CA Spectrum® and CA Performance Center

Integration Guide

CA Spectrum Release 9.3 - CA Performance Center r2.3.00

CA Technologies Product References

This document references the following CA Technologies products:

- CA Spectrum®
- CA Performance Center
- CA NetQoS® Performance Center
- CA Infrastructure Management Data Aggregator (Data Aggregator)
- CA Network Flow Analysis (formerly CA ReporterAnalyzer™)
- CA Application Delivery Analysis (formerly CA SuperAgent®)
- CA NetQoS NetVoyant® (NetVoyant)

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 7

Understanding the CA Spectrum - CA Performance Center Integration 7
- Solution Architecture 8
- Upgrade Considerations 10
- Supported Features 10

Component Requirements 12
- Model Synchronization Eligibility 13
- Device Model Synchronization 13

Chapter 2: Configuring the Integration 15

How to Integrate CA Spectrum and CA Performance Center 15
- Configure CA Spectrum as a Data Source in CA Performance Center 16
- Enable Event Polling in CA Spectrum 18

How to Enable CA Spectrum Device Monitoring with CA Infrastructure Management 19
- Add an SNMP Profile to Gather Performance Data 20
- Add Device Models to CA Performance Center IP Domain Models 22
- Enable Synchronized Discovery 26

Chapter 3: Using the Integration 27

Support for CA Performance Center IP Domains 27
- Error When Adding Device to IP Domain 28

Pingable Devices in CA Performance Center Have Little Data 28

Group Synchronization 29
- Enable Tenant Access to Data 29

Drill Down into CA Performance Center Performance Data 31

Known Anomalies 31

Chapter 4: Maintaining the Integration 33

Modifying Data Sources After Integration 33

Restoring the SpectroSERVER Database 33

Remove CA Spectrum as a Data Source in CA Performance Center 34

Enabling Debug Logging 35

Appendix A: Support Additional Event Types 37

How to Configure Events for Integration with CA Performance Center 37

Obtain a Developer ID 38
Update the netqos-integration-application-config.xml File 38
Update the Event Disposition File 40
Create Event Format Files 41
Create Probable Cause Files 41
Deploy the Changes 42

Index **47**

Chapter 1: Introduction

This section contains the following topics:

Understanding the CA Spectrum - CA Performance Center Integration (see page 7)
Component Requirements (see page 12)

Understanding the CA Spectrum - CA Performance Center Integration

CA Spectrum - CA Performance Center integration lets you share models, Global Collections, and events between two powerful infrastructure management systems.

The CA Spectrum data source contributes the following item types to CA Performance Center:

- Devices
- Interfaces
- Groups

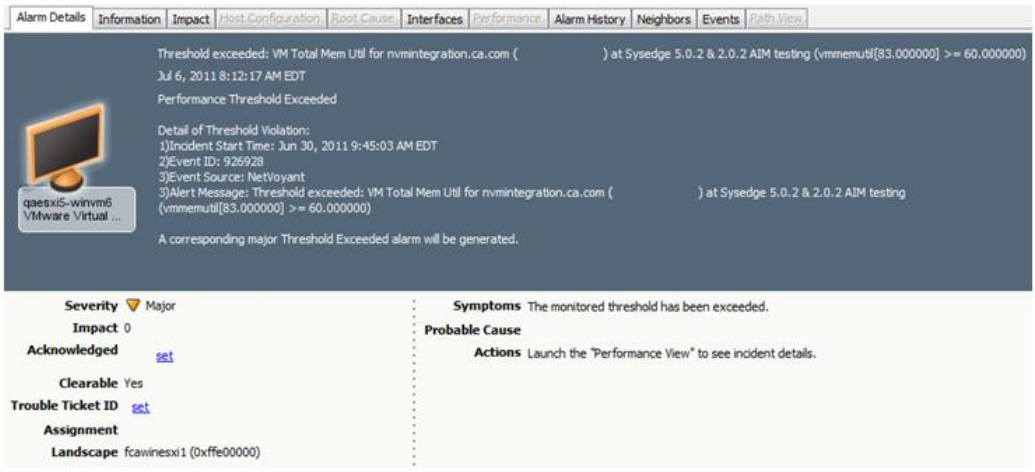
CA Spectrum also retrieves and displays infrastructure performance events from the CA Performance Center Event Manager. As a result, you can see performance and fault alarms side-by-side in OneClick.

CA Performance Center retrieves devices from CA Spectrum to extend the CA Performance Center device Inventory. You can determine which devices are retrieved. The interfaces that are associated with each device are added to the Inventory automatically; however, they are subject to CA Infrastructure Management Data Aggregator interface filtering.

CA Performance Center IP domains are synchronized and displayed in OneClick. You can add device models to them. The items in these IP domains are synchronized with CA Performance Center, and their data is included in dashboards. Your CA Spectrum Global Collections become groups in the CA Performance Center Groups tree.

The integration extracts event data from the CA Performance Center Event Manager and converts it into CA Spectrum events. These events then raise CA Spectrum alarms on models in the SpectroSERVER topology. As clear events are processed, corresponding CA Spectrum alarms are cleared automatically. Polling for supported events begins when synchronization has completed. These events are converted into CA Spectrum alarm set or clear events and asserted on models in each landscape.

Alarms based on device performance, such as Time over Threshold and Deviation from Normal events, are generated in CA Spectrum to supplement fault and availability monitoring. The CA Spectrum alarms that originate in the Event Manager can be viewed in the OneClick Console.



Finally, the integration enables a Data Aggregator data source to discover CA Spectrum devices without requiring you to manually create discovery profiles. The system creates discovery profiles, which are scheduled by default but can also be run manually.

Solution Architecture

The following facts describe the architecture of the CA Spectrum - CA Performance Center integration:

- One SpectroSERVER or a Distributed SpectroSERVER (DSS) can be synchronized with CA Performance Center by specifying the OneClick web server as a CA Performance Center data source.
  - Full synchronization occurs when the data source is first added to CA Performance Center.

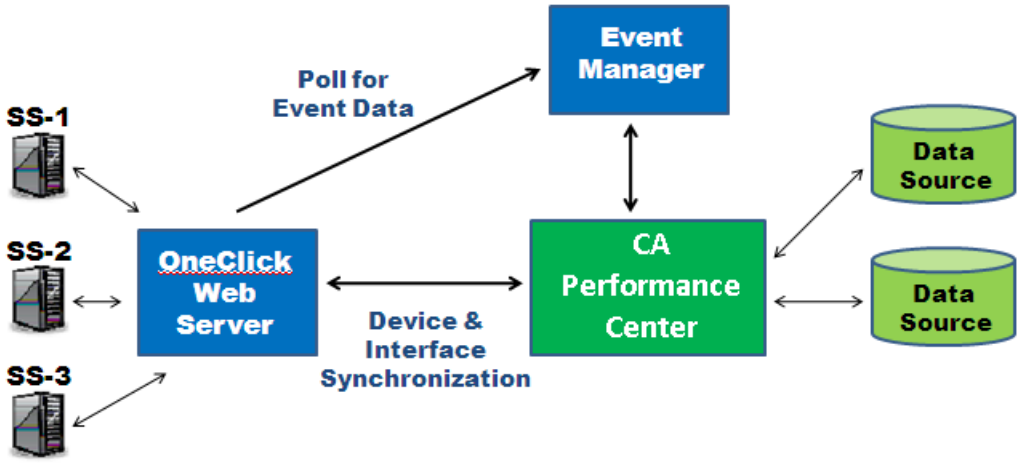
    Important! If a full synchronization is required after you add the data source, we recommend running it during nonbusiness hours.
  - Incremental synchronization occurs every 5 minutes.

