HP Network Node Manager i Software

Step-by-Step Guide to Deploying NNMi

NNMi 9.1x Patch 1

This document describes deploying a new NNMi 9.10 installation on a small test network. The steps included are similar to those you would take to deploy NNMi in a production network.

Read this document, and then use the *HP Network Node Manager i Software Deployment Reference* as a resource. It contains many details that extend beyond the technical scope of this document.

To find the latest *HP Network Node Manager i Software Deployment Reference, see* http://h20230.www2.hp.com/selfsolve/manuals.

CONTENTS

The Basic Steps: A Roadmap

This document assumes you have completed the following prerequisites:

- You have installed NNMi.
- Your server meets all the system prerequisites, including the patch requirements and kernel parameters shown in the *HP Network Node Manager i Software System and Device Support Matrix*, available at http://h20230.www2.hp.com/selfsolve/manuals.

Caution: The NNMi installation script does not check that your server meets the system prerequisites. Ignoring these requirements can cause issues after you complete your installation.

The examples in this document are of an NNMi installation on a Linux server. If you are using NNMi installed on a Windows server, convert any paths and commands.

This document describes the following tasks:

1. Apply the License
2. Back up the Original Configuration
3. Sign in to NNMi and Create Users
4. Set up Communication Configuration
5. Configure Discovery
6. Configure Monitoring
7. Configure Incidents, Traps, and Automatic Actions
8. Configure the NNMi Console
9. Maintain NNMi
10. Check NNMi Health

It also includes Best Practices and Example Usage Scenarios.

See the *HP Network Node Manager i Software Deployment Reference*, available at http://h20230.www2.hp.com/selfsolve/manuals, for information about the following topics:

1. Security Groups and Multi-tenancy
2. Integration with other HP products such as HP Operations Manager (HP OM), HP Universal Configuration Management Database (HP UCMDB), and third-party products
3. High Availability or Application Failover
4. Using a remote Oracle database
5. NNM iSPIs, such as NNM iSPI for Performance and NNM iSPI for MPLS

Apply the License

You can use the instant-on license or obtain a larger temporary license from HP.

Contact your HP Sales Representative or your Authorized Hewlett-Packard Reseller for information about the NNMi licensing structure, and to learn how to add license tiers for enterprise installations. To obtain additional license keys, go to the HP License Key Delivery Service: https://webware.hp.com/welcome.asp

Note: The instant-on license enables NNMi for 250 nodes.

You can install the license using the command line. The following command shows an example of installing the license using the `nnmlicense.ovpl` script:

```
nnmlicense.ovpl NNM -f ./mylicense.key
```

Back up the Original Configuration

Make a backup of the original NNMi configuration before making any changes. This way, you can revert back to the original configuration if needed.

To back up the original NNMi configuration, complete the following steps:

1. Create a directory on the NNMi management server where you want to keep the original configuration files. For this example, create a directory called /var/tmp/origconfig.
2. Run the **`nnmconfigexport.ovpl`** command using the **`-c`** and **`-f`** options. The **`–c`** option specifies *all configurations* and the **`–f`** option specifies the directory.

   The following command shows an example of running the `nnmconfigexport.ovpl` script:

   ```
   nnmconfigexport.ovpl -c all -f /var/tmp/origconfig/
   ```

   After you run the **`nnmconfigexport.ovpl`** script, NNMi displays output similar to the following:

   ```
   Successfully exported /var/tmp/origconfig/incident.xml.
   Successfully exported /var/tmp/origconfig/status.xml.
   …
   Successfully exported /var/tmp/origconfig/account.xml.
   Successfully exported /var/tmp/origconfig/securitymappings.xml.
   Successfully exported /var/tmp/origconfig/security.xml.
   ```

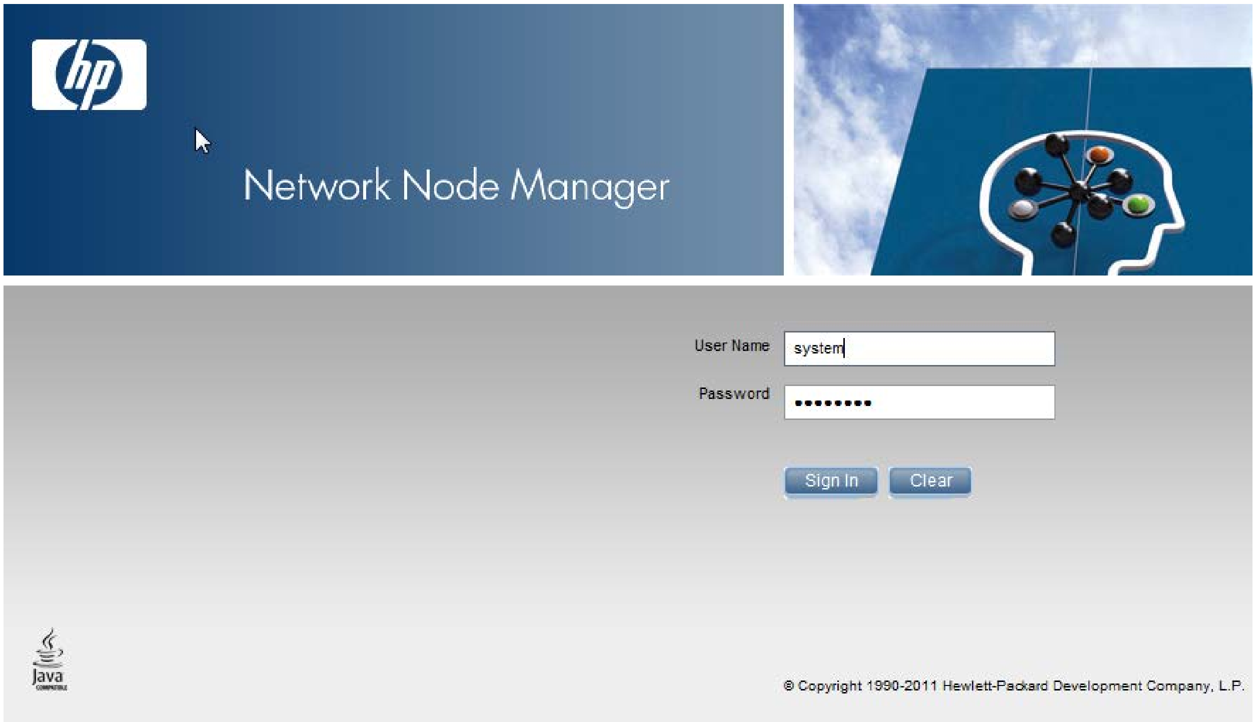
Sign in to NNMi and Create Users

Initial Sign In

Access NNMi using a browser such as Internet Explorer or Mozilla Firefox. Use a URL similar to the following, inserting your server name and the port you selected for communication during the installation process:

```
http://<serverName>:<port number>/nnm
```

Figure 1: NNMi Sign In Screen



User Name: system

Password: ●●●●●●●●●

© Copyright 1990-2011 Hewlett-Packard Development Company, L.P.

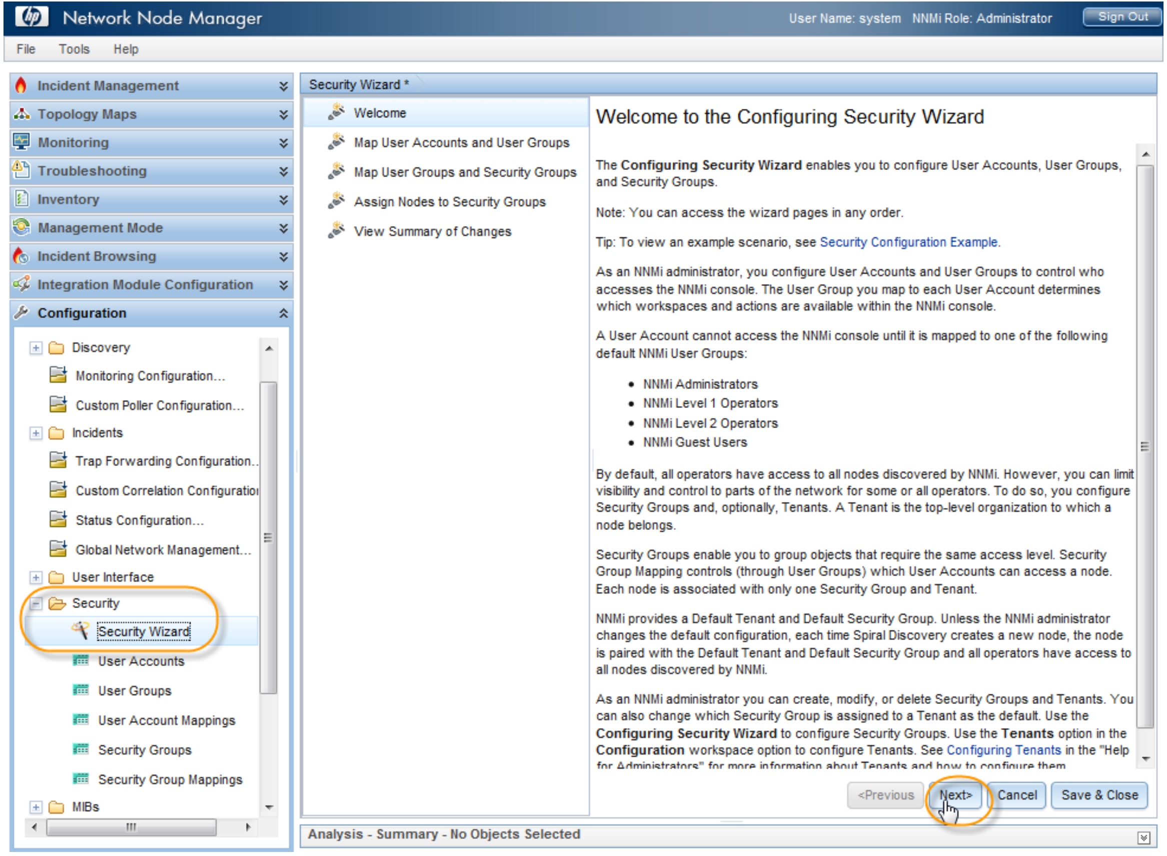
Create User Accounts and Roles

Do not use the `system` user name in most cases. Create and use an administrator account for most of your work, following these instructions:

1. From the workspace navigation panel, select the **Configuration** workspace.
2. Expand the **Security** folder.
3. Click **Security Wizard**, and then click **Next**.

You should see the Security Wizard Welcome Page.

Figure 2: Security Wizard: Welcome Page



Welcome to the Configuring Security Wizard

The **Configuring Security Wizard** enables you to configure User Accounts, User Groups, and Security Groups.

Note: You can access the wizard pages in any order.

Tip: To view an example scenario, see Security Configuration Example.

As an NNMi administrator, you configure User Accounts and User Groups to control who accesses the NNMi console. The User Group you map to each User Account determines which workspaces and actions are available within the NNMi console.

A User Account cannot access the NNMi console until it is mapped to one of the following default NNMi User Groups:

- NNMi Administrators
- NNMi Level 1 Operators
- NNMi Level 2 Operators
- NNMi Guest Users

By default, all operators have access to all nodes discovered by NNMi. However, you can limit visibility and control to parts of the network for some or all operators. To do so, you configure Security Groups and, optionally, Tenants. A Tenant is the top-level organization to which a node belongs.

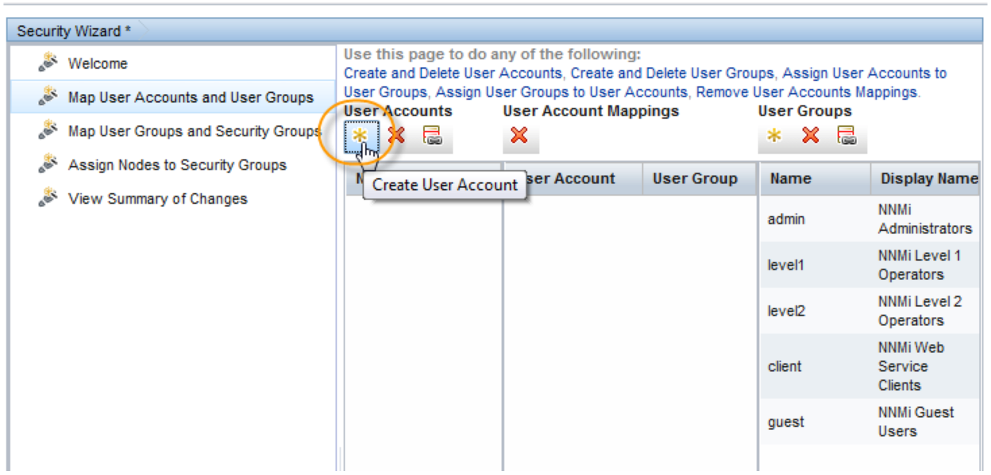
Security Groups enable you to group objects that require the same access level. Security Group Mapping controls (through User Groups) which User Accounts can access a node. Each node is associated with only one Security Group and Tenant.

NNMi provides a Default Tenant and Default Security Group. Unless the NNMi administrator changes the default configuration, each time Spiral Discovery creates a new node, the node is paired with the Default Tenant and Default Security Group and all operators have access to all nodes discovered by NNMi.

As an NNMi administrator you can create, modify, or delete Security Groups and Tenants. You can also change which Security Group is assigned to a Tenant as the default. Use the **Configuring Security Wizard** to configure Security Groups. Use the **Tenants** option in the **Configuration** workspace option to configure Tenants. See Configuring Tenants in the "Help for Administrators" for more information about Tenants and how to configure them.

4. Navigate to **User Accounts** and click the ✳ icon.

Figure 3: Security Wizard: Create User Account

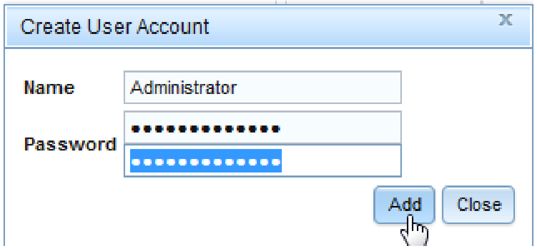


Use this page to do any of the following:
Create and Delete User Accounts, Create and Delete User Groups, Assign User Accounts to User Groups, Assign User Groups to User Accounts, Remove User Accounts Mappings.

Name	Display Name
admin	NNMi Administrators
level1	NNMi Level 1 Operators
level2	NNMi Level 2 Operators
client	NNMi Web Service Clients
guest	NNMi Guest Users

5. In the Create User Account dialog box, enter the account information, click **Add**, and then click **Close**.

Figure 4: Security Wizard: Create User Account Dialog Box



Create User Account

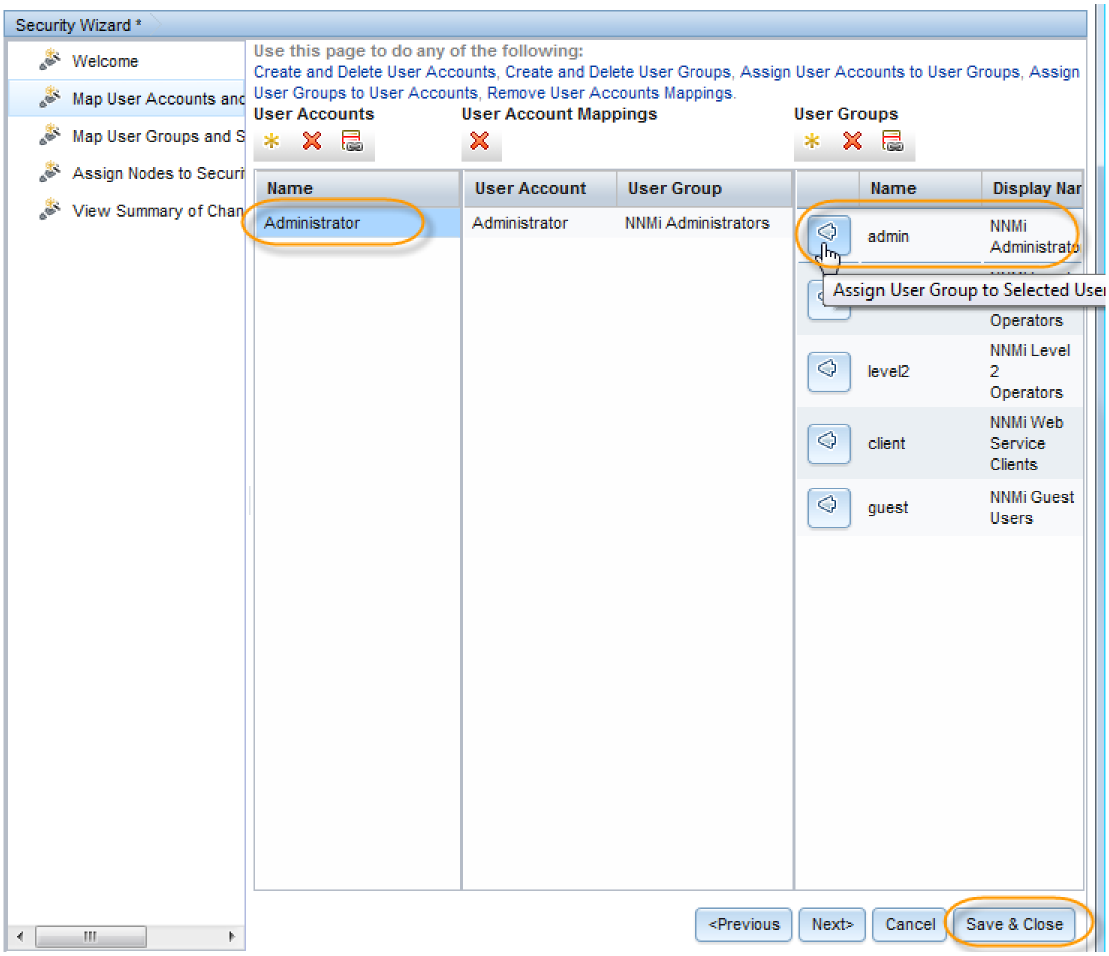
Name: Administrator

Password: ••••••••••••••
••••••••••••••

6. Click the new account name in the **User Accounts** column, and then click the ◁ icon next to the appropriate User Group to create the User Account Mapping.
7. Click 💾 **Save and Close**, and then click **OK > OK** to accept the changes.

Tip: User Account Mappings replace the "Role" concept in previous versions of NNMi.

Figure 5: Security Wizard: Assign User Group to User Account



Security Wizard *

Use this page to do any of the following:
Create and Delete User Accounts, Create and Delete User Groups, Assign User Accounts to User Groups, Assign User Groups to User Accounts, Remove User Accounts Mappings.

User Accounts

Name
Administrator

User Account Mappings

User Account	User Group
Administrator	NNMi Administrators

User Groups

	Name	Display Nar
◁	admin	NNMi Administrato
◁		Operators
◁	level2	NNMi Level 2 Operators
◁	client	NNMi Web Service Clients
◁	guest	NNMi Guest Users

Assign User Group to Selected User

8. Sign out of NNMi and sign in with the new User Account Name to make sure it works correctly.

Set up Communication Configuration

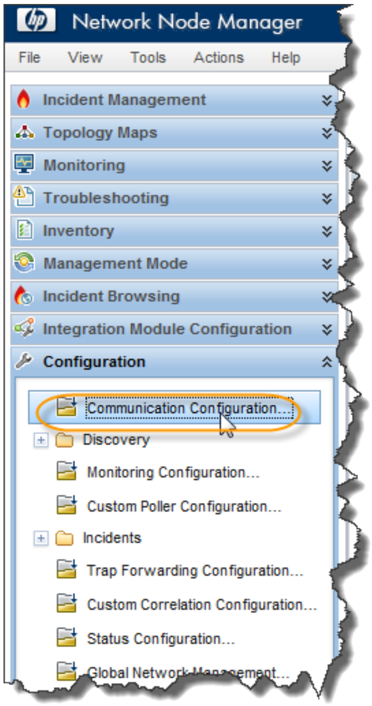
By default, NNMi performs *SNMP community string discovery*. This example describes how to use this default method.

Tip: Unlike previous versions of NNMi, you do not configure a prioritized list of SNMP community strings.

By default, NNMi tries all possible community strings sequentially. NNMi selects the first community string that results in a response from a node as the SNMP community string for that node. In this example, configure only the default community strings. You can implement more complex solutions with this configuration, but in most cases, this is an adequate approach.

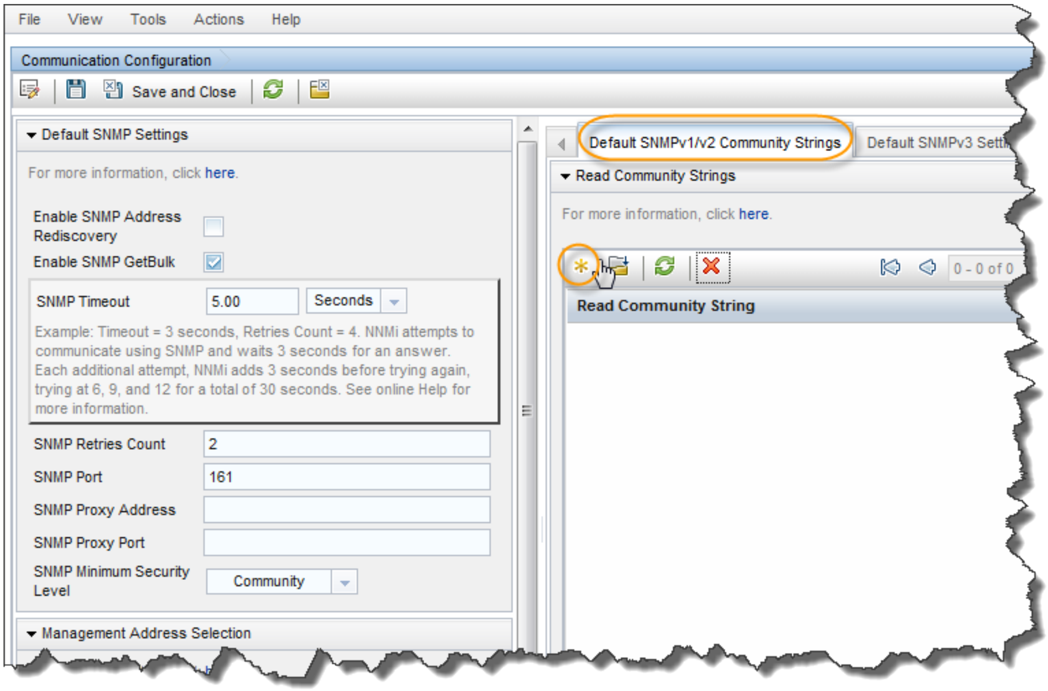
1. From the workspace navigation panel, select the **Configuration** workspace, and then click **Communication Configuration**.

