CA Performance Center

Operator Guide

2.4.1

CA Technologies Product References

This document references the following CA Technologies products and components:

- CA Performance Center
- CA Infrastructure Management Data Aggregator
- CA NetQoS® Performance Center
- CA Single Sign-On
- CA Network Flow Analysis
- CA Application Delivery Analysis
- CA Unified Communications Monitor
- CA eHealth
- CA Spectrum

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Getting Started with CA Performance Center 7

About CA Performance Center 7
Key Terms and Concepts 8
Launch CA Performance Center 9

Chapter 2: Setting Up Your Environment 11

User Account Time Zones 11
Change Settings for Your Own User Account 12

Chapter 3: Using the Inventory Pages 13

Inventory of Managed Items 13
Inventory Pages 14
Performing Searches 15
- Search for a Managed Item 15
- Narrowing a Search with Filters 16

Chapter 4: Reporting 17

Dashboards and Reports 17
- Viewing Data in CA Performance Center 18
- Open a Dashboard Page 19
- Types of Report Pages 19
- Factory Dashboards 20
- Context Page Navigation 20
- Device Name Display 20

View Options 21
- Change the Time Frame for a Dashboard 22
- Zoom in to Narrow the Time Frame 24
- Set a Custom Time Frame 25
- Change the Context for a Dashboard 25
- Change the Data Context for a View 26

Sharing Data with Other Users 27
- Print a Report 28
- Send a Report by Email 29
- Set Up a Recurring Email Schedule 30
- Manage Email Schedules 32

Generate a URL for a View 32

Chapter 5: Events 35

Events 35
Event Types 35
Event List View 36
Event Details 37
Event Properties 38
Manage Event Retention 39
Notifications 40
EventManager Format Usage for Traps 42
nhLiveAlarm Format Usage for Traps 43

Chapter 6: Working with Groups 47

Groups 47
Types of Groups 48
Groups for Multi-Tenant Deployments 49
Create Your Own Custom Groups 51
Add Managed Items to a Group Manually 52
Add Managed Items to a Group Using Rules 53

Glossary 57

Index 61

Chapter 1: Getting Started with CA Performance Center

This section contains the following topics:

[About CA Performance Center](#) (see page 7)
[Key Terms and Concepts](#) (see page 8)
[Launch CA Performance Center](#) (see page 9)

About CA Performance Center

CA Performance Center is a web-based reporting interface that helps you effectively manage your physical and virtual networks, applications, and devices. CA Performance Center dashboards and reports present performance data from network and systems-monitoring products. You can compare large amounts of statistical data from multiple sources in one web page.

CA Performance Center takes a "performance-first" approach to application service delivery. This approach places end users in the primary role. To understand how well an IT organization supports application delivery to users, you must capture and analyze data from applications, devices, and the network.

CA Performance Center offers role-specific views of application response times, traffic composition, infrastructure health, and flow-based diagnostics.

Key Terms and Concepts

To use CA Performance Center effectively, familiarize yourself with the following terms and concepts:

Data Sources

Data sources are the supported products that provide performance and configuration data to CA Performance Center. Data source products that monitor, collect, and aggregate data can often function independently. However, once they are registered to an instance of CA Performance Center, they are known as data sources.

Dashboards

Dashboards are dynamic report-building pages within the CA Performance Center user interface. They appear as menu items that are accessible from the Dashboards tab. Each dashboard is a collection of views that present data from registered data sources on a single web page. The layout, views, time interval, and group context of each dashboard can be customized.

Reports

Reports are static output from an on-demand selection or an exported dashboard page. Reports that you export from a dashboard create a static data set from the data and information in the associated dashboard. On-demand reports capture a data set from a single managed item or group in the Inventory. You can print reports, send them by email, or export them in CSV or PDF format. For each format, the report captures a selected data set.

Views

Views, or *data views*, present statistical data, usually in a graph or table format. Each view represents a discrete set of collected data. Depending on your user account role rights, you can add and edit individual views or remove them from a dashboard page. In some cases, you can export the data to a file in CSV format.

Tabs

Tabs are the prominent links across the top of the CA Performance Center interface that let you view dashboards and open administration tools. For example, the Dashboards tab lets you select a dashboard page to view from a menu.

Menus

Menus are segments of the Dashboards tab that are used to organize dashboards by their content. By default, Administrators and Designers can customize menus and assign them to user account roles.

CA Performance Center also provides factory (predefined) menus for particular types of roles, such as a manager or engineer.

Roles

The *role* is a parameter assigned to a user account that controls user access to product features and dashboard pages. Based on user job functions, the role grants administrative access to product configuration using *role rights*. Roles let users access data and product features that they require to perform their duties and restrict access to features that they do not require. Roles can be defined differently in the data sources than in CA Performance Center. However, they are shared among data source products registered to the same CA Performance Center instance.

Groups

A *group* is a filter definition that functions as a container for managed items. Groups let you logically organize managed items in a tree structure, with each group containing subgroups or managed items. The structure is propagated to the data sources, where it enables drilldown from top-level groups into data from an increasingly narrow but related context.

Launch CA Performance Center

Once you have run the CA Performance Center Setup program and the installation has completed, you can launch the console program from a web browser.

Follow these steps:

1. Open a web browser.
2. In the address field, enter the following address:

   `http://<server IP address>:8181/pc/desktop/page`

   <server IP address>

   Is the IP address of the computer where you installed the software.

   8181

   Is the port number.

   The browser displays the Login page.
3. Type your CA Performance Center username and password in the fields provided.
4. (Optional) Select 'Remember me on this computer' to remain logged in beyond the timeout period that the administrator has set.
5. Click Log In.

   The CA Performance Center console opens to your home dashboard.

Chapter 2: Setting Up Your Environment

This section contains the following topics:

User Account Time Zones (see page 11)
Change Settings for Your Own User Account (see page 12)

User Account Time Zones

The time zone setting for each user account determines the time zone that is applied to dashboards. This setting applies to all dashboards viewed while the associated operator is logged in to CA Performance Center.

An appropriate time zone is set for a user by the administrator when the user account is created. Typically, the time zone matches the locale of the computer that the operator uses to access CA Performance Center.

If the role for your user account has the required role right, you can change the time zone for your own user account.

Change Settings for Your Own User Account

The time zone associated with each user account determines how data is displayed in dashboards and views. The administrator usually sets the time zone and preferred language for each user during user account creation. The time zone should match the locale of the computer that the operator uses to access CA Performance Center.

If your user account has the required role right, you can change the time zone and other parameters for your own user account.

Follow these steps:

1. Log in to your user account.
2. Click the name of your user account where it appears in the upper right corner of the console user interface.

   The User Settings dialog opens.

   Your role rights determine the parameters that you can change for your own account.
3. Select the appropriate language for your account from the Preferred Language drop-down list.
4. Supply your email address in the Email Address field.
5. Select the appropriate time zone from the Time Zone list.

   Note: The default time zone is UTC (Coordinated Universal Time).
6. Change your default reporting group by selecting another group from the drop-down list.

   The list only includes groups from your permission groups.
7. Change your password by first typing in your current password.
8. Supply a new password. Then type the new password again to confirm it.
9. Click Save to save your changes.

Chapter 3: Using the Inventory Pages

This section contains the following topics:

Inventory of Managed Items (see page 13)
Inventory Pages (see page 14)
Performing Searches (see page 15)

Inventory of Managed Items

The Inventory page is available from the Inventory tab. The Inventory contains a list of all items that all data sources discover and monitor, called *managed items*. Managed items of all types, such as applications, devices, or interfaces, appear in list views on Inventory pages. Use the Inventory to create on-demand reports.

A 'Consoles' section of the page contains a list of links to any registered data sources with separate consoles. The necessary product privilege to each data source is required for access.

The Inventory list shows only categories of items currently available to CA Performance Center from the registered data sources. Further, it only displays items that are members of the groups in your user account permission set. The categories are links that let you access filtered lists that show all managed items of the selected type.

The list pages provide minimal information to identify each item, such as device hostnames or IP addresses. Select a check box to enable on-demand reporting for a managed item.

