CA Spectrum® and CA Nimsoft

CA Spectrum - CA Nimsoft Integration Guide

CA Spectrum Release 9.4 / CA Nimsoft

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

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: Integration Overview

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

- Provides holistic view of availability of host servers on network and their performance data for fault management in a single pane of application. It also provides end to end root cause and impact analysis across network and server elements, extending CA Spectrum core capabilities to other infrastructure domains.
- Advance condition correlation between CA Nimsoft and CA Spectrum helps in building the robust fault management.
- Leverage CA Nimsoft capabilities for server management and use the CA Spectrum network management capabilities for an end to end infrastructure management.

Chapter 2: Integrating CA Spectrum and CA Nimsoft through the Web Server for Server Management

This section describes how to set up the integration between the current releases of CA Spectrum and CA Nimsoft through the web server for server management. It also describes how to use its features to perform specific tasks such as synchronize inventory, manage alarms and events, and run reports.

This section contains the following topics:

How to Integrate CA Spectrum and CA Nimsoft through the Web Server

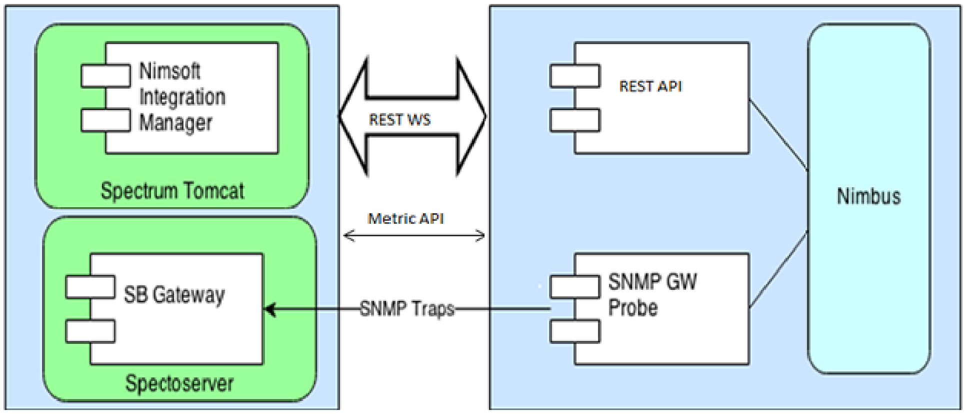
The main intent of the CA Spectrum and CA Nimsoft integration is to support server management. The HostServer models resulting from the integration provides traditional Spectrum capabilities such as layer2 connectivity and fault isolation with the features supported by Nimsoft monitor. You can use the Launch-in-Context feature to launch the CA Nimsoft Unified Management Portal (UMP) view from the server models in CA Spectrum to view the server information.

When the CA Nimsoft and CA Spectrum integration is enabled from the OneClick Administration page, CA Spectrum receives the data from CA Nimsoft through the Rest API. Once we get the data from the Rest API, Nimsoft hosts are modeled in CA Spectrum.

The alert data is sent from CA Nimsoft to the SpectroSERVER of CA Spectrum through the Southbound Gateway component. The received data is mapped to a CA Spectrum event. The Southbound Gateway determines the appropriate EventAdmin model to forward the event.

Metric violation traps that are coming from CA Nimsoft are asserted on the respective Nimsoft host models in CA Spectrum.

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



Review the following process to integrate CA Nimsoft and CA Spectrum through the Web Server:

1. Review the Prerequisites and Considerations (see page 11)
2. Deploy and Configure Probes (see page 12)
3. Enable the Integration (see page 13)

Prerequisites and Recommendations

Consider the following prerequisites for the CA Spectrum and CA Nimsoft integration:

- Licensed installations of CA Spectrum Release 9.4 and CA Nimsoft Management System (NMS) 7.6 are required.
- The snmpgtw, cdm, net_connect, nisrest probes must be deployed and configured before integrating CA Nimsoft and CA Spectrum through the Web Server.
- For Launch-in-Context to work, UMP must be configured to NMS.

Consider the following recommendations for the integration:

- If a new SpectroSERVER is added to the Distributed SpectroSERVER (DSS) setup, you must restart the OneClick server.
- If a child SpectroSERVER is removed from the DSS setup, restart the OneClick server.
- If anyone of the available SpectroSERVER is initialized to legacy database or another database, restart the OneClick server.
- Specify a SpectroSERVER that has less load as the dedicated SpectroSERVER for CA Nimsoft integration.
- Use a OneClick web server which is not integrated with Spectrum Report Manager.
- If any of the following configuration details are modified from other OneClick web server then the web server becomes integration server:
  - Nimsoft Server Address
  - Nimsoft Server Port
  - UMP Server Address
  - UMP Server Port
  - Dedicated SpectroSERVER

Deploy and Configure Probes

To enable the CA Spectrum and CA Nimsoft integration, deploy and configure the following CA Nimsoft probes on CA Nimsoft server:

snmpgtw

Sends traps from CA Nimsoft to CA Spectrum. The SNMP gateway converts alarms to SNMP trap messages that are readable by any SNMP-based event manager.

cdm

Monitors performance and load on critical system resources such as CPU, Disk, and Memory. The Nimsoft CPU, Disk & Memory (cdm) probe generates alarms that are based on configured threshold values and trending statistics.

net_connect

Measures network connectivity that is based on "ping" (ICMP ECHO) and the TCP connections to a list of user-defined services. The service can be NetBIOS, Telnet, FTP, and HTTP. The probe supports the Nimsoft Monitor family of solutions by sending quality of service (QoS) messages.

nisrest

Queries the CA Nimsoft Manager using the Restfull Services API to retrieve the list of Nimsoft models to be monitored.

You can configure the CA Nimsoft probes through the Probe Configuration interface. For more information, see the *CA Nimsoft Documentation*.

Enable the Integration

You can enable the CA Spectrum and CA Nimsoft integration through the web server from the OneClick Administration page. Specify the Nimsoft Configuration information such as Nimsoft Server Host Name, Nimsoft Server Port, Unified Management Portal (UMP) Server Host Name, and UMP Server Port to enable the integration.

Follow these steps:

1. Open the OneClick Administration page.

   The OneClick Administration page opens.

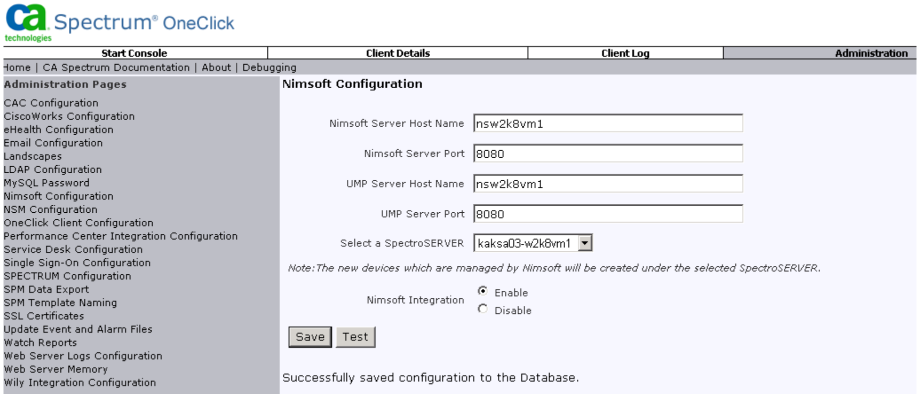
2. Click the Administration tab.