Figure 6: Communication Configuration


Network Node Manager
File
View
Tools
Actions
Help
Incident Management
Topology Maps
Monitoring
Troubleshooting
Inventory
Management Mode
Incident Browsing
Integration Module Configuration
Configuration
Communication Configuration...
Discovery
Monitoring Configuration...
Custom Poller Configuration...
Incidents
Trap Forwarding Configuration...
Custom Correlation Configuration...
Status Configuration...
Global Network Management...

2. Click the **Default SNMPv1/v2 Community Strings** tab, and then click the ✳ icon to create a new community string.

Figure 7: Communication Configuration: Default SNMPv1/v2 Community Strings Tab


File
View
Tools
Actions
Help
Communication Configuration
Save and Close
Default SNMP Settings
For more information, click here.
Management Address Selection
Default SNMPv1/v2 Community Strings
Default SNMPv3 Setti
Read Community Strings
For more information, click here.
0 - 0 of 0
Read Community String

Enable SNMP Address Rediscovery □

Enable SNMP GetBulk ☑

SNMP Timeout 5.00 Seconds

Example: Timeout = 3 seconds, Retries Count = 4. NNMi attempts to communicate using SNMP and waits 3 seconds for an answer. Each additional attempt, NNMi adds 3 seconds before trying again, trying at 6, 9, and 12 for a total of 30 seconds. See online Help for more information.

SNMP Retries Count 2

SNMP Port 161

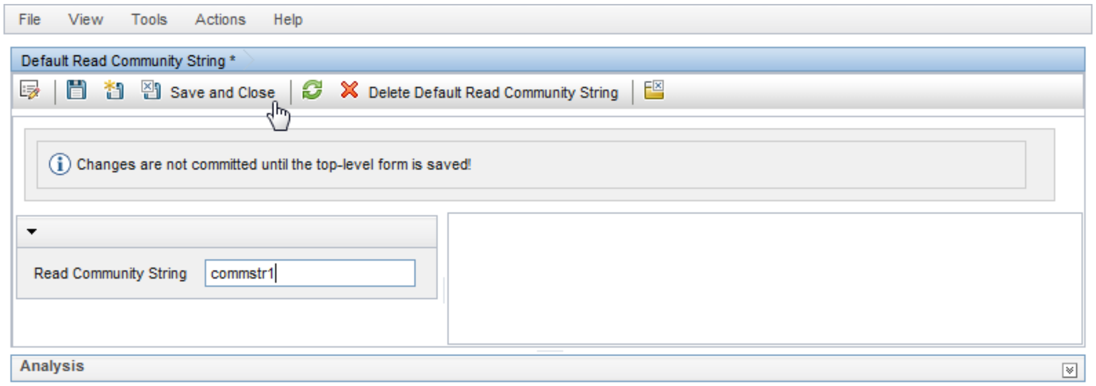
SNMP Proxy Address

SNMP Proxy Port

SNMP Minimum Security Level Community

3. Enter your community string, and then click **Save and Close**.

Figure 8: Default Read Community String


File
View
Tools
Actions
Help
Default Read Community String *
Save and Close
Delete Default Read Community String
Analysis

Changes are not committed until the top-level form is saved!

Read Community String commstr1

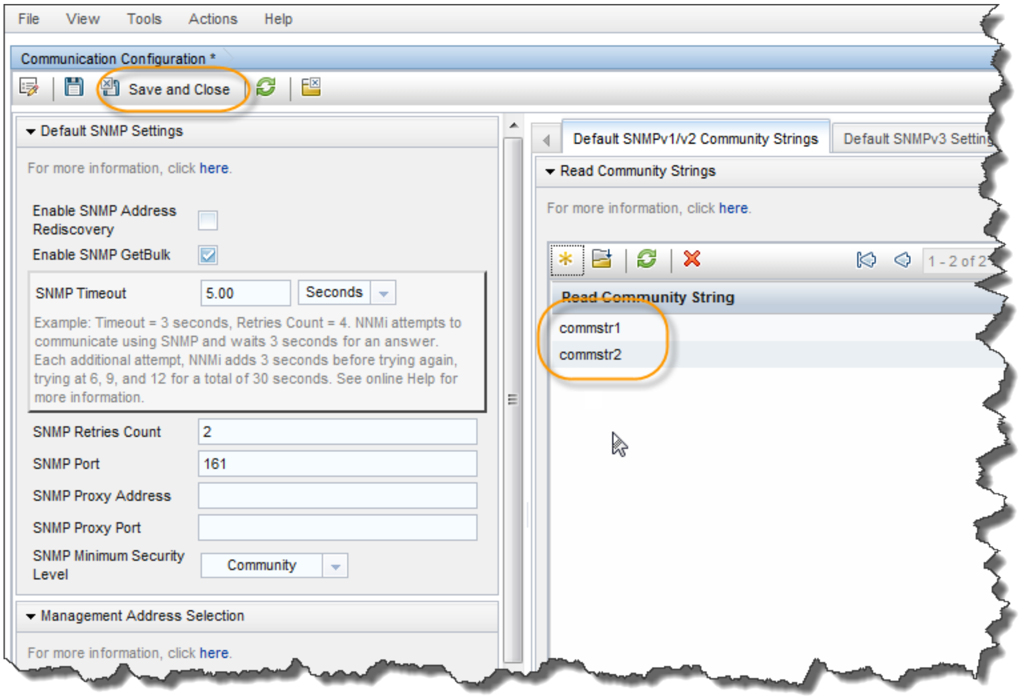
4. Repeat the previous steps for all your community strings.

Tip: Explore the other Communication configuration options in case you want to make additional changes.

5. When you finish configuring your community strings, click **Save and Close** in the **Communication Configuration** form to save your changes.

Your SNMP configuration is complete.

Figure 9: Communication Configuration: Save and Close



Default SNMP Settings

For more information, click here.

Enable SNMP Address Rediscovery □

Enable SNMP GetBulk ☑

SNMP Timeout 5.00 Seconds

Example: Timeout = 3 seconds, Retries Count = 4. NNMi attempts to communicate using SNMP and waits 3 seconds for an answer. Each additional attempt, NNMi adds 3 seconds before trying again, trying at 6, 9, and 12 for a total of 30 seconds. See online Help for more information.

SNMP Retries Count 2

SNMP Port 161

SNMP Proxy Address

SNMP Proxy Port

SNMP Minimum Security Level Community

Management Address Selection

For more information, click here.

Read Community Strings

For more information, click here.

Read Community String
commstr1
commstr2

Configure Discovery

NNMi supports two methods of discovery: *list-based and automatic*. Each method offers advantages.

List-based discovery uses a list of node names or addresses as input and only discovers the nodes contained in that list. NNMi discovers no additional node names or addresses beyond those contained in this list. This method gives you control over what is discovered and managed by NNMi. Each node in the list is known as a seed.

Note: NNMi loads each seed even if its IP address is outside of the Auto-Discovery range.

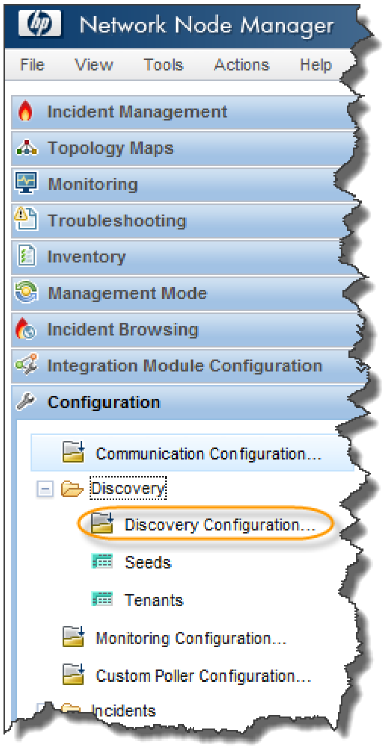
Tip: If you load a seed as an IP address for a device, it is a good practice to specify the preferred management address (usually the loopback address with Cisco gear) as the seed.

Automatic discovery finds nodes on the network based on user-specified criteria. You can configure NNMi to restrict discovered nodes based by address range, SNMP values (such as system object ID), device type, and other methods. You can configure automatic discovery with a single seed node; although even this node is not required if you enable the optional *ping- sweep* feature.

The following example describes an automatic discovery based on an address range. Additionally, this example shows you how to load a couple of seed nodes.

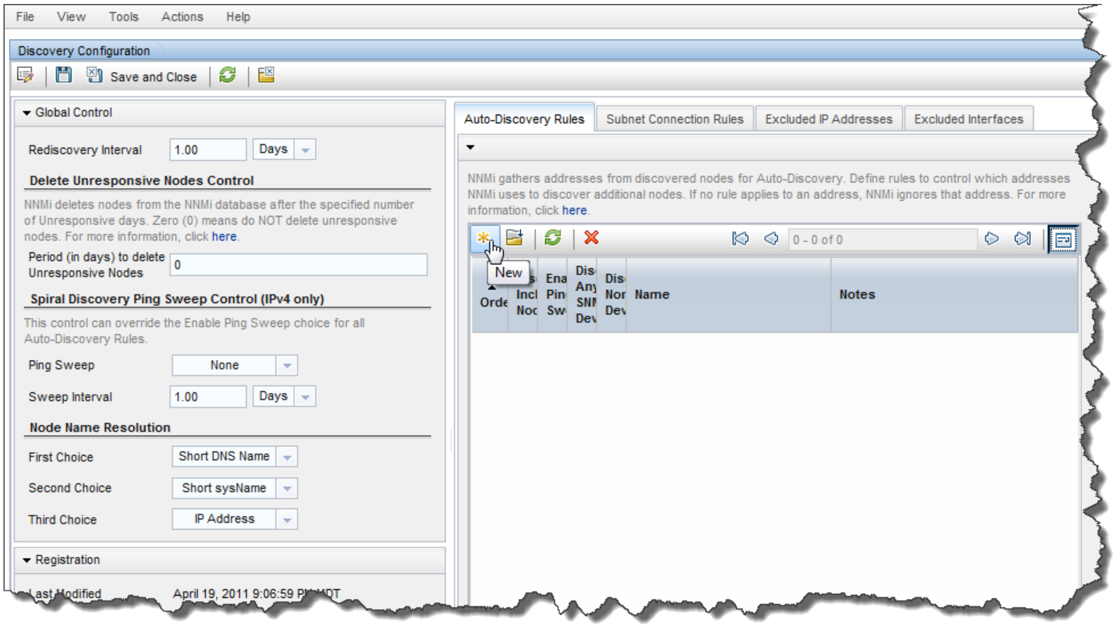
1. From the workspace navigation panel, select the **Configuration** workspace, expand the **Discovery** folder, and then click **Discovery Configuration**.

Figure 10: Discovery Configuration


Network Node Manager
File View Tools Actions Help
Incident Management
Topology Maps
Monitoring
Troubleshooting
Inventory
Management Mode
Incident Browsing
Integration Module Configuration
Configuration
Communication Configuration...
Discovery
Discovery Configuration...
Seeds
Tenants
Monitoring Configuration...
Custom Poller Configuration...
Incidents

2. Click the **Auto-Discovery Rules** tab, and then click the ✳ icon to create a new rule.

Figure 11: Discovery Configuration: Auto-Discovery Rules



Rediscovery Interval 1.00 Days

Delete Unresponsive Nodes Control

NNMi deletes nodes from the NNMi database after the specified number of Unresponsive days. Zero (0) means do NOT delete unresponsive nodes. For more information, click here.

Period (in days) to delete Unresponsive Nodes 0

Spiral Discovery Ping Sweep Control (IPv4 only)

This control can override the Enable Ping Sweep choice for all Auto-Discovery Rules.

Ping Sweep None

Sweep Interval 1.00 Days

Node Name Resolution

First Choice Short DNS Name

Second Choice Short sysName

Third Choice IP Address

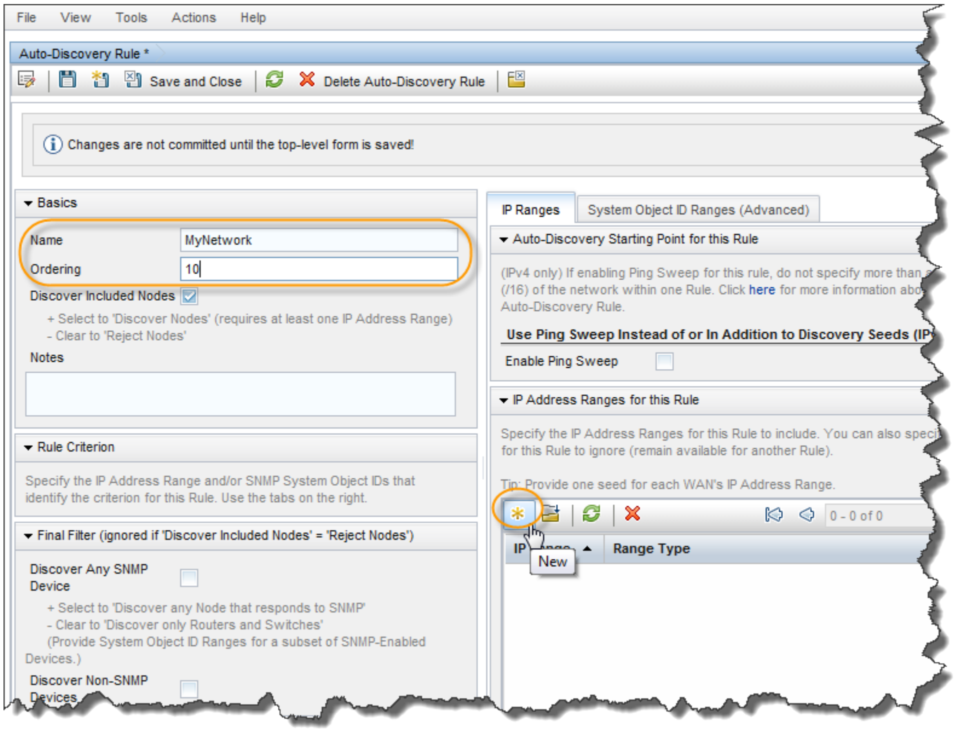
Last Modified April 19, 2011 9:06:59 PM MDT

NNMi gathers addresses from discovered nodes for Auto-Discovery. Define rules to control which addresses NNMi uses to discover additional nodes. If no rule applies to an address, NNMi ignores that address. For more information, click here.

3. Fill out the Basics section

Tip: NNMi uses the **Ordering** attribute value to prioritize multiple Auto-Discovery Rules. This example uses only one Auto-Discovery Rule.

Figure 12: Auto-Discovery Rule: Ordering Attribute


File
View
Tools
Actions
Help
Auto-Discovery Rule *
Save and Close
Delete Auto-Discovery Rule
Basics
IP Ranges
System Object ID Ranges (Advanced)
Auto-Discovery Starting Point for this Rule
Rule Criterion
IP Address Ranges for this Rule
New
IP Range
Range Type
0 - 0 of 0

Changes are not committed until the top-level form is saved!

Name: MyNetwork

Ordering: 10

Discover Included Nodes ☑

+ Select to 'Discover Nodes' (requires at least one IP Address Range)
- Clear to 'Reject Nodes'

Notes

Specify the IP Address Range and/or SNMP System Object IDs that identify the criterion for this Rule. Use the tabs on the right.

Final Filter (ignored if 'Discover Included Nodes' = 'Reject Nodes')

Discover Any SNMP Device □

+ Select to 'Discover any Node that responds to SNMP'
- Clear to 'Discover only Routers and Switches'
(Provide System Object ID Ranges for a subset of SNMP-Enabled Devices.)

Discover Non-SNMP Devices □

(IPv4 only) If enabling Ping Sweep for this rule, do not specify more than (/16) of the network within one Rule. Click here for more information abo Auto-Discovery Rule.

Use Ping Sweep Instead of or In Addition to Discovery Seeds (IP

Enable Ping Sweep □

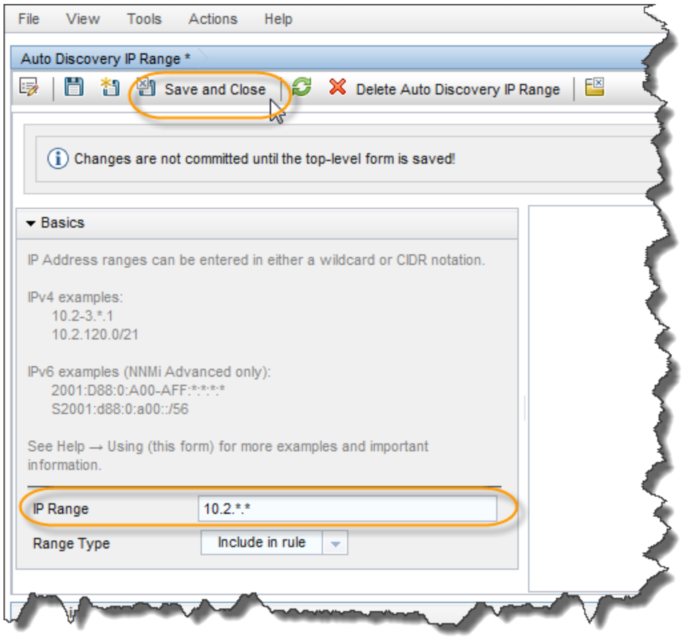
Specify the IP Address Ranges for this Rule to include. You can also speci for this Rule to ignore (remain available for another Rule).

Tip: Provide one seed for each WAN's IP Address Range.

4. Click the ✳ icon to open an entry screen for the IP Range in this rule.

5. In the **IP Range** text box, enter the IP range you want to discover. Notice that you can enter both inclusive rules (`Include in rule`) and exclusive rules (`Ignored by rule`). The exclusive rules take priority over the inclusive rules.

Figure 13: Auto-Discovery IP Range



Changes are not committed until the top-level form is saved!

IP Address ranges can be entered in either a wildcard or CIDR notation.

IPv4 examples:
10.2-3.*.1
10.2.120.0/21

IPv6 examples (NNMi Advanced only):
2001:D88:0:A00-AFF:*:*:*:*
S2001:d88:0:a00::/56

See Help → Using (this form) for more examples and important information.

IP Range: 10.2.*.*

Range Type: Include in rule

6. Click **Save and Close** on this form as well as on the Auto-Discovery Rule form to save your changes.

This example does not use the ping-sweep feature.

Tip: If you choose to use the ping-sweep feature in your environment, NNMi sweeps across a maximum of a class B network (for example, 10.2.*.*) for each Auto-Discovery Rule.

Note the following:

- By default, NNMi discovers only routers and switches within the defined IP address range. To discover nodes beyond switches and routers, add system object ID ranges that include your other devices.
- If a node has multiple addresses, such as a router, then only one of the addresses must fall within the IP range. This address does not need to be the loopback address. NNMi might discover more nodes than you initially expect if you enter addresses other than the loopback addresses.

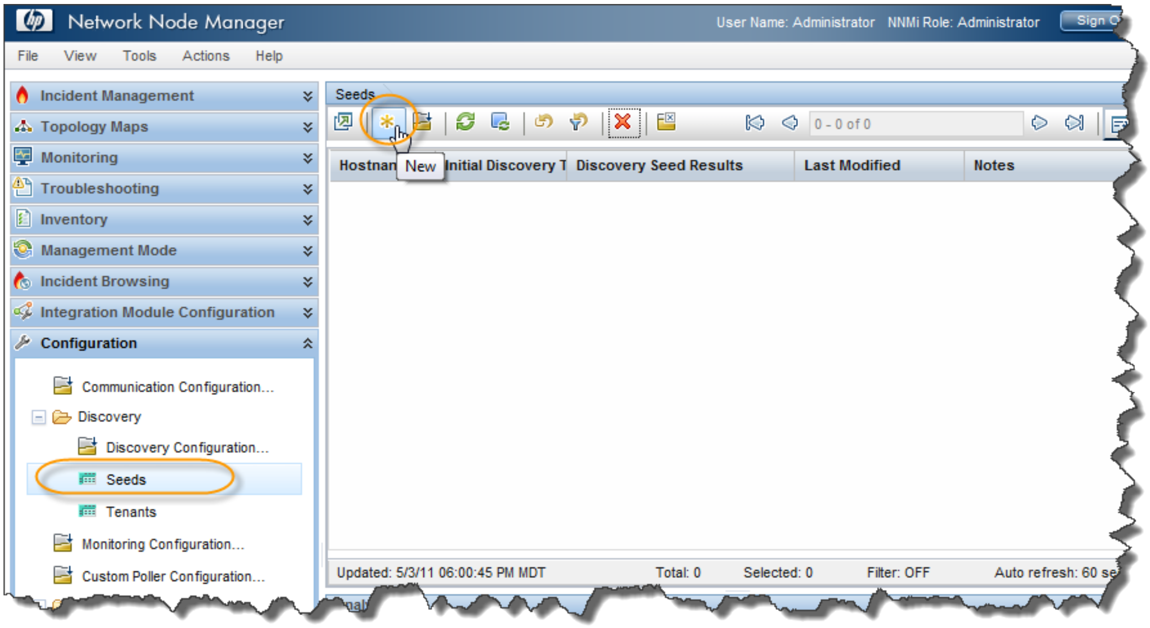
You now have one Auto-Discovery Rule defined. In most cases you only need one Auto-Discovery Rule since each rule can be quite complex.

