CA Spectrum® and CA Nimsoft

CA Spectrum - CA Nimsoft Integration Guide

CA Spectrum Release 9.3 / CA Nimsoft

CA Technologies Product References

This document references the following CA Technologies products:

- CA Spectrum®
- CA Spectrum® Southbound Gateway Toolkit (Southbound Gateway)
- CA Nimsoft

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

About CA Nimsoft Infrastructure Manager 8
CA Nimsoft and CA Spectrum Integration 8
    Coexistence and Compatibility with Previous Integrations 9
Integration Architecture 9
Alarms, Events and Views 11

Chapter 2: Integrating CA Nimsoft and CA Spectrum through the Southbound Gateway 13

Review the Prerequisites and Considerations 14
Install and Configure CA Spectrum 16
Deploy and Configure Probes 17
Configure CA Nimsoft Infrastructure Manager 20
Create an EventAdmin Model for the Nimsoft Server 24
Verify the Received Events and Alarms in OneClick 25

Chapter 3: Disable the Integration 27

Performance Considerations 27

Index 29

Chapter 1: Introduction

CA Nimsoft is a system management tool with a SaaS deployment architecture while CA Spectrum is a tool for Network Discovery and Fault Management. CA Nimsoft integrated with CA Spectrum provides a more comprehensive infrastructure management solution.

CA Nimsoft products are used to monitor and manage business services within the IT infrastructure including network components, servers, databases, applications, and virtualized environments. CA Nimsoft provides an array of capabilities that improve the speed of deployment, unify management, and maximize performance and uptime. The key features of CA Nimsoft include:

- Automated Device Discovery
- Multi-Vendor Device Support
- Multi-tenancy
- SaaS Deployment options
- Centralized Message Center
- Performance and Availability Monitoring
- Intelligent Alerting
- Customizable Performance and Availability Reports
- Integrated Wireless
- Active Directory Integration
- Storage Monitoring and Reporting

This section contains the following topics:

About CA Nimsoft Infrastructure Manager (see page 8)
CA Nimsoft and CA Spectrum Integration (see page 8)
Integration Architecture (see page 9)
Alarms, Events and Views (see page 11)

About CA Nimsoft Infrastructure Manager

CA Nimsoft Infrastructure Manager is a component of CA Nimsoft Monitor. CA Nimsoft Infrastructure Manager provides monitoring and management solutions for systems, applications, and networks. CA Nimsoft Infrastructure Manager is the primary interface for configuration and management of the CA Nimsoft system and provides the following features:

- A Windows Explorer-style overview of systems being monitored.
- An alarm window to view all alarms and messages.

The Infrastructure Manager can connect to multiple hubs (such as active or backup hubs). The Infrastructure Manager lets you control, configure, and manage all Robots and Probes that are connected to an active hub. Probes, Robots, and Hubs are the components of Infrastructure Manager. For more information, see the *CA Nimsoft Infrastructure Manager Reference Guide.*

CA Nimsoft and CA Spectrum Integration

CA Nimsoft and CA Spectrum are integrated through the CA Spectrum Southbound Gateway component (SBGW). This integration is unidirectional (CA Nimsoft to CA Spectrum), and supports multiple outstanding alarms, of various types, per device.

The CA Spectrum - CA Nimsoft Integration expands the CA Spectrum model of the infrastructure with information and alarms from CA Nimsoft and provides the following benefits:

- Receive events and alerts in CA Spectrum from CA Nimsoft probes.
- Obtain extended CA Spectrum monitoring capabilities leveraging the intelligence of CA Nimsoft probes
- Use the Nimsoft SLA rules to trigger events that create alert conditions in CA Spectrum.
- Use CA Spectrum root cause analysis capabilities to perform basic root cause analysis on events and alerts that are created by CA Nimsoft.

Coexistence and Compatibility with Previous Integrations

Multiple integrations between CA Nimsoft and CA Spectrum have been developed in the past. You can install the current integration without uninstalling the previous integration because the present design uses distinct traps and developer IDs (event prefixes).

The current and previous integrations can therefore coexist. However, the two integrations do not share information with each other. The integrations remain as two separate integrations. We recommend activating only one integration with CA Nimsoft at a time.

Integration Architecture

When an issue occurs in the infrastructure, alert data is sent from CA Nimsoft to the SpectroSERVER of CA Spectrum through the Southbound Gateway component. SpectroSERVER is a primary server for CA Spectrum. For more information, see the *CA Spectrum Concepts Guide*.

