or click **Close**.
The components are added to the group. You can now work with the new component group. For example:

8 To view Component Graphs:

   a Highlight the new group and click **Details** at the top of the page.

   b Click **Component Graphs**, then check **All on Same Graph**.

Note When using the **All on Same Graph** functionality, ensure that no more than 10 items are being displayed on the same graph for best usability.

---

9 To view events for the component group, click **Events** .

10 To disable monitoring on one or more components, click **See All** at the top of the page.

   a Select the components you want to disable.

   b Click **Action > Monitoring**.

   c Click **Yes** to disable monitoring.

Event Management 4

Events, and the graphs generated from performance monitoring, are the primary operational tools for understanding the state of your environment.

Basic Event Fields

To enter the event management system, an event must contain values for the device, severity, and summary fields. If an event is missing any of these fields, then Cisco UCS Performance Manager rejects it.

Basic event fields are:

- device
- ipAddress
- eventState
- severity
- summary
- message
- evid

device and ipAddress Fields

The device field is a free-form text field that allows up to 255 characters. Cisco UCS Performance Manager accepts any value for this field. If the device field contains an IP address, then the system queries for devices with a matching address. If it finds a match, it changes the device field to the found device identifier.

The ipAddress field is a free-form text field. This field is not required. If the system cannot successfully locate a device based on the event's device field content, it attempts to find the device based the event ipAddress field content, if present.

Cisco UCS Performance Manager automatically adds information to incoming events that match a device. Fields added are:

- **prodState**- Specifies the device's current production state.
- **DeviceClass**- Classifies the device.
- **ApplicationGroups**- Specifies the application groups (if any) to which the device is assigned.
- **IntegratedInfrastructure**- Integrated infrastructure (if any) to which the device is assigned.
- **DevicePriority**- Priority assigned to the device.

For more information about these fields, refer to the chapters titled "Production States and Maintenance Windows" and "Organizers and Path Navigation."

eventState Field

The eventState field defines the current state of an event. This field is often updated after an event has been created. Values for this numeric field are 0-6, defined as follows:

Number	Name	Description
0	New	
1	Acknowledged	
2	Suppressed	
3	Closed	State given to an event that was closed as the result of a user action.
4	Cleared	State given to an event that was cleared by a corresponding clear event.
5	Dropped	State given to an event that was dropped via an event transform. These events are never persisted by the system.
6	Aged	State given to an event that was automatically closed by the system according to the severity and last seen time of the event.

severity Field

The severity field defines the severity of the event. Values for this numeric field are 0-5, defined as follows:

Number	Name	Color
0	Clear	Green
1	Debug	Grey
2	Info	Blue
3	Warning	Yellow
4	Error	Orange
5	Critical	Red

summary and message Fields

The summary and message fields are free-form text fields. The summary field allows up to 255 characters. The message field allows up to 4096 characters. These fields usually contain similar data.

The system handles these fields differently, depending on whether one or both are present on an incoming event:

- If only summary is present, then the system copies its contents into message and truncates summary contents to 128 characters.
- If only message is present, then the system copies its contents into summary and truncates summary contents to 128 characters.
- If summary and message are both present, then the system truncates summary contents to 128 characters.

As a result, data loss is possible only if the message or summary content exceeds 65535 characters, or if both fields are present and the summary content exceeds 128 characters.

To ensure that enough detail can be contained within the 128-character summary field limit, avoid reproducing information in the summary that exists on other fields (such as device, component, or severity).

Other Fields

Events include numerous other standard fields. Some control how an event is mapped and correlated; others provide information about the event.

The following table lists additional event fields.

Field	Description
dedupid	Dynamically generated fingerprint that allows the system to perform de-duplication on repeating events that share similar characteristics.
component	Free-form text field (maximum 255 characters) that allows additional context to be given to events (for example, the interface name for an interface threshold event).
eventClass	Name of the event class into which this event has been created or mapped.
eventKey	Free-form text field (maximum 128 characters) that allows another specificity key to be used to drive the de-duplication and auto-clearing correlation process.
eventClassKey	Free-form text field (maximum 128 characters) that is used as the first step in mapping an unknown event into an event class.
eventGroup	Free-form text field (maximum 64 characters) that can be used to group similar types of events. This is primarily an extension point for customization. Currently not used in a standard system.
stateChange	Last time that any information about the event changed.
firstTime	First time that the event occurred.
lastTime	Most recent time that the event occurred.
count	Number of occurrences of the event between the firstTime and lastTime.
prodState	Production state of the device, updated when an event occurs. This value is not changed when a device's production state is changed; it always reflects the state when the event was received by the system.
agent	Typically the name of the daemon that generated the event. For example, an SNMP threshold event will have zenperfsnmp as its agent.
DeviceClass	Device class of the device that the event is related to.
IntegratedInfrastructure	Pipe-delimited list of integrated infrastructures that the device is contained within.
ApplicationGroup	Pipe-delimited list of application groups that the device is contained within.
facility	Only present on events coming from syslog. The syslog facility.
priority	Only present on events coming from syslog. The syslog priority.
ntevid	Only present on events coming from Windows event log. The NT Event ID.
ownerid	Name of the user who acknowledged this event.

Field	Description
clearid	Only present on events in the archive that were auto-cleared. The evid of the event that cleared this one.
DevicePriority	Priority of the device that the event is related to.
eventClassMapping	If this event was matched by one of the configured event class mappings, contains the name of that mapping rule.
monitor	In a distributed setup, contains the name of the collector from which the event originated.

Details

In addition to the standard fields, the system also allows events to add an arbitrary number of additional name/value pairs to events to give them more context.

De-Duplication

Cisco UCS Performance Manager uses an event "de-duplication" feature, based on the concept of an event's fingerprint. Within the system, this fingerprint is the "dedupid." All of the standard events that the system creates as a result of its polling activities are de-duplicated, with no setup required. However, you can apply de-duplicating to events that arrive from other sources, such as syslog, SNMP traps, or a Windows event log.

The most important de-duplication concept is the *fingerprint*. An event's fingerprint (or dedupid) is composed of a pipe-delimited string that contains these event fields:

- device
- component (can be blank)
- eventClass
- eventKey (can be blank)
- severity
- summary (omitted from the dedupid if eventKey is non-blank)

When the component and eventKey fields are blank, a dedupid appears similar to:

www.example.com||/Status/Web||4|WebTx check failed

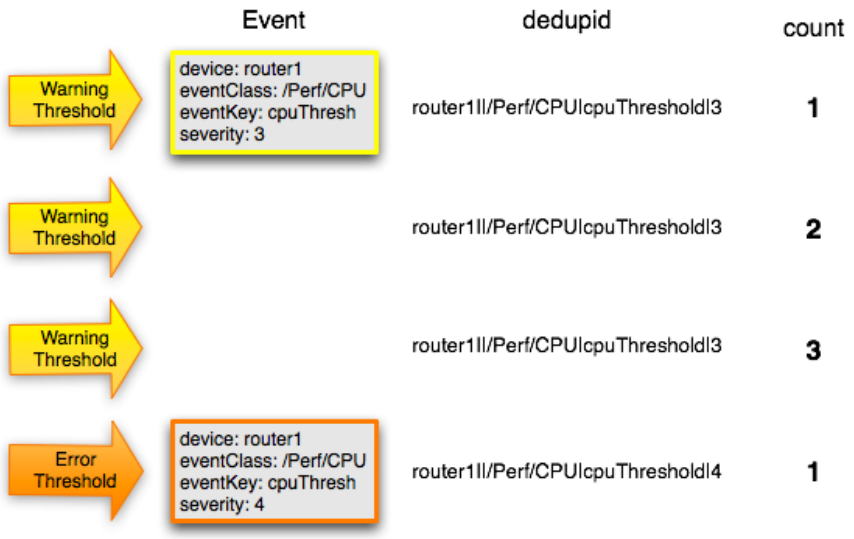
When the component and eventKey fields are present, a dedupid appears similar to:

router1.example.com|FastEthernet0/1|/Perf/Interface|threshName

When a new event is received by the system, the dedupid is constructed. If it matches the dedupid for any active event, the existing event is updated with properties of the new event occurrence and the event's count is incremented by one, and the lastTime field is updated to be the created time of the new event occurrence. If it does not match the dedupid of any active events, then it is inserted into the active event table with a count of 1, and the firstTime and lastTime fields are set to the created time of the new event.

The following illustration depicts a de-duplication scenario in which an identical event occurs three times, followed by one that is different in a single aspect of the dedupid fingerprint.

Figure 44: Event De-Duplication



If you want to change the way de-duplication behaves, you can use an event transform to alter one of the fields used to build the dedupid. You also can use a transform to directly modify the dedupid field, for more powerful cross-device event de-duplication.

Auto-Clear Correlation

The auto-clearing feature is similar to the de-duplication feature. It also is based on the event's fingerprint. The difference is which event fields make up the fingerprint, and what happens when a new event matches an existing event's fingerprint.

All of the standard events created as a result of polling activities do auto-clearing by themselves. As with de-duplication, you would invoke auto-clearing manually only to handle events that come from other sources, such as syslog, a Windows event log, or SNMP traps.

If a component has been identified for the event, then the auto-clear fingerprint consists of these fields:

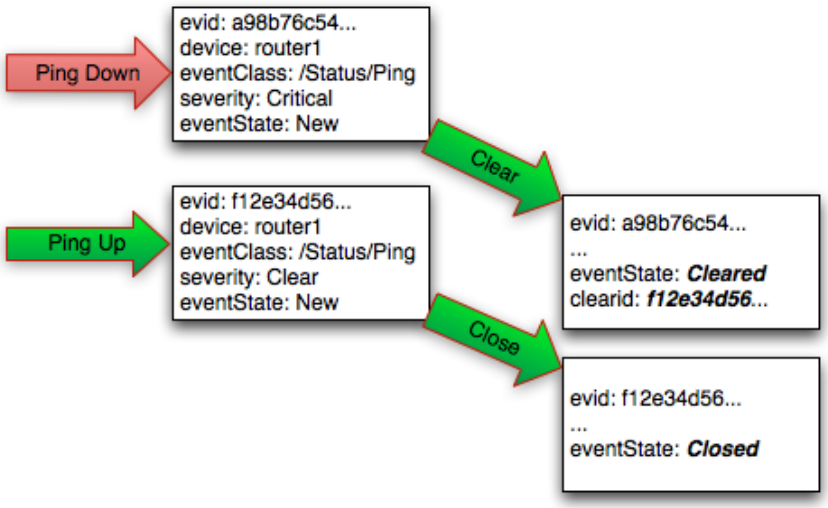
- If component UUID exists:
  - component UUID
  - eventClass
  - eventKey (can be blank)
- If component UUID does not exist:
  - device
  - component (can be blank)
  - eventKey (can be blank)
  - eventClass

When a new event comes into the system with a special 0 (Clear) severity, Cisco UCS Performance Manager checks all active events to see if they match the auto-clear fingerprint of the new event. All active events that match the auto-clear fingerprint are updated with a Cleared state, and the clearid field is set to the UUID of the clear event. After a configurable period of time, all events in a closed state (Closed, Cleared, and Aged) are moved from the active events table to the event archive.

If an event is cleared by the clear event, it is also inserted into the active events table with a status of Closed; otherwise, it is dropped. This is done to prevent extraneous clear messages from filling your events database.

The following illustration depicts a standard ping down event and its associated clear event.

Figure 45: Event Auto-Clear



If you need to manually invoke the auto-clearing correlation system, you can use an event transform to make sure that the clear event has the 0 (Clear) severity set. You also need to ensure that the device, component, and eventClass fields match the events you intend to clear.

Note Avoid making clear events too generic; otherwise, you may inadvertently clear a wider range of events than you intend.

Event Consoles

Cisco UCS Performance Manager features multiple event consoles that allow you to view and manage events. Each console shows different events subsets, depending on your current context.

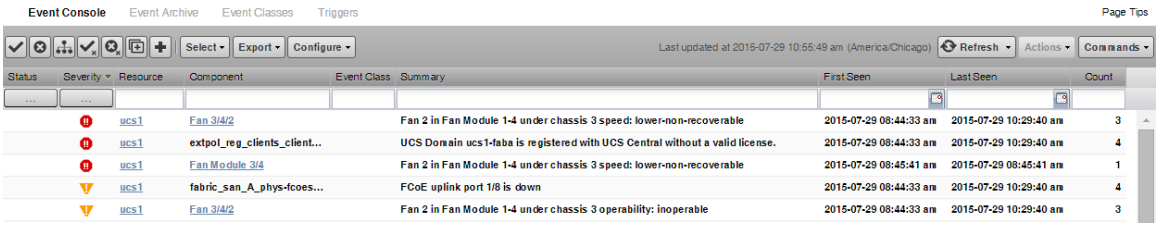
Event consoles are:

- **Master**- To access this console, click Events on the Navigation menu. You can view all events from this console.
- **Contextual**- Contextual event consoles are found throughout the system. Each time you see an Events selection for a device, device organizer, component, or event class, you can view event information that has been automatically filtered to show events specific to the current context.

Master Event Console

The master event console is the system's central nervous system, enabling you to view and manage events. It displays the repository of all events that have been collected by the system.

Figure 46: Event Console



Selecting Events

To select one or more events in the event console, you can:

- Click a row to select a single event
- Ctrl-Click rows to select multiple events, or Shift-Click to select a range of events

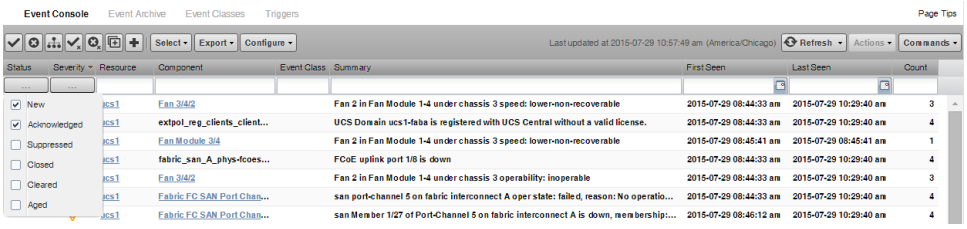
Sorting and Filtering Events

You can sort and filter events that appear in the event console to customize your view.

You can sort events by any column that appears in the event console. To sort events, click a column header. Clicking the header toggles between ascending and descending sort order.

Filter options appear below each column header. A match value can be any full string or a subset of a string, optionally with the wildcard (*) contained in the values in that column. You can also use "`||`" (OR), or "`!!`" (NOT) expressions to further target your filters. For example, typing `!!status` in the Event Class filter will return all the non-status class events.

Figure 47: Event Console Filter Options



You can filter the events that appear in the list in several ways, depending on the field type:

- **Resource** - Enter a match value to limit the list.
- **Component** - Enter a match value to limit the list.
- **Event Class** - Enter a match value to limit the list.
- **Summary** - Enter a match value to limit the list.
- **First Seen** - Enter a value or use a date selection tool to limit the list.
- **Last Seen** - Enter a value or use a date selection tool to limit the list.
- **Count** - Enter a value to filter the list, as follows:
  - *N* - Displays events with a count equal to *N*.
  - *:N* - Displays events with a count less than or equal to *N*.
  - *M:N* - Displays events with a count between *M* and *N* (inclusive).
  - *M:* - Displays events with a count greater than or equal to *M*.

To clear filters, select **Configure > Clear filters**.

You also can re-arrange the display order of columns in the event console. Click-and-drag column headers to change their display.

Working with Live Search

By default, the system uses a "live search" feature to help you locate information. From the event console, you can search for information by:

- **Device** (name) - Device name searches:
  - Are case-insensitive.
  - Are tokenized on whitespace (meaning that any searches that span whitespace and do not start with a complete token will return no results).
  - If quoted, return only exact matches.
- **Component**- Component searches:
  - Are case-insensitive.
  - Are tokenized on whitespace (meaning that any searches that span whitespace and do not start with a complete token will return no results).
  - If quoted, return only exact matches.
- **Summary**- Summary searches:
  - Are case-insensitive.
  - Are tokenized on whitespace (meaning that any searches that span whitespace and do not start with a complete token will return no results).
- **Event class**- Event class searches:
  - Are case-insensitive.
  - Are tokenized on / (slash). If the search begins with a slash, and ends with a slash or asterisk, then event classes are searched by using a "starts with" approach. If a search starts with a slash and ends with any other character, then event classes are searched by using an exact match for the event class. If a search does not begin with a slash, then event classes are searched by using a sub-string match on each event class.
- **IP Address**- IP address searches (for IPv4 and IPv6 values):
  - Are tokenized by . (period) and : (colon). For example, the following searches would return a result of 129.168.1.100:
    - 168
    - 168.1
    - 129.16*
    - *29
- **First Seen**, **Last Seen**, **State Change**- This field is not tokenized; date searches are converted to numeric representations, and then ranges using these representations are created. Search values are inclusive. Searches on date fields will search from the value entered. Any results that match the value or any value in the future are returned.

  The following searches would return the First Seen time of 2014-05-04 15:52:52:

  - First Seen: 2014-05-01 00:00:00
  - First Seen: 2014-05-04 15:52:52

With live search enabled (the default behavior), the system filters available information immediately. It presents increasingly refined information with each character you type in the search window. When disabled, search responds only after you enter one or more characters and then press Enter.

Saving an Event Console View

You can save your event console view by bookmarking it for quick access later. To do this:

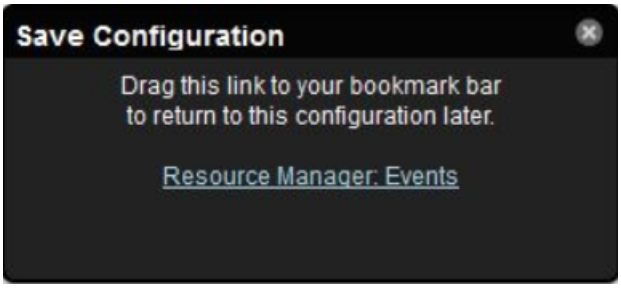
1 Select **Configure > Save this configuration**.

A dialog containing a link to the current view appears.

2 Click and drag the link to the bookmarks link on your browser's menu bar.

A link titled "Event Console" appears in your bookmarks list.

Figure 48: Saving a Custom View (Bookmark)



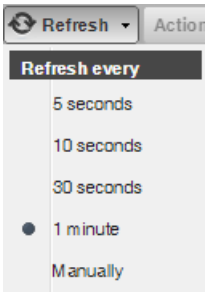
Note You may want to re-title the bookmark, particularly if you choose to save more than one event console view.

Refreshing the View

You can refresh the list of events manually or specify that they refresh automatically. To manually refresh the view, click **Refresh**. You can manually refresh at any time, even if you have an automatic refresh interval specified.

To set up automatic refresh, select one of the time increments from the Refresh list.

Figure 49: Automatic Refresh Selections



Viewing Event Details

You can view details for any event in the system. To view details, double-click an event row.

The Event Details area appears.

Figure 50: Event Details

To see more information about the event, click the Event Management, Device State, Event Data, or Event Details link. To display the event information in a new window, click the icon located at the top right.

You can use the Log area to add specific information about the event. Enter details, and then click **Add**.

Acknowledging Events

You may want to mark an event as "acknowledged" to indicate, for example, that you have taken action to remedy a problem. To mark events as acknowledged:

1 Select one or more events in the event console view.
2 Click the **Acknowledge Events** icon.

A check mark appears for each acknowledged event.

Returning Events to New Status

You may want to return a previously acknowledged event to "new" status (revoke its "acknowledged" status). To do this:

1 Select one or more events in the event console view.
2 Click the **Unacknowledge Events** icon.

A check mark no longer appears in the event row, and the event is returned to "new" status.

Classifying Events

Classifying events lets you associate events shown as **/Unknown** with a specific event class. To classify an unknown event, an event class key must be specified for the event.

To classify events:

1 Select one or more **/Unknown** events in the event console view.
2 Click the **Reclassify an Event** icon.

The Classify Events dialog appears.

3 Select an event class from the list of options, and then click **Submit**.

Note You can also classify events from the event archive.

Closing Events

When you no longer want to actively monitor an event (after you acknowledge it, for example), you can specify to close the event and move it to the event archive according to a configured event archive interval. To do this:

1 Select one or more events in the event console view.
2 Click the **Close Events** icon.

The selected events are closed and moved to the archive at the specified interval.

To view events in the event archive, select **Events > Event Archive**.

Note Users with no assigned role can view all events in the archive.

Reopening Events

You can reopen events in the active event console that are in the Closed, Cleared, or Aged state.

To reopen events:

1 Select one or more Closed, Cleared, or Aged events.
2 Click the **Reopen Events** icon.

The selected events are returned to active status.

Note You cannot re-open a closed event if another active event with the same fingerprint exists. Before you can re-open the closed event, you must close the new event.