Next, this example explains how to add a seed node.

Tip: It is better to add a router as a seed rather than a switch because routers provide a larger set of addresses for NNMi discovery.

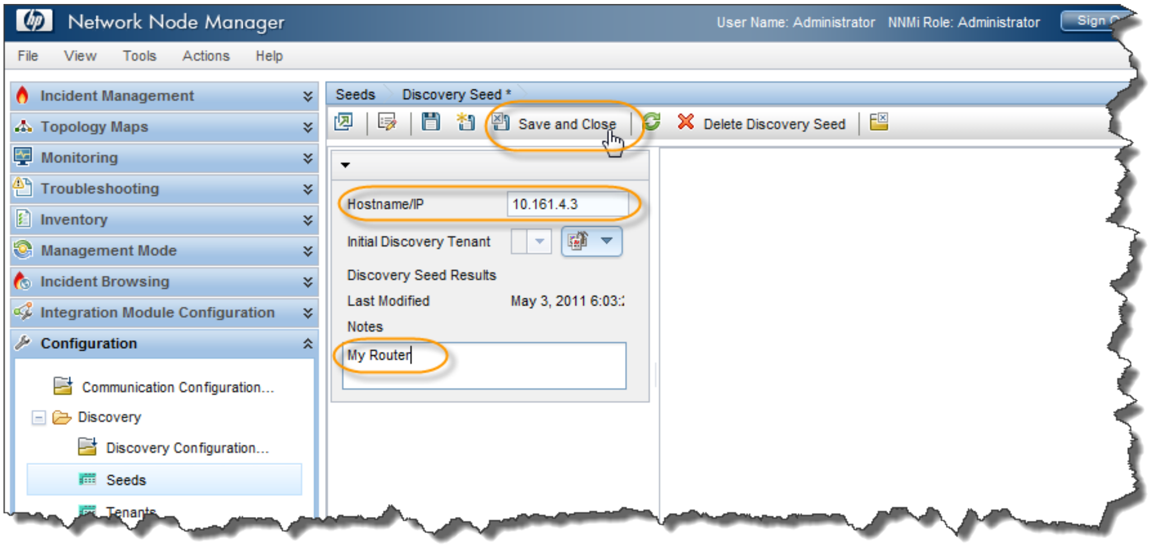
1. From the workspace navigation panel, select the **Configuration** workspace, expand the **Discovery** folder, and then click **Seeds**.
2. Click the ✳ icon to create a new seed.

Figure 14: Discovery: Seeds



3. In the **Discovery Seed** form, enter the hostname or IP address and any Notes, as desired, and then click **Save and Close**.

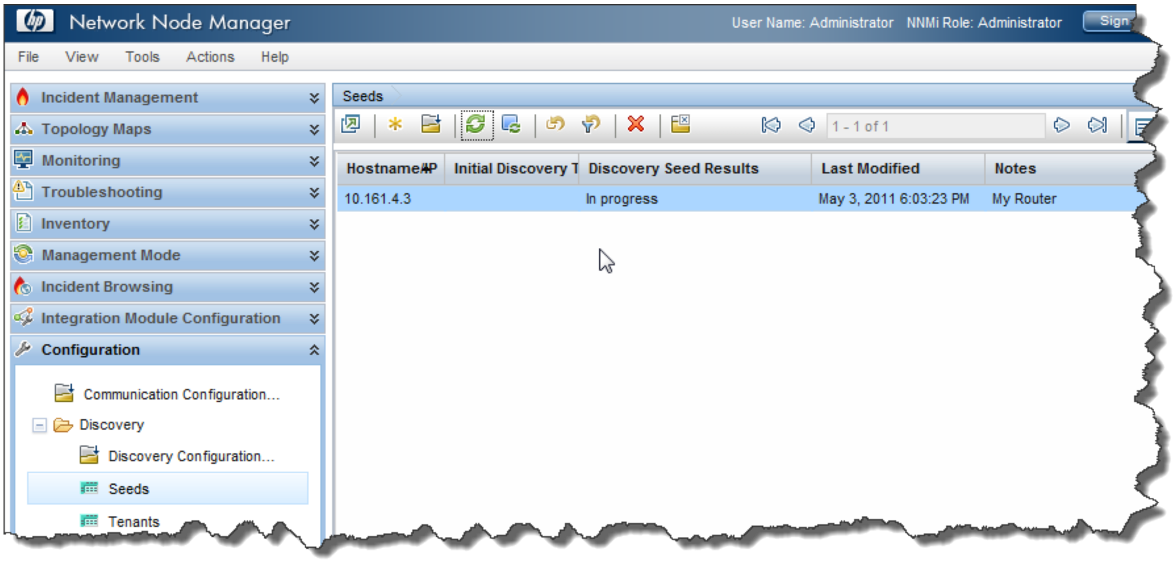
Figure 15: Seeds: Discovery Seed



Hostname/IP	10.161.4.3
Initial Discovery Tenant	
Discovery Seed Results	
Last Modified	May 3, 2011 6:03::
Notes	My Router

Tip: Examine the Discovery Seed Results column in the Seeds table to determine the discovery status of each seed. As NNMi begins discovering the node, NNMi displays the progress as `In progress`. When the discovery completes, the Discovery Seed Results entry changes to `Node Created`.

Figure 16: Seeds: Discovery Seed Results



Hostname/IP	Initial Discovery T	Discovery Seed Results	Last Modified	Notes
10.161.4.3		In progress	May 3, 2011 6:03:23 PM	My Router

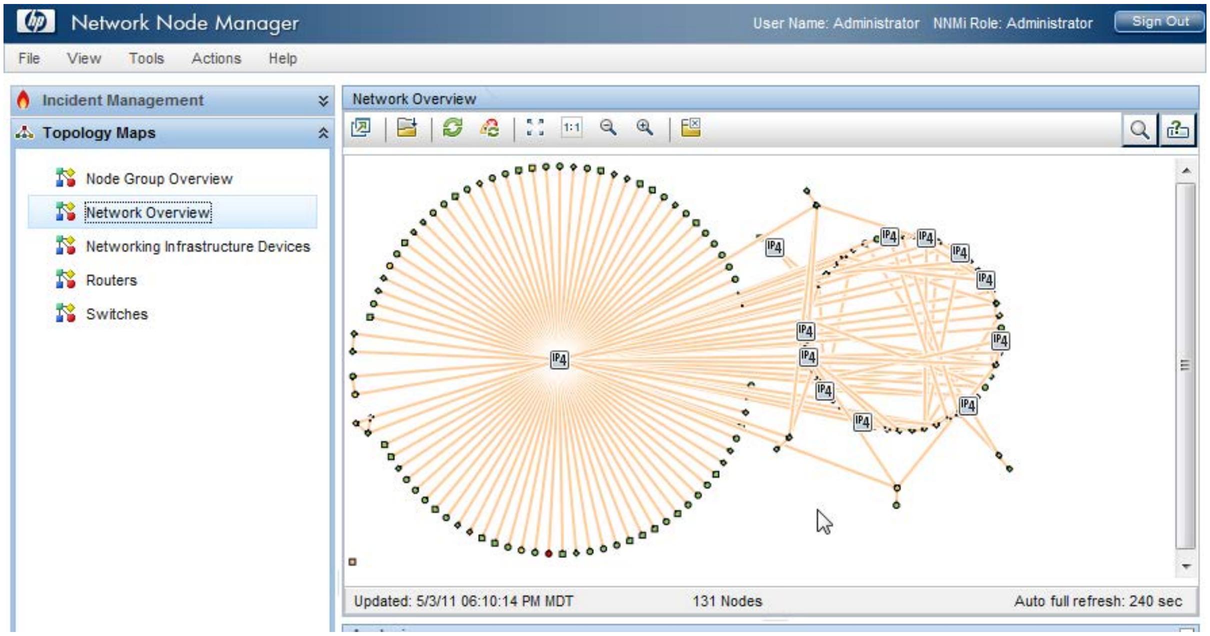
Tip: You can also load a list of seeds from a file using the `nnmloadseeds.ovpl` script. This script enables you to load a large number of seed nodes. If you use list-based discovery rather than Auto-Discovery Rules, you can load all of your nodes using the `nnmloadseeds.ovpl` script. See the `nnmloadseeds.ovpl` reference page or the UNIX manpage for more information.

When you use the Auto-Discovery method, Auto Discovery begins finding other switches and routers that have addresses within the address range specified in your Auto-Discovery Rule. Initially NNMi shows nodes without displaying status. Eventually NNMi shows a status for each discovered node.

The **Network Overview** map is useful to display discovery progress in smaller environments because the **Network Overview** map displays a limited number of nodes and connections.

Tip: Click **Refresh** on the **Network Overview** map to display the initial nodes.

Figure 17: Topology Maps: Network Overview


Network Node Manager
User Name: Administrator NNMi Role: Administrator
Sign Out
File View Tools Actions Help
Incident Management
Topology Maps
Node Group Overview
Network Overview
Networking Infrastructure Devices
Routers
Switches
Network Overview
IP4
Updated: 5/3/11 06:10:14 PM MDT
131 Nodes
Auto full refresh: 240 sec

Configure Monitoring

Monitoring in NNMi is flexible and easy to configure. By default, NNMi uses SNMP polling rather than ICMP (ping) polling. The exception to this is non-SNMP nodes—NNMi polls these nodes using ICMP. You can enable ICMP polling more broadly if desired.

By default, NNMi polls *connected* interfaces. A connected interface in NNMi is an interface that is connected in the NNMi topology, which does not always include mapping to interfaces that have a wire connected.

Consider the following scenario:

- An access switch with 48 ports is connected to desktop computers and one uplink port.
- NNMi discovered the uplink node, but has not discovered any of the desktop computers.

In this case, only the uplink port will be considered *connected* to NNMi because it does not have a representation of the connection to the desktop computers. In most cases, this is the desired behavior. Usually, you will not want NNMi to notify you every time a computer is turned off for the evening.

In the following example, the `c2900xl-1` switch is an access switch with one uplink (`Fa0/2`). As shown in Figure 19: Node Form: List of Interfaces, only one interface is monitored.

Figure 18: Map View: One Interface Monitored

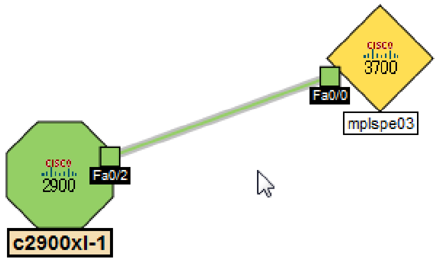
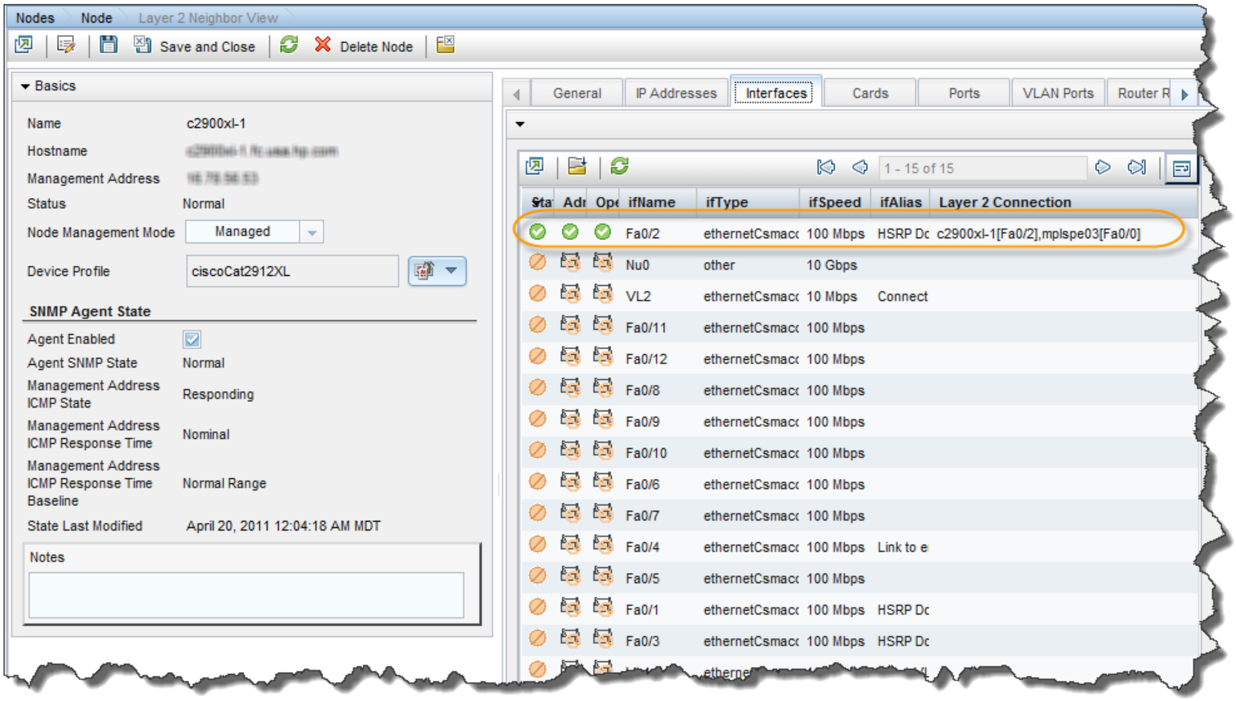


Figure 19: Node Form: List of Interfaces



Basics

Name	c2900xl-1
Hostname	[redacted]
Management Address	[redacted]
Status	Normal
Node Management Mode	Managed
Device Profile	ciscoCat2912XL

SNMP Agent State

Agent Enabled	☑
Agent SNMP State	Normal
Management Address ICMP State	Responding
Management Address ICMP Response Time	Nominal
Management Address ICMP Response Time Baseline	Normal Range
State Last Modified	April 20, 2011 12:04:18 AM MDT

Notes

Sta	Adı	Ope	ifName	ifType	ifSpeed	ifAlias	Layer 2 Connection
✓	✓	✓	Fa0/2	ethernetCsmacc	100 Mbps	HSRP Dc	c2900xl-1[Fa0/2],mplspe03[Fa0/0]
⊘			Nu0	other	10 Gbps		
⊘			VL2	ethernetCsmacc	10 Mbps	Connect	
⊘			Fa0/11	ethernetCsmacc	100 Mbps		
⊘			Fa0/12	ethernetCsmacc	100 Mbps		
⊘			Fa0/8	ethernetCsmacc	100 Mbps		
⊘			Fa0/9	ethernetCsmacc	100 Mbps		
⊘			Fa0/10	ethernetCsmacc	100 Mbps		
⊘			Fa0/6	ethernetCsmacc	100 Mbps		
⊘			Fa0/7	ethernetCsmacc	100 Mbps		
⊘			Fa0/4	ethernetCsmacc	100 Mbps	Link to e	
⊘			Fa0/5	ethernetCsmacc	100 Mbps		
⊘			Fa0/1	ethernetCsmacc	100 Mbps	HSRP Dc	
⊘			Fa0/3	ethernetCsmacc	100 Mbps	HSRP Dc	
⊘				etherne			

The second default behavior applies to routers. For routers, NNMi monitors most interfaces that host IP addresses. NNMi assumes that if an administrator takes the time to configure an IP address on an interface, it is desirable to monitor that interface. In some cases, NNMi models these interfaces as being connected; however, in other cases, NNMi models these interfaces as being unconnected. An example of this is a router that has an interface that connects to a WAN cloud. NNMi might not discover and model the connection to the cloud, but NNMi monitors the router interface by default.

When modifying this default behavior, note the following:

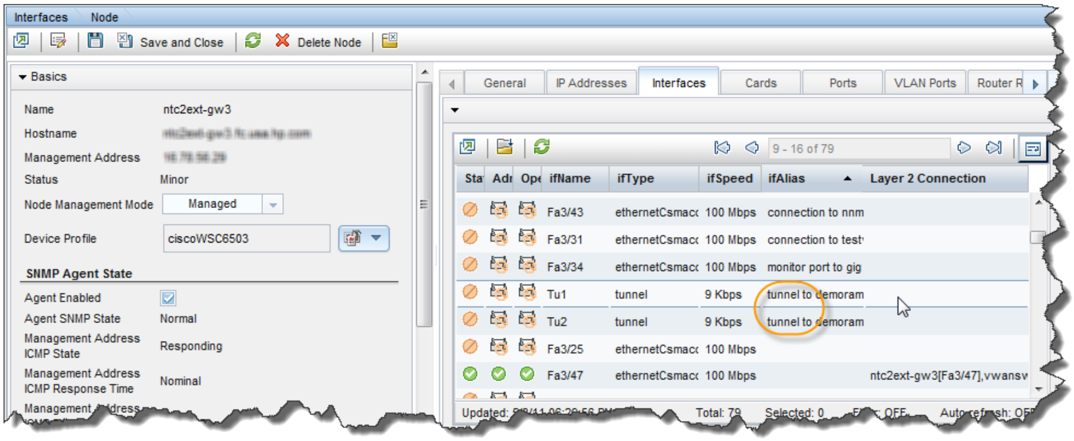
- NNMi enables you to modify monitoring settings in high volume.
- NNMi does this by using filters to apply monitoring to individual nodes, interfaces, and addresses. These filters are the same filters available for the user interface.
- Although this document focuses on nodes and interfaces, NNMi monitors additional entities such as Fans, and HSRP groups.

Consider the following scenario:

- Interfaces on a subset of nodes have an `IfAlias` that begins with `tunnel to`.
- You determine that NNMi needs to monitor these interfaces if their speed is 9 Kbs.

Using NNMi you can create a filter to identify any interfaces that match these criteria. After creating this filter, you apply monitoring settings to these interfaces.

Figure 20: Node Form: Apply Monitoring Settings



Name	ntc2ext-gw3
Hostname	[redacted]
Management Address	[redacted]
Status	Minor
Node Management Mode	Managed
Device Profile	ciscoWSC6503

SNMP Agent State

Agent Enabled	☑
Agent SNMP State	Normal
Management Address ICMP State	Responding
Management Address ICMP Response Time	Nominal
Management Address	

Sta	Adı	Opı	ifName	ifType	ifSpeed	ifAlias	Layer 2 Connection
⊘			Fa3/43	ethernetCsmacc	100 Mbps	connection to nnm	
⊘			Fa3/31	ethernetCsmacc	100 Mbps	connection to test	
⊘			Fa3/34	ethernetCsmacc	100 Mbps	monitor port to gig	
⊘			Tu1	tunnel	9 Kbps	tunnel to demoram	
⊘			Tu2	tunnel	9 Kbps	tunnel to demoram	
⊘			Fa3/25	ethernetCsmacc	100 Mbps		
✓	✓	✓	Fa3/47	ethernetCsmacc	100 Mbps		ntc2ext-gw3[Fa3/47],vwansv

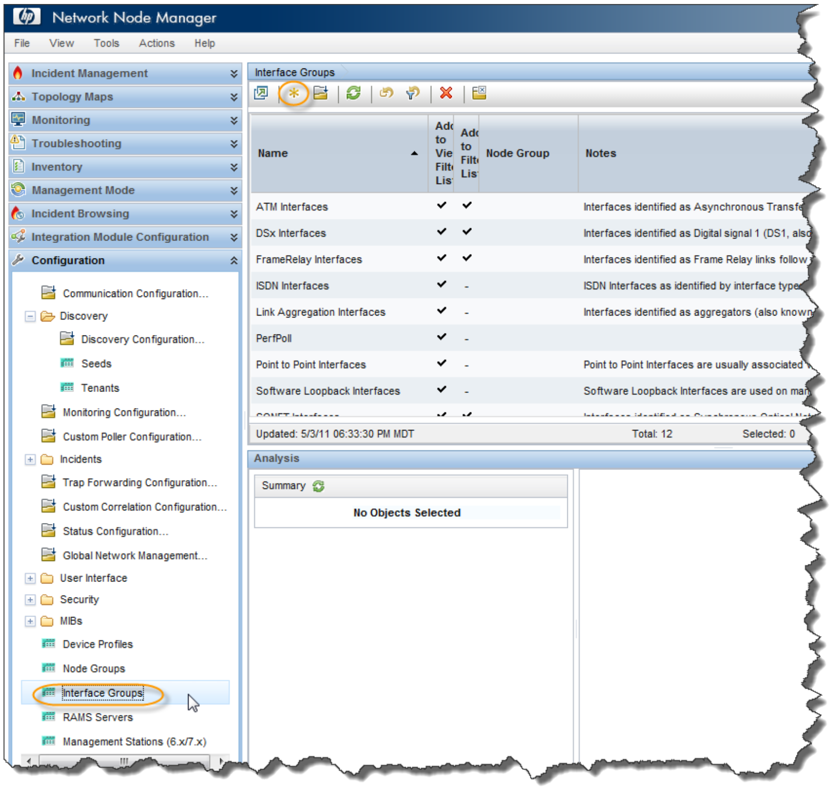
Updated: 9/9/11 06:29:56 PM Total: 79 Selected: 0 Filter: OFF Auto-refresh: OFF

Create an Interface Group for Monitoring

NNMi enables you to create groups of nodes and interfaces. To create an Interface Group, follow these steps:

1. From the workspace navigation panel, select the **Configuration** workspace, and then click **Interface Groups**.

Figure 21: Configuration: Interface Groups


Network Node Manager
File View Tools Actions Help
Incident Management
Topology Maps
Monitoring
Troubleshooting
Inventory
Management Mode
Incident Browsing
Integration Module Configuration
Configuration
Communication Configuration...
Discovery
Discovery Configuration...
Seeds
Tenants
Monitoring Configuration...
Custom Poller Configuration...
Incidents
Trap Forwarding Configuration...
Custom Correlation Configuration...
Status Configuration...
Global Network Management...
User Interface
Security
MIBs
Device Profiles
Node Groups
Interface Groups
RAMS Servers
Management Stations (6.x/7.x)
Interface Groups
Analysis
Summary

Name	Add to View Filter List	Add to Filter List	Node Group	Notes
ATM Interfaces	✓	✓		Interfaces identified as Asynchronous Transfe
DSx Interfaces	✓	✓		Interfaces identified as Digital signal 1 (DS1, also
FrameRelay Interfaces	✓	✓		Interfaces identified as Frame Relay links follow
ISDN Interfaces	✓	-		ISDN Interfaces as identified by interface type
Link Aggregation Interfaces	✓	-		Interfaces identified as aggregators (also known
PerfPoll	✓	-		
Point to Point Interfaces	✓	-		Point to Point Interfaces are usually associated
Software Loopback Interfaces	✓	-		Software Loopback Interfaces are used on man

Updated: 5/3/11 06:33:30 PM MDT Total: 12 Selected: 0

No Objects Selected

2. Click the ✱ icon to create a new Interface Group.

3. Enter **`Important 9kbs Tunnels`**, or some other descriptive name, in the **Name** text box.

Tip: Do not restrict this Interface Group to a specific Node Group; although often, you will do so.