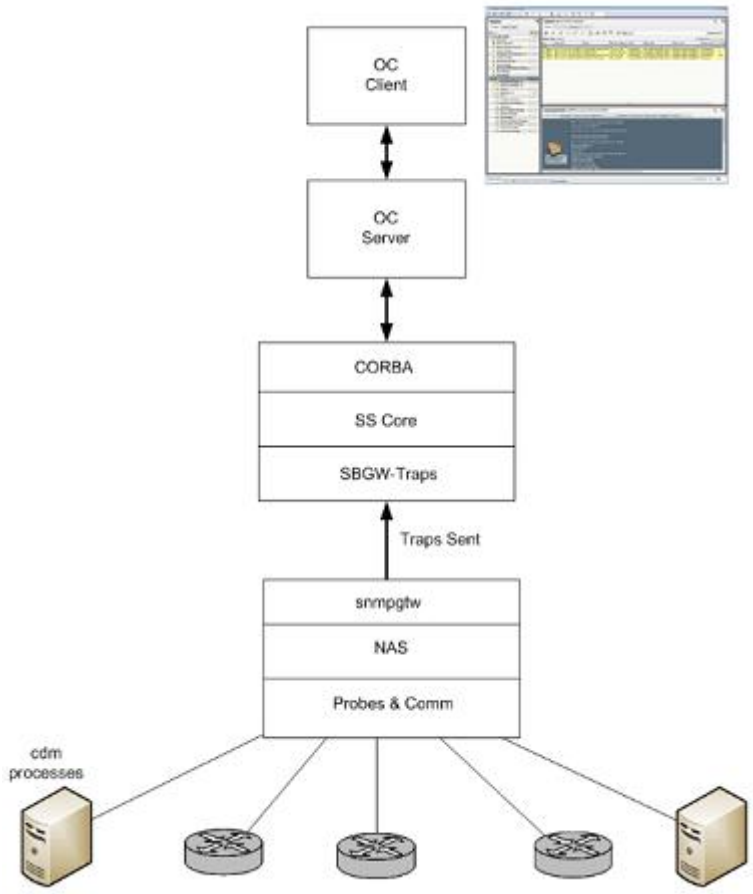
Using the Southbound Gateway, you can centralize network management, allowing CA Spectrum to capture and display data. Alert data is organized into CA Spectrum event and alarm data as appropriate and is displayed within OneClick.

The Southbound Gateway can be used with any incoming alert data stream format. The Southbound Gateway provides a simple, non-programmatic integration point for systems that can generate SNMP traps. It is also useful for managing non-SNMP environments. Southbound Gateway supplies an import tool that accepts XML-formatted alert data in case the system with which you are integrating cannot generate SNMP traps. For more information, see the *Southbound Gateway Guide*.

Once the Southbound Gateway receives the alert data, the data is mapped to a CA Spectrum event in an AlertMap file. The Southbound Gateway determines the appropriate EventAdmin model to receive the alert data based on the IP address of the host computer that is sending the data. The IP address of the host computer should match the IP address that is used to create the EventAdmin model.

The CA Spectrum EventAdmin model receives the trap and translates it into a CA Spectrum event. If the event corresponds to a critical, major, or minor condition, the corresponding alarm is raised on a CA Spectrum model. The model where the alarm is raised depends on a few factors. We recommend having a previously modeled device in CA Spectrum. If the device model is present in CA Spectrum, the alarm is asserted against the existing device model. If the device model does not exist in CA Spectrum the alarm is asserted against an auto-created EventModel of the Nimsoft Robot that is reporting the condition.

The following diagram illustrates the CA Nimsoft - CA Spectrum Integration Architecture:



Nimsoft Probes

Provide the intelligence to manage specific components on a managed device. For example, the cdm processes probe is responsible for monitoring CPU, disk, and memory usage on target hosts. Over 135 CA Nimsoft probes are available, to let you manage the entire IT infrastructure, including servers, network devices, applications, and databases.

Nimsoft Alarm Server (NAS)

Receives and manages incoming alarm messages. The Nimsoft Alarm Server supports message suppression and provides clients with services such as event updates, message filtering, automated actions, and mirroring capabilities.

Nimsoft SNMP Gateway Probe (snmpgtw)

Sends out the traps from Nimsoft to CA Spectrum. This probe converts alarms to SNMP-Trap messages which are readable by any SNMP-based management system. It subscribes to CA Nimsoft internal alarms and processes these alarms into SNMP traps with all the information about the alarm that is encoded in the trap varbinds.

Alarms, Events and Views

CA Spectrum receives alerts (usually SNMP traps) from problem areas in the computing infrastructure. These alerts are converted into events and alarms that are displayed in OneClick. CA Spectrum uses a series of event configuration files to determine how events and alarms are processed.

Alarms

An *alarm* is an object that indicates a user-actionable, abnormal condition that exists in the managed environment. Usually an alarm is generated when an event has occurred, and the EventDisp file specifies that an alarm is generated. When the abnormal condition that caused the alarm in CA Nimsoft clears, the corresponding alarm in CA Spectrum is cleared automatically by another event.