Exporting Event Data

You can export data from the event console to a comma-separated value (`.csv`) or XML file. You can select individual events (to export only those events), or make no selections (to export all events that match the current filter criteria).

To export events:

1 Optionally select one or more events.
2 Select **Export > CSV** or **Export > XML**. By default, the exported file is named `events.` *Extension*.

Creating Events

To create events from the event console, click the **Add an Event** icon.

For more information about manual event creation, see the section titled "Creating Events Manually."

Creating Events Manually

You can manually create events. While this is not something you would do as part of normal system operation, it can be helpful when you are attempting to test mappings and transforms you have created.

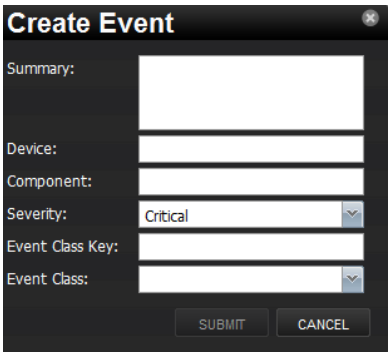
Creating Events through the User Interface

To create events manually through the user interface:

1 Navigate to Events, then click the **Add an Event** icon.

The Create Event dialog appears.

Figure 51: Create Event Dialog



2 Complete the basic event fields. Event class mappings are applied only for events that do not already have an event class.

Event Classes

Event classes are a simple organizational structure for the different types of events that the system generates and receives. This organization is useful for driving alerting and reporting. You can, for example, create an alerting rule that sends you an email or pages you when the availability of a Web site or page is affected by filtering on the `/Status/Web` event class.

Following is a subset of the default event classes. You can create additional event classes as needed.

- /Status - Used for events affecting availability.
  - /Status/Ping - Ping up/down events
  - /Status/Snmp - SNMP up/down events
  - /Status/Web - Web site or page up/down events
- /Perf - Used for performance threshold events.
  - /Perf/CPU - CPU utilization events
  - /Perf/Memory - Memory utilization or paging events
  - /Perf/Interface - Network interface utilization events
- /App - Application-related events.
- /Change - Events created when the system finds changes in your environment.

Mapping and Transformation

The event mapping and transformation system allows you to perform a wide range of operations, from altering the severity of certain events to altering nearly every field on an event, based on complex rules.

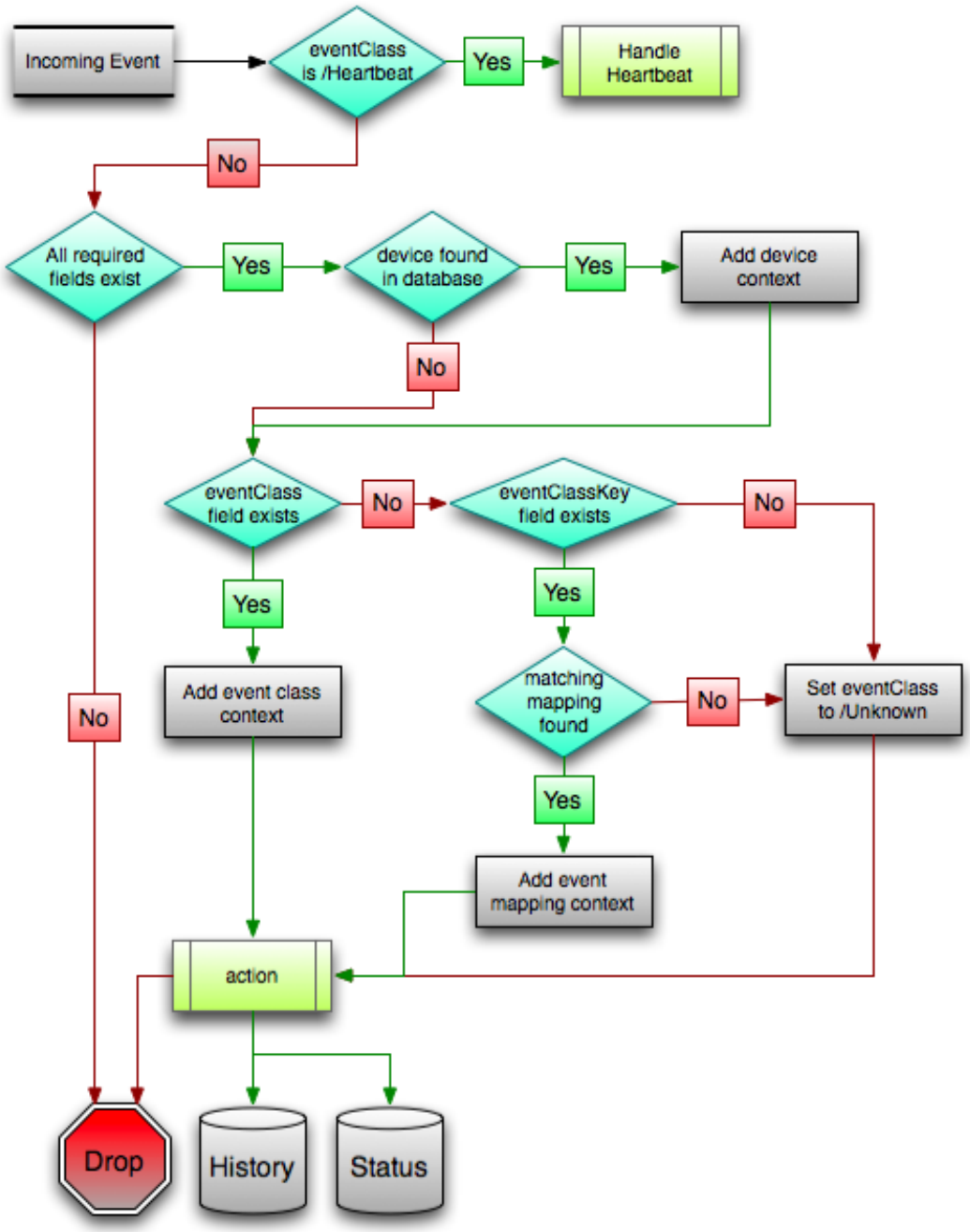
You cannot alter the following fields through event transformation. (This is because they are set after transformation has been performed.)

- evid

- firstTime
- lastTime
- count

The following illustration shows the path followed by an incoming event in the event mapping system.

Figure 52: Event Processing



The mapping and transformation process begins with the "eventClass field exists" decision. This also is one of the more important differentiators in how you must handle a particular type of event.

Event Class Mappings

To view event class mappings, select **Events > Event Classes**, and then select **Mapping Instances** in the drop-down list. This allows you to see all event class mappings in a single location. The ID column shows the mapping's event class.

You can create event class mappings directly from the event classes, but this requires that you know the event class key. A simpler way to create event class mappings is through the event console:

1. Select an event that you want to match in the event console.
2. Click the **Reclassify an Event** icon.

   The Classify Events dialog appears.
3. Select the event class to which you want to map the event, and then click **Submit**.

   This creates the event class mapping with the correct event class key, and example text against which you can develop your regular expression.

When editing an event class mapping, you can control which events it will match, as well as other properties:

- **Matching tab**
  - **Event Class Key**- Must match the incoming event's Event Class Key field for this mapping to be considered as a match for events.
  - **Rule**- Provides a programmatic secondary match requirement. It takes a Python expression. If the expression evaluates to True for an event, this mapping is applied.
  - **Regex**- The regular expression match is used only in cases where the rule property is blank. It takes a Perl Compatible Regular Expression (PCRE). If the regex matches an event's message field, then this mapping is applied.
  - **Explanation**- Free-form text field that can be used to add an explanation field to any event that matches this mapping.
  - **Resolution**- Free-form text field that can be used to add a resolution field to any event that matches this mapping.
- **Transforms tab**- Takes Python code that will be executed on the event only if it matches this mapping. For more details on transforms, see the section titled "Event Class Transform."
- **Configuration Properties tab**- Listing of Configuration Properties defined for this event class.
- **Sequence tab**- Sequence number of this mapping. This number determines the order in which mappings with the same event class key are evaluated.

When a captured event occurs, it will not have a pre-defined event class. For this type of event, you must create an event class mapping if you want to affect the event. If a captured event occurs and none of the event class mappings in the system match it, its event class will be set to /Unknown, and it will retain all of the default properties with which it began.

The next step of evaluation for events without an event class is to check the Event Class Key field. This controls which event class mapping the event will match. If the event has a blank event class key, or its event class key does not match any event class mappings in the system, the special “defaultmapping” event class key is searched for instead. This provides for a way to map events even if they have a blank or unpredictable event class key.

Event Class Mapping Sequence

The sequence area of an event class mapping (select Sequence in the left panel) allows you to provide more than one mapping for the same event class key. In this case, the sequence is evaluated in ascending order until a full (rule or regex) match is found.

For example, suppose a router is sending in unclassified events that need to be mapped to two event classes:

- /Events/Router/fanDown
- /Events/Router/fanUnknown

The event class key for both has been sent to "router", but one has a message of "Fan Down" and the other has no message at all. The mapping on /Events/Router/fanDown has an event class key of "router" and a regex of "Fan Down." The mapping on /Events/Router/fanUnknown has only an event class key of "router" and (in this example) no regex. Because the fanUnknown mapping matches the fanDown events, the evaluation of fanDown needs to occur first.

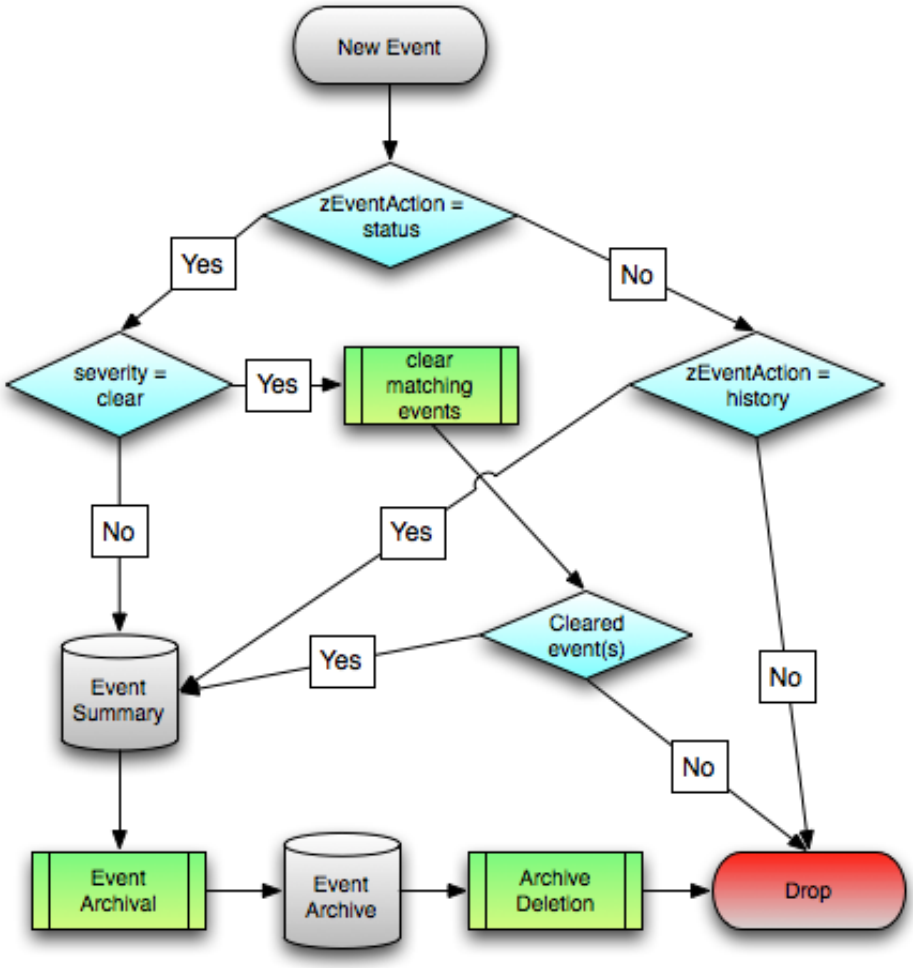
You can modify the evaluation of mappings with the same event class key in the Sequence area of any of those event class mappings. In the previous example, you could go to either mapping, select Sequence, and both mappings would be displayed. You can set one to 0, and the other to 1. (You can enter other values, but they will be changed to the shortest list of integers, starting with 0.) Setting fanDown to 0 and fanUnknown to 1 will ensure that the events will be mapped properly.

Event Life Cycle

In addition to manual methods for getting events into the status table or event archive, there are automated processes that move events from status into the archive. The *event life cycle* is defined as all of the ways that events can be added to, moved in, and deleted from the database.

The following illustration depicts the event life cycle.

Figure 53: Event Life Cycle



Automatic Event Aging

From the Event Configuration page (**Advanced > Settings > Events**), you can set up automatic aging of events. Aging of events will automatically update active events that match the severity and aging threshold to a status of Aged. After the configured event archive interval, all Closed, Aged, and Cleared events are moved to the event archive.

Properties that control this behavior are:

- **Don't Age This Severity and Above** - Options are Age All Events, Critical, Error, Warning, Info, Debug, and Clear. By default, this value is set to Error, meaning that all events with a status of Error or Critical are not aged.
- **Event Aging Threshold (minutes)** - Set the time value, in minutes, that an event must reach before it is aged. By default, this is 240 minutes.
- **Event Aging Interval (milliseconds)** - The interval when events are scanned to perform autoaging. By default, this is 60000 milliseconds (60 sec).
- **Event Aging Limit** - The maximum number of events to age in each interval. The limit should be kept relatively low to prevent large database transactions. By default, this is 1000 events.
- **Event Archive Threshold (minutes)** - Specify the number of minutes since a closed event was last seen before it is moved to the event archive. The minimum value is 1; the maximum value is 43200.
- **Event Archive Interval (milliseconds)** - The interval when events are scanned for moving to the archive. By default, this is 60000 milliseconds (60 sec).
- **Event Archive Limit** - The maximum number of events to archive in each interval. The limit should be kept relatively low to prevent large database transactions. By default, this is 1000 events.
- **Delete Archived Events Older Than (days)** - The number of days that events in the event archive are saved. By default, they are kept in the archive for 90 days. The minimum value is 1 and the maximum value is determined by the range of event archive partitions. With the default configuration, the maximum value is 1000 days.
- **Default Syslog Priority** - Specify the default severity level assigned to an event coming from zensyslog if no priority can be determined from the event.
- **Default Availability Report (days)** - Enter the number of days to include in the automatically generated Availability Report. This report shows a graphical summary of availability and status.
- **Max Event Size in Bytes** - The maximum size of an event that will be processed in bytes. Events that are too large will be logged and dropped. Events that will become too big will have their details overwritten with new details. By default, this is 32768 bytes.
- **Summary Index Interval (milliseconds)** - The default indexing interval of the event summary in milliseconds. By default, this is 1000 milliseconds (1 sec).
- **Archive Index Interval (milliseconds)** - The default indexing interval of the event archive in milliseconds. By default, this is 30000 milliseconds (30 sec).
- **Index Limit** - The number of events to index in each index interval. By default, this is 1000 events.
- **Event Time Purge Interval (days)** - The number of days that event occurrence time are kept. By default, they are kept for 7 days. The minimum value is 1 and the maximum value is determined by the range of event time partitions. With the default configuration, the maximum value is 7 days.
- **Enable Event Flapping Detection** - Select this check box if you wish to enable event flapping detection. If an event is created and then cleared *flapping_threshold* times in *event_flapping_interval* time then an event of event flapping event class is created.
- **Event Flapping Event Class** - The event class under which generated flapping events belong.
- **Clear Event Heartbeats** - Click **Clear** to clear the event heartbeats.

Automatic Archived Event Cleanup

You can set up automatic purging of events from the event archive from the Event Configuration page (**Advanced > Settings > Events**). When events are purged, they can be recovered only from backups.

The property that controls this behavior is Delete Archived Events Older Than (days). Acceptable values are between 1 and 1000 (days).

Production States and Maintenance Windows

5

Production state determines the level of monitoring and alerting applied to an individual device. Typically, alerting rules specify that the system will monitor and create events for devices that are in the "Production" production state. *Maintenance windows* are planned time periods used to temporarily modify alerting rules so that event-generated alerts are temporarily halted during the window.

Production States

Production state determines whether a device is monitored, and can be used to control several elements of the event system, such as whether an event will produce a remote alert (email or page).

Choose a production state for a device based on whether you want:

- The device to be monitored
- The device to appear on the dashboard
- Alerting to occur

The following table lists production states and their characteristics.

Production State	Devices Monitored?	Appear on Dashboard?
Production	yes	yes
Pre-Production	yes	no
Test	yes	no
Maintenance	yes	may appear
Decommissioned	no	no

When you add a device to the system, its default state is Production. You may want to add triggers and notifications to alert you to various conditions that occur in the system, such as production state changes or a severity level being reached. For example, you can set up a trigger when a device is in either a production or a maintenance state and has a severity of Error or higher. You can then notify users when this trigger condition is met. For more information, see *Working with Triggers and Notifications* on page 18.

Setting the Production State for Devices

To set the production state for a device:

1 Click a device name in the list of devices. The Device Overview page appears.

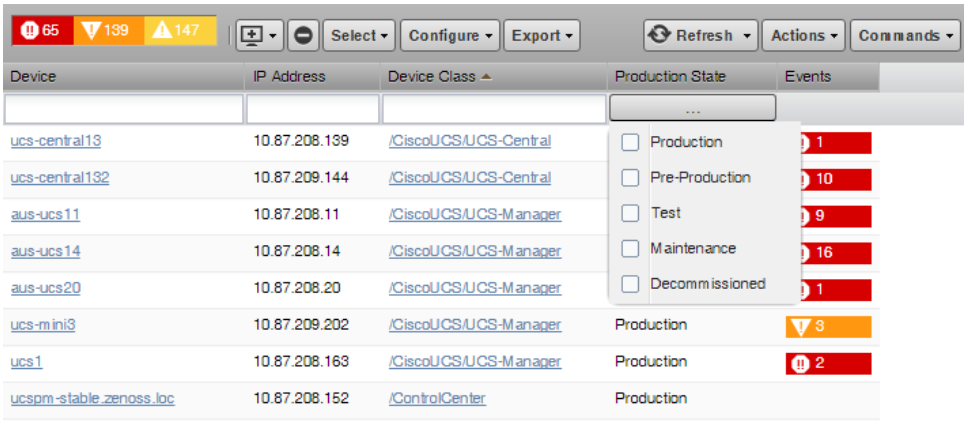
2 Select a production state from the list of options, and then click **Save**.

To set the production state for a group of devices:

1 Select a category of devices (by class or group) from the hierarchy.
2 From the list of options in the Production State column, select a production state.

The newly selected state is applied to all devices that appear in the list.

Figure 54: Select Production State (Multiple Devices)



Maintenance Windows

Maintenance windows allow scheduled production state changes of a device or all devices in an application group. You might want to set up a maintenance window, for example, to prevent alerts and warnings while you perform configuration changes or reboot a device.

Note In lieu of setting up a maintenance window, you can change the production state for a device manually at the time you want to make changes.

When the maintenance window starts, the production state of the device is set to the value of Start Production State (Maintenance). When the maintenance window closes, the production state of the device reverts to the value of Stop Production State (the state the device was in prior to maintenance).

Maintenance Window Events

When a maintenance window starts, an event is created with the following information:

- depuid - zenactions | *Monitor* | *MaintenanceWindowName* | *TargetOrganizerOrDevice*
- prodState - *StartProductionState*
- severity - Info
- summary/message - Maintenance window starting *MaintenanceWindow* for *Target*
- eventClass - /Status/Update
- eventClassKey - mw_change
- maintenance_devices - *Target*
- maintenance_window - *MaintenanceWindow*

When a maintenance window stops, an event is created with the following information:

- severity - Clear

- summary/message - Maintenance window stopping *MaintenanceWindow* for *Target*
- prodState - -99 (meaning "unknown.")

Maintenance window events auto-clear, meaning that stop events clear start events.

Creating and Using Maintenance Windows

You can create a maintenance window for an individual device or group of devices in the devices hierarchy.

Create a Maintenance Window for a Single Device

To create a maintenance window for a device:

1. Click a device name in the devices list.

   The device Overview page appears.
2. In the left panel, select **Administration**.
3. In the Maintenance Windows area, select Add Maint Window from the Action menu.

   The Add Maintenance Window dialog appears.
4. Enter a name for the maintenance window, and then click **OK**.

   The newly defined maintenance window appears in the list.
5. Click the name in the list to show the maintenance window status page.
6. Define the attributes for the maintenance window:

   - **Name** - Name of the maintenance window.
   - **Enabled** - Select True to make the maintenance window active, or False to de-activate it.
   - **Start** - Specify a date and time for the window to become active. The time should be specified in 24-hour format and in UTC (Universal Coordinated Time), not local time.
   - **Duration** - Specify the length of time for the window to be in effect.
   - **Repeat** - Specify how often to repeat the maintenance window. Default value is Never.
   - **Start Production State** - Define the production state for the window when the maintenance period begins. Default value is Maintenance.
   - **Stop Production State** - Shows the production state that will be in effect when the maintenance period ends.
7. Click **Save**.