4. Click the **Additional Filters** tab to access the **Filter Editor** used to define the filter logic.

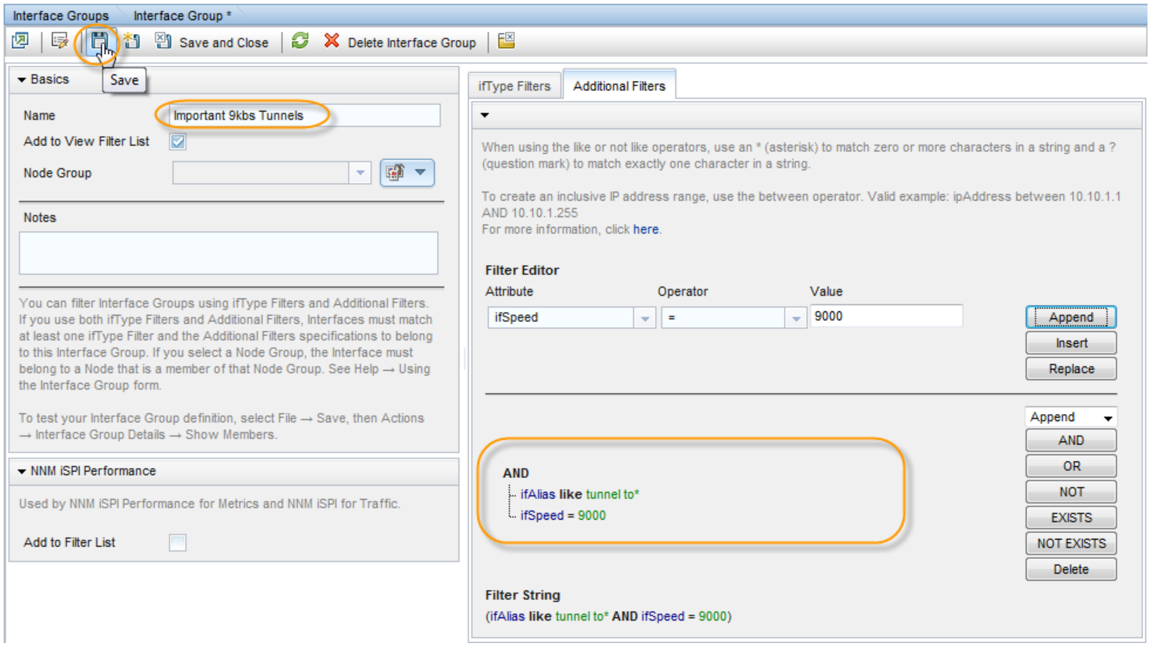
You define a filter expression by selecting an `Attribute`, an `Operator` and a `value`. You can use the `like` operator along with an asterisk for variable matching.

In this example, use an AND condition for the two attributes.

Tip: If you encounter problems when defining your logic, close the form without saving it to return to the last saved value. Then re-open the form and begin again.

Note: If you define an IfType filter (on the **IfType Filters** tab), then it is always logically AND'ed with the filters on the **Additional Filters** tab.

Figure 22: Interface Groups: Save



Name: Important 9kbs Tunnels

Add to View Filter List: ☑

Node Group:

Notes

You can filter Interface Groups using ifType Filters and Additional Filters. If you use both ifType Filters and Additional Filters, Interfaces must match at least one ifType Filter and the Additional Filters specifications to belong to this Interface Group. If you select a Node Group, the Interface must belong to a Node that is a member of that Node Group. See Help → Using the Interface Group form.

To test your Interface Group definition, select File → Save, then Actions → Interface Group Details → Show Members.

Used by NNM iSPI Performance for Metrics and NNM iSPI for Traffic.

Add to Filter List: □

When using the like or not like operators, use an * (asterisk) to match zero or more characters in a string and a ? (question mark) to match exactly one character in a string.

To create an inclusive IP address range, use the between operator. Valid example: ipAddress between 10.10.1.1 AND 10.10.1.255
For more information, click here.

Filter Editor

Attribute	Operator	Value
ifSpeed	=	9000

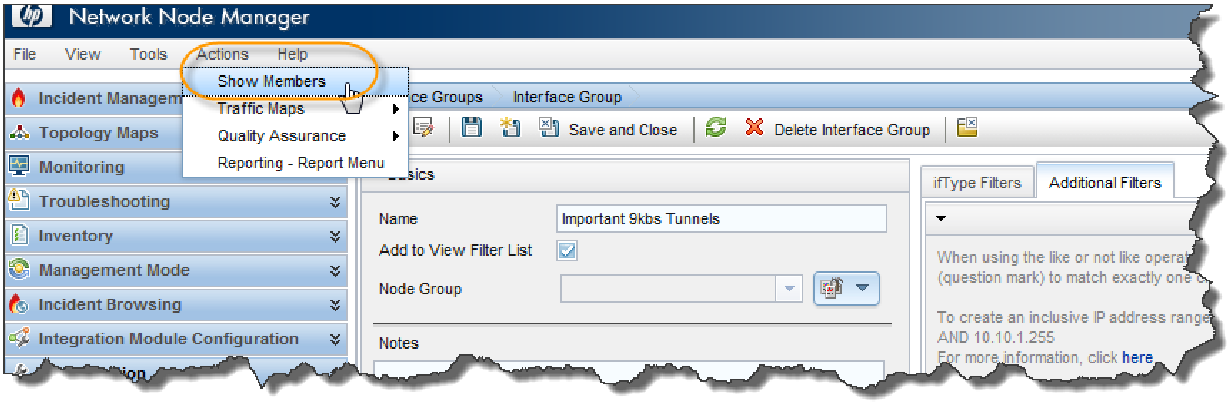
```
AND
 ifAlias like tunnel to*
 ifSpeed = 9000
```

Filter String
(ifAlias like tunnel to* AND ifSpeed = 9000)

5. After you specify your filter, save the filter, but do not close it.
6. Verify that the filter works as expected using the **Actions > Show Members** menu item.

NNMi displays all items that pass the filter criteria.

Figure 23: Actions: Show Interface Group Members



Name: Important 9kbs Tunnels

Add to View Filter List: ☑

Node Group:

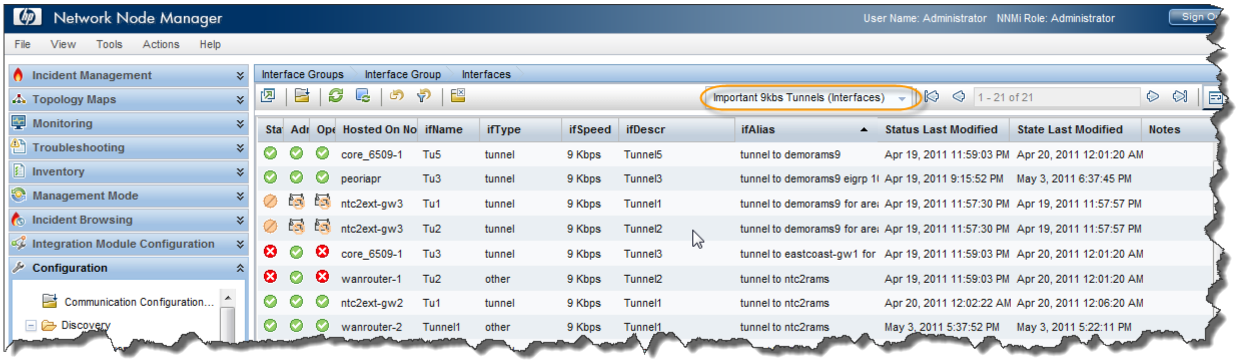
Notes

When using the like or not like opera
(question mark) to match exactly one c

To create an inclusive IP address range
AND 10.10.1.255
For more information, click here

7. Verify the results. In this example, you can see that the filter matched a number of interfaces in the network. NNMi is already monitoring some of them.

Figure 24: Interfaces: Interface Group Filter Results



Sta	Adı	Ope	Hosted On No	ifName	ifType	ifSpeed	ifDescr	ifAlias	Status Last Modified	State Last Modified	Notes
✓	✓	✓	core_6509-1	Tu5	tunnel	9 Kbps	Tunnel5	tunnel to demorams9	Apr 19, 2011 11:59:03 PM	Apr 20, 2011 12:01:20 AM	
✓	✓	✓	peoriapr	Tu3	tunnel	9 Kbps	Tunnel3	tunnel to demorams9 eigrp 1(	Apr 19, 2011 9:15:52 PM	May 3, 2011 6:37:45 PM	
⊘			ntc2ext-gw3	Tu1	tunnel	9 Kbps	Tunnel1	tunnel to demorams9 for are:	Apr 19, 2011 11:57:30 PM	Apr 19, 2011 11:57:57 PM	
⊘			ntc2ext-gw3	Tu2	tunnel	9 Kbps	Tunnel2	tunnel to demorams9 for are:	Apr 19, 2011 11:57:30 PM	Apr 19, 2011 11:57:57 PM	
✗	✓	✗	core_6509-1	Tu3	tunnel	9 Kbps	Tunnel3	tunnel to eastcoast-gw1 for	Apr 19, 2011 11:59:03 PM	Apr 20, 2011 12:01:20 AM	
✗	✓	✗	wanrouter-1	Tu2	other	9 Kbps	Tunnel2	tunnel to ntc2rams	Apr 19, 2011 11:59:03 PM	Apr 20, 2011 12:01:20 AM	
✓	✓	✓	ntc2ext-gw2	Tu1	tunnel	9 Kbps	Tunnel1	tunnel to ntc2rams	Apr 20, 2011 12:02:22 AM	Apr 20, 2011 12:06:20 AM	
✓	✓	✓	wanrouter-2	Tunnel1	other	9 Kbps	Tunnel1	tunnel to ntc2rams	May 3, 2011 5:37:52 PM	May 3, 2011 5:22:11 PM	

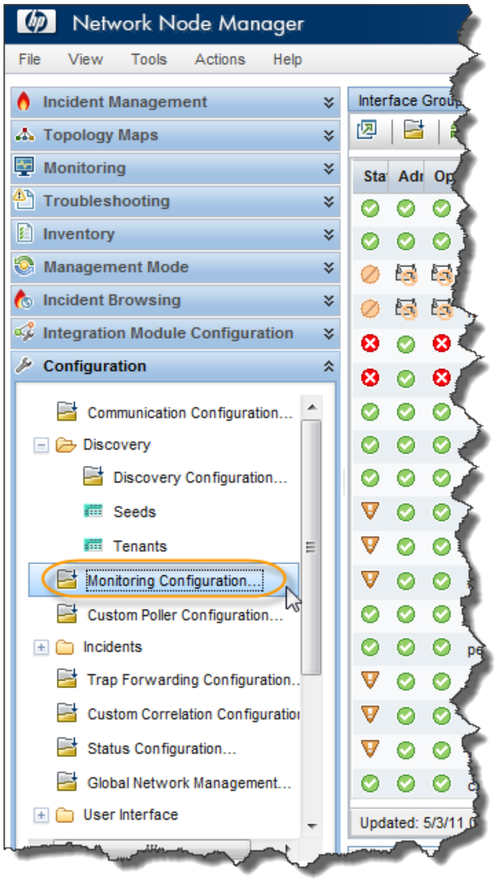
Apply Monitoring to an Interface Group

To monitor the interfaces defined by the filter just created, apply monitoring to this Interface Group. You can apply monitoring to both Node Groups and Interface Groups.

Note: NNMi considers an interface setting to be a higher priority than a node setting.

1. From the workspace navigation panel, select the **Configuration** workspace, and then click **Monitoring Configuration**.

Figure 25: Monitoring Configuration

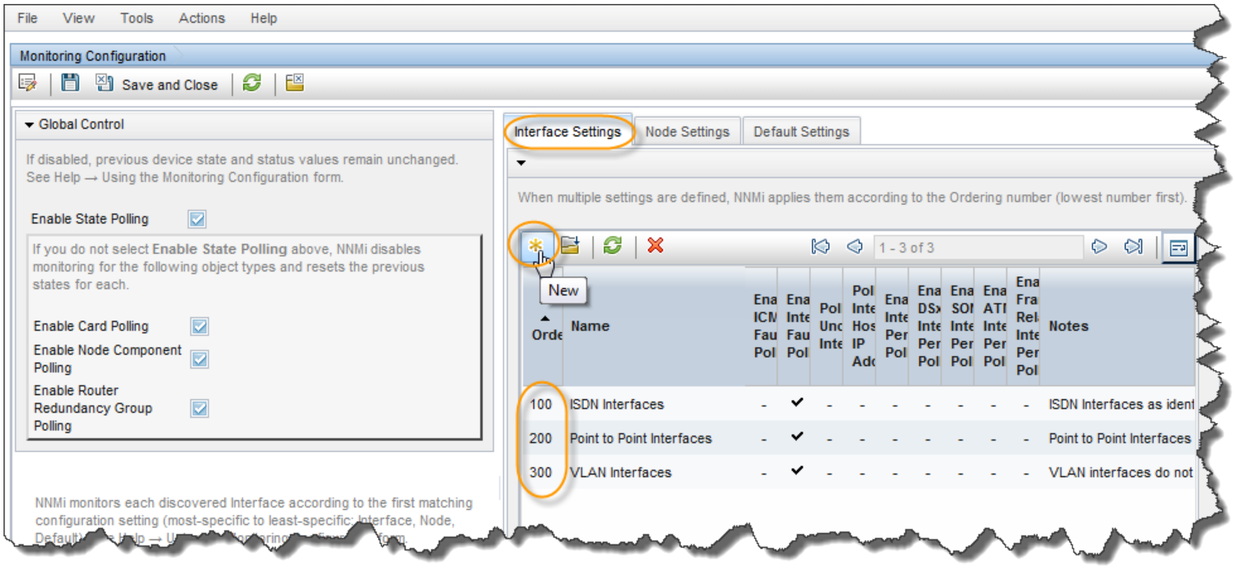

Network Node Manager
File View Tools Actions Help
Incident Management
Topology Maps
Monitoring
Troubleshooting
Inventory
Management Mode
Incident Browsing
Integration Module Configuration
Configuration
Communication Configuration...
Discovery
Discovery Configuration...
Seeds
Tenants
Monitoring Configuration...
Custom Poller Configuration...
Incidents
Trap Forwarding Configuration...
Custom Correlation Configuratio
Status Configuration...
Global Network Management...
User Interface
Interface Grou
Sta Adı Op
Updated: 5/3/11

2. Click the **Interface Settings** tab.

Tip: Take note of the current Ordering values. These define priority if an interface belongs to multiple groups.

In this example, the highest priority is `100`.

Figure 26: Monitoring Configuration: Interface Settings Tab



If disabled, previous device state and status values remain unchanged. See Help → Using the Monitoring Configuration form.

Enable State Polling ☑

If you do not select **Enable State Polling** above, NNMi disables monitoring for the following object types and resets the previous states for each.

Enable Card Polling ☑

Enable Node Component Polling ☑

Enable Router Redundancy Group Polling ☑

NNMi monitors each discovered Interface according to the first matching configuration setting (most-specific to least-specific: Interface, Node, Default). See Help → Using the Monitoring Configuration form.

When multiple settings are defined, NNMi applies them according to the Ordering number (lowest number first).

Orde	Name	Ena ICM Fau Pol	Ena Inte Fau Pol	Pol Unc Inte	Pol Inte Hos IP Adc	Ena Inte Per Pol	Ena DSx Inte Per Pol	Ena SOI Inte Per Pol	Ena ATI Inte Per Pol	Ena Fra Rel Inte Per Pol	Notes
100	ISDN Interfaces	-	✓	-	-	-	-	-	-	-	ISDN Interfaces as ident
200	Point to Point Interfaces	-	✓	-	-	-	-	-	-	-	Point to Point Interfaces
300	VLAN Interfaces	-	✓	-	-	-	-	-	-	-	VLAN interfaces do not

3. Click the ✳ icon.

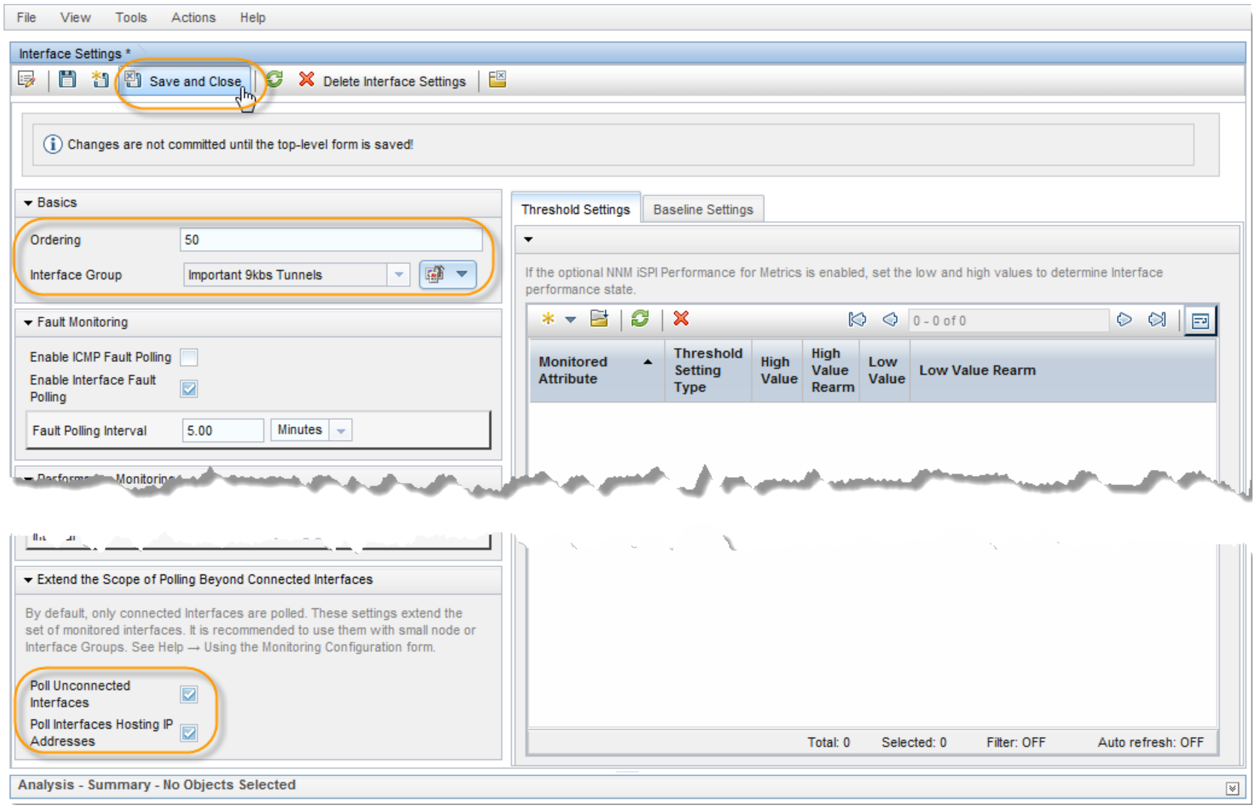
4. Enter an **Ordering** value that configures this setting to have a higher priority than other settings. This ensures that these interfaces get polled. NNMi considers lower numbers to be higher priority. You also want to choose an **Ordering** value that takes into consideration future configurations. For example, if you set this number to `1`, that sets the highest priority possible and limits your future entries. For this example, enter `50`.

5. Extend the monitoring scope. To monitor these interfaces regardless of whether they are connected, click all the check boxes in the Extend the Scope of Polling Beyond Connected Interfaces area of the form.

6. Use the **Quick Find** feature to select your newly created Interface Group. Then click **Save and Close**.

7. Click **Save and Close** at the top level **Monitoring Configuration** form to save your changes.

Figure 27: Interface Settings: Save and Close



Interface Settings *

Changes are not committed until the top-level form is saved!

Basics

Ordering 50

Interface Group Important 9kbs Tunnels

Fault Monitoring

Enable ICMP Fault Polling ☐

Enable Interface Fault Polling ☑

Fault Polling Interval 5.00 Minutes

Performance Monitoring

Extend the Scope of Polling Beyond Connected Interfaces

By default, only connected Interfaces are polled. These settings extend the set of monitored interfaces. It is recommended to use them with small node or Interface Groups. See Help → Using the Monitoring Configuration form.