Events

An *event* is an object representing an instantaneous occurrence within CA Spectrum. Events usually indicate that something significant has occurred in relation to the model or other component. Most device model types have an associated EventDisp event configuration file. After an AlertMap file converts an SNMP trap into an event, the EventDisp file instructs CA Spectrum on how to handle the event for a specific model. Event processing includes logging the event and generating an alarm.

Views

A *view* in CA Spectrum is a way to organize data that can be viewed or manipulated. Management and Hierarchical views are two main types of views in CA Spectrum. Management views focus on various ways to represent data concerning a specific managed element. Hierarchical views represent ways to structure your network data. For more information, see the *CA Spectrum Concepts Guide*.

Chapter 2: Integrating CA Nimsoft and CA Spectrum through the Southbound Gateway

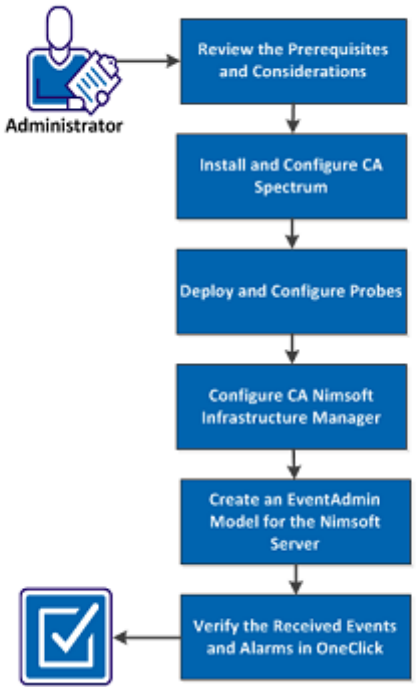
The CA Spectrum and CA Nimsoft integration is performed through the CA Spectrum Southbound Gateway component. The component asserts the alarm against the existing device model or against an auto-created event model of CA Nimsoft Robot. CA Spectrum EventModel is used when a full device model for the network entity does not exist in CA Spectrum. This integration supports multiple alarms types per model, such as Low Disk, Excessive CPU usage, and Traffic Threshold violation.

Note: The CA Spectrum and CA Nimsoft integration currently supports only a single instance of a given alarm.

As an administrator, configure CA Nimsoft to send alert data to CA Spectrum. CA Nimsoft sends the trap data to the host name and port where the SpectroSERVER is running. By default, CA Spectrum uses standard SNMP trap port 162. You can modify the port by changing the snmp_trap_port parameter in the CA Spectrum .vnmrc file that is located in the CA Spectrum directory.

The following diagram illustrates the process to integrate CA Nimsoft and CA Spectrum through the Southbound Gateway:

Integrating CA Nimsoft and CA Spectrum through the Southbound Gateway



Perform the following tasks to integrate CA Nimsoft and CA Spectrum through the Southbound Gateway:

1. Review the Prerequisites and Considerations (see page 14)
2. Install and Configure CA Spectrum (see page 16)
3. Deploy and Configure Probes (see page 17)
4. Configure CA Nimsoft Infrastructure Manager (see page 20)
5. Create an EventAdmin Model for the Nimsoft Server (see page 24)
6. Verify the Received Events and Alarms in OneClick (see page 25)

This section contains the following topics:

Review the Prerequisites and Considerations (see page 14)
Install and Configure CA Spectrum (see page 16)
Deploy and Configure Probes (see page 17)
Configure CA Nimsoft Infrastructure Manager (see page 20)
Create an EventAdmin Model for the Nimsoft Server (see page 24)
Verify the Received Events and Alarms in OneClick (see page 25)

Review the Prerequisites and Considerations

Verify the following prerequisites before installing and configuring the CA Spectrum - CA Nimsoft Integration:

- Licensed installations of CA Spectrum 9.3 and CA Nimsoft Management System (version 6.2 or later) are required.

  Note: If you plan to install CA Spectrum as a user other than Administrator, disable User Account Control (UAC) on Windows. For more information, see the *CA Spectrum Installation Guide*.

- Verify that the system where you want to install CA Spectrum has a static IP address.
- Standard CA Spectrum supported platforms and hardware are required.

Verify the following considerations:

- The current integration does not attempt to upgrade previous (that is field-developed) integrations. We plan to support upgrades to future versions of this integration.
- This integration requires CA Spectrum to use the SNMP Trap port (162) for communication from CA Nimsoft. For more information, see http://docs.nimsoft.com/prodhelp/en_US/Library/index.htm?toc.htm?ServerDocsIndex.html
- This integration connects to only a single CA Nimsoft instance.
- This integration depends on trap reception because typical SNMPv1 traps are unconfirmed. Traps can be dropped in transit and not recognized.

Install and Configure CA Spectrum

CA Spectrum installation software requires administrator privileges to evaluate available resources and run custom installation scripts. An initial installation generates residual files with administrator ownership. Subsequent upgrade installations also require administrator privileges.

