Cisco UCS Performance Manager Administration Guide

First Published: October 2014

Release 1.0.0

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

Contents

1 Using Cisco UCS Performance Manager

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.

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.

Dashboard

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

- Dashboard view
- Topology view

Dashboard View

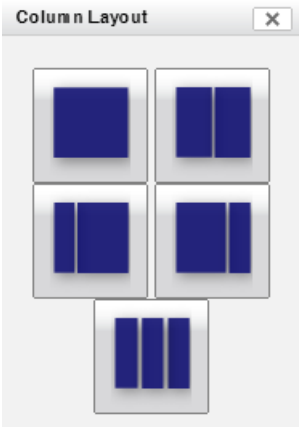
The Dashboard view can be customized to display a variety of information including the following portlets. The default portlets are indicated as such:

- Blade Server Capacity
- Chassis Capacity (Default)
- Device Issues
- Domain Overview (Default)
- Daemon Processes Down
- Integrated Infrastructure Events
- Out Of Balance Events
- Production States
- Service Profiles (Default)
- Site Window
- Top Level Organizers

- UCS Inventory (Default)
- Messages
- Watch List
- Welcome to UCS Peformance Manager (Default)

To configure the layout of the Dashboard view:

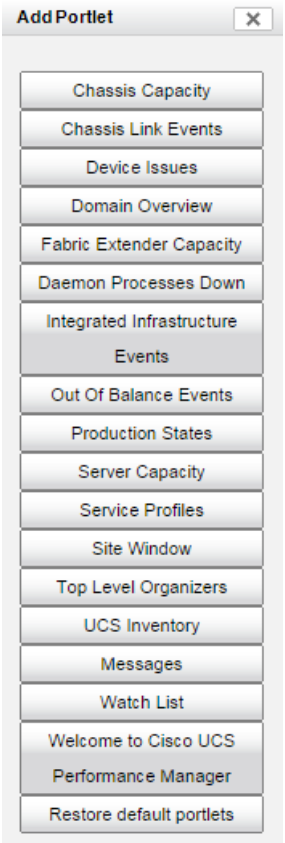
1 Click **Configure layout...**. The Column Layout dialog appears.



2 Click the desired column layout configuration. The two equal column layout is the default value.

To add portlets to the Dashboard view:

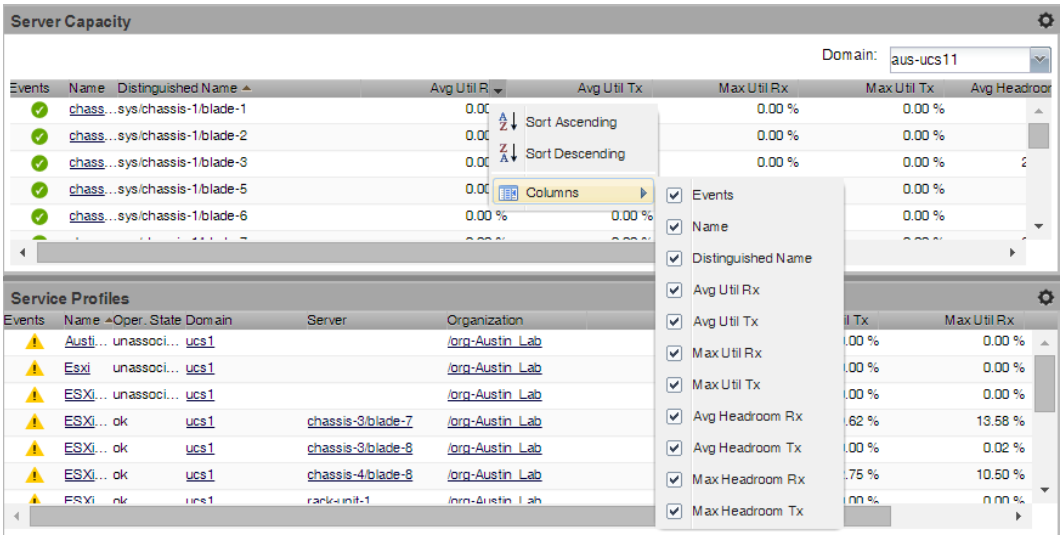
1 Click **Add portlet...**. The Add Portlet dialog appears.



2 Click the name of the portlet you want to add. If you want to add another portlet, repeat this procedure.
3 (optional) Move the portlet within the Dashboard view by clicking and dragging it to the desired location.

To configure the display within a portlet:

1 Click the Settings icon in the upper-right corner of the portlet.
2 Edit the settings as appropriate. Each portlet has a different set of settings based on the displayed information.
3 Click **Save Settings**.
4 Sort based on a column by hovering over the column header and clicking the arrow to display the sort and display options.
5 Add or remove columns by hovering over the **Columns** entry and clearing the check boxes of column to hide.



To delete a portlet from the Dashboard view:

1 Click the Settings icon in the upper-right corner of the portlet.
2 Click the **Remove Portlet** link.

Topology View

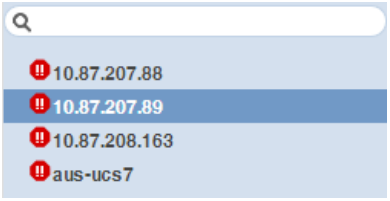
The main content of the Topology view of the dashboard contains portlets that provide information about the system and your infrastructure. These portlets display:

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

Figure 1: All Domains Portlet

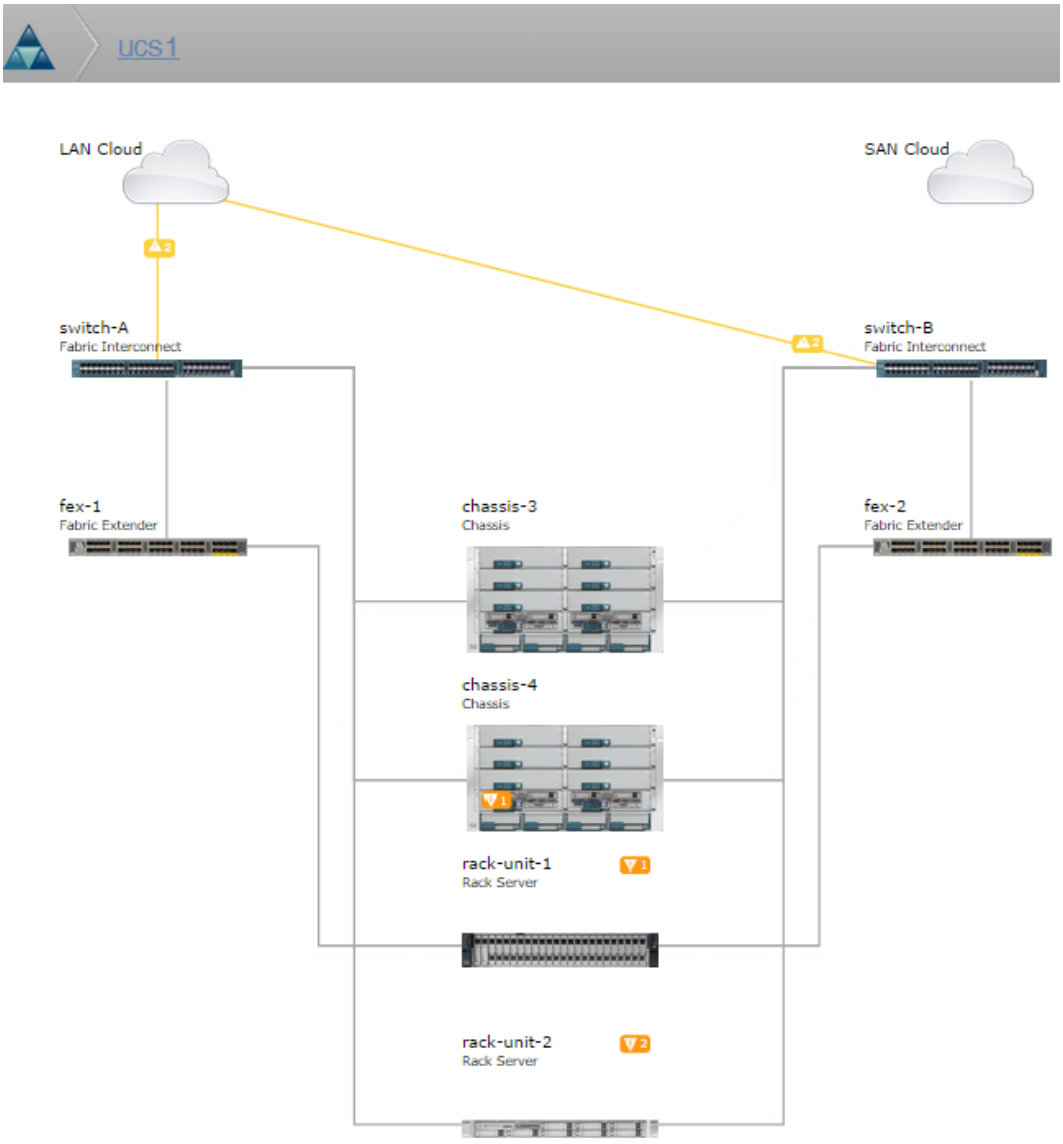
- **Devices** - Displays a list of devices, associated with color-coded severity levels. Click a device name to view details.

Figure 2: Devices Portlet



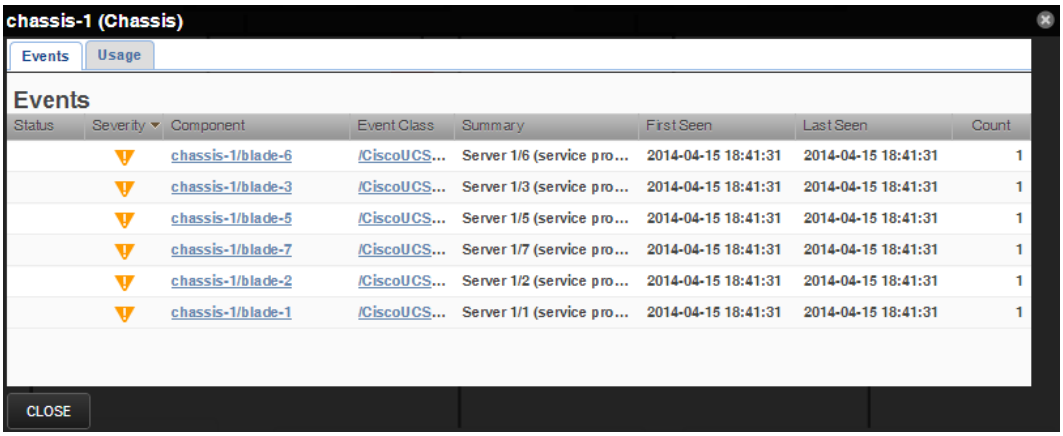
- **Overall Ethernet Bandwidth Utilization** - Indication of the total bandwidth utilization of all Cisco UCS Performance Manager domains. Shown as a percent.
- **Connected Ethernet Ports Bandwidth Utilization** - Indication of the total connected ports bandwidth utilization. Shown as a percent.
- **UCS 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 click on the lines between modules to show the network links. In the figure below, clicking on the line between switch-A and the LAN Cloud will display the event.

Figure 3: Device Topology



Click an event alert warning to show the Events detail page. You can also see today's usage information and links to the blade servers by clicking the Usage tab.

Figure 4: Events Detail Page



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.

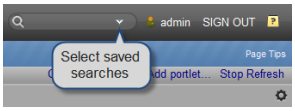
Navigation

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 5: User Information Area



The User information area offers information and selections:

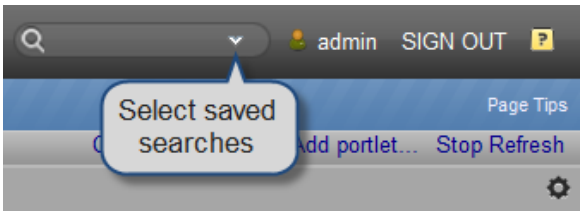
- **Login ID**- The ID of the user currently logged in appears at the far left of this area. Click the ID to edit user settings, such as authentication information, roles, and groups. (You also can access user settings from the **Advanced > Settings > Users** page.)
- **Sign Out**- Click to log out of 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.

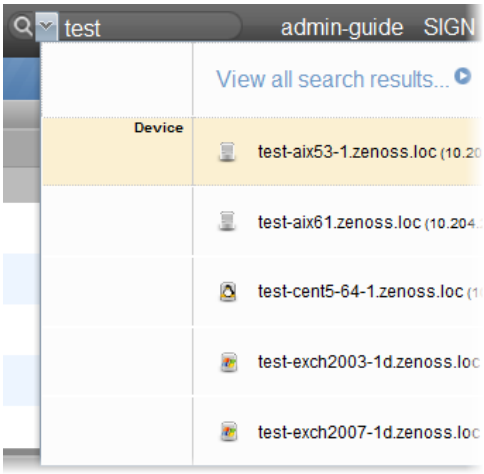
In the Cisco UCS Performance Manager interface, the search feature is located adjacent to the user information area.

Figure 6: Search Field



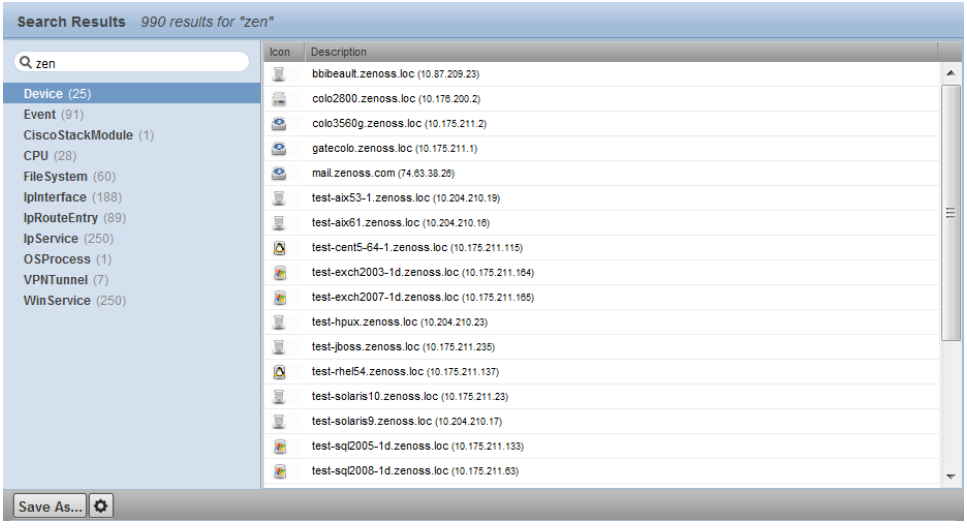
Enter part or all of a name in the search box at the top right of the interface. The system displays matches, categorized by type.

Figure 7: Search Results



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

Figure 8: 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:

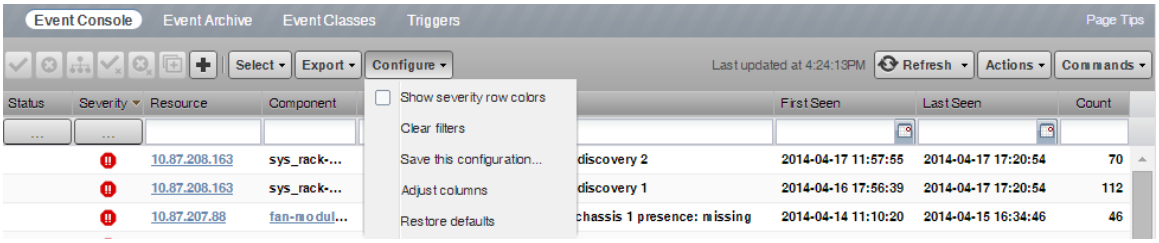
- Action menu located at the bottom of the Search Results page.
- Search box located at the top of the interface. Click the arrow, and then select **Manage Saved Searches**.

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 9: Event Console



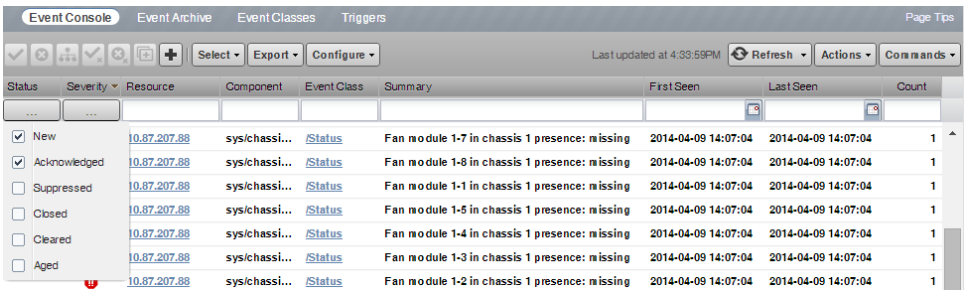
Sorting and Filtering Events

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 contained in the values in that column. You can also use AND, OR, or !! expressions to further target your filters. For example, typing `!!status` in the Event Class filter will return all the non-status class events.

Figure 10: 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, select **Configure > Actionable**. 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 14.

Saving a Custom View

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

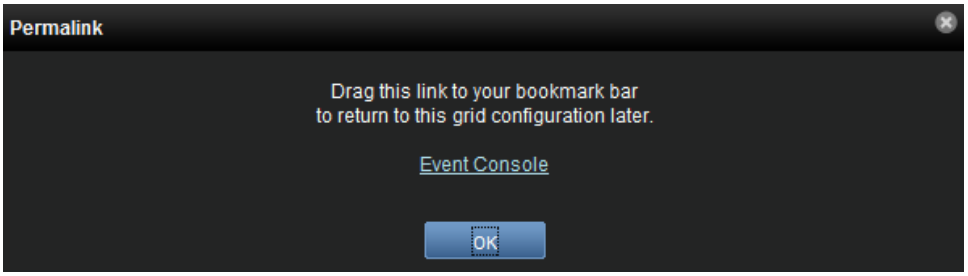
1 Select **Configure > Save this configuration**.

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 11: Saving a Custom View (Bookmark)



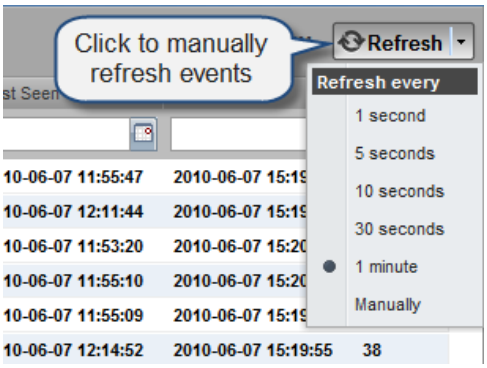
Note You may want to re-title the bookmark, particularly if you choose to save more than one event console view.

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 12: Automatic Refresh Selections



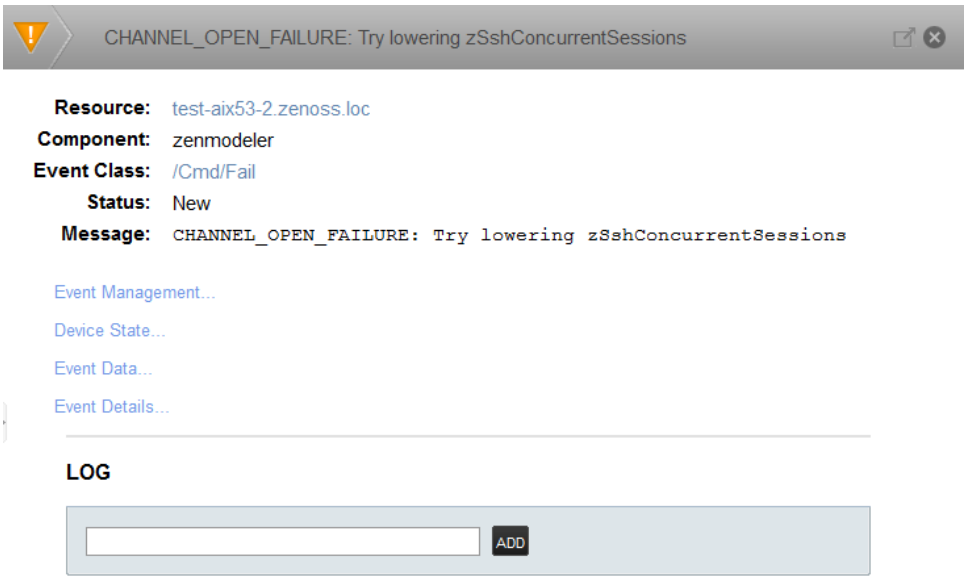
Viewing Event Details

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 13: 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.