If multiple data sources monitor a single managed item, CA Performance Center reconciles its identity and creates a single item in the Inventory.

More information:

Performing Searches (see page 15)
Inventory Pages (see page 14)

Inventory Pages

The Inventory tab lets you access lists of managed items, which are organized by type. Inventory pages and views provide high-level information to help you identify managed items and groups of items, facilitating troubleshooting. Select a check box to enable on-demand reporting for a managed item.

Items in the Inventory are organized into the following categories:

- Groups and Sites
- Devices and Servers
- Interfaces
- Interface Addresses
- Device Components

Additional categories are available based on the data sources that are registered:

eHealth Elements

Devices or resources (such as routers, servers, interfaces, modems, or applications) for which CA eHealth collects and analyzes data to generate reports.

Applications

Combinations of servers and port numbers that are defined for monitoring with CA Application Delivery Analysis.

Networks

Ranges of IP addresses that are defined as networks for monitoring with CA Application Delivery Analysis.

Voice Interfaces

Interfaces from voice gateway devices or other media devices that CA Unified Communications Monitor discovers and monitors.

VoIP Locations

CA Unified Communications Monitor Locations, which are created to organize report data from unified communications systems.

Inventory categories are also divided into individual list views that appear by default on relevant dashboards. These views let you drill down into item context pages from related dashboards.

A "Consoles" section contains hyperlinks to the management consoles of registered data sources that are installed on separate servers.

Performing Searches

Some deployments scale to hundreds of thousands of managed items. Multiple search features help you locate data for specific items or groups of items.

If your user account has the required role right, you can begin your search from the Inventory tab. On this tab, you can view a list of managed item types. Click a link to see a list of items. Then search among the items themselves in the list using the search field and the sorting and paging features below the list view.

Inventory and Search Results pages also provide access to on-demand reports.

Note: The ability to view the Inventory and perform a global search is granted to individual operators with their role. Only users with the 'View Inventory and Search' role right can view the Inventory tab.

Perform a global search using the search field at the top of any page. This type of search scans all items in the database, across all data sources. A global search returns lists of all items in the Inventory that match your search, sorted by item type. Filtering the results further is also supported in each view. For more information, see Narrowing a Search with Filters (see page 16).

A more limited search feature is available for table views and does not require a special role right. The search that you perform from a table footer filters out managed items that would otherwise appear in that view. No items from other views or dashboards are displayed.

Search for a Managed Item

You can navigate directly to contextual information about a single managed item, such as a router or server that seems to be associated with a network issue. Search fields for data views let you search for items within selected views. Within the search results, you can click a link to see data views filtered by a selected item (Context pages).

Follow these steps:

1. Navigate to a dashboard page (see page 19) where you want to begin your search.
2. Enter a search string in the search field, and click Enter.

   You can supply a text string, a search string containing numbers, or a combination of both.

   The search results are displayed within categories of similar items. The item type is indicated.

3. Click one of the items in the list with a type of Server.

   A Server Context page for the selected item opens.

   The Details tab is selected by default. This page provides more data to identify the server, including its manufacturer and model, its group context, and the SNMP information associated with it.

   The group context information on this tab helps you to locate the server.

More information:

Narrowing a Search with Filters (see page 16)

Narrowing a Search with Filters

You can narrow or broaden the searches that you perform by adding a wildcard character or filter text to the Search field. Filters can be applied to a global search or to a view-level search.

You can use an asterisk (*) as a wildcard character in your searches. For example:

- “serv*” returns all the rows with entries starting with “serv”.
- “*erver” returns all the rows with entries ending in “erver”.
- “*server*” is the same as “server” and returns all the words that contain the word “server” - such as my_server, or server1, or just server.
- “ser*ver” finds all the words that start with “ser” and end with “ver” including “server”.

You can add multiple search words to narrow the search further. For example, if you search for devices using the search string “server 192.168*”, the search returns all servers on the 192.168.0.0/16 network.

If your environment contains many managed items, such as 4 million servers, we recommend filtering global searches. Otherwise, a limit on each global search preserves user interface performance.

Chapter 4: Reporting

This section contains the following topics:

Dashboards and Reports (see page 17)
View Options (see page 21)
Sharing Data with Other Users (see page 27)

Dashboards and Reports

Dashboards are dynamic report-building pages within the CA Performance Center user interface. They appear as menu items that are accessible from the Dashboards tab. Each dashboard is a collection of views that present data from registered data sources on a single web page. The layout, views, time interval, and group context of each dashboard can be customized.

Note: Your user account role rights determine the dashboards that you can see.

Reports are static output from an on-demand selection or an exported dashboard page. Reports that you export from a dashboard create a static data set from the data and information in the associated dashboard. On-demand reports capture a data set from a single managed item or group in the Inventory. You can print reports, send them by email, or export them in CSV or PDF format. For each format, the report captures a selected data set.

Dashboards are organized in menus. *Menus* are segments of the Dashboards tab that are used to organize dashboards by their content. By default, Administrators and Designers can customize menus and assign them to user account roles.

CA Performance Center offers a set of factory dashboards and menus, which are available for use immediately after registering data sources. Users with the required role rights can also extensively customize dashboards, menus, and views to create a custom system for individual operators.

The menus and dashboards that are available to you are displayed when you hover over or click the Dashboards tab.

Viewing Data in CA Performance Center

Dashboard pages display dynamic views of data that CA Performance Center receives, interprets, and formats from registered data sources. *Views*, or *data views*, present statistical data, usually in a graph or table format. Each view represents a discrete set of collected data. Depending on your user account role rights, you can add and edit individual views or remove them from a dashboard page. In some cases, you can export the data to a file in CSV format.

View placement on dashboard pages is flexible. Users with the required role rights can customize dashboards. They can, for example, place views of application performance data next to views of volume data to help troubleshoot issues from a single page.

The predefined dashboards are organized into workflows. Hyperlinks let you drill down from Top N views to more detailed metrics from a narrow context, such as an individual device. Built-in workflows direct you to data that is related to the metric you are reviewing. For example, you can see a view of discards when you drill down from a view of interface utilization.

Create custom groups to display data for a specific set of sites, devices, or interfaces. You can apply these groups to dashboards using the group selector (the 'change' link at the top left). You can change the “context” of the dashboard to analyze data for specific groupings. You can also select a managed item or a group of items and rapidly generate an on-demand report for a selected metric family and time frame.

Views that show data for a group contain rollups of data from data sources. Views of data for a single managed item often provide a drilldown path directly to the data source. The Single Sign-On feature lets you navigate from a dashboard to a data source interface if your user account has the 'Drill into Data Sources' role right.

More information:

Dashboards and Reports (see page 17)

Open a Dashboard Page

You can access the CA Performance Center reporting interface from the Dashboards tab. Dashboards are customizable pages that contain views of data from various sources. If your role rights permit it, you can export the current dashboard as an email message or as a PDF.

When you log in to CA Performance Center, the first page you see is the default dashboard.

Follow these steps:

1. Use the mouse pointer to hover over the Dashboards tab on the main toolbar.

   A series of menus that correspond to reporting categories appears.

   Note: Only menus that are assigned to your user account role appear.

2. Select a dashboard from one of the menus.

   The page refreshes to show the dashboard.

   By default, the views on the page reflect the most recently collected data.

Types of Report Pages

Two categories of dashboards are available by default or through customization:

- *Summary pages* provide high-level information, such as averages from groups of managed items. Summary dashboards often provide a drilldown path to more detailed, related pages from a selected context.
- *Context pages* provide specific, focused performance or status data from a narrow context, such as a single router or server. These pages are available as drill-down links or tabs from Summary dashboards.

To drill in to a detailed view from a Summary dashboard, take one of the following steps:

- Right-click the item to select the context page that you want to see.
- Click the item to open the default context page.

Note: Your role rights must include the ability to Drill into Views.

Default sets of context pages are available for individual devices, interfaces, and servers. These pages include a set of customizable tabs that let you access more specific context data for a selected managed item. For example, the Router context includes tabs for Health, Utilization, and Error data.