Important! The C:\Program Files\CA directory on Windows platforms and the /opt/CA directory on Linux and Solaris platforms are automatically created during the CA Spectrum first-time installation. CA Spectrum components that are also common to other CA products are intentionally installed into this directory. This directory is automatically updated as needed during a CA Spectrum upgrade. Do not remove files from this directory.

A CA Spectrum installation is required to integrate CA Nimsoft and CA Spectrum through the Southbound Gateway. You can install CA Spectrum on Windows, Linux, or Solaris platforms.

Follow these steps:

1. Stop all non-CA Spectrum running applications.
2. Perform the following actions:
   - Log off from OneClick in the Client Details web page and shut down the OneClick client.

     Note: For more information, see the *CA Spectrum Administrator Guide.*
   - Click Stop SpectroSERVER to stop the SpectroSERVER and the Archive Manager in the CA Spectrum Control Panel and then close the CA Spectrum Control Panel.

     Note: For more information, see the *CA Spectrum Administrator Guide.*
   - Stop all VnmSh connections.

     Note: For more information, see the *Command Line Interface User Guide.*
   - Close all Bash shells.

   Important! Disable your antivirus software real-time protection before installing CA Spectrum. Disabling helps avoid potential problems with files that can be in use by the real-time protection software.
3. Log in as a user with administrator rights.
4. Insert the installation medium into the appropriate drive. If auto-run is disabled, you can double-click the setupnt.exe file from the Explorer view to start the installation.

   The installation starts.
5. Install CA Spectrum. For more information, see the *CA Spectrum Installation Guide*.

Deploy and Configure Probes

CA Nimsoft Probes are small, dedicated applications that monitor specific resources or events. Each probe can be easily configured for your specific monitoring requirements.

The SNMP Gateway probe sends traps from CA Nimsoft to CA Spectrum. To integrate CA Nimsoft with CA Spectrum, configure the SNMP Gateway probe (snmpgtw) through CA Nimsoft Infrastructure Manager.

The SNMP gateway converts alarms to SNMP trap messages that are readable by any SNMP-based event manager. The SNMP gateway maps the various severity levels to enterprise-specific trap types. For more information, see http://docs.nimsoft.com/prodhelp/en_US/Probes/GettingStarted/.

Follow these steps:

1. Open CA Nimsoft Infrastructure Manager.
2. From the Console window, select Archive, Nimsoft Server hub, and Robot.

   A list of predefined probes is displayed.
3. Select a package name in the archive folder.
4. Drag and drop the package name to the domain/hub/robot.

   A View Distribution Progress dialog opens.
5. Click Close Dialog after distribution has completed.

   The probe is deployed to the specified location.

6. To configure the probe, double-click the probe that you deployed.

   The Probe Configuration window opens.

7. Click the Setup tab.

   The Setup window opens with the following options:

   Active

   Activates or deactivates this probe.

   Subject(s)

   Specifies the Nimsoft subject that is transformed. Subject is a text string, that classifies the Nimsoft message for all components of CA Nimsoft.

   Default: Alarm

   Trap variables

   Indicates a unique identifier of the SNMP operation where the traps are triggered.