   Links to various OneClick web server configuration pages is displayed.

3. Click the Nimsoft Configuration link in the left panel.

   The Nimsoft Configuration page opens.

   The following image illustrates the configuration options that are available in the Nimsoft Configuration window:



Nimsoft Configuration

Nimsoft Server Host Name: nsw2k8vm1

Nimsoft Server Port: 8080

UMP Server Host Name: nsw2k8vm1

UMP Server Port: 8080

Select a SpectroSERVER: kaksa03-w2k8vm1

Note:The new devices which are managed by Nimsoft will be created under the selected SpectroSERVER.

Nimsoft Integration: ● Enable ○ Disable

Successfully saved configuration to the Database.

   Nimsoft Server Host Name

   Indicates the IP address/hostname of the Nimsoft Server.

   Nimsoft Server Port

   Indicates the server port number of CA Nimsoft Monitor.

   UMP Server Host Name

   Indicates the IP address/hostname of UMP.

   UMP Server Port

   Indicates the server port number of UMP.

4. Select the SpectroSERVER for the new Nimsoft Host models to be created.

5. To enable the Nimsoft integration, select Enable and click Test.

   If test is successful, Successfully connected to Nimsoft message appears.

6. Click Save.

   Successfully saved configuration to the database message appears.

   CA Nimsoft Integration is now enabled.

Disable the Integration

You can disable the CA Spectrum and CA Nimsoft Integration from the OneClick Administration page.

Note: You must disable CA Nimsoft integration from the web server on which the integration is enabled.

Follow these steps:

1. Open the OneClick Administration page.

   The OneClick Administration page opens.

2. Click the Administration tab.

   Links to various OneClick web server configuration pages is displayed.

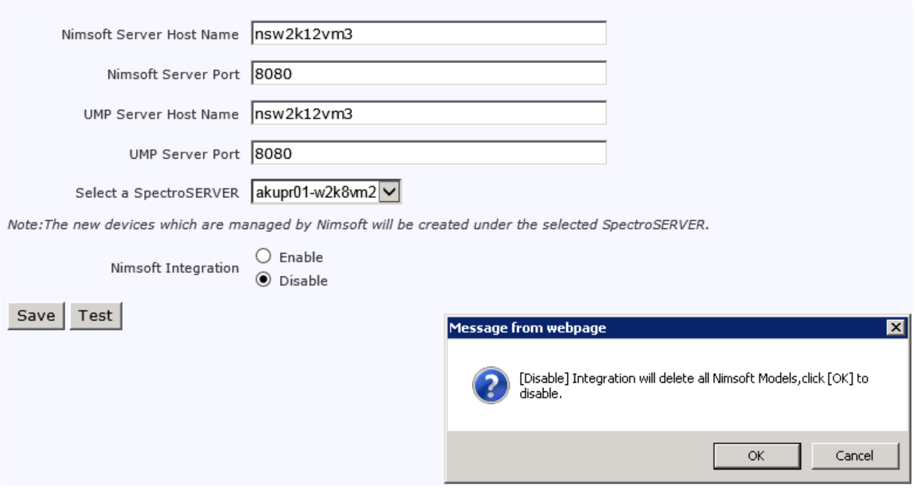
3. Click the Nimsoft Configuration link in the left panel.

   The Nimsoft Configuration window opens.

4. To disable the Nimsoft integration, select Disable and click Save.

   The confirmation dialog appears.

   The following image displays the confirmation dialog that appears after disabling the integration:



Nimsoft Server Host Name: nsw2k12vm3

Nimsoft Server Port: 8080

UMP Server Host Name: nsw2k12vm3

UMP Server Port: 8080

Select a SpectroSERVER: akupr01-w2k8vm2

Note:The new devices which are managed by Nimsoft will be created under the selected SpectroSERVER.

Nimsoft Integration: ○ Enable ● Disable

Message from webpage

[Disable] Integration will delete all Nimsoft Models,click [OK] to disable.

5. To confirm, click Ok.

   CA Nimsoft integration is disabled successfully.

Note: Wait for the all the Nimsoft Host server models and the folder hierarchy to be cleared from the Nimsoft Manager in the OneClick view after disabling the integration. To validate, search for any Nimsoft Host Server models, using the search option.

Incremental Sync and Full Sync

This Integration supports incremental and full synchronization. When the CA Spectrum and CA Nimsoft integration is enabled, synchronization occurs automatically with the default scheduled timings displayed in the OneClick view.

Incremental Synchronization

Additions and modifications of devices in CA Nimsoft are reflected in CA Spectrum after incremental synchronization. You can set the Incremental Sync interval in the OneClick view.

Full Synchronization

Full synchronization occurs when the CA Spectrum and CA Nimsoft integration is enabled. Thereafter, the full synchronization occurs at a scheduled time based on the schedule that is selected in the OneClick view. During full sync CA Spectrum queries CA Nimsoft for all the hosts that are managed by CA Nimsoft. Once Spectrum receives this data, reconciliation is performed and new hosts (if any) are modeled in Spectrum. The un-managed hosts are removed.

The minimum schedule time for full sync is one day. The last full sync time in the OneClick view displays the previous full sync completion time. The sync times are based on the OneClick tomcat server time.

Note: Do not schedule the incremental or full sync at smaller intervals, you may experience a performance impact if the number of servers being monitored by CA Nimsoft is large.

Important! Schedule full synchronization during non-business hours.

Follow these steps:

1. Open the CA Spectrum OneClick console.
2. From the Navigation panel, select Nimsoft Manager.

   The Contents pane for Nimsoft Manager opens.
3. Click the Information tab and select Nimsoft Sync Configuration.

   Information on incremental and full synchronization is displayed.
4. To schedule incremental sync, click set.

   The Time interval window opens.
5. Specify the time interval and click Ok.

   Default: 300 minutes

   Incremental sync is scheduled

6. To schedule full sync, click the Schedule button that is available in the Nimsoft Sync Configuration section.

   The Create Schedule window opens.

7. Specify the following Recurrence information:

   - Days

     Default: 7

     Maximum: 31

   - Hours

     Default: 00:01

     Maximum: 23:59

8. Click Ok.

   Full sync is scheduled.

QoS Metrics

QoS Metric Information provides the metrics for both CPU and memory usage. From the Navigation Pane of OneClick Console, you can access the QoS metrics information of the available Nimsoft Host Models. The following metrics are available for each Nimsoft Host Model modeled in CA Spectrum:

- QoS CPU Usage Metrics
- QoS Multi Usage Metrics
- QoS Memory Metrics
- QoS Disk Metrics

Follow these steps:

1. From the OneClick Console, select the Nimsoft Host Model available in the Navigation Panel.

   Contents Pane for the selected Nimsoft Host Model is displayed.