Create a Maintenance Window for a Group of Devices

To create a maintenance window for a group of devices:

1. Select a group of devices from the devices hierarchy or devices list and click **Details** in the left column.
2. In the left panel, select **Administration**.
3. In the Maintenance Windows area, select Add Maint Window from the Action menu.

   The Add Maintenance Window dialog appears.
4. Enter a name for the maintenance window, and then click **OK**.

   The newly defined maintenance window appears in the list.
5. Click the name in the list to show the maintenance window status page.
6. Define the attributes for the maintenance window:

   - **Name** - Name of the maintenance window.
   - **Enabled** - Select True to make the maintenance window active, or False to de-activate it.

- **Start** - Specify a date and time for the window to become active. The time should be specified in 24-hour format and in UTC (Universal Coordinated Time), not local time.
- **Duration** - Specify the length of time for the window to be in effect.
- **Repeat** - Specify how often to repeat the maintenance window. Default value is Never.
- **Start Production State** - Define the production state for the window when the maintenance period begins. Default value is Maintenance.
- **Stop Production State** - Shows the production state that will be in effect when the maintenance period ends.

7 Click **Save**.

Organizers and Path Navigation 6

You can group system objects, including devices and sub-systems. A device, for example, can belong to multiple classifications, including a device class and an application group.

Classes

The most important organizers are *classes*, which comprise:

- Device classes
- Event classes
- Service classes
- Product classes

The class hierarchy includes all defined and standard classes and sub-classes.

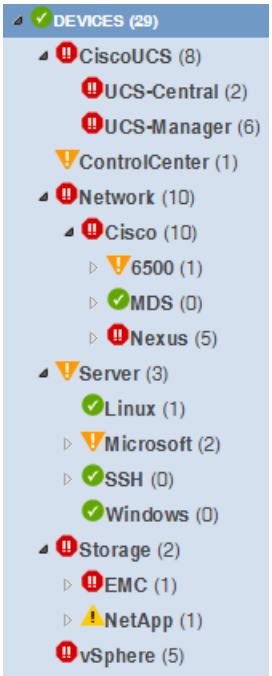
The following procedures are illustrated using device classes and sub-classes, but the same concepts apply to event classes, service classes, and product classes. When you add a device to the system, you should (after providing the network name or IP address) specify its device class. Templates can be set at any level in the device class hierarchy.

Viewing Device Classes

To view device classes and the devices they contain, select Infrastructure from the Navigation menu.

The device list appears. The top of the devices hierarchy lists device classes. Click a class name to view devices in that class, or expand it to show sub-classes.

Figure 55: Devices Hierarchy



An indicator appears next to each listed class to show whether there are events associated with any devices in that class.

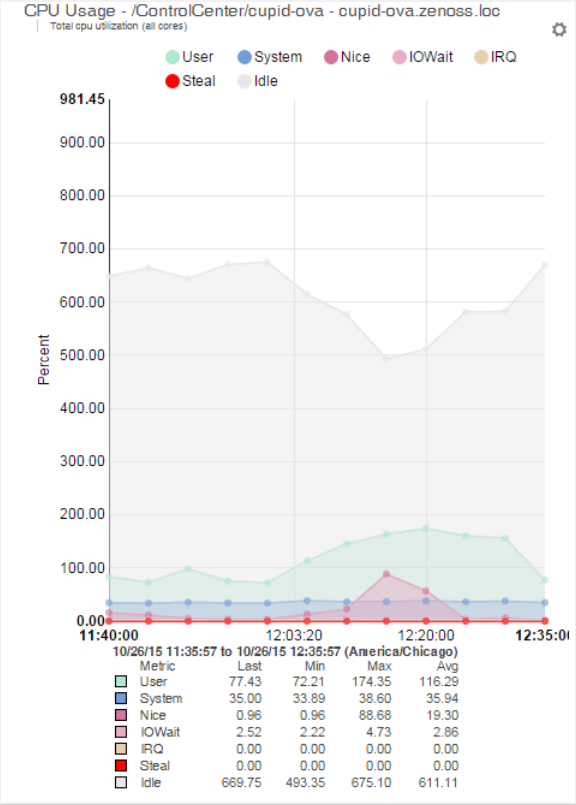
Self Monitoring

7

Cisco UCS Performance Manager provides self-monitoring of the application itself as well as its internal functions. It uses Control Center as its application management and orchestration system. The Control Center is automatically added as a managed resource within Cisco UCS Performance Manager so that you can see the internal components and their performance data. There are additional views available of the Control Center and all the internal services associated with it as well as the hubs and collectors that are defined within the system.

Note Since the Control Center host has multiple cores, any graph that displays information about total utilization will add the values for all cores. For example, if your host has 8 cores, you will see the sum of all utilization displayed as 800 percent. As such, you may see values for Idle CPU usage in the 400-700 percent range.

Figure 56: Total CPU Usage



About Collectors

A *collector* is a set of collection daemons, on the Cisco UCS Performance Manager host or another host, that shares a common configuration. That configuration contains values, such as:

- Number of seconds between SNMP collections cycles
- Default discovery networks
- Maximum number of `zenprocess` parallel jobs

Each collector has its own copy of each of the Cisco UCS Performance Manager collection daemons. For example, Cisco UCS Performance Manager initially contains collection daemons with names like `zenperfsnmp`, `zenprocess`, and `zenping`.

About Hubs

Cisco UCS Performance Manager supports multiple hubs. A *hub* represents an instance of the `zenhub` daemon, through which all collector daemons communicate with the object and event databases. Hubs are now associated with a resource pool which helps with better collector distribution.

All collectors must belong to exactly one hub; however, a hub can have many collectors associated with it. All hubs (and indirectly all collectors) refer to the same object and event databases. Typically, only very large systems with more than five collectors (or more than 1,500 devices) benefit from multiple hubs.

The `ZooKeeper` service on the HBase cluster now maintains configuration data and provide distributed synchronization and group services.

Navigating Collectors and Hubs

To view and manage collectors and hubs:

1. Log in as the Cisco UCS Performance Manager user.
2. From the navigation menu, select **Advanced > Control Center**.

   The Control Center All Services page appears.

Figure 57: Control Center - All Services

Settings Move Devices **Control Center** Monitoring Templates Jobs

All Services

Start Stop Restart

Name	Type	Uptime	AutoStart	Restart	State	Host
CentralQuery	daemon	6 days, 9:06:34.813614	☑		Up	ucspm-stable.zenoss.loc
HMaster	daemon	6 days, 9:06:26.678772	☑		Up	ucspm-stable.zenoss.loc
Imp4MariaDB	daemon		☐		Down	
Imp4OpenTSDB	daemon		☐		Down	
localhost	hub				...	
localhost	collector				...	
collectorredis	daemon	6 days, 9:06:15.053303	☑		Up	ucspm-stable.zenoss.loc
MetricShipper	daemon	6 days, 9:06:33.888581	☑		Up	ucspm-stable.zenoss.loc
zencommand	daemon	6 days, 9:06:17.002472	☑		Up	ucspm-stable.zenoss.loc
zenmail	daemon		☐		Down	
zenmodeler	daemon	6 days, 9:06:15.942412	☑		Up	ucspm-stable.zenoss.loc
zenperfsnmp	daemon	6 days, 9:06:15.928226	☑		Up	ucspm-stable.zenoss.loc
zenping	daemon	6 days, 9:06:16.972205	☑		Up	ucspm-stable.zenoss.loc
zenpropertymon...	daemon	6 days, 9:06:17.017761	☑		Up	ucspm-stable.zenoss.loc
zenpython	daemon	6 days, 9:06:16.987216	☑		Up	ucspm-stable.zenoss.loc
zenucsevents	daemon	6 days, 9:06:16.956418	☑		Up	ucspm-stable.zenoss.loc
zenvsphere	daemon	5 days, 0:15:49.037176	☑		Up	ucspm-stable.zenoss.loc
zminion	daemon	6 days, 9:06:15.901294	☑		Up	ucspm-stable.zenoss.loc
zenhub	daemon	6 days, 9:06:15.875667	☑		Up	ucspm-stable.zenoss.loc
mariadb-events	daemon	6 days, 9:06:24.785442	☑		Up	ucspm-stable.zenoss.loc
mariadb-model	daemon	6 days, 9:06:24.798263	☑		Up	ucspm-stable.zenoss.loc

The page lists existing hubs and collectors in hierarchical form. Hubs are listed at the top level; collectors are nested below the hub to which they belong.

From this page, you can:

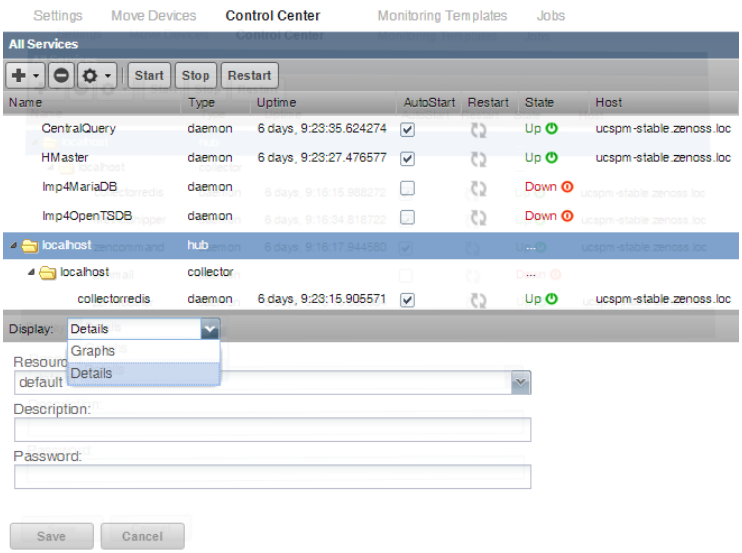
- Add a hub or a collector
- Delete a hub (which also deletes its associated collectors) or a collector

> **Note** You cannot delete the default hub and collector (localhost)

- View and edit hub settings
- Configure associated monitoring and performance templates

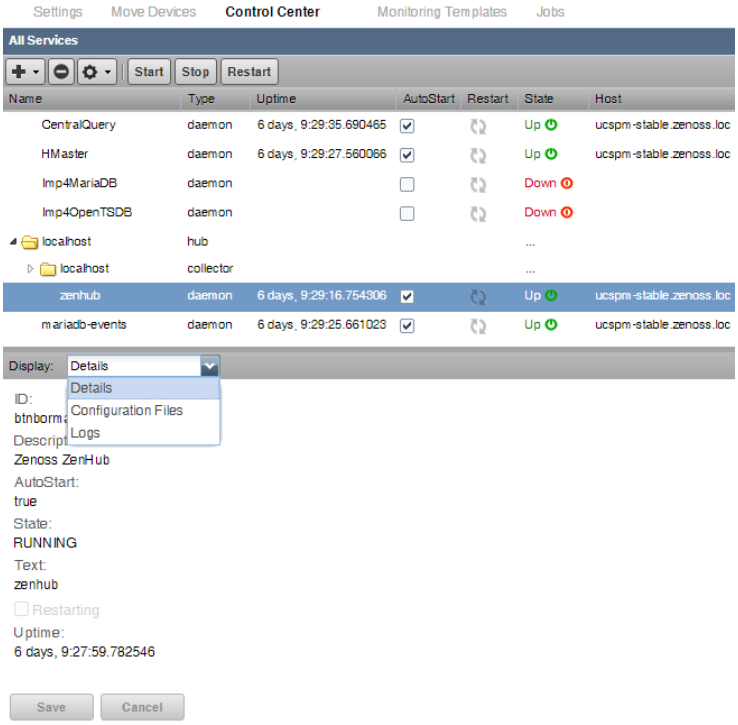
Select a hub to display details and graphs. The Resource Pool ID for the hub is displayed and can be changed if needed. You can add a description and password if needed.

Figure 58: Control Center - Hub Details



Select the `zenhub` daemon to view the details about the daemon, its logs, and to view and edit its configuration. Use the buttons on the top of the window to start, stop, or restart it.

Figure 59: Control Center - Daemon Details



Collector Data Storage

Cisco UCS Performance Manager no longer uses RRD files on the collectors for data storage. We have created a centralized storage framework for this data which uses a Redis key-value store on the collector and then ships that data to an OpenTSDB (time series database) instance that runs on Hadoop and HBase.

Deleting Collectors

When you delete a collector, its devices are left without an assigned collector. Cisco recommends that you reassign assigned devices prior to deleting a collector.

To delete a collector, click the name of the hub where the collector exists from the main collectors page. The Hub overview page appears. From the list of Collectors, select the collector you want to delete. From the Action menu, select Delete Collector.

When you delete collectors using this Cisco UCS Performance Manager instance, they are not removed or "uninstalled" in any way from the collector device. They continue to exist on the device until manually removed through the file system.

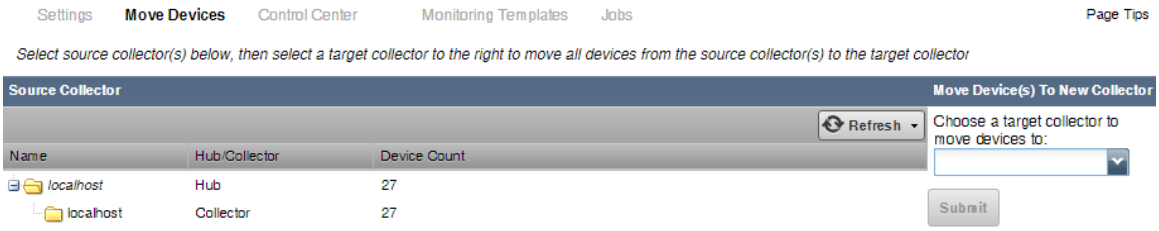
Moving Devices Between Collectors

To move devices from one collector to another.

1 From the Navigation menu, select **Advanced > Move Devices**.

The Move Devices screen appears.

Figure 60: Move Devices



2 Select the source collector(s) you want to move, then select a target collector to move the devices to from the drop-down list.

3 Click **Submit** to confirm. Cisco UCS Performance Manager moves the devices to the newly selected collector.

Managing Users 8

Cisco UCS Performance Manager has several default users that are initially created when you install the system:

- **ccuser** - This is the default account for gaining access to the Control Center browser interface. For more information on the `ccuser`, see the *Cisco UCS Performance Manager Installation Guide*.
- **root** - This is the account that by default has access to all commands and files on the system. It is also referred to as the root account or the superuser. For more information on the `root` account, see *Cisco UCS Performance Manager Installation Guide*.
- **admin** - This is the default administrator account for logging in to Cisco UCS Performance Manager. The `admin` account can make changes that will affect other users of the system.

Every user within Cisco UCS Performance Manager has a unique user ID, which allows an administrator to assign group permissions and alerting rules that are unique to each user. Unique IDs also help ensure secure access to the system.

To create and manage user accounts, you must be logged in to the system `admin` account, or as a user with extended privileges.

Creating User Accounts

To create a user account:

1. From the Navigation menu, select **Advanced**.

   The Settings page appears.
2. In the left panel, select **Users**.

   The users and groups administration page appears.
3. From the Action icon, select Add New User.

   The Add User dialog appears.
4. In the Username field, enter a unique name for the account.
5. In the Email field, enter the user account email address. Any alerts that you set up for this user will be send to this address.
6. Click **OK**.

   The user appears in the User List.

After creating the account, edit the account to provide a password and additional user details.

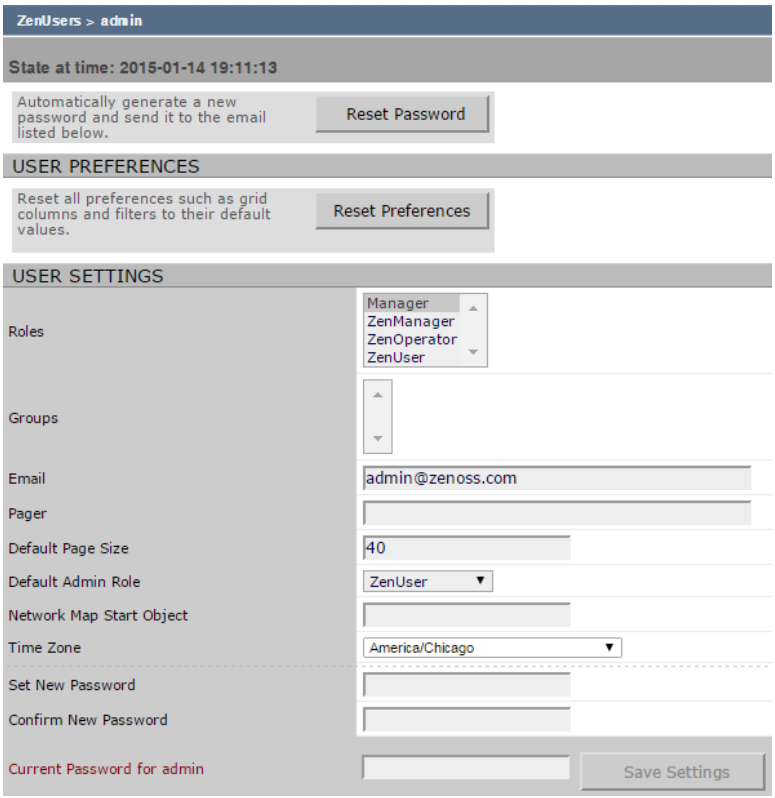
Editing User Accounts

To access and edit user account information:

1 In the Users list, click the name of the user you want to edit.

The edit user page appears. The following example shows the admin user.

Figure 61: Edit User



2 Make changes to one or more settings:

- **Reset Password** - Facilitates user self-service by allowing a user to reset his or her own password. Click to reset and email the new password to the email address associated with the user's account.
- **User Preferences** - Resets all preferences such as grid columns and filters to their default values.
- **Roles** - Assign one or more roles (user privileges) to the user. To edit or assign roles, you must be a system Admin or be assigned the Manager role.

  For more information about user roles, and for a list of available roles and the privileges they provide, see *Roles* on page 92.
- **Groups** - Specify one or more groups to which this user belongs.
- **Email** - Enter the user's email address. To verify that the address is valid, click the test link.
- **Pager** - Enter the user's pager number.
- **Default Page Size** - Controls how many entries (by default) appear in tables. Enter a value for the default page size. The default value is 40.
- **Default Admin Role** - Select the default role that this user will have for administered objects associated with him or her.
- **Network Map Start Object** - Specify the default view for this user in the network map.

- **Time Zone** - Specify the time zone to be displayed on all charts and graphs within the product. This only affects the user interface. To change the time zone of the virtual machine that is running Cisco UCS Performance Manager, see the instructions in the *Cisco UCS Performance Manager Installation Guide*.
- **Set New Password / Confirm New Password** - Enter a new password for the user and confirm the entry.

Enter your password, and then click **Save** to confirm and save the changes for the user.

Associating Objects with Specific Users

You can associate any object in the system with a particular user, for monitoring or reporting purposes. Once associated with a user, you can then assign the user a specific role that applies to his privileges with respect to that object.

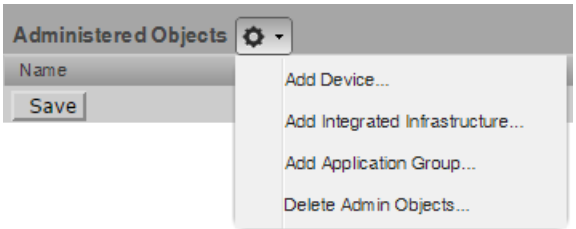
For more information about object-specific roles, see *Roles* on page 92.

To create an object association:

1 From **Advanced > Settings**, select **Users** in the left panel.
2 Select a user.
3 From the Edit page, select **Administered Objects** in the left panel.

The list of administered objects appears.

Figure 62: Administered Objects - Add Object



4 Select an object type from the Administered Objects Action menu. You can add:

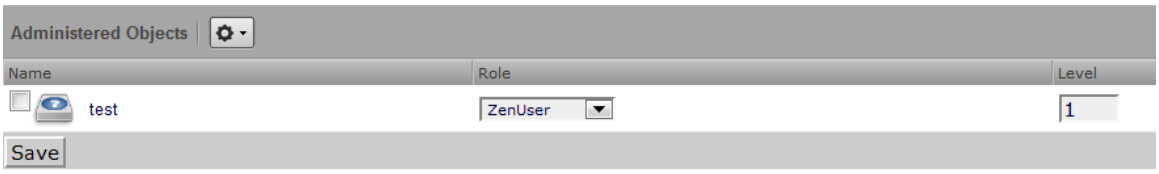
- Device
- Integrated Infrastructure
- Application Group

The Add Administered Device dialog appears.