Factory Dashboards

In addition to custom dashboards that the administrator has created, multiple factory (predefined) dashboards are available. When you log in, you see all dashboards in the menus that have been assigned to your user account. View the full list of dashboards that you can access by hovering on the Dashboards tab.

When you register a new data source, it sends its own set of factory dashboards. If your user account has the required role rights, you can edit dashboards and can save the changes to your own user account.

The dashboards you create or modify appear in your My Dashboards menu.

Context Page Navigation

You can frequently access more information about individual managed items from dashboards. Most dashboards are composed of views of summary data, such as hourly rollups or averages from a group of items. If additional data is available from the data source, you can click linked items on the dashboard page to drill down into *context pages*.

Note: The role right to Drill into Views is required.

The views on context pages show filtered data from a narrow context, such as a view of data from a single managed item. Use the links to drill down into specific data and home in on the source of a performance problem.

In data views from some data sources, you can also right-click the name of an item in a table view to access a menu. For example, right-click the link that corresponds to an item name in the Inventory section. A menu lets you select a related context page, containing more granular data.

Finally, some context pages include tabs to additional pages of detailed data. Click a tab to see data that has been filtered by a selected managed item or type of item.

Device Name Display

Users with the predefined Administrator role can define aliases for device names. The alias is then displayed, where appropriate, in CA Performance Center views.

A device alias is a user-configured name that is applied to the associated managed item in CA Performance Center. If an alias is not defined, the discovered device name is displayed. If the alias is used, you can still view the discovered names on the Details tab of the Interface or Device Context pages.

View Options

Many views offer a search feature and other settings that you can change to modify the view. In addition to filtering and time frame (see page 25) options, the following options are available for most data views:

- Editing view settings  , such as changing its title or severity categories.
- Seeing more data by selecting another "page" of a table view.
- Increasing or decreasing the number of items that are shown per "page".
- Collapsing the view so that the data is hidden.
- Changing the managed item context (see page 26) for the data shown in the view.

  Note: Users with the 'Save Changes to Shared Views' role right can save view modifications to their own user account. The changes persist after logout. However, other users cannot see changes to views.

Other view options are specific to the selected view. The available options depend on the format and data source.

Trend View Options

The trend views that are available in context pages let you quickly and easily change the trend lines that are displayed on the graph. The following options also apply to multitrend views:

- Right-click a metric in the chart legend and select Hide to remove it from the view.
- Exclude all other metrics by right-clicking a metric in the legend and selecting Focus.
- Narrow the focus to a precise time frame using the zoom feature (see page 24).

Trend views also include an option to add a "goal line" as a visual indication of performance levels or thresholds. You can supply any value or label for the goal line, and you can show or hide the goal line for a selected trend view.

Table View Options

In table views, you can drill down to detailed data for individual items. Use the page feature to see metrics from a longer list of items. Increase the Max Per Page value to increase the size of the view and the number of table rows per page.

You can sort table data columns by selected metrics and also select columns to include. Click a table column to sort. A white arrow on the column lets you access a menu of table column options. Select Columns to enable and disable the metrics that were enabled for the table by default.

Browser View Options

The *browser view* is a unique view type that lets you add a URL to a selected report page. You can use this view to compare external factors alongside your network performance views. Also, the browser view lets you update internal and external data dynamically. The URL must be for a web page that supports embedded iframes.

Multiple external factors can affect the performance of your network and servers, such as world events and adverse weather conditions. The ability to view a weather map and news headlines alongside performance data views on a single report page can help you better understand patterns in network performance.

Device Admin Option

When a view does not display Data Aggregator data, this option lets you drill down directly to the Data Aggregator Admin page to troubleshoot monitored devices and items.

More information:

Change the Data Context for a View (see page 26)
Generate a URL for a View (see page 32)

Change the Time Frame for a Dashboard

You can change the time frame for a dashboard you are viewing. Change the time frame to see performance data from an earlier time of day or from another date.

Changing the time frame is useful for troubleshooting performance issues. For example, if data from the past day contains an anomaly, you can change the time frame to show data from the last seven days. The time frame helps you determine whether the same issue is occurring regularly.

When you change the time frame for a dashboard, it is applied to all views on the page, and to all dashboards in that window. However, you can view dashboards in multiple windows and can apply a different time frame to each dashboard.

Follow these steps:

1. Select a dashboard from the Dashboards tab.
2. Click to select some of the following time and date options on the toolbar:

   Time period drop-down list

   Lets you select a predefined time frame for the data.

   Default: Last Hour.

   Back button

   Shifts the time frame for the data back by one increment of the present interval (such as Last Day or Last Hour).

   Date and Calendar drop-down lists

   Let you select a start and end date for the data from a calendar view.

   Time of Day drop-down lists

   Let you select a start and end time from a list of 15-minute time intervals in the 24-hour format.

   Forward button

   Shifts the time frame for the data forward by one increment of the present interval (such as Last Day or Last Hour).

3. To define a custom time frame, take one or more of the following steps:
   - Click the start date and select a new start date from the calendar that appears.
   - Click the end date and select a new end date from the calendar that appears.
   - Click the start hour or minute and select a new hour or minute from the drop-down menu.
   - Click the end hour or minute and select a new hour or minute from the drop-down menu.
4. Click Set.

   The page is refreshed, and the data displayed in the views reflects the new time frame.
5. (Optional) Scroll backward or forward in time. Use the Back and Forward buttons on either side of the timestamp to shift the time frame by one increment of the present interval.

   If you are viewing data for the last day, click the left arrow to scroll back in time by one day. Or click Latest to see the most recently collected data.

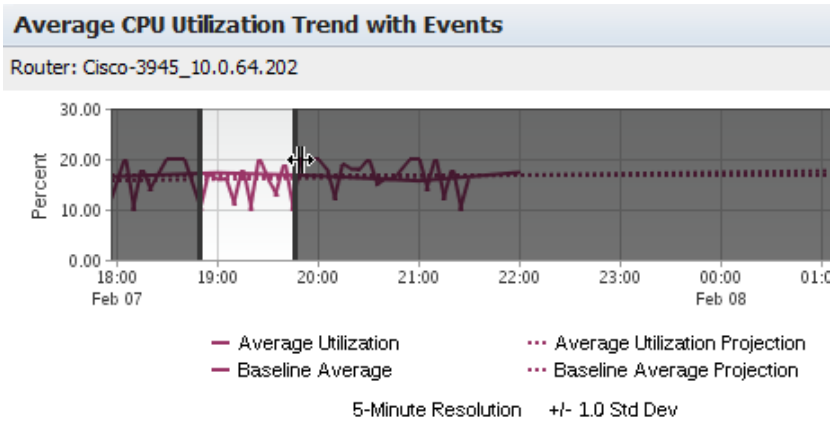
Zoom in to Narrow the Time Frame

You can look more closely at the data points from a small range by using the zoom feature. The ability to "zoom in" on a time frame is available for views that contain trend (line) charts. The feature is not available for bar charts, tables, or gauges.

Follow these steps:

1. Navigate to a dashboard page (see page 19).
2. (Optional) Change the time frame, if necessary.
3. Select a view that contains a line chart.

   Note: You cannot zoom in on a bar chart, table, or gauge.
4. Click and drag, using the mouse to select an area of the chart.



   Select an area that spans at least 30 minutes. Black lines appear to indicate a valid selection.

   When you release the mouse button, the custom time period you selected is applied to the current view.
5. (Optional) Click Undo, just below the view, to return to the previous time frame.

   The view is refreshed. The previous time period is now applied to the view.
6. (Optional) Click Apply to Dashboard.

   The dashboard page is refreshed. The new time period is now applied to all views on the current dashboard page.

Set a Custom Time Frame

You can select a precise time frame for the performance data shown in the current dashboard. You can select the day, the start time, and the end time using the time period selectors.

Follow these steps:

1. Navigate to a dashboard (see page 19).
2. Click the date links in the upper-left corner of the dashboard page to open the calendar panes.
3. Select the beginning day and ending day of the new time period on the calendar panes.
4. Click the hours or minutes links to specify the beginning and ending times of the new time period.
5. Click Set.

   The custom time frame is applied to the dashboard you are viewing.