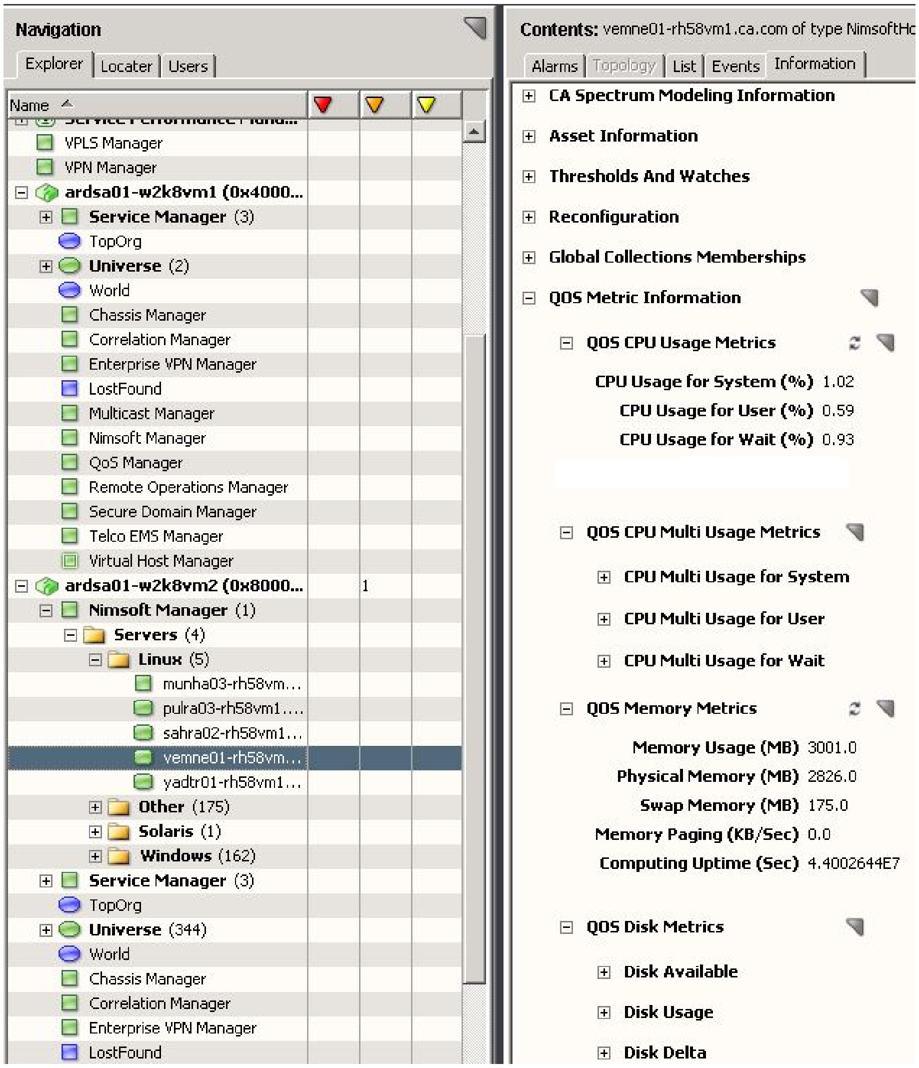
2. Click the Information tab on Contents Pane.

   Nimsoft Host Model information is displayed.

3. Expand QoS Metric Information SubView.

   QoS Metrics for the selected Nimsoft Host Model is displayed.

   The following image displays the QoS Metrics for the Nimsoft Host Model in CA Spectrum:



Contents: vemne01-rh58vm1.ca.com of type NimsoftHc

CPU Usage for System (%) 1.02
CPU Usage for User (%) 0.59
CPU Usage for Wait (%) 0.93

Memory Usage (MB) 3001.0
Physical Memory (MB) 2826.0
Swap Memory (MB) 175.0
Memory Paging (KB/Sec) 0.0
Computing Uptime (Sec) 4.4002644E7

The following QoS Metrics are supported in this integration:

CPU Usage for System

Specifies the time that CPU spends on system tasks in percent.

CPU Usage for User

Measures the time that CPU spends on user tasks in percent.

CPU Usage for Wait

Measures the time the CPU waits when accessing external memory or another device in percent.

CPU Multi Usage for System

Measures the time the CPU spends on system tasks in percent.

CPU Multi Usage for User

Measures the time that CPU spends on user tasks in percent.

CPU Multi Usage for Wait

Measures the time the CPU waits when accessing external memory or another device in percent.

Disk Available

Measures the amount of total available disk space for the file system. The Disk Available metrics are populated for only Network file systems.

Disk Usage

Measures the amount of total used disk space in the file system.

Disk Delta

Measures the amount of total disk usage change in the file system.

Memory Usage

Measures the amount of total available memory (physical and virtual memory) used in megabytes

Physical Memory

Measures the amount of total available physical memory that is used in megabytes.

Swap Memory

Measures the space on the disk that is used for the swap file in megabytes.

Memory Paging

Measures the amount of memory that is sent or reads from virtual memory in kilobytes/second.

Computing Uptime

Measures the computer uptime in seconds every hour.

Note: You may experience latency in loading QoS Metrics as the values are generated dynamically from Nimsoft server, when queried.

Launch-in-Context

The Launch-in-context feature is used to view the Unified Management Portal (UMP) of the host for the CA Nimsoft host model. This feature provides a detailed information about the Nimsoft host model such as disk usage, cpu usage, processor queue length, paging, and memory usage. The information about the Nimsoft host model is displayed graphically.

If you are launching the UMP view for the first time in a browser, a dialog for user credentials appear. The user credentials dialog does not appear if you are launching the UMP view using the same browser instance.

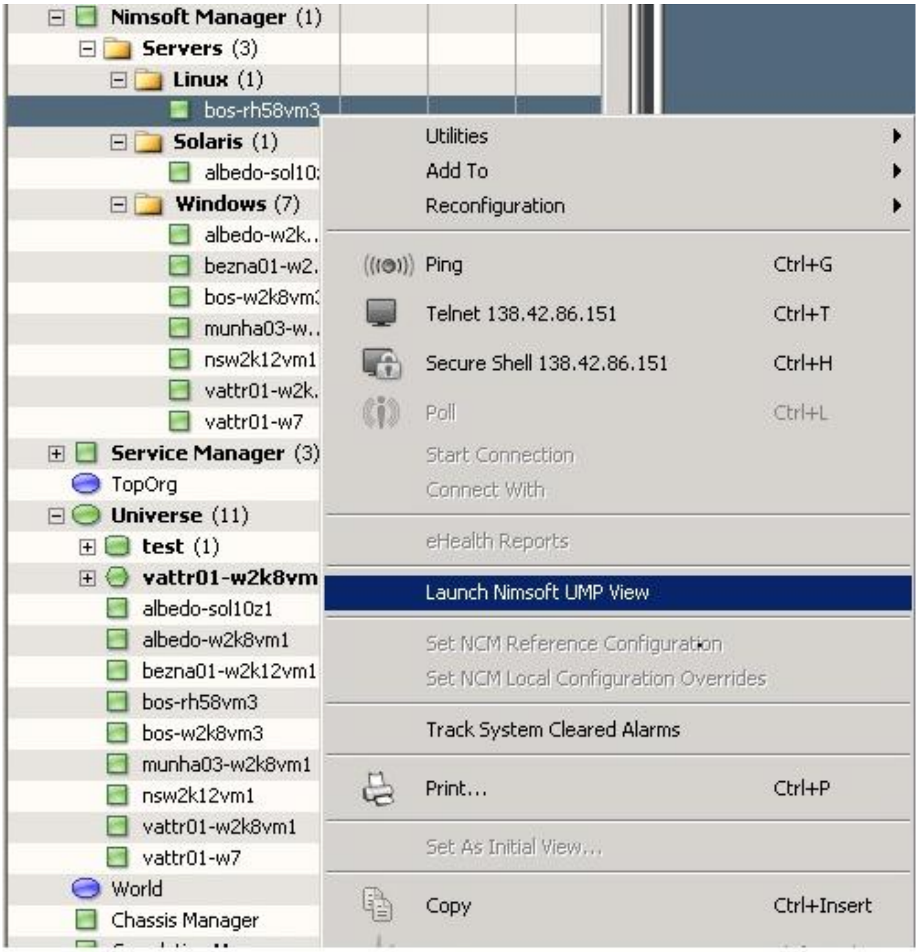
Follow these steps:

1. Open the CA Spectrum OneClick console.
2. From the Navigation panel, select Nimsoft Manager and Servers.

   A complete list of host models is displayed in respective folders.
3. Right-click a host model and select Launch Nimsoft UMP View.