    Additions, removals, and modifications of devices, interfaces, and Global Collections in CA Spectrum are reflected in CA Performance Center after incremental synchronization.
- Each landscape in the DSS is defined as a CA Performance Center group.
- Devices and interfaces in the DSS are synchronized with CA Performance Center and added to the appropriate landscape group.

- OneClick polls the Event Manager for events that are relevant to a specified landscape group. This polling happens every 60 seconds by default. Any retrieved events are then translated to CA Spectrum events, which can generate or clear alarms.

  Important! CA Performance Center-related alarm processing in CA Spectrum applies to device and interface models that have been synchronized to CA Performance Center. Only events that are related to devices or interfaces that are modeled in CA Spectrum are processed by OneClick.

- The Event Manager database is polled for supported events at each polling interval. With CA Performance Center v2.0.00 and later, you can modify supported events (see page 37).



Upgrade Considerations

In previous versions of the CA Spectrum - CA Performance Center integration, all CA Spectrum models were contributed to the CA Performance Center Inventory. And these models were always associated with the Default IP Domain. With CA Spectrum Release 9.3 and CA Performance Center Release 2.3, you can precisely control the items that CA Spectrum contributes to CA Infrastructure Management, and you can control IP domain membership. The OneClick features for creating and maintaining Global Collections can now be applied to IP domains.

Be sure to account for the following key considerations when you are planning for the integration:

- Only those models that you have added to a CA Performance Center IP Domain model in OneClick are synchronized with CA Performance Center.
- The devices are added to CA Performance Center based on the specific CA Performance Center IP Domain with which the device models are associated in CA Spectrum.
- If you are upgrading an existing integration, you must at minimum define the contents of the default CA Performance Center IP Domain model in CA Spectrum. You can add additional IP domains as required in the CA Performance Center Admin pages.
- To move a device from the CA Performance Center Default IP Domain to another domain, you must first add the device to the desired IP Domain in CA Spectrum.

  If the device already exists in CA Performance Center, however, you must delete the device from the Default IP Domain. At the next synchronization, the device will be added to the updated IP domain in CA Performance Center.

Supported Features

Important! Many of the integration features in CA Spectrum Release 9.3 are *only* supported by CA Performance Center r2.3.00.

Earlier versions of CA Spectrum integrate with both CA NetQoS Performance Center v6.1 and CA Performance Center v2.0.00 through r2.2.00. To integrate with CA Performance Center versions that predate r2.300, consult an earlier version of this guide.

The following list identifies supported features in the integration between CA Spectrum Release 9.3 and CA Performance Center Release 2.3.00.

Events

- ThresholdViolation events: These events from Data Aggregator and CA Network Flow Analysis data sources are integrated and supported by default in CA Spectrum.
- Other events: By updating an XML file and some event support files, you can instruct OneClick to handle events in the Event Manager database that were reported by other data sources.

IP Domains

- CA Performance Center IP domains are synchronized as CA Performance Center IP Domain models in OneClick. Place device models into CA Performance Center IP Domains manually, or define collection rules to dynamically collect device models. The contents of the CA Performance Center IP domain model are used to keep the IP domain membership up to date in CA Performance Center. As new devices are sent to CA Performance Center from CA Spectrum, they are assigned to the IP domain that corresponds to their CA Performance Center IP Domain membership in CA Spectrum.

Groups

- Your CA Spectrum Global Collections and landscapes are synchronized with CA Performance Center and displayed as groups in the CA Performance Center Groups tree. As part of the Groups tree, you can leverage the synchronized Global Collections in a variety of ways:
  - Create reporting groups
  - Define site membership
  - Drive the content of other custom groups and collections
- CA Spectrum devices can be added to CA Performance Center Service Provider groups and shared among multiple tenant users.

Drilldown from OneClick to CA Performance Center Performance Data

- You can access CA Performance Center performance data from CA Spectrum device and interface models. You gain rapid access to information about device performance issues in context.

Synchronized Discovery

- Shared discovery eases administrative burden.
- Place CA Infrastructure Management Data Collectors where you require them and leverage discovery data from multiple SpectroSERVERs. Determine the appropriate number of IP Domains that are required, and deploy a Data Collector for each IP Domain.

  At device inventory synchronization, Data Aggregator determines whether each device is new or is already in the inventory. When Data Aggregator encounters a device that it is not monitoring, it adds the IP address to a predefined Discovery profile. A discovery profile is defined for each IP Domain. The IP address for each device is added to the corresponding discovery profile based on its membership in a CA Performance Center IP Domain model within CA Spectrum. You can then run this Discovery profile manually, or you can let it run once a day through an automatically configured threshold.

Intelligent Interface Synchronization

- Device monitoring by CA Spectrum always includes all associated interfaces. CA Performance Center retrieves information about all interfaces from CA Spectrum.

  However, the interface inventory in CA Performance Center does not include interfaces that have only been contributed by CA Spectrum. Instead, the inventory is filtered to include interfaces that are monitored by a performance monitoring data source, such as Data Aggregator or CA Network Flow Analysis.

Component Requirements

CA Spectrum - CA Performance Center integration requires the following component versions:

Required components:

- CA Spectrum Release 9.3
- CA Performance Center Release 2.3.00

  Consult an earlier version of this guide if you plan to integrate CA Spectrum Release 9.3 with CA NetQoS Performance Center v6.1 or an earlier version of CA Spectrum or CA Performance Center.

Optional components (use the latest versions):

- Data Aggregator (Required to enable many integration features)
- CA Network Flow Analysis
- CA Application Delivery Analysis

You can find the specific versions of supported data sources in the Compatibility section of the CA Support website.

Model Synchronization Eligibility

One of the following sets of criteria must be met for a CA Spectrum model to be eligible for synchronization with CA Performance Center:

- Models that are derived from CA Spectrum model type *Device* that have:
  - A valid IP address
  - Membership in a CA Performance Center IPDomain model
  - A Model_State (attribute 0x1007c) of Active

    Note: If Model_State is not Active, processing of the model is postponed until the next synchronization.
- Models that are derived from CA Spectrum model type *Port* that have:
  - A parent device that has been synchronized, which means that the parent device is Active and is a member of a CA Performance Center IP Domain
  - A valid IfIndex value

Device Model Synchronization

For device model synchronization, CA Spectrum-CA Performance Center integration uses Model_Class (attribute 0x11ee8) to determine the CA Performance Center SubType of a device, as follows:

Model_Class	SubType
Router	Router
Switch-Router	Router
Switch	Switches
Workstation-Server	Workstations

The default SubType of 'Other' is used for models whose Model_Class is not specified in the table.

Note: The table above shows the specific mappings of Model_Class to device SubType for CA Spectrum data sources. If the device is contributed by additional data sources, such as Data Aggregator, it is possible that CA Performance Center will display a different SubType for the device.

Chapter 2: Configuring the Integration

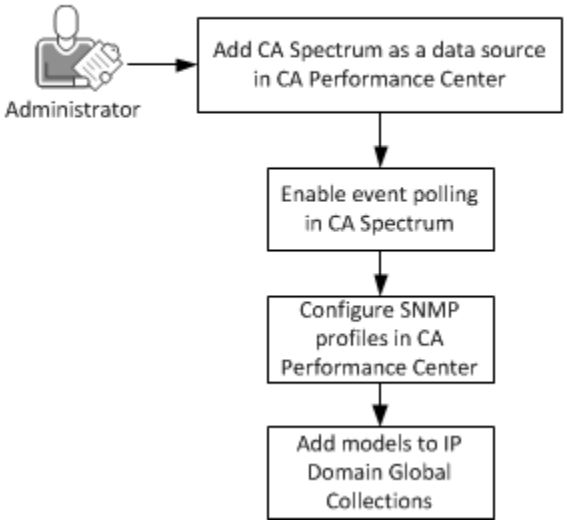
This section contains the following topics:

How to Integrate CA Spectrum and CA Performance Center (see page 15)
How to Enable CA Spectrum Device Monitoring with CA Infrastructure Management (see page 19)

How to Integrate CA Spectrum and CA Performance Center

The following diagram shows the major steps that are required to configure the CA Spectrum and CA Performance Center integration:

Integrating CA Spectrum and CA Performance Center



If you plan to have Data Aggregator discover the devices that CA Spectrum contributes (the optional Step 5, below), register the Data Aggregator data source (see page 26) first, and enable the option to Discover Devices from other Data Sources. Data Collectors must also be installed for each IP Domain to which CA Spectrum will contribute device models.