Change the Context for a Dashboard

You can customize a dashboard by selecting a different data context for the data. The default group setting for the views that are shown on all dashboards is 'All Groups'. When you select another group for a standard dashboard, you apply a new filter to all views on the page. From a context page, such as details about a single router, you can select another managed item as the view context.

You can also view dashboards in multiple windows and apply a different data context to each dashboard.

Follow these steps:

1. Navigate to the dashboard that you want to modify.
2. (Optional) Change the time frame, if necessary.
3. Click the [change] link above the time period selectors.

   [change] link

   Lets you select another group or managed item context for reporting.

   A dialog opens with filtering options.
4. Click to select another managed item. Or expand nodes in the Groups tree to select a group context.

   Data from the new item or group appears in the view.

5. Click OK.

   All views on the page are refreshed to reflect the new data context. The change applies until you log out. To change the context so that the change persists across login sessions, edit the dashboard.

6. (Optional) Open another browser instance, log in, and open the same dashboard.

   You can now compare the same views with two different item context settings.

More information:

Change the Data Context for a View (see page 26)

Change the Data Context for a View

You can change the context for a single view on a dashboard. The default group setting for the views that are shown on all dashboards is 'All Groups'. However, you can change the page-level context to filter using any other group.

Filters that are appropriate for each type of view drive the context for a view or page. Change the context to show data from a different managed item or from a different set of managed items.

Changing the context for a view is useful for troubleshooting performance issues. For example, assume that a view does not show performance data that appears to correlate with a problem you are investigating. You can select another managed item to compare data from the same time frame. You can edit a view of disk utilization for physical servers to show disk utilization for Virtual Machines instead. Or you can compare data from different geographical regions by leveraging your group structure to change the group context.

Follow these steps:

1. Open the dashboard that contains the view that you want to modify.
2. (Optional) Change the time frame, if necessary.
3. Click the Edit icon  in the view whose context you want to change, and select Edit from the menu.

   The View Settings dialog opens.

4. Change the view Title or Subtitle to reflect the new context.

   The context types that are available depend on the type of view.

5. Take one of the following steps, depending on the context type you selected:

   - Click to expand folders in the Groups filter tree, and select the group whose data you want to see in the view.
   - Locate the managed item whose data you want to see in the view, and click the link in the table.

6. Select the scope of your changes from the Apply Changes drop-down. Select one of the following options:

   - For All Tenant Users: Saves the changes so that they are only available to users associated with your tenant (possibly the Default Tenant).
   - My User Account: Saves the changes to your user account as a default for this view.
   - My Current Session: Reverts the changes when you log out.

   Note: The availability of these options depends on your user account role rights.

7. Click Save.

   The view is updated with data from the new context. The lock icon  and the name of your selected context appear in the view subtitle. The icon indicates that this view is fixed to the selected context, and no longer follows the context set for the dashboard page.

   To change the context of a view back to page-level context, select 'All Groups' in step 5 in these instructions.

You can also change the context for a dashboard (see page 25), which applies the selected group or managed item as a filter to all views on the page.

Sharing Data with Other Users

Multiple options let you share dashboards and views with coworkers. You can export a dashboard to a static report in PDF format. You can set up schedules to send reports automatically on a regular basis.

You can also export individual views. Publish views on a web page, such as an intranet site. Or export data from a view to a file in CSV format. For all data-export options, certain user account role rights are required.

Print a Report

If your user account has the required role right, you can export the current dashboard contents as a printed report. The Print feature first displays the current dashboard page in PDF format.

Follow these steps:

1. Navigate to the dashboard (see page 19) that you want to export as a report.
2. (Optional) Change the time frame (see page 22).
3. Click the Print link on the toolbar.

   The report is exported as a PDF. Typically, it is displayed in a separate browser window.

   The data uses the current dashboard settings.
4. (Optional) Save the PDF to the local computer using the options in your PDF viewer.
5. Click the Print icon in the browser toolbar.

   The report page is sent to the local default printer.

Send a Report by Email

If your user account has the required role right, you can export the current dashboard contents as a report attached to an email message. The Email feature lets you specify the email address of the recipient and also the Subject line of the email message. The report is attached to the message as a document in PDF format.

To send reports by email, your user account must have a role with the 'Send Reports by Email' role right. The administrator must also configure an email server.

Follow these steps:

1. Open the dashboard that you want to send in an email message.
2. (Optional) Change the timeframe, if necessary.
3. Click the Email icon on the toolbar.
4. Supply information for the following fields:

   Send To

   Specifies the email addresses where the report should be sent. Use the standard format:

   <name>@<domain>

   Note: Use commas or semicolons to separate multiple addresses. Or you can enter an email alias that includes multiple recipients.

   Subject

   Appears in the email Subject line; describes the emailed report.

   Example: The dashboard title and any components whose data is included in the report.

   Message

   (Optional) Is a message to accompany the emailed report.

5. Click Send Now to send the message immediately.

   Or select Send on a Schedule to create a schedule to send the email message on a regular basis. For more information, see Set Up a Recurring Email Schedule (see page 30).

6. Click OK.

   The CA Performance Center server generates a PDF from the current dashboard and sends the report as an attachment to an email message.

Set Up a Recurring Email Schedule

Each dashboard contains options to export and send data in reports. Your user account must have the 'Send Reports by Email' role right.

You can send a report by email immediately, or you can create a schedule for recurring emailed reports. For example, you can email interface utilization reports each week to coworkers in the IT department for capacity planning.

Note: The administrator must specify an email server to enable this feature.

Follow these steps:

1. Log in to CA Performance Center and select a report from the menus on the Dashboards tab.
2. Click Email.

   The Email Dashboard dialog opens.
3. Complete the following fields:

   Dashboard

   A read-only field that identifies the name of the dashboard. The dashboard name appears in the filename of the report that is attached to the email. The dashboard name also appears in the Dashboard column in the list of email schedules on the Manage Scheduled Emails (see page 32) page.

   Send To

   Specifies the email addresses where the report should be sent. Use the standard format:

   <name>@<domain>

   Subject

   Appears in the email Subject line; describes the emailed report.

   Example: The dashboard title and any components whose data is included in the report.

   Message

   (Optional) Is a message to accompany the emailed report.
4. Select one of the following Scheduling Options:

   Send Now

   Sends the email message immediately.

Send Daily

Sends the email message once per day. If enabled, reveals check boxes where you can select the day of the week when the report is sent.

Default: Send the emailed report every weekday (Monday - Friday) at 0:30 hours in the time zone of the logged-in user. The data in the report reflects the previous 24 hours.

Send Weekly

Sends the email message once per week. If enabled, lets you select the day of the week to send the report.

By default, the weekly schedule sends the emailed report every Sunday at 01:00 in your timezone.

Default: The data in the report reflects the previous seven days (Saturday - Sunday).

Week Ends on

Determines the day when the week ends. The start of the week is automatically adjusted to include seven days.

Send Monthly

Sends the email message once per month. Sends the report on the first Sunday of each month at 01:00 in the time zone of the Management Console. The data in the report reflects the previous 30 days.

Send Email at

Determines the time of day when the message is sent. The start of the month is automatically adjusted to include 30 days.

Send Quarterly

Sends the email message once per quarter. Sends the report on the first Sunday of each quarter at 01:00 in the time zone of the Management Console. The data in the report reflects the previous three months.

First Quarter Ends in

Determines the month when the quarter ends. The start of the quarter is automatically adjusted to include three months. All other quarters are also adjusted to proceed from the first quarter.

Send Yearly

Sends the email message once per calendar year. Sends the report on the last day of the month you select for the 'Year ends in' parameter. The data in the report reflects the previous 12 months.

Year Ends in

Determines the month when the year ends. The start of the year is automatically adjusted to include 365 days.

Send email at [time of day]

Sends the email message at a time you select.

5. Click Save to save the schedule.

   The report is saved as a PDF file and attached to an email message. It is sent immediately or according to the schedule you selected.

Manage Email Schedules

Users with the required role rights can set up schedules to send reports by email on a recurring basis. Selected dashboard data is exported in report format and sent to designated users according to a regular schedule.