Poll Unconnected Interfaces ☑

Poll Interfaces Hosting IP Addresses ☑

If the optional NNM iSPI Performance for Metrics is enabled, set the low and high values to determine Interface performance state.

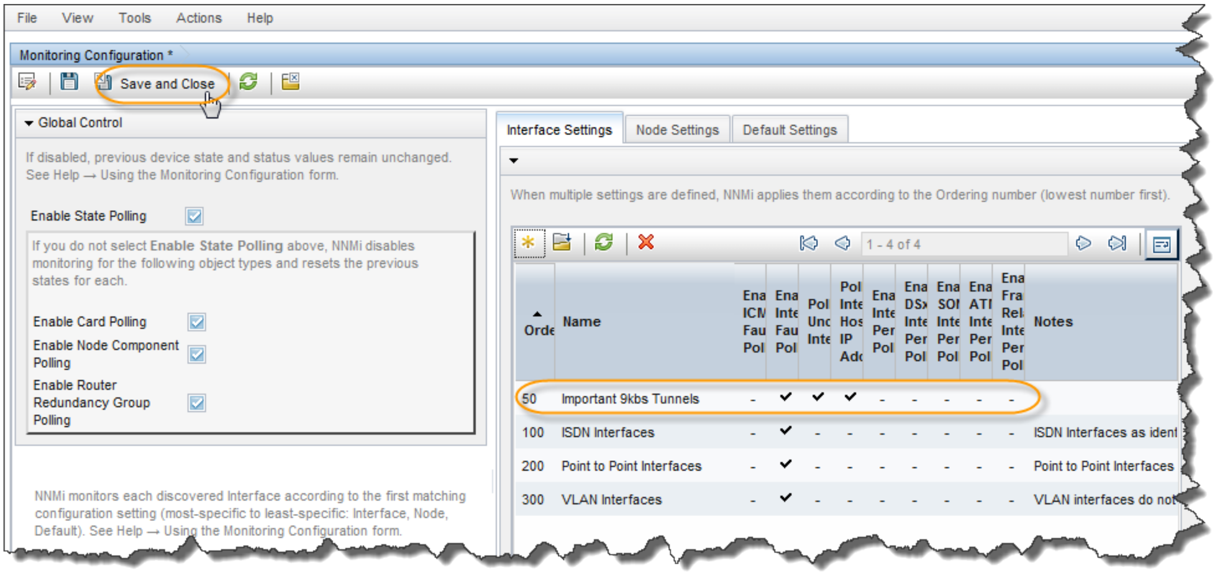
0 - 0 of 0

Monitored Attribute	Threshold Setting Type	High Value	High Value Rearm	Low Value	Low Value Rearm

Total: 0 Selected: 0 Filter: OFF Auto refresh: OFF

Analysis - Summary - No Objects Selected

Figure 28: Monitoring Configuration: Save and Close



Monitoring Configuration *

Global Control

If disabled, previous device state and status values remain unchanged. See Help → Using the Monitoring Configuration form.

Enable State Polling ☑

If you do not select **Enable State Polling** above, NNMi disables monitoring for the following object types and resets the previous states for each.

Enable Card Polling ☑

Enable Node Component Polling ☑

Enable Router Redundancy Group Polling ☑

NNMi monitors each discovered Interface according to the first matching configuration setting (most-specific to least-specific: Interface, Node, Default). See Help → Using the Monitoring Configuration form.

When multiple settings are defined, NNMi applies them according to the Ordering number (lowest number first).

1 - 4 of 4

Orde	Name	Ena ICM Fau Pol	Ena Inte Fau Pol	Pol Unc Inte	Pol Inte Hos IP Adc	Ena Inte Per Pol	Ena DSx Inte Per Pol	Ena SOI Inte Per Pol	Ena ATI Inte Per Pol	Ena Fra Rel Inte Per Pol	Notes
50	Important 9kbs Tunnels	-	✓	✓	✓	-	-	-	-	-	
100	ISDN Interfaces	-	✓	-	-	-	-	-	-	-	ISDN Interfaces as ident
200	Point to Point Interfaces	-	✓	-	-	-	-	-	-	-	Point to Point Interfaces
300	VLAN Interfaces	-	✓	-	-	-	-	-	-	-	VLAN interfaces do not

Now that you have a monitoring setting that applies to everything in this Interface Group, NNMi uses SNMP to monitor any interface that matches the `Important 9kbs Tunnels` filter.

Test the Monitoring Settings

You can test your new monitoring settings in many different ways. For this example, use the following steps:

1. From the workspace navigation panel, select the **Inventory** workspace, and then click **Interfaces**.
2. Use the drop-down menu to select the new Interface Group, `Important 9kbs Tunnels`.

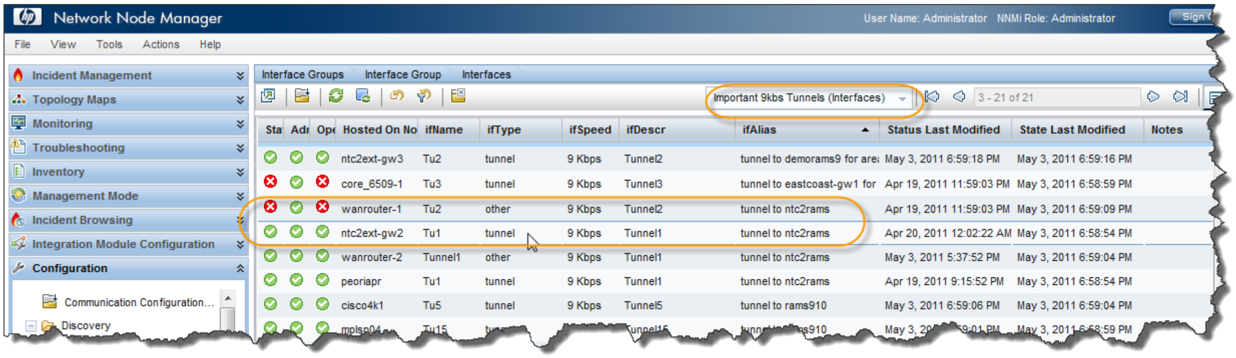
This filters the table to only show the interfaces in this Interface Group.

Tip: You might notice that some of the interfaces have an Administrative State of Not Polled. It can take a few minutes for your Monitoring configuration changes to take effect. To manually force the interfaces to be polled, perform a Status Poll command on one of the nodes hosting these interfaces. You should see them all begin to acquire status.

To perform a Status Poll on a node:

1. From the workspace navigation panel, select the **Inventory** workspace, and then click **Nodes**.
2. Select the node you want to poll, and then use the **Actions > Polling > Status Poll** command to start the Status Poll.

Figure 29: Interfaces: Important 9kbs Tunnels Filter



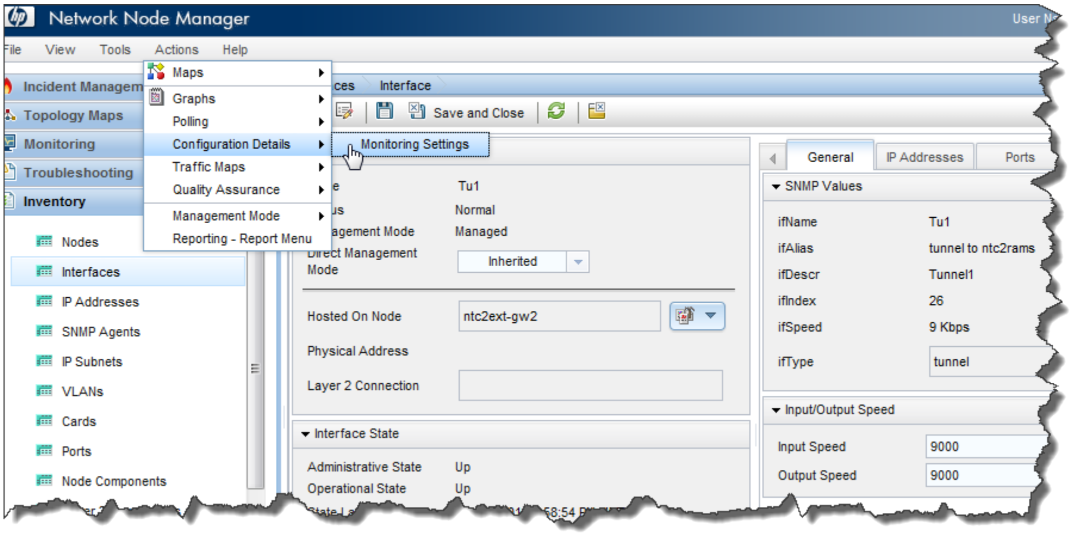
Sta	Adı	Ope	Hosted On No	ifName	ifType	ifSpeed	ifDescr	ifAlias	Status Last Modified	State Last Modified	Notes
✓	✓	✓	ntc2ext-gw3	Tu2	tunnel	9 Kbps	Tunnel2	tunnel to demorams9 for are	May 3, 2011 6:59:18 PM	May 3, 2011 6:59:16 PM	
✗	✓	✗	core_6509-1	Tu3	tunnel	9 Kbps	Tunnel3	tunnel to eastcoast-gw1 for	Apr 19, 2011 11:59:03 PM	May 3, 2011 6:58:59 PM	
✗	✓	✗	wanrouter-1	Tu2	other	9 Kbps	Tunnel2	tunnel to ntc2rams	Apr 19, 2011 11:59:03 PM	May 3, 2011 6:59:09 PM	
✓	✓	✓	ntc2ext-gw2	Tu1	tunnel	9 Kbps	Tunnel1	tunnel to ntc2rams	Apr 20, 2011 12:02:22 AM	May 3, 2011 6:58:54 PM	
✓	✓	✓	wanrouter-2	Tunnel1	other	9 Kbps	Tunnel1	tunnel to ntc2rams	May 3, 2011 5:37:52 PM	May 3, 2011 6:59:04 PM	
✓	✓	✓	peoriapr	Tu1	tunnel	9 Kbps	Tunnel1	tunnel to ntc2rams	Apr 19, 2011 9:15:52 PM	May 3, 2011 6:58:54 PM	
✓	✓	✓	cisco4k1	Tu5	tunnel	9 Kbps	Tunnel5	tunnel to rams910	May 3, 2011 6:59:06 PM	May 3, 2011 6:59:04 PM	
✓	✓	✓	mplsp04	Tu15			Tunnel15	s910	May 3, 20	May 3, 2011 6:58:59 PM	

Open one of the interfaces highlighted in the previous figure and check the monitoring settings to confirm that your monitoring settings are working properly.

To check monitoring settings for an interface:

1. Double-click the interface.
2. Click **Actions > Configuration Details > Monitoring Settings** to view the monitoring configuration for the selected interface.

Figure 30: Actions: Monitoring Settings



e Tu1
us Normal
agement Mode Managed
Direct Management Mode Inherited

Hosted On Node ntc2ext-gw2
Physical Address
Layer 2 Connection

Interface State

Administrative State Up
Operational State Up

SNMP Values

ifName Tu1
ifAlias tunnel to ntc2rams
ifDescr Tunnel1
ifIndex 26
ifSpeed 9 Kbps
ifType tunnel

Input/Output Speed

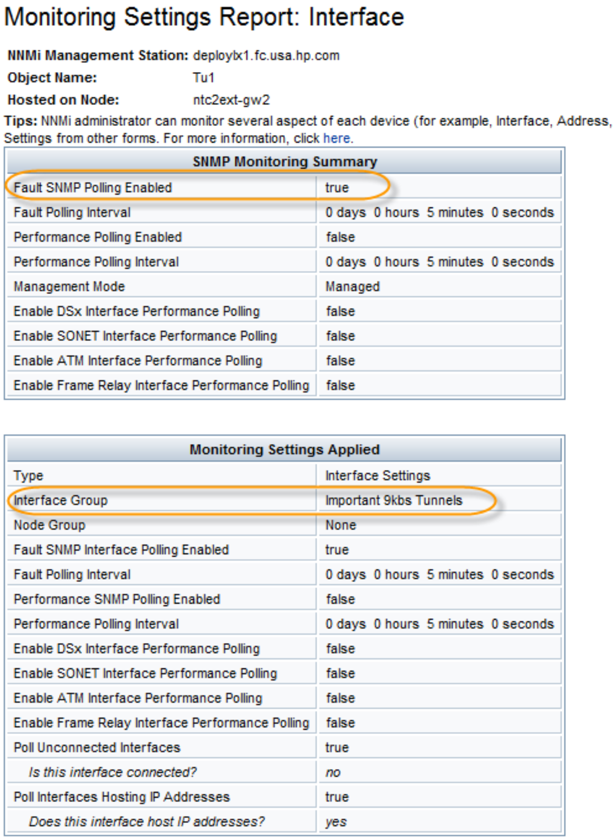
Input Speed 9000
Output Speed 9000

This example report confirms that the monitoring settings are working properly:

First, you can see that NNMi applied the monitoring settings for the `Important 9kbs Tunnels` group to this interface. This shows you that the monitoring settings are properly associated with this interface.

Second, you can see that NNMi has `Fault SNMP Polling Enabled` set to true. This indicates that the new monitoring settings are successfully applied to the `Important 9kbs Tunnels` Interface Group.

Figure 31: Monitoring Settings Report: Interface



Monitoring Settings Report: Interface

NNMi Management Station: deploylx1.fc.usa.hp.com
Object Name: Tu1
Hosted on Node: ntc2ext-gw2
Tips: NNMi administrator can monitor several aspect of each device (for example, Interface, Address,
Settings from other forms. For more information, click here.

SNMP Monitoring Summary	
Fault SNMP Polling Enabled	true
Fault Polling Interval	0 days 0 hours 5 minutes 0 seconds
Performance Polling Enabled	false
Performance Polling Interval	0 days 0 hours 5 minutes 0 seconds
Management Mode	Managed
Enable DSx Interface Performance Polling	false
Enable SONET Interface Performance Polling	false
Enable ATM Interface Performance Polling	false
Enable Frame Relay Interface Performance Polling	false

Monitoring Settings Applied	
Type	Interface Settings
Interface Group	Important 9kbs Tunnels
Node Group	None
Fault SNMP Interface Polling Enabled	true
Fault Polling Interval	0 days 0 hours 5 minutes 0 seconds
Performance SNMP Polling Enabled	false
Performance Polling Interval	0 days 0 hours 5 minutes 0 seconds
Enable DSx Interface Performance Polling	false
Enable SONET Interface Performance Polling	false
Enable ATM Interface Performance Polling	false
Enable Frame Relay Interface Performance Polling	false
Poll Unconnected Interfaces	true
Is this interface connected?	*no*
Poll Interfaces Hosting IP Addresses	true
Does this interface host IP addresses?	*yes*

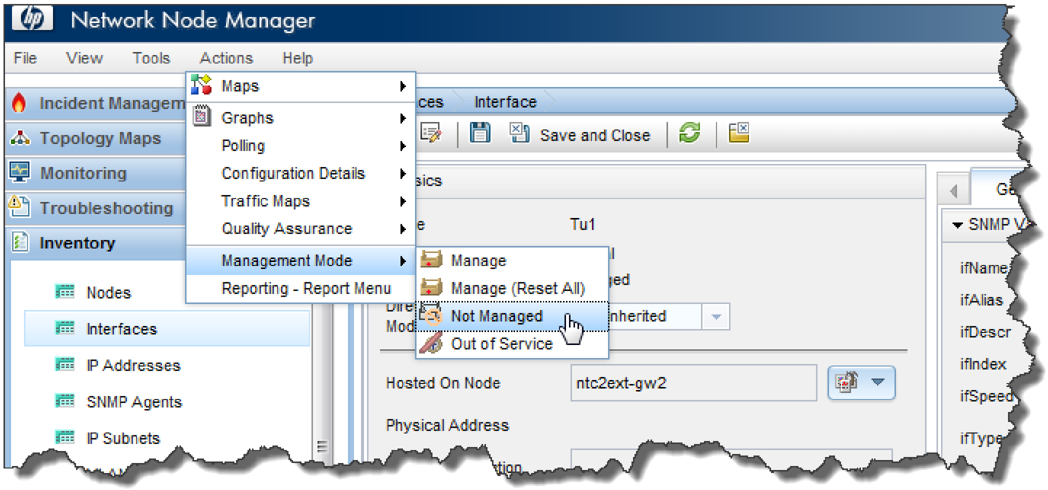
Monitoring Exceptions

You can manually force an interface or node to be unmonitored.

From the **Interface** form, click **Actions > Management Mode > Not Managed** to switch to unmanaging the interface.

NNMi no longer monitors this interface regardless of the monitoring settings.

Figure 32: Actions: Management Mode: Not Managed



NNMi does not presently have the same approach that NNM used to force an interface to be unmonitored. Currently, unmanaging an interface is only a *negative override*.

See *Forcing an Interface to be Polled,* available at http://h20230.www2.hp.com/selfsolve/manuals, to force NNMi to monitor an interface.

Configure Incidents, Traps, and Automatic Actions

Configure Incidents

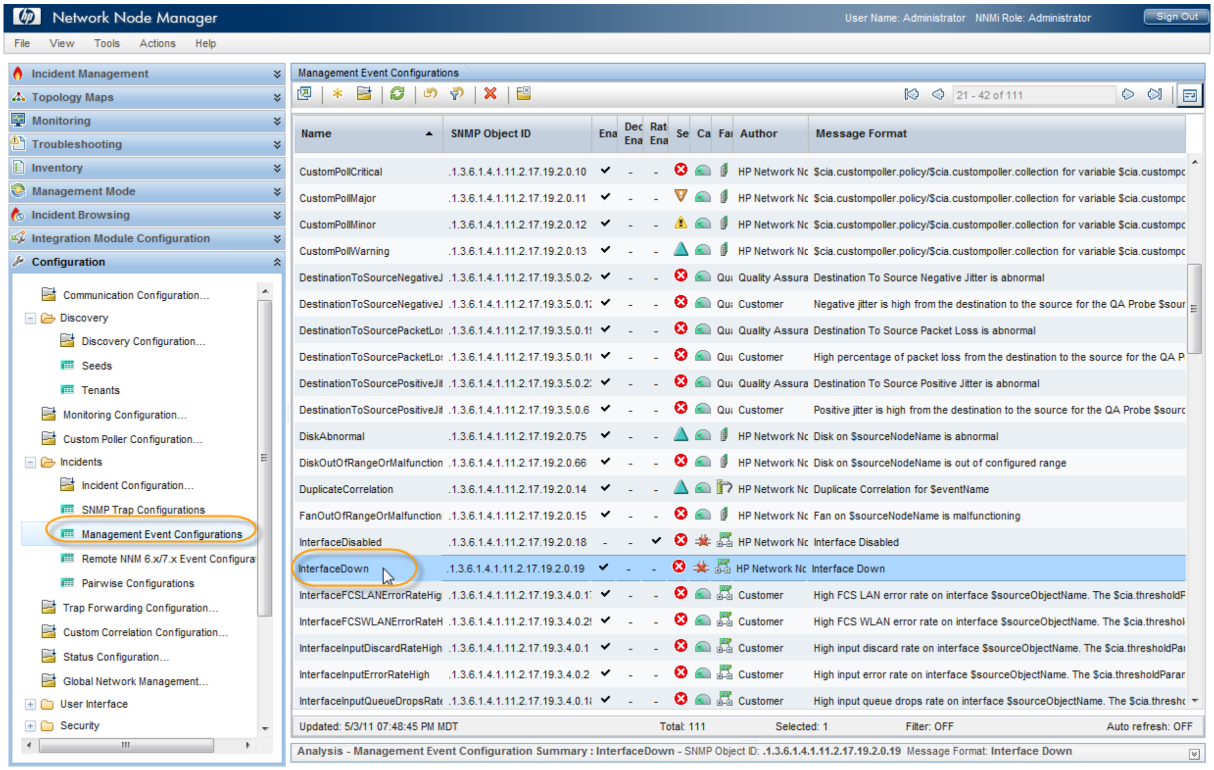
With NNMi, you can change certain aspects of an incident. Some examples include enabling an incident, formatting a message, enabling de-duplication, and enabling rate correlation.

This example describes how to enhance the `InterfaceDown` (Interface Down) incident to include the `Interface Alias` in the message.

1. From the workspace navigation panel, select the **Configuration** workspace, and then click **Incidents > Management Event Configurations**.