Follow these steps:

1. Configure CA Spectrum as a Data Source in CA Performance Center (see page 16).
2. Enable Event Polling in CA Spectrum (see page 18).
3. Configure SNMP Profiles in CA Performance Center. (see page 28)
4. Add Models to IP Domain Global Collections (see page 22).
5. (Optional) Enable Discovery Synchronization with CA Infrastructure Management Data Aggregator (see page 19).

The optional step to enable discovery synchronization involves some configuration in CA Performance Center and in the Data Aggregator component.

Configure CA Spectrum as a Data Source in CA Performance Center

Add CA Spectrum as a data source in CA Performance Center so that these components can share information.

Follow these steps:

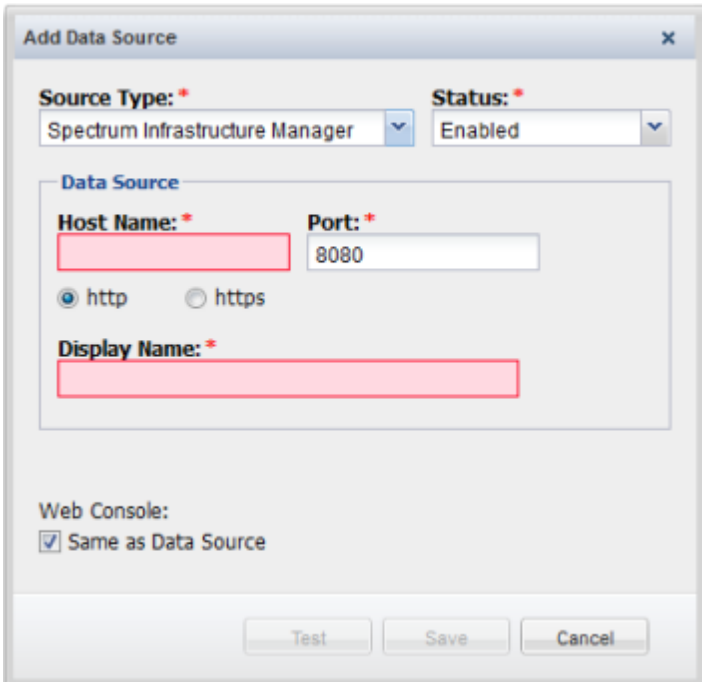
1. Launch the CA Performance Center console and click Admin, Data Sources.

   The Manage Data Sources page opens.

2. Click Add.

   The Add Data Source dialog opens.

3. Select 'Spectrum Infrastructure Manager' in the Source Type field.



4. Complete the following fields:

   - **Status**. Select Enabled in the Status field.

     Tip: You can select Disabled to disable the data source without deleting it.

   - **Host Name**. Provide the IP address or DNS host name of the OneClick server.
   - **Port**. Provide the port number to use when contacting the OneClick server.
   - **Protocol**. Select the protocol to use to contact the data source. Select **https** if your network uses SSL for communications. Verify that you have configured the system correctly before you select the https **option**.
   - **Display Name**. Provide a name for the data source. By default, the data source type and the host name are combined to create the display name.

- **Same as Data Source**. Select the check box if the Web Console is on the OneClick server.

  Or clear the Same as Data Source check box if the Web Console is on a different server. Then complete the following fields:

  - **Host Name**. Provide the IP address or DNS host name of the Web Console server.
  - **Port**. Provide the port number to use when contacting the Web Console server.
  - **Protocol**. Select the protocol to use to contact the Web Console server: http or https.

5. Click Test to verify that CA Performance Center can contact the OneClick server and the Web Server.
6. Click Save.

   You have added CA Spectrum as a data source and the synchronization process is initiated.

Enable Event Polling in CA Spectrum

Enable event polling that takes place between the SpectroSERVER and CA Performance Center. You can specify how often CA Spectrum queries the CA Performance Center Event Manager component for events. Perform this step in the OneClick Administration pages.

Follow these steps:

1. Click Administration in the OneClick home page.

   The Administration Pages open.

2. Click Performance Center Integration Configuration in the left panel.

   The Performance Center Integration Configuration page opens.

3. Enter the desired polling interval, in seconds, in the Event Polling Interval field.

   The default value is 60 seconds. Enter a value greater than or equal to 30 seconds.

4. Select the Enabled option in the Event Polling field.
5. Click Save.

   CA Spectrum - CA Performance Center integration is now enabled. The event polling settings take effect on the next polling cycle.

How to Enable CA Spectrum Device Monitoring with CA Infrastructure Management

The integration between CA Spectrum and CA Performance Center lets a Data Aggregator monitor CA Spectrum devices. This configuration is optional and requires some additional configuration. We recommend performing these optional steps before you register the CA Spectrum data source.

To enable CA Infrastructure Management monitoring of the devices and interfaces that CA Spectrum discovers, take the following steps:

1. Create SNMP profiles in CA Performance Center (see page 20) for the SNMP-capable devices that are modeled in CA Spectrum.
2. Create IP domains in CA Performance Center. For more information, see the online Help for CA Performance Center.

   When database synchronization occurs, all IP domains are sent to CA Spectrum, where they appear in OneClick as special Global Collections, with a unique icon.
3. Install and assign a Data Collector for each IP domain.
4. Enable the CA Infrastructure Management Data Collector to discover CA Spectrum devices (see page 26).

   Synchronized discovery requires less administration and enables your SpectroSERVERs to provide data to the Data Collectors that you can position where they are required.
5. Add the models to the appropriate IP Domains in OneClick (see page 22).

   During synchronization, all CA Spectrum models that are associated with the CA Performance Center IP Domains are passed to the CA Infrastructure Management Data Aggregator. The associated CA Spectrum devices are discovered for CA Infrastructure Management Data Aggregator monitoring.
6. Create custom monitoring profiles for CA Spectrum devices and apply them to collections in the Data Aggregator administration pages.

   Monitoring profiles for a limited set of metrics are applied to the device items as Data Aggregator discovers them. These profiles determine how devices are polled for performance data. For more information, see the online Help for CA Infrastructure Management Data Aggregator.

As CA Spectrum adds devices to CA Performance Center, they are added to discovery profiles. Each discovery profile is automatically configured to run with a daily schedule. You can also run them manually or adjust the schedule as required to keep the Data Aggregator up-to-date with new devices from CA Spectrum.

If SNMP throttling is configured on CA Spectrum, it does not apply to ongoing polling by Data Aggregator. This feature protects critical devices from failing in case too many polling flows are configured. The throttling mechanism applies to any monitoring or discovery activities. Therefore, if you have configured CA Spectrum to throttle SNMP requests for a given device, apply the same setting in Data Aggregator.

Add an SNMP Profile to Gather Performance Data

To supply the information that is required to enable SNMP polling for performance metrics, create SNMP profiles in CA Performance Center. Global administrators and tenant administrators can create SNMP profiles to let CA Performance Center data sources query devices for performance data. You can create these profiles for SNMPv1/v2c or for SNMPv3.