Users who have the role right to schedule emails can also manage email schedules for other users.

Follow these steps:

1. Log in as a user with the role right to 'Send Reports by Email'.
2. Select Admin, System Settings, and click Scheduled Emails.

   The Manage Scheduled Emails page opens.

   The page displays the current list of email schedules.

   Note: Tenant administrators only see the items that are associated with their tenant.
3. Select the email schedule that you want to change, and click Edit.

   The Email Dashboard dialog opens.
4. View or change the settings for email schedules. For more information, see Set Up a Recurring Email Schedule (see page 30).
5. Click Save.

Generate a URL for a View

You can export a view and share it with coworkers who do not have access to dashboards. CA Performance Center can generate a special uniform resource locator (URL) to recreate a selected data view on demand. The URL lets you add the view to a web page or intranet site to share performance data with coworkers. The Generate URL feature lets you involve others in capacity-planning and infrastructure upgrade decisions and lets you share status information.

A security token is included with each URL. This token is based on the user who is logged in at the time of URL generation. Consequently, any user who can access the exported view can see the same data that the original user who exported the URL could see. Note, however, that the token applies only to the initial view. If the user who is accessing the exported view attempts to drill in, he or she is asked to authenticate. The drilldown only succeeds after successful authentication, and then only for a user account with the Drill into Views role right. Finally, an option is included to let the token (and thus, the view) expire after a selected time period.

Follow these steps:

1. Log in as a user with the 'Generate URLs from Views' role right.
2. Navigate to the dashboard that contains the view for which you want to generate a URL.
3. Click the Edit icon  on the view, and select Generate URL.

   The Generate URL dialog opens. The URL is displayed in the URL field.
4. Enable or disable the following required parameters for the exported view:

   View Container

   Displays the chart or graph with a surrounding container. The container includes the title of the view in a title bar and a black outline around the chart or graph.

   Default: Enabled

   Copyright

   Shows the copyright information for the web page in the view if enabled.

   Drill Down

   Enables users to drill down from the view into the underlying data source for more detailed data. These users must have a minimal product privilege to the data source and the 'Drill into Data Sources' role right to use this feature.

   Default: Enabled.
5. Select from the following time frame options:

   Time Options

   Let you change the time frame for the data in the exported view. Supply a custom time frame in the Start Time and End Time fields, or select a Time Range from the drop-down list.

Token Expiration Options

Control view expiration. The default, 'Never' expires, lets the exported view display indefinitely.

If you want the view to expire, select a timeout period from the Token Expiration list. The URL includes an encrypted token that causes the view to expire after the specified timeout period.

The token does not enable the user who interacts with the generated view to drill down for more data.

6. (Optional) Click Preview to see how the view looks with the options you have selected.
7. Copy the URL displayed at the top of the page to the Clipboard.
8. Paste it to the destination where you want to display the view.
9. Click OK.
10. The Generate URL window closes.

Chapter 5: Events

This section contains the following topics:

Events (see page 35)
Event Types (see page 35)
Event List View (see page 36)
Event Details (see page 37)
Event Properties (see page 38)
Manage Event Retention (see page 39)
Notifications (see page 40)

Events

An *event* is a message that is triggered by an instantaneous occurrence in your networking infrastructure, usually indicating that something significant has occurred. Events are reported for several reasons. They are reported when data exceeds a threshold or when configuration changes are detected. View a list of events on the Events Display dashboard.

When data that triggers an event is reported, the Event Manager component of CA Infrastructure Management processes the event data. The Event Manager is integrated with CA Spectrum. As a result, events typically generate an alarm that can be viewed in CA Spectrum. The severity level assigned to each event depends on event configuration in CA Spectrum.

Events provide information for monitoring the health and status of your networking environment. Each event includes useful data for troubleshooting.

Event Types

Each event includes an event type and often includes an event subtype. This information helps CA Infrastructure Management process events according to a set of rules. You can configure these rules in CA Spectrum to make sure you are informed about the status and health of your infrastructure.

Events can be categorized as the following types:

- Poll events—Result from polling or the analysis of poll data.
- Trap events—Result from trap inputs.
- Threshold event—Triggered by threshold violations on devices. Administrators can configure thresholds in CA Spectrum.

- Configuration change—Reports on items that are created, removed, or modified.
- Unknown event—Indicates an event of unknown origin.
- Any—Represents a wildcard event type that notifies you about every event submitted to the Event Manager.

Administrators can also define custom event types in CA Infrastructure Management administration.

Event List View

The Events view contains a list of recently reported events.

By default, the Events view contains the following information:

Date/Time

Are the date and time that the event was reported to the Event Manager.

Name

Identifies the managed item that is associated with the performance data.

Item Type Name

Identifies the type of managed item.

Item Subtype

Is the subtype of the indicated managed item. Further identifies the item type, such as a router or switch as a subtype of device.

Event Type

Is the type of event that the data source reported to the Event Manager, such as Threshold.

Event Subtype

Specifies the type of event more narrowly. When available, event subtypes let you further categorize events. Using event subtypes, you can sort the event data into related groups of events. For example, the subtypes for a threshold event include interface, storage, and CPU.

Description

Describes the event that occurred. Usually lists the event source.

Device Name

Is the IP address or hostname of the device where the event was reported.

More info:

Event Details (see page 37)

Event Details

Click to select any event in the Events View, and click Details. The Event Details view provides detailed information about the event, such as its source, duration, and associated MIB variables.

By default, the Event Details view includes the following information:

Event ID

Is an internally assigned value to identify the event.

Event Type

Is the type of event that the data source reported to the Event Manager, such as Threshold.

Event Subtype

Specifies the type of event more narrowly. When available, event subtypes let you further categorize events. Using event subtypes, you can sort the event data into related groups of events. For example, the subtypes for a threshold event include interface, storage, and CPU.

Occurred On

Are the date and time when the event was reported.

Description

Describes the event that occurred. Usually lists the event source.

Device Name

Identifies the managed item that was the source of the performance data.

Property Name

Is the name of the event property. For more information, see Event Properties (see page 38).

Value

Is the value associated with the indicated event property at the time the event was reported.

Event Properties

Event Details may include the following event properties. Event properties are reported by the data source.

Description

Describes the Event Profile that was used.

Event Rule

Identifies a rule with its name, ID, and description and defines the parameters for how an event is generated.

Event Profile Rule Name

Identifies the name of the Event Rule.

Event Profile Rule ID

Is the unique ID within the Event Profile.

Event Profile Rule Description

Describes the Event Rule.

Event Profile Rule Type

Indicates the type of rule. Valid type values:

Constant - ExceedThreshold and ClearThresholds reflect constant values.

StandardDeviation- ExceedThreshold and ClearThreshold are defined in terms of the number of standard deviation units from the mean.

Event Profile Enabled

Defines whether the rule is enabled.

Event Profile Technology Facet

Defines the name of the technology certification referenced by the event rule.

Event Profile Performance Metric

Is the attribute (metric) from the metric family to evaluate.

Event Profile Exceed Operator

Is the comparison operator used to compare the Performance Metric and the Exceed Threshold.

Event Profile Exceed Threshold

Is the value used to compare to the Performance Metric using the Exceed Operator to generate an event.

Constant - Reflects constant values.

Standard Deviation- Represents the number of standard deviation units from the mean.

Event Profile Duration

Is the number of seconds required for the condition to be true (for set or clear).

Event Profile Window

Is the number of seconds over which to evaluate the condition (for set or clear).

Event Profile Clear Operator

Is the comparison operator used to compare the Performance Metric and the Clear Threshold to clear the event.

Event Profile Clear Threshold

Is the value used to compare to the Performance Metric using the Clear Operator to clear an event.

Constant - Reflects constant values.

StandardDeviation- Represents the number of standard deviation units from the mean.

Item Create Time

Specifies the date and time the item was created.

Item Description

Describes the item.

Item Name

Identifies the name of the item.

Manage Event Retention

By default, events are retained for 30 days in the Event Manager database. You can edit the number of days that events are retained.

