Best Practices For Domain Groups

CA Unified Communications Monitor

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: Introduction

CA Unified Communications Monitor (UC Monitor) versions 3.1 and 3.2 support the ability to report on separate enterprise networks with overlapping or redundant IP addresses as separate domains. The ability to monitor using custom domain groups is a feature designed for a managed services environment. Support for this feature is implemented as part of the grouping feature in CA NetQoS Performance Center (NPC) version 6.1.

Monitoring multiple, discrete enterprises as separate domains is a complicated undertaking. This document is designed to help you successfully deploy this multi-faceted feature. Use the best practices in this document to optimize custom domain monitoring while avoiding disruptions to ongoing data collection and reporting in UC Monitor.

Monitoring per domain adds tremendous value for Internet Service Providers (ISPs) who manage the unified communications systems of multiple customers. Deploying domain groups ensures data privacy and allows the ISP to segregate data from separate customer networks, without considering whether addressing schemes produce overlapping IP addresses. Appropriately configured, UC Monitor allows ISP staff to monitor VoIP and video performance within a single domain while preventing individuals from sharing data among domains.

Custom Domains in UC Monitor

Monitoring by domain means that overlapping IP addresses can be monitored separately, with either no or carefully controlled sharing of secure data. The overlapping IP address can correspond to separate enterprise networks or can have different domain name assignments.

When you deploy custom domains in UC Monitor, the phone traffic from entities that use the same IP addresses can be monitored separately. Your current Location definitions can be used to report performance data for each distinct customer environment with an appended domain identifier. UC Monitor operators can be granted access to report data per domain, similar to the way that reporting per group is handled.

Domain support is implemented as part of the grouping feature in NPC version 6.1. To enable monitoring by domain, register the UC Monitor data source with NPC. No domain parameters are available in the Administration section of the UC Monitor management console until you create at least one custom domain group in NPC.

Domains are special system groups that can be customized. Domains organize monitored items into separate containers, but domain groups offer the unique ability to distinguish multiple items that have the same IP address. Domains can be monitored and reported on separately, but the overview reports provide a view of all domains to show which have degraded call performance.

Other UC Monitor groups are populated by group rules or by a manual process. Domains are populated by the collector. When a new managed item is discovered, the collector associates it with a custom domain based on the IP Domain parameter in the collector Properties dialog.

Domains also possess another trait typical of CA Performance Center groups: they are a shared configuration resource, common to all NPC data sources. Custom definitions created in other data sources can be used in UC Monitor. You can see a list of custom domain definitions from all data sources in the Groups tree.

When to Use Custom Domains

In many cases, you can use NPC groups and Location definitions within UC Monitor to distinguish separate geographical areas and network architectures within your system. Deployment of custom domain groups requires consideration of your unique situation and requirements.

The custom domain groups feature was designed for a managed services environment. The feature adds significant value for large Internet Service Providers (ISP), with multiple customers whose networks can contain redundant IP addresses or even phone numbers. In such a situation, custom domain groups allow you to monitor data from each customer network separately. ISP staff can be assigned access permissions to items in a single domain.

A less ideal situation for deploying domain groups is a hosted service provider solution, where the provider has full control of call servers and voice gateways. The collectors perform domain separation and associate managed items with domains, with each collector placing items into one domain. Therefore, the ISP is responsible for managing multiple collectors to accommodate all domains. Issues with firewalls and private networks also come into play, depending on how the ISP has segregated each hosted solution. A collector on the customer network must be able to communicate with a central management console at the data center that the ISP manages.

Chapter 2: Domains in CA NetQoS Performance Center

NPC domains provide a way to indicate that two managed items that otherwise appear as duplicate IP addresses are actually two different IP addresses. Monitoring by domain allows for NPC data sources to be deployed in a service provider environment, in which multiple networks can be monitored as separate entities.