   The Nimsoft UMP login page opens.

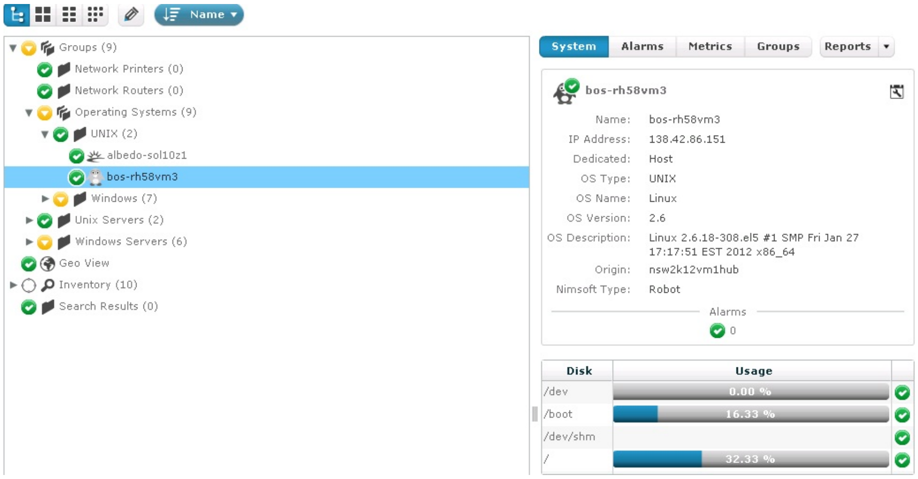
   The following image displays the available host models and the option to launch the UMP view from the OneClick console:



4. Enter the Nimsoft UMP credentials and click Login.

   The selected model details are displayed and the Nimsoft UMP login is successful.

   The following image displays the Nimsoft UMP view:



bos-rh58vm3

Name: bos-rh58vm3
IP Address: 138.42.86.151
Dedicated: Host
OS Type: UNIX
OS Name: Linux
OS Version: 2.6
OS Description: Linux 2.6.18-308.el5 #1 SMP Fri Jan 27 17:17:51 EST 2012 x86_64
Origin: nsw2k12vm1hub
Nimsoft Type: Robot

Alarms
✓ 0

Disk	Usage	
/dev	0.00 %	✓
/boot	16.33 %	✓
/dev/shm		✓
/	32.33 %	✓

Locater Search

You can use the search functionality in the Locater tab to find the Nimsoft related devices that are available in the CA Spectrum environment. Search can be performed based on the Operating system type such as Windows, Linux, Solaris, and Other. Using this functionality, you can also search for all the NimsoftHostServer models and Nimsoft models that are available in CA Spectrum. The Search results appear in the Results tab of the Contents panel. Detailed information for application models that are selected in the results list appears in the Component Detail panel. Access Locater search from the Locater tab of the Navigation Panel.

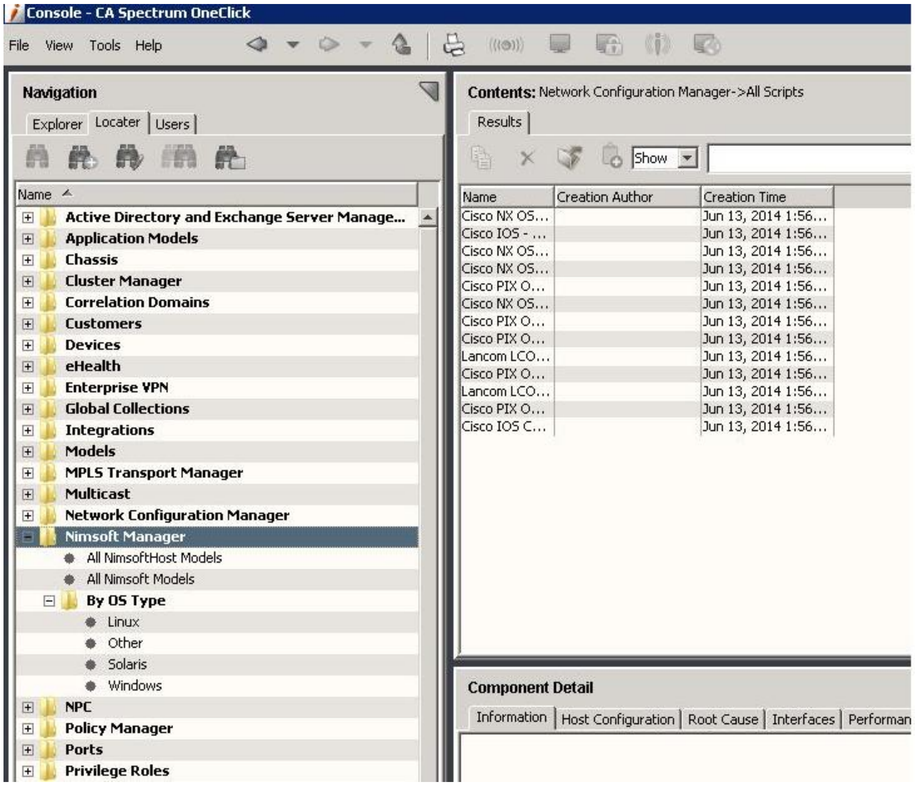
Follow these steps:

1. Open the CA Spectrum OneClick Console.
2. From the Navigation Panel, Click the Locater tab.

   The Search Options window opens.
3. Expand Nimsoft Manager and select the models.

   The Locater Search results are displayed in the Contents pane.

   The following figure displays the Locater Search results for Nimsoft Configuration Manager:



Contents: Network Configuration Manager->All Scripts

Name	Creation Author	Creation Time
Cisco NX OS…		Jun 13, 2014 1:56…
Cisco IOS - …		Jun 13, 2014 1:56…
Cisco NX OS…		Jun 13, 2014 1:56…
Cisco NX OS…		Jun 13, 2014 1:56…
Cisco PIX O…		Jun 13, 2014 1:56…
Cisco NX OS…		Jun 13, 2014 1:56…
Cisco PIX O…		Jun 13, 2014 1:56…
Cisco PIX O…		Jun 13, 2014 1:56…
Lancom LCO…		Jun 13, 2014 1:56…
Cisco PIX O…		Jun 13, 2014 1:56…
Lancom LCO…		Jun 13, 2014 1:56…
Cisco PIX O…		Jun 13, 2014 1:56…
Cisco IOS C…		Jun 13, 2014 1:56…

Reports

You can generate asset, alarm, availability, and WEBI reports for the CA Nimsoft hosts. You can access InfoView from the OneClick home page to generate and manage reports. For more information, see the *Spectrum Report Manager User Guide*.