Follow these steps:

1. Open the file:

   `/opt/CA/PerformanceCenter/EM/webapps/EventManager/WEB-INF/em.properties`

2. Set the **Event.Retention** value to the number of days you want events to be retained in the database. Save your changes.

3. Stop the Event Manager service using the command line:

   ```
   service caperfcenter_eventmanager stop
   ```

4. Restart the Event Manager service using the command line:

   ```
   service caperfcenter_eventmanager start
   ```

   The new event retention value becomes effective.

Note: Depending on the platform the Event Manager is running on, you can use other methods to stop and start the Event Manager.

Notifications

Notifications can be configured for events coming from a data source to the Event Manager. The incoming events are evaluated against the conditions that you configure for the notification criteria. Only when the criteria are met does Event Manager take a notification action. If an event does not trigger a notification, the event can still be displayed in the Event List.

Note: For information about which data sources are supported for notifications, see the *CA Performance Center Readme*.

A user only configures and receives notifications for events for an item in a group to which the user has access.

Important! Create an SNMP profile with the outgoing trap port (typically 162) before creating the notification.

Consider the following information:

- Notifications are user-specific; users cannot see the notifications of others.
- The action to delete event notifications does not affect the actual or future events.

The following notification types are available in the Create/Edit Notifications wizard:

Trap

Sends trap notifications to fault or network management system (NMS) in your environment, such as CA Spectrum. Supports multiple destinations. The first destination is required.

Two MIB choices are available in the Notifications wizard to provide compatibility for existing customers.

Note: The trap receivers must be preconfigured to receive traps. Each destination can have its own configuration regarding SNMP community and IPV4 destination. For more information about trap formats, see the corresponding NMS documentation for your trap receiver.

Supported roles: Users with the Administrator role (global administrators) can configure trap notifications. Administrators must also have product privileges to a data source that creates events.

Email

Sends email notifications to one or more recipients when an event is raised or cleared. Provides a link in the email to the context page for the device or component that triggered the alarm.

Supported roles: Users with the Create Notifications role right and users with the Administrator role and product permission can configure email notifications. However, the Administrator role must first specify an SMTP server.

Administrators can view, create, or delete notifications from the Admin, Notifications menu in the CA Performance Center user interface. The Notifications option only displays when Event Manager is enabled and in a synchronized state of Available.

Note: As a Default Tenant Administrator, you can create a notification for a tenant administrator or tenant user by working in a real user context. Log in as a tenant administrator or tenant user. Alternatively, the Default Tenant administrator can administer the tenant and then proxy to the user to create a tenant-scoped notification.

Alternatively, administrators can use the Event Manager API. Access the self-documenting interface on the Event Manager host using this URL: http://*hostname:*8281/EventManager/webservice/notifications/documentation.

Users can create email notifications from the My Settings, Notifications menu.

More Information:

nhLiveAlarm Format Usage for Traps (see page 43)
EventManager Format Usage for Traps (see page 42)

EventManager Format Usage for Traps

The EventManager MIB is supported for trap notifications. If needed, the MIB files can be found in:

InstallLocation/PerformanceCenter/PC/webapps/pc/mibs/netqos-em-mib

InstallLocation

Is the directory where CA Performance Center was installed.

When the EventManager format choice is selected, the trap will be sent out with the following variables:

netQosEventId

Specifies an identifier that Event Manager assigned to the event.

netQoSEventType

Specifies the type of event.

netQoSEventCategory

Categorizes the event.

Values: 0 Unknown, 1 Fault, 2 Config, 3 Accounting, 4 Performance, 5 Security

netQoSEventSeverity

Specifies the severity of the event.

Values: 0 Normal, 1 Unknown, 2 Minor, 3 Major, 4 Critical, 5 Unavailable

netQoSEventDescription

Describes the event.

netQoSEventState

Specifies the current state of the event. Each state has its own notification.

Values: 0 opened, 1 acknowledged, 2 closed, 3 cleared

netQoSEventOpenTime

Specifies the UTC timestamp (from the eventState timestamp).

netQoSEventMapURL

No value is available. The "" string will be sent.

netQoSEventDetailsURL

No value is available. The "" string will be sent.

netQoSEventAssociatedItemURL

Specifies the URL to the item web page.

netQoSEventItemName

Specifies the item name. There is one notification per item.

Maximum length: 127 bytes

netQoSEventItemType

Specifies the item type.

Maximum length: 32 bytes

netQoSEventItemSubtype

Specifies the item subtype.

Maximum length: 32 bytes

netQoSEventItemIpAddress

Specifies an IP address for the item or an empty string.

netQoSEventPropertyName

Specifies one name set for each property. There will be a PropertyName for each property in the event. (The properties will vary by the event type.)

Maximum length: 128 bytes

netQoSEventPropertyValue

Specifies the property value for the event. There will be a PropertyValue for each property in the event. (The properties will vary by the event type.)

nhLiveAlarm Format Usage for Traps

The nhLiveAlarm MIB is supported for trap notifications. If needed, the MIB files can be found in:

InstallLocation/PerformanceCenter/PC/webapps/pc/mibs/concord-diagmon.mib

InstallLocation

Is the directory where CA Performance Center was installed.

When using the nhLiveAlarm format for trap notifications, be aware of the following restrictions. Many of the variable values described by the CA eHealth trap MIB have changed from integrations with earlier versions of NetQoS Performance Center.

nhServerIp

No value is available. The "" string will be sent.

nhServerName

No value is available. The "" string will be sent.

nhServerPort

No value is available. The "" string will be sent.

nhElementIp

Specifies the IP address of the item or "" if no IP address exists.

nhElementName

Specifies the item name.

nhElementId

Specifies the item CA Performance Center ID (global ID).

nhStartTime

Specifies the timestamp from the event.

nhDisplayStr

Specifies the value for the MaxThresholdValue variable from the event.

nhGroup

No value is available. The "" string will be sent.

nhGroupList

No value is available. The "" string will be sent.

nhExceptionType

No value is available. The "" string will be sent.

nhVariable

Specifies variables in the event profile rule.

nhSeverity

Specifies the severity of the event.

nhOpenViewSeverity

No value is available. The "" string will be sent.

nhProfile

Specifies the event profile name.

nhExceptionId

Specifies the event ID.

nhTechType

No value is available. The "" string will be sent.

nhEventCarrier

No value is available. The "" string will be sent.

nhElementAlias

No value is available. The "" string will be sent.

nhComponent

No value is available. The "" string will be sent.

nhDescription

Contains the event description.

nhAlarmOccurId

Specifies the alarm ID.

profileId

Specifies the event profile ID.

nhElementBaseType

Specifies the item type.

Chapter 6: Working with Groups

This section contains the following topics:

Groups (see page 47)
Types of Groups (see page 48)
Groups for Multi-Tenant Deployments (see page 49)
Create Your Own Custom Groups (see page 51)

Groups

The administrator can create a custom group structure to organize managed items in CA Performance Center. Groups act like filters to make reported data more useful. Custom groups let you view the items that you must monitor in an organized structure.

Groups determine the data that you see in dashboards when you log in. The group that is applied as a filter to the current dashboard is the *group context* for that dashboard. When you first log in to CA Performance Center, the pages you see reflect the context of your *default permission group*.

You can change the default group for your own user account so that data from another group is reflected in dashboards by default. You can also change the context for a dashboard or for an individual view.

If the administrator has enabled the "My Custom Groups" feature for your user account, you can create your own groups of items. The groups you create are only visible to you.

More information:

Types of Groups (see page 48)
Groups for Multi-Tenant Deployments (see page 49)
Create Your Own Custom Groups (see page 51)

Types of Groups

Groups are organized into a hierarchical tree structure. The Groups tree helps you define relationships, policies, and dependencies among services, devices, applications, locations, and users within your organization. The following list summarizes the types of groups in the Groups tree:

System Groups 

Are read-only groups automatically created by CA Performance Center based on information from data sources. These groups cannot be edited (as indicated by the "lock" symbol). But they can be viewed, applied as permission groups to user accounts, or copied to custom or site groups.