5 Specify the component you want to add as an administered object, and then click **OK**.

The object appears in the Administered Devices list for the user.

Figure 63: Administered Objects - Objects Added



6 Optionally, change the role that is associated for this user on this object.

Note The default role assigned to the user for an administered object is specified by the Default Admin Role field on the Edit page.

7 Click **Save** to save changes.

User Groups

Cisco UCS Performance Manager allows you to create user groups. By grouping users, you can aggregate rules and apply them across multiple user accounts.

Viewing User Groups

To view user groups, select **Advanced > Settings**, and then select **Users** from the left panel.

The groups area shows each user group and the users assigned to that group.

Creating User Groups

You can create user groups to aggregate rules and apply them across multiple user accounts.

To create a user group:

1 Navigate to **Advanced > Settings**.
2 In the left panel, select **Users**.

   The Users page appears.
3 From the Groups area Action menu, select **Add New Group**.

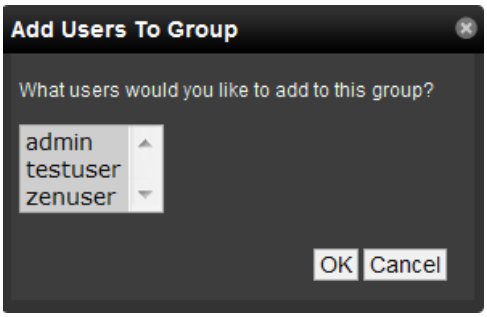
   The Add Group dialog appears.
4 In the Group field, enter a name for this user group, and then click **OK**.

   The group name appears in the Groups list.
5 Click the name of the group you created.

   The Users in Group page appears.
6 From the Action menu, select Add User.

   The Add User to Group dialog appears.

Figure 64: Add User to Group



7 From the User list of selections, select one or more users you want to add to the group, and then click **OK**.

   The user or users you select appear in the list of users for this group.

Roles

A role is a group of permissions that you can assign to users or groups.

The following table lists available roles.

Role	Permissions
ZenUser	Provides global read-only access to system objects.
ZenManager	Provides global read-write access to system objects.
Manager	Provides global read-write access to system objects. Additionally provides read-write access to the Zope object database.
ZenOperator	Provides event management. Combine the ZenOperator role with the ZenUser role to allow users read-only access to the system, but also allow them to acknowledge and close events, move events to history, and add log messages to events. You can associate the ZenOperator role with an individual device, a device class, or a group of devices.

Device Access Control Lists

About Device Access Control Lists (ACL)

Cisco UCS Performance Manager supports fine-grained security controls. For example, this control can be used to give limited access to certain departments within a large organization or limit a customer to see only his own data. A user with limited access to objects also has a more limited view of features within the system. As an example, most global views, such as the network map, event console, and all types of class management, are not available. The device list is available, as is the application group device organizer. A limited set of reports can also be accessed.

Key Elements

Following are key elements of device ACLs.

Permissions and Roles

Actions in the system are assigned permissions. For instance to access the device edit screen you must have the “Change Device” permission. Permissions are not assigned directly to a user; instead, permissions are granted to roles, which are then assigned to a user. A common example is the ZenUser role. Its primary permission is “View,” which grants read-only access to all objects. ZenManagers have additional permissions such as “Change Device,” which grants them access to the device edit screen. When you assign a role to a user using the Roles field (on the Edit page), it is global.

Administered Objects

Device ACLs provide limited control to various objects within the system. Administered objects are the same as the device organizers: Devices and Groups. If access is granted to any device organizer, it flows down to all devices within that organizer. To assign access to objects for a restricted user, you must have the Manager or ZenManager roles. The system grants access to objects is granted using the user's or user group's administered objects. To limit access, you must not assign a “global” role to the user or group.

Assigning Administered Object Access

For each user or group there is an Administered Objects selection, which lets you add items for each type of administered object. After adding an object you can assign it a role. Roles can be different for each object, so a user or group might have ZenUser on a particular device but ZenManager on an application group. If multiple roles are granted to a device though direct assignment and through the application group the resulting permissions will be

additive. In the example above, if the device was in the application group, the user would inherit the ZenManager role on the device.

Example: Restricted User with ZenUser Role

1. As admin or any user account with Manager or ZenManager role, create a user named acltest. Set a password for the user.
2. Make sure that no role is assigned to the user.
3. Edit the user's administered objects.
4. Add an existing device to the user.

   The device's role will default to ZenUser.
5. Log out of your browser, or open a second browser and then log in as acltest.
6. Select Infrastructure.

   You should see only the device you assigned to acltest.
7. Navigate to the device and notice that the edit capabilities are not available. This is because you are in read-only mode for this device.

Example: Restricted User with ZenOperator Role

The ZenUser role from the previous section allows read-only access to devices. By adding the ZenOperator role to specific devices, device classes, or groups of devices, a user will be able to acknowledge and close events, move events to history, and add log messages to events.

To add the ZenOperator role to specific devices, device classes, or groups of devices:

1. Select the user name whose role must be changed on certain devices.
2. In the left-hand pane, click Administered Objects.
3. Click the Action icon and choose the device, device class, or other device organizer to which you want to grant the ZenOperator role.
4. Select the ZenOperator role from the drop-down menu for the newly selected device, device class, or device organizer.

The user now has the ZenUser role for all devices in this instance, with the exception of the device(s) selected above which function under the ZenOperator role.

Example: Restricted User with ZenManager Role

Following the example above:

1. Change the acltest user's role to "ZenManager" on the device. (You must to do this as a user with ZenManager global rights.)
2. Go back to the acltest user's administered objects and set the role on the device to ZenManager.
3. As acltest, navigate back to the device. You now have access to edit the device.

Example: Adding Device Organizers

1. Go to Groups and create a group called "RestrictGroup."
2. Go to the acltest user's administered objects and add the group to the user.
3. Logged in as acltest, notice that groups can be added to a user.
4. Place a device within this group and as acltest you should not only see the device within the group but also in the device list.

Restricted User Organizer Management

1. Give the acltest user ZenManager on your restricted group.
2. As acltest, you can now add sub-organizers under the restricted group.

Viewing Events

A user in restricted mode does not have access to the global event console. The available events for the user can be seen under his organizers.

Reporting 9

Cisco UCS Performance Manager provides many useful summaries of monitored resources at the **Reports** tab of the Cisco UCS Performance Manager web interface.

Note If you experience any stairstepping in your graphs, you may want to change the reporting collection interval in Cisco UCS Performance Manager. For example, setting the reporting collection interval to 60 minutes tells Cisco UCS Performance Manager to update the API-driven reporting data at that interval which is different than the native collection interval.

To view a report, select the report's name in the left column.

Scheduling Reports

You can use `cron` to schedule reports from Cisco UCS Performance Manager at a defined interval. This procedure is optional. You can always generate on-demand reports using the Reports menu in Cisco UCS Performance Manager. In order to mail out reports, you must first enter the credentials for your SMTP host, port, username, and password in the **Advanced > Settings** page. Unfortunately, `localhost` SMTP configuration is not available for use with Cisco UCS Performance Manager.

To schedule a report to be generated and mailed out using `cron`:

1. Navigate to the report through the Reports menu and click on its name. Using Firebug or Chrome Developer tools, note the source frame URL, also called the referer. You will need this as an input later in this procedure. An example source frame URL is: `zport/dmd/Reports/Cisco%20UCS%20Capacity%20Reports/Storage%20Utilization%20vs%20Capacity?adapt=false`
2. In another browser window, log in to the Control Center master host as a user with `sudo` privileges.
3. Schedule `cron` to generate and mail a PDF of a report.

```
/etc/crontab
```

4. Add a line to `crontab` to define the time and command to run. For example:

```
30 16 * * * root serviced service run zope reportmail -u "http://
localhost:8080/<source_frame_url_of_report>" -U user -p password -a
 email@domain.com -f email@domain.com
```

This example will run the `serviced service run zope reportmail` command with the indicated arguments as the `root` user every day at 4:30p.m. Customize this example for your particular backup needs.

> **Note** The format for `crontab` entries is: `minute hour day_of_month month day_of_week user command`

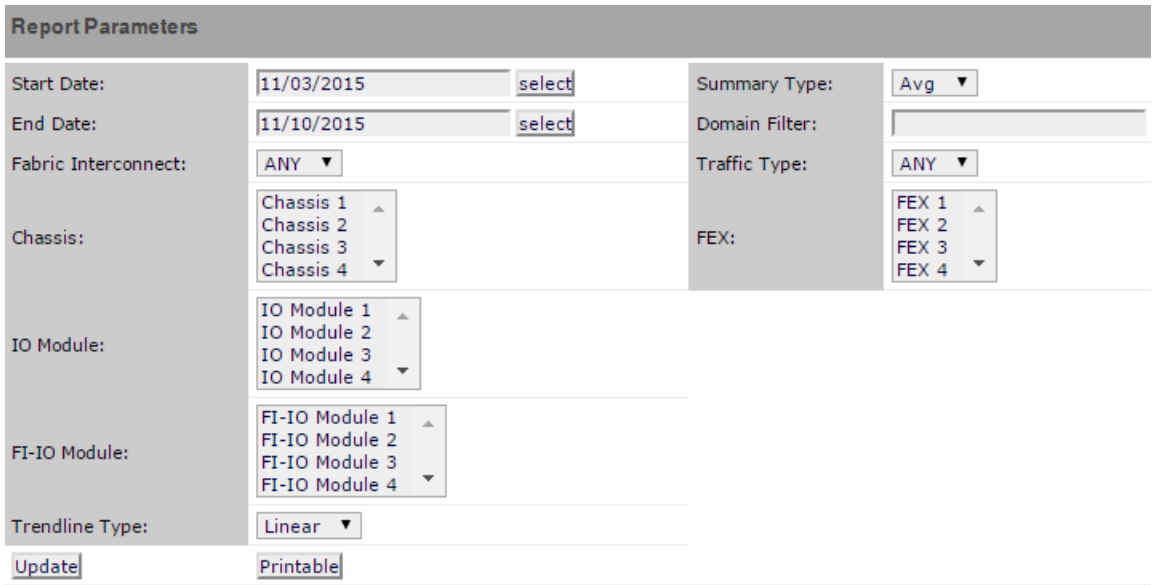
Cisco UCS Capacity Reports

The following reports highlight Cisco UCS capacity calculations. In reports that have a graphical display, you can click **Printable** to generate a printable version of the graphs in the report. For reports that are tabular, you can click **Export all** to generate a `.csv` file showing the data in spreadsheet form.

Aggregate Bandwidth Utilization

A summary of the aggregate throughput shown per chassis, per fabric extender, and per I/O module for each domain. Three graphs are shown per domain. You can see the individual components of these graphs on the particular device's component page. For example, to see the throughput on fex-2 of a particular device, you would click **Infrastructure**, then click the device name and select **Fabric Extenders** from the Components list. Click **fex-2** to display the graph of the throughput in the bottom pane. This represents this fabric extender's part in the total throughput displayed in this report.

Report Parameters



The following fields filter the results.

Start Date

End Date

The first and last dates of the range of dates to include in the report. To select a date from a calendar, click **select**. The default range is the week ending with the current date.

Summary Type

The type of summary that is to be displayed. **Average** is based on the 15-minute data collection, while **Max** is only taken once a day.

Domain Filter

A substring search of domains to include. A partial name matches all interface names that include it. You may also use a regular expression for this filter.

Fabric Interconnect

Select the FI to filter by.

Traffic Type

Type of traffic to display. Choose from **ANY**, **Tx** or **Rx**.

Chassis, FEX, IO Module, Shared Adaptor, FI-IO Module

Select the items to filter by. You can multi-select by Ctrl-clicking your selections.

Trendline Type

The calculation used to determine the trendline. Only available selection is **Linear**.

To generate or refresh the report, click **Update**.

To generate a printable version of the report, click **Printable**, then use the print functionality on your browser.

The following is an example of the three graphs generated per domain.

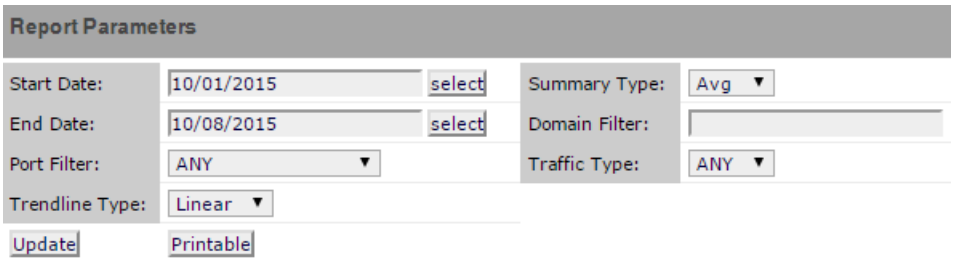
The following are some example scenarios that may be seen in graphs along with their corresponding description:

- If a graph shows 16.48 G (Current value) for Chassis-3, it is the aggregate (or sum) of Receiving (Rx) and Sending (Tx) bits of Chassis-3
- If a graph shows 1.89 M (Max value) for Fex-2, it is the aggregate (or sum) of the Receiving (Rx) and Sending (Tx) bits that happens on the ports connected to Fex-2.
- If a graph shows 17.15 G (Average value) for an IO module (e.g., Chassis-1_slot-1), it is the aggregate (or sum) of Receiving (Rx) and Sending (Tx) bits that are transferred specfically to the IO module.

Aggregate Port Pool Utilization

A summary of the aggregate port pool throughput per domain. Each domain is displayed in a separate graph with a separate line for each server port. You can see the individual components of these graphs on the particular device's component page.

Report Filtering



The following fields filter the results.

Start Date

End Date

The first and last dates of the range of dates to include in the report. To select a date from a calendar, click **select**. The default range is the week ending with the current date.

Summary Type

The type of summary that is to be displayed. **Average** is based on the 15-minute data collection, while **Max** is only taken once a day.

Domain Filter

A substring search of domains to include. A partial name matches all interface names that include it. You may also use a regular expression for this filter.

Port Filter

Select the type of ports to filter by. Options include **ANY**, **Port Channels**, **Server Ports**, and **Stand Alone Ports**.

Traffic Type

Type of traffic to display. Choose from **ANY**, **Tx** or **Rx**.

Trendline Type

The calculation used to determine the trendline. Only available selection is **Linear**.

To generate or refresh the report, click **Update**.

To generate a printable version of the report, click **Printable**, then use the print functionality on your browser.

The following is an example of the graph generated for throughput on a particular domain that is broken down by server port.

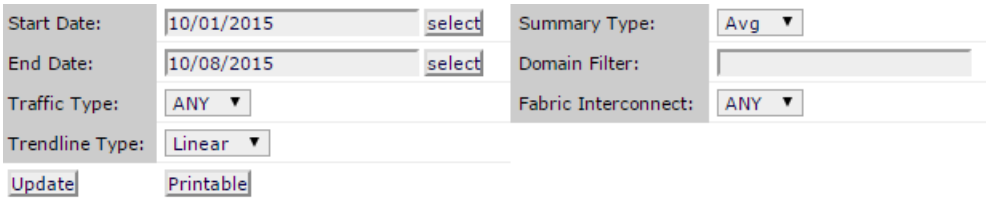
The following are some example scenarios that may be seen in graphs along with their corresponding description:

- If Switch-A to Fex-2 server ports shows a current value of 1G, the server ports that connect Switch A and Fex-2 transmit a total of 1Gbps, which includes both receiving and sending.
- If Switch-A to Chassis-1 server ports shows an average value of 2G, the server ports that connect Switch-A and Chassis-1 transmit an average of 2Gbps, which includes both receiving and sending.
- If Switch-B to Rack Server-1 server ports shows a maximum value of 5G, the server ports that connect Switch-B and Rack Server-1 transmit a total of 5Gbps, which includes both receiving and sending.

Bandwidth Utilization vs. Capacity

A summary of the total bandwidth utilization compared with capacity for each domain. Each domain has its own graph. The graph shows the percentage of utilization for both Rx (receiving or incoming) and Tx (transmitting or outgoing) network traffic. You can view individual components of this graph by viewing the Fabric Interconnect Capacity Utilization graph which can be found on the Fabric Interconnect component of your device.

Report Filtering



The following fields filter the results.

Start Date

End Date

The first and last dates of the range of dates to include in the report. To select a date from a calendar, click **select**. The default range is the week ending with the current date.

Summary Type

The type of summary that is to be displayed. **Average** is based on the 15-minute data collection, while **Max** is only taken once a day.

Domain Filter

A substring search of domains to include. A partial name matches all interface names that include it. You may also use a regular expression for this filter.

Traffic Type

Type of traffic to display. Choose from **ANY**, **Tx** or **Rx**.

Fabric Interconnect

Select the FI to filter by.

Trendline Type

The calculation used to determine the trendline. Only available selection is **Linear**.

To generate or refresh the report, click **Update**.

To generate a printable version of the report, click **Printable**, then use the print functionality on your browser.

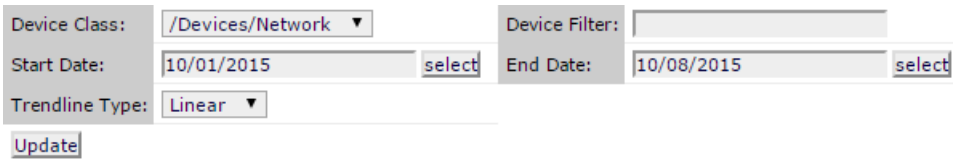
The following is an example scenarios that may be seen in graphs along with its corresponding description:

- If sys_switch-A shows a value of 10% for Rx, it uses only 10% of this fabric interconnect switch, e.g., if the fabric interconnect has a capacity of 800Gbps for Rx, then only 80Gbps is used for Rx. A similar calculation can be made for Tx.

Interface 95th Percentile

The Interface 95th Percentile report shows both the average input and output traffic rate as well as the 95th percentile value of the input and output traffic rate. The report is generated in a tabular form with the calculations shown by each interface.

Report Filtering



The following fields filter the results.

Device Class

The device class associated with the interfaces to include in the report. The default is `/Devices/Network`, all network devices.

Device Filter

The complete or partial name of the interfaces to include in the report. Letter case is ignored. A partial name matches all interface names that include it. You may also use a regular expression for this filter.

Start Date

End Date

The first and last dates of the range of dates to include in the report. To select a date from a calendar, click **select**. The default range is the week ending with the current date.

Trendline Type

The calculation used to determine the trendline. Only available selection is **Linear**.

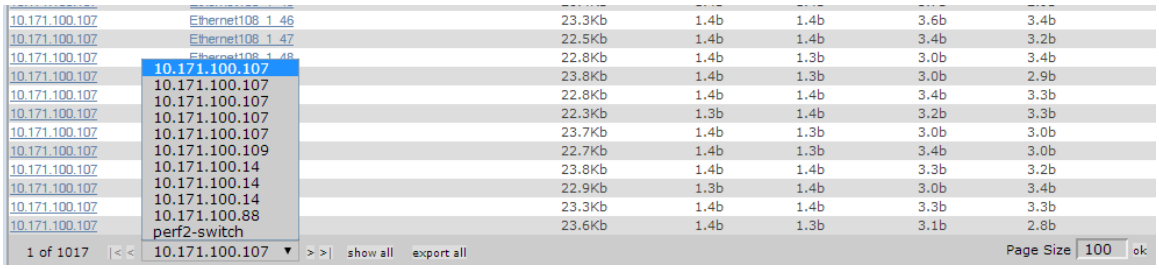
To generate or refresh the report, click **Update**.

Report Contents

Column	Content
Device	The name of the device that contains the interface, with a link to its overview page.
Interface	The name of the interface, with a link to its overview page.
Description	A description of the interface.
Speed	The maximum transfer rate the interface supports, per second.
In Avg	The average input traffic through the interface, per second .

Column	Content
Out Avg	The average output traffic through the interface, per second.
95% In	The input traffic rate of the 95th percentile.
95% Out	The output traffic rate of the 95th percentile.
Forecasted In Exhaustion	Projected date of exhaustion for input traffic.
Forecasted Out Exhaustion	Projected date of exhaustion for output traffic.

The following shows the navigation bar at the bottom of the report. To quickly navigate to other pages, select the device name from the pop-up list. In this example, there are 5 pages of results from device 10.171.100.107 followed by one page of results from device 10.171.100.109, etc.

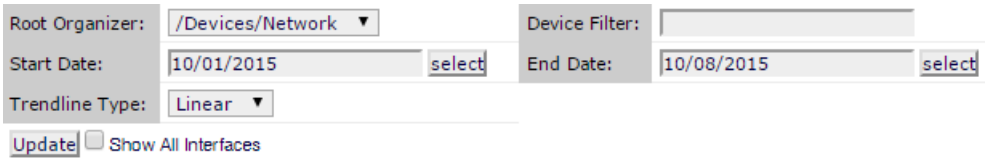


Click **Export all** to export the report as a `.csv` file.