Device models are contributed to CA Performance Center with specific IP Domains. The IP domain may be part of the default tenant or a user created tenant. When you create SNMP Profiles to discover devices that CA Spectrum contributes, verify that the SNMP Profiles are created in the appropriate tenant space

Follow these steps:

1. Log in to CA Performance Center as a global administrator or tenant administrator.
2. (Optional) If you have logged in as a global administrator, administer a selected tenant.
3. Select Admin, SNMP Profiles in the menu bar.

   The Manage SNMP Profiles page displays the current list of SNMP profiles.
4. Click New.

   The Add SNMP Profile dialog opens.
5. Complete the fields and change any default settings as needed. Some fields apply only to SNMPv3.

   Profile Name

   Defines a name for the SNMP profile. Profile names must be unique, cannot be duplicated across SNMP versions, and are not case-sensitive.

   SNMP Version

   Specifies the version of SNMP that the profile uses. Because SNMPv1 and SNMPv2C are similar from a security standpoint, they share a single option. SNMPv3 is a separate option.

Port

Identifies the port that is used to make SNMP connections to devices associated with this profile.

Note: Optional parameter for SNMPv1/v2C.

Default: 161.

User Name

(SNMPv3 Only) Identifies the user for the profile, whose secret keys were used potentially to authenticate and encrypt the SNMPv3 packets. The User Name is a character string.

Context Name

(SNMPv3 Only) Identifies the collection of management information that is accessible by an SNMP entity. An octet string that is necessary for providing end-to-end identification and for retrieving data from an SNMPv3 agent.

Community Name

(SNMPv1/v2C Only) Defines a secure string that lets the data source query the MIB of the associated device. The community that you supply must provide read-only access to the device MIB.

Note: In the default SNMP profile, the community is 'public'.

Verify Community Name

Confirms the secure community string (name).

Authentication Protocol

(SNMPv3 Only) Specifies the authentication protocol to use when contacting devices associated with this profile. The following algorithms for authenticating SNMPv3 packets are supported:

- None (do not attempt authentication)
- MD5 (Message Digest 5)
- SHA (Secure Hash Algorithm)

Authentication Password

(SNMPv3 Only) Specifies the password for authentication using SNMPv3 and the selected authentication protocol.

Note: Supply an authentication password that contains at least eight characters. Some data sources do not support authentication passwords or privacy passwords that fall below this minimum length. They treat the SNMP profile as invalid, and some data is not collected. Blank passwords are not supported for SNMPv3 profiles with MD5 or SHA as the Authentication Protocol.

Verify Authentication Password

Confirms the authentication password.

Privacy Protocol

(Optional) Specifies the encryption protocol to use for data flows sent to any devices or servers associated with this profile, as follows:

- None (do not encrypt communications)
- DES
- AES 128
- Triple DES

Note: The privacy protocol option is not enabled until authentication is enabled for this profile.

Privacy Password

Defines the password used when exchanging encryption keys. See the Note for a possible length requirement.

Verify Privacy Password

Defines the password used when exchanging encryption keys.

Use by default for new devices

Specifies whether the information in this profile is used by default. CA Performance Center uses this information to contact any new items that are discovered from monitored traffic. If it fails, the next profile in priority order is used. Disable this parameter to exclude a profile from discovery.

Note: This parameter does not apply to CA Infrastructure Management Data Aggregator data sources.

6. Click Save.

   The Manage SNMP Profiles page opens. The new profile appears in the list.

   CA Performance Center automatically performs a global synchronization to send the profile information to all registered data sources.

Add Device Models to CA Performance Center IP Domain Models

After database synchronization occurs, the IP domains that you created in CA Performance Center are displayed as CA Performance Center IP Domains in OneClick. The device models that you add to these IP Domains are associated with IP domain definitions in CA Performance Center, polled by Data Aggregator, and included in dashboards.

You can also apply Search criteria to an IP Domain or Global Collection (see page 24) so that its membership is updated dynamically.

Although CA Performance Center IP Domain models are not Global Collections, they share many properties. Consequently, the configuration of a CA Performance Center IP Domain uses many of the common Global Collection dialogs. But these IP Domain models are designated with a special icon in OneClick: 

Note: CA Spectrum devices can only be members of a single IPDomain model type. If you attempt to add a model to multiple IP domains, you see an error message (see page 28).

Follow these steps:

1. In any topology, take *one* of the following steps to select a device model to add to an IP Domain:

   - **Single model selection:** In the Navigation panel, right-click a modeled element and select Add To, Global Collection(s).

     The Select Global Collections dialog opens. CA Performance Center IP Domain models appear in the list among your Global Collections.

     Note: Or you can right-click a single model in a topology view and select Add To, Global Collection(s).

   - **Multiple model selection:** To multiselect models in a topology view, take the following steps:

     a. Press and hold the SHIFT key and individually select the modeled elements.

     b. While the SHIFT key is pressed, right-click the last selected modeled element and select Add To, Global Collection(s).

     The Select Global Collections dialog opens. CA Performance Center IP Domain models appear in the list among your Global Collections.

2. Select the name of the IP Domain model where you want to add the models.

   IP Domains are designated with a special icon: 

3. Click OK.

   If Data Aggregator has been configured to discover devices from other data sources, the devices from CA Spectrum are discovered by Data Aggregator at the next synchronization. The devices are added to CA Performance Center with an IP domain association that mirrors the CA Performance Center IP Domain membership in CA Spectrum.

   Verify that SNMP profiles (see page 20) for monitored devices are available in CA Performance Center and create them if necessary.

Update IP Domain Membership Dynamically

In addition to selecting individual models for CA Performance Center IP Domain models, you can populate IP Domains with dynamic members. Adding dynamic members to the models that represent CA Performance Center IP domains lets you precisely populate IP domains with devices that belong to them.

Dynamic membership is based on rules and on search criteria that you specify. Dynamic members of a CA Performance Center IP Domain only remain in the CA Performance Center IP Domain as long as they meet the specified search criteria. Changes are automatically synchronized with CA Performance Center.

Follow these steps:

1. In the Explorer tab of the Navigation panel, navigate to the Global Collections node, and locate the CA Performance Center IP Domains.
2. Right-click a CA Performance Center IP Domain, and select Edit Global Collection.

   IP Domains are designated with a special icon: 

   The Edit Global Collection dialog opens.
3. Click 'Search Options'.
4. Complete any of the following fields to create a single search expression:

   Attribute

   Specifies the attribute of a device to filter. From the drop-down list of commonly used attributes, select the attribute that you want to use. The predefined list might not include the attribute that you want. In this case, click Attribute to specify the model type (device, port, or other) and its associated attribute that you want to find.

   Note: If you choose an alphabetic attribute value, you can either clear (ignore) or select (include) the Ignore Case check box.

   Comparison Type

   Specifies the type of comparison to be made against the value that is specified in the Attribute field. Only the comparison types appropriate to the attribute data type are available.

   Ignore Case

   Determines whether the comparison is case-sensitive. If you do not select this check box, the comparison is case-sensitive. This selection is only enabled when it is appropriate for the data type of the attribute you selected.

Attribute Value

Enter the desired attribute value to search.

Devices Only

Specifies that the search results list includes only devices.

5. (Optional) To use a wildcard character or regular expression in the Attribute Value field, select a valid attribute in the Attribute field. Select 'Matches Pattern' in the Comparison Type field. Then select one of the following options:

   Specify Wildcard Now

   Lets you search for a value using a wildcard. For more information about the available wildcards, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

   Specify RegExp Now

   Lets you create a search using Perl Compatible Regular Expression (PCRE) matching on attributes of the type 'text string'. Text string searches are available only for Matches Pattern comparison types. PCRE matching helps you to find and group models using specific pattern searches that are more advanced than existing searches or wildcard searches.