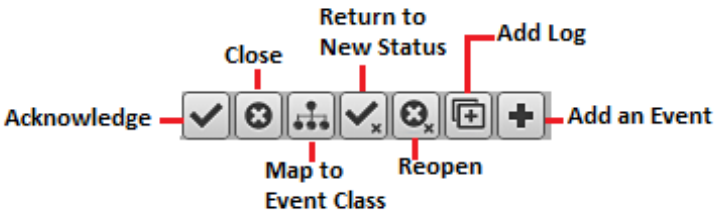
Managing Events

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 14: Event Management Options



Running a Command

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

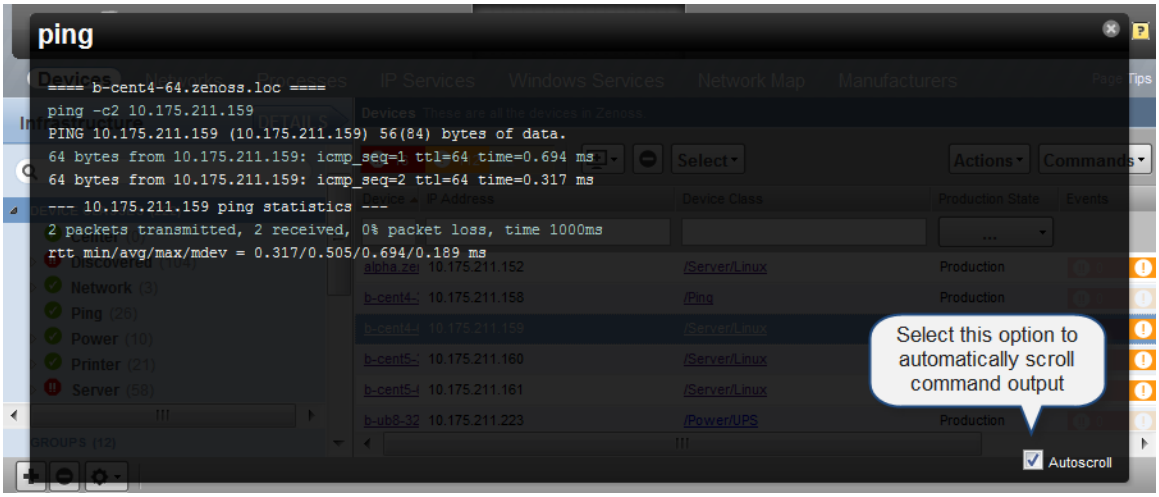
The system includes several built-in commands, such as `ping` and `traceroute`.

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 15: 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.

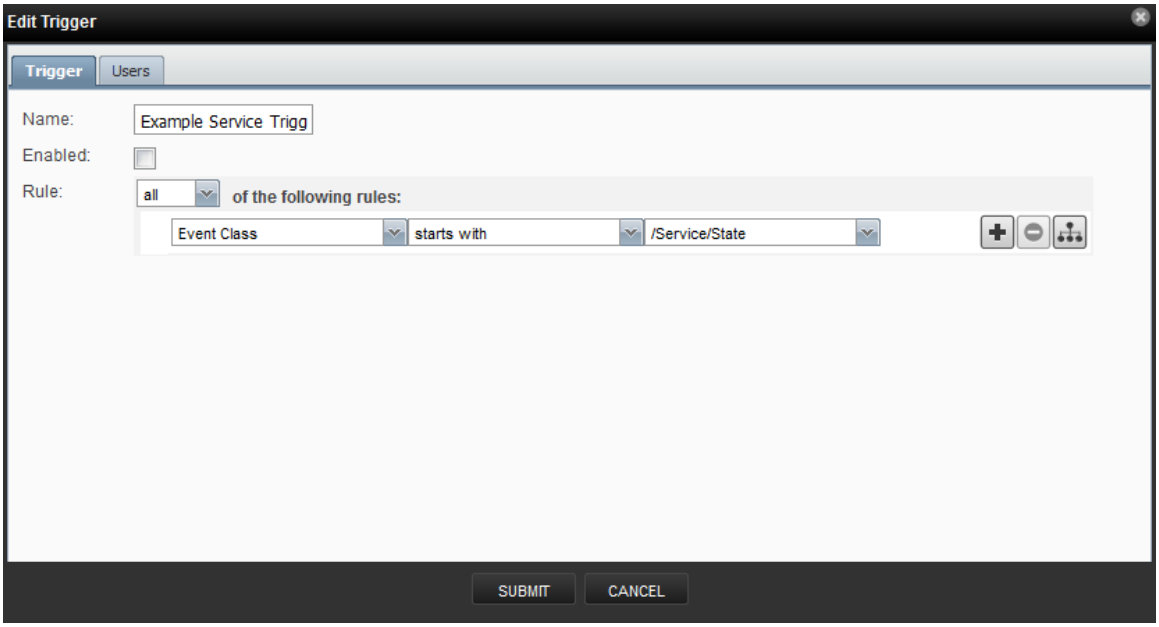
The Add Trigger dialog appears.

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 16: 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.

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:

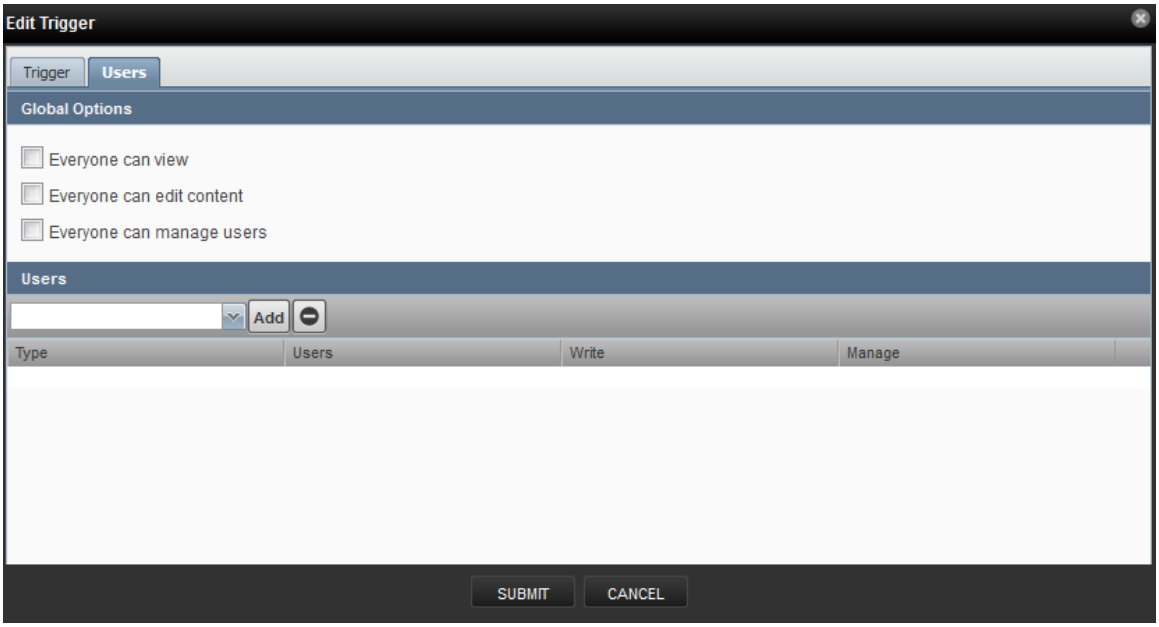
- admin, Manager, and ZenManager roles
- Trigger owner

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 17: 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

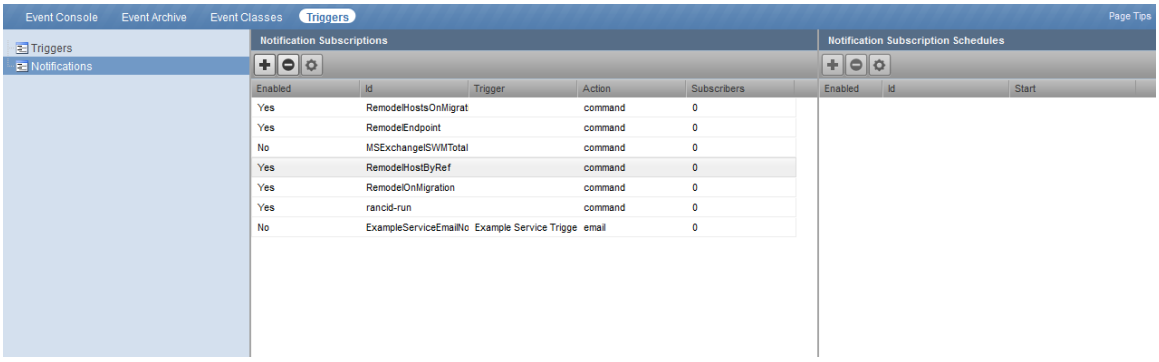
Creating or Editing a Notification

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 18: 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.

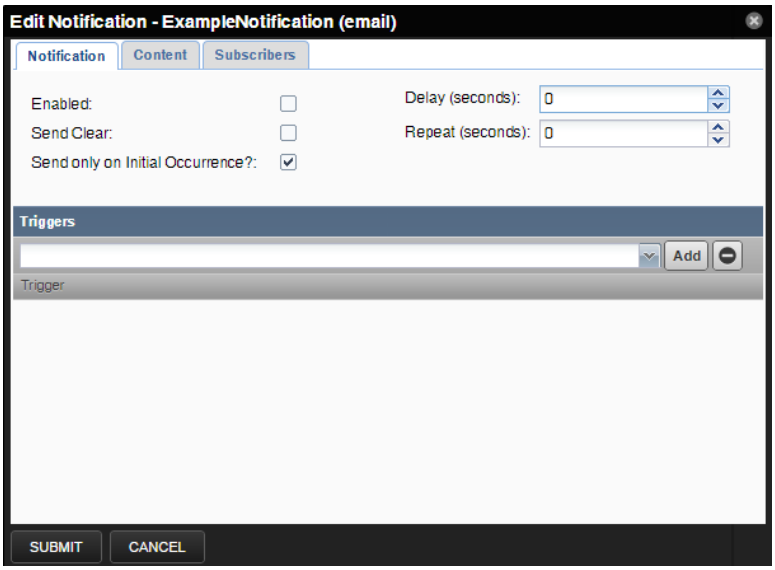
- **Syslog** - Sends a message to the syslog.
- **SNMP Trap** - Sends an SNMP trap when an event matches a trigger rule.

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 19: 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

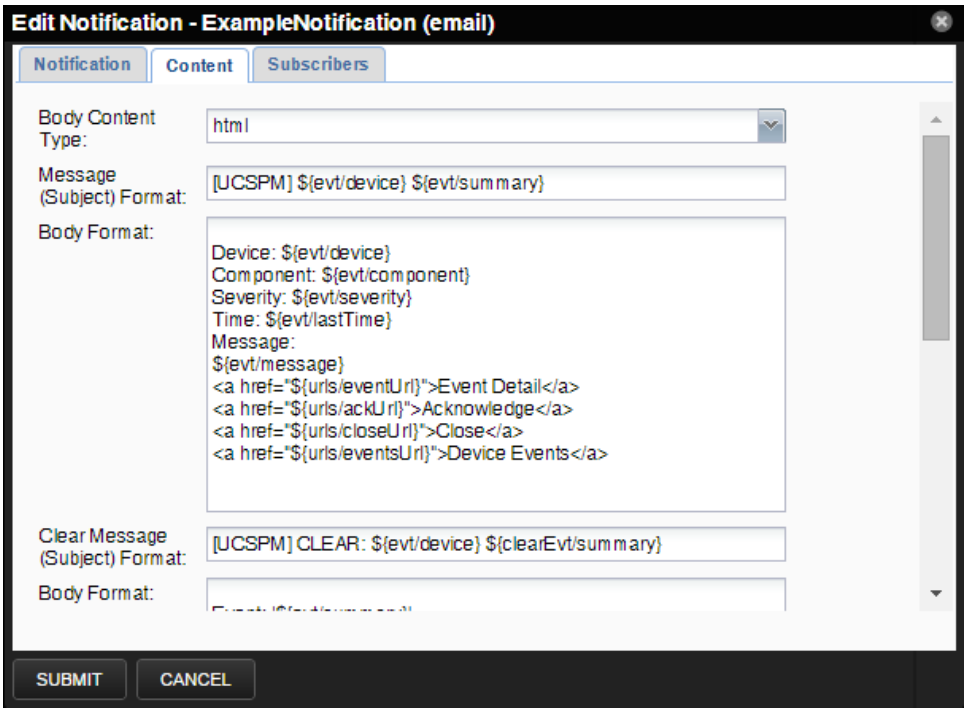
To define notification content, click the **Content** tab of the notification.

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 setings** - Used to define SMTP port, username, and password

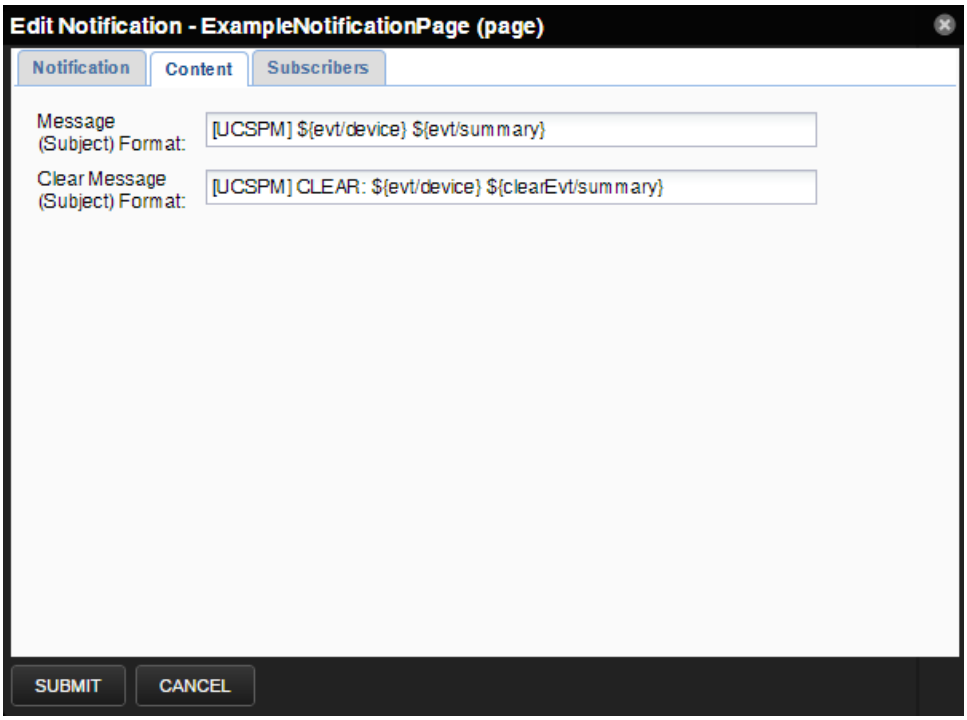
Figure 20: Define Notification Content (Email)



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 21: 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/
  - DevicePriority
  - agent
  - clearid
  - component
  - count
  - created
  - dedupid
  - device
  - eventClass
  - eventClassKey
  - eventGroup
  - eventKey
  - eventState
  - evid

- facility
- firstTime
- ipAddress
- lastTime
- manager
- message
- ntevid
- ownerid
- priority
- prodState
- severity
- stateChange
- status
- summary

Note The `message` and `summary` names are, by default, wrapped in double quotes in event commands.

- eventSummary/ and clearEventSummary/
  - uuid
  - occurence
  - status
  - first_seen_time
  - status_change_time
  - last_seen_time
  - count
  - current_user_uuid
  - current_user_name
  - cleared_by_event_uuid
  - notes
  - audit_log
  - update_time
  - created_time
  - fingerprint
  - event_class
  - event_class_key
  - event_class_mapping_uuid
  - actor
  - summary
  - message
  - severity
  - event_key
  - event_group
  - agent
  - syslog_priority
  - syslog_facility
  - nt_event_code
  - monitor
  - tags
- urls/

- ackUrl
- closeUrl
- reopenUrl
- eventUrl
- eventsUrl

ZenPacks also can define additional notification actions, and can extend the context available to notifications to add additional objects or attributes.

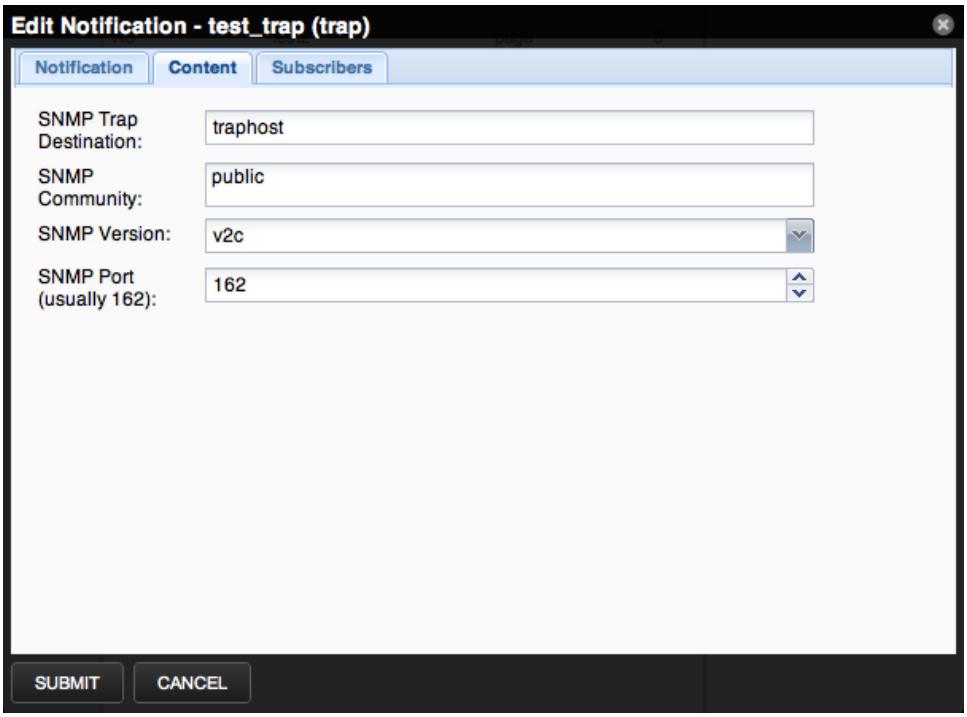
Defining the SNMP Trap Host

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 v1.
- **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 22: Edit Notification Content (SNMP Trap)



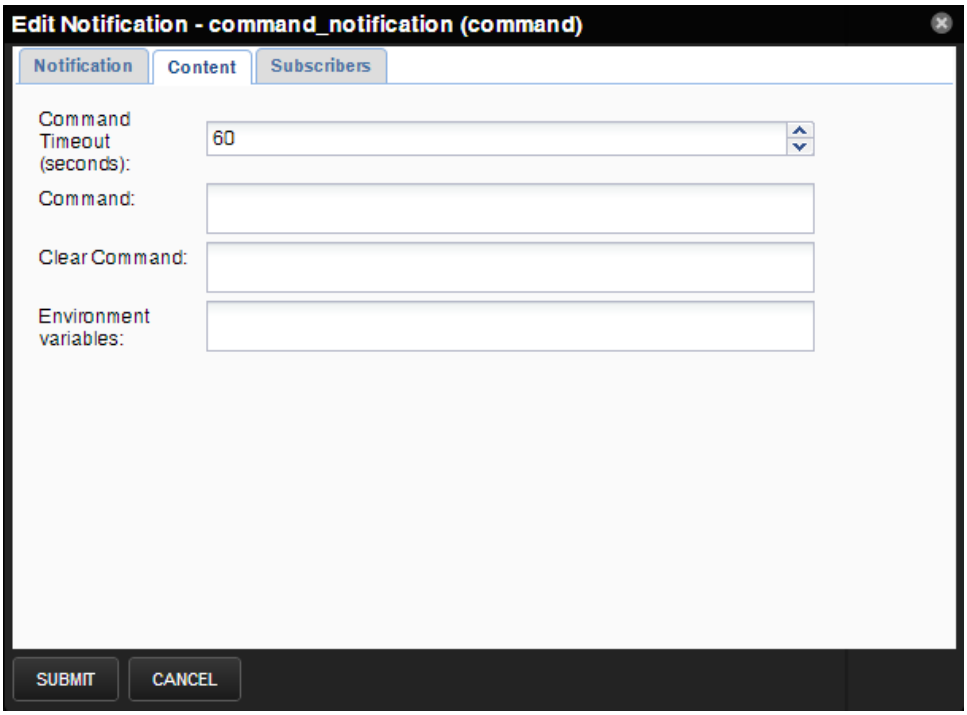
Defining Commands to Run

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 23: Edit Notification Content (Command)



Setting 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.