2. Double-click the `InterfaceDown` incident configuration.

Figure 33: Configuration: Management Event Configurations


Network Node Manager
User Name: Administrator NNMi Role: Administrator
Sign Out
File
View
Tools
Actions
Help
Incident Management
Topology Maps
Monitoring
Troubleshooting
Inventory
Management Mode
Incident Browsing
Integration Module Configuration
Configuration
Communication Configuration...
Discovery
Discovery Configuration...
Seeds
Tenants
Monitoring Configuration...
Custom Poller Configuration...
Incidents
Incident Configuration...
SNMP Trap Configurations
Management Event Configurations
Remote NNM 6.x/7.x Event Configura
Pairwise Configurations
Trap Forwarding Configuration...
Custom Correlation Configuration...
Status Configuration...
Global Network Management...
User Interface
Security
Management Event Configurations
21 - 42 of 111

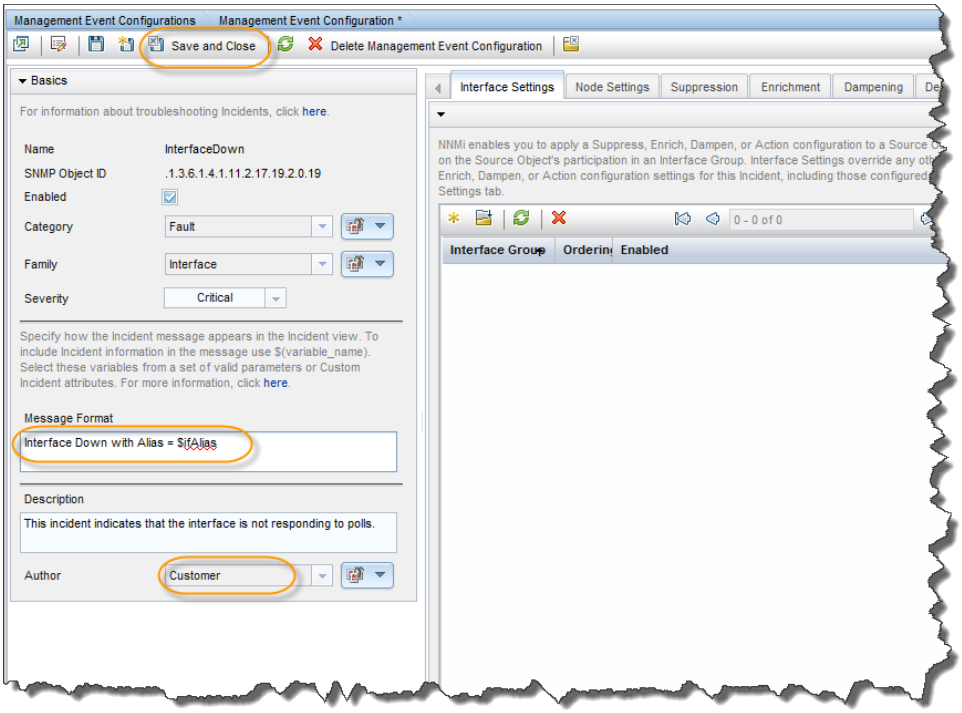
Name	SNMP Object ID	Ena	Dec Ena	Rat Ena	Se	Ca	Fa	Author	Message Format
CustomPollCritical	.1.3.6.1.4.1.11.2.17.19.2.0.10	✓	-	-	✖			HP Network Nc	$cia.custompoller.policy/$cia.custompoller.collection for variable $cia.custompc
CustomPollMajor	.1.3.6.1.4.1.11.2.17.19.2.0.11	✓	-	-	▽			HP Network Nc	$cia.custompoller.policy/$cia.custompoller.collection for variable $cia.custompc
CustomPollMinor	.1.3.6.1.4.1.11.2.17.19.2.0.12	✓	-	-	⚠			HP Network Nc	$cia.custompoller.policy/$cia.custompoller.collection for variable $cia.custompc
CustomPollWarning	.1.3.6.1.4.1.11.2.17.19.2.0.13	✓	-	-	▲			HP Network Nc	$cia.custompoller.policy/$cia.custompoller.collection for variable $cia.custompc
DestinationToSourceNegativeJ	.1.3.6.1.4.1.11.2.17.19.3.5.0.2	✓	-	-	✖		Qu	Quality Assura	Destination To Source Negative Jitter is abnormal
DestinationToSourceNegativeJ	.1.3.6.1.4.1.11.2.17.19.3.5.0.1	✓	-	-	✖		Qu	Customer	Negative jitter is high from the destination to the source for the QA Probe $sour
DestinationToSourcePacketLo	.1.3.6.1.4.1.11.2.17.19.3.5.0.1	✓	-	-	✖		Qu	Quality Assura	Destination To Source Packet Loss is abnormal
DestinationToSourcePacketLo	.1.3.6.1.4.1.11.2.17.19.3.5.0.1	✓	-	-	✖		Qu	Customer	High percentage of packet loss from the destination to the source for the QA P
DestinationToSourcePositiveJi	.1.3.6.1.4.1.11.2.17.19.3.5.0.2	✓	-	-	✖		Qu	Quality Assura	Destination To Source Positive Jitter is abnormal
DestinationToSourcePositiveJi	.1.3.6.1.4.1.11.2.17.19.3.5.0.6	✓	-	-	✖		Qu	Customer	Positive jitter is high from the destination to the source for the QA Probe $sourc
DiskAbnormal	.1.3.6.1.4.1.11.2.17.19.2.0.75	✓	-	-	▲			HP Network Nc	Disk on $sourceNodeName is abnormal
DiskOutOfRangeOrMalfunction	.1.3.6.1.4.1.11.2.17.19.2.0.66	✓	-	-	✖			HP Network Nc	Disk on $sourceNodeName is out of configured range
DuplicateCorrelation	.1.3.6.1.4.1.11.2.17.19.2.0.14	✓	-	-	▲			HP Network Nc	Duplicate Correlation for $eventName
FanOutOfRangeOrMalfunction	.1.3.6.1.4.1.11.2.17.19.2.0.15	✓	-	-	✖			HP Network Nc	Fan on $sourceNodeName is malfunctioning
InterfaceDisabled	.1.3.6.1.4.1.11.2.17.19.2.0.18	-	-	✓	✖			HP Network Nc	Interface Disabled
InterfaceDown	.1.3.6.1.4.1.11.2.17.19.2.0.19	✓	-	-	✖			HP Network Nc	Interface Down
InterfaceFCSLANErrorRateHig	.1.3.6.1.4.1.11.2.17.19.3.4.0.1	✓	-	-	✖			Customer	High FCS LAN error rate on interface $sourceObjectName. The $cia.thresholdF
InterfaceFCSWLANErrorRateH	.1.3.6.1.4.1.11.2.17.19.3.4.0.2	✓	-	-	✖			Customer	High FCS WLAN error rate on interface $sourceObjectName. The $cia.threshol
InterfaceInputDiscardRateHigh	.1.3.6.1.4.1.11.2.17.19.3.4.0.1	✓	-	-	✖			Customer	High input discard rate on interface $sourceObjectName. The $cia.thresholdPa
InterfaceInputErrorRateHigh	.1.3.6.1.4.1.11.2.17.19.3.4.0.2	✓	-	-	✖			Customer	High input error rate on interface $sourceObjectName. The $cia.thresholdParar
InterfaceInputQueueDropsRate	.1.3.6.1.4.1.11.2.17.19.3.4.0.1	✓	-	-	✖			Customer	High input queue drops rate on interface $sourceObjectName. The $cia.threshc

Updated: 5/3/11 07:48:45 PM MDT Total: 111 Selected: 1 Filter: OFF Auto refresh: OFF

Analysis - Management Event Configuration Summary : InterfaceDown - SNMP Object ID: .1.3.6.1.4.1.11.2.17.19.2.0.19 Message Format: Interface Down

3. Before continuing, see "*Valid Parameters for Configuring Incident Messages*" in the NNMi help to view the possible arguments that can be added to a message format. In this example, add the argument `$ifAlias` to the incident message as shown in the following example.

Figure 34: Management Event Configuration: Message Format



Management Event Configurations
Management Event Configuration *

Save and Close
Delete Management Event Configuration

Basics

For information about troubleshooting Incidents, click here.

Name	InterfaceDown
SNMP Object ID	.1.3.6.1.4.1.11.2.17.19.2.0.19
Enabled	☑
Category	Fault
Family	Interface
Severity	Critical

Specify how the Incident message appears in the Incident view. To include Incident information in the message use $(variable_name). Select these variables from a set of valid parameters or Custom Incident attributes. For more information, click here.

Message Format
Interface Down with Alias = $ifAlias

Description
This incident indicates that the interface is not responding to polls.

Author
Customer

NNMi enables you to apply a Suppress, Enrich, Dampen, or Action configuration to a Source O on the Source Object's participation in an Interface Group. Interface Settings override any oth Enrich, Dampen, or Action configuration settings for this Incident, including those configured Settings tab.

0 - 0 of 0

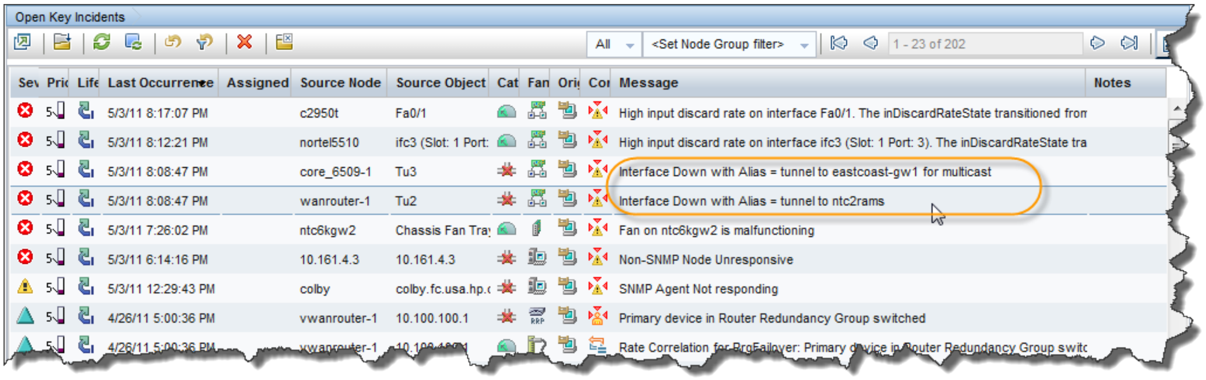
Interface Group	Ordering	Enabled

4. Change the **Author** to **Customer** using **Quick Find**.
5. Finally, click **Save and Close** on this form and in the **Management Event Configuration** form.

As shown in the following **Open Key Incidents** view example, all `InterfaceDown` incidents show the `$ifAlias` parameter.

Note: If there is no alias on the interface, NNMi displays `null` for the alias.

Figure 35: Open Key Incidents



Open Key Incidents

All
<Set Node Group filter>
1 - 23 of 202

Sev	Pric	Life	Last Occurrence	Assigned	Source Node	Source Object	Cat	Fan	Ori	Cor	Message	Notes
✖	5		5/3/11 8:17:07 PM		c2950t	Fa0/1					High input discard rate on interface Fa0/1. The inDiscardRateState transitioned from	
✖	5		5/3/11 8:12:21 PM		nortel5510	ifc3 (Slot: 1 Port:					High input discard rate on interface ifc3 (Slot: 1 Port: 3). The inDiscardRateState tra	
✖	5		5/3/11 8:08:47 PM		core_6509-1	Tu3					Interface Down with Alias = tunnel to eastcoast-gw1 for multicast	
✖	5		5/3/11 8:08:47 PM		wanrouter-1	Tu2					Interface Down with Alias = tunnel to ntc2rams	
✖	5		5/3/11 7:26:02 PM		ntc6kgw2	Chassis Fan Tray					Fan on ntc6kgw2 is malfunctioning	
✖	5		5/3/11 6:14:16 PM		10.161.4.3	10.161.4.3					Non-SNMP Node Unresponsive	
⚠	5		5/3/11 12:29:43 PM		colby	colby.fc.usa.hp.c					SNMP Agent Not responding	
▲	5		4/26/11 5:00:36 PM		vwanrouter-1	10.100.100.1					Primary device in Router Redundancy Group switched	
▲	5		4/26/11 5:00:36 PM		vwanrouter-1	10.100.100.1					Rate Correlation for RrgFailover: Primary device in Router Redundancy Group switc	

Configure Traps

Tip: See *Step- by-Step Guide to Incident Management*, available at http://h20230.www2.hp.com/selfsolve/manuals, for more details about working with traps in NNMi

Note: To receive a trap into the NNMi Incident Browser, you must load the MIB that contains the trap definitions into NNMi.

For this example, you need to load three MIBs to satisfy the dependencies. You first load the `ruggedcom.mib` file, followed by the `rcsysinfo.mib` file. Then you can load the traps from the `ruggedcomtraps.mib` file. Use the **`nnmloadmib.ovpl`** command to load the MIBs into NNMi.

Note: You can also use the NNMi console to load MIBs.

To load MIBs using the command line:

1. Run the **`nnmloadmib.ovpl -load ./ruggedcom.mib`** command. This loads the `ruggedcom.mib` definitions.
2. Run the **`nnmloadmib.ovpl -load ./rcsysinfo.mib`** command. This loads the `rcsysinfo.mib` definitions.
3. Run the **`nnmloadmib.ovpl -load ./ruggedcomtraps.mib`** command. This loads the `ruggedcomtraps.mib` file.

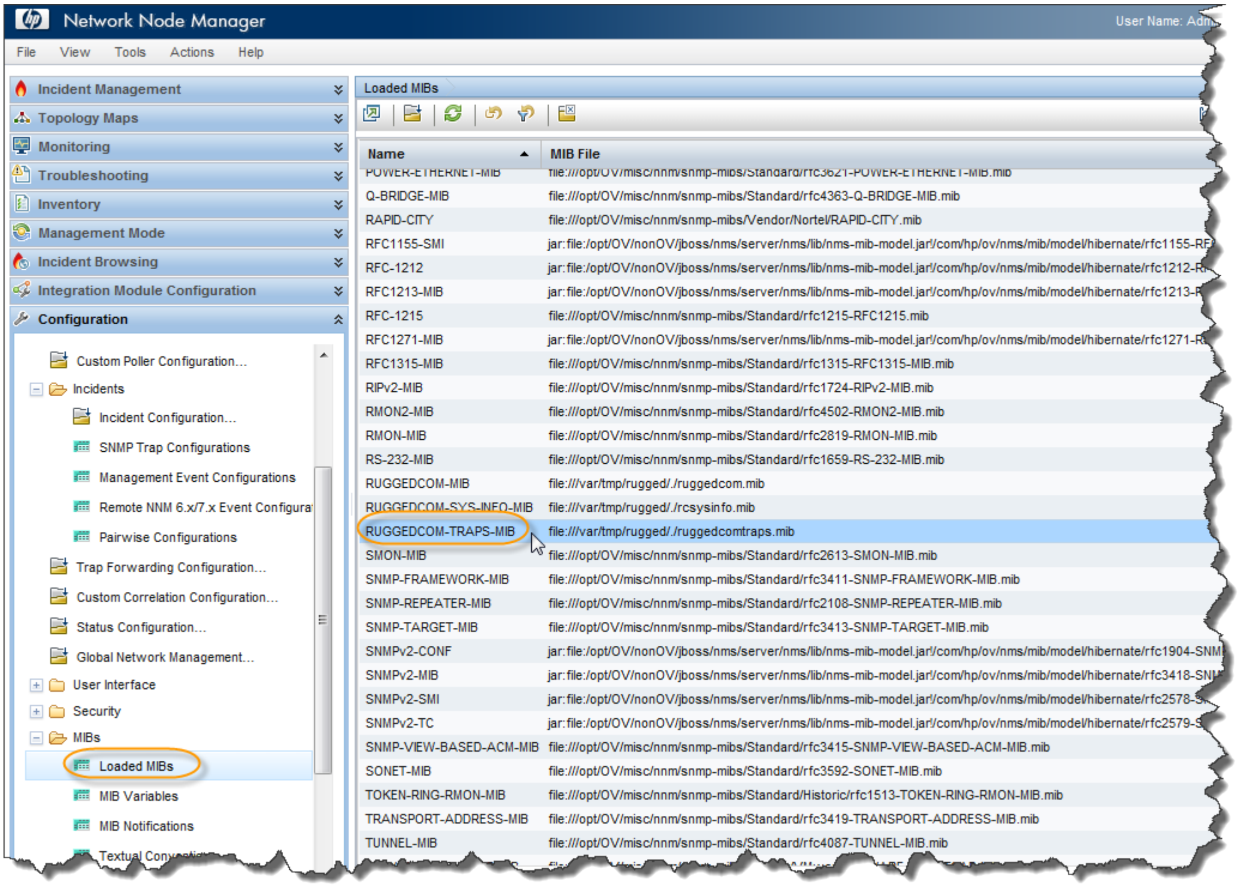
Next, verify that the MIBs are loaded:

1. From the workspace navigation panel, select the **Configuration** workspace, and then click **MIBs > Loaded MIBs**.

Notice the newly loaded `Rugged Com` MIBs.

2. Take note of the traps module (`RUGGEDCOM-TRAPS-MIB`). You will need this for the next command.

Figure 36: Configuration: Loaded MIBs



Name	MIB File
POWER-ETHERNET-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc3621-POWER-ETHERNET-MIB.mib
Q-BRIDGE-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc4363-Q-BRIDGE-MIB.mib
RAPID-CITY	file:///opt/OV/misc/nnm/snmp-mibs/Vendor/Nortel/RAPID-CITY.mib
RFC1155-SMI	jar:file:/opt/OV/nonOV/jboss/nms/server/nms/lib/nms-mib-model.jar!/com/hp/ov/nms/mib/model/hibernate/rfc1155-RF
RFC-1212	jar:file:/opt/OV/nonOV/jboss/nms/server/nms/lib/nms-mib-model.jar!/com/hp/ov/nms/mib/model/hibernate/rfc1212-R
RFC1213-MIB	jar:file:/opt/OV/nonOV/jboss/nms/server/nms/lib/nms-mib-model.jar!/com/hp/ov/nms/mib/model/hibernate/rfc1213-R
RFC-1215	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc1215-RFC1215.mib
RFC1271-MIB	jar:file:/opt/OV/nonOV/jboss/nms/server/nms/lib/nms-mib-model.jar!/com/hp/ov/nms/mib/model/hibernate/rfc1271-R
RFC1315-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc1315-RFC1315-MIB.mib
RIPv2-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc1724-RIPv2-MIB.mib
RMON2-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc4502-RMON2-MIB.mib
RMON-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc2819-RMON-MIB.mib
RS-232-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc1659-RS-232-MIB.mib
RUGGEDCOM-MIB	file:///var/tmp/rugged/./ruggedcom.mib
RUGGEDCOM-SYS-INFO-MIB	file:///var/tmp/rugged/./rcsysinfo.mib
RUGGEDCOM-TRAPS-MIB	file:///var/tmp/rugged/./ruggedcomtraps.mib
SMON-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc2613-SMON-MIB.mib
SNMP-FRAMEWORK-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc3411-SNMP-FRAMEWORK-MIB.mib
SNMP-REPEATER-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc2108-SNMP-REPEATER-MIB.mib
SNMP-TARGET-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc3413-SNMP-TARGET-MIB.mib
SNMPv2-CONF	jar:file:/opt/OV/nonOV/jboss/nms/server/nms/lib/nms-mib-model.jar!/com/hp/ov/nms/mib/model/hibernate/rfc1904-SNM
SNMPv2-MIB	jar:file:/opt/OV/nonOV/jboss/nms/server/nms/lib/nms-mib-model.jar!/com/hp/ov/nms/mib/model/hibernate/rfc3418-SN
SNMPv2-SMI	jar:file:/opt/OV/nonOV/jboss/nms/server/nms/lib/nms-mib-model.jar!/com/hp/ov/nms/mib/model/hibernate/rfc2578-S
SNMPv2-TC	jar:file:/opt/OV/nonOV/jboss/nms/server/nms/lib/nms-mib-model.jar!/com/hp/ov/nms/mib/model/hibernate/rfc2579-S
SNMP-VIEW-BASED-ACM-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc3415-SNMP-VIEW-BASED-ACM-MIB.mib
SONET-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc3592-SONET-MIB.mib
TOKEN-RING-RMON-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/Historic/rfc1513-TOKEN-RING-RMON-MIB.mib
TRANSPORT-ADDRESS-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc3419-TRANSPORT-ADDRESS-MIB.mib
TUNNEL-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc4087-TUNNEL-MIB.mib

4. Run the **`nnmincidentcfg.ovpl -loadTraps RUGGEDCOM-TRAPS-MIB`** command to load the traps from this module. You should see output similar to the following:

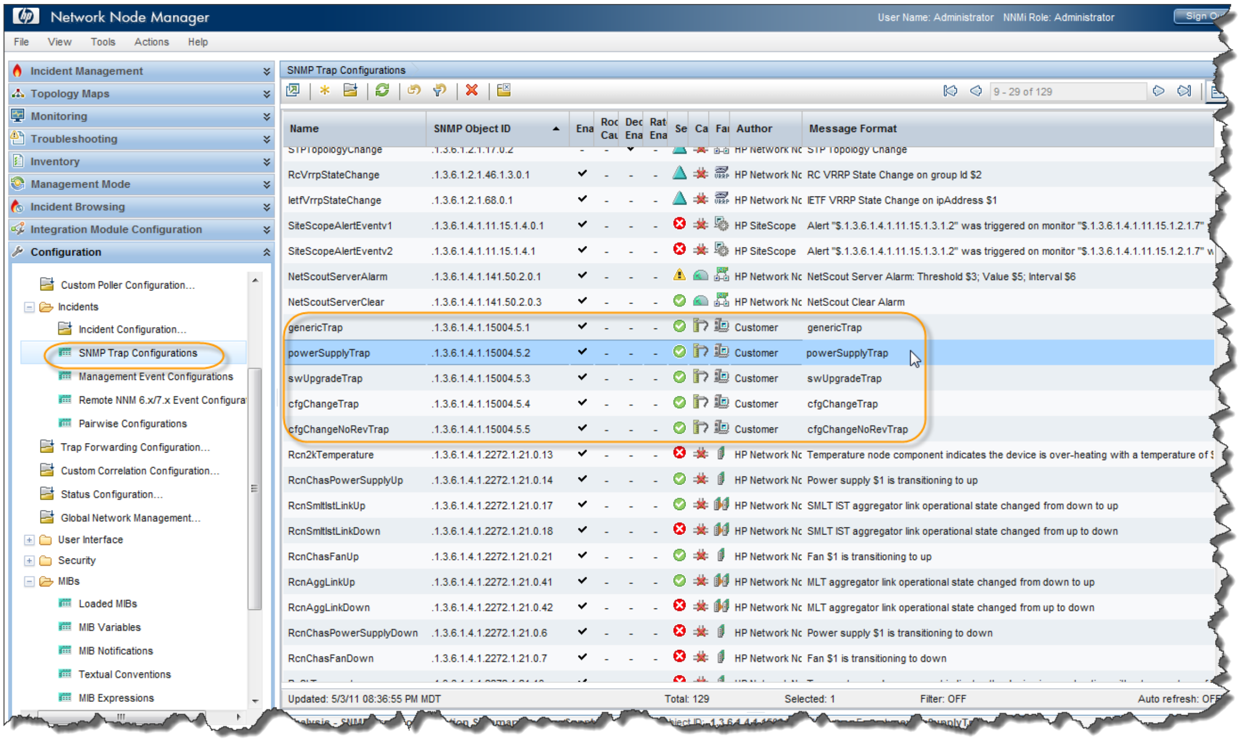
```
SNMP trap(s) from mib module loaded: RUGGEDCOM-TRAPS-MIB.
Number of traps: 5.
The following traps were added to incident configuration:
cfgChangeNoRevTrap - .1.3.6.1.4.1.15004.5.5
cfgChangeTrap - .1.3.6.1.4.1.15004.5.4
powerSupplyTrap - .1.3.6.1.4.1.15004.5.2
swUpgradeTrap - .1.3.6.1.4.1.15004.5.3
genericTrap - .1.3.6.1.4.1.15004.5.1
```

You now have four new traps defined in NNMi. To view them:

1. From the workspace navigation panel, select the **Configuration** workspace, and then click **Incidents > SNMP Trap Configurations**.
2. Sort the traps by **SNMP Object ID**.