Interface Utilization

The Interface Utilization report shows the average, maximum, and minimum input and output traffic rate. The report is generated in a tabular form with the calculations shown by each interface.

Report Filtering



The following fields filter the results.

Device Class

The device class associated with the interfaces to include in the report. The default is `/Devices/Network`, all network devices.

Device Filter

The complete or partial name of the interfaces to include in the report. Letter case is ignored. A partial name matches all interface names that include it. You may also use a regular expression for this filter.

Start Date

End Date

The first and last dates of the range of dates to include in the report. To select a date from a calendar, click **select**. The default range is the week ending with the current date.

Trendline Type

The calculation used to determine the trendline. Only available selection is **Linear**.

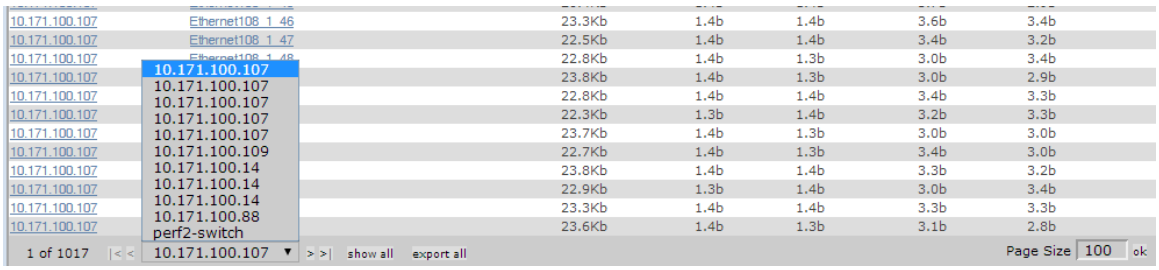
To generate or refresh the report, click **Update**. If you want to show all interfaces on the report, check the **Show All Interfaces** box before clicking **Update**.

Report Contents

Column	Content
Device	The name of the device that contains the interface, with a link to its overview page.
Interface	The name of the interface, with a link to its overview page.
Description	A description of the interface.
Speed	The maximum transfer rate the interface supports, per second.
In Avg	The average input traffic through the interface, per second.
Out Avg	The average output traffic through the interface, per second.
In Max	The maximum input traffic through the interface, per second.
Out Max	The maximum output traffic through the interface, per second.
In Min	The minimum input traffic through the interface, per second.
Out Min	The minimum output traffic through the interface, per second.
Forecasted In Exhaustion	Projected date of exhaustion for input traffic.
Forecasted Out Exhaustion	Projected date of exhaustion for output traffic.

Note In order for the In Max and Out Max values to be calculated, you need to have at least 8 hours worth of data, otherwise a N/A value will be returned.

The following shows the navigation bar at the bottom of the report. To quickly navigate to other pages, select the device name from the pop-up list. In this example, there are 5 pages of results from device 10.171.100.107 followed by one page of results from device 10.171.100.109, etc.

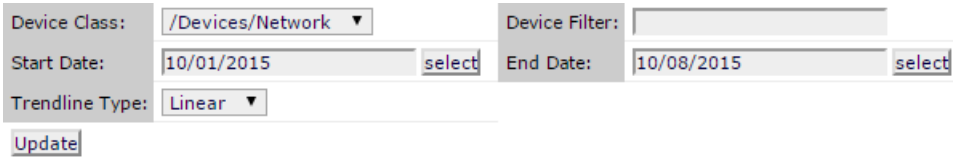


Click **Export all** to export the report as a `.csv` file.

Interface Volume

The Interface Volume report shows the total input and output traffic for the report period, along with a calculation of the input and output traffic per day. The report is generated in a tabular form with the calculations shown by each interface.

Report Parameters



The following fields filter the results.

Device Class

The device class associated with the interfaces to include in the report. The default is `/Devices/Network`, all network devices.

Device Filter

The complete or partial name of the interfaces to include in the report. Letter case is ignored. A partial name matches all interface names that include it. You may also use a regular expression for this filter.

Start Date

End Date

The first and last dates of the range of dates to include in the report. To select a date from a calendar, click **select**. The default range is the week ending with the current date.

Trendline Type

The calculation used to determine the trendline. Only available selection is **Linear**.

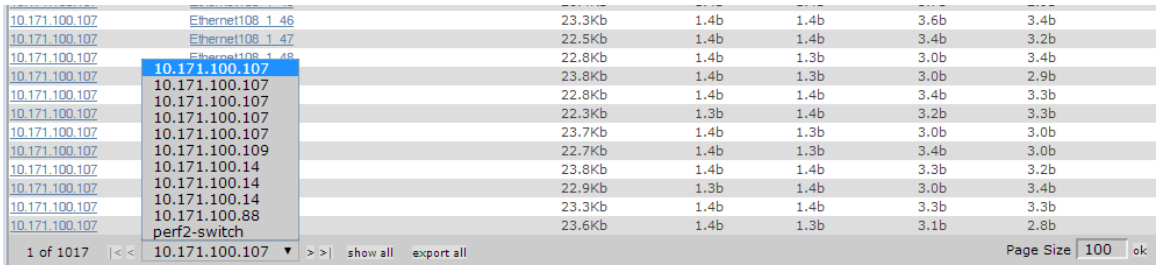
To generate or refresh the report, click **Update**.

Report Contents

Column	Content
Device	The name of the device that contains the interface, with a link to its overview page.
Interface	The name of the interface, with a link to its overview page.
Description	A description of the interface.
Speed	The maximum transfer rate the interface supports, per second.
In Vol	The input traffic through the interface for the time period of the report.
In Vol/day	The input traffic through the interface, per day.
Out Vol	The output traffic through the interface for the time period of the report.
Out Vol/ day	The output traffic through the interface, per day.
Total Vol	Total volume of traffic through the interface for the time period of the report.
Forecasted In Exhaustion	Projected date of exhaustion for input traffic.

Column	Content
Forecasted Out Exhaustion	Projected date of exhaustion for output traffic.

The following shows the navigation bar at the bottom of the report. To quickly navigate to other pages, select the device name from the pop-up list. In this example, there are 5 pages of results from device 10.171.100.107 followed by one page of results from device 10.171.100.109, etc.

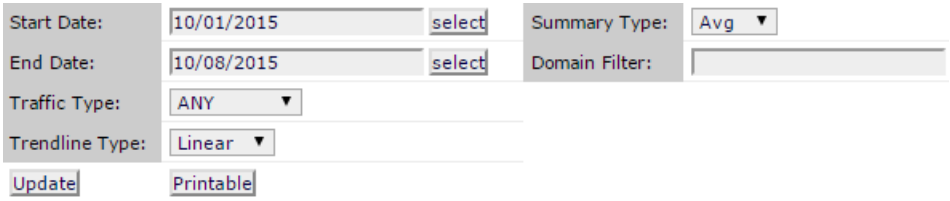


Click **Export all** to export the report as a `.csv` file.

Port Utilization

The report displays the total bandwidth broken down by LAN uplink, fiber channel uplink, appliance, and server ports.

Report Parameters



The following fields filter the results.

Start Date

End Date

The first and last dates of the range of dates to include in the report. To select a date from a calendar, click **select**. The default range is the week ending with the current date.

Summary Type

The type of summary that is to be displayed. **Average** is based on the 15-minute data collection, while **Max** is only taken once a day.

Domain Filter

A substring search of domains to include. A partial name matches all interface names that include it. You may also use a regular expression for this filter.

Traffic Type

Type of traffic to display. Choose from **ANY**, **Tx** or **Rx**.

Trendline Type

The calculation used to determine the trendline. Only available selection is **Linear**.

To generate or refresh the report, click **Update**.

To generate a printable version of the report, click **Printable**, then use the print functionality on your browser.

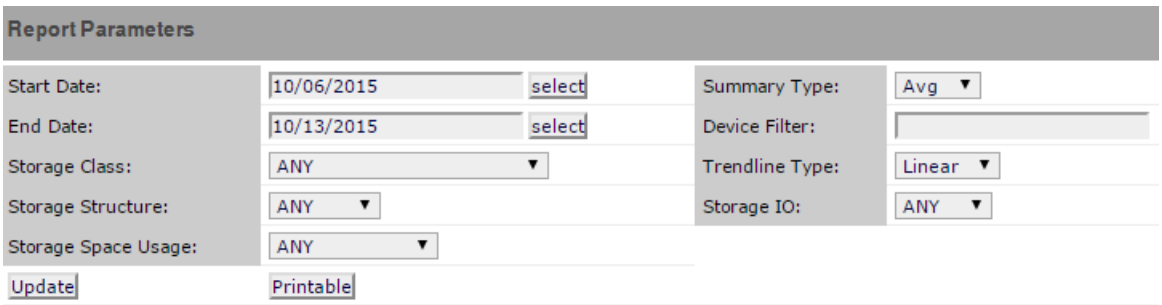
The following is an example scenarios that may be seen in graphs along with its corresponding description:

- If the Server ports current value is 10G, then all the ports that have the Server port interface role are transmitting data at a combined rate of 10Gbps.
- If the LAN Uplink ports maximum value is 200M, then the ports connected from the Fabric Interconnect switch to the LAN network transfers data at 200Mbps.

Storage Utilization vs. Capacity

A summary of the total storage utilization compared with capacity for each storage device. Each device has its own group of graphs and may display some of the following information: Storage Utilization, Bytes Per Cycle, Managed Space Usage, Time Utilization, Data Throughput, Raw Space Usage, Datastore IO Rate, and Datastore IO Disk Usage. The graphs display both the current utilization and capacity along with projected values all on the same graph. Use the following report parameters to filter the report to the devices and type of information you are most interested in.

Report Filtering



The following fields filter the results.

Start Date

End Date

The first and last dates of the range of dates to include in the report. To select a date from a calendar, click **select**. The default range is the week ending with the current date.

Summary Type

The type of summary that is to be displayed. **Average** is based on the 15-minute data collection, while **Max** is only taken once a day.

Device Filter

A substring search of devices to include. A partial name matches all interface names that include it. You may also use a regular expression for this filter.

Storage Class

Select the storage device class to filter by. You can select all devices class by selecting **ANY**.

Trendline Type

The calculation used to determine the trendline. Only available selection is **Linear**.

Storage Structure

Type of storage structure. Choose from **ANY**, **Disk** or **Inodes**.

Storage IO

Type of storage process. Choose from **ANY**, **Read** or **Write**.

Storage Space Usage

Type of storage space usage. Choose from **ANY**, **Total**, **Used**, **Subscribed**, **Managed**, **Uncommitted**, **Raw**, or **Capacity**.

To generate or refresh the report, click **Update**.

To generate a printable version of the report, click **Printable**, then use the print functionality on your browser.

Cisco UCS Reports

For each of the following Cisco UCS reports, you can click **Export all** to generate a `.csv` file showing the data in spreadsheet form.

Free Memory Slots

This report lists the number of free memory slots in each component grouped by domain. There are no filtering capability in this report.

Report Contents

Column	Content
Name	The domain name.
Component	The component being reported on.
Free Slots	The number of free memory slots on the corresponding component. At the bottom of this column, a list of total free memory slots is displayed.

Click **Export all** to export the report as a `.csv` file.

Hardware Inventory

This reports lists the inventory of the UCS devices being monitored.

Report Contents

Column	Content
UCS Device	The name of the UCS device. Clicking the link takes you to the device overview page.
Component	Lists components and related sub-components of the device. Clicking a link takes you to the appropriate device component page.
Manufacturer	The manufacturer of the component.
Model	The model number of the component.
Serial #	The serial number of the component.
Description	Detailed information about the component.

Click **Export all** to export the report as a `.csv` file.

Enterprise Reports

For each of the following Enterprise reports, you can click **Export all** to generate a `.csv` file showing the data in spreadsheet form.

95th Percentile

A summary of the regular and sustained utilization of network interfaces.

95th percentile is a standard calculation used to evaluate the input and output utilization of network interfaces. The 95th percentile calculation reveals how much network capacity is needed 95 percent of the time.

Report Filtering

The following fields filter the results.

Device Class

The device class associated with the interfaces to include in the report. The default is `/Devices`, all device classes.

Device Filter

The complete or partial name of the interfaces to include in the report. Letter case is ignored. A partial name matches all interface names that include it. You may also use a regular expression for this filter.

Start Date

End Date

The first and last dates of the range of dates to include in the report. To select a date from a calendar, click **select**. The default range is the week ending with the current date.

To generate or refresh the report, click **Update**.

Report Contents

Column	Content
Device	The name of the device that contains the interface, with a link to its overview page.
Interface	The name of the interface, with a link to its overview page.
Description	A description of the interface.
Speed	The maximum transfer rate the interface supports, per second.
In Avg	The average input traffic through the interface, per second.
Out Avg	The average output traffic through the interface, per second.
95% In	The input traffic rate of the 95th percentile, per second.
95% Out	The output traffic rate of the 95th percentile, per second.

Cisco Inventory

This report lists all the Cisco devices being monitored.

Report Filtering

Device Class

The device class to use for filtering. The default is `/Network/Cisco`.

Group

The specific group to consider when running the report. The default is `All`. The group could be a specific application group.

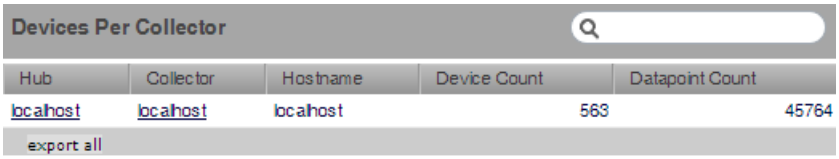
To generate or refresh the report, click **Update**.

Report Contents

Column	Content
Name	The name of the Cisco device. Clicking the link takes you to the device overview page.
IP Address	Lists the IP address of the Cisco device.
Model	The model of the device. Clicking the link takes you to the Manufacturers Overview page for that product.
Serial #	The serial number of the Cisco device.
Type	The type of Cisco product, e.g., Device.

Datapoints Per Collector

This report shows the number of devices and data points per collector, which is useful for gauging how much monitoring load is on each collector.



Report Contents

Column	Content
Hub	Name of the hub the collector is on
Collector	Name of the collector the devices are on
Hostname	Hostname location
Device Count	Total number of devices on the collector
Datapoint Count	Total number of data points being generated on the collector

Defined Thresholds

The Defined Thresholds report provides details about all thresholds defined in the system. The report links to the target of each threshold. The target can be a device class, individual device, or individual component.

This report is useful for administering the system. You can use it to quickly identify which threshold events can occur within the system, and the severity of those events.

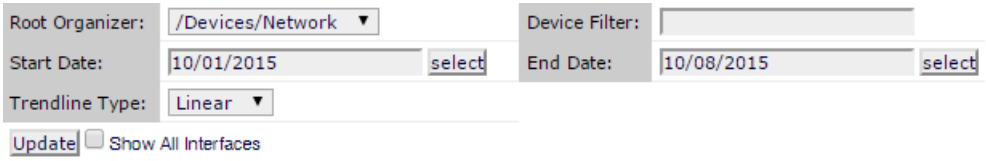
Report Contents

Column	Content
Target	The device class of the defined threshold.
Template	The template associated with the defined threshold.
Threshold	The name of the defined threshold. Clicking the link takes you to the Performance Template where the threshold is defined.
Severity	The severity level assigned to the alert when the threshold is reached.
Enabled	The enabled status of the threshold.

Interface Utilization

The Interface Utilization report shows the average, maximum, and minimum input and output traffic rate. The report is generated in a tabular form with the calculations shown by each interface.

Report Filtering



The following fields filter the results.

Device Class

The device class associated with the interfaces to include in the report. The default is `/Devices/Network`, all network devices.

Device Filter

The complete or partial name of the interfaces to include in the report. Letter case is ignored. A partial name matches all interface names that include it. You may also use a regular expression for this filter.

Start Date

End Date

The first and last dates of the range of dates to include in the report. To select a date from a calendar, click **select**. The default range is the week ending with the current date.

Trendline Type

The calculation used to determine the trendline. Only available selection is **Linear**.

To generate or refresh the report, click **Update**. If you want to show all interfaces on the report, check the **Show All Interfaces** box before clicking **Update**.

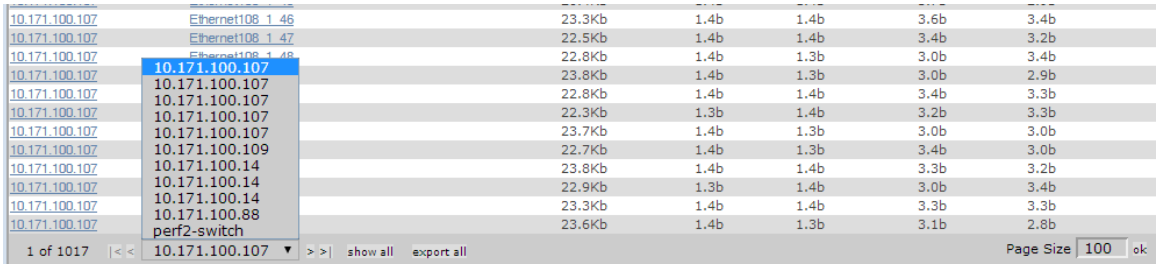
Report Contents

Column	Content
Path	Path to the device class.
Device	The name of the device that contains the interface, with a link to its overview page.
Interface	The name of the interface, with a link to its overview page.
Description	A description of the interface.
Speed	The maximum transfer rate the interface supports, per second.

Column	Content
In Avg	The average input traffic through the interface, per second.
Out Avg	The average output traffic through the interface, per second.
In Max	The maximum input traffic through the interface, per second.
Out Max	The maximum output traffic through the interface, per second.
95% In	The input traffic rate of the 95th percentile, per second.
95% Out	The output traffic rate of the 95th percentile, per second.

Note In order for the In Max and Out Max values to be calculated, you need to have at least 8 hours worth of data, otherwise a N/A value will be returned.

The following shows the navigation bar at the bottom of the report. To quickly navigate to other pages, select the device name from the pop-up list. In this example, there are 5 pages of results from device 10.171.100.107 followed by one page of results from device 10.171.100.109, etc.



Click **Export all** to export the report as a `.csv` file.

Notifications and Triggers by Recipient

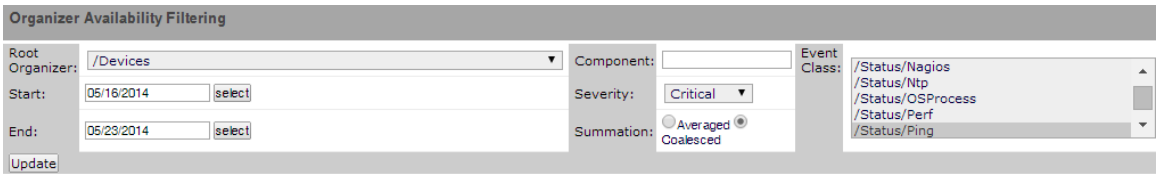
Organizer Availability

This report provides the availability percentage of all network organizers in the system. It can be filtered by organizer, event class, component, event severity, and date.

You can report on the availability of device classes or application groups within a defined time frame. This report offers two reporting modes:

- **Averaged** - Defines the organizer as available for the average availability time for all devices contained in it.
- **Coalesced** - Defines the organizer as available only if all devices are available during a certain time period.

Report Filtering



Root Organizer

The device class to use for filtering. The default is `/Devices`.

Start Date

End Date

The first and last dates of the range of dates to include in the report. To select a date from a calendar, click **select**. The default range is the week ending with the current date.

Component

The specific group to consider when running the report. The default is `All`. The group could be a specific application group.

Severity

The severity level to filter by. The default is `Critical`. If another level is wanted, select it from the drop-down list.

Summation

Select between `Averaged` and `Coalesced` depending on how you want to define the organizer as available. The default is `Coalesced`.

Event Class

The event class to use for filtering. The default is `/Status/Ping`.

To generate or refresh the report, click **Update**.

Note If you export the report, be sure to format the percentage columns to show percentages instead of decimal values.

Users Group Membership (User to Group Mapping)

A list of Cisco UCS Performance Manager users and the groups to which they belong.

Column	Content
User	The name of a user, with a link to the user's **USER SETTINGS** page.
Groups	The list of groups to which the user belongs. Each name includes a link to the group's **Users in Group** page.

Performance Reports

Availability Report

Shows the percentage of time that a device or component is considered available. You can filter this report on device, component, event class, or severity. You can also limit the time frame for the availability.