Domain monitoring is enabled for each data source that is registered with NPC. However, domain identifiers and configuration parameters are not visible in the data sources until at least one custom domain group is created in NPC. The following managed types are associated with the default domain after domain monitoring is enabled:

- Devices
- Interfaces and interface addresses
- Networks
- Locations

The collector populates all domains that are known to UC Monitor. The collector associates all items that it discovers with the default domain until the administrator selects a custom domain in the collector Properties dialog. After the collector creates a domain association for managed items, UC Monitor reports a domain identifier during synchronization with NPC. The information is stored in the UC Monitor database with a DomainID property. Items whose domain IDs are not reported are automatically placed in the default domain.

Domains are shared among data sources that are registered to the same NPC instance. Domain containers appear in the NPC Groups tree as system groups. However, the Group Properties view does not itemize the items that are assigned to each container.

NPC domain administration lets you specify a primary and secondary name server for each domain you define. UC Monitor uses only the primary DNS server, but in an environment with multiple data sources, these parameters can be useful. Other data sources also allow multiple domains to share DNS name servers by using parameters for a proxy server address and a port number on each server.

How Domain Associations Vary

Some managed items are directly associated with domain identifiers when they are stored in the UC Monitor database. These items, which report a domain ID to NPC during synchronization, include the following types:

- Locations
- Voice gateways and other media devices
- Call servers
- Collectors

Other items are only indirectly associated with domains because they have a relationship to a managed item with a domain identifier:

- Phones—Associated with call servers, which have domain IDs
- Call server groups—Contain call servers, which have domain IDs
- Subnets—Included in Locations, but not directly associated with domain groups
- Voice interfaces—Associated with voice gateways, which have domain IDs
- Trunk Groups—Contain voice interfaces.

These items have no direct association with a domain. Therefore you can place them into groups that span multiple domains. For example, you can create a group of voice interfaces from voice gateways that are associated with different domains. Or you can add call servers from different domains to a single call server group. However, creating such cross-domain groups is not recommended in most circumstances.

Threshold assignments can also span domains. Without proper attention to domain associations, you might assign a Call Server Group threshold to a group that contains call servers from multiple domains. Such a threshold assignment is not recommended. Similarly, codec thresholds are not available per domain. They are subnet- and domain-agnostic and only apply to the type of codec that is detected from call traffic.

SNMP profiles are cross-domain parameters by default, but, like thresholds, SNMP profiles can be exclusively assigned to devices in a domain. Each voice gateway, for example, can be edited to select an SNMP profile. Creating an SNMP profile for each domain is a recommended best practice. If you create such a domain-specific SNMP profile, use a naming convention to help you identify it.

Enabling Domains

An administrator defines domains in the Manage Groups section of the NPC Admin tab. After domain definitions are synchronized with the data sources, they are available for the UC Monitor administrator to assign to collectors. At least one custom domain must be created in NPC before the necessary parameters are exposed.

After a custom CA Performance Center domain is created and synchronization occurs, the UC Monitor management console displays the required parameters in various places throughout the Administration section. The Location List reflects the new domain and the new default Locations for the External, None, and Unassigned categories. A custom domain requires one default Location for each category so that all phones detected in call traffic can be properly classified, even phones in subnets that do not fall into one of the defined Locations. Domain designations also appear in report views, where domain identity is indicated by an additional “IP Domain” column in the data tables.

The UC Monitor administrator can edit the properties of each collector to customize the IP Domain parameter that appears when custom domains are enabled. The collector immediately begins associating items with the custom domain.

Chapter 3: Best Practices

Using domains in UC Monitor requires configuration in both NPC and the UC Monitor management console. As a result, implementing domain monitoring in your environment requires coordination between product interfaces and the intervention of the administrators for both NPC and UC Monitor. The topics in this section are intended to help you implement custom domains without disrupting ongoing data collection.

Locations

The collector associates discovered items with a custom domain. Domain associations are not applied retroactively, nor are they applied to items that the collector does not discover. Some managed items in UC Monitor are manually defined. Phones, call servers, and voice gateways are discovered during monitoring. Locations and call server groups are not. You edit Location definitions to select a custom domain, otherwise the Locations are placed in the default domain.