Notice that all of the traps are loaded as *enabled*. You may want to disable all but the ones you specifically want to receive. You may want to make configuration modifications at this time.

Figure 37: Configuration: SNMP Trap Configurations



Name	SNMP Object ID	Ena	Roc Cau	Dec Ena	Rat Ena	Se	Ca	Fai	Author	Message Format
STPTopologyChange	.1.3.6.1.2.1.17.0.2	-	-	✓	-	▲			HP Network Nc	STP Topology Change
RcVrrpStateChange	.1.3.6.1.2.1.46.1.3.0.1	✓	-	-	-	▲			HP Network Nc	RC VRRP State Change on group Id $2
IetfVrrpStateChange	.1.3.6.1.2.1.68.0.1	✓	-	-	-	▲			HP Network Nc	IETF VRRP State Change on ipAddress $1
SiteScopeAlertEventv1	.1.3.6.1.4.1.11.15.1.4.0.1	✓	-	-	-	⊗			HP SiteScope	Alert "$.1.3.6.1.4.1.11.15.1.3.1.2" was triggered on monitor "$.1.3.6.1.4.1.11.15.1.2.1.7"
SiteScopeAlertEventv2	.1.3.6.1.4.1.11.15.1.4.1	✓	-	-	-	⊗			HP SiteScope	Alert "$.1.3.6.1.4.1.11.15.1.3.1.2" was triggered on monitor "$.1.3.6.1.4.1.11.15.1.2.1.7" w
NetScoutServerAlarm	.1.3.6.1.4.1.141.50.2.0.1	✓	-	-	-	⚠			HP Network Nc	NetScout Server Alarm: Threshold $3; Value $5; Interval $6
NetScoutServerClear	.1.3.6.1.4.1.141.50.2.0.3	✓	-	-	-	✓			HP Network Nc	NetScout Clear Alarm
genericTrap	.1.3.6.1.4.1.15004.5.1	✓	-	-	-	✓			Customer	genericTrap
powerSupplyTrap	.1.3.6.1.4.1.15004.5.2	✓	-	-	-	✓			Customer	powerSupplyTrap
swUpgradeTrap	.1.3.6.1.4.1.15004.5.3	✓	-	-	-	✓			Customer	swUpgradeTrap
cfgChangeTrap	.1.3.6.1.4.1.15004.5.4	✓	-	-	-	✓			Customer	cfgChangeTrap
cfgChangeNoRevTrap	.1.3.6.1.4.1.15004.5.5	✓	-	-	-	✓			Customer	cfgChangeNoRevTrap
Rcn2kTemperature	.1.3.6.1.4.1.2272.1.21.0.13	✓	-	-	-	⊗			HP Network Nc	Temperature node component indicates the device is over-heating with a temperature of $
RcnChasPowerSupplyUp	.1.3.6.1.4.1.2272.1.21.0.14	✓	-	-	-	✓			HP Network Nc	Power supply $1 is transitioning to up
RcnSmltIstLinkUp	.1.3.6.1.4.1.2272.1.21.0.17	✓	-	-	-	✓			HP Network Nc	SMLT IST aggregator link operational state changed from down to up
RcnSmltIstLinkDown	.1.3.6.1.4.1.2272.1.21.0.18	✓	-	-	-	⊗			HP Network Nc	SMLT IST aggregator link operational state changed from up to down
RcnChasFanUp	.1.3.6.1.4.1.2272.1.21.0.21	✓	-	-	-	✓			HP Network Nc	Fan $1 is transitioning to up
RcnAggLinkUp	.1.3.6.1.4.1.2272.1.21.0.41	✓	-	-	-	✓			HP Network Nc	MLT aggregator link operational state changed from down to up
RcnAggLinkDown	.1.3.6.1.4.1.2272.1.21.0.42	✓	-	-	-	⊗			HP Network Nc	MLT aggregator link operational state changed from up to down
RcnChasPowerSupplyDown	.1.3.6.1.4.1.2272.1.21.0.6	✓	-	-	-	⊗			HP Network Nc	Power supply $1 is transitioning to down
RcnChasFanDown	.1.3.6.1.4.1.2272.1.21.0.7	✓	-	-	-	⊗			HP Network Nc	Fan $1 is transitioning to down

Updated: 5/3/11 08:36:55 PM MDT Total: 129 Selected: 1 Filter: OFF Auto refresh: OFF

Configure Automatic Actions

You can configure automatic actions for incidents. Usually you do this for only management events rather than for SNMP traps, because it is hard to predict the rate and volume of traps. NNMi automatic actions can be executable commands, command line scripts, or Python scripts. The Python scripts execute within NNMi's Java virtual machine (JVM) so they execute quickly. Since NNMi uses a Java interpreter for Python, NNMi refers to these scripts as `Jython`.

In NNMi, actions are based on Lifecycle Sate changes for incidents. You can configure NNMi to take one action when an interface goes down and another action when the interface comes back up again. To do this, configure both actions on the `InterfaceDown` incident, but associate one action with the Lifecycle State set to `Registered` and the other action with the Lifecycle State set to `Closed`. Usually NNMi does not generate an associated up incident.

Note: When NNMi generates an incident, it assigns the `Registered` state to the incident.

To configure NNMi to run a Perl script when it receives a Node Down incident, do the following:

1. Place your script in the `actions` directory.

   Note: For security reasons, you must be `root` or `administrator` to access this directory.

   For this example, assume the `actions` directory appears in the following location:

   - *Windows*: `\Documents and Settings\All Users\Application Data\HP\HP BTO Software\shared\nnm\actions`
   - *UNIX*: `/var/opt/OV/shared/nnm/actions`

The `actions` directory can be in a different location depending on how you installed NNMi. For this example, the script is named `writelog.ovpl`. Copy this script into the `actions` directory. Make sure that your script is executable.

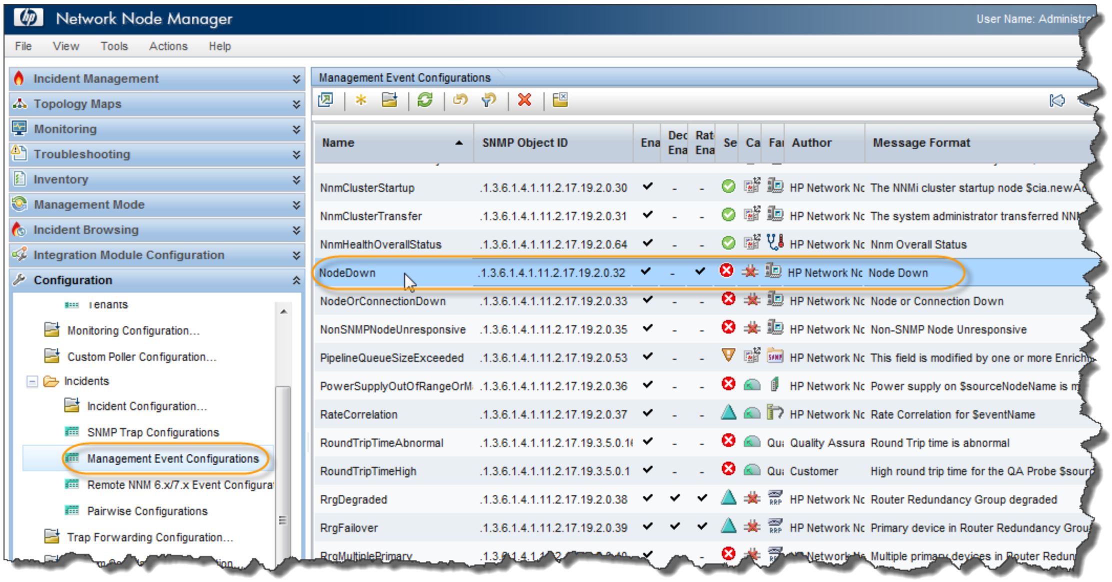
2. To associate this script with an action on this incident:

   a. From the workspace navigation panel, select the **Configuration** workspace.

   b. Click **Incidents > Management Event Configuration**.

   c. Double-click the `NodeDown` incident.

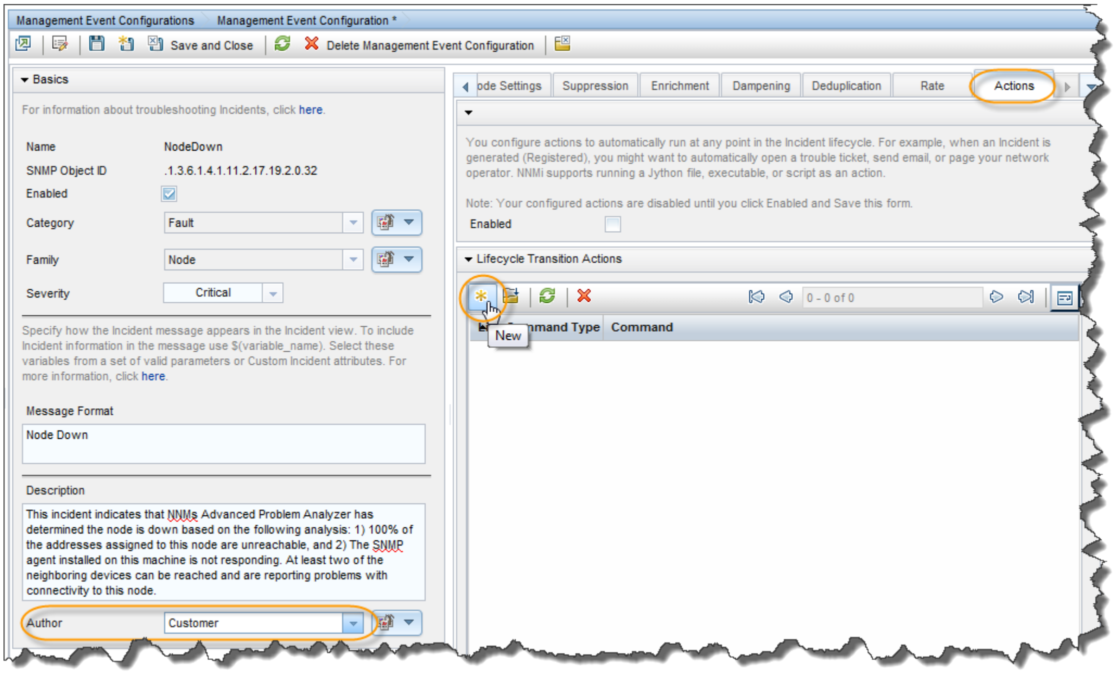
Figure 38: Management Event Configurations: NodeDown Incident



Name	SNMP Object ID	Ena	Dec Ena	Rat Ena	Se	Ca	Fa	Author	Message Format
NnmClusterStartup	.1.3.6.1.4.1.11.2.17.19.2.0.30	✓	-	-	✓			HP Network Nc	The NNMi cluster startup node $cia.newA
NnmClusterTransfer	.1.3.6.1.4.1.11.2.17.19.2.0.31	✓	-	-	✓			HP Network Nc	The system administrator transferred NN
NnmHealthOverallStatus	.1.3.6.1.4.1.11.2.17.19.2.0.64	✓	-	-	✓			HP Network Nc	Nnm Overall Status
NodeDown	.1.3.6.1.4.1.11.2.17.19.2.0.32	✓	-	✓	⊗			HP Network Nc	Node Down
NodeOrConnectionDown	.1.3.6.1.4.1.11.2.17.19.2.0.33	✓	-	-	⊗			HP Network Nc	Node or Connection Down
NonSNMPNodeUnresponsive	.1.3.6.1.4.1.11.2.17.19.2.0.35	✓	-	-	⊗			HP Network Nc	Non-SNMP Node Unresponsive
PipelineQueueSizeExceeded	.1.3.6.1.4.1.11.2.17.19.2.0.53	✓	-	-	▽			HP Network Nc	This field is modified by one or more Enrich
PowerSupplyOutOfRangeOrM	.1.3.6.1.4.1.11.2.17.19.2.0.36	✓	-	-	⊗			HP Network Nc	Power supply on $sourceNodeName is m
RateCorrelation	.1.3.6.1.4.1.11.2.17.19.2.0.37	✓	-	-	▲			HP Network Nc	Rate Correlation for $eventName
RoundTripTimeAbnormal	.1.3.6.1.4.1.11.2.17.19.3.5.0.1(	✓	-	-	⊗		Qu:	Quality Assura	Round Trip time is abnormal
RoundTripTimeHigh	.1.3.6.1.4.1.11.2.17.19.3.5.0.1	✓	-	-	⊗		Qu:	Customer	High round trip time for the QA Probe $sour
RrgDegraded	.1.3.6.1.4.1.11.2.17.19.2.0.38	✓	✓	✓	▲			HP Network Nc	Router Redundancy Group degraded
RrgFailover	.1.3.6.1.4.1.11.2.17.19.2.0.39	✓	✓	✓	▲			HP Network Nc	Primary device in Router Redundancy Grou
RrgMultiplePrimary	.1.3.6.1.4.1.11.2.17.19.2.0.40	✓		-	⊗			HP Network Nc	Multiple primary devices in Router Redun

3. Change the **Author** to **Customer**, click the **Actions** tab, and click the ✳ icon.

Figure 39: Management Event Configuration: Actions Tab


Management Event Configurations
Management Event Configuration *
Save and Close
Delete Management Event Configuration
Basics
ode Settings
Suppression
Enrichment
Dampening
Deduplication
Rate
Actions
Lifecycle Transition Actions
0 - 0 of 0
New

For information about troubleshooting Incidents, click here.

Name NodeDown

SNMP Object ID .1.3.6.1.4.1.11.2.17.19.2.0.32

Enabled ☑

Category Fault

Family Node

Severity Critical

Specify how the Incident message appears in the Incident view. To include Incident information in the message use $(variable_name). Select these variables from a set of valid parameters or Custom Incident attributes. For more information, click here.

Message Format

Node Down

Description

This incident indicates that NNMs Advanced Problem Analyzer has determined the node is down based on the following analysis: 1) 100% of the addresses assigned to this node are unreachable, and 2) The SNMP agent installed on this machine is not responding. At least two of the neighboring devices can be reached and are reporting problems with connectivity to this node.

Author Customer

You configure actions to automatically run at any point in the Incident lifecycle. For example, when an Incident is generated (Registered), you might want to automatically open a trouble ticket, send email, or page your network operator. NNMi supports running a Jython file, executable, or script as an action.

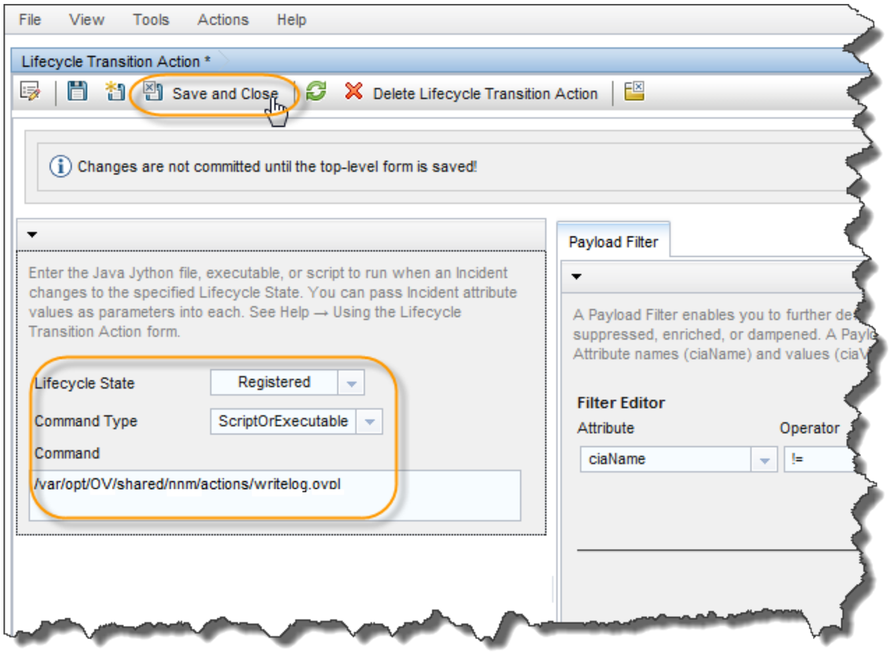
Note: Your configured actions are disabled until you click Enabled and Save this form.

Enabled □

Command Type	Command

4. Select the appropriate **Lifecycle State** (`Registered` in this example).
5. Set the **Command Type** to `ScriptOrExecutable`.
6. Enter the name of the command, including the complete path to the executable, and then click **Save and Close**.

Figure 40: Lifecycle Transition Action



Changes are not committed until the top-level form is saved!

Enter the Java Jython file, executable, or script to run when an Incident changes to the specified Lifecycle State. You can pass Incident attribute values as parameters into each. See Help → Using the Lifecycle Transition Action form.

Lifecycle State: Registered

Command Type: ScriptOrExecutable

Command: /var/opt/OV/shared/nnm/actions/writelog.ovpl

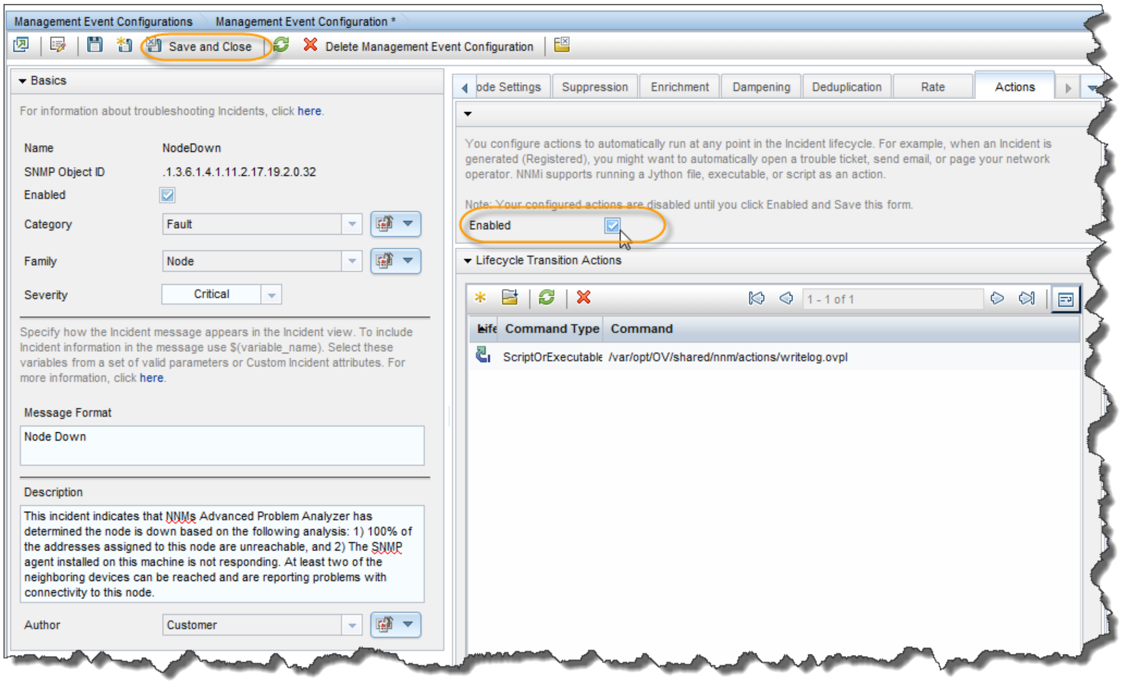
A Payload Filter enables you to further de suppressed, enriched, or dampened. A Payl Attribute names (ciaName) and values (ciaV

Attribute: ciaName

Operator: !=

7. Click the **Enabled** check box to enable the action.

Figure 41: Management Event Configuration: Actions Tab: Enable Action


Management Event Configurations
Management Event Configuration *
Save and Close
Delete Management Event Configuration
Basics
ode Settings
Suppression
Enrichment
Dampening
Deduplication
Rate
Actions
Lifecycle Transition Actions
1 - 1 of 1

For information about troubleshooting Incidents, click here.

Name	NodeDown
SNMP Object ID	.1.3.6.1.4.1.11.2.17.19.2.0.32
Enabled	☑
Category	Fault
Family	Node
Severity	Critical

Specify how the Incident message appears in the Incident view. To include Incident information in the message use $(variable_name). Select these variables from a set of valid parameters or Custom Incident attributes. For more information, click here.

