CA Unified Communications Monitor

Working with Groups, IP Domains, and Tenants in CA Performance Center

Version 3.5

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: Working with Groups, IP Domains, and Tenants in CA Performance Center

Consider the usefulness of organizing your Locations and devices into IP domains, groups, or tenants. These organization tools serve several purposes:

- Organize managed items in a way that facilitates reporting.
- Control the managed items and associated data that each UC Monitor operator can view.
- Enable the monitoring of multiple enterprises with overlapping IP addresses as separate entities.

IP domains and groups are supported in CA Performance Center and CA NetQoS Performance Center version 6.1. Tenants are supported only in CA Performance Center. UC Monitor must be a registered data source to enable these features.

Only a user with the administrator role in CA Performance Center or CA NetQoS Performance Center can create and edit IP domains, groups, and tenants.

This section contains the following topics:

What are IP Domains?

CA Performance Center supports monitoring by IP domain. *IP domains* are logical groupings that identify data collected from different devices and networks. Monitoring by domain means that IP addresses with associated interfaces or applications that belong to separate customer networks are monitored separately. When combined with appropriate permissions, IP domains are monitored from a single console, but users view data only for the domains that they monitor.

IP domains function much like groups to contain managed items. Like groups, they are created in CA Performance Center, but the task of assigning items to domains is performed in the UC Monitor management console.

IP domains are optional in a standard CA Performance Center installation. However, IP domains are required when you want to deploy CA Performance Center in a multi-tenant environment.

Note: For complete information about managing domains, see the *CA Performance Center Administrator Guide*.

How IP Domains Work

IP domains let you address potential IP address conflicts. Domain identifiers indicate that two managed items that otherwise appear as duplicate IP addresses are actually two *different* managed items. For example, a router with a single IP address could have multiple interfaces, each belonging to a different enterprise. The DNS identity of each interface would determine its IP domain. Data from items in the domain would be reported for a single tenant corresponding to the interface owner.

The domain dimension lets CA data sources function in a service-provider environment. The same software monitors multiple networks as separate entities. The domain lets data collectors associate managed items and data with the appropriate service provider customer, or *tenant*.

Domain monitoring is enabled for each data source as soon as it is registered. However, domain identifiers are not visible in the data sources until at least one custom IP domain definition has been created in CA Performance Center. The following managed item types are associated with the Default Domain once domain monitoring is enabled:

- Devices
- Interfaces and interface addresses
- Networks
- VoIP Locations

The data sources that monitor these item types report up a domain identifier and other properties during synchronization with CA Performance Center. A data source can associate an item with a domain by including a domain ID property. Any item whose domain ID is not reported is automatically placed in the Default Domain.

CA Performance Center users with the Administrator role can create custom IP domains. They are sent down to the data sources during synchronization, where they are available for use during data collection configuration. Domain definitions are shared among data sources that are registered to the same CA Performance Center instance.

In the Groups tree, the Domains group is contained within the Inventory group, which is itself a subgroup of the Tenant. The Domains group includes the Default Domain and any custom domains that you have created.

Items that are not assigned to a custom domain in a data source are associated with the Default Domain. This assignment is transparent to users who are not using custom IP domains to identify monitored traffic.

How Do IP Domains Work with UC Monitor?

The task of creating IP domain definitions is performed in CA Performance Center. But the UC Monitor administrator determines the IP domain assignments of monitored items by selecting the appropriate IP domain for each collector.

After IP domain definitions are synchronized with data sources, they are available for use during data collection configuration. Define at least one custom IP domain in CA Performance Center to expose the necessary parameters in the UC Monitor management console.

The IP domain definitions that are synchronized to UC Monitor are assigned to collectors. A collector associates all discovered items with the default IP domain until the administrator assigns a custom IP domain in the collector Properties dialog. These items are then automatically associated with the custom IP domain, but only as they are rediscovered. IP domain assignments are not applied retroactively.

Endpoints are discovered during monitoring. Locations and call server groups are not. You manually edit Location definitions to select a custom IP domain for the IP Domain field. Otherwise, Locations are placed in the default IP domain.

After you create an IP domain, the Location List reflects the new IP domain after the first synchronization. New default Locations for the <External>, <None>, and <Unassigned> categories are included in the list so that one of each appears in each domain. Each IP domain, including the default IP domain, must retain these Locations so that all endpoints detected in call traffic can be properly classified. IP domain designations also appear in report views, where an IP Domain column indicates domain identity.

Enable IP Domain Monitoring at the Collector

After you define an IP domain in CA Performance Center and data source synchronization has occurred, the IP Domain field is available in the collector Properties dialog. The collectors that you add to a distributed system also have this field. Use this field to associate a selected IP domain with the performance data taken from calls running between monitored endpoints.

Follow these steps:

1. Click Administration, Data Collection, Collectors in the navigation bar.

   The Collection Device List opens.

2. Select a collector.

3. Click Edit.

   The Collection Device Properties page opens.