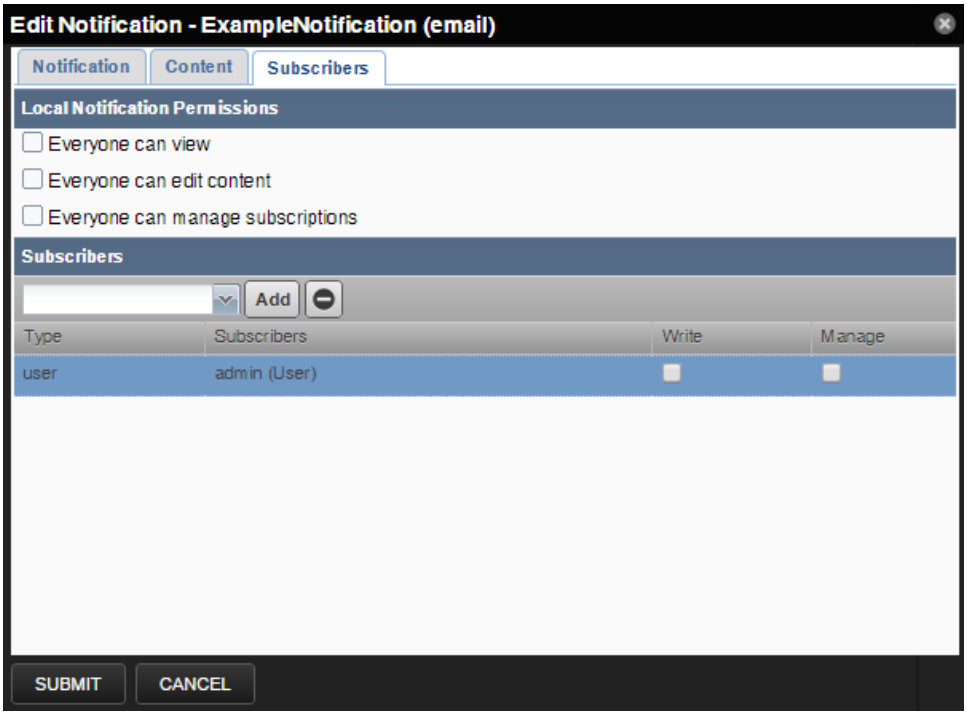
Global options are:

- **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 24: 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.

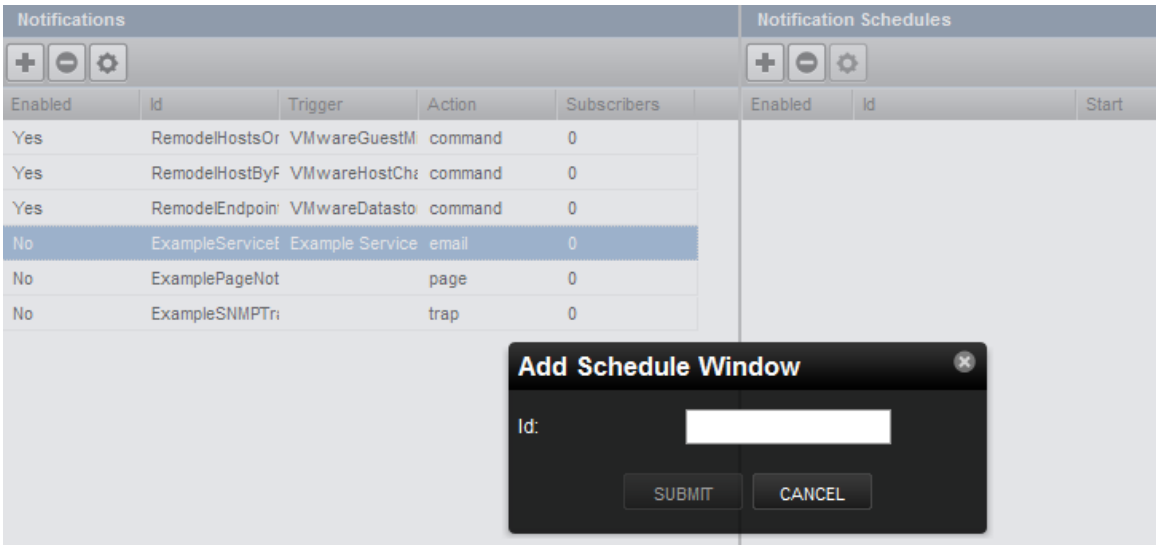
Setting Up Notification Schedules

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 25: Add Notification Schedule



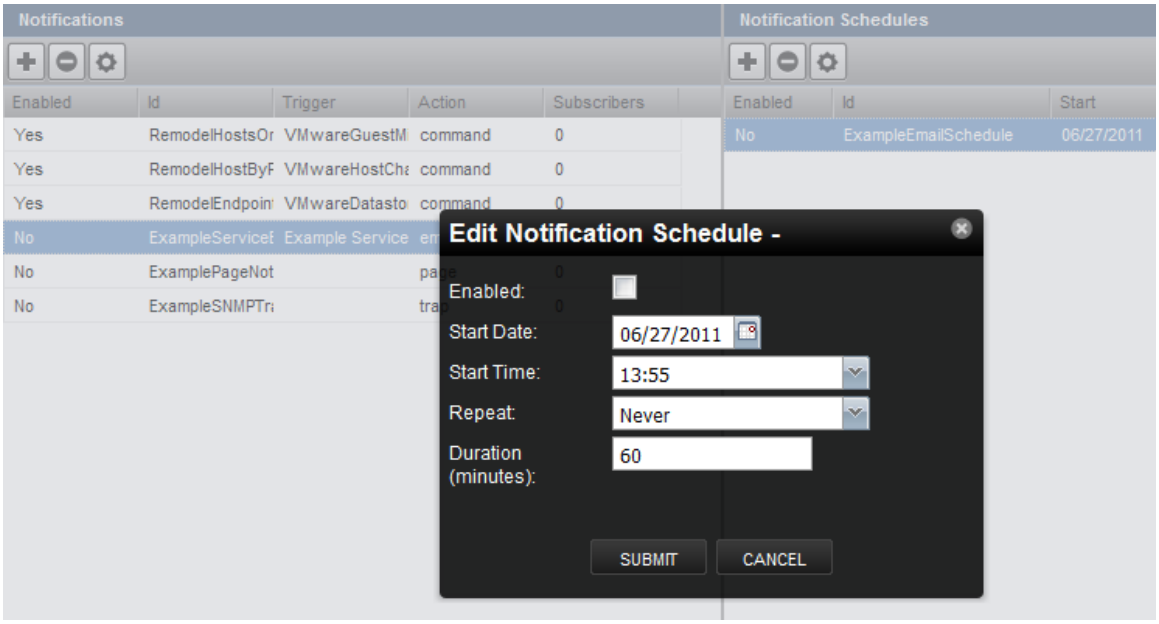
3 Enter a schedule ID, and then click **Submit**.

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 26: Edit Notification Schedule



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 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.

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

Note If you have a Cisco UCS Performance Manager Express license, you will only see the **Add Cisco UCS** option.

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 dialog, you can enter credentials for your UCS domain.

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 discovered device.

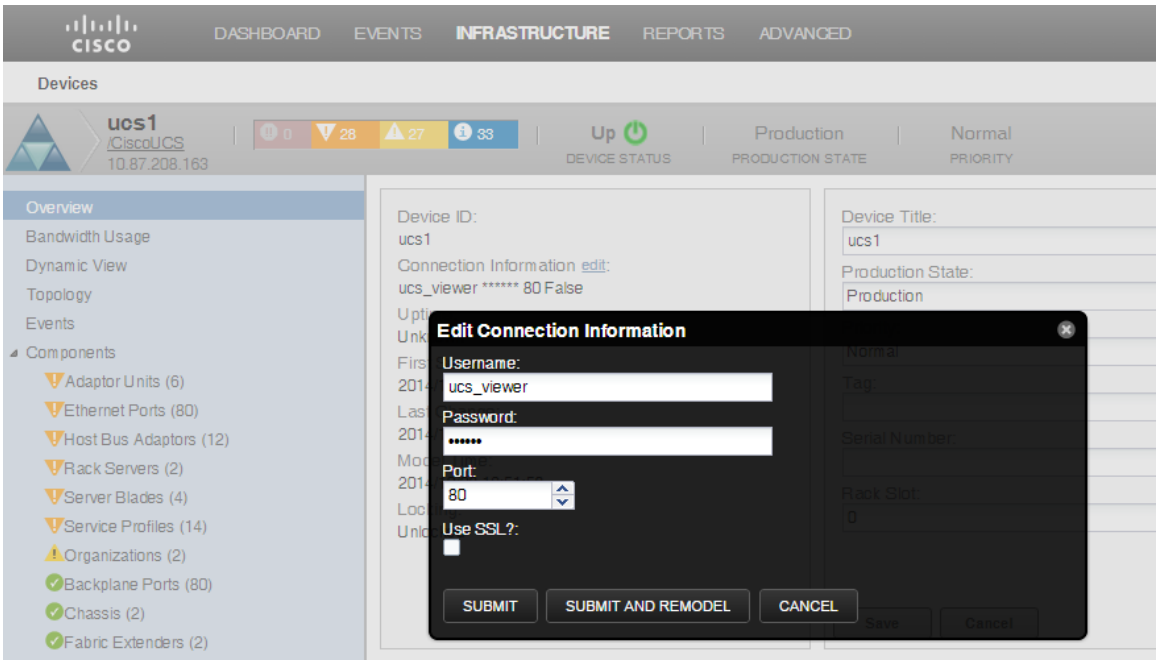
To add or edit information:

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.



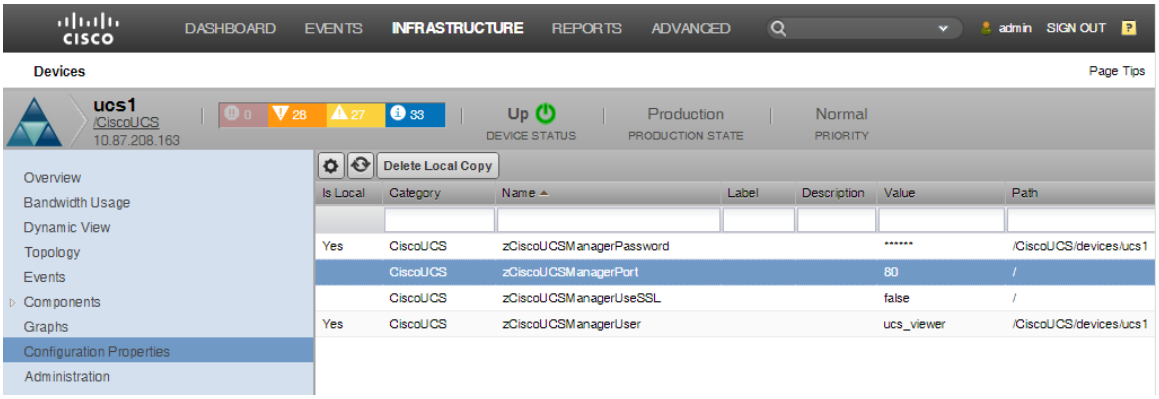
3. Edit the username, password, and/or port and select whether or not to use SSL.
4. Click **Submit** to submit the new connection information. The device will be remodeled at the next scheduled remodeling time.

   or

   Click **Submit and Remodel** to submit the new connection information and begin and 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 propery you want to change. The Edit Config Property dialog appears.

3 Edit the appropriate fields 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

Note This functionality is not available with a Cisco UCS Performance Manager Express license.

To model devices, the system can use:

- SNMP
- SSH
- WinRM
- Telnet

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.

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:

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

If the command returns any stack traces, check the community forums for assistance. Otherwise, forward these details to Support for assistance:

- Command you ran
- Stack trace or stack traces returned
- Version of your Cisco UCS Performance Manager instance
- OS version and patch level for the remote device

3 Working with Devices

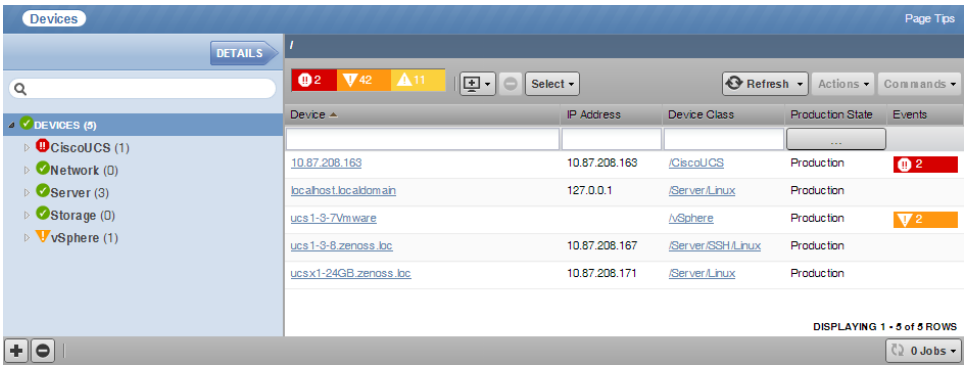
This chapter provides information and procedures for managing devices in the system.

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 27: Device List



Devices Hierarchy

Devices are organized in the tree view by:

- Devices
- Application Groups
- Integrated Infrastructure

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:

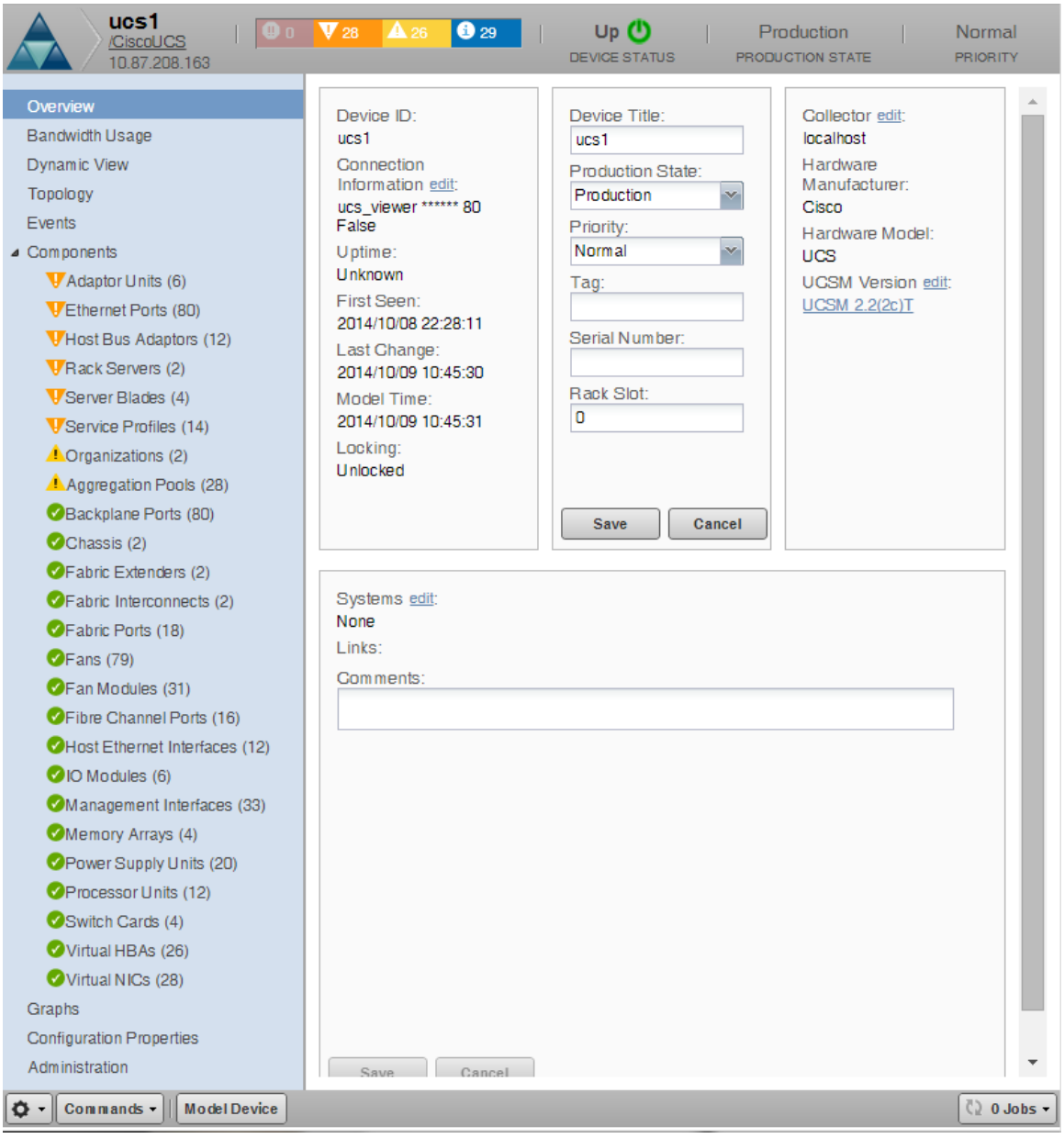
- Move devices to a different class (not available with Cisco UCS Performance Manager Express license)

- Assign devices to Application 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 28: 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)

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 title
- Production state
- Priority
- Tag
- Serial number
- Rack slot
- Collector
- Hardware and software manufacturer and model

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, such as:

- Bandwidth Usage
- Dynamic view
- Topology
- Events
- Components
- Graphs
- Configuration Properties
- Administration

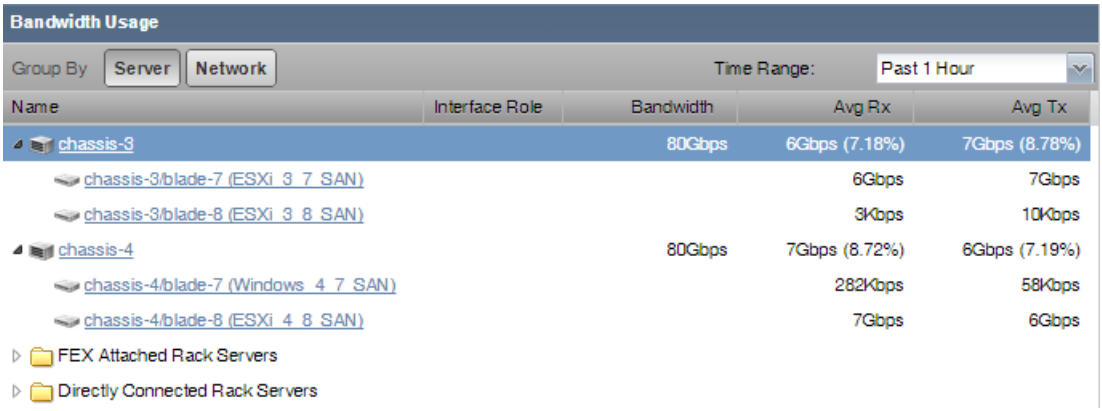
Information that appears here varies depending on device type.