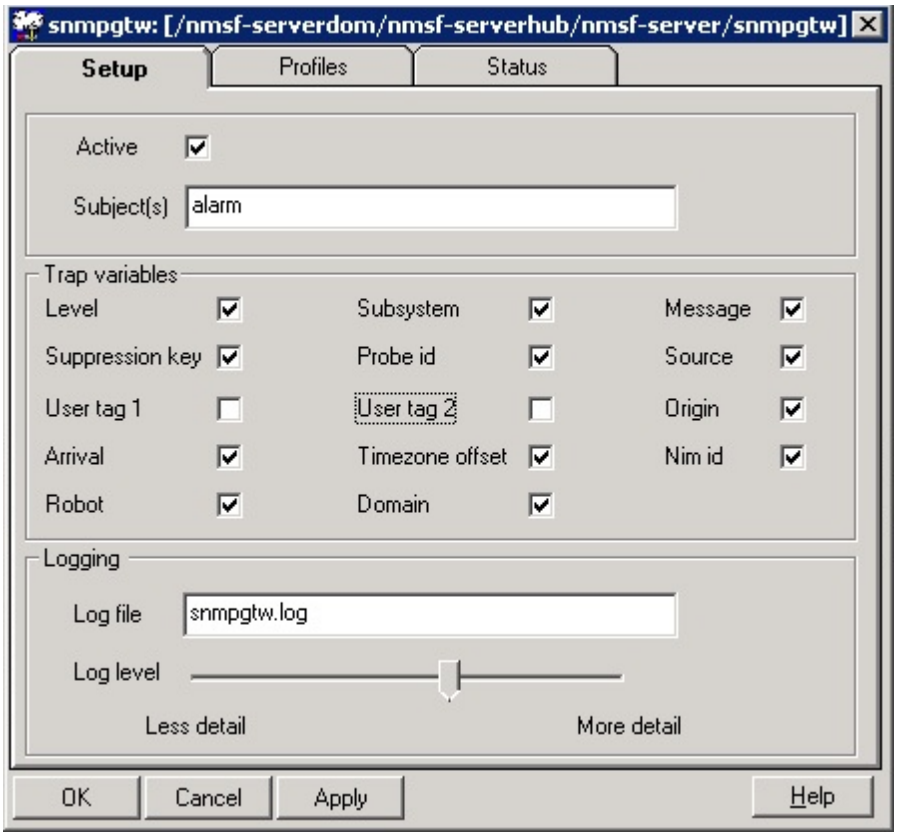
   Log file

   Specifies the file where the probe logs information about its internal activity.

   Log level

   Sets the level of details for the data that is written to the log-file. We recommend logging as little data as possible during normal operation to minimize disk consumption. You can then increase the amount of detail when debugging.

The following image illustrates the options that are available in the Setup window:



8. Click the Profiles tab.

   The Profile window opens. For more information, see Configure CA Nimsoft Infrastructure Manager (see page 20).

9. Click Ok.

   The snmpgtw probe is deployed and configured.

Configure CA Nimsoft Infrastructure Manager

The CA Nimsoft Infrastructure Manager is the primary interface for configuration and management of the CA Nimsoft system.

Configure CA Nimsoft Monitor to manage entities on your network through CA Nimsoft Infrastructure Manager or the Unified Management Portal. To integrate CA Nimsoft with CA Spectrum, configure the SNMP Gateway probe (snmpgtw) through CA Nimsoft Infrastructure Manager. For more information, see Deploy and Configure Probes (see page 17).

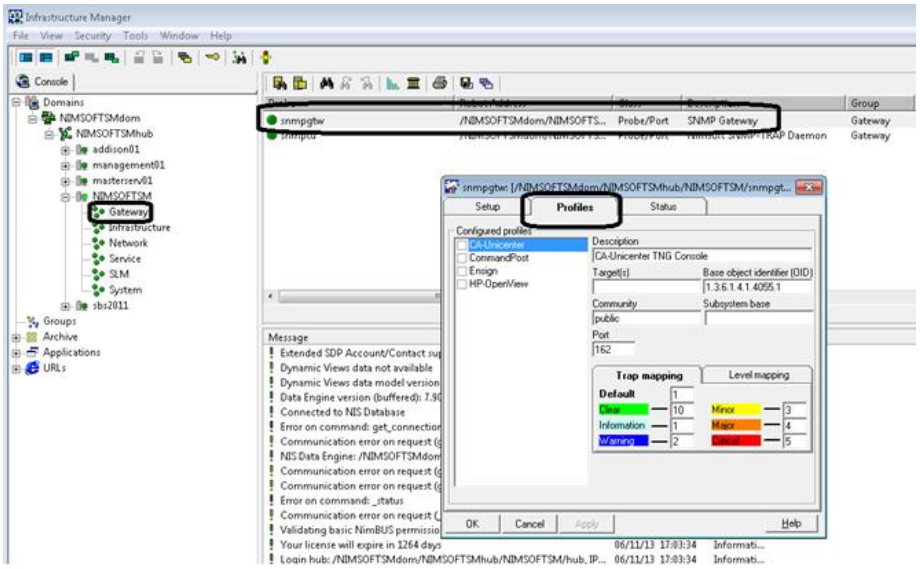
A profile is created in the SNMP Gateway Probe to communicate to the CA Nimsoft Monitor about the traps to send, the conditions under which to send them, and where to send them.

Follow these steps:

1. Open CA Nimsoft Infrastructure Manager.
2. From the Console window, select Domains, Nimsoft Server Domain, Nimsoft Server Hub, Nimsoft Primary Hub and then Gateway.

   A list of Probes is displayed.

   The following image displays the navigation to snmpgtw probe:



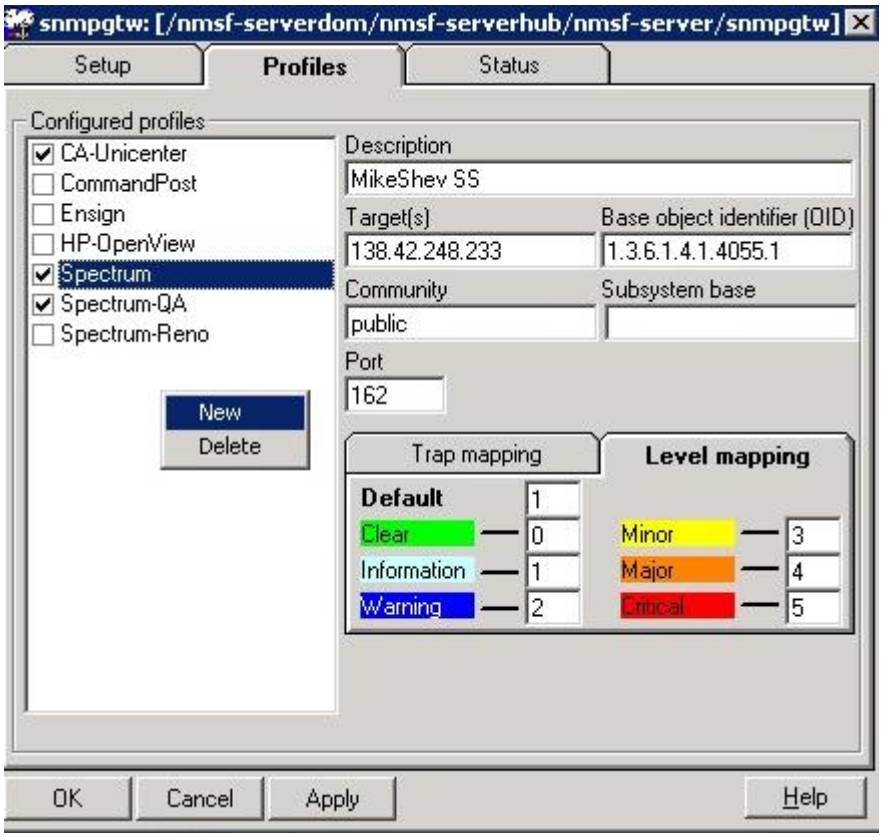
3. Double-click the snmpgtw probe.

   The Probe Configuration window opens.

4. Click the Profiles tab.

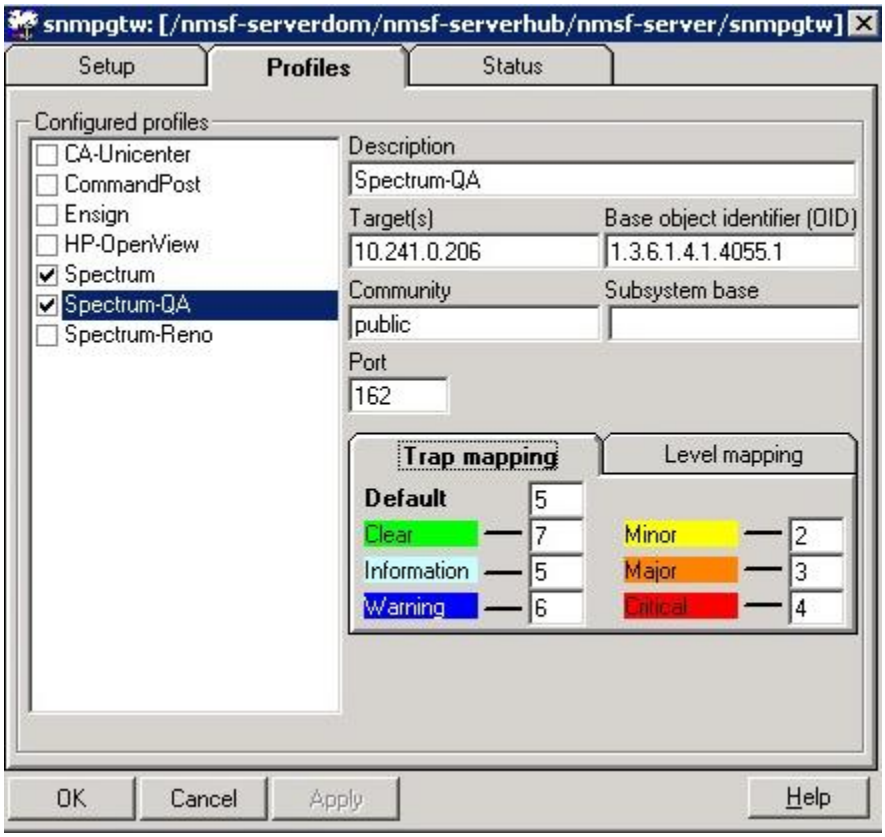
5. Right-click the Configured Profiles workspace and select New.

   The following image the illustrates the procedure to create a new profile:



6. Enter the name of the profile. For example, you can supply Spectrum-*Server name*.
7. To enable the profile, click Spectrum in the list of Configured profiles.

   The following image illustrates the options that are available in the Profiles window.



Target(s)

Specifies the SpectroSERVER IP address. Indicates the network node where the SNMP traps can be sent.

Base Object Identifier (OID)

Indicates the SNMP Object identifier to be used in the trap packages generated.