Items that the collector rediscovers after custom domains are implemented can be associated with a domain. However, it is more time-consuming to assign items to custom domains after collection is underway. Therefore, we recommend using a fresh product installation to deploy this feature. As a best practice, enable custom domain monitoring before creating Location definitions. Doing so will also avoid filling your database with redundant data from items that are duplicated before the domain association and after it has been applied.

Assign Domains to Existing Locations

You can deploy custom domains after Location definitions are already in use, but it requires a few more steps. All Locations that were previously defined continue to be associated with the default domain until you manually edit Location properties.

The following steps are an overview of the process. The UC Monitor online help provides complete instructions.

Follow these steps:

1. Export the current list of Location definitions.
2. Verify the contents of the exported .csv file.
3. Delete all Location definitions.
4. Import the .csv file, selecting the new domain in the IP Domain parameter.

As a best practice, ensure that no Location is associated with the default domain. This domain is not readily identified in reports, which makes it difficult to distinguish customer data. For the same reason, be conscientious in assigning all phone subnets, at all customer sites, to Location definitions. The Unassigned Location appears the same in reports for all domains.

Purge Duplicate Locations from the Database

After assigning domains to Locations, the database can duplicate Location entries from before and after the association. As a best practice, purge the duplicate entries. The UC Monitor database purging option does not let you selectively prune the database on a per-domain basis. Also keep in mind that automatic weekly database maintenance applies to the entire console, not to a selected domain.

The maximum call density for the UC Monitor database is ten million calls for one month. In our testing, we divided the ten million calls by the number of domains, assuming that most monitored customer networks have similar numbers of phones and similar call activity. However, your situation, and that of your individual customers, can be more variable.

When your individual customer networks have large call volumes, consider employing separate management consoles for each domain and register each as a data source for the same NPC instance. You can register up to four UC Monitor data sources. In most cases, however, multiple data sources are not necessary. Judicious database pruning and maintenance will allow for excellent report performance.

User Accounts and Permissions

We recommend adding custom domain groups to the user accounts listed in NPC so that UC Monitor operators can see the items that they contain. As you update user accounts, keep in mind the following points:

- The administrator typically needs access to all domain groups.
- Each product operator with user account privileges should only be granted access to a single domain.
- A user with permission to see any managed item in a custom domain also has automatic access to data from all other items in that domain group.

  It is not necessary to grant users explicit permission to see the items in a domain group.
- Do not add the All VoIP Locations group to user permissions in a multiple-domain environment.

  If a UC Monitor user permission set has the All VoIP Locations Group, that user has access to data from all domains.

Factors to Consider

As you analyze reports from different customer domains, remember that user account permissions determine the items each UC Monitor operator sees in reports. This rule also applies to options in the Administration pages. The administrator typically needs access to all domain groups for easy management of domain settings. For example, the administrator must see domain identifiers for all collectors, Locations, call servers, and voice gateways. These identifiers are concealed from users without the necessary permissions. In NPC, use the Permission Groups section of the Edit User page to add all domain groups to the permission set of each administrator account.

Generally, users cannot see the Administration options. They can see items for their own user account, such as their time zone and schedules they created for sending reports by email. In certain circumstances, users are prevented from seeing items in their own accounts because they do not have permission to see the relevant domain. Keep in mind this point when updating or troubleshooting issues with user accounts.

Each product operator with user account privileges should only be granted access to one domain. Generally, individual users only need access to one domain. This method of assigning permissions ensures appropriate security of data from separate customer networks.

AVAYA MONITORING TIP: Avaya trunk groups are managed items that lack domain identifiers. As a result, they are not included when you add domains to user account permissions. Add them as individual permission groups. Locations, media devices, and call servers are managed items, with domain identifiers based on your collector configuration. In contrast, Avaya trunk groups are treated as groups in NPC, and groups do not have domain identifiers.