6. (Optional) Click the Show Advanced button to create a search that is based on a compound clause. For example you can choose to populate the CA Performance Center IP Domain based on existing Global Collections, or Secure Domain Connector information. For more information, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

7. (Optional) Select the Real-Time Update check box.

   This option disables the update interval. It also adds or removes models from the CA Performance Center IP Domain when they meet or no longer meet the search criteria.

8. (Optional) Supply a value in the 'Run search to update Global Collection membership every <> hours' field.

   This value determines how often OneClick conducts a search to update the dynamic membership of the CA Performance Center IP Domain.

9. Click OK.

   The Search Options dialog closes and the Global Collection dialog opens.

10. Click Landscapes to identify the landscapes to include when searching models to populate the CA Performance Center IP Domain.

11. Click OK.

    The CA Performance Center IP Domain model now has a dynamic membership. Any adjustments that are automatically applied to the membership of this CA Performance Center IP Domain are synchronized to CA Performance Center.

Enable Synchronized Discovery

When you enable the Data Aggregator component to discover CA Spectrum devices, you enable a large set of functionality. The integration can enhance CA Spectrum fault and availability monitoring with device performance alerts that are based on the analysis of historical data. You can also drill down into device performance data in context from OneClick. And you can monitor the same devices with two different infrastructure management systems without additional discovery administration.

Follow these steps:

1. Launch the CA Performance Center console and click Admin, Data Sources.

   The Manage Data Sources page opens.

2. Select the Data Aggregator data source in the list, and click Edit.

   The Edit Data Source dialog opens.

3. Select the option to Discover devices from other data sources.

4. Click Save.

   Enabling the Data Aggregator component to discover devices from other data sources initiates a synchronization of the CA Infrastructure Management device inventory with CA Spectrum. If CA Infrastructure Management determines that a device known to CA Spectrum is not in the CA Infrastructure Management inventory, the IP address of the device is added to an automatically created discovery profile. This discovery profile is configured to run with a daily schedule by default. You can run the discovery manually or adjust the schedule to meet your requirements.

   For more information, see the CA Infrastructure Management Data Aggregator online Help.

Smart Interface Filtering

CA Spectrum can contribute interfaces to CA Performance Center that do not appear in the CA Performance Center Inventory unless they are monitored by another data source, such as Data Aggregator or CA Network Flow Analysis. This behavior results from the Data Aggregator interface filtering feature.

CA Spectrum does not collect performance data from interfaces. As a result, an interface that CA Spectrum discovers and sends to Data Aggregator does not have any visible data in CA Performance Center dashboards unless another data source is also monitoring that interface.

If you right-click an interface model in OneClick, the option to drill down into the matching data context in CA Performance Center is not available to you if that interface is filtered out of the corresponding monitoring profile in CA Infrastructure Management.

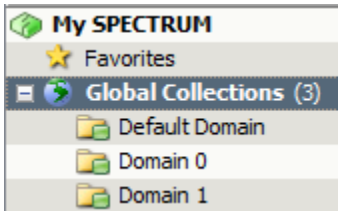
Chapter 3: Using the Integration

This section contains the following topics:

Support for CA Performance Center IP Domains (see page 27)
Pingable Devices in CA Performance Center Have Little Data (see page 28)
Group Synchronization (see page 29)
Drill Down into CA Performance Center Performance Data (see page 31)
Known Anomalies (see page 31)

Support for CA Performance Center IP Domains

When you register the CA Spectrum data source in CA Performance Center, database synchronization occurs. CA Spectrum retrieves a list of IP domains from CA Performance Center. All IP domain definitions are sent over, regardless of their association with individual tenants. OneClickdisplays these CA Performance Center IP Domain models in the same area as CA Spectrum Global Collections in the OneClick Navigation panel. The CA Performance Center IP Domain models have the same names as the CA Performance Center IP domain definitions:



Use these IP domains to determine which models are synchronized with CA Infrastructure Management. To include a device model in CA Infrastructure Management monitoring and make it available in CA Performance Center dashboards, add it to an IP domain (see page 22) in OneClick.

Take care to add only device models that should be synchronized with CA Performance Center. When the device models are synchronized, they are associated with the corresponding IP domain in CA Performance Center. The CA Performance Center IP domain may belong to the Default Tenant, or to any custom tenant. Do not add interface models. Device interfaces are automatically added to the IP domain with which their device is associated.

CA Spectrum devices can only be members of a single IPDomain model type. If you attempt to add a model to multiple IP domains, you see an error message (see page 36).

Error When Adding Device to IP Domain

Symptom:

I tried to add a device to a CA Performance Center IP domain in OneClick. I received an error message that stated, "The following models could not be added to the Global Collection *Domain Name*." An additional statement claimed that the models did not exist. But I have verified that the models do exist in the landscape.

Solution:

You see this message if you attempt to add a device that is already associated with an existing IP domain to another IP domain. This error can occur if, for example, the device was added to the IP domain either manually or dynamically, using a Global Collection rule. The portion of the error message stating that "The model does not exist" is inaccurate. We plan to address this issue in a future version of the CA Spectrum software.

Pingable Devices in CA Performance Center Have Little Data

Symptom:

After synchronization, some devices that CA Spectrum contributed to CA Performance Center appear to have a Subtype of Pingable in the Inventory view. They should be classified as Router or Switch. They are legitimate devices that should be reporting lots of performance data.

Solution:

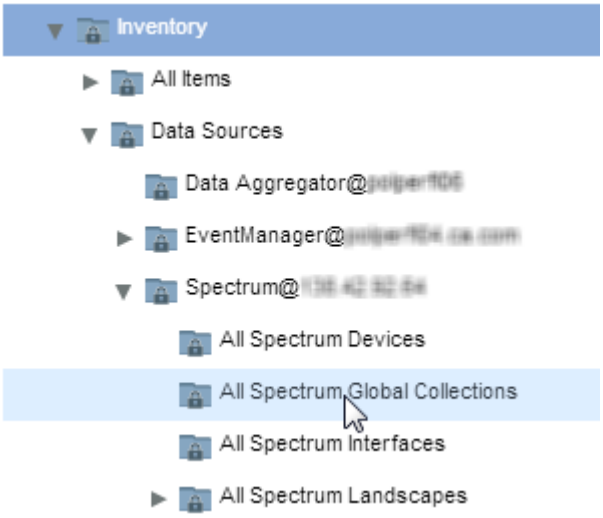
A *pingable device* refers to a device that does not allow SNMP polling and is therefore contacted using ICMP ping tests for status and reachability statistics. Devices that are sent over from CA Spectrum can appear to be Pingable and have only status and availability data because of configuration issues. Take the following steps:

- Make sure that CA Performance Center has an SNMP profile with the appropriate credentials to collect SNNP data from the device. For more information, see Add an SNMP Profile to Gather Performance Data (see page 24).
- Make sure that the correct SNMP profiles are specified in the discovery profile that corresponds to the device.
- Check firewall configuration. If the SNMP and discovery configurations are correct, a network ACL or firewall adjustment can be required to enable the Data Collector to collect SNMP data for the device.

Make sure that the Data Collectors that are assigned to the IP domain of each pingable device have network access to the devices. The level of access must be comparable to that of the SpectroSERVER or Secure Domain Connector that monitors the device in CA Spectrum.

Group Synchronization

If you already have CA Spectrum Global Collections that you want to continue to use, they are synchronized with CA Performance Center. All managed items in your Global Collections become members of groups, which are displayed in the CA Performance Center Groups tree.



You can also add those managed items to CA Performance Center Service Provider groups (see page 29), which enable tenant users to manage them and view their data.