Default: 1.3.6.1.4.1.4055.1

Community String

Indicates the SNMP community string that is used in the SNMP traps.

Trap Mapping

Classifies the incoming traps by trap type and takes different actions for different trap types. You can map the severity levels of the alerts to SNMP traps.

For example, provide the following values for trap mapping:

Default: 5

- Clear: 7
- Informational: 5
- Warning: 6
- Minor: 2
- Major: 3
- Critical: 4

Note: If you want to disable informational and warning messages at the source level, remove the mappings for Default, Warning, and Informational in Trap Mapping. For more information, see Performance Considerations (see page 27).

Level Mapping

Identifies the severity levels with different codes. You can map the Nimsoft severity levels to the corresponding level in the receiving system by specifying the correct code.

For example, provide the following values for level mapping:

Default: 1

- Clear: 0
- Informational: 1
- Warning: 2
- Minor: 3
- Major: 4
- Critical: 5

8. Click Apply and Ok.

CA Nimsoft Infrastructure Manager is configured to integrate CA Nimsoft with CA Spectrum.

Create an EventAdmin Model for the Nimsoft Server

The CA Spectrum EventAdmin model receives events from the Southbound Gateway and transfers the event data to EventModels or device models depending on how the integration is configured. Alarms can be created from this event data.

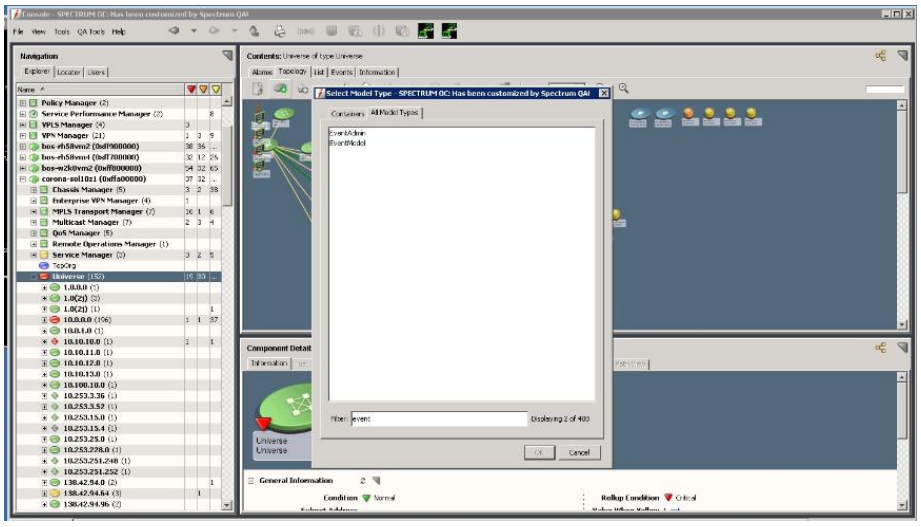
The EventModel is a model type that represents a unique source of event data on the system that is managed by the EventAdmin application. A given EventAdmin model can contain one or many instantiated EventModels. Each event that is received through the Southbound Gateway contains information that uniquely identifies the source of that event. The EventAdmin model receives the event, finds the unique event source, and passes the event to the target destination. Create an EventAdmin model for the Nimsoft server to support the integration.

Follow these steps:

1. Open the CA Spectrum OneClick Console.
2. From the Navigation Panel, select SpectroSERVER, and then Universe.
3. Click the Topology tab in the Contents Panel and click Create New Model by Type.

   The Select Model Type dialog opens.

   The following image displays the model types to be created:



4. In the All Model types tab, click EventAdmin.
5. Click OK.

   The Create Model of Type EventAdmin dialog opens.

6. Configure the following parameters:

   Name

   (Optional) Defines the EventAdmin model name. This model name appears in the field at the top of the EventAdmin icon.

   Network Address

   Specifies the network address of the event source host computer. Required for all integrations that are based on the SNMP traps.

   Security String

   (Optional) Defines who can view and edit this model.

   Manager Name

   When this attribute is set on the EventAdmin model, all EventModels contained within this EventAdmin also have this attribute.

   EventModel Prefix

   Verifies the naming prefix for all EventModels that are associated with a particular EventAdmin model. This field is related to the EventModel Name for all the EventModels contained by this EventAdmin. It is also useful for sorting and filtering.

   Default: 0x06330000

7. Click OK.

   The EventAdmin model is generated. A default EventModel is also created and is contained in the EventAdmin model. This model is used for fault tolerance functionality that represents the unique source.

Verify the Received Events and Alarms in OneClick

The EventAdmin Model receives an event from CA Nimsoft and sends it to the EventModel in OneClick. The event generates an alarm on this model. To verify that the integration is configured correctly, we recommend viewing the details of the alarm data from the Alarm Details tab in OneClick. The generic and subsystem-specific events are created in OneClick. You can also verify the design pattern of these events/alarms.