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.



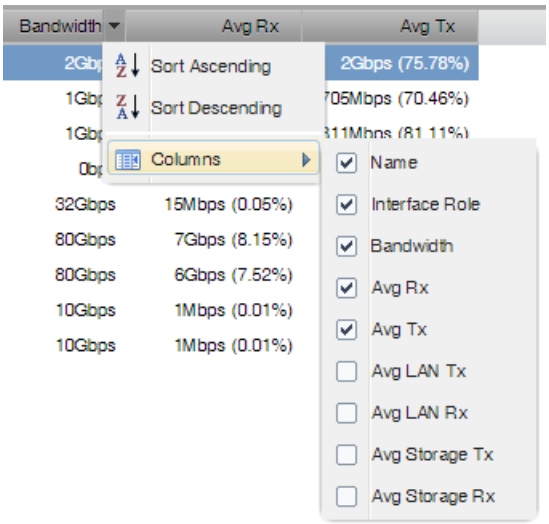
3 The bandwidth for the chassis appears along with the average transmitted and average received rates broken down by blade.

Note The aggregation pool values (e.g., the top level chassis/fex) are calculated at an interval of 30 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.

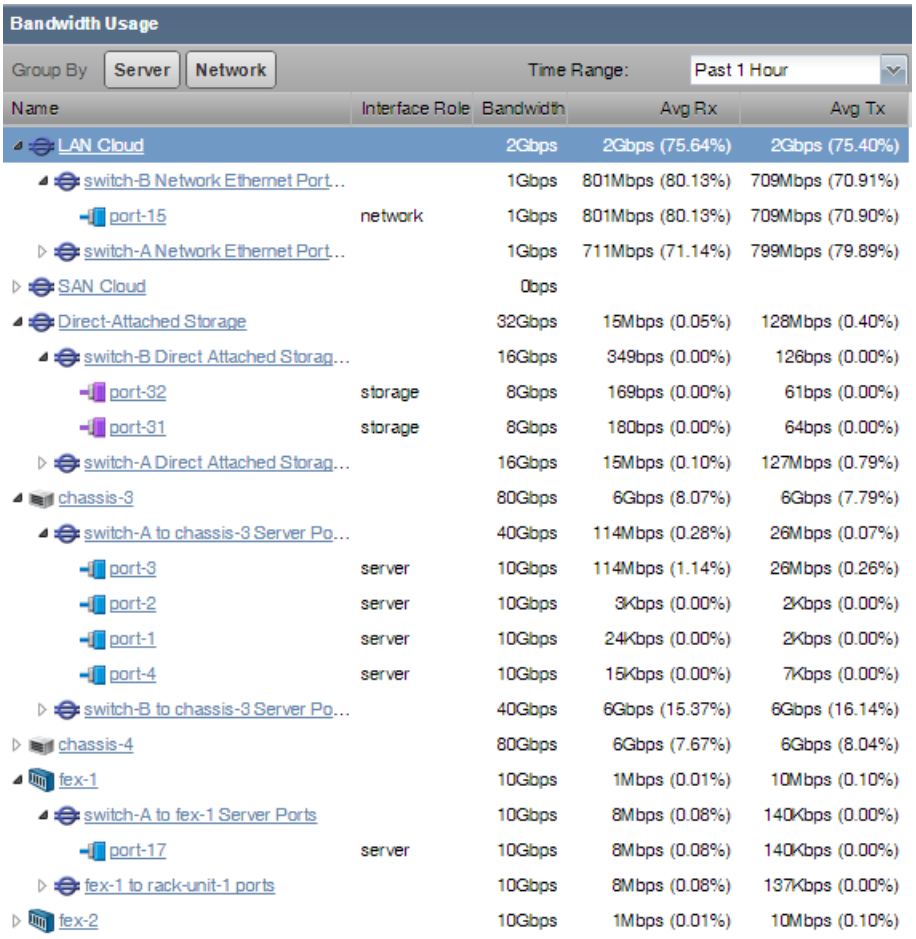
5 You can add or remove columns from the display by clicking the arrow next to any column header, scrolling down to **Columns** and selecting the information you are interested in displaying from the flyout menu.



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.



Bandwidth Usage

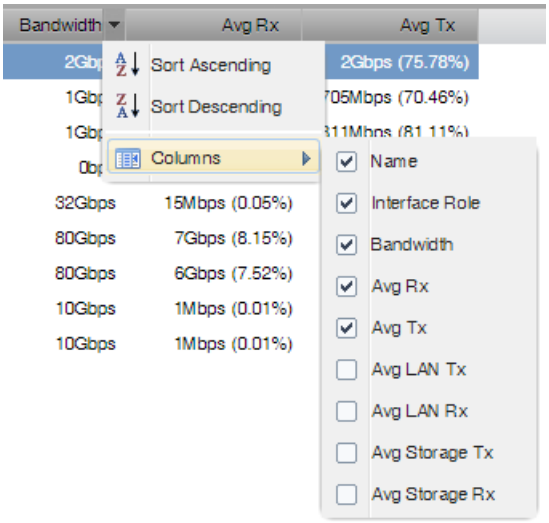
Group By: Server | Network — Time Range: Past 1 Hour

Name	Interface Role	Bandwidth	Avg Rx	Avg Tx
LAN Cloud		2Gbps	2Gbps (75.64%)	2Gbps (75.40%)
switch-B Network Ethernet Port...		1Gbps	801Mbps (80.13%)	709Mbps (70.91%)
port-15	network	1Gbps	801Mbps (80.13%)	709Mbps (70.90%)
switch-A Network Ethernet Port...		1Gbps	711Mbps (71.14%)	799Mbps (79.89%)
SAN Cloud		0bps		
Direct-Attached Storage		32Gbps	15Mbps (0.05%)	128Mbps (0.40%)
switch-B Direct Attached Storag...		16Gbps	349bps (0.00%)	126bps (0.00%)
port-32	storage	8Gbps	169bps (0.00%)	61bps (0.00%)
port-31	storage	8Gbps	180bps (0.00%)	64bps (0.00%)
switch-A Direct Attached Storag...		16Gbps	15Mbps (0.10%)	127Mbps (0.79%)
chassis-3		80Gbps	6Gbps (8.07%)	6Gbps (7.79%)
switch-A to chassis-3 Server Po...		40Gbps	114Mbps (0.28%)	26Mbps (0.07%)
port-3	server	10Gbps	114Mbps (1.14%)	26Mbps (0.26%)
port-2	server	10Gbps	3Kbps (0.00%)	2Kbps (0.00%)
port-1	server	10Gbps	24Kbps (0.00%)	2Kbps (0.00%)
port-4	server	10Gbps	15Kbps (0.00%)	7Kbps (0.00%)
switch-B to chassis-3 Server Po...		40Gbps	6Gbps (15.37%)	6Gbps (16.14%)
chassis-4		80Gbps	6Gbps (7.67%)	6Gbps (8.04%)
fex-1		10Gbps	1Mbps (0.01%)	10Mbps (0.10%)
switch-A to fex-1 Server Ports		10Gbps	8Mbps (0.08%)	140Kbps (0.00%)
port-17	server	10Gbps	8Mbps (0.08%)	140Kbps (0.00%)
fex-1 to rack-unit-1 ports		10Gbps	8Mbps (0.08%)	137Kbps (0.00%)
fex-2		10Gbps	1Mbps (0.01%)	10Mbps (0.10%)

Note The aggregation pool values (e.g., the top level chassis/fex) are calculated at an interval of 30 minutes which may result in some variance compared to the sum of the values of the underlying ports.

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.

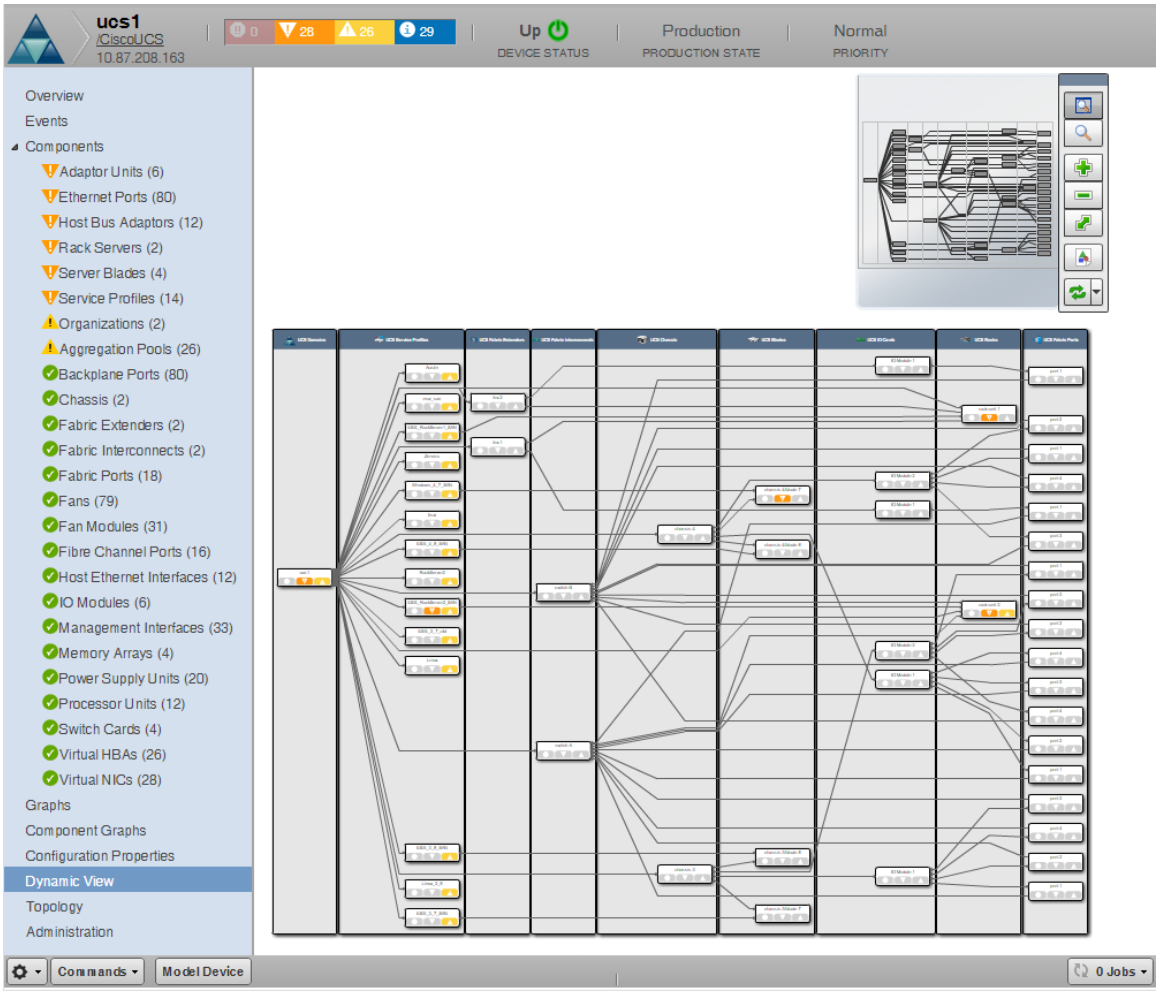


Dynamic View

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

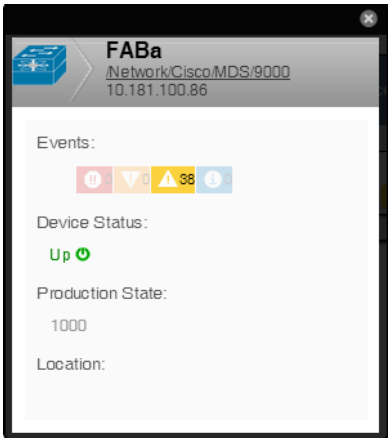
You can access the dynamic view from application groups and an integrated infrastructure. Depending on the object type, different relationships are illustrated. Each dynamic view shows related objects in a graph. Each object in that graph displays its associated event information.

Note For vSphere, the only dynamic view available is through an application 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 29: Dynamic View: Inspector Panel

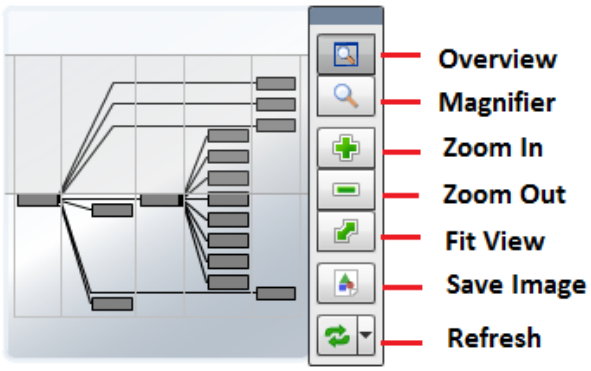


View controls appear to the right of the graph. These allow you to adjust your view:

- **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 30: 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 cluster.

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

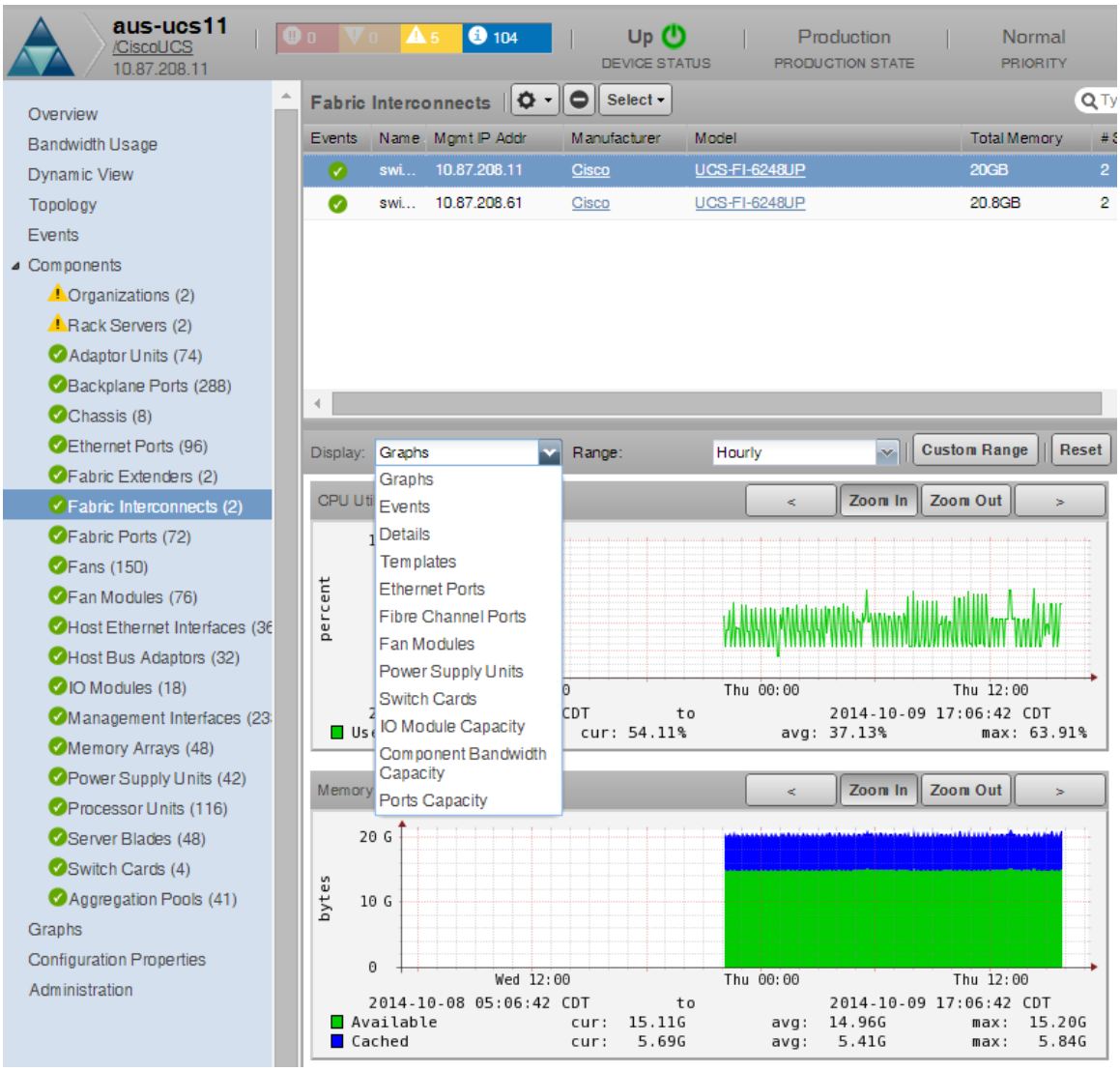
The Components view provides information about the different types of device components, including:

- 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 31: 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.

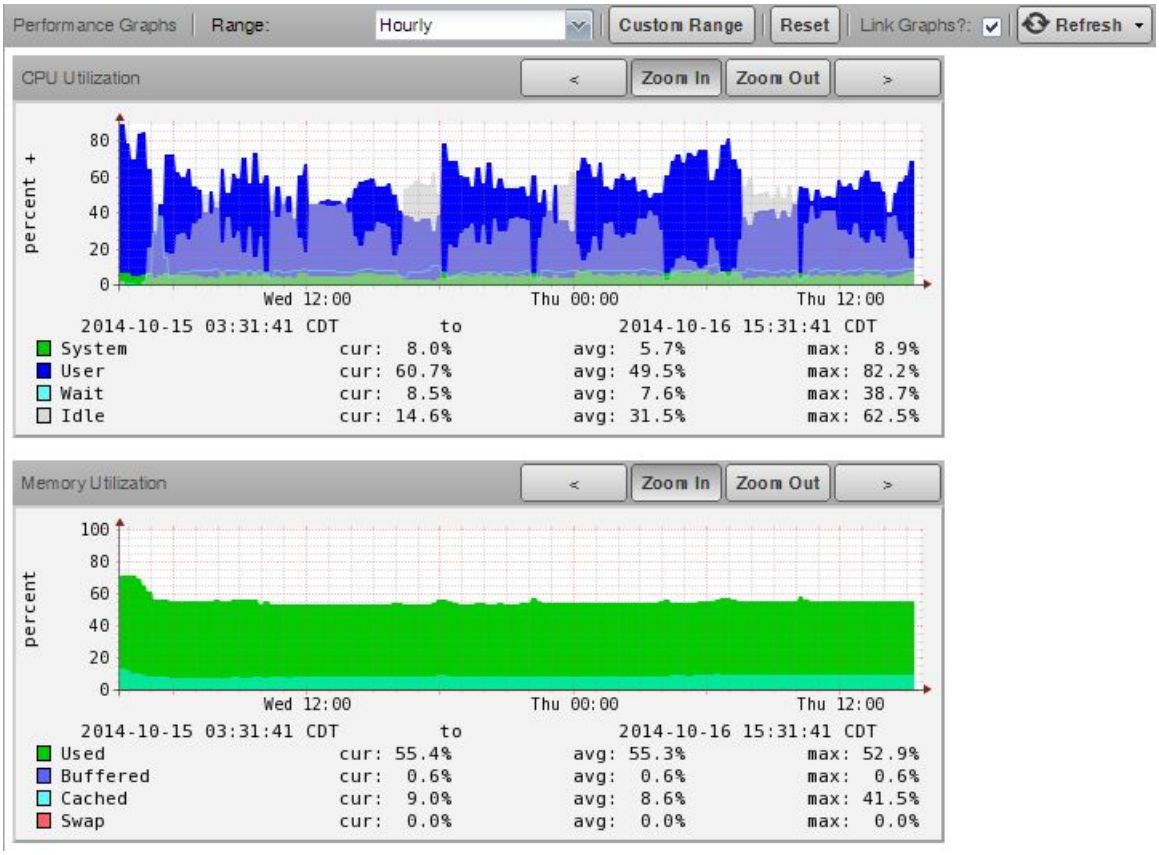
From this view, you can:

- 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. To access graphs, select **Graphs** in the left panel. The following figure shows performance graphs for a Linux server.