Outage Events

This section lists the events that mark the beginning and end of either a planned or unplanned model outage. The following list of events is used for the calculation of availability reports for Nimsoft Host Server Models.

- Up events
    - 0x6330057
    - 0x6330000
- Down events
    - 0x6330003
    - 0x6330056

Standard up and down events are ignored for Nimsoft Host Server Models while calculating the outages. For an existing spectrum model the outage is calculated based on standard up and down events.

Traps and Alarms Support

This integration supports the following alarms:

Generic Alarms

If any threshold violation occur on Nimsoft hosts, generic alarms are raised.

Event Code Range: 0x630000 - 0x630005

Disk Alarms

If the disk usage is high or the disk space availability is low on Nimsoft hosts, disk alarms are raised.

Event Code Range: 0x630030 - 0x630035

Memory Alarms

If low memory or any threshold violations are noticed on Nimsoft hosts, raise memory alarms.

Event Code Range: 0x630040 - 0x630045

CPU Alarms

If CPU utilization is high on Nimsoft hosts, CPU alarms are raised.

Event Code Range: 0x630050 - 0x630055

Condition Correlation and Fault Isolation in CA Nimsoft Integration

If a managed device stops responding to polls, the CA Spectrum fault isolation algorithm determines whether to create a critical alarm for the Nimsoft hosts or suppress its alarm state. The unreachable device is the root cause of the alarm.

After the integration of CA Spectrum and CA Nimsoft, the events/alarms are received from both Spectrum polling and CA Nimsoft. Consider the following scenarios to apply condition correlation:

Scenario 1

If a Spectrum event is generated on the Nimsoft host before the Nimsoft event, condition correlation applies and the Nimsoft event suppresses the Spectrum event.

Scenario 2

If a Nimsoft Event is generated on the Nimsoft host before the Spectrum event, condition correlation applies and the events are asserted on their respective host.

Scenario 3

If only Spectrum event is generated on the Nimsoft host, condition correlation cannot be performed until the Nimsoft event is generated and the Spectrum Event is displayed on the Nimsoft host.

Scenario 4

If only Nimsoft event is generated, you cannot perform condition correlation and the Nimsoft Event is displayed on the Nimsoft host.

Debugging

Debugging in CA Spectrum lets you track the data flow from CA Nimsoft to CA Spectrum. It investigates and resolves integration related issues. The Start Client Debug Console contains various debug modules. Turn on Nimsoft Integration Information to track alerts and CIs that flow from CA Nimsoft to CA Spectrum.

To use Start Client Debug Console, you must first have a running OneClick client. This debug tool lets you turn on debugging output that can be seen in the Java Web Start log.

Follow these steps:

1. Open the OneClick Adminstration page.

   The OneClick Adminstration page opens.

2. Click the Administration tab.

   Links to various OneClick web server configuration pages is displayed.

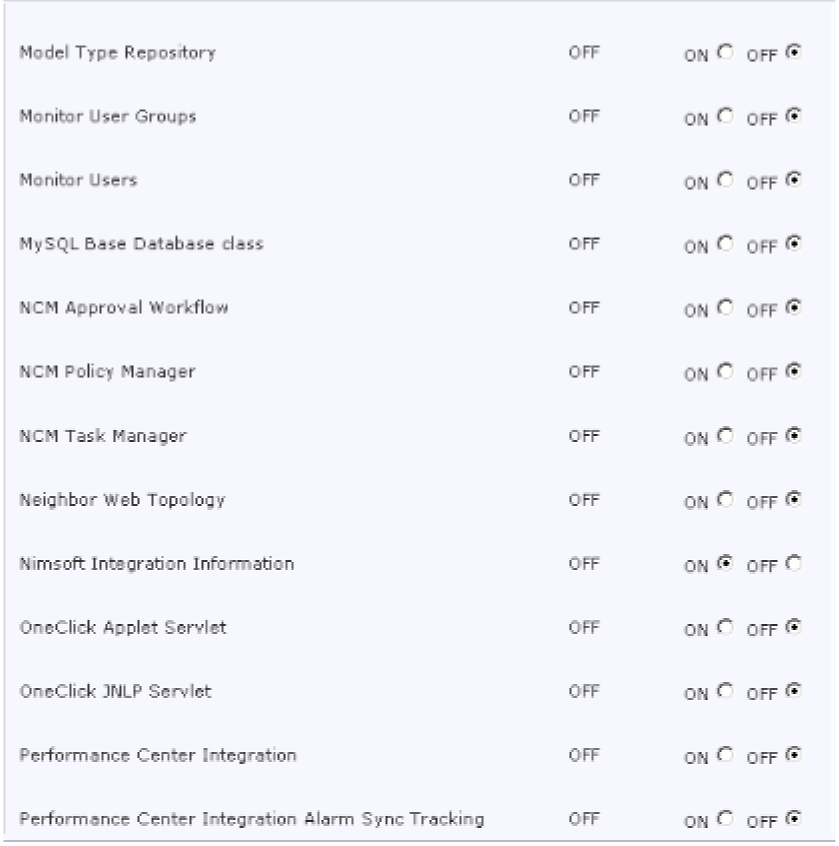
3. Click the Debugging tab.

   A panel with various links to view debugging output opens.

4. Click Start Client Debug Console.

   A list of debug modules is displayed.

   The following image displays the list of available debug modules:



Model Type Repository	OFF	ON ○	OFF ●
Monitor User Groups	OFF	ON ○	OFF ●
Monitor Users	OFF	ON ○	OFF ●
MySQL Base Database class	OFF	ON ○	OFF ●
NCM Approval Workflow	OFF	ON ○	OFF ●
NCM Policy Manager	OFF	ON ○	OFF ●
NCM Task Manager	OFF	ON ○	OFF ●
Neighbor Web Topology	OFF	ON ○	OFF ●
Nimsoft Integration Information	OFF	ON ●	OFF ○
OneClick Applet Servlet	OFF	ON ○	OFF ●
OneClick JNLP Servlet	OFF	ON ○	OFF ●
Performance Center Integration	OFF	ON ○	OFF ●
Performance Center Integration Alarm Sync Tracking	OFF	ON ○	OFF ●

5. To enable debug, select On for the Nimsoft Integration Information debug module.

6. Select Max as Desired Level and click Apply.

   Debug is enabled.

7. To disable debug, select OFF and click Apply.

   Debug is disabled.

Appendix A: Troubleshooting

This section contains the following topics:

Alarm Forwarding Not Working for CA Nimsoft

Symptom:

On a Distributed SpectroSERVER (DSS) setup, when the Nimsoft managed hosts are modeled in Spectrum on landscapes other than Main Location Server (MLS), the Nimsoft alarms that are raised on hosts may not get forwarded to the host models in non-MLS landscapes.