Restricting Call Watch Access

We recommend restricting most users from viewing Call Watch data in a deployment with multiple custom domains. Because the UC Monitor Call Watch feature does not support domain identification, you cannot restrict user account access to a subset of Call Watch data. If data privacy is a concern, prevent user access to all Call Watch data by removing that permission from their user account role.

With no domain identification for a Call Watch definition, you can create a Call Watch for a phone in the network of Customer A and find that a phone in the network of Customer C, with the same phone number, is also watched.

Thresholds

Administrators who customize and assign thresholds to Locations need explicit permission to view all domain groups. The Threshold List section of UC Monitor Administration does not include information to identify threshold settings for selected domains. To apply custom thresholds for each domain, use a naming convention for the custom settings that identifies the intended domain.

The incident response actions that you associate with thresholds also lack a domain identifier. Therefore, create separate thresholds with separate incident responses and associated actions for each domain so that notifications can be sent to the appropriate IT staff member. Each staff member should only be able to see data from one domain. With custom incident responses, as with thresholds, use a naming convention to identify the domain in the Incident Response List.

You may think that report settings (specifically, custom filters) are domain-agnostic. Even users whose permissions do not include a domain can see that domain name in the Settings dialogs. But such filtering is applied to reports only when the user permissions allow access to data associated with a selected domain.

NAT Environments

Network Address Translation (NAT) requires some extra planning during UC Monitor installation. When NAT is not active, you can configure the collector by selecting the IP address of the NICs from the Add Collector Administration page. However, in a NAT environment, the management console cannot identify the management IP address because it has been translated after passing through the firewall. The management console discovers collectors but cannot necessarily find the correct address for NICs whose addresses were translated by a firewall.

As a best practice, record the IP address of the management and monitor NIC as you complete the hardware setup steps on each collector. Then you can select the correct address for each when you add the collector to the management console.

Manual configuration of managed items, such as call servers and voice gateways, lets you find the DNS hostname when you know the IP address. You can also find the IP address when you know the DNS hostname. In a NAT environment, these options can return the wrong address if DNS is not properly configured.

And as with any active firewall, open the required ports to allow communications among UC Monitor components. A list of required ports is provided in the *CA Unified Communications Monitor Installation Guide*.

Deleting Domain Groups

Domain associations are stored with managed items in the UC Monitor database. As a result, domains that are used in UC Monitor cannot be deleted from NPC. Deleted domain groups are marked as inactive in UC Monitor and not exposed in reports that display new data.

Inactive domains are mostly invisible and do not interfere with ongoing monitoring or reporting. You can unregister a UC Monitor data source that contains inactive domains. However, reregistration of the data source sends the domain group back to NPC during synchronization because managed items in the UC Monitor database retain the association.

In most cases, the following work flow is recommended for deleting a custom domain group definition:

1. Delete the domain group from the NPC Groups tree.
2. Remove the IP Domain assignment from the collector Properties dialog in UC Monitor Administration.

We recommend selecting another custom domain for the collector. Otherwise, the collector associates items with the default domain.

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

Chapter 4: Conclusion

Customers who subscribe to managed unified communications services expect excellent performance from the systems. Generally, end users have a low tolerance for poor call quality because they are accustomed to the reliability and clarity of the PSTN. UC Monitor can help you monitor end-to-end VoIP and video call performance for multiple customers while still maintaining data privacy. By deploying custom domain groups in NPC, UC Monitor operators can track and troubleshoot call setup and call quality on separate customer networks from one reporting console.

This document prescribes steps to take to configure and deploy custom domain groups for the greatest potential gain in monitoring scope, IT staff productivity, and console performance. However, custom domain groups represent a new product feature. We cannot claim to have tested this feature in every possible network architecture, nor have we encountered every potentially confusing aspect of custom domain deployment with NPC. We encourage you to engage in an ongoing conversation with your CA Sales or Technical Representative to keep this document up to date with information useful to you and others who deploy this feature.