Enable Tenant Access to Data

To monitor devices with both CA Spectrum and CA Infrastructure Management, you must explicitly add models to CA Performance Center IP Domains. At the first synchronization, CA Spectrum creates CA Performance Center IPDomain models in OneClick from all IP domains in CA Performance Center, including the Default Domain. Device models within CA Spectrum can then be added to CA Performance Center IP Domains, enabling them to be synchronized with CA Performance Center. Those CA Spectrum devices are always associated with the same IP domain in CA Infrastructure Management and are also associated with the tenant that owns the IP domain.

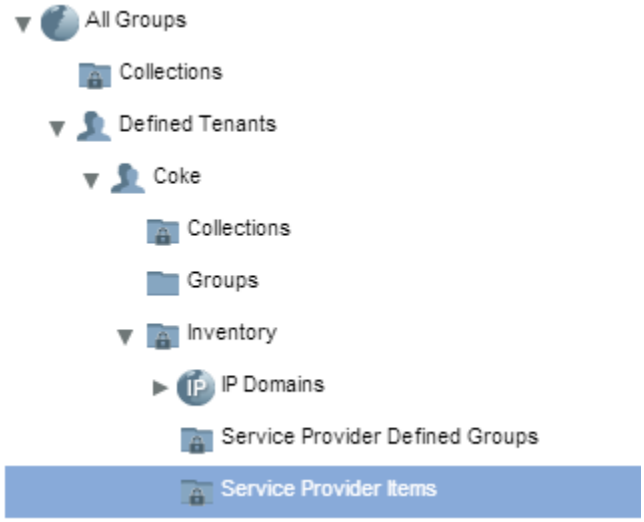
If you choose to associate CA Spectrum device models with IP domains in the Default Tenant space only, you can leverage CA Performance Center Service Provider groups. These groups enable specific tenants to access the devices in CA Performance Center. You can thus grant access to device data to other tenant users. Set up Service Provider groups for tenant users so that they can monitor devices and components that are associated with the Default Domain.

Follow these steps:

1. In OneClick, add the device models that you want additional tenant users to monitor to the Default Domain Global Collection.
2. Log in to CA Performance Center as a user with the predefined Administrator role.
3. Initiate a manual synchronization of the CA Spectrum data source.

   For more information, see the CA Performance Center online Help.
4. Select Admin, Groups in the menu bar.

   The Manage Groups page displays current groups in a tree structure.
5. Expand the Defined Tenants group in the Groups tree.
6. Locate the tenant to which you want to grant access to selected CA Spectrum devices.
7. Expand the Inventory group under the tenant group.
8. Select the Service Provider Items group.



9. Click the Items tab in the right pane, and click Add Item Type.

   The Add Items dialog opens. You can begin adding the items to the Service Provider Items group.

10. Add all CA Spectrum models that you want the users who are associated with this tenant to be able to monitor.
11. Click Close when you have finished adding items.

Now the tenant users can see items that are being managed in the Default Tenant space in their inventory. Tenant users can also add these items to tenant groups to organize reporting.

Drill Down into CA Performance Center Performance Data

You can navigate to CA Performance Center performance data directly from models in OneClick. Drill down from any device or interface model that is also available in CA Performance Center.

Although CA Spectrum can contribute an interface model to CA Performance Center, an interface item only appears in CA Performance Center when a data source other than CA Spectrum is contributing performance data for it. If the interface is not being monitored by another data source, such as Data Aggregator or CA Network Flow Analysis, the right-click drill-down option is not available. For more information, see Smart Interface Filtering (see page 26).

Follow these steps:

1. In the OneClick Navigation panel, expand the CA Performance Center IP Domains that were synchronized from CA Infrastructure Management.
2. Select a model in one of these collections.
3. Right-click the model, and select the option to navigate to CA Performance Center.

   Note: This option is also available when you select the model on a Topology map or from Locater search results.

   The CA Performance Center user interface opens in a separate window. The device context associated with the selected model is preselected.

Known Anomalies

CA Spectrum - CA Performance Center integration has the following known anomalies:

- Event processing behavior is undefined when a device is modeled as a nonproxy model on more than one landscape.
- Some data sources do not support IPv6 addresses. Proper mapping does not occur when CA Spectrum uses an IPv6 primary address for a device but the reporting data source does not support IPv6 addresses. To correct the mapping, destroy the CA Spectrum model and rediscover it using an IPv4 address. After the next incremental synchronization, the model will be mapped properly.

- When a CA Performance Center event is received for a model that is in maintenance mode in CA Spectrum, the event is not processed, in accordance with expected maintenance mode behavior.
- CA Spectrum can fall out of synchronization when the Event Manager data source is removed. If this situation occurs, follow these steps:

  a. Remove the CA Spectrum data source.

  b. Register the Event Manager data source again.

  c. Register the CA Spectrum data source again.

  Important! This situation only applies to CA NetQoS Performance Center v6.1. It does not apply to CA Performance Center. Do not delete the data source from CA Performance Center unless CA Support advises you to do so.

More information:

Modifying Data Sources After Integration (see page 33)
Remove CA Spectrum as a Data Source in CA Performance Center (see page 34)

Chapter 4: Maintaining the Integration

This section contains the following topics:

Modifying Data Sources After Integration (see page 33)
Restoring the SpectroSERVER Database (see page 33)
Remove CA Spectrum as a Data Source in CA Performance Center (see page 34)
Enabling Debug Logging (see page 35)

Modifying Data Sources After Integration

Important! The correct procedure must be followed to enable data to synchronize correctly between CA Spectrum and CA Performance Center.

Use the following guidelines when restoring a data source in CA Performance Center after CA Spectrum-CA Performance Center integration has already been configured:

- If CA Spectrum exists as a data source in CA Performance Center when you restore another data source, restart tomcat.
- If CA Spectrum does not exist as a data source in CA Performance Center, add other data sources first and then add CA Spectrum as a data source.

Restoring the SpectroSERVER Database

To restore the SpectroSERVER database to a previous state after CA Spectrum - CA Performance Center integration, complete the following steps.

Important! The correct procedure must be followed to enable data to synchronize correctly between CA Spectrum and CA Performance Center.

Follow these steps:

1. Remove CA Spectrum as a data source in CA Performance Center (see page 34).
2. Restore the SpectroSERVER database.

   Note: For information about restoring the SpectroSERVER database, see the *Database Management Guide*.
3. Restart the OneClick server.
4. Add CA Spectrum as a data source in CA Performance Center (see page 16).

Remove CA Spectrum as a Data Source in CA Performance Center

When restoring the SpectroSERVER database to a previous state, unregister the CA Spectrum data source. This process helps to establish correct synchronization between CA Spectrum and CA Performance Center after the database has been restored.

Deleting selected data sources from CA Performance Center can have negative consequences. Only administrators with the Delete Data Sources role right can delete a data source from CA Performance Center. This role right is not granted by default and must be assigned to the role as a separate step.

Follow these steps:

1. Log in as a user with the Administrator role.
2. Navigate to the Manage Roles page.

   The page displays the current list of roles.
3. Select the Administrator role, and click Edit. The role right to Delete Data Sources is only available to this predefined role.

   The Edit Role Rights dialog opens.
4. Select Performance Center, and click Edit.

   The Edit Role Rights dialog lets you select individual access rights for this role.

   Assigned role rights are grayed out because they are read-only for this role.
5. Select Delete Data Sources. Click the right arrow to move it from the Available Rights list to the Selected Rights list.
6. Click OK. Then click Save to save your change to the role.

   Note: You must be logged in with a user account that has the Administrator role that you have just edited.
7. Click Admin, Data Source Settings, and select Data Sources.

   The Manage Data Sources page opens.
8. Select the CA Spectrum data source, and click Delete.