The value the percent available is calculated by first summing the duration of all events of a particular class with a production state of `Production` and with a severity greater than or equal to a specified severity. This sum is then divided by the total duration of the time range, and then subtracted from 1 and multiplied by 100 to get the percent available, as in the following equation:

```
1 - ((Total event down time) / (total duration)) * 100
```

Note Events whose firsttime and lasttime fields are the same are not used in the calculation. These could represent an event that occurs and is subsequently cleared by the next event, or an event that has happened only once in the specific date range.

CPU Utilization

Shows monitored interfaces, devices, load averages, and % utility. You can customize start and end dates, and summary type (average or maximum).

Interface Utilization

Shows the traffic through all network interfaces monitored by Cisco UCS Performance Manager.

Columns included in the report:

- **Device** - Interface's device
- **Interface** - Interface
- **Speed** - Interface's rated bandwidth, in bits per second
- **Input** - Average traffic going out of the interface, in bits per second
- **Output** - Average traffic coming in to the interface, in bits per second
- **Total** - Total average traffic across the interface, in bits per second
- **% Util** - Average fraction of the interface's bandwidth consumed

Memory Utilization

Provides system-wide information about the memory usage for devices in Cisco UCS Performance Manager.

Columns included in the report:

- **Device** - Name of the device
- **Total** - Total memory
- **Available** - Available memory
- **Cache Memory** - Cache memory
- **Buffered Memory** - Buffered memory
- **% Util** - Percentage of memory utilized

Threshold Summary

Provides information about the devices that are approaching or exceeding their thresholds.

Columns included in the report:

- **Device** - Name of the device
- **Component** - Component affected
- **Event Class** - Event class. You can filter which event classes are displayed from the Event Class drop-down list.
- **Count** - Number of occurrences
- **Duration** - Length of time
- **%** - Percentage

System Reports

For each of the following System reports, you can click **Export all** to generate a `.csv` file showing the data in spreadsheet form.

Non-UCS Servers

This report lists the non-UCS servers that are being monitored, but are not part of the Cisco UCS Performance Manager licensing. The following information is provided:

- Server name

- Server type
- Monitoring status

You can contact Cisco Support to update your licensing agreement to cover these devices or you can delete them from Cisco UCS Performance Manager. For more information about deleting devices, see *Deleting a Device* on page 55.

VMware vSphere Reports

The following operational reports are available for vSphere. Access these reports from the **Reports > vSphere** page:

- **Clusters** - Shows all clusters, with the count of VMs (total and powered on), hosts, and CPU/Memory utilization within each cluster.
- **Datastores** - Shows all datastores, with the number of connected VMs (total and powered on) and the disk space available and consumed on each datastore.
- **Hosts** - Shows all hosts, with the count of VMs (total and powered on), hosts, CPU/Memory reservation and utilization on each host
- **VMs** - Shows all VMs, their operating system, CPU/Memory utilization, and which host/cluster they reside within.
- **VMware Utilization** - Provides a summary of VMs, CPU, memory, and disk utilization over a specified time interval, broken down by host.

For each of these tabular reports, you can click **Export all** to generate a `.csv` file showing the data in spreadsheet form.

General Administration and Settings 10

Events Settings

You can adjust events settings for:

- Events database connection
- Event maintenance

Changing Events Database Connection Information

To edit events database connection settings, make changes in the `zeneventserver.conf` file. You can edit the file directly, or run a configuration script.

Configurable database connection settings are:

- **JDBC Hostname (zep.jdbc.hostname)**- Specify the IP address of the host.
- **JDBC Port (zep.jdbc.port)**- Specify the port to use when accessing the events database.
- **JDBC Database Name (zep.jdbc.dbname)**- Specify the database name.
- **JDBC Username (zep.jdbc.username)**- Specify the user name for the database.
- **JDBC Password (zep.jdbc.password)**- Specify the password for the database.

To edit these values, run the `zeneventserver` configuration script, as follows:

```
zeneventserver-config -u zep.jdbc.
      Name=
      Value
```

Where *Name* is the partial setting name and *Value* is the value you want to specify for the setting.

Changing Events Maintenance Settings

To edit maintenance settings, make changes to one or more fields on the Event Configuration page (**Advanced > Settings > Events**):

- **Don't Age This Severity and Above** - Options are Age All Events, Critical, Error, Warning, Info, Debug, and Clear. By default, this value is set to Error, meaning that all events with a status of Error or Critical are not aged.
- **Event Aging Threshold (minutes)** - Set the time value, in minutes, that an event must reach before it is aged. By default, this is 240 minutes.

- **Event Aging Interval (milliseconds)** - The interval when events are scanned to perform autoaging. By default, this is 60000 milliseconds (60 sec).
- **Event Aging Limit** - The maximum number of events to age in each interval. The limit should be kept relatively low to prevent large database transactions. By default, this is 1000 events.
- **Event Archive Threshold (minutes)** - Specify the number of minutes since a closed event was last seen before it is moved to the event archive. The minimum value is 1; the maximum value is 43200.
- **Event Archive Interval (milliseconds)** - The interval when events are scanned for moving to the archive. By default, this is 60000 milliseconds (60 sec).
- **Event Archive Limit** - The maximum number of events to archive in each interval. The limit should be kept relatively low to prevent large database transactions. By default, this is 1000 events.
- **Delete Archived Events Older Than (days)** - The number of days that events in the event archive are saved. By default, they are kept in the archive for 90 days. The minimum value is 1 and the maximum value is determined by the range of event archive partitions. With the default configuration, the maximum value is 1000 days.
- **Default Syslog Priority** - Specify the default severity level assigned to an event coming from zensyslog if no priority can be determined from the event.
- **Default Availability Report (days)** - Enter the number of days to include in the automatically generated Availability Report. This report shows a graphical summary of availability and status.
- **Max Event Size in Bytes** - The maximum size of an event that will be processed in bytes. Events that are too large will be logged and dropped. Events that will become too big will have their details overwritten with new details. By default, this is 32768 bytes.
- **Summary Index Interval (milliseconds)** - The default indexing interval of the event summary in milliseconds. By default, this is 1000 milliseconds (1 sec).
- **Archive Index Interval (milliseconds)** - The default indexing interval of the event archive in milliseconds. By default, this is 30000 milliseconds (30 sec).
- **Index Limit** - The number of events to index in each index interval. By default, this is 1000 events.
- **Event Time Purge Interval (days)** - The number of days that event occurrence time are kept. By default, they are kept for 7 days. The minimum value is 1 and the maximum value is determined by the range of event time partitions. With the default configuration, the maximum value is 7 days.
- **Enable Event Flapping Detection** - Select this check box if you wish to enable event flapping detection. If an event is created and then cleared *flapping_threshold* times in *event_flapping_interval* time then an event of event flapping event class is created.
- **Event Flapping Event Class** - The event class under which generated flapping events belong.
- **Clear Event Heartbeats** - Click **Clear** to clear the event heartbeats.

Rebuilding the Events Index

If you encounter inconsistent search results, you can rebuild the events index.

1. Log in to an account on the Control Center master host that has permission to use the Control Center command-line interface.
2. Stop zeneventserver:

```
serviced service stop zeneventserver
```

3. Attach to the Cisco UCS Performance Manager application.

```
serviced service attach zope/0
```

4. Delete the index:

```
rm -rf $ZENHOME/var/zeneventserver/index
```

5 Exit the container session.

```
exit
```

6 Restart zeneventserver:

```
serviced service start zeneventserver
```

Depending on the number of events in the database, it may take a significant amount of time for indexing to complete. Until every event is indexed, the number of events shown in the event console may be inconsistent.

Thresholds

Thresholds define expected bounds for data points. When the value returned by a data point violates a threshold, the system creates an event. There are several threshold types available:

- MinMax
- ValueChange
- CiscoStatus
- PredictiveThreshold

There are many thresholds already defined in the system. You can see all the defined thresholds in the Defined Thresholds report which can be accessed on the **Reports > Enterprise Reports** menu.

The following sections describe each type of threshold and how to create a new one and edit an existing one.

MinMax Threshold

MinMax thresholds inspect incoming data to determine whether it exceeds a given maximum or falls below a given minimum. You can use a MinMax threshold to check for these scenarios:

- *The current value is less than a minimum value.* To do this, you should set only a minimum value for the threshold. Any value less than this number results in creation of a threshold event.
- *The current value is greater than a maximum value.* To do this, you should set only a maximum value for the threshold. Any value greater than this number results in creation of a threshold event.
- *The current value is not a single, pre-defined number.* To do this, you should set the minimum and maximum values for the threshold to the same value. This will be the only "good" number. If the returned value is not this number, then a threshold event is created.
- *The current value falls outside a pre-defined range.* To do this, you should set the minimum value to the lowest value within the good range, and the maximum value to the highest value within the good range. If the returned value is less than the minimum, or greater than the maximum, then a threshold event is created.
- *The current value falls within a pre-defined range.* To do this, you should set the minimum value to the highest value within the bad range, and the maximum value to the lowest value within the bad range. If the returned value is greater than the maximum, and less than the minimum, then a threshold event is created.

ValueChange Threshold

ValueChange thresholds inspect incoming data to determine whether a status change has occured and if so issues an event based on the defined severity.

CiscoStatus Threshold

The CiscoStatus threshold is a special threshold that uses preconfigured maps of numeric values returned by SNMP datasources to Cisco UCS Performance Manager event severities. The following is an example OID and its mapped values. For a complete list of OIDs and values that are supported, visit *http://wiki.zenoss.org/CiscoStatus_Threshold*.

CISCO-ENTITY-FRU-CONTROL-MIB::cefcModuleOperStatus

- (1) unknown - Critical
- (2) OK - Clear
- (3) disabled - Clear
- (4) OK (diag failed) - Warning
- (5) boot - Warning
- (6) self-test - Warning
- (7) failed - Critical
- (8) missing - Critical
- (9) mismatch w/parent - Critical
- (10) mismatch w/config - Critical
- (11) diag-failed - Critical
- (12) dormant - Critical
- (13) out of service (admin) - Info
- (14) out of service (environ) - Critical
- (15) powered down - Critical
- (16) powered up - Critical
- (17) power denied - Critical
- (18) power cycle - Warning
- (19) OK (power warning) - Warning
- (20) OK (power critical) - Critical
- (21) sync in progress - Clear
- (22) upgrading - Critical
- (23) OK (auth failed) - Critical

PredictiveThreshold

The predictive threshold allows you to use data from the past to project a value in the future and send an event if the future projected threshold is breached during a pre-defined time period. Cisco UCS Performance Manager uses a linear projection algorithm for all projections. For example, you could predict total raw storage capacity of a disk or the bandwidth utilization percentage. Several predictive thresholds are already defined in the system. You can see all the defined thresholds in the Defined Thresholds report which can be accessed on the **Reports > Enterprise Reports** menu.

Predictive thresholds are also used for creating a trendline on a graph. You can add the threshold to the management of graph points so that a trendline will be added to the graph. For detailed steps, see the *Cisco UCS Performance Manager User Guide*.

Adding Thresholds

Follow these steps to define a threshold for a data point:

1. From the Navigation menu, select **Advanced > Monitoring Templates**.
2. Click on the template that contains the data point you want to use in your threshold. The Data Sources window is populated with folders containing all the data points being collected.
3. Select the data point by opening the appropriate folder in the data source and clicking on the data point row.

4 In the Thresholds area, click the **Add** icon.

The Add Threshold dialog appears.

5 Enter a name and select the threshold type, then click **Add**. The threshold name and type is displayed in the Thresholds window.

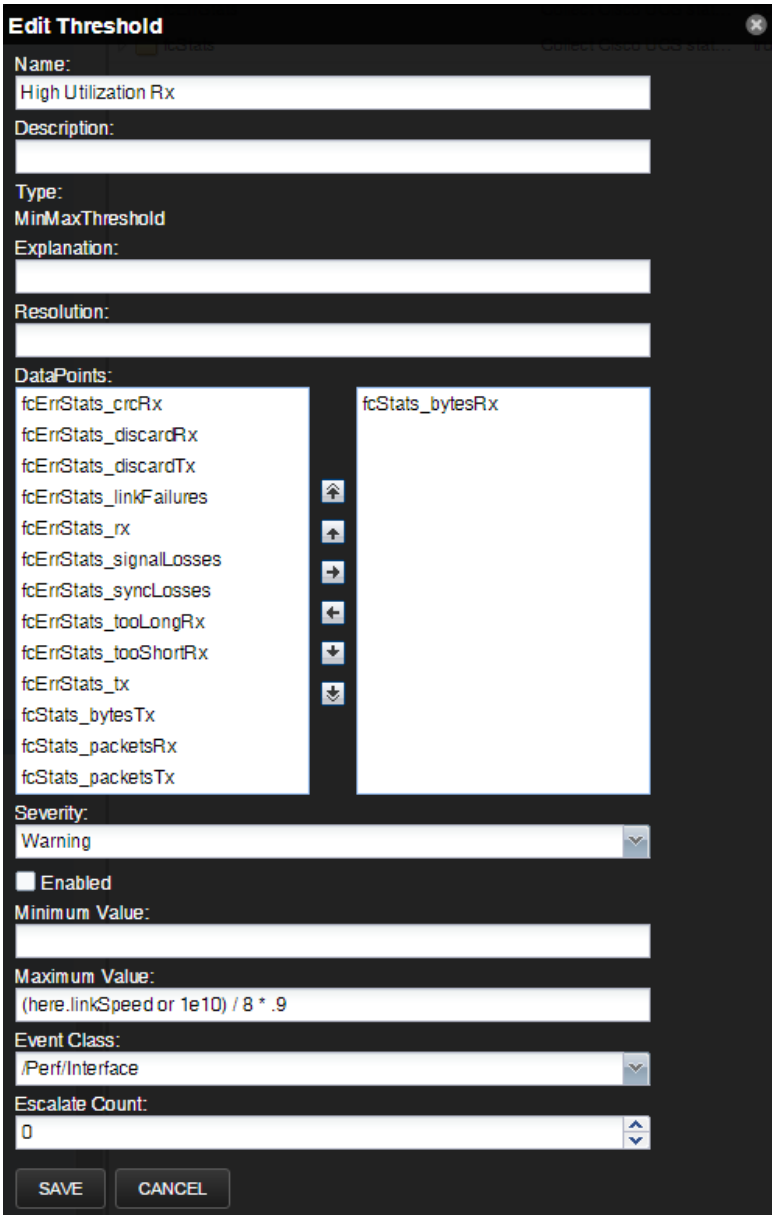
Editing MinMax thresholds

The threshold must be created by the Add Threshold functionality or already be defined in the system before you can edit it.

To edit a MinMax threshold:

1 Double-click the threshold in the list. The Edit Threshold dialog appears.

Figure 65: Edit Threshold



2 Enter or select values to define the threshold:

- **Name**- Displays the value for the ID you entered on the Add a New Threshold dialog.
- **Description**- Description of the threshold that you entered on the Add a New Threshold dialog. The description is included in each event that is created from this threshold.
- **Type**- Type of threshold that you selected. You cannot change the type of threshold. If you want a different type of threshold, you need to create a new one and assign the correct type.
- **Explanation**- Information field where a user can enter information about what the event means. This field is included in each event that is created from this threshold
- **Resolution**- Information field where a user can enter information about what to do to resolve the event. This field is included in each event that is created from this threshold.
- **Data Points**- Select one or more data points to which this threshold will apply and click the right-arrow button to move them to the selected column.
- **Severity**- Select the severity level of the first event triggered when this threshold is breached.
- **Enabled**- Select the check box to enable the threshold, or clear the check box to disable it.
- **Minimum Value**- If this field contains a value, then each time one of the select data points falls below this value an event is triggered. This field may contain a number or a Python expression.

  When using a Python expression, the variable *here* references the device or component for which data is being collected. For example, a 90% threshold might be specified as:

  ```
  (here.linkSpeed or 1e10) /8 * .9
  ```

  The division by 8 is needed because interface speed frequently is reported in bits/second, where the performance data is bytes/second.
- **Maximum Value**- If this field contains a value, then each time one of the selected data points goes above this value an event is triggered. This field may contain a number or a Python expression.
- **Event Class**- Select the event class of the event that will be triggered when this threshold is breached.
- **Escalate Count**- Enter the number of consecutive times this threshold can be broken before the event severity is escalated by one step. A value of zero (0) indicates that the severity will not escalate.

3 Click **Save** to confirm the edits.

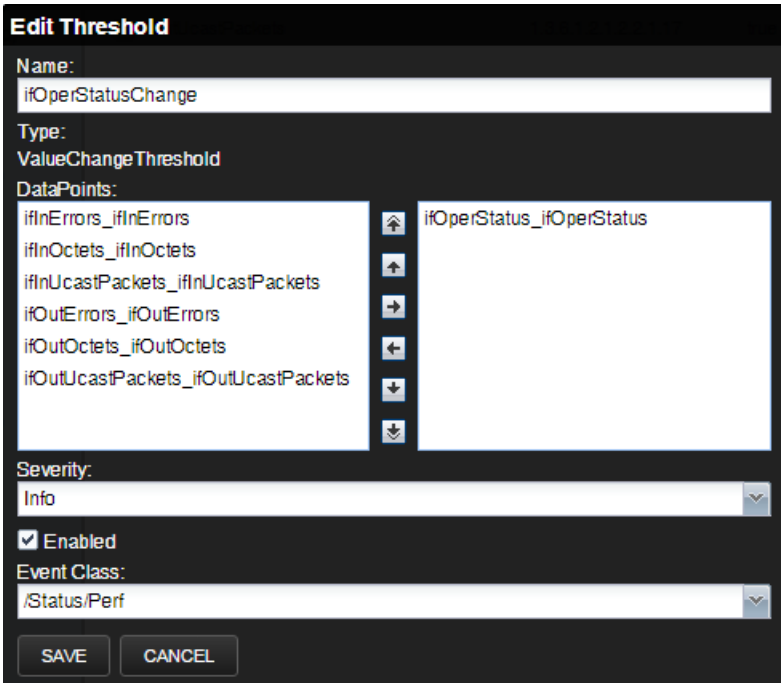
Editing ValueChange thresholds

The threshold must be created by the Add Threshold functionality or already be defined in the system before you can edit it.

To edit a ValueChange threshold:

1 Double-click the threshold in the list. The Edit Threshold dialog appears.

Figure 66: Edit Threshold



2 Enter or select values to define the threshold:

- **Name**- Displays the value for the ID you entered on the Add a New Threshold dialog.
- **Type**- Type of threshold that you selected. You cannot change the type of threshold. If you want a different type of threshold, you need to create a new one and assign the correct type.
- **Data Points**- Select one or more data points to which this threshold will apply and click the right-arrow button to move them to the selected column. When the data point changes status, an event will be triggered.
- **Severity**- Select the severity level of the first event triggered when this threshold is breached.
- **Enabled**- Select the check box to enable the threshold, or clear the check box to disable it.
- **Event Class**- Select the event class of the event that will be triggered when this threshold is breached.

3 Click **Save** to confirm the edits.

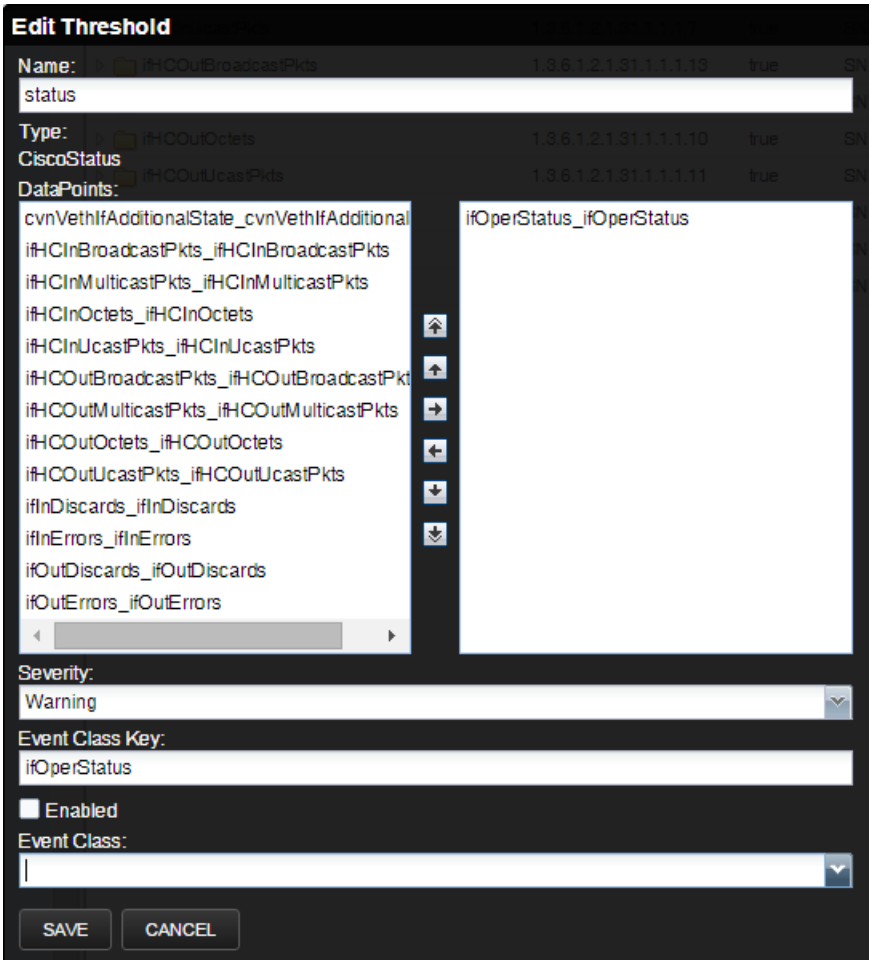
Editing CiscoStatus thresholds

The threshold must be created by the Add Threshold functionality or already be defined in the system before you can edit it.