Figure 32: Device (Graphs)



Note You can use the arrow key and magnifying glass controls on the sides of each graph to change the graph view, scrolling through or zooming in or out of a graph.

You can control these performance graph options:

- **Range** - Select the span of time displayed in the graph. You can select:
  - Hourly - Past 36 hours
  - Daily - Past ten days
  - Weekly - Past six weeks
  - Monthly - Past 15 months
  - Yearly - Past two years
- **Custom Range** - Click to set a custom range. Enter the Start Date/Time and the End Date/Time to display.
- **Reset** - Click to return to the default (initial view) of the graphs.
- **Link graphs** - By default, all graphs move together. If you click the back arrow for a graph, for example, then all graphs move backward. De-select the Link graphs option to control each graph individually.
- **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 the Refresh button each time you want an updated graph.

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.

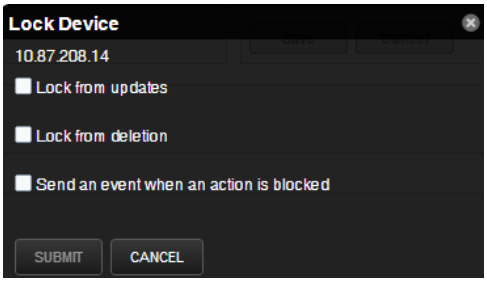
Note Device locking prevents changes and deletion due to remodeling. It does not prevent manual changes and deletion.

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 33: Lock Device Dialog



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

   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.

To rename a device:

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

The Rename Device dialog appears.

3 Enter the new name for the device, and then click **Submit**.

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.
2 At the bottom of the device overview page, select Model Device from the Action menu.

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

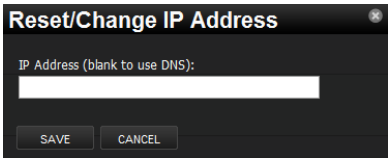
Resetting the Device Manage IP Address

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 34: 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.

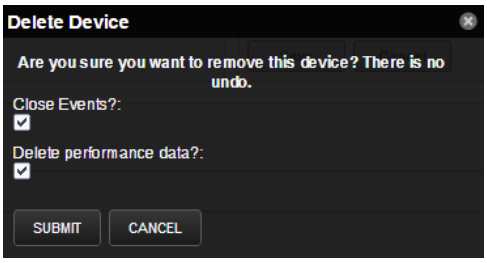
Deleting a Device

To delete a device from the system:

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

The Delete Device dialog appears.

Figure 35: Delete Device



3 Optionally change the selections to delete current events or performance data for the device. By default, events and performance data are removed.
4 Click **Submit**.

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

Working with Application Groups

Application 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 application group. In addition, you can quickly identify which of these operating systems are affected by capacity issues. Application groups can only be used for Linux and Windows targets. There are many different use cases for setting up application groups. One scenario would be to set up an application group for production devices and another for test devices. Another scenario might be to create an application group for devices supporting a particular business unit or location.

Creating an Application Group

To create an application group using devices that are already being monitored:

1 Navigate to the **Infrastructure** page to view a list of the monitored devices.
2 Click **Application 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 application group (e.g., Production or Austin). Click **Submit**. The new application group name appears in the left column.
5 Click **Devices** or a device class to display a list of monitored devices.
6 Select the device(s) you want to add to the application 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.

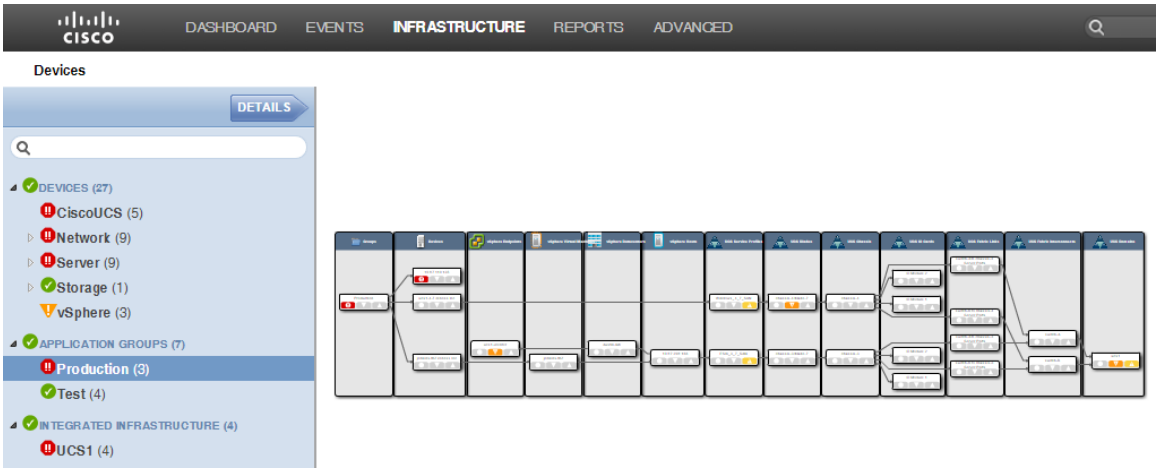
---

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

Viewing Application Group Dynamic View

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

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

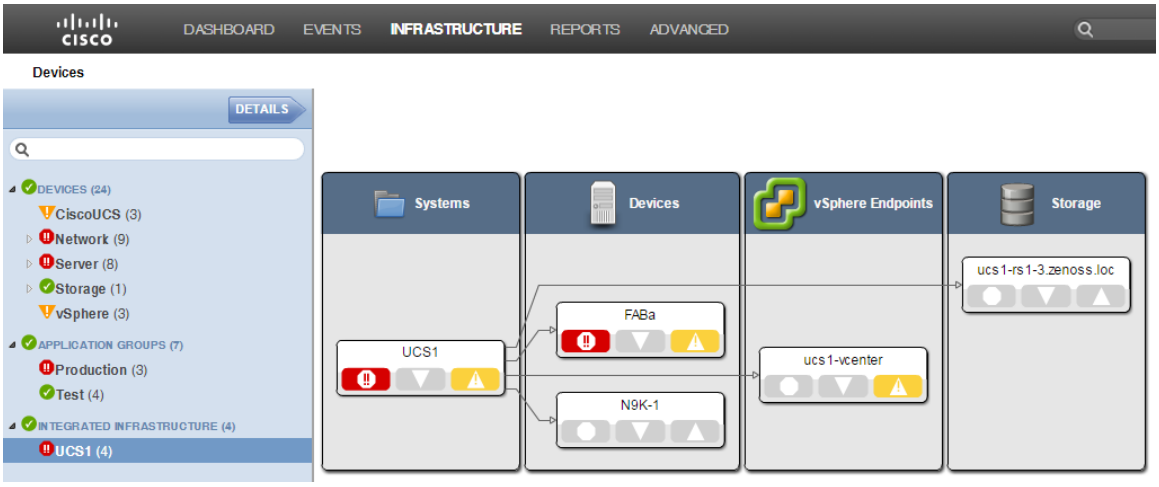
Note Be sure to click anywhere on the row that is not a hyperlink to select it. If you click a hyperlink, you will be taken to the specific details page.

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.

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

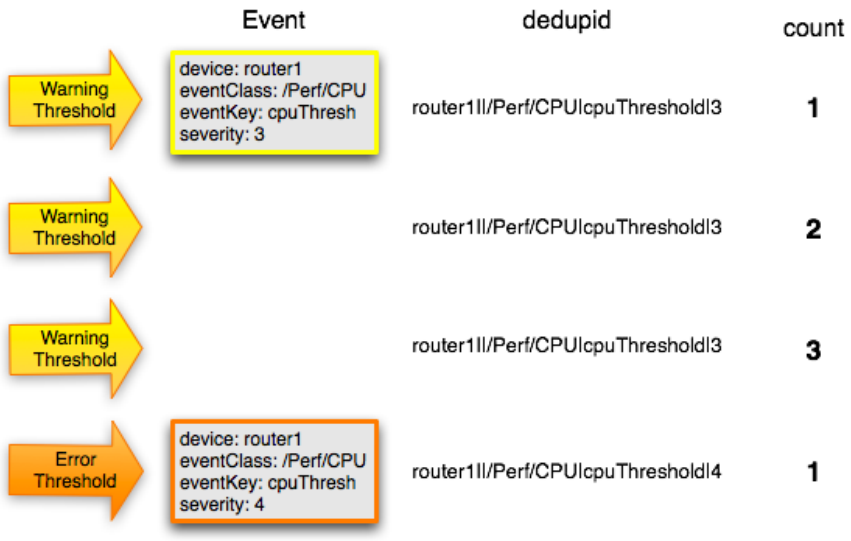
When the component and eventKey fields are present, a dedupid appears similar to:

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 36: 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:

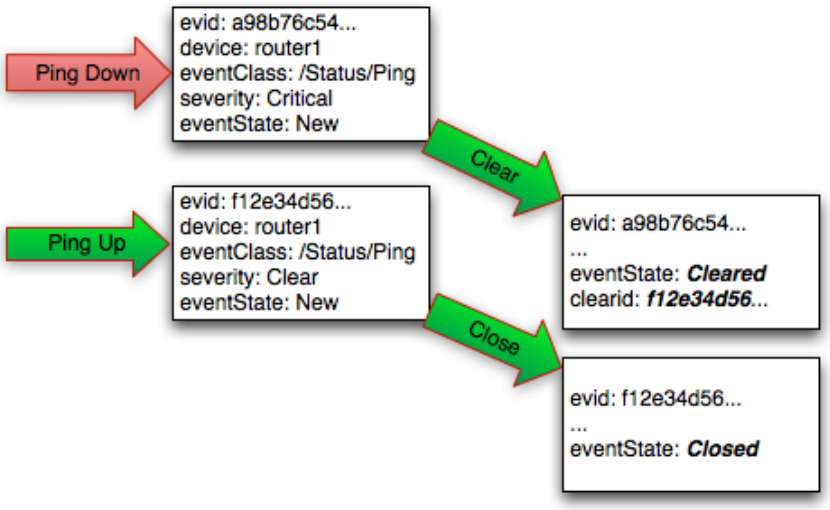
- If component UUID exists:
  - component UUID
  - eventClass
  - eventKey (can be blank)
- If component UUID does not exist:
  - device
  - component (can be blank)
  - eventKey (can be blank)
  - eventClass

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 37: 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.

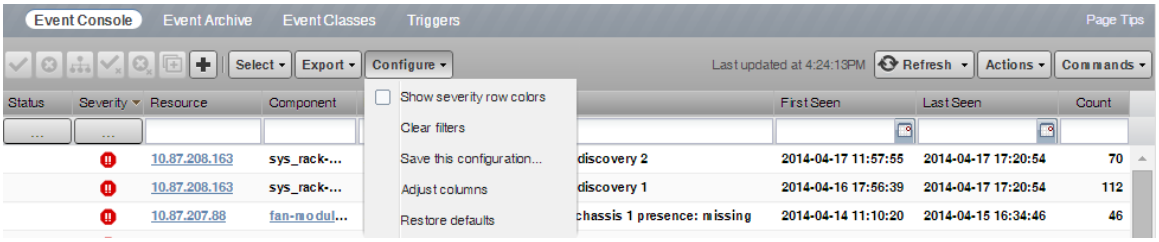
Event consoles are:

- **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 38: 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

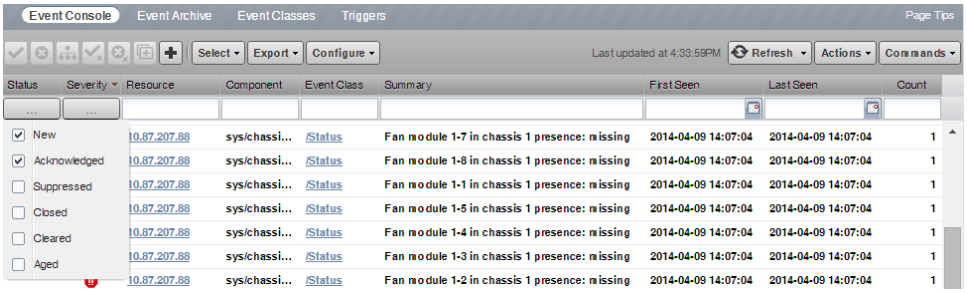
Sorting and Filtering Events

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 contained in the values in that column. You can also use AND, OR, or !! expressions to further target your filters. For example, typing `!!status` in the Event Class filter will return all the non-status class events.

Figure 39: 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:

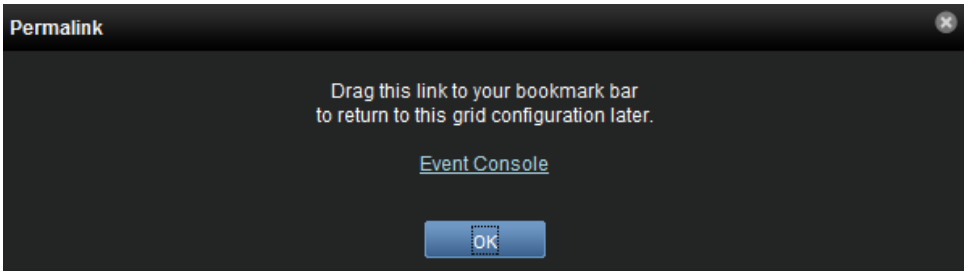
1 Select **Configure > Save this configuration**.

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 40: Saving a Custom View (Bookmark)



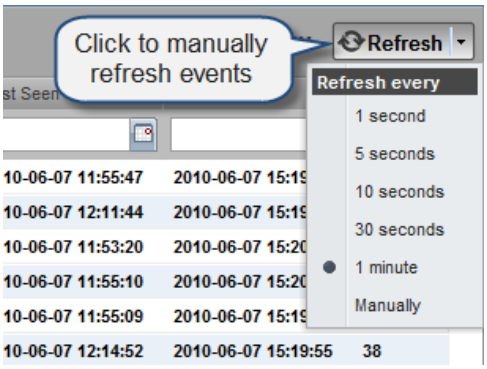
Note You may want to re-title the bookmark, particularly if you choose to save more than one event console view.

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 41: Automatic Refresh Selections

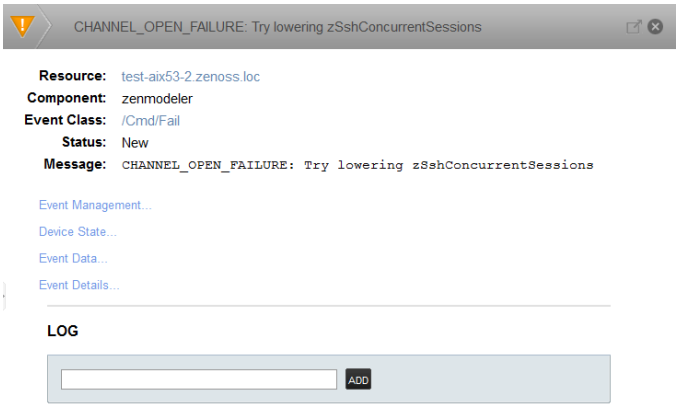


Viewing Event Details

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

The Event Details area appears.

Figure 42: 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.

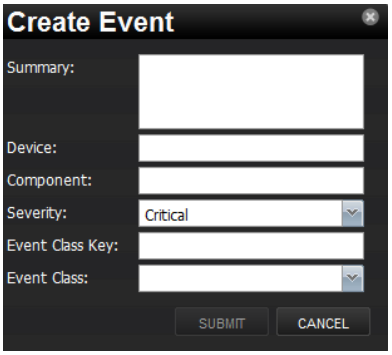
Creating Events through the User Interface

To create events manually through the user interface:

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

The Create Event dialog appears.

Figure 43: 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

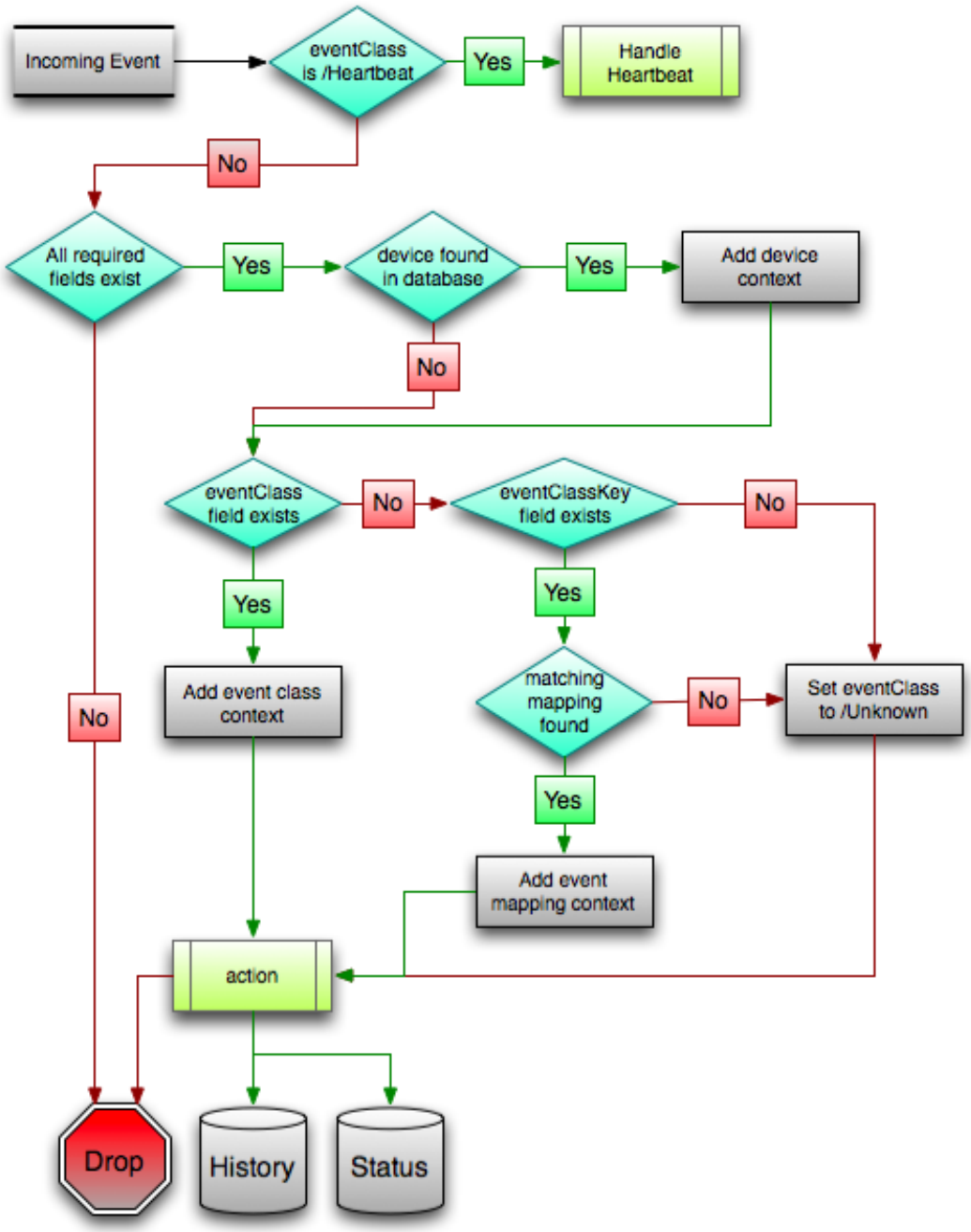
The event mapping and transformation system allows you to perform a wide range of operations, from altering the severity of certain events to altering nearly every field on an event, based on complex rules.