Follow these steps:

1. Open the OneClick Console.
2. Select the EventModel in the Navigation panel.

3. To view events, click the Events tab in the Contents panel.

   Events are displayed with the following event types:

   Generic Events

   Indicates the events that are not related to CPU, Disk, and Memory subsystems.

   The range starts from 0x06330000 - 0x6330005.

   Subsystem Specific Events

   Indicates the events that are related to CPU, Disk, and Memory subsystems. You can verify the following event range for the subsytem-specific events:

   - CPU

     0x06330050 - 0x6330055

   - Disk

     0x06330030 - 0x6330035

   - Memory

     0x06330040 - 0x6330045

4. Verify the following design pattern of these events/alarms:
   - 0x063300x0 Clear Event
   - 0x063300x1 Minor Event / Alarm
   - 0x063300x2 Major Event / Alarm
   - 0x063300x3 Critical Event / Alarm
   - 0x063300x4 Informational Event
5. To view alarms, click the Alarms tab.

   Alarms are displayed.

6. Click the Alarm Details tab in the Component Detail panel to view the alarm details.

   Events and Alarms that are generated in OneClick are verified.

Note: Alarms that are manually cleared in the Nimsoft Alarm Console do not clear the corresponding alarms in CA Spectrum. This behavior is caused by a known imitation of the SNMP Gateway probe (snmpgtw). Therefore, when you clear alarms in CA Nimsoft, the alarms accumulate in CA Spectrum, causing high alarm counts. These alarms must be manually cleared in CA Spectrum.

Chapter 3: Disable the Integration

You can disable the CA Nimsoft - CA Spectrum Integration, if you want to stop generating alarms and events in OneClick. On disabling the integration, the EventAdmin model no longer receives events from CA Nimsoft and the events are not forwarded to the EventModel model in OneClick.

Follow these steps:

1. Open CA Nimsoft Infrastructure Manager.
2. From the Console page, select Gateway.

   The SNMP Gateway window opens.
3. Click the Profiles tab.

   The Configured Profiles window opens.
4. Right-click a Profile, select Delete.

   Profile is deleted.
5. Click Ok.

   The Integration is disabled.

This section contains the following topics:

Performance Considerations (see page 27)

Performance Considerations

CA Nimsoft - CA Spectrum integration through the Southbound Gateway supports and implements all severities and traps (such as Informational, Warning, Minor, Major, Critical, Clear).

Note: By default, CA Nimsoft snmpgtw is configured to send alerts (traps) for messages of all severity levels.

The volume of events and alarms that are generated by CA Nimsoft in CA Spectrum depends on the number, type and condition of managed elements. In situations where performance is an issue, you can disable these messages at the CA Nimsoft Infrastructure Manager.

For example, if the trap storm detection threshold of CA Spectrum exceeds a certain level, it indicates that performance is degraded. By default this threshold is configured for 20 traps/second from a single device. In a moderately large CA Nimsoft installation, the CA Spectrum default trap storm threshold can be exceeded easily, and when it is exceeded, traps are dropped. To preserve the most critical traps, we recommend disabling the informational and warning messages. In this way, bandwidth is not used on less severe situations and the critical traps can be handled by CA Spectrum.

To handle this situation, you can disable the informational messages that are sent by CA Nimsoft. In this way the problem can be resolved at the source level. If the trap storm threshold is exceeded, the warning messages can be disabled and not sent to CA Spectrum. You can also raise the trap storm threshold to 25 or 30 traps/second, if the SpectroSERVER has sufficient capacity.

If after disabling the informational and warning messages, the number of alerts from CA Nimsoft still exceeds the trap storm threshold, consult CA Nimsoft documentation to determine ways to limit the number or types of traps being sent to CA Spectrum. By default all alarms are filtered. Therefore, you can change the alarm messages that are filtered by snmpgtw. You can also change the alarm setting to alarm_new and alarm_clear messages, which can reduce the total traffic from CA Nimsoft to CA Spectrum.

Note: If you change the alarm setting to alarm_new and alarm_clear message, the alarm counts may not be correctly incremented in CA Spectrum as a single message for each occurrence of an alarm that is received.

Index

C

CORBA • 9

E

EventAdmin • 9, 24, 25

L

Log file • 17
Log level • 17

N

Network Address • 24
    EventModel Prefix • 24
    Manager Name • 24
    Security String • 24
Nimsoft Alarm Server • 9

R

robots • 8, 9, 17

S

snmpgtw • 17
Southbound Gateway • 8, 9
    SNMP • 9

T

Target • 20
    Base Object Identifier • 20
    Community String • 20
    Level Mapping • 20
    Trap Mapping • 20
Trap variables • 17
Traps • 9, 11
    Alarms • 8, 9, 11
    Events • 9, 11, 25
    Views • 11