Solution:

To fix this issue, create the EventAdmin models manually for Nimsoft Integration on all the landscapes in DSS when the integration is enabled. Review the following scenarios before creating the EventAdmin model manually:

Scenario 1:

For fresh integration or if the Nimsoft models (existing models or Nimsoft host models) are on landscapes other than MLS, create the EventAdmin models manually on other landscapes so that the alarms are forwarded to hosts.

Note: Use the default options while creating the EventAdmin model and do not enable the Alert_Forwarding_Enabled attribute.

Follow these steps:

1. To launch the OneClick Console, select Start Console at the top of the OneClick page, and log in as a CA Spectrum administrator.
2. Select the SpectroSERVER and Universe on the Explorer tab of the OneClick Navigation panel.
3. Select the Topology tab on the Contents panel and click the Create a New Model by Type icon.

   The Select Model Type dialog appears.
4. Click the All Model Types tab.
5. Select EventAdmin and click OK.

   The Create Model of Type dialog appears.
6. Enter the name and IP address of the CA Nimsoft server and click OK.

   The CA Nimsoft server is added to the topology as the selected model type. For more information about creating a model in OneClick, see the *CA Spectrum Modeling and Managing Your IT Infrastructure Administrator Guide*.

Scenario 2:

If CA Nimsoft Integration is enabled through the Southbound Gateway and an EventAdmin model already exists on a landscape, the attribute SBG_AlertForwardingEnabled must be enabled for the existing EventAdmin. The EventAdmin models must be created manually on other landscapes.

Follow these steps:

1. To create an EventAdmin model manually, follow the instructions that are documented for Scenario 1.
2. To enable the SBG_AlertForwardingEnabled attribute, select the EventAdmin in the OneClick Topology.
3. Select the Attributes tab in the Component Detail panel.
4. Select SBG_AlertForwardingEnabled in the left window of the Attributes panel.

   The attribute is added to the right window of the Attributes panel.
5. Double-click SBG_AlertForwardingEnabled in the right window, and select Yes. Click OK.

   The SBG_AlertForwardingEnabled attribute is enabled.

Note: You must delete EventAdmin and the associated event models when the integration is disabled.

The Technology Folders Cannot be Created Automatically, if Deleted.

Symptom:

If the technology folders (such as Windows, Linux, Solaris, and Other) that are available in Nimsoft Manager are deleted, the folders cannot be created automatically.

Solution:

Do not delete the technology folders (such as Windows, Linux, Solaris, and Other) that are available in Nimsoft Manager. If you delete these folders, you must disable and enable the integration to create the folders.

Chapter 3: CA Nimsoft and CA Spectrum Integration through the Southbound Gateway

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.

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*.

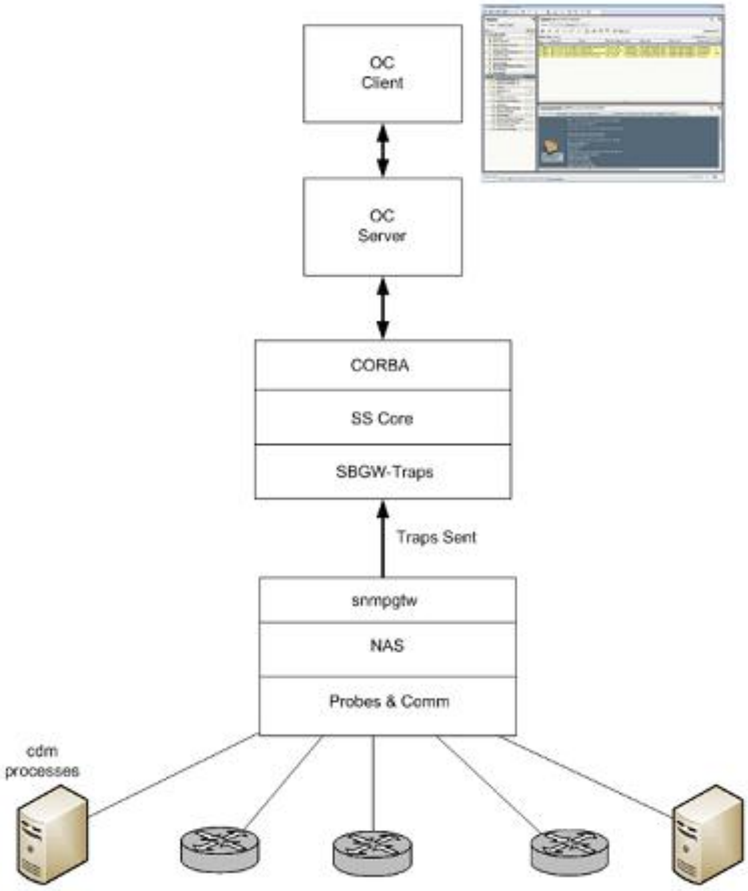
Using the Southbound Gateway, you can centralize network management, allowing CA Spectrum to capture and display data. Alert data is organized into CA Spectrum event and alarm data as appropriate and is displayed within OneClick.

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.

Coexistence and Compatibility with Previous Integrations

Multiple integrations between CA Spectrum and CA Nimsoft 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.

Chapter 4: Integrating CA Nimsoft and CA Spectrum through the Southbound Gateway

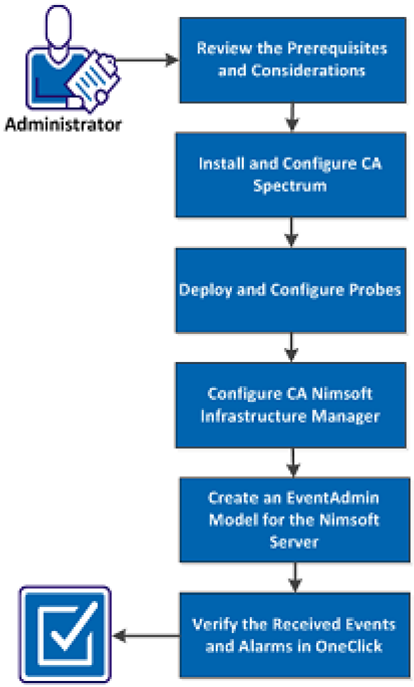
The CA Spectrum and CA Nimsoft integration is performed through the CA Spectrum Southbound Gateway component. The component asserts the alarm against the existing device model or against an auto-created event model of CA Nimsoft Robot. CA Spectrum EventModel is used when a full device model for the network 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. CA Spectrum accepts an individual SNMP trap packet to a maximum size of 65467 bytes. 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


Administrator
Review the Prerequisites and Considerations
Install and Configure CA Spectrum
Deploy and Configure Probes
Configure CA Nimsoft Infrastructure Manager
Create an EventAdmin Model for the Nimsoft Server
Verify the Received Events and Alarms in OneClick

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

1. Review the Prerequisites and Considerations (see page 38)
2. Install and Configure CA Spectrum (see page 40)
3. Deploy and Configure Probes (see page 41)
4. Configure CA Nimsoft Infrastructure Manager (see page 44)
5. Create an EventAdmin Model for the Nimsoft Server (see page 48)
6. Verify the Received Events and Alarms in OneClick (see page 49)

This section contains the following topics:

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.
- For the events and alarms to be raised on the correct CA Spectrum model, use IP address instead of host name to model the entity on CA Nimsoft. If a host name is used for entities that are modeled in CA Nimsoft, CA Spectrum alarms are raised on the EventModel of robot hosting the probe.