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 44: 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 Mappings in the left panel. This allows you to see all event class mappings in a single location. The EventClass 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:

- **Event Class Key**- Must match the incoming event's Event Class Key field for this mapping to be considered as a match for events.
- **Sequence**- Sequence number of this mapping. This number determines the order in which mappings with the same event class key are evaluated.
- **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.
- **Transform**- 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."
- **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.

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

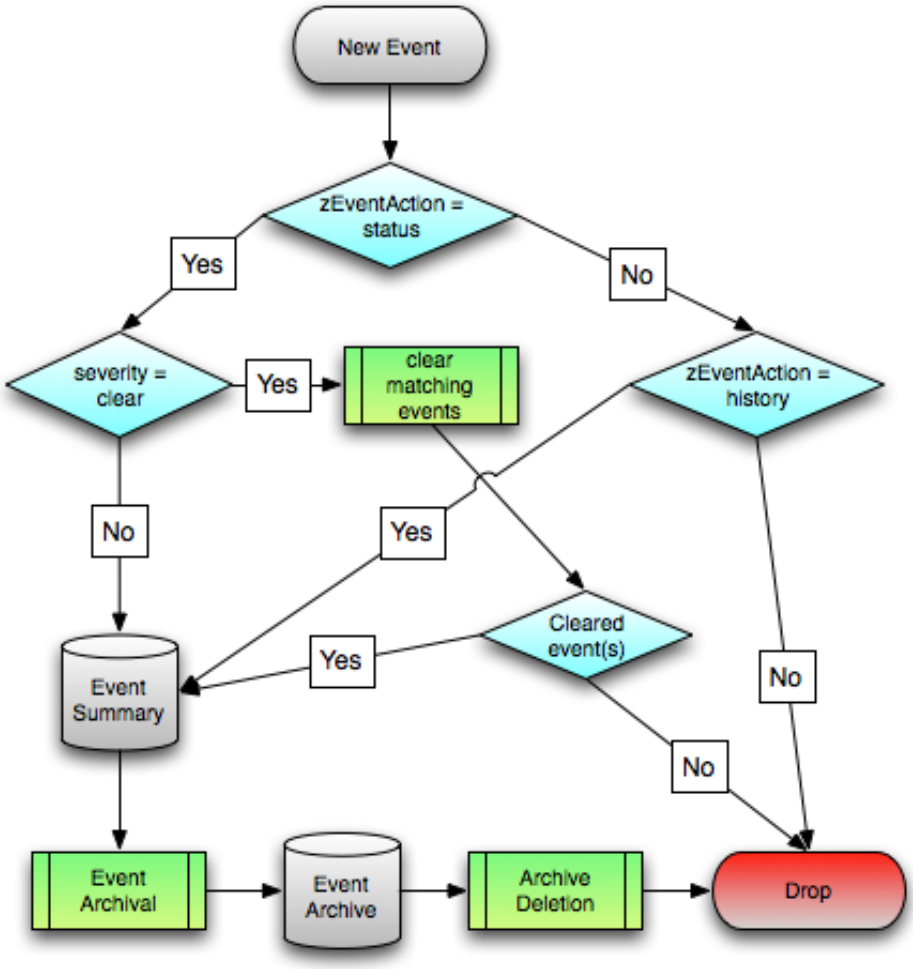
would be displayed. You can set one to 0, and the other to 1. (You can enter other values, but they will be changed to the shortest list of integers, starting with 0.) Setting fanDown to 0 and fanUnknown to 1 will ensure that the events will be mapped properly.

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 45: 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)** -
- **Event Aging Limit** -
- **Event Archive Threshold (minutes)** -
- **Event Archive Interval (milliseconds)** - 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 Limit** -
- **Delete Archived Events Older Than (days)** -
- **Default Syslog Priority** -
- **Default Availability Report (days)** -
- **Max Event Size in Bytes** -
- **Summary Index Interval (milliseconds)** -
- **Archive Index Interval (milliseconds)** -
- **Index Limit** -
- **Event Time Purge Interval (days)** -
- **Enable Event Flapping Detection** -
- **Event Flapping Event Class** -
- **Clear 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).

SNMP Traps and Event Transforms

Note This functionality is not available with a Cisco UCS Performance Manager Express license.

An SNMP trap is a message that is initiated by a network element and sent to the network management system. Often, traps indicate a failure of some sort, such as a router message indicating a power supply failure, or a printer message indicating an "out-of-ink" condition.

If an SNMP trap enters the system, and Cisco UCS Performance Manager cannot identify the event (the event is classified as "/Unknown"), then you can classify the event so that the system handles it consistently.

Classifying SNMP Traps

To classify an SNMP trap event:

1. From the Event Console, select the unknown event or events.
2. Click (Map to event class).

   The Classify Events dialog appears.
3. Select /App, and then click **Submit**.

To edit this classification:

1 From the Navigation area, select Events > Event Classes.
2 In the left panel, select Mappings.
3 Select the event map you created.
4 In the left panel, select Edit.

The edit page appears. This page contains rules used to map the event to the /App category. This rule, since it matches the trap by a specific OID, is all that is needed.

In the Transform area, you can enter code to modify the summary. For example, if you want to set the summary string to "Spam Filter Detects Virus," then you can enter:

```
evt.summary = "Spam Filter Detects Virus"
```

A trap has a header with some standard information, followed by a sequence of attribute/values.

You have indicated you want the value for the OID ".1.3.6.1.4.1.9789.1500.2.5" as the summary. If you had the MIB loaded, you could do this:

```
evt.summary = evt.spamFilterDetectsVirus
```

However, the OID and the data is still in there. Instead, use the slightly more cryptic:

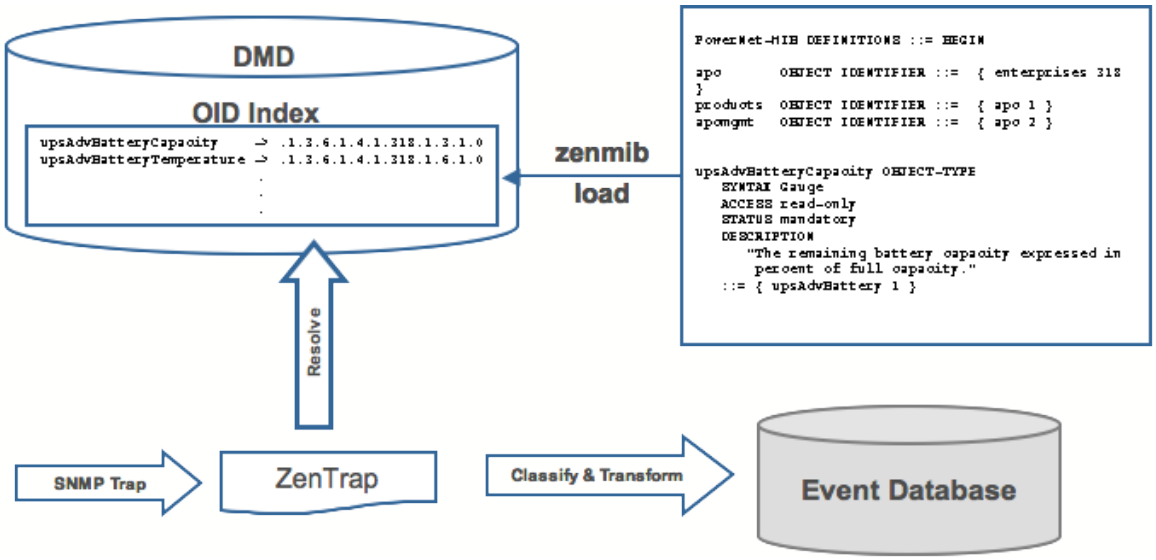
```
evt.summary = getattr(evt, ".1.3.6.1.4.9789.1500.2.5", "Unexpected missing
 OID")
```

The "device" object for the event has been made available, as well:

```
evt.summary = getattr(evt, ".1.3.6.1.4.9789.1500.2.5", "Unexpected missing
 OID") \ + " from device " + device.getId()
```

Cisco UCS Performance Manager uses MIBs to translate SNMP traps that contain raw OID values. Loading a MIB into the system allows it to translate numeric OIDs such as .1.3.6.1.2.1.1.6 into descriptive phrases like “sysAppGroup”. It also makes it easier to manipulate the events in an event mapping.

Figure 46: SNMP TRAP Transform



Following is a small demonstration MIB.

```
NOTIFICATION-TEST-MIB DEFINITIONS ::= BEGIN IMPORTS ucdavis FROM UCD-SNMP-
MIB NOTIFICATION-TYPE FROM SNMPv2-SMI ; demonotifs OBJECT IDENTIFIER ::=
```

```
{ ucdavis 991 } demo-notif NOTIFICATION-TYPE OBJECTS { sysAppGroup }
STATUS current DESCRIPTION "Just a test notification" ::= { demonotifs
17 } END
```

Transforming Events with Event Mappings

To modify events as they arrive, create an event map through the user interface:

1. Create an event class.
2. Go to the event console and create an event mapping in this class from the existing event.
3. Edit the map.
4. In the Transform area, update the event with detail data. The entry field allows you to insert Python scripts. The event is provided as "evt" and the device as "dev."

   In this case, extract the sysAppGroup event detail and make it the summary with:

   ```
   evt.summary = evt.sysAppGroup
   ```
5. Save the event mapping.

If you move the event to the event archive and resend the trap, the summary for the trap should now read the device name in the application group you assigned.

If you encounter problems with the transform, check the `zentrap.log` file for errors that occurred.

Event Transforms Based on Event Class

When an event arrives in the system, you can change values (such as severity). For example, you can make the summary more informative, or change severity according to text within the summary.

Each event class allows for a short Python script to be executed when an event arrives.

Example

A user may want full file system threshold events on `/data`to be critical. Add the following Python script in the Threshold Transform of /Events/Perf/Filesystem:

```
if evt.component == '/data' and evt.severity != 0: evt.severity = 5
```

Like event mappings for event class keys, "evt" and ""dev" objects are available in the script of the transform.

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

Typically, devices begin in the system in “Pre-Production.” In this state, devices are monitored by default, but no remote alerting occurs, and events are not shown on the dashboard. Once a device is in full “Production” state, monitoring occurs and remote alerts are sent. If service needs to be performed on a device, its state can be set to “Maintenance” to temporarily block any remote alerts.

When you add a device to the system, its default state is Production.

Setting the Production State for Devices

To set the production state for a device:

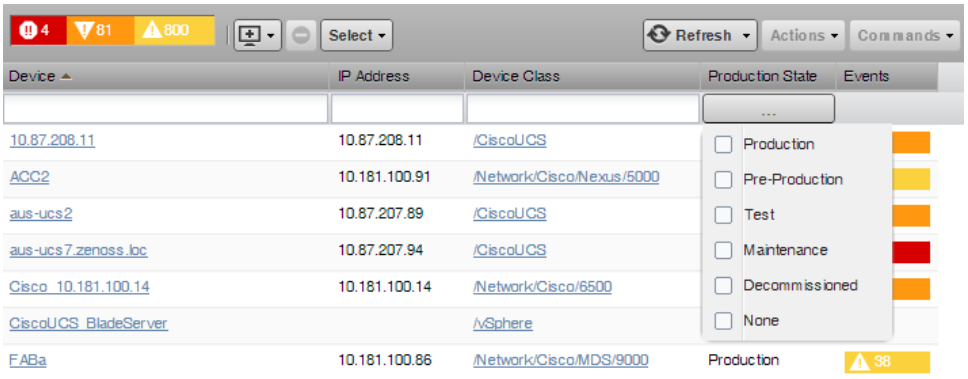
1 Click a device name in the list of devices. The device Overview page appears.
2 Select a production state from the list of options, and then click **Save**.

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 47: 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 (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.
- **Duration** - Specify the length of time for the window to be in effect.
- **Repeat** - Specify how often to repeat the maintenance winodw. Default value is Never.
- **Start Production State**- Define the production state for the window when the maintenance period begins.
- **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.

2 Click **Details**.

3 In the left panel, select Administration.

4 In the Maintenance Windows area, select Add Maint Window from the Action icon.

The Add Maintenance Window dialog appears.

5 Enter a name for the maintenance window, and then click **OK**.

The newly defined maintenance window appears in the list.

6 Click the name in the list to show the maintenance window status page.

7 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.
- **Duration** - Specify the length of time for the window to be in effect.

- **Repeat** - Specify how often to repeat the maintenance winodw. Default value is Never.
- **Start Production State** - Define the production state for the window when the maintenance period begins.
- **Stop Production State** - Shows the production state that will be in effect when the maintenance period ends.

8 Click **Save**.

6 Organizers and Path Navigation

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.

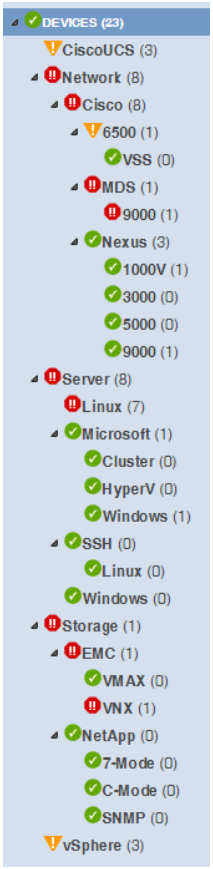
The following procedures are illustrated using device classes and sub-classes, but the same concepts apply to event classes, service classes, and product classes. When you add a device to the system, you should (after providing the network name or IP address) specify its device class. Templates can be 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 48: Devices Hierarchy



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

Managing Users 7

Each user has a unique user ID, which allows you 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.

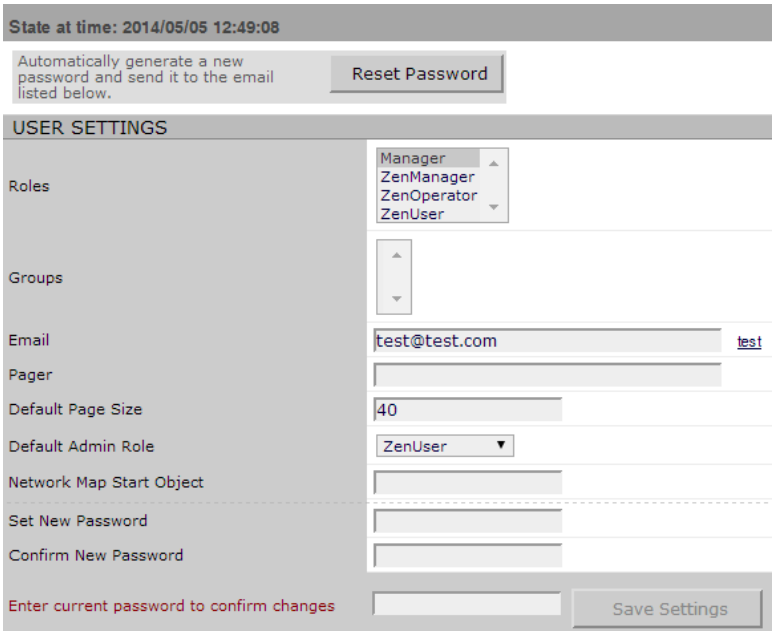
Editing User Accounts

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.

Figure 49: 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.
- **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 74.
- **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.
- **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.
- **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 74.

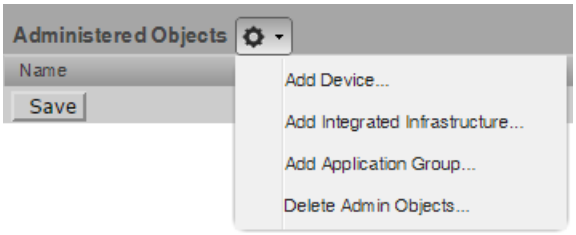
To create an object association:

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 50: Administered Objects - Add Object



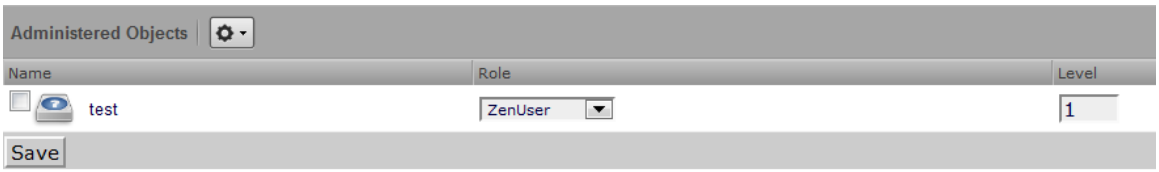
4 Select an object type from the Administered Objects Action menu. You can add:

- 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 51: 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 Select Advanced > Settings.
2 In the left panel, select Users

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

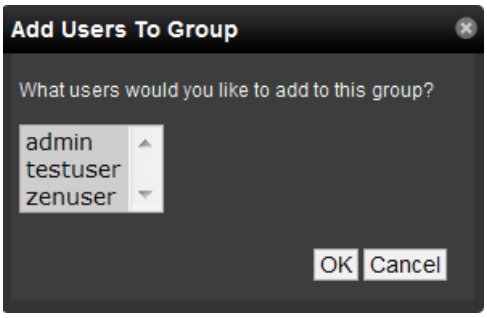
The Add Group dialog appears.
4 In the Group field, enter a name for this user group, and then click **OK**.

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 52: 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.

8 Reporting

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 of 15 minutes.

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

Cisco UCS Capacity Reports

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.

Graph Vertical Scaling

The type of scale used to display the graph. **Linear** plots data on a linear scale. If you have data that is in a very small range, you may want to switch to **Logarithmic** to focus on that data.

Domain Filter

A substring search of domains to include. A partial name matches all interface names that include it.

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

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.