   The Delete Data Source page opens.
9. Click Delete, and then click Yes to confirm the deletion.

   The data source is successfully deleted, and synchronization between CA Spectrum and CA Performance Center no longer occurs.

   CA Performance Center IP Domain models in OneClick are automatically deleted.

Enabling Debug Logging

To facilitate the investigation of issues, enable CA Performance Center integration debug logging on the OneClick Web Server.

Follow these steps:

1. Click Administration, Debugging, Web Server Debug Page (Runtime) on the OneClick home page.
2. Select ON for the 'Performance Center Integration' option.
3. Select ON for the 'Performance Center Integration Sync' option.

Note: Enabling CA Performance Center integration debug logging can generate a large volume of data in a short amount of time.

Appendix A: Support Additional Event Types

This section contains the following topics:

How to Configure Events for Integration with CA Performance Center (see page 37)

How to Configure Events for Integration with CA Performance Center

With the integration of CA Spectrum r9.2.2 and later and CA Performance Center v2.0.00 and later, events for which CA Spectrum polls are specified in an XML file. Based on the contents of the default XML file, CA Spectrum polls for ThresholdViolation events automatically. If you do not modify the XML file, information is obtained from the Event Manager database for ThesholdViolation events only.

You can also configure CA Spectrum to poll for any event in the Event Manager database. To do so, modify the XML file and set up other event support files in CA Spectrum. In addition, for CA Spectrum to process a modified event, the device or port must be modeled in CA Spectrum and included in the synchronization process.

To configure CA Spectrum to poll for specific events, take the steps that are listed below. A complete example (see page 42) is provided.

Note: To poll for ThresholdViolation events only, no action is required.

1. Obtain a developer ID to create event codes (see page 38).
2. Update the netqos-integration-application-config.xml file to specify additional events and alarms (see page 38).
3. Update the event disposition file to map the events to CA Spectrum event files (see page 40).
4. Create an event format file for each event. (see page 41)
5. Create a probable cause file for each alarm code. (see page 41)
6. Deploy the changes by restarting the SpectroSERVER and OneClick servers. (see page 42)

Obtain a Developer ID

When defining events for the CA Spectrum - CA Performance Center integration, you use identifying event codes. The first 2 bytes of any event code contain a developer ID. You can obtain a registered developer ID from CA so that you can specify unique codes for your events. Using a unique developer ID lets you easily recognize your new codes in OneClick and prevents potential conflicts with other CA Spectrum event codes.

To obtain a developer ID from CA, contact CA Technical Support.

Update the netqos-integration-application-config.xml File

CA Spectrum uses the netqos-integration-application-config.xml file to determine the events for which to poll. CA Spectrum polls for ThresholdViolation events by default. To poll for more events, modify the netqos-integration-application-config.xml to define the event codes (see page 38) and associated alarms (see page 39) for each event.

The netqos-integration-application-config.xml file is located in the following directory:

$SPECROOT\tomcat\webapps\spectrum\WEB-INF\netqos\config\container

Define Events

The eventTypeManager bean defines the events for which CA Spectrum polls. The entries for ThresholdViolation events appear in the file by default. You can manually add more events.

```
<bean id="eventTypeManager"
   class="com.ca.im.netqos.integration.event.type.EventTypeManager">
   <property name="interestingEventTypes">
     <map>
       <entry key="ThresholdViolation" value-ref="thresholdViolationAlarmCodes" />
       <entry key="TestEvent" value-ref="TestEventAlarmCodes" />
     </map>
   </property>
   <property name="alarmClearCodes">
     <map>
       <entry key="ThresholdViolation" value="0x5c40009" />
       <entry key="TestEvent" value="TestEventAlarmClearCode" />
     </map>
   </property>
</bean>
```

Update the following property elements to add events that CA Spectrum can include in polling:

interestingEventTypes

Specifies the types of events to include in polling. Each entry element identifies a specific event type and an alarm code map value. The ThresholdViolation entry is included by default. Add an entry element, as follows:

```
<entry key="TestEvent" value-ref="TestEventAlarmCodes" />
```

TestEvent

Specifies the name of an event in the Event Manager database.

TestEventAlarmCodes

Specifies the value of the map that identifies the alarms for this event.

Note: The alarm code map is described in the next section.

alarmClearCodes

Specifies the alarm clear codes for polled events. The default alarm clear code for the ThresholdViolation event is 0x5c40009. For each event, add an entry element, as follows:

```
<entry key="TestEvent" value="TestEventAlarmClearCode" />
```

TestEvent

Specifies the name of the event that was added for polling.

TestEventAlarmClearCode

Specifies the alarm clear code for the event.

Define Alarms

An alarm map defines the alarm code values that are associated with a particular event. For each polled event (or, each interestingEventTypes entry), a corresponding alarm map must be defined. The alarm map for the ThresholdViolation event appears in the file by default, and an alarm map for each custom event must be added manually.

```
<bean id="thresholdViolationAlarmCodes"
    class="org.springframework.beans.factory.config.MapFactoryBean">
    <property name="sourceMap">
      <map>
        <entry key="1" value="0x5c40010" />
        <entry key="2" value="0x5c40011" />
        <entry key="3" value="0x5c40012" />
      </map>
    </property>
</bean>
```

```
<bean id="testEventAlarmCodes"
    class="org.springframework.beans.factory.config.MapFactoryBean">
    <property name="sourceMap">
      <map>
        <entry key="alarmSev1" value="alarmCode1" />
        <entry key="alarmSev2" value="alarmCode2" />
        <entry key="alarmSev3" value="alarmCode3" />
      </map>
    </property>
</bean>
```

To add alarm maps for custom events, add a bean element for each event and update the following values:

testEventAlarmCodes

Specifies the alarm code map value for a particular event. This value is established on the interestingEventTypes entry and must match that value.

alarmSev1 - alarmCode1, alarmSev2 - alarmCode2, alarmSev3 - alarmCode3

Specifies the *alarmSeverity* - *alarmCode* pairs for a particular event. For example, for the default ThresholdViolation event, the Minor (1), Major (2), and Critical (3) alarm codes are 0x5c40010, 0x5c40011, and 0x5c40012, respectively.

Update the Event Disposition File

The Event Disposition (EventDisp) file is used to determine how to process the events configured in the netqos-integration-application-config.xml file. Each event entry maps an event to a CA Spectrum event file.

The EventDisp file for CA Spectrum-CA Performance Center integration is located in:

<$SPECROOT>\SS\CsVendor\netqos

For the default ThresholdViolation event, the following entries map the alarm codes to individual CA Spectrum event files:

```
#PC Threshold
0x5c40010 E 50 A 1,0x5c40010,107
0x5c40011 E 50 A 2,0x5c40011,107
0x5c40012 E 50 A 3,0x5c40012,107
0x5c40009 E 50 C 0x5c40010,107 C 0x5c40011,107 C 0x5c40012,107
```

For each custom event, add new event map entries to the file. The following example shows syntax that generates or clears alarms that are based on the event code.

```
#New Event
alarmCode1E 50 A 1, alarmCode1_filename,107
alarmCode2E 50 A 2, alarmCode2_filename,107
alarmCode3E 50 A 3, alarmCode3_filename,107
alarmClearCode4E 50 C alarmCode1,107 C alarmCode2,107 C alarmCode3,107
```

Note: For more information about using Event Disposition files, including syntax and examples, see the *Event Configuration User Guide*.

Create Event Format Files

An event format file contains the message about the event that is displayed to users on the Events tab in OneClick. Each new event that is defined in the netqos-integration-application-config.xml file requires an event format file. The file enables the event to display correctly in the OneClick Events view.