To edit a ValueChange threshold:

1 Double-click the threshold in the list. The Edit Threshold dialog appears.

Figure 67: Edit Threshold



2 Enter or select values to define the threshold:

- **Name**- Displays the value for the ID you entered on the Add a New Threshold dialog.
- **Type**- Type of threshold that you selected. You cannot change the type of threshold. If you want a different type of threshold, you need to create a new one and assign the correct type.
- **Data Points**- Select one or more data points to which this threshold will apply and click the right-arrow button to move them to the selected column. When the data point changes status, an event will be triggered.
- **Severity**- Select the severity level of the first event triggered when this threshold is breached.
- **Event Class Key**- The event class key from the data point you selected will be shown here.
- **Enabled**- Select the check box to enable the threshold, or clear the check box to disable it.
- **Event Class**- Select the event class of the event that will be triggered when this threshold is breached.

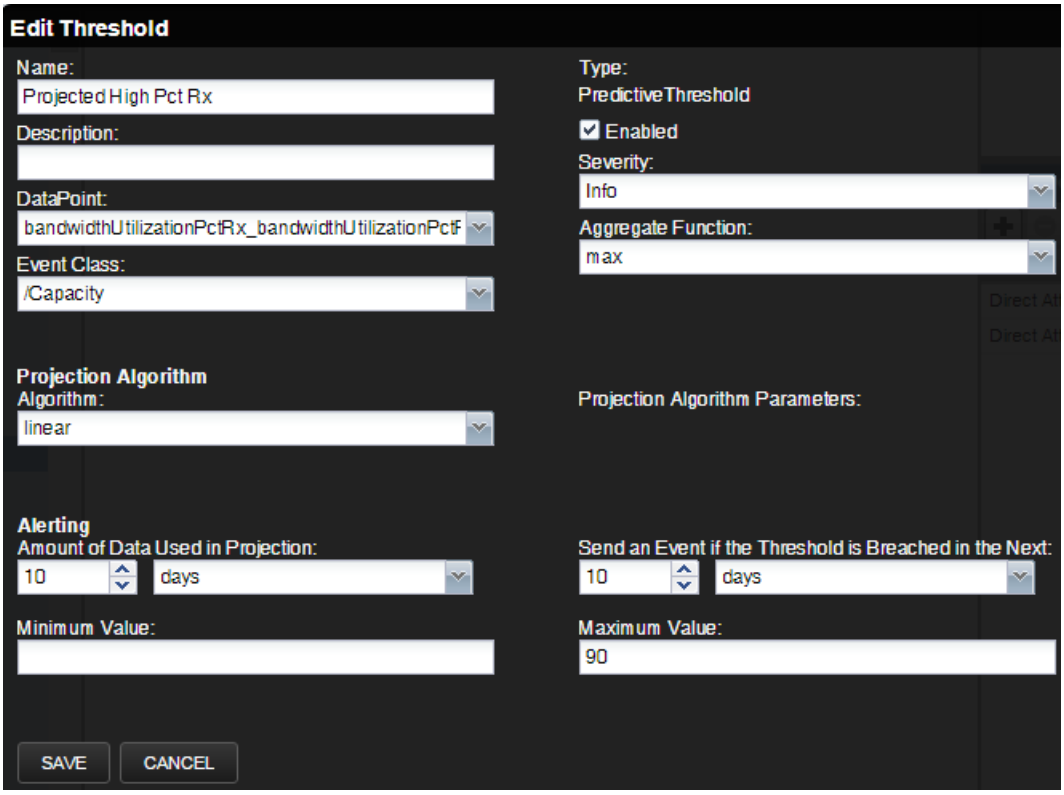
3 Click **Save** to confirm the edits.

Editing PredictiveThresholds

The threshold must be created by the Add Threshold functionality or already be defined in the system before you can edit it.

1 Double-click the threshold in the list. The Edit Threshold dialog appears.

Figure 68: Edit Threshold



2 Enter or select values to define the threshold:

- **Name**- Displays the value for the ID you entered on the Add a New Threshold dialog.
- **Description**- Description of the threshold that you entered on the Add a New Threshold dialog. The description is included in each event that is created from this threshold.
- **Data Point**- Select the data point to which this threshold will apply.
- **Event Class**- Select the event class of the event that will be triggered when this threshold is breached.
- **Type**- Type of threshold that you selected. You cannot change the type of threshold. If you want a different type of threshold, you need to create a new one and assign the correct type.
- **Enabled**- Select the check box to enable the threshold, or clear the check box to disable it.
- **Severity**- Select the severity level of the first event triggered when this threshold is breached.
- **Aggregate Function**- The type of function to use when analyzing the past data. For example, do you look at the peak values in the past or average values. The default value is `max`.
- **Algorithm**- Algorithm to use for the projection. Value is linear.
- **Projection Algorithm Parameters**- Some algorithms need additional parameters. Enter them as required.
- **Amount of Data Used in Projection**- Set the amount of historical data to be used when calculating the projection.
- **Send an Event if the Threshold is Breached in the Next**- Set the timeframe in days, weeks, or months. If the threshold is breached within this time period in the future, an event will be sent.
- **Minimum Value**- If this field contains a value, then each time one of the select data points falls below this value an event is triggered. This field may contain a number or a Python expression. An expression is required when using gauge or calculated values.

When using an expression, the variable *here* references the device or component for which data is being collected. For example, a 90% threshold for interface speed might be specified as:

```
(here.linkSpeed or 1e10) /8 * .9
```

The division by 8 is needed because interface speed frequently is reported in bits/second, where the performance data is bytes/second.

- **Maximum Value**- If this field contains a value, then each time one of the selected data points goes above this value an event is triggered. This field may contain a number or a Python expression. An expression is required for gauge or calculated values.

3 Click **Save** to confirm the edits.

Performance Data Retention

Cisco UCS Performance Manager stores all performance data (a.k.a., metrics) in HBase using OpenTSDB. The default retention policy saves performance data for 90 days. To change the default, the time to live (TTL) must be adjusted on the OpenTSDB column families in HBase.

Note TTL is defined in seconds.

Once a TTL value is changed, the data retention will adjust on the next major HBase compaction, which by default is once per day.

Changing the Peformance Data Retention Time

To change the peformance data retention time from the default value of 90 days:

1 Log in to the Control Center master host as a user with `sudo` and `docker` privileges.

2 Stop the opentsdb writer service.

```
serviced service stop opentsdb/writer
```

3 Execute the following command to list all the services and their SERVICEID values. Take note of the SERVICEID for the opentsdb reader service. It will be used as an argument in the following step.

```
serviced service list
```

4 Execute the following command where `$id` is the opentsdb reader SERVICEID and `$ttl` is your desired TTL value, in seconds.

```
serviced service shell $id /opt/opentsdb/set-opentsdb-table-ttl.sh
 $ttl
```

5 Start the opentsdb writer service.

```
serviced service start opentsdb/writer
```

Audit Logging

The audit log tracks user actions in syslog or log files. The system maintains logged information in a format optimized for searching and reporting.

Logged information can appear in several locations:

- Log file
- Rotating log files (limited by time or size)
- syslog

By default, the `$ZENHOME/log/audit.log` file stores the latest 10MB of data, with three rolling backups.

Configuring the Audit Logs

Settings in the `$ZENHOME/etc/audit_log.conf` configuration file determine the location and content of logged information output.

The `audit_log.conf` and `audit_log.conf.example` files are created at installation (if they do not exist).

An entry in the audit log indicates that a user attempted an action, but does not always indicate whether that action was successful. For example, a log entry stating that a user added a device simply indicates that the user created a job to add the device; however, the job could still fail when it runs at a later time.

As shown in the following sample, the configuration file contains examples and instructions for each of the output methods.

```
## Audit Log configuration file
## ## Initially this outputs up to 10 megs to ZENHOME/log/audit.log with
 3 backups.
##
## To output to the syslog or somewhere else:
## - Uncomment the desired handlers and formatters, or create your own.
## - Update the "keys" lists under [handlers] and [formatters].
## - Update the "handlers" list under [logger_audit].
## - Restart Zope with "zenwebserver restart".
##
## To change the log severity level:
## - Update "level" under [logger_audit]
##
## This file has all the features of the Python logging file format:
## http://docs.python.org/library/logging.config.html#configuration-file-
format

[loggers]
## DO NOT CHANGE
keys=audit

##
##
## List all output handlers here. (part 1 of 3)
## This should match part 3 below.
##
## Example: keys=syslog,file,rotatingfile,timedrotatingfile,console
##
##
[handlers]
keys=rotatingfile

##
##
## List all string formatters here. (part 2 of 3)
##
## Example: keys=syslog,file,console
##
##
```

```
[formatters]
keys=file

[logger_audit]
## DO NOT CHANGE
qualname=zen.audit
propagate=0

##
##
## This is the severity level of all audit messages.
## (DEBUG, INFO, WARNING, ERROR, CRITICAL)
##
## You can override the level of individual handlers below,
## or keep them as NOTSET to use this default level.
##
##
level=INFO

##
##
## List all output handlers here. (part 3 of 3)
## This should match part 1 above, except "handlers=" not "keys=".
##
## Example: handlers=syslog,file,rotatingfile,timedrotatingfile,console
##
##
handlers=rotatingfile
########################## Output Handlers

## SysLog
##
## See http://docs.python.org/library/
logging.handlers.html#sysloghandler
##
## Here are typical configurations:
##
## Linux: args=('/dev/log', handlers.SysLogHandler.LOG_USER)
## OS/X : args=('/var/run/syslog', handlers.SysLogHandler.LOG_USER)
## UDP : args=(('localhost', handlers.SYSLOG_UDP_PORT),
##                                handlers.SysLogHandler.LOG_USER)
##
##
##[handler_syslog]
##class=handlers.SysLogHandler
##level=NOTSET
##formatter=syslog
##args=()

## File
##
## See http://docs.python.org/library/logging.handlers.html#filehandler
##
## To store in ZENHOME/log:
 class=Products.ZenUtils.configlog.ZenFileHandler
## To store elsewhere: class=FileHandler
##
## Format and example:
## args=(filename, mode, encoding, delay)
## args=('audit.log', 'a', None, True)
##
```

```
##
##[handler_file]
##class=Products.ZenUtils.configlog.ZenFileHandler
##level=NOTSET
##formatter=file
##args=('audit.log', 'a', None, True)


## RotatingFile
##
## See http://docs.python.org/library/
logging.handlers.html#rotatingfilehandler
##
## To store in ZENHOME/log:
 class=Products.ZenUtils.configlog.ZenRotatingFileHandler
## To store elsewhere: class=handlers.RotatingFileHandler
##
## Format:
## args=(filename, mode, maxBytes, backupCount, encoding, delay)
##
## Example of one 10-meg file in ZENHOME/log/
## args=('audit.log', 'a', 10000000, 0, None, True)
##
## Example of ten 1-meg files in ZENHOME/log/audit/. The path must
 already exist.
## args=('audit/audit.log', 'a', 1000000, 10, None, True)
##
##
[handler_rotatingfile]
class=Products.ZenUtils.configlog.ZenRotatingFileHandler
level=NOTSET
formatter=file
args=('audit.log', 'a', 10485760, 3, None, True)


## TimedRotatingFile
##
## See http://docs.python.org/library/
logging.handlers.html#timedrotatingfilehandler
##
## To store in ZENHOME/log:
 class=Products.ZenUtils.configlog.ZenTimedRotatingFileHandler
## To store elsewhere: class=handlers.TimedRotatingFileHandler
##
## Format and example:
## args=(filename, when, interval, backupCount, encoding, delay, utc)
##
## Example of weekly log files for the past year in ZENHOME/log/audit/
## args=('audit/weekly.log', 'midnight', 7, 52, None, True, False)
##
##
##[handler_rotatingfile]
##class=Products.ZenUtils.configlog.ZenTimedRotatingFileHandler
##level=NOTSET
##formatter=file
##args=('audit/weekly.log', 'midnight', 7, 52, None, True, False)


## Console
##
## See http://docs.python.org/library/
logging.handlers.html#streamhandler
```

```
##
##
##[handler_console]
##class=StreamHandler
##level=NOTSET
##formatter=console
##args=(sys.stdout,)


######################### String Formatters
##
## These must be uncommented if used by a handler above.
##
## See the very bottom of http://docs.python.org/library/
logging.config.html
##
##

##[formatter_syslog]
##format=zenoss[%(process)d]: %(message)s


[formatter_file]
format=%(asctime)s %(message)s
datefmt=%Y-%m-%d %H:%M:%S


##[formatter_console]
##format=Audit: %(asctime)s %(message)s
##datefmt=%H:%M:%S
```

After editing the `audit_log.conf` file, restart Zope with the command:

```
zenwebserver restart
```

Examples

While enabled, user actions are tracked as specified by the configuration file.

Example 1

```
Sep 12 12:55:10 zenoss[8432] user=hsolo action=SetDeviceClass
  kind=Device device=/Devices/Server/Linux/devices/emailsrv05
  deviceclass=/Devices/Server/SSH/Linux
```

In this example, user hsolo moved device "emailsrv05" from device class /Server/Linux to /Server/SSH/Linux.

Example 2

```
Sep 12 12:57:19 zenoss[8432] user=lskywalker action=Edit
  kind=ThresholdClass maxval=100 minval=0 old_minval=-100
  thresholdclass="/Devices/Server/Linux/rrdTemplates/Device/thresholds/
CPU pct"
```

In this example, user lskywalker edited values of threshold "CPU pct" by adding a max value of 100 and changing the min from -100 to 0.

Searching File Content

You can use central logging tools or grep to parse the configuration file content. Using Splunk, for example, searching for "device=*/localhost" finds any action on machines named localhost in any device class. Searching for "action=Add kind=User | table user username" creates a table that lists new users and which user added them.

Utility

The `zensendaudit` utility allows you to log custom messages. For example:

```
zensendaudit Hello world.
```

generates the output:

```
Message sent: Hello world.
```

Further, it logs this message to the configured syslog or files:

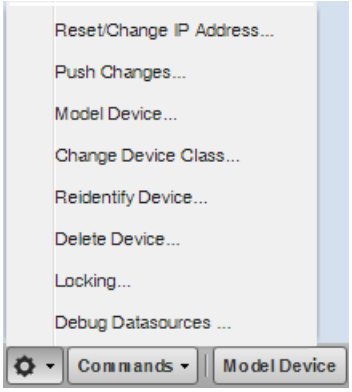
```
zenoss[9350]: user=admin type=ManualEntry comment="Hello world."
```

Debug Logging

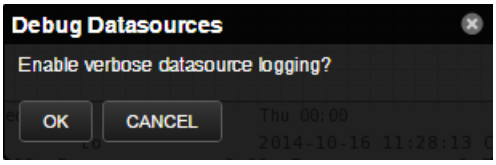
With debug logging enabled for all Calculated Performance datasources, a UCS domain produces alot of logging. However, this is not satisfactory when debugging a particular datasource. In order to effectively diagnose a graphs that is displaying NaN values, you need to debug each datasource involved in creating that graph.

To turn on debug logging at the device level:

1. From the Navigation menu, select **Infrastructure**. The Devices page appears.
2. Select the Device you want to turn on debug logging for. The Overview page for that device appears.
3. Click the **Action** menu, and select **Debug Datasources**.



4. In the Debug Datasources dialog, click **OK**.



Support Bundles

If you contact Cisco Support about an issue with your Cisco UCS Performance Manager system, you may be asked to send a support bundle and/or serviced and docker logs to help the technicians find a solution to your issue. These support bundles contain logs and system information that is valuable to the Support team.

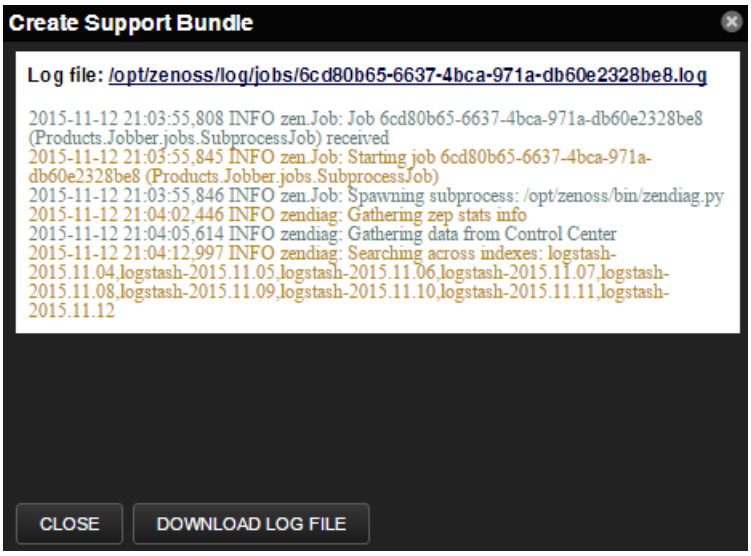
Creating Support Bundles

You may be asked to send a support bundle to Cisco Support to help troubleshoot an issue with your system. This support bundle contains the logs and system status that the Support team needs to solve your issue.

To create a support bundle:

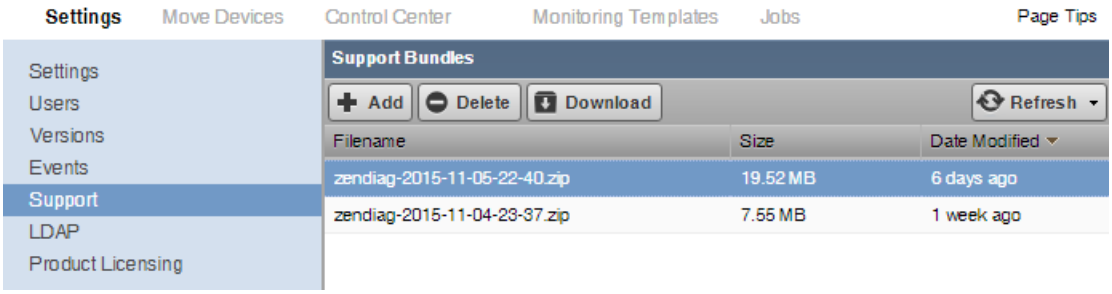
1. As an administator, navigate to **Advanced > Support**. The Support Bundles window appears.
2. Click **Add**. A window appears indicating that the support bundle will continue to be gathered even after closing the window.
3. Click **OK**. The Create Support Bundle window displays. Click **Close**. The support bundle will continue to be gathered. You can monitor the job log for progress. You can continue working with the system during this time.

Figure 69: Create Support Bundle window



4. When the completed support bundle is displayed in the Support Bundles window, click on its row and click **Download** to send the support bundle `.zip` file to your browser's downloads folder.

Figure 70: Support Bundles window



Deleting Support Bundles

From time-to-time you may want to clean up your system by deleting old support bundles that are no longer needed for troubleshooting purposes.

To delete support bundles from your system:

1. As an administator, navigate to **Advanced > Support**. The Support Bundles window appears.
2. Click the row of the support bundle(s) you want to delete. Be sure that you have selected the bundle(s) you want deleted since there is no confirmation window once you click **Delete**.
3. If you are sure of your selections, click **Delete**. The selected bundle(s) will be removed from the system.

Gathering serviced and docker logs

You may need to gather serviced and docker logs separately to help troubleshoot an issue, since these logs cannot be collected by the support bundle process.