Graph Vertical Scaling

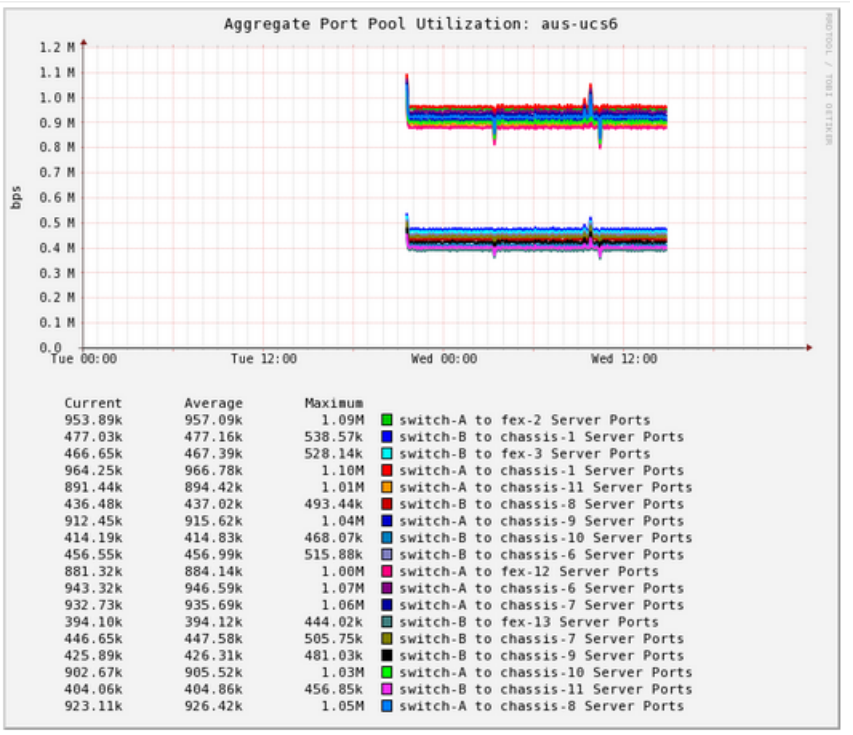
The type of scale used to display the graph. **Linear** plots data on a linear scale. If you have data that is in a very small range, you may want to switch to **Logarithmic** to focus on that data.

Domain Filter

A substring search of domains to include. A partial name matches all interface names that include it.

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

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.

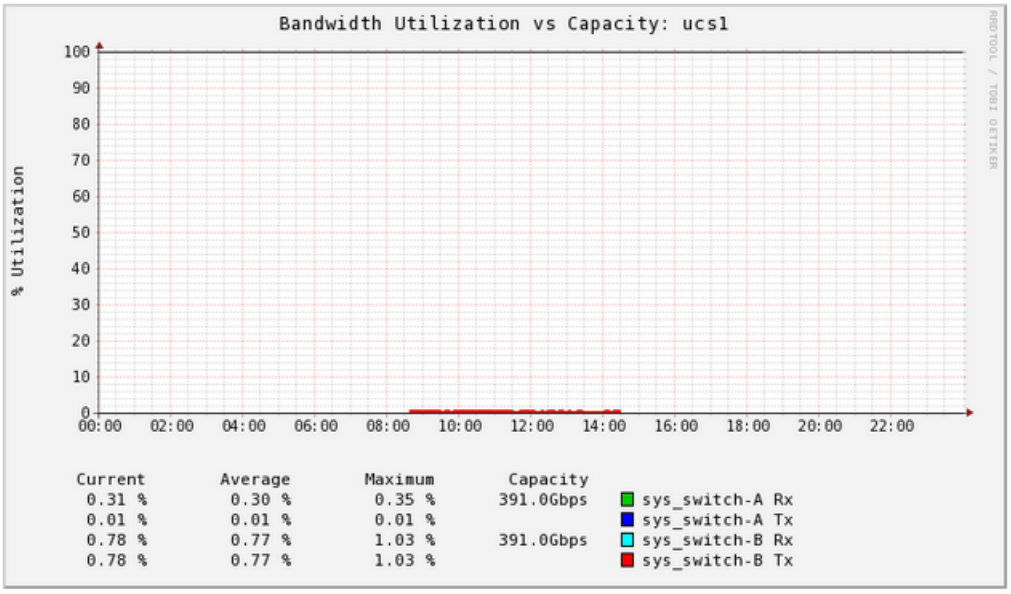
Domain Filter

A substring search of domains to include. A partial name matches all interface names that include it.

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

The following is an example of the graph generated for the bandwidth utilization divided up into receiving and tranmitting traffic per switch.

Note The traffic on the sample domain in this report is very small (averaging less than 1%).



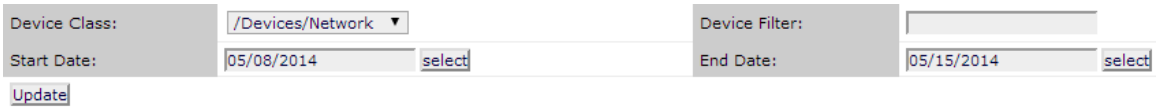
The following is an example scenarios that may be seen in graphs along with its corresponding description:

- 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.

Start Date

End Date

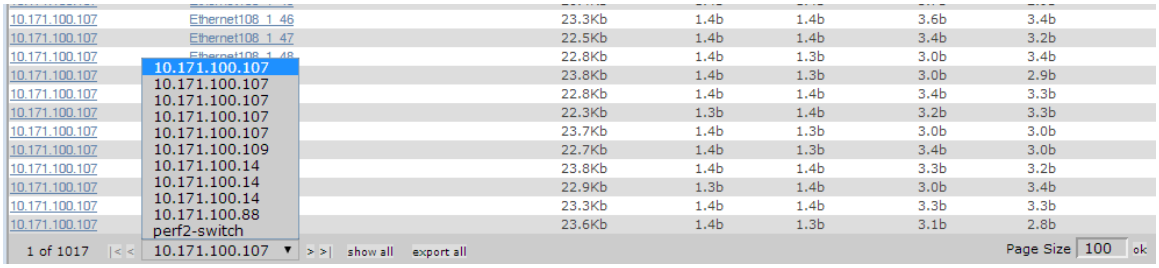
The first and last dates of the range of dates to include in the report. To select a date from a calendar, click **select**. The default range is the week ending with the current date.

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.
95% Out	The output traffic rate of the 95th percentile.

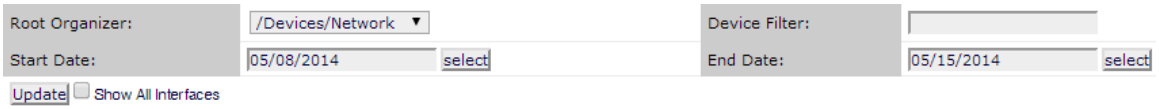
The following shows the navigation bar at the bottom of the report. To quickly navigate to other pages, select the device name from the pop-up list. In this example, there are 5 pages of results from device 10.171.100.107 followed by one page of results from device 10.171.100.109, etc.



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.

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.

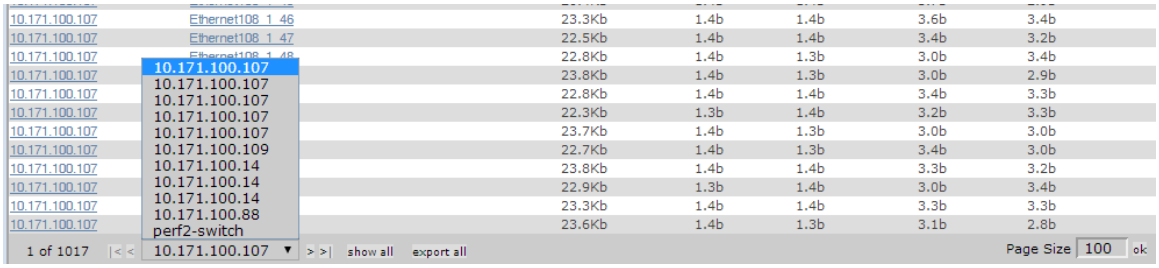
To generate or refresh the report, click **Update**. If you want to show all interfaces on the report, check the **Show All Interfaces** box before clicking **Update**.

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.

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.

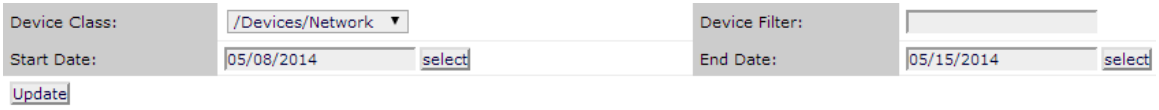
The following shows the navigation bar at the bottom of the report. To quickly navigate to other pages, select the device name from the pop-up list. In this example, there are 5 pages of results from device 10.171.100.107 followed by one page of results from device 10.171.100.109, etc.



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.

Start Date

End Date

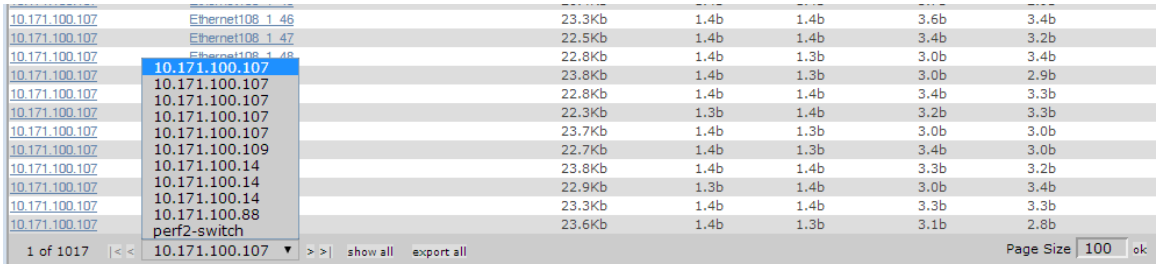
The first and last dates of the range of dates to include in the report. To select a date from a calendar, click **select**. The default range is the week ending with the current date.

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 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.

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.



Port Utilization

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

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.

Graph Vertical Scaling

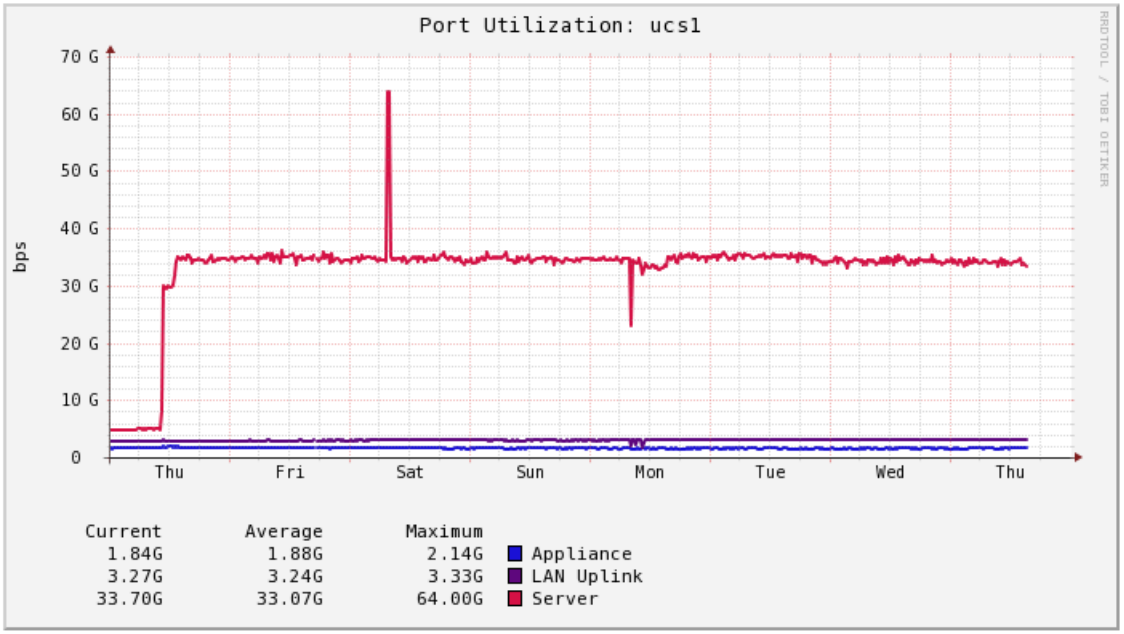
The type of scale used to display the graph. **Linear** plots data on a linear scale. If you have data that is in a very small range, you may want to switch to **Logarithmic** to focus on that data.

Domain Filter

A substring search of domains to include. A partial name matches all interface names that include it.

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

The following is an example of the graph generated for the port utilization broken up into its components.



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.

Cisco UCS Reports

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 Memory 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.

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.

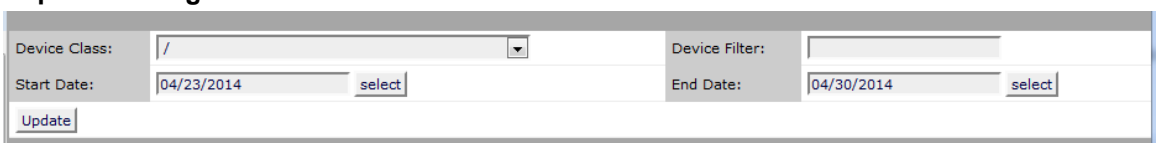
Enterprise Reports

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.

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**.

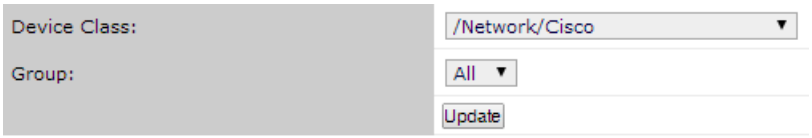
Report Contents

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.
95% Out	The output traffic rate of the 95th percentile.

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

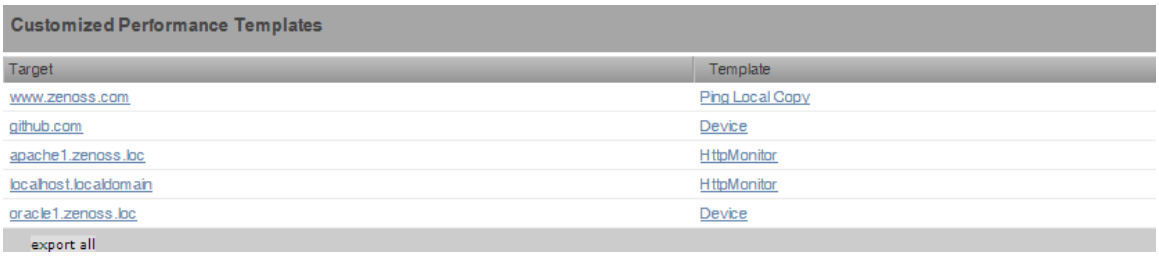
The specific group to consider when running the report. The default is `All`. The group could be a specific application group.

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.

Customized Performance Templates



Data Sources in Use

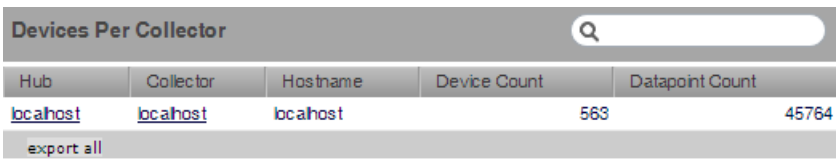
This reports lists the data sources defined in the system.

Report Contents

Column	Content
Device Class	The device class of the data source in use.
Template	The template associated with the data source in use.
Data Source Name	The name of the data source.
Data Source Type	The type of connection for the data source.
ZenPack	The ZenPack related to the data source.

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	
Collector	
Hostname	
Device Count	
Datapoint Count	

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.
ZenPack	The ZenPack related to the data source.

Event Time to Resolution

This report shows, for each user, the total time taken to acknowledge or clear events. Results are organized by user. It is helpful for tracking response time SLAs in a NOC-type environment.

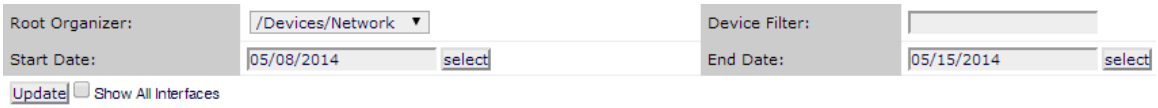
Report Contents

Column	Content
User	The user responsible for taking action on an event.
Severity	The severity of the event.
Time to Ack	The amount of time to acknowledge the event.
Time to Archive	The amount of time to clear and archive the event.

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.

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.

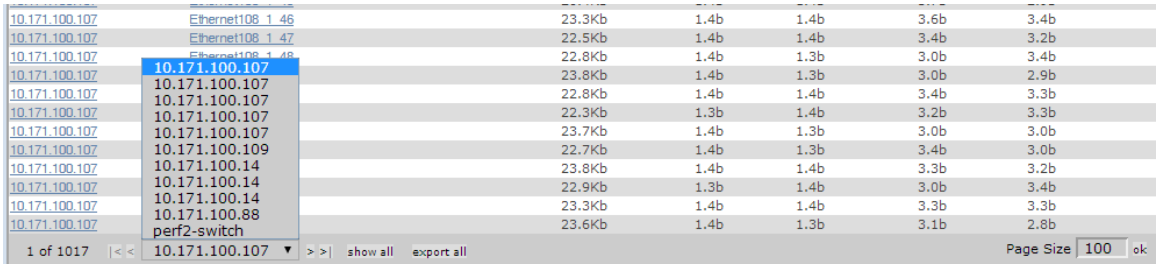
To generate or refresh the report, click **Update**. If you want to show all interfaces on the report, check the **Show All Interfaces** box before clicking **Update**.

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.

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.

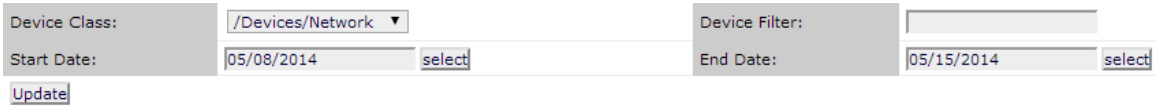
The following shows the navigation bar at the bottom of the report. To quickly navigate to other pages, select the device name from the pop-up list. In this example, there are 5 pages of results from device 10.171.100.107 followed by one page of results from device 10.171.100.109, etc.



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.

Start Date

End Date

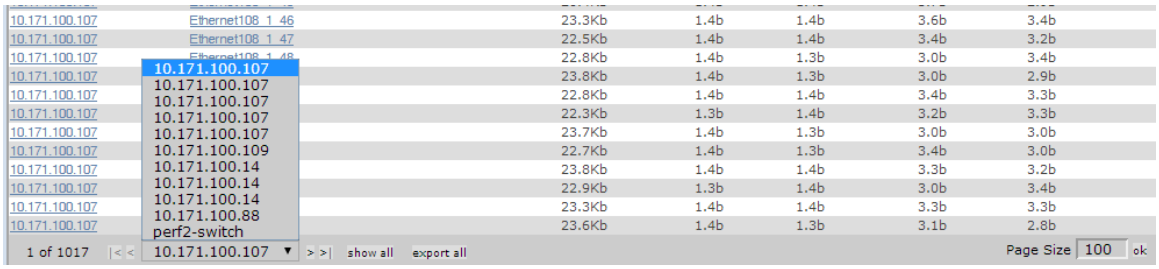
The first and last dates of the range of dates to include in the report. To select a date from a calendar, click **select**. The default range is the week ending with the current date.

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 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.

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.



Maintenance Windows

This report shows all defined windows that are active during a selected time period.

To change the reporting time period, enter Start and End dates (or click **Select** to select dates from a calendar). Click **Update** to refresh the report.

Report Contents

Column	Content
Name	Name of the maintenance window.
Target	
Start Date	Date the maintenance window becomes active.
Duration	Length of time for the maintenance window to be in effect.
Repeat	Repeat interval of the maintenance window.

Network Topology

Shows the layout of the network, according to the routes that Cisco UCS Performance Manager understands, starting from the collector and ending at the remote devices associated with the collector.

The report does not return data if the host on which the Cisco UCS Performance Manager collector is running does not have a device created in the device management database (DMD) object which stores the basic model of the network in the Zope database (ZODB). Create a device representing the collector in the DMD, and then run report again.