4. Select the appropriate domain from the IP Domain field.

5. Click Save.

6. Repeat steps 2 through 5 for each collector. Each collector creates an association with the same IP domain for all phones and devices that it discovers.

7. Reload the collectors to send them the domain information.

   After you configure the system, the IP domain designation is included for each endpoint where it appears in reports. You can also verify IP domain identity in the Location List or Voice Gateway List.

Note: IP domains are populated with managed items when items are discovered from call traffic. You manually assign IP domains to Location definitions because Locations are not discovered. For more information, see Change Domain Assignments (see page 11).

Enable IP Domain Monitoring at the Lync Collector

When you configure a Lync collector in a Microsoft environment, data is automatically associated with the default IP domain.

The following tips are best practices for Microsoft customers who use multiple domains.

- Each monitoring server is automatically discovered in the default IP domain. All of its data is associated with the Locations and media devices in that IP domain.
- Change the IP domain association of each Lync collector server, which rediscovers call servers and media devices for that domain.
- Create or import Location definitions for the IP domain. You can perform this task before or after the collector IP domain is updated. From this point on, all data that is received from the Lync collector is associated with the proper IP domain.

- Across all IP domains, the initial data collection from each monitoring server (for example, from each MSP customer) is discovered in the default IP domain. Ideally, instances of overlapping data are brief.
- Do not use the default IP domain for user permissions.
- You can delete call servers and media devices that are associated with the default IP domain.

Using IP Domains as Permission Groups

As a best practice, add IP domains to user accounts to let users see the items in the domains. Permission to see an item in an IP domain automatically grants access to all other items in that domain. You do not need to grant explicit permission for each item in an IP domain. Similarly, do not add the All VoIP Locations domain to user permissions in a multiple-domain environment. Doing so implicitly grants that user access to data from all IP domains.

Another best practice is to grant the administrator permission to see all IP domains. This action simplifies IP domain administration. For example, the administrator can see IP domain identifiers for all collectors, Locations, call servers, and voice gateways. By contrast, individual users only need access to one IP domain.

Avaya trunk groups do not have IP domain identifiers. As a result, they are not included when you add IP domains to user account permissions. Instead, you add Avaya trunk groups as individual permission groups. Locations, media devices, and call servers are managed items, with IP domain identifiers based on your collector configuration. Avaya trunk groups are treated as groups in CA Performance Center, and groups do not have IP domain identifiers.

Change IP Domain Assignments

The process of classifying collected data in the UC Monitor database prevents Location and IP domain designations from being applied retroactively. Subnets that were already in the database when they were added to a Location definition remain categorized as <Unassigned> in historical data views. These same subnets are correctly placed in the Location in new views. Similar logic applies to the use of custom IP domains. Those same subnets are associated with custom IP domains when new calls are made, with no effect on data already collected.

When you create an IP domain in CA Performance Center, all Locations that were previously defined are associated with the default IP domain. You can edit Locations to remove subnets, select the custom IP domain, and then add the subnets back to the Locations. This manual procedure is often time-consuming. We recommend the following work flow instead.

Follow these steps:

1. Export the current list of Location definitions, as discussed in Export a List of Locations.
2. Verify the contents of the exported .csv file.
3. Delete all Location definitions, as discussed in Manage Location Definitions.
4. Select the new IP domain in the Properties dialog, as discussed in Enable IP Domain Monitoring at the Collector (see page 10).
5. Import the .csv file, as discussed in Import Location Definitions.

Delete IP Domains

Like the associations between performance statistics and managed items, IP domain associations are stored with items in the UC Monitor database. As a result, you cannot delete IP domains from UC Monitor. Deleted IP domains are marked as inactive in UC Monitor and not exposed in reports that display new data. For example, you can deregister and then reregister the UC Monitor data source. At the first synchronization, the inactive IP domain is sent to CA Performance Center because managed items in the UC Monitor database retain the association.

In most cases, the following work flow is recommended.

Follow these steps:

1. Delete the IP domain from CA Performance Center. For more information, see the *CA Performance Center Administrator Guide*.
2. Change the assignment in the IP Domain field for the deleted domain. For more information, see Change Collection Device Properties.

   Note: Select another IP domain for the collector. Otherwise, the collector associates items with the default IP domain.

   Data that was previously collected and associated with the deleted IP domain remains associated with it and is displayed as such in historical reports.

What are Groups?

The Groups feature is a powerful tool that lets administrators organize data and control who can view it. When a performance issue is reported, the permission groups that are assigned to user accounts let operators effectively analyze data in a logical flow. From a group, operators can drill down to information about one item in the group.

The administrator can create a custom group structure to organize managed items in CA Performance Center. Groups act like filters to organize related items and make reported data more useful. For example, a group can represent a physical location, a device and its interfaces, or a group of similar devices. Custom groups let operators view the items they must monitor while limiting their access to the selected data.

Properly configured, groups can prevent CA Performance Center operators from viewing selected data for security reasons. The administrator can selectively grant user access to data that falls within their area of responsibility. Groups can also facilitate performance monitoring, reporting, and troubleshooting.