To get serviced logs from the system:

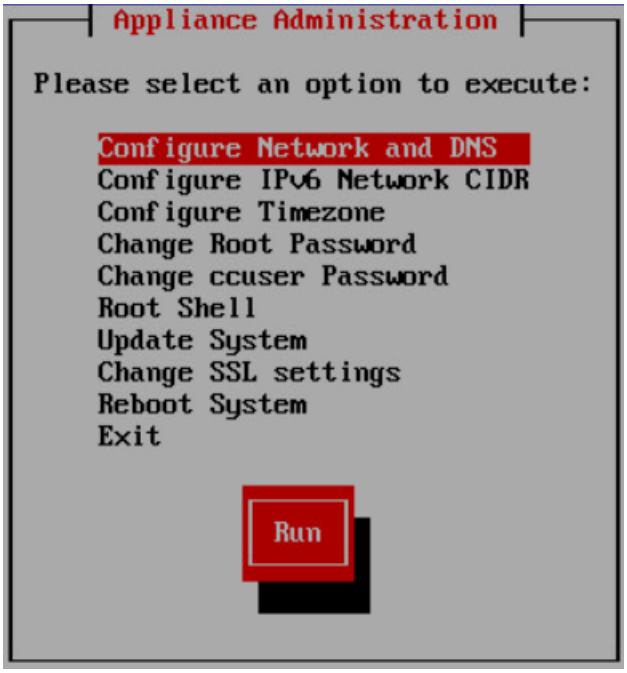
1. Gain access to the console interface of the Cisco UCS Performance Manager virtual machine through your hypervisor.

   Figure 71: Login prompt

   ```
   Welcome to UCS Performance Manager

   To access the Control Center UI, please browse to:

      https://ucspm
      (default username/password is ccuser/ucspm)

   Ensure that ucspm is resolvable to 10.87.209.179, either through your
   DNS system or through a HOSTS entry on the browser client. For more
   information refer to the installation notes.

   You can log in to this console to perform administrative tasks such
   as setting up networking and safely rebooting this system. The
   default root password is 'ucspm' and should be changed for
   security reasons.

   Linux Kernel 3.10.0-229.14.1.el7.x86_64 on an x86_64
   ucspm login:
   ```

2. In the console window, log in as the `root` user.

Figure 72: Application Administration menu



3 Start a command-line session as `root`.

   a In the **Application Administration** menu, use the down-arrow key to select **Root Shell**.

   b Press the **Tab** key to select **Run**, and then press the **Return** key.

   The menu is replaced by a command prompt similar to the following example:

```
[root@ucspm-master ~]#
```

4 Execute the following command to create the `serviced.log` file in the `/tmp` directory.

```
journalctl -u serviced -o cat > /tmp/serviced.log
```

5 Execute the following command to create the `docker.log` file in the `/tmp` directory.

```
journalctl -u docker -o cat > /tmp/docker.log
```

Setting Portlet Permissions

By setting permissions, you determine which users can view and interact with portlets. Permissions settings restrict which Zope Access Control List (ACL) can access each portlet.

Before you can successfully set portlet permissions, you must assign the user a specific Cisco UCS Performance Manager role. (You assign roles from the user edit page, from **Advanced > Settings**.) Each user role is mapped to one or more Zope ACL permissions, which allow you to restrict the portlets a permission level can see.

A user's specific portlet permissions are defined in part by Zope ACL permissions, and in part by the role to which he is assigned.

User Role to ACL Mapping

The following table shows how user roles map to ACLs.

User Roles	ACLPermission
ZenUser, ZenOperator	ZenCommon, View
ZenManager, Manager	ZenCommon, View, Manage DMD
No Role, Administered Objs	ZenCommon

Backup and Restore

In some situations, you might want to back up configuration information and data from a Cisco UCS Performance Manager instance, and then later restore that instance. You might back up on a regular schedule to provide a historical archive; or infrequently, such as when you want to move data from one instance to another or perhaps duplicate an instance for testing or failover purposes.

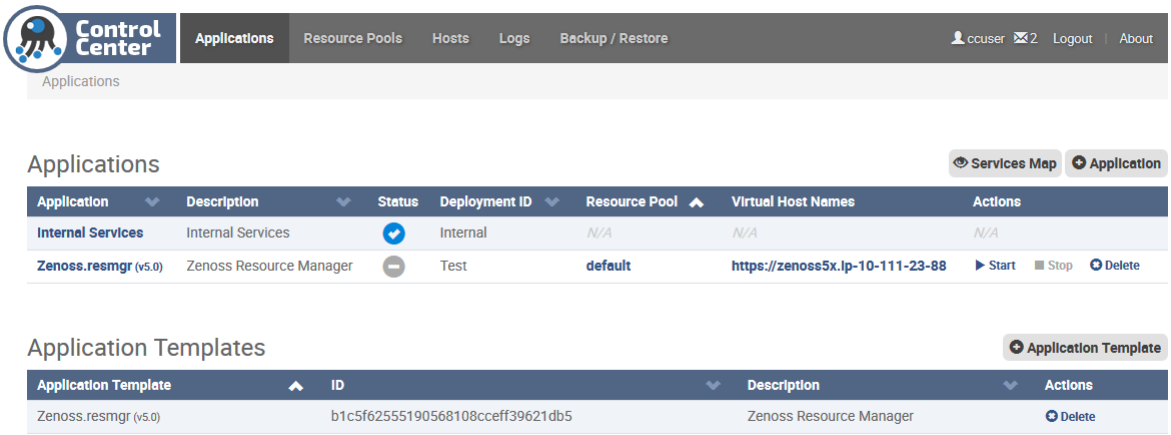
The backup process saves the state of all services and data to a `.tgz` file which can be restored on that cluster or be duplicated on a similar cluster.

Note You must perform your backups on the Cisco UCS Performance Manager instance using the documented procedures below. Do not use the backup and restore functionality provided by your vSphere environment as a substitute to these procedures.

Backing Up Cisco UCS Performance Manager

To take a backup of Cisco UCS Performance Manager:

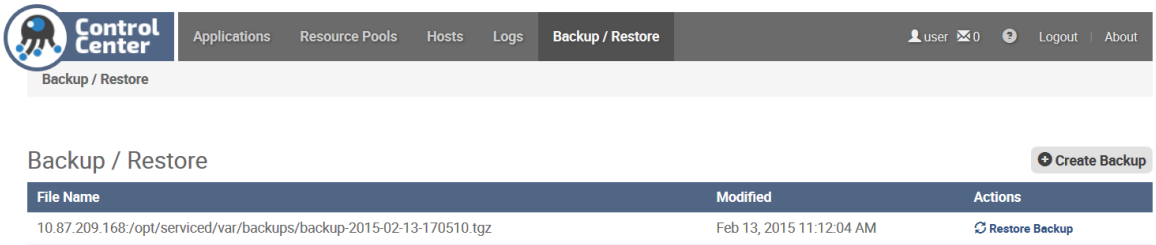
1 Log in to the Control Center browser interface.



2 Click the **Backup / Restore** tab. The Backup / Restore page appears.

3 Click **Create Backup**. You will be asked to confirm your selection by clicking **Create Backup** again.

4 When the backup is complete, you will see the path of the `.tgz` file displayed.



Scheduling Backups

You can use `cron` to schedule backups of Cisco UCS Performance Manager at a defined interval. This procedure is optional. You can always take an on-demand backup using the Control Center interface.

To schedule a backup using `cron`:

1. Log in to the Control Center master host as a user with `sudo` privileges.
2. Schedule `cron` to perform a backup:

```
/etc/crontab
```

3. Add a line to `crontab` to define the time and command to run to perform the backup. For example:

```
0 2 1 * * root serviced backup /opt/serviced/var/backups
```

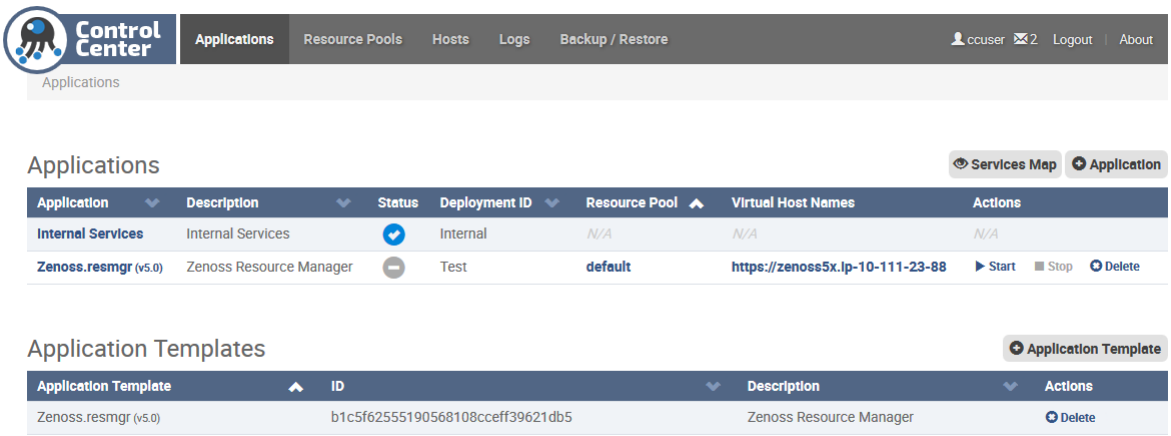
This example will run the `serviced backup` command as the `root` user on the first day of each month at 2:00a.m. and will put the backup file in the `/opt/serviced/var/backups` directory. Customize this example for your particular backup needs.

Note The format for `crontab` entries is: `minute hour day_of_month month day_of_week user command`

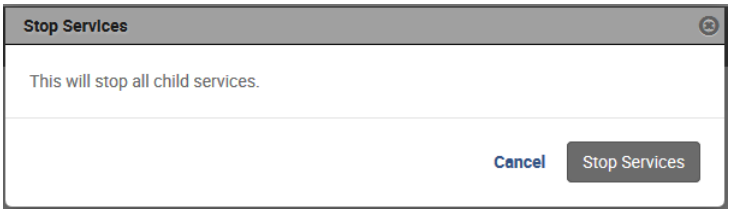
Restoring Cisco UCS Performance Manager from a Backup

You can restore your Cisco UCS Performance Manager instance from any given backup `.tgz` file. You could also duplicate your instance on a similar cluster for testing or failover purposes by restoring a backup `.tgz` file to a new similarly configured cluster.

1. Log in to the Control Center browser interface.



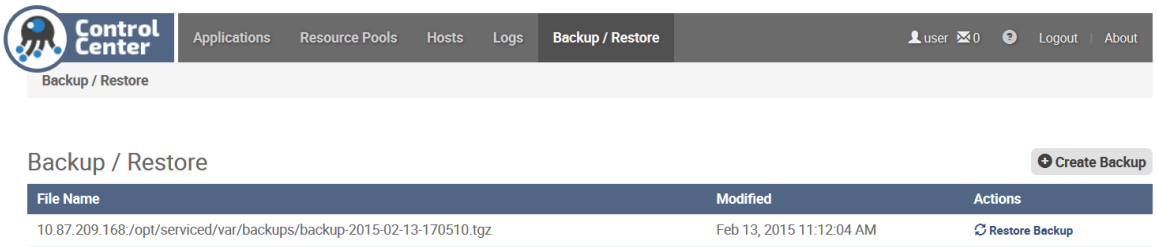
2. In the **Applications** table, identify the name of the Cisco UCS Performance Manager instance to modify.
3. Stop the instance, and verify its subservices are stopped.
   a. In the **Actions** column of the **Applications** table, click **Stop**.



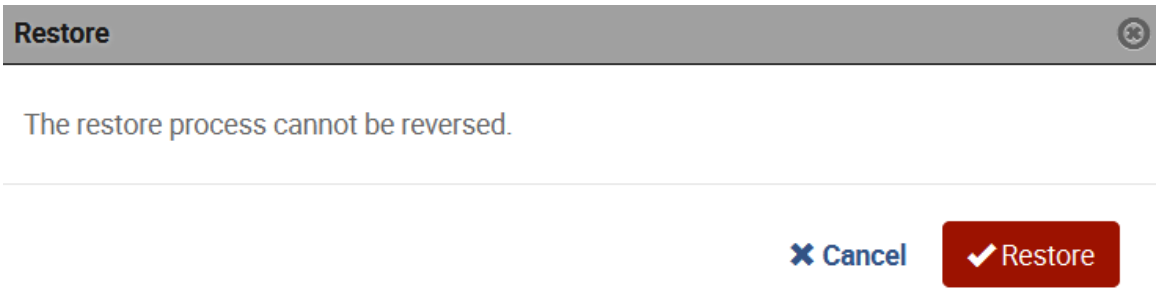
b In the **Stop Services** dialog, click **Stop Services**.

c In the **Applications** column of the **Applications** table, click the name of the stopped instance, and then scroll down to the **Services** table to verify everything is stopped.

4 Click the **Backup / Restore** tab. The Backup / Restore page appears listing your backup files.



5 Click **Restore Backup** next to the backup file you want to use to restore your Cisco UCS Performance Manager application. You will be asked to confirm your selection by clicking **Restore**.



6 When the restore is finished, click the **Applications** tab, then click **Start** next to the Cisco UCS Performance Manager instance you just restored.

Working with the Job Manager

The Job Manager runs background tasks, such as discovering a network or adding a device. When you ask the system to perform one of these tasks, it adds a job to the queue. Jobs are run by the `zenjobs` daemon.

Not all actions are performed in the Job Manager. Some jobs are run automatically in the foreground. Others, such as moving devices, depend on user interface configuration settings.

When running jobs in the foreground, do not navigate away from the current page until the action completes.

Viewing the Job Manager

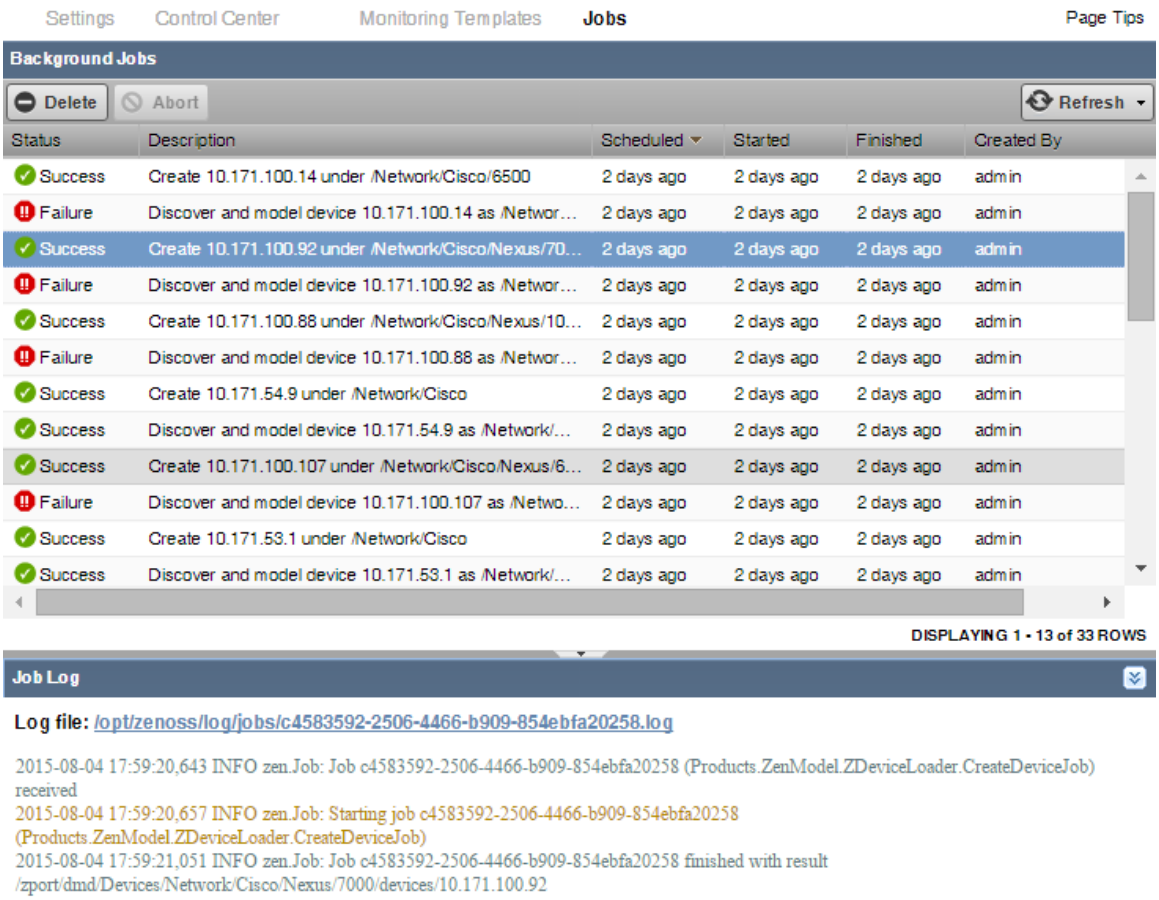
To access the Job Manager:

1 From the Navigation menu, select Advanced.

The Settings page appears.

2 From the menu, select **Jobs**.

Figure 73: Job Manager



The jobs list appears and shows information about all jobs currently in the system.

- **Status** - Shows the current job status. Status options are Pending (waiting for `zenjobs` to begin running), Running, Succeeded, and Failed.
- **Description** - Provides a description of the job.
- **Scheduled** - Shows when the job was scheduled to begin.
- **Started / Finished** - Provide information about the time period in which the job ran.
- **Created By** - User that created the job.

The lower section of the page displays the job log for the job selected in the list. You can view job info here, or by viewing the log file.

Stopping and Deleting Jobs

To stop a job, select it in the list, and then click **Abort**. The `zenjobs` daemon will not run the job.

To remove a job from the system, select it and then click **Delete**.

Host Name Changes

If you change the host name of your Cisco UCS Performance Manager server, then you must clear and rebuild queues before the `zenhub` and `zenjobs` daemons will restart.

To work around this issue, you can issue the following commands (although any data queued at restart time will be lost):

```
export VHOST="/zenoss"
export USER="zenoss"
export PASS="zenoss"
rabbitmqctl stop_app
rabbitmqctl reset
rabbitmqctl start_app
rabbitmqctl add_vhost "$VHOST"
rabbitmqctl add_user "$USER" "$PASS"
rabbitmqctl set_permissions -p "$VHOST" "$USER" '.*' '.*' '.*'
```

Glossary of terms

aggregation pools

A logical bundling of multiple physical network interfaces, commonly known as a port channel. For example, the Per Chassis Ethernet Pools includes all links from all chassis to all fabric interconnects which is used for chassis bandwidth balance comparison. For more examples, see the Aggregation Pools component section of CiscoUCS devices.

bandwidth utilization

The total amount of bandwidth being used by an aggregation pool, a port, a fabric interconnect, a FEX, etc.

component

Object contained by a device. Components include interfaces, OS processes, file systems, CPUs, and hard drives.

data point

Data returned from a data source. In many cases, there is only one data point for a data source (such as in SNMP); but there may also be many data points for a data source (such as when a command results in the output of several variables).

data source

Method used to collect monitoring information. Example data sources include SNMP OIDs, SSH commands, and perfmon paths.

device

Primary monitoring object in the system. Generally, a device is the combination of hardware and an operating system.

device class

Special type of organizer used to manage how the system models and monitors devices through the use of monitoring templates.

discovery

Process by which Cisco UCS Performance Manager gathers detailed information about devices in the infrastructure. Results of discovery are used to populate the model.

event

Manifestation of important occurrence within the system. Events are generated internally (such as when a threshold is exceeded) or externally (such as through a syslog message or SNMP trap).

event class

Categorization system used to organize event rules.

event rules

Controls how events are manipulated as they enter the system (for example, changing the severity of an event).

graph

Displays one or more data points, thresholds, or both.

headroom

The unused bandwidth in an aggregation pool, a port, a fabric interconnect (FI), a FEX, etc. For example, if an aggregation pool including 4 ports between a chassis and the FIs has 40 GB of capacity and if the bandwidth use of that pool is 25 GB, then the headroom is 15 GB.

integrated infrastructure

A bundle of compute, storage, networking, and virtualization components. Most integrated infrastructures are bought as one from a vendor:

- NetApp FlexPod
- VCE Vblock
- EMC VSPEX

All of these have UCS as the common compute element, Nexus as networking components, and VMware as virtualization.

managed resource

Servers, networks, virtual machines, and other devices in the IT environment.

model

Representation of the IT infrastructure. The model tells the system "what is out there" and how to monitor it.

monitoring template

Description of what to monitor on a device or device component. Monitoring templates comprise four main elements: data sources, data points, thresholds, and graphs.

notification

Sends email or pages to system users or groups when certain events occur.

organizer

Hierarchical system used to describe groups within the application. Cisco UCS Performance Manager also includes special organizers, which are classes that control system configuration.

out of balance

Indicates that the bandwidth use is quite different among the ports in an aggregation pool. This can often be corrected by reconfiguration, for example, by moving a service profile from one chassis to another.

resource component

Interfaces, services and processes, and installed software in the IT environment.

service profile

A service profile is a software definition of a server and its LAN and SAN network connectivity, in other words, a service profile defines a single server and its storage and networking characteristics.

threshold

Defines a value beyond which a data point should not go. When a threshold is reached, the system generates an event. Typically, threshold events use the `/Capacity` event class.

trigger

Determines how and when notifications are sent. Specifies a rule comprising a series of one or more conditions.

ID: 2013.15.338