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.

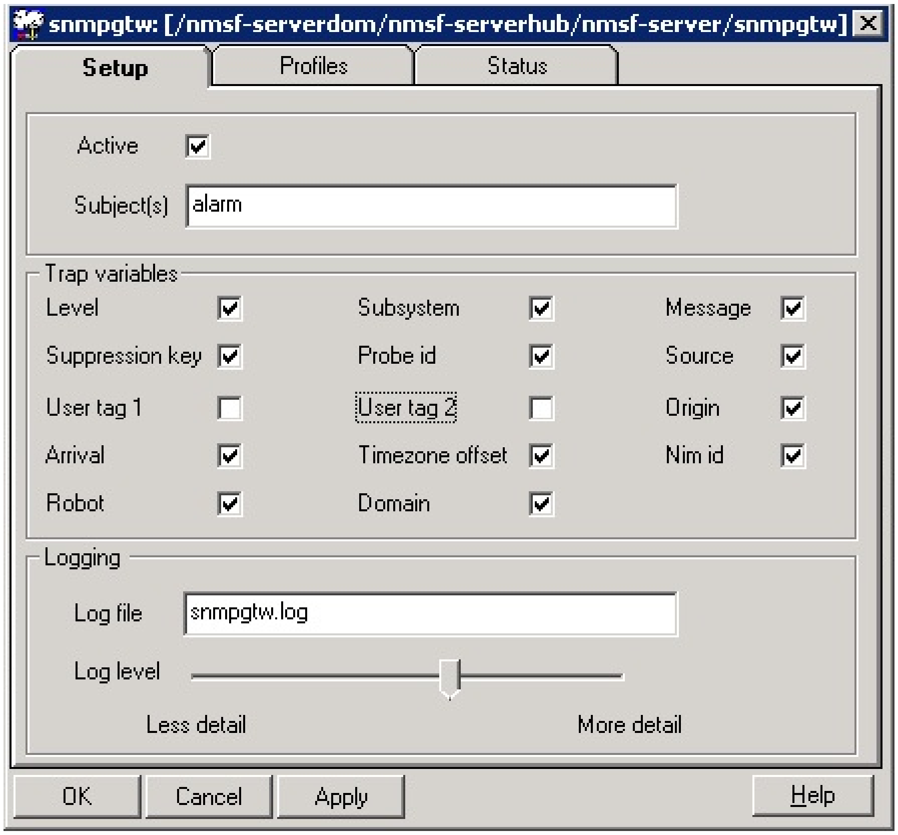
   Log file

   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:



snmpgtw: [/nmsf-serverdom/nmsf-serverhub/nmsf-server/snmpgtw]
Setup
Profiles
Status
OK
Cancel
Apply
Help

Active ☑

Subject(s) alarm

Trap variables

Level ☑ Subsystem ☑ Message ☑

Suppression key ☑ Probe id ☑ Source ☑

User tag 1 □ User tag 2 □ Origin ☑

Arrival ☑ Timezone offset ☑ Nim id ☑

Robot ☑ Domain ☑

Logging

Log file snmpgtw.log

Log level

Less detail More detail

8. Click the Profiles tab.

   The Profile window opens. For more information, see Configure CA Nimsoft Infrastructure Manager (see page 44).

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 41).

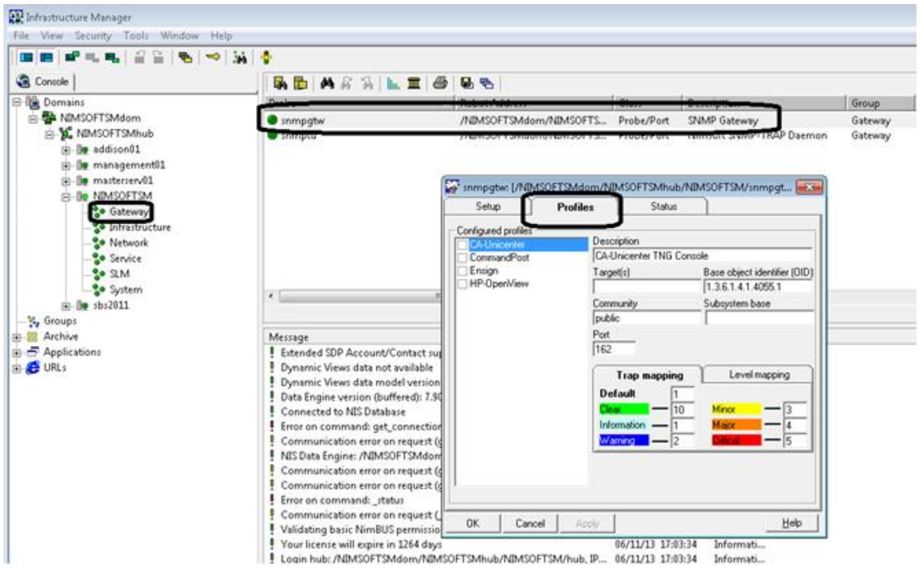
A profile is created in the SNMP Gateway Probe to communicate to the CA Nimsoft Monitor about the traps to send, the conditions under which to send them, and where to send them.

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:



snmpgtw /NIMSOFTSMdom/NIMSOFTS... Probe/Port SNMP Gateway Gateway

snmptd /NIMSOFTSMdom/NIMSOFTS... Probe/Port Nimsoft SNMP-TRAP Daemon Gateway

Configured profiles:

- □ CA-Unicenter
- □ CommandPost
- □ Ensign
- □ HP-OpenView

Description: CA-Unicenter TNG Console

Target(s):

Base object identifier (OID): 1.3.6.1.4.1.4055.1

Community: public

Subsystem base:

Port: 162

Trap mapping			
Default	1		
Clear	10	Minor	3
Information	1	Major	4
Warning	2	Critical	5

```
! Extended SDP Account/Contact su
! Dynamic Views data not available
! Dynamic Views data model version
! Data Engine version (buffered): 7.9
! Connected to NIS Database
! Error on command: get_connection
! Communication error on request (
! NIS Data Engine: /NIMSOFTSMdom
! Communication error on request (
! Communication error on request (
! Error on command: _status
! Communication error on request (
! Validating basic NimBUS permissio
! Your license will expire in 1264 days                          06/11/13 17:03:34   Informati...
! Login hub: /NIMSOFTSMdom/NIMSOFTSMhub/NIMSOFTSM/hub, IP...     06/11/13 17:03:34   Informati...
```