Custom Groups 

Create hierarchical levels and organize items into logical relationships within the Groups tree. Custom groups at the top level of the Groups tree typically represent geographical, topological, or functional divisions within your organization. Lower-level custom groups (or subgroups) typically represent managed item types, such as devices, services, or applications. Or these subgroups can represent the job functions of IT staff.

Only administrators can create and edit custom groups. They filter the data in CA Performance Center dashboards and views. The group context for a dashboard or view determines the data that is presented.

Site Groups 

Are special custom groups based on sites, such as branch offices, or on physical locations, such as regions or cities. Site groups let you create navigation functions within CA Performance Center dashboards to present views across all sites. They include a Time Zone and a Business Hours parameter to let you see prioritized data from business-critical times of day.

Site groups also provide a granular context to apply to dashboards. For example, after you create a site group for each of your sites, a single dashboard can report on each site individually. We strongly recommend creating a site group for each data center within your enterprise and for other major infrastructure locations.

Group References

Are read-only copies of system or custom groups. When you copy a group to another location in the Groups tree, a group reference appears. User permissions can be allocated using group references. Using references lets you create a group structure once, and then copy that structure to other parts of the Groups tree. Changes to group references can only be made to the original custom group, but they are propagated to all reference locations.

Select a group reference to access a link to the original group. Clicking the link expands the node in the Groups tree and opens the Properties tab for the original group.

Groups for Multi-Tenant Deployments

When the global administrator (the administrator for the Default Tenant) creates at least one tenant, features to support multi-tenancy are enabled. "Multi-tenant deployments" consist of multiple discrete enterprises with potentially overlapping IP addresses. More groups appear in the Groups tree to let the administrator organize tenant inventories and allocate permissions:

Defined Tenants

Includes all tenants. Tenants are used with IP domains to monitor separate customer environments with a single CA Performance Center instance. Each tenant can contain multiple subgroups of items that are not shared among tenants.

Tenant administrators can create custom groups within their tenant. For the global administrator, tenant groups appear under the Tenant node in the Groups tree.

Service Provider Global Groups

Contains groups of items that help the global administrator manage tenant environments. These groups let the administrator visualize and organize shared items–any items that are not explicitly associated with a tenant IP domain.

The groups that allocate access to data from shared items appear under each tenant. See "Service Provider Defined Groups."

When you expand the top-level Inventory group, the following group appears in a multi-tenant deployment:

Domains

Includes all of the custom IP domains that are used to associate managed items with tenants. Also includes the Default Domain, which contains all items that are not explicitly assigned to a custom domain. For more information, see IP Domains.

In a multi-tenant deployment, each tenant has its own groups. Tenant users cannot see items outside of the tenant group unless the global administrator grants such access with Service Provider groups.

Groups (Tenant)

Lets the global administrator or tenant administrator create custom groups. Select this node to enable the Add Group button.

Inventory (Tenant)

Includes all managed items that are associated with the tenant IP domains. Items from all registered data sources can appear in this group.

Each tenant also has the following system subgroups in its Inventory group:

IP Domains

Represents the IP domains that are associated with this tenant. Any managed items that have been discovered are associated with this tenant through its IP domains. To see the managed items of the tenant, click a tenant IP domain in the Groups tree.

Service Provider Defined Groups

Includes groups that the global administrator has populated with shared items whose data this tenant can access. Use these groups to grant access to data from shared devices to selected tenant user accounts.

For example, a router that the service provider owns handles traffic from multiple tenant domains. Using Service Provider Defined groups, the global administrator can allocate tenant access to data from that router. This strategy lets the tenant perform some independent monitoring and verification of system performance.

Service Provider Items

Contains all items that are not explicitly associated with a tenant IP domain. Such items are automatically placed in this group. The global administrator can then place these items into 'Service Provider Defined Groups' to allocate tenant access to data from shared items.

Create Your Own Custom Groups

If the "My Custom Groups" feature is enabled for your user account, you can place managed items in custom groups to organize them. The groups that appear in your "My Custom Groups" area are visible only to you.

Important! If you create a group for a CA Infrastructure Management Data Aggregator data source, we recommend limiting group membership to 10,000 items. This count includes the children of managed items. Observing this limit keeps reporting time to less than 10 seconds.

Follow these steps:

1. Log in to CA Performance Center.

   If your user account has the My Custom Groups feature enabled, you see a My Settings tab on the console toolbar.

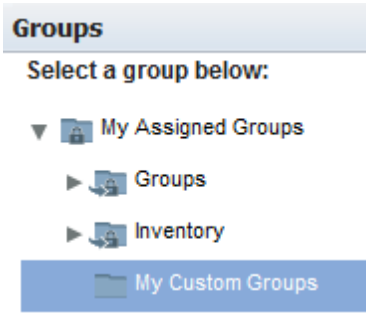
2. Select My Settings, and click My Custom Groups.

   The My Custom Groups page shows a tree view of group structure and a tabbed view of group properties.

   Note: The groups that you can see are groups that the administrator selected for you, based on your responsibilities.

   The page displays groups in a tree structure.

3. Locate the My Custom Groups node in the My Assigned Groups tree. You can add groups as subgroups of this node.

   Note: The custom groups that the administrator created cannot be edited within the My Custom Groups interface. These read-only groups appear as group references; their properties tab shows a path to the original group.

4. Right-click the My Custom Groups node, and select Add New Group.

   The Add Group window opens.

   The New tab is selected by default.

5. Supply values for the following parameters:

   Group Name

   Specifies a name for the group. Do not use the following special characters in group names: /&\,%.

   Description

   (Optional) Helps you identify the group.

6. Confirm the setting for the following parameter:

   Include the children of managed items

   Adds the children of managed items automatically when the items are added to this group. If you disable this option and add a router to the group, the interfaces on that router are not included. Therefore, their data is not visible in drilldown views.

   Default: Selected.

7. Select Custom or Site from the Group Type list.

   If you selected Site as the type, an additional parameter appears:

   Location

   Identifies a physical location that is associated with the site group, such as a city or a branch office.

8. Click Save.

   The new group appears in the My Assigned Groups tree. No other CA Performance Center user can see this group.

   The group contains no items until you add them. You have two options for adding items to a custom group:

   - Manually populate the group by adding items.
   - Create rules to manage group membership.

More information:

Add Managed Items to a Group Using Rules (see page 53)
Add Managed Items to a Group Manually (see page 52)

Add Managed Items to a Group Manually

You can populate custom groups manually, by adding managed items that you select.

Note: System groups appear with a "lock" symbol in the Groups tree to indicate their read-only status. You cannot add items to or remove them from system groups. Further, custom groups that the administrator created are also locked.

Follow these steps:

1. Log in to CA Performance Center.
2. Select My Settings, and click My Custom Groups.

   The My Custom Groups page shows a tree view of group structure and a tabbed view of group properties.
3. Expand nodes in the Groups tree to locate and select the group to which you want to add managed items.

   If items have already been added to this group, they appear in the right pane.

   Note: Items that are added directly to a group as a manual step appear as Direct Items in the Group Properties pane. Items that are added to a group because they are children of a managed item are Inherited Items in the Group Properties.
4. Click the Items tab in the right pane.

   The Show Items list appears.
5. Click Add Item Type.

   The Add Items dialog opens.
6. Select the type of item to add from the Available Items list.

   The available items depend on the item type, the data sources registered, and the items discovered.

   To see additional pages of items, click the links below the list. Or use the Search field to search for an item in the list.
7. Select items by clicking their check boxes. Click the check box in the table header row to select all items on a page.
8. Click Add Items.

   The Items tab refreshes to show the new group members, but the Add Items dialog remains open.
9. Click Close when you have finished adding items.

Add Managed Items to a Group Using Rules

It can be difficult to keep custom groups up-to-date when systems and networks change. Therefore, you can use rules to populate your custom groups. Newly discovered items that meet rule specifications are added to groups. Similarly, if they do not meet rule requirements or are no longer monitored, items are removed.