The file name must match the alarm code (for example, alarm code 0x5c40010 uses the file "Event05c40010"). And the file must exist in the following directory:

<$SPECROOT>\SG-Support\CsEvFormat

The following is an example of the file format:

```
{d "%w- %d %m-, %Y - %T"} - {S 109} is reporting a minor threshold violation.
Detail of Threshold Violation:
        1) Incident Start Time: {D 111}
        2) Event ID: {S 107}
        3) Event Source: {S 113}
        4) Alert Message: {S 76620}
A corresponding minor Threshold Violation Alarm will be generated.
(event [{e}])
```

Note: For more information, see the *Event Configuration User Guide*.

Create Probable Cause Files

A probable cause file defines the symptoms, probable causes, and recommended corrective actions for an alarm. Each new alarm code requires a probable cause file so that the alarm displays correctly in the OneClick Alarms view.

The file name must match the alarm code (for example, alarm code 0x5c40010 uses the file "Prob05c40010"). And the file must exist in the following directory:

<$SPECROOT>\SG-Support\CsPCause

The following is an example of the file format:

```
A minor threshold violation has occurred.
SYMPTOMS:
The monitored threshold has been exceeded.
PROBABLE CAUSES:
RECOMMENDED ACTIONS:
Launch the "Performance View" to see incident details.
```

Note: For more information, including syntax, see the *Event Configuration User Guide*.

Deploy the Changes

After all configuration changes have been made, restart the SpectroSERVER and OneClick servers.

Event polling now reflects any changes that you have made.

Example

This example shows how to configure CA Spectrum to poll for a specific event in the Event Manager database. The event in this example identifies when a router device experiences high memory usage.

1. Identify a device or port for which you want CA Spectrum to poll for in the Event Manager database. If the device or port is not modeled in CA Spectrum, model the element. For example, to monitor specific events for a particular router, the router must be modeled in the CA Spectrum database.
2. Obtain a developer ID from CA Technical Support for use with CA Spectrum-CA Performance Center integration. This example uses the default developer ID value, 0xffff.
3. Identify the events for which CA Spectrum polls. For example, you can identify any occurrence when the router device experiences high memory utilization. This example refers to this event as "RouterHighMemory".

4. Define the event by modifying the XML file:

   a. Open the following file for editing:

      <$SPECROOT>\tomcat\webapps\spectrum\WEB-INF\netqos\config\container\netqos-integration-application-config.xml

   b. Define the custom event. Update the existing eventTypeManager element as follows: add the RouterHighMemory event to the list of events for which to poll, establish an alarm map value, and specify a default alarm clear code.

      The following code shows these changes. Notice that the alarm clear code uses a developer ID.

```
<bean id="eventTypeManager"
   class="com.ca.im.netqos.integration.event.type.EventTypeManager">
   <property name="interestingEventTypes">
     <map>
       <entry key="ThresholdViolation"
value-ref="thresholdViolationAlarmCodes" />
       <entry key="RouterHighMemory"
value-ref="RouterHighMemoryAlarmCodes" />
     </map>
   </property>
   <property name="alarmClearCodes">
     <map>
       <entry key="ThresholdViolation" value="0x5c40009" />
       <entry key="RouterHighMemory" value="0xffff0004" />
     </map>
   </property>
</bean>
```

   c. Define the alarm map by adding the following new bean element:

```
<bean id="RouterHighMemoryAlarmCodes"
    class="org.springframework.beans.factory.config.MapFactoryBean">
    <property name="sourceMap">
      <map>
        <entry key="1" value="0xffff0001" />
        <entry key="2" value="0xffff0002" />
        <entry key="3" value="0xffff0003" />
      </map>
    </property>
</bean>
```

   d. Save and close the file.

5. Specify how CA Spectrum processes the encountered event by updating the Event Disposition file:

   a. Open the following file for editing:

      <$SPECROOT>\SS\CsVendor\netqos\EventDisp

   b. Add the following map entries for the RouterHighMemory event:

      ```
      #RouterHighMemory Event
      0xffff0001E 50 A 1, 0xffff0001,107
      0xffff0002E 50 A 2, 0xffff0002,107
      0xffff0003E 50 A 3, 0xffff0003,107
      0xffff0004E 50 C 0xffff0001,107 C 0xffff0002,107 C 0xffff0003,107
      ```

   c. Save and close the file.

6. Create an event format file for each of the alarm codes using the following naming convention (*AlarmCode* - *EventFormatFile*):

   - 0xffff0001 - Eventffff0001
   - 0xffff0002 - Eventffff0002
   - 0xffff0003 - Eventffff0003
   - 0xffff0004 - Eventffff0004

   a. Create a text file containing content similar to the following text:

      ```
      {d "%w- %d %m-, %Y - %T"} - {S 109} is reporting a minor threshold violation.
      Detail of Threshold Violation:
              1) Incident Start Time: {D 111}
              2) Event ID: {S 107}
              3) Event Source: {S 113}
              4) Alert Message: {S 76620}
      A corresponding minor Threshold Violation Alarm will be generated.
      (event [{e}])
      ```

      Note: When creating Eventffff0004, use appropriate wording for clearing an alarm.

   b. Save the file to the following location:

      <$SPECROOT>\SG-Support\CsEvFormat

   c. Repeat steps a and b for each alarm code.

7. Create a probable cause file for each of the alarm codes using the following naming convention (*AlarmCode* - *ProbableCauseFile*):
   - 0xffff0001 - Probffff0001
   - 0xffff0002 - Probffff0002
   - 0xffff0003 - Probffff0003
   - 0xffff0004 - Probffff0004

   a. Create a text file containing content similar to the following text:

   ```
   A minor threshold violation has occurred.
   SYMPTOMS:
   The monitored threshold has been exceeded.
   PROBABLE CAUSES:
   RECOMMENDED ACTIONS:
   Launch the "Performance View" to see incident details.
   ```

   b. Save the file to the following location:

   <*$SPECROOT*>\SG-Support\CsPCause

   c. Repeat steps a and b for each alarm code.

8. Restart the SpectroSERVER and OneClick servers.

   When the integration is complete, CA Spectrum uses the updated files to poll for the RouterHighMemory event, generating events and alarms as specified.

Index

A

alarm clearing • 7
alarm set • 7
anomalies • 31

C

CA Network Flow Analysis • 10, 12
configuring • 15
contacting technical support • 3
custom events • 37
customer support, contacting • 3

D

Data Aggregator • 10, 12, 26
data sources • 16, 31, 33
  adding • 16
  removing • 34
debug logging • 35
developer ID • 38
device model synchronization • 13
distributed SpectroSERVER • 8

E

event disposition file • 40
event format file • 41
Event Manager • 8
  version • 12
event polling • 7, 8, 18

F

full synchronization • 8

G

Global Collections • 7, 10, 15, 19
groups • 7, 10, 29

I

incremental synchronization • 8
interfaces • 10, 19, 31
  no data for • 26
IP domains • 10, 19, 27
IPv6 addresses • 31

M

maintenance mode • 31
model eligibility • 13
Model_class • 13
multi-tenancy • 10
  enabling • 22, 29
  support for • 22, 27, 29

N

netqos-integration-application-config.xml • 38
NetVoyant • 12
non-proxy model • 31

P

Performance Center group • 8
Performance Center Integration Configuration Page • 18
Performance Center version • 12
pingable devices • 20, 28
probable cause file • 41

R

ReporterAnalyzer • 12
router • 13

S

Service Provider Groups • 19, 27, 29
SNMP profiles • 19, 20, 28
SpectroSERVER database • 33
SuperAgent • 12
support, contacting • 3
switch • 13
switch-router • 13
synchronization • 8
synchronized discovery • 10, 19, 26

T

technical support, contacting • 3

V

version compatibility • 10, 12

W

workstation-server • 13

X

XML file • 38