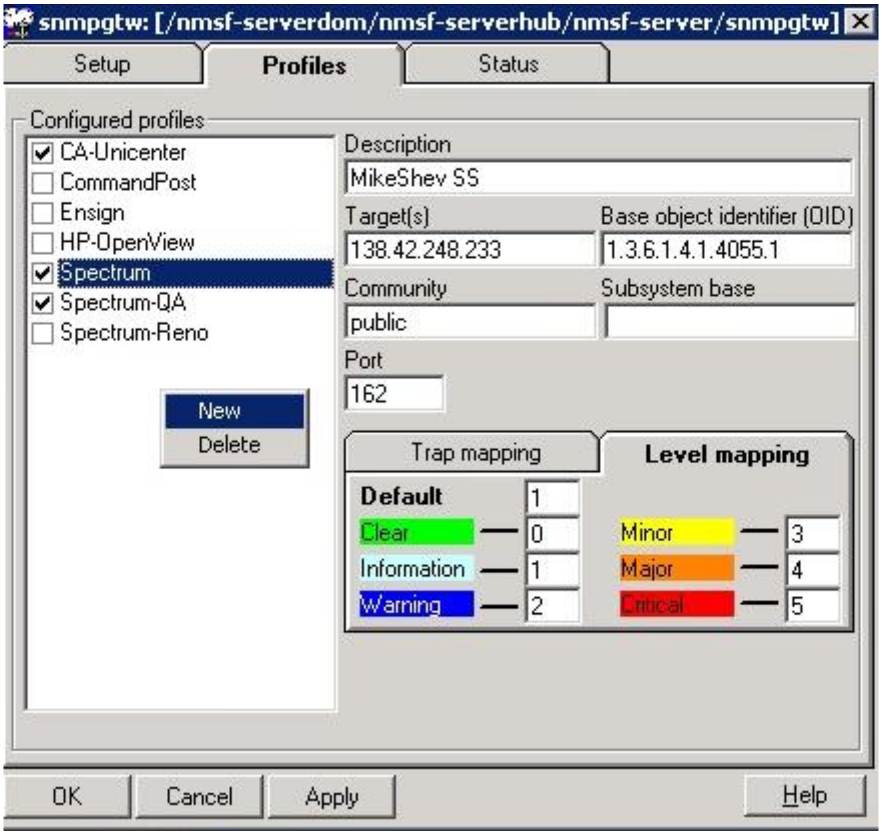
3. Double-click the snmpgtw probe.

   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:



Configured profiles

- ☑ CA-Unicenter
- ☐ CommandPost
- ☐ Ensign
- ☐ HP-OpenView
- ☑ Spectrum
- ☑ Spectrum-QA
- ☐ Spectrum-Reno

Description: MikeShev SS

Target(s): 138.42.248.233

Base object identifier (OID): 1.3.6.1.4.1.4055.1

Community: public

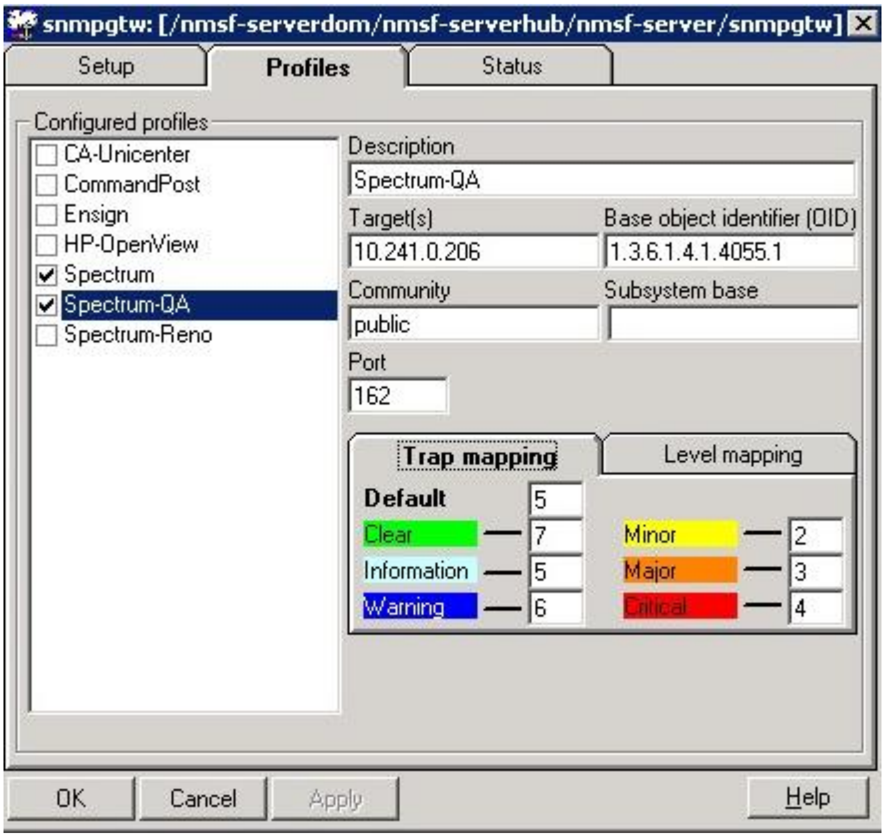
Subsystem base:

Port: 162

Default	1		
Clear	0	Minor	3
Information	1	Major	4
Warning	2	Critical	5

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.



snmpgtw: [/nmsf-serverdom/nmsf-serverhub/nmsf-server/snmpgtw]

Configured profiles

- □ CA-Unicenter
- □ CommandPost
- □ Ensign
- □ HP-OpenView
- ☑ Spectrum
- ☑ Spectrum-QA
- □ Spectrum-Reno

Description: Spectrum-QA

Target(s): 10.241.0.206

Base object identifier (OID): 1.3.6.1.4.1.4055.1

Community: public

Subsystem base:

Port: 162

Default	5		
Clear	7	Minor	2
Information	5	Major	3
Warning	6	Critical	4

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 53).

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.

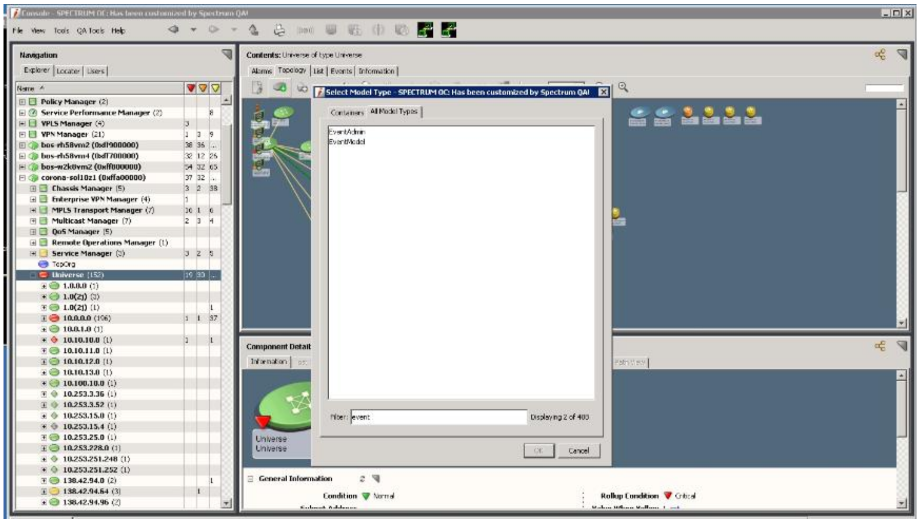
The EventModel is a model type that represents a unique source of event data on the system that is managed by the EventAdmin application. A given EventAdmin model can contain one or many instantiated EventModels. Each event that is received through the Southbound Gateway contains information that uniquely 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:

   EventAdmin
   EventModel

   Filter: event
   Displaying 2 of 400

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

Note: You can review the following table to know how the CA Nimsoft message severities are mapped to CA Spectrum events and alarms:

Nimsoft	Spectrum
Informational	Event only
Warning	Event only
Minor	Minor Alarm
Major	Major Alarm
Critical	Critical Alarm

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 5: 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

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