Follow these steps:

1. Log in to CA Performance Center.
2. Select My Settings, and click My Custom Groups.

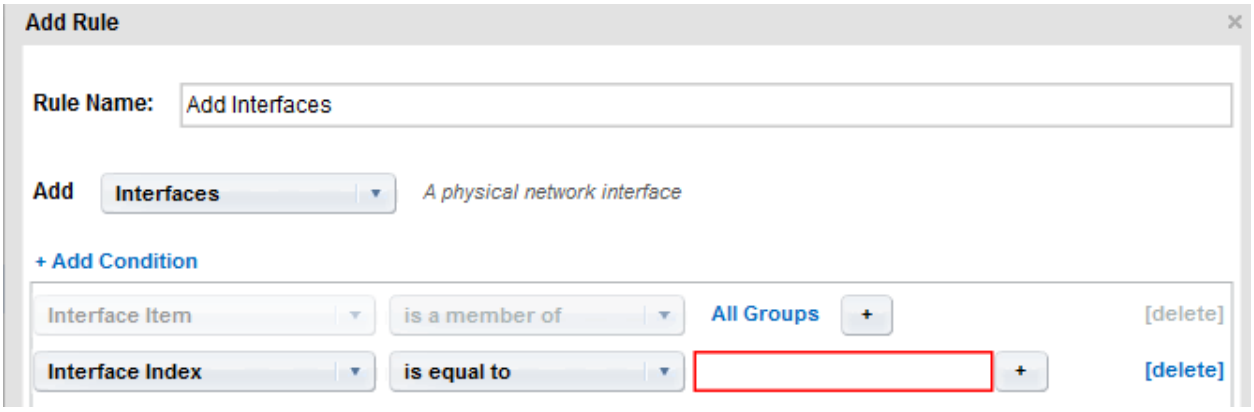
   The My Custom Groups page shows a tree view of group structure and a tabbed view of group properties.
3. Expand nodes in the Groups tree to locate and select the group to which you want to add managed items.

   If items have already been added to this group, they appear in the right pane.
4. Click the Properties tab in the right pane.
5. Click the Rules tab on the Properties page, and then click Add Rule.

   The Add Rule dialog opens.
6. Supply a name for the rule.
7. Select the type of managed item that you would like to add to the group from the Add list.

   Available options vary based on the data sources registered with CA Performance Center.
8. Click Add Condition.

   A row of drop-down lists and fields appears.



9. Select a method for identifying managed items. For example, select Device Type. The options include item description, name, type, and IP address.

   The remaining lists are updated to match the type of item selected.
10. Select a method for matching from the second list. For example, select 'is equal to'.

    Important! Use CIDR notation for the IP addresses that you supply for the 'is in subnet' and 'is not in subnet' options. Use dotted-decimal notation for the IP addresses that you supply for the 'is between' and 'is not between' options.

11. (Optional) Enter a text string to match in the remaining condition field. For example, to add all routers and servers in the Southwest region, supply a string that corresponds to the appropriate naming convention, such as "sw*".

    Note: Wildcard characters are accepted in this field, such as an asterisk (*) for a multicharacter match.

12. (Optional) To add 'OR' matches, click + at the end of the condition.

    An 'OR' drop-down list appears.

13. (Optional) To add 'AND' matches, click Add Condition.

    Three more dropdown lists appear.

    Note: An 'AND' condition indicator does not appear. By contrast, an 'OR' indicator appears when you select an 'OR' operator.

14. Click Preview Results to confirm that the new rule is including the items you want.

    The results are shown in the Group Rules Preview window. You can expand each item type to see the specific items added.

15. (Optional) Click +Add Rule to add other item types to the group.

    Each item type requires its own rule.

16. When you have finished creating rules, you can click Save or Save and Run Rules:

    - Save - Saves the rules without running the rules. The group is populated during the next global synchronization, which occurs approximately every 5 minutes.
    - Save and Run Rules - Saves the rules and populates the group immediately.

Glossary

Context pages

Context pages provide specific, focused performance or status data from a narrow context, such as a single router or server. These pages are available as drill-down links or tabs from Summary dashboards.

dashboards

Dashboards are dynamic report-building pages within the CA Performance Center user interface. They appear as menu items that are accessible from the Dashboards tab. Each dashboard is a collection of views that present data from registered data sources on a single web page. The layout, views, time interval, and group context of each dashboard can be customized.

data sources

Data sources are the supported products that provide performance and configuration data to CA Performance Center. Data source products that monitor, collect, and aggregate data can often function independently. However, once they are registered to an instance of CA Performance Center, they are known as data sources.

drill down

To *drill down* means to navigate from one data view or dashboard in CA Performance Center to another, more detailed data view or context page. The new page displays data from the same timeframe, for the same managed item or set of items.

event

An *event* is a message that is triggered by an instantaneous occurrence in your networking infrastructure, usually indicating that something significant has occurred. Events are reported for several reasons. They are reported when data exceeds a threshold or when configuration changes are detected.

group

A *group* is a filter definition that functions as a container for managed items. Groups let you logically organize managed items in a tree structure, with each group containing subgroups or managed items. The structure is propagated to the data sources, where it enables drilldown from top-level groups into data from an increasingly narrow but related context.

menus

Menus are segments of the Dashboards tab that are used to organize dashboards by their content. By default, Administrators and Designers can customize menus and assign them to user account roles.

My Dashboards menu

The *My Dashboard*s menu is a dashboard container that can be personalized for each operator who has a user account in CA Performance Center. Any dashboard that you customize—by moving items to different positions in the layout, for example—appears in your My Dashboards menu. Such modifications are not available to other users.

reports

Reports are static output from an on-demand selection or an exported dashboard page. Reports that you export from a dashboard create a static data set from the data and information in the associated dashboard. On-demand reports capture a data set from a single managed item or group in the Inventory. You can print reports, send them by email, or export them in CSV or PDF format. For each format, the report captures a selected data set.

site groups

Site groups are custom groups that are based on physical locations, such as a city, region, office, or campus. Typically, site groups contain items and subgroups of items that are grouped by location. Adding site groups to other custom groups in your tree structure allows you to build geographically and logically organized reports. Site groups enable business-hour filtering of dashboard views.

statistical data

The *statistical analysis data set* includes minimum, maximum, mean (average), standard deviation, and other metrics that are recalculated hourly to include the most recently collected data. This data helps to characterize past performance for selected monitored parameters, and helps to assess present performance and estimate future performance. For example, comparing current CPU utilization to a known baseline average level helps to determine whether current utilization is within a typical range. A monitored parameter that exceeds a baseline can indicate additional load on the server from a new application process, an increase in the number of users or sessions, or an increase in the amount of data being processed.

Baseline averages and other statistical data are updated hourly, averaging up to 30 “same-hour” hourly roll-up samples for each one of the preceding 30 days.

Summary pages

Summary pages provide high-level information, such as averages from groups of managed items. Summary dashboards often provide a drilldown path to more detailed, related pages from a selected context.

threshold event

A *threshold event* is one of several event types managed by CA Infrastructure Management. When your devices violate a threshold value, CA Infrastructure Management creates one of these events, which can trigger a corresponding alarm.

view

Views, or *data views*, present statistical data, usually in a graph or table format. Each view represents a discrete set of collected data. Depending on your user account role rights, you can add and edit individual views or remove them from a dashboard page. In some cases, you can export the data to a file in CSV format.

Index

A

alias • 20

B

browser view • 21

C

Consoles • 13
context page • 14, 20
CSV export feature • 27

D

dashboard • 17, 22, 25
data source • 8

E

element • 14
email, sending reports by • 30
events • 35, 36
    details • 37, 38
    notifications • 40, 42, 43

F

focus • 21

G

groups • 48
    My Custom • 51
    references • 48

I

Inventory • 13, 14

L

language, preferred • 12

M

menus • 8, 17
metric family • 38
multi-tenancy • 49
My Custom Groups • 51

N

notifications, role right for • 40

O

on-demand reports • 15

R

report • 17, 19
    adding • 14
    on-demand • 13

S

Service Provider group • 49
Single Sign-On • 17
site group • 48
system group • 48

T

tables • 18, 21
    modifying • 21
time zone • 12
troubleshooting
    Inventory • 13

U

URL, generating • 27, 32
user accounts
    modifying • 12

V

view • 8, 21
    exporting • 28, 29, 32
    modifying • 21, 26