An invalid route entry (for example, 'Missing link here' value in the Route column) indicates that Cisco UCS Performance Manager cannot determine how to route from one device to another. Correct this by adding a network interface to the model (no new hardware required) and then adding a new route entry from the last device in the route to the device (the IP address shown at the far right of the table).

Report Filtering

Collectors

Select the collector to base the report on. Connections from this collector to associated devices will be shown in the report.

Show valid routes?

Select this check box to show valid connections between the selected collector and remote devices.

Show invalid routes?

Select this check box to show invalid connections between the selected collector and remote devices. An invalid route indicates that a route from the collector to the device could not be determined.

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

Report Contents

Column	Content
Collector	Name of the collector.
Route	Route from the collector to the device.
Device IP Address	IP address of the device.
Device Name	Name of the device.
Repeat	Repeat interval of the maintenance window.

Notifications and Triggers by Recipient

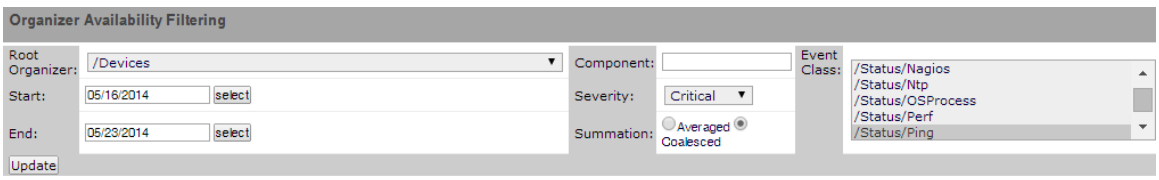
Organizer Availability

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**.

Organizer Graphs

This reports shows graphical data about a given organizer. The information displayed varies depending on the type of organizer. For example, selecting `/Devices/Network/Cisco` as an organizer displays graphs on CPU and Memory Utilization, Throughput, Errors, etc.

Report Filtering

Organizer

The class to use for filtering. The default is `/Groups`.

Filter

Additional text filter to refine results. The default is `.*` which returns all graphs available for the selected organizer.

Start Date

End Date

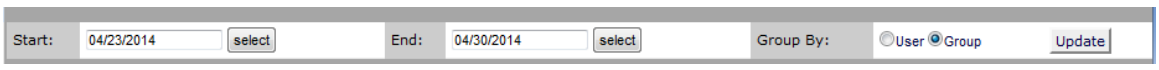
The first and last dates of the range of dates to include in the report. To select a date from a calendar, click **select**. The default range is the week ending with the current date.

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

User Event Activity

A list of users or groups and the number of events each has acknowledged and archived.

Report Filtering



The following fields define the report.

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.

Group By

The type of report to create, **User** or **Group**.

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

Report Contents

Column	Content
User or **Group**	The column label and content depend on the report selection. **User** The name of a user, with a link to the user's **USER SETTINGS** page. **Group** The name of a group, with a link to the group's **Users in Group** page.
# Acknowledged	The total number of events acknowledged by the user or group during the reporting period.
# Archived	The total number of events archived (cleared) by the user or group during the reporting period.

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.

VM to Datastore

This report lists the mappings between virtual machines (VM) and their datastore.

Report Contents

Column	Content
Endpoint Device	The name of the endpoint device. Clicking the name takes you to the Device Overview page.
Host	The name of the host on the Endpoint Device. Clicking the name takes you to the Hosts view on the appropriate Device page.
VM	The name of the virtual machine. Clicking the name takes you to the VMs view on the appropriate Device page.
Datastore	The name of the datastore. Clicking the name takes you to the Datastores view on the appropriate Device page.

9 General Administration and Settings

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**- Select a severity level (Clear, Debug, Info, Warning, Error, or Critical). Events with this severity level and severity levels above this one will not be aged by the system.
- **Event Aging Threshold**(minutes) - Specify how long the system should wait before aging an event.
- **Event Archive Interval**(minutes) - Specify how long a closed event remains in the Event Console before moving to the event archive.

- **Delete Archived Events Older Than**(days) - Enter a value in days. Cisco UCS Performance Manager will automatically delete events from the event archive that are older than this value.
- **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.

Rebuilding the Events Index

If you encounter inconsistent search results, you can rebuild the events index. As the zenoss user, follow these steps:

1 Stop zeneventserver:

```
zeneventserver stop
```

2 Delete the index:

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

3 Restart zeneventserver:

```
zeneventserver start
```

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.

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."
```

Stopping Audit Logging

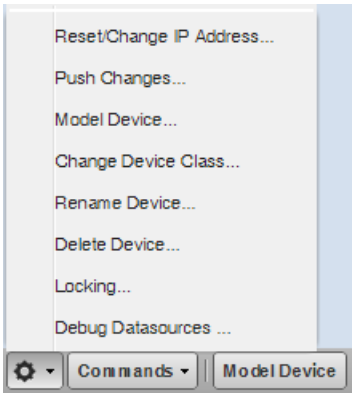
Audit logging has minimal impact on system performance; however, you can disable audit logging by removing the ZenPacks.zenoss.AuditLog ZenPack. If re-installed, the system does not overwrite the existing configuration and example files, so that you can refer to the `audit_log.conf.example` file if needed.

Debug Logging

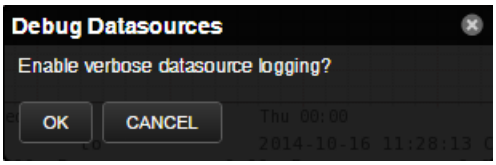
With debug logging enabled for all Calculated Performance datasources, a UCS domain produces alot of logging. However, this is not satisfactory when debugging a particular datasource. In order to effectively diagnose a graphs that is displaying NaN values, you need to debug each datasource involved in 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**.



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	ACL Permission
ZenUser, ZenOperator	ZenCommon, View
ZenManager, Manager	ZenCommon, View, Manage DMD
No Role, Administered Objs	ZenCommon

Setting Permissions

To set portlet permissions:

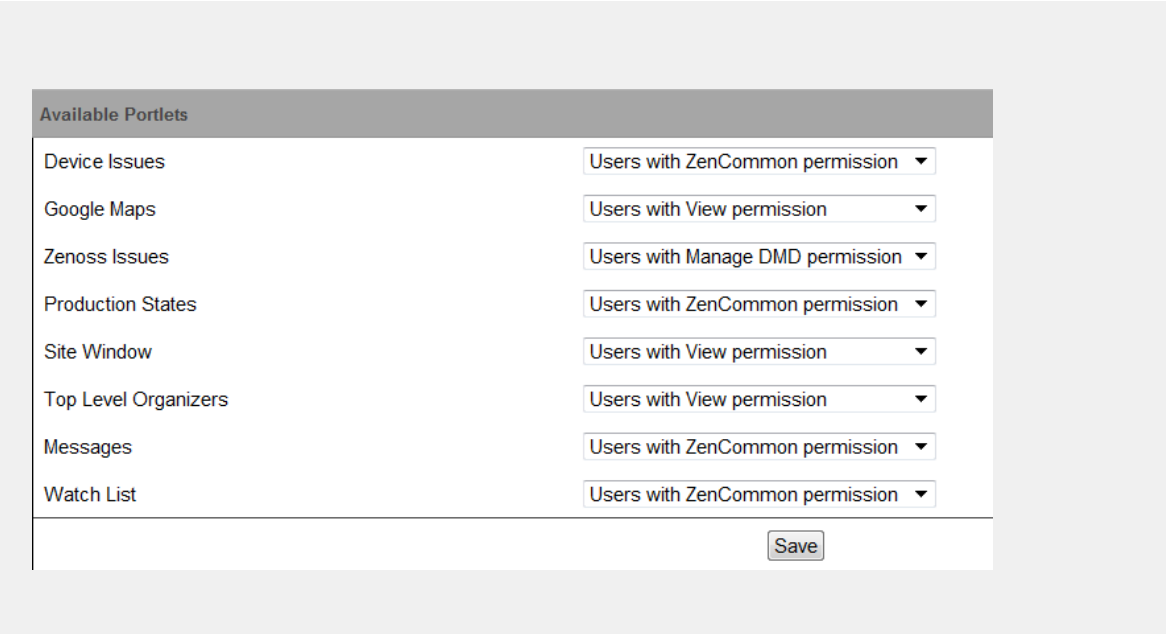
1. Select Advanced from the Navigation menu.

   The Settings page appears.

2 In the left panel, select Portlets.

The Portlets page appears.

Figure 53: Portlet Permissions



3 For one or more portlets in the Available Portlets list, select the permissions you want to apply.

4 Click **Save**.

Troubleshooting: Users Cannot See All Portlets

You may mistakenly block users from being able to access some portlets. Often, this happens when a user has been set to see only particular devices. By default, this user will see only portlets set to the ZenCommon permission level. In effect, this blocks three of six portlets.

To remedy this problem, you can:

- Change the permission levels (on the Portlets page) to ZenCommon, or
- Change the user role to a role higher than "No Role."

Backup and Recovery

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 do this periodically, to take regular "snapshots" of your instance to archive; or infrequently, such as to move data from one instance to another, or to restore a setup after performing a fresh installation. The system provides tools that enable you to manage these backup and restore tasks.

Note To ensure successful backup and recovery, you must use the `zenbackup` and `zenrestore` scripts. Manual backup of Cisco UCS Performance Manager data is not supported, and will not result in successful recovery.

With backup (`zenbackup`) and restore (zenrestore), the system includes:

- Events database
- Zope database, which includes all devices, users, and event mappings

- `$ZENHOME/etc` directory, which contains configuration files for the system daemons
- `$ZENHOME/perf` directory, which contains performance data

Note The remote hubs and collectors are not backed up when using `zenbackup.` You must set up a separate fileserver backup for these remote hubs and collectors.

Suggestions for a successful backup and restore experience:

- If you have the available disk space, tar and zip `$ZENHOME` before starting any backup or restore operation.
- Before running a backup or restore operation, run the `zenoss stop` command on the master and on all remote hubs and collectors.
- Avoid using these tools to go from a newer version of Cisco UCS Performance Manager to an older version.
- If you use these tools to go from an older version to a newer version, you should run `zenmigrate` after the restore operation.
- If restoring to a different installation (one that differs from the backup version), make sure file paths in the `$ZENHOME/etc/*.conf`files are appropriate for the new environment after you restore.

The following sections describe backup and restore scripts, as well as options for controlling their behavior.

Backup (zenbackup)

The backup script is `$ZENHOME/bin/zenbackup`. Typical use of `zenbackup` looks like:

```
> zenbackup --file=BACKUPFILEPATH
```

If the system is running then you can run `zenbackup` without any arguments. A backup file will be placed in `$ZENHOME/backups`.

Backup Options

The following table lists frequently used `zenbackup` options.

Note Use the `zenbackup --help` command to see a complete list of `zenbackup` options.

Option	Description
`--cacheservers=` *CacheServers*	Specifies memcached servers to use for the object cache (for example, 127.0.0.1:11211).
`--compress-transport=` *CompressTransport*	Compress transport for MySQL backup and restore. The default value is True. Set to False to disable over-fast links that do not benefit from compression.
`-C` *ConfigFile*, `--configfile=` *ConfigFile*	Uses an alternate configuration file.
`--dont-fetch-args`	Instructs `zenbackup`not to attempt to get values for `zepdbhost`, `zepdbport`, `zepdbname`, `zepdbuser`, and `zepdbpass` from `$ZENHOME/etc/zeneventserver.conf`. You must specify the options manually to access the events database.
`--genconf`	Generates a template configuration file.
`--genxmltable`	Generates a Docbook table showing command-line switches.
`--genxmlconfigs`	Generates an XML file containing command-line switches.

Option	Description
`--file=` *Filename*	Specifies a location for the backup file. By default, it is named `zenoss_` *Date*`.tgz` and placed in `$ZENHOME/backups`.
`-h, --help`	Shows help contents.
`--host=` *Host*	Host name of the MySQL object store.
`--logseverity=` *LogSeverity*	Set the logging severity threshold.
--mysqldb= *MySQLDB*	Specifies the name of the database for the MySQL object store.
`--mysqluser=` *MySQLUser*	Specifies the user name for the MySQL object store.
`--mysqlpasswd=` *MySQLPasswd*	Specifies the password for the MySQL object store.
`--no-eventsdb`	Disables saving the events database as part of the backup.
`--no-perfdata`	Disables saving performance data in the backup.
`--no-save-mysql-access`	Instructs `zenbackup`not to save `host`, `port`, `mysqluser`, `mysqlpassword`, `mysqldb`, `zepdbhost`, `zepdbport`, `zepdbuser`, `zepdbpass`, and `zepdbname` as part of the backup file. Use this to prevent your backup files from containing a MySQL user name and password.
`no-zodb`	Disables saving the ZODB database and installed ZenPacks in the backup.
`--port=` *Port*	Specifies the port of the MySQL object store.
`--stdout`	Tells `zenbackup`to send the backup information to standard output instead of to a file. Incompatible with `--verbose`.
`--temp-dir=` *TempDir*	Specifies a directory to use for temporary storage.
`-v, --verbose`	Prints progress messages. Incompatible with `--stdout`.
`--version`	Shows the program's version number.
`--zepdbhost=` *ZEPDbHost*	Specifies the ZEP database server host. By default, this is fetched from the system unless `--dont-fetch-args` is set.
`--zepdbname=` *ZEPDbName*	Specifies the ZEP database name. By default, this is fetched from the system unless `--dont-fetch-args` is set.
`--zepdbpass=` *ZEPDbPass*	ZEP database password. y default, this is fetched from the system unless `--dont-fetch-args`is set.
`--zepdbport=` *ZEPDbPort*	Specifies the ZEP database server port number. By default, this is fetched from the system unless `--dont-fetch-args` is set.
`--zepdbuser=` *ZEPDbUser*	Specifies the ZEP database user name. By default, this is fetched from the system unless `--dont-fetch-args` is set.

Create a Backup from the UI

To back up your system instance from the UI:

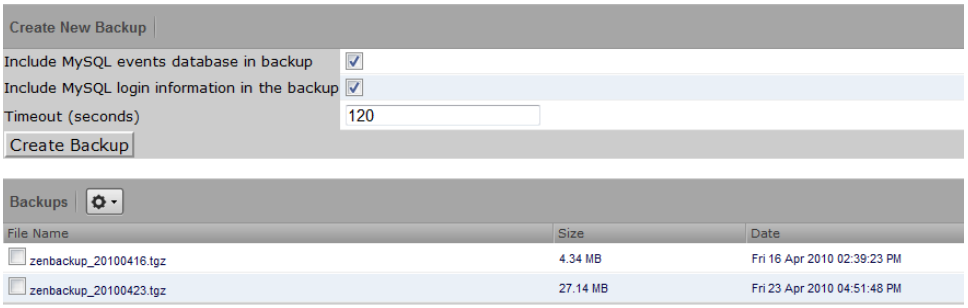
1 From the Navigation menu, select Advanced.

The Settings page appears.

2 In the left panel, select Backups.

The Backups page appears.

Figure 54: Backup



3 In the Create New Backup area, enter information or make selections for the backup. Options available are a subset of those available from the `zenbackup`command line tool.

4 Click **Create Backup**.

Delete a Backup

To delete a backup from the interface:

1 From the Navigation menu, select Advanced > Settings.

2 In the left panel, select Backups.

The Backups page appears. The Backups area lists all backup files in `$ZENHOME/backups`.

3 Select one or more files in the list, and then select Delete Backup from the Action menu.

4 Click **Delete** in the Delete Backup dialog to confirm the action.

Note Backup files can become large as your databases grow, so you may want to limit the number of backups you keep if drive space becomes an issue.

Remote Backups

Keeping backups on your server should help you recover if one of your databases becomes corrupt or your configuration becomes problematic. However, you should keep at least one recent backup file on a different server (ideally at a different physical location) in case a physical disk fails.

Restore (zenrestore)

The restore script is `$ZENHOME/bin/zenrestore`. Typical use of `zenrestore` looks like:

```
> zenrestore --file=BACKUPFILEPATH
```

Before restoring your system, run the `zenoss stop` command on the master and on all remote hubs and collectors.

Restore Options

The following table lists frequently used zenrestore options.

Note Use the `zenrestore --help` command to see a complete list of `zenrestore` options.

Option	Description
`--file`	This is a backup file created with zenbackup You must specify either `--file` or `--dir`.
`--dir`	The path to an unzipped backup file. You must specify either `--file` or `--dir`.
`--no-eventsdb`	Do not restore the events database. If the backup file does not contain MySQL events data then `zenrestore` will not modify your events database even if you do not specify `--no-eventsdb`.
`no-perfdata`	Disables saving performance data in the backup.
`no-zodb`	Disables saving the ZODB database and installed ZenPacks in the backup.
`-v, --verbose`	Print progress messages.

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

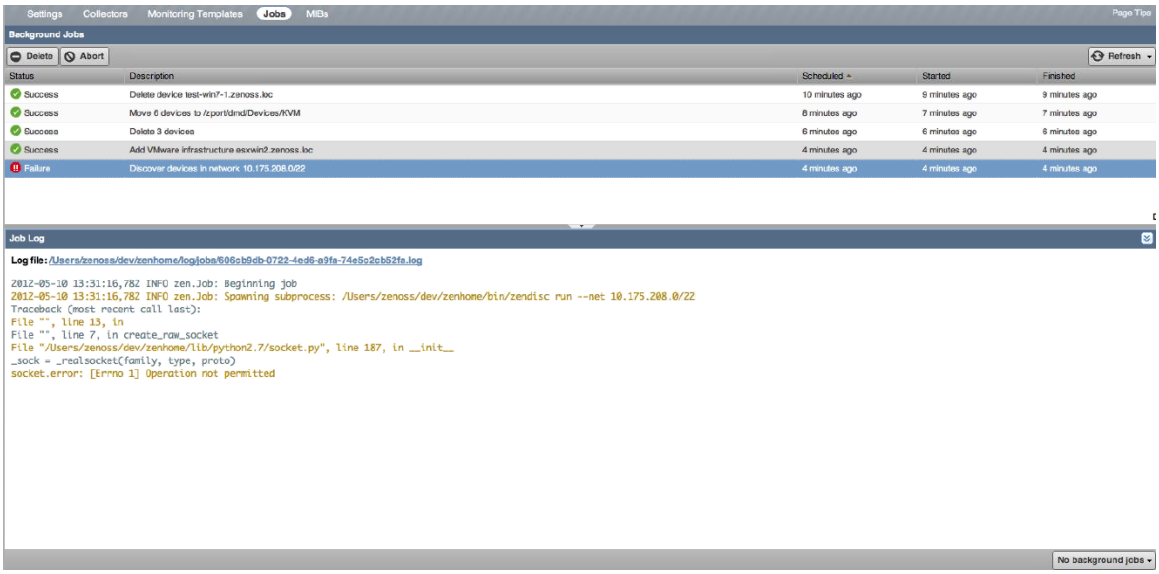
To access the Job Manager:

1 From the Navigation menu, select Advanced.

The Settings page appears.

2 In the left panel, select Jobs.

Figure 55: 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.

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**.

Configuring Jobs

You can determine, when moving devices, whether the action is performed immediately or as a job. By default, if you select five or more devices, the move action is performed as a job. To adjust this setting:

1 Select Advanced > Settings.
2 Select User Interface in the left panel.
3 Enter a value for Device Move Job Threshold, and then click **Save**.

Running the zenjobs Daemon

You can stop and start the `zenjobs` daemon from the command line, and from Advanced > Settings (Daemons selection).

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" '.*' '.*' '.*'
```

Versions and Update Checks

You can check to see if there is a newer version of Cisco UCS Performance Manager available. Click **Advanced > Versions** to view all of the software component versions installed.

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 application groups. 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.