Tenants include special types of system groups to maintain separation among customer deployments. Tenants can also contain entire custom grouping structures.

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 shown in the Groups tree:

System Groups 

Are read-only groups automatically created by CA Performance Center based on information provided by 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 presented 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.

Recommendations for UC Monitor Groups

Use UC Monitor groups to organize your call servers, media devices, voice interfaces, and Locations. Properly organizing your devices and Locations into groups lets you:

- Manage and organize reports.
- Assign UC Monitor user permissions appropriately.

Set up groups that resemble the reporting structure of your IT organization, the geography of your organization, or the logical structure of your system. To ensure group validity, always position call servers and media devices at the nodes in the Groups tree where access permissions are applied. Groups can contain multiple levels of subgroups. A user with permission to view a group can also view all of its subgroups.

You cannot manage groups in the UC Monitor management console. To create and edit groups for Locations and devices, register UC Monitor as a data source for CA Performance Center. After registration is complete, access to the group management interface requires you to log in to CA Performance Center with administrator privileges.

Note: For complete information about managing groups, see the *CA Performance Center Administrator Guide*.

Working with Avaya Trunk Groups

During SNMP polling by the collector, the Avaya Communication Manager reports Avaya trunk group names. Administrators typically use these group names when configuring the system through the Avaya Site Administration (ASA) interface. This practice can easily lead to redundant trunk group names, which then appear identical in reports.

We recommend using the ASA interface to assign unique names that make each trunk group readily distinguishable in CA Performance Center reports. You can change names after monitoring has begun. No report data is lost because internal identifiers correlate the previous names with the new ones.

Important: You can add an IP domain to a user account as a permission group. You add Avaya trunk groups with that IP domain assignment as individual permission groups. These trunk groups are treated as groups in CA Performance Center. Groups do not have explicit IP domain identifiers.

More information

What are IP Domains? (see page 7)

Working with Cisco Trunk Groups

In a Cisco environment, use trunk groups to reflect your actual usage and routing patterns in reports.

Trunk groups are not discovered from the call servers or from network traffic, but are instead created as groups of voice interfaces in CA Performance Center. You can see them on the CA Performance Center Inventory tab.

Create group rules that automatically place gateway voice interfaces into custom groups, which you designate as trunk groups using a clear naming convention. These special trunk groups can only contain items of the voice interface type.

Cisco administrators must periodically verify the voice interface capacity values from a device MIB. This information can be viewed on the Voice Gateway Properties page. The Voice Interface reports use the information in the Channel Capacity column to calculate interface usage as a percentage of capacity. These reports are less accurate when the device MIB incorrectly reports the gateway voice channel capacity.

As a best practice, verify that all known gateway voice interfaces have the number of channels correctly configured. The collector typically can get this capacity information from polling the gateway. If it changes, however, this information is not updated in the device MIB. To verify Cisco voice interface capacity data, see Managing Voice Gateways.

UC Monitor operators can see unexpected items in reports when you do not carefully create groups and user account permissions. Specifically, do not place gateway voice interfaces in groups that you then copy into subgroup containers. An operator with permission to view a container group can also see all its subgroups. As a result, that operator can see the same interface group twice in the Top Trunk Groups report: where it appears in its own group, and where it appears in its container group.

This behavior is unavoidable because the Trunk Group reports do not handle container groups the same way that they handle trunk groups. Specifically, only the custom groups that (directly) contain at least one voice interface are identified as trunk groups. To UC Monitor, a voice interface that belongs to a trunk group *and* to a subgroup is included twice in the Top Trunk Groups report. The voice interface does not appear to be a duplicate because only one instance is a member of a trunk group.

To avoid duplication of trunk groups in the Trunk Group reports, verify that trunk groups contain only voice interfaces. When a non-voice interface item is detected, the group is not handled as a trunk group. And then either:

- Do not place trunk groups into container groups that you then copy into other positions in the Groups tree.
- Assign permissions at the level of each specific trunk group, not above it, at the container level.

What are Tenants?

By default, all managed items and their data are associated with the Default Tenant. Adding custom tenants to CA Performance Center lets you create separate CA Performance Center monitoring environments that you administer from a single user interface. A *tenant* represents a customer environment that a managed service provider administers. Each tenant environment is independent and effectively functions as a separate instance of CA Performance Center. Each instance can contain multiple users and roles that are not shared among tenants.

The basic tenant definition contains a few parameters to identify the MSP customer and let other operators access managed items and configuration for the customer. Each tenant must contain at least one IP domain. You or the tenant administrator can then set up as many of the following definitions as required to manage the enterprise infrastructure and applications:

- SNMP profiles
- Additional user accounts
- Roles
- Custom groups
- Custom dashboards
- Custom menus

Custom IP domains provide the means of associating managed items with their tenants. A valid tenant definition contains at least one custom IP domain. As soon as a valid tenant exists in CA Performance Center, all items whose IP addresses match the tenant domain are associated with that tenant.

Index