Message Format

Node Down

Description

This incident indicates that NNMs Advanced Problem Analyzer has determined the node is down based on the following analysis: 1) 100% of the addresses assigned to this node are unreachable, and 2) The SNMP agent installed on this machine is not responding. At least two of the neighboring devices can be reached and are reporting problems with connectivity to this node.

Author: Customer

You configure actions to automatically run at any point in the Incident lifecycle. For example, when an Incident is generated (Registered), you might want to automatically open a trouble ticket, send email, or page your network operator. NNMi supports running a Jython file, executable, or script as an action.

Note: Your configured actions are disabled until you click Enabled and Save this form.

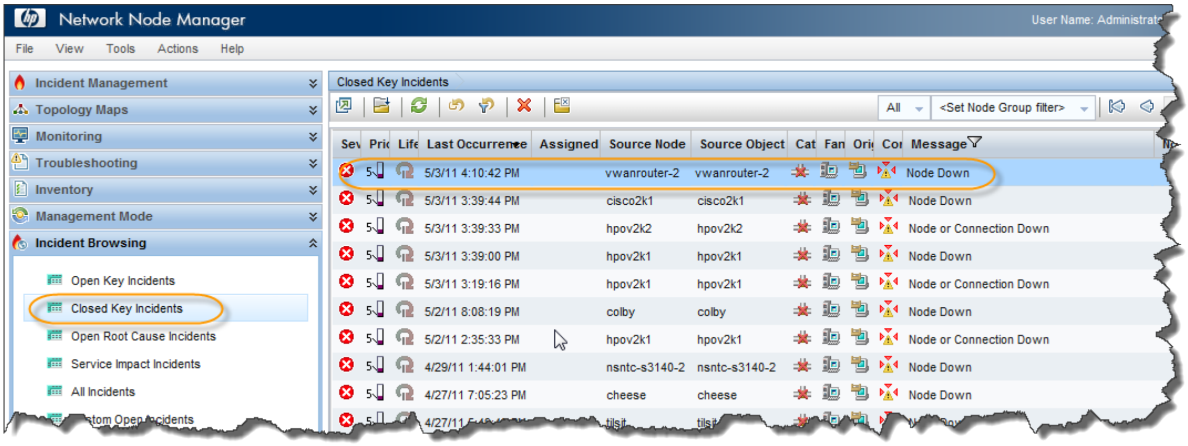
Enabled ☑

Life	Command Type	Command
	ScriptOrExecutable	/var/opt/OV/shared/nnm/actions/writelog.ovpl

Next, you need to test the action. The easiest way to do this is to look for a previous occurrence of the `NodeDown` incident:

1. From the workspace navigation panel, select the **Incident Browsing** workspace, and then click **Closed Key Incidents**.

Figure 42: Incident Browsing: Closed Key Incidents View



Closed Key Incidents

Pri	Last Occurrence	Assigned	Source Node	Source Object	Message
5	5/3/11 4:10:42 PM		vwanrouter-2	vwanrouter-2	Node Down
5	5/3/11 3:39:44 PM		cisco2k1	cisco2k1	Node Down
5	5/3/11 3:39:33 PM		hpov2k2	hpov2k2	Node or Connection Down
5	5/3/11 3:39:00 PM		hpov2k1	hpov2k1	Node Down
5	5/3/11 3:19:16 PM		hpov2k1	hpov2k1	Node or Connection Down
5	5/2/11 8:08:19 PM		colby	colby	Node Down
5	5/2/11 2:35:33 PM		hpov2k1	hpov2k1	Node or Connection Down
5	4/29/11 1:44:01 PM		nsntc-s3140-2	nsntc-s3140-2	Node Down
5	4/27/11 7:05:23 PM		cheese	cheese	Node Down
5	4/27/11		tilsit	tilsit	

2. Open a `NodeDown` incident that NNMi closed.

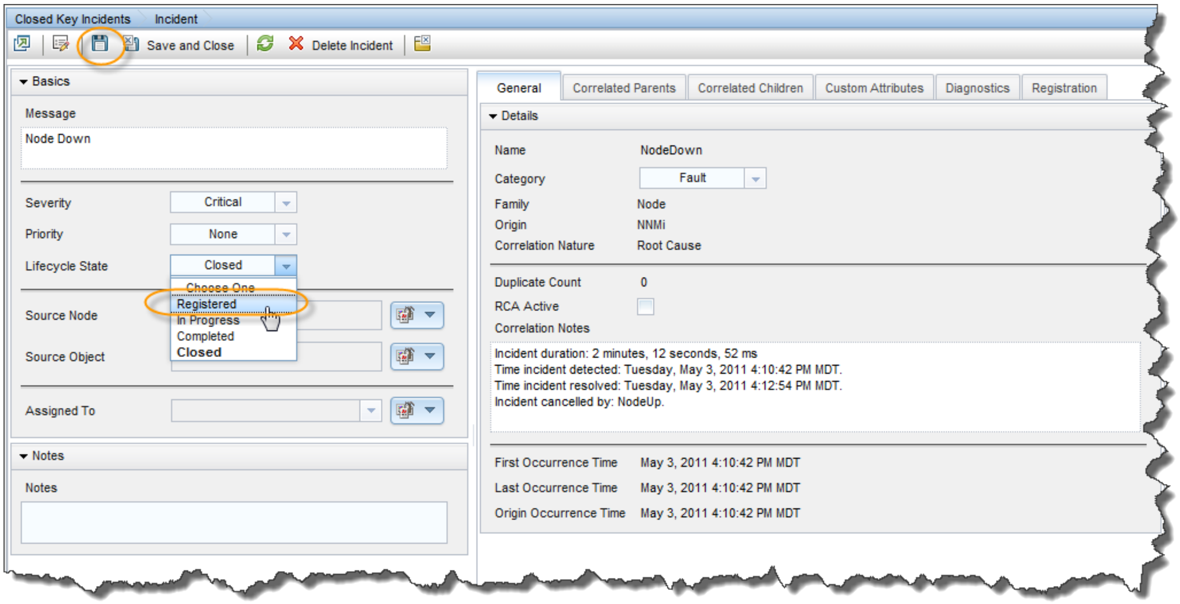
In this example `Closed` means that the interface is back up. NNMi automatically closes an incident when a fault is cleared. (You can re-open the incident by setting the **Lifecycle State** to `Registered`. After you take this action, NNMi behaves as if the incident is opened for the first time when executing actions.)

3. Set the **Lifecycle State** to `Registered`.

This causes your action to execute after you save this form (saving the **Lifecycle State** change). If you change the **Lifecycle State** without saving the change, NNMi takes no action.

4. Click **Save** after each **Lifecycle State** change.

Figure 43: Incident Form: Registered Lifecycle State



Message	Node Down
Severity	Critical
Priority	None
Lifecycle State	Closed
Source Node	
Source Object	
Assigned To	
Notes	

Name	NodeDown
Category	Fault
Family	Node
Origin	NNMi
Correlation Nature	Root Cause
Duplicate Count	0
RCA Active	□
Correlation Notes	

Incident duration: 2 minutes, 12 seconds, 52 ms
Time incident detected: Tuesday, May 3, 2011 4:10:42 PM MDT.
Time incident resolved: Tuesday, May 3, 2011 4:12:54 PM MDT.
Incident cancelled by: NodeUp.

First Occurrence Time	May 3, 2011 4:10:42 PM MDT
Last Occurrence Time	May 3, 2011 4:10:42 PM MDT
Origin Occurrence Time	May 3, 2011 4:10:42 PM MDT

After saving your change, verify your action's results. In this case, look at the log file associated with this script. After you finish testing, set the **Lifecycle State** back to `Closed`, and then save the incident to return it to its original state.

Configure the NNMi Console

Configure Node Groups

To enhance diagnostics, create Node Group maps, which show the nodes contained in a Node Group.

See *A Practical Example of Using Node Groups* in the *HP Network Node Manager i Software Deployment Reference,* available at http://h20230.www2.hp.com/selfsolve/manuals, for more information about configuring Node Groups.

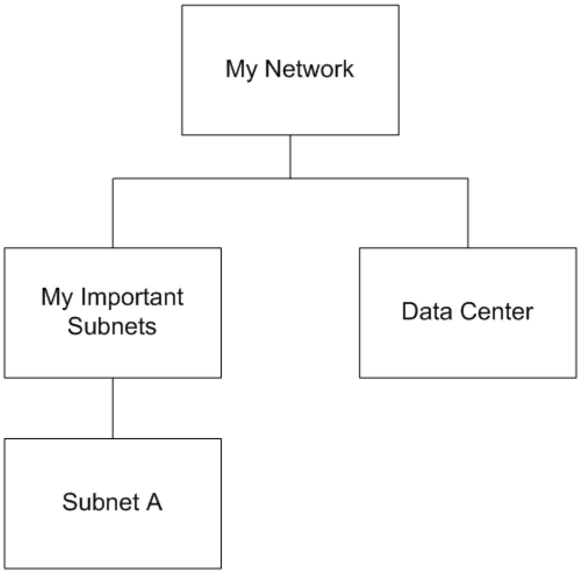
This example creates Node Groups for a few different subnets.

Tip: You want these Node Groups to refer to management addresses rather than addresses on the node. You also want these Node Groups to contain nodes based on names.

Note: The same node can be in multiple Node Groups.

The following diagram describes an example hierarchy of Node Groups:

Figure 44: Hierarchy of Groups



Subnet A = Management Address of 192.125.*.*

Data Center = Nodes that have a system name beginning with "data_center"

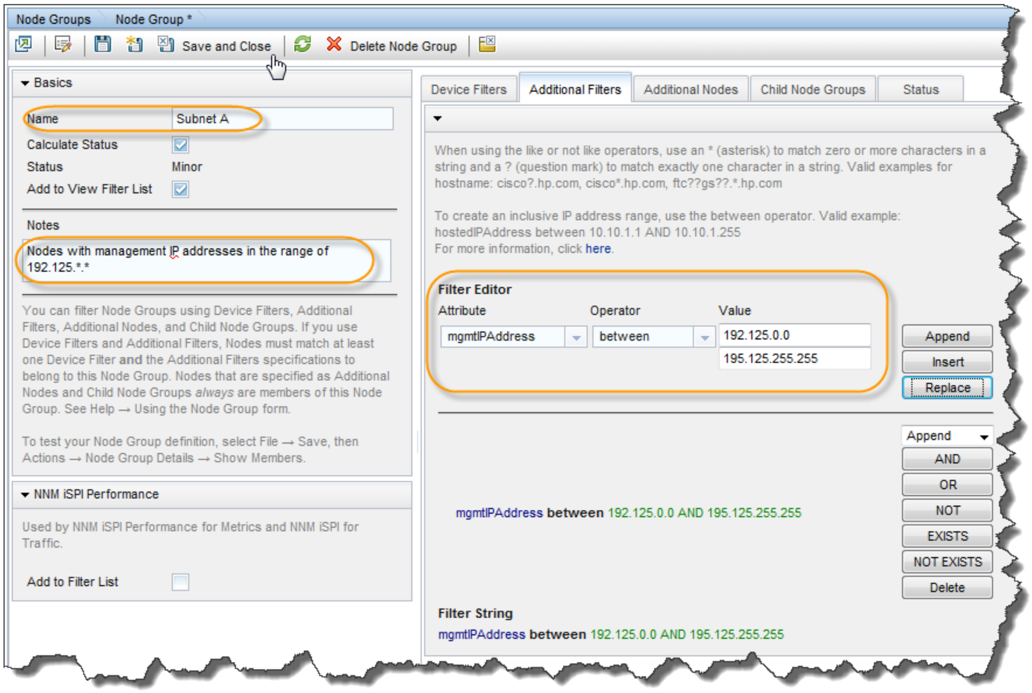
Note the following:

- Only the Subnet A Node Group and Data Center Node Group are populated with nodes. The My Important Subnets Node Group shows structure in the hierarchy and is populated only with a Child Node Group.
- It is easiest to work your way up the hierarchy.

1. Create the Subnet A Node Group as shown in the following example:

Tip: Notice the unique expression for IP address ranges.

Figure 45: Node Group: Basics



Basics

Name: Subnet A
Calculate Status: ☑
Status: Minor
Add to View Filter List: ☑

Notes: Nodes with management IP addresses in the range of 192.125.*.*

You can filter Node Groups using Device Filters, Additional Filters, Additional Nodes, and Child Node Groups. If you use Device Filters and Additional Filters, Nodes must match at least one Device Filter and the Additional Filters specifications to belong to this Node Group. Nodes that are specified as Additional Nodes and Child Node Groups *always* are members of this Node Group. See Help → Using the Node Group form.

To test your Node Group definition, select File → Save, then Actions → Node Group Details → Show Members.

NNM iSPI Performance

Used by NNM iSPI Performance for Metrics and NNM iSPI for Traffic.

Add to Filter List: □

When using the like or not like operators, use an * (asterisk) to match zero or more characters in a string and a ? (question mark) to match exactly one character in a string. Valid examples for hostname: cisco?.hp.com, cisco*.hp.com, ftc??gs??.*.hp.com

To create an inclusive IP address range, use the between operator. Valid example: hostedIPAddress between 10.10.1.1 AND 10.10.1.255
For more information, click here.

Filter Editor

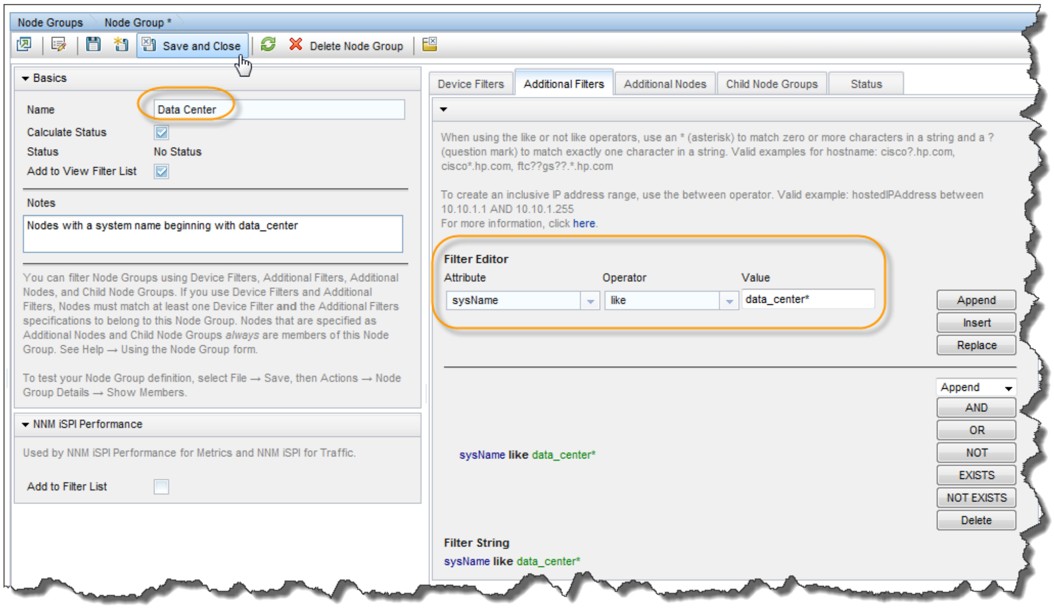
Attribute	Operator	Value
mgmtIPAddress	between	192.125.0.0 195.125.255.255

mgmtIPAddress **between** 192.125.0.0 AND 195.125.255.255

Filter String
mgmtIPAddress **between** 192.125.0.0 AND 195.125.255.255

2. Next, create the Data Center Node Group.

Figure 46: Node Group: Additional Filters Tab



Name: Data Center

Calculate Status ☑

Status: No Status

Add to View Filter List ☑

Notes: Nodes with a system name beginning with data_center

You can filter Node Groups using Device Filters, Additional Filters, Additional Nodes, and Child Node Groups. If you use Device Filters and Additional Filters, Nodes must match at least one Device Filter **and** the Additional Filters specifications to belong to this Node Group. Nodes that are specified as Additional Nodes and Child Node Groups *always* are members of this Node Group. See Help → Using the Node Group form.

To test your Node Group definition, select File → Save, then Actions → Node Group Details → Show Members.

Used by NNM iSPI Performance for Metrics and NNM iSPI for Traffic.

Add to Filter List □

When using the like or not like operators, use an * (asterisk) to match zero or more characters in a string and a ? (question mark) to match exactly one character in a string. Valid examples for hostname: cisco?.hp.com, cisco*.hp.com, ftc??gs??.*.hp.com

To create an inclusive IP address range, use the between operator. Valid example: hostedIPAddress between 10.10.1.1 AND 10.10.1.255
For more information, click here.

Filter Editor

Attribute	Operator	Value
sysName	like	data_center*

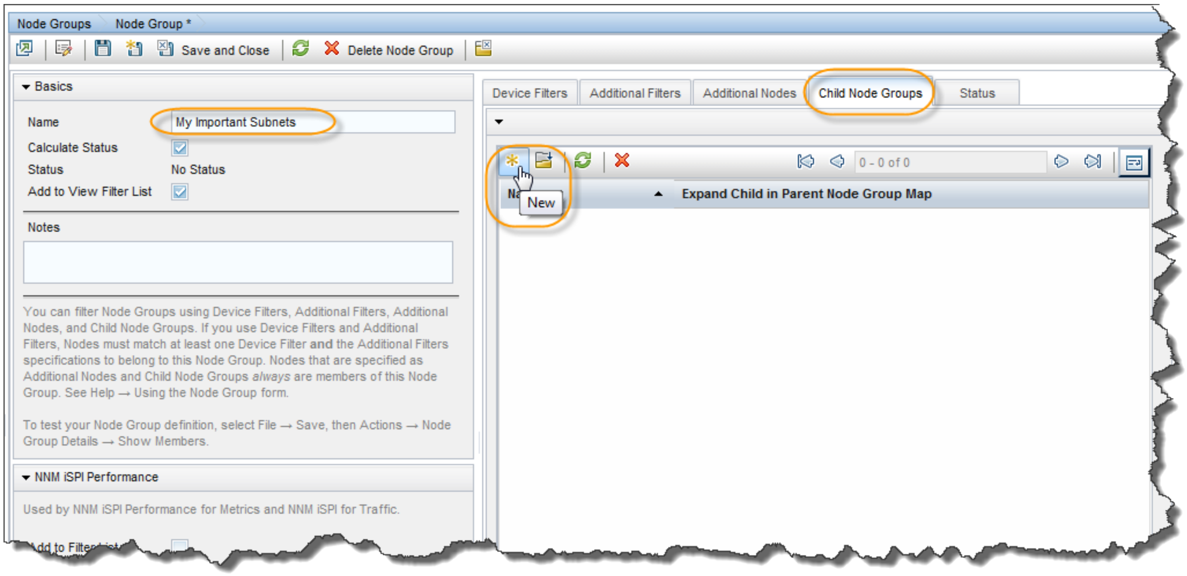
sysName **like** data_center*

Filter String
sysName **like** data_center*

Next, create the Node Group called My Important Subnets:

1. On the Node Groups form, click the ✳ icon.
2. Enter `My Important Subnets` in the **Name** text box.
3. Click the **Child Node Groups** tab, and then click the ✳ icon.

Figure 47: Node Group: Child Node Group Tab



Name: My Important Subnets

Calculate Status ☑

Status: No Status

Add to View Filter List ☑

Notes

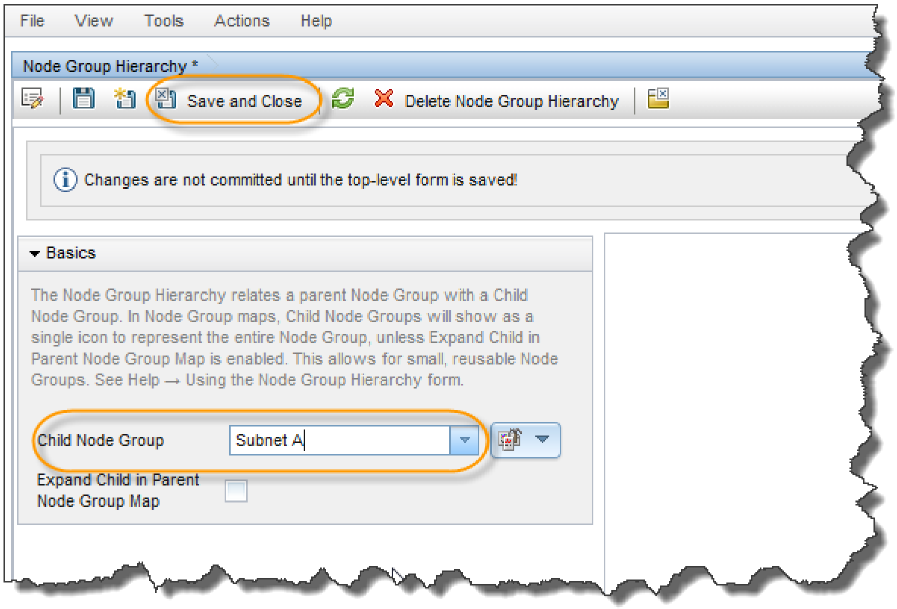
You can filter Node Groups using Device Filters, Additional Filters, Additional Nodes, and Child Node Groups. If you use Device Filters and Additional Filters, Nodes must match at least one Device Filter **and** the Additional Filters specifications to belong to this Node Group. Nodes that are specified as Additional Nodes and Child Node Groups *always* are members of this Node Group. See Help → Using the Node Group form.

To test your Node Group definition, select File → Save, then Actions → Node Group Details → Show Members.

Used by NNM iSPI Performance for Metrics and NNM iSPI for Traffic.

4. Click ▾, and then click **Quick Find**. Click the **Subnet A** Child Node Group, and then click **OK**.

Figure 48: Node Group Hierarchy: Assign Child Node Group Name



Changes are not committed until the top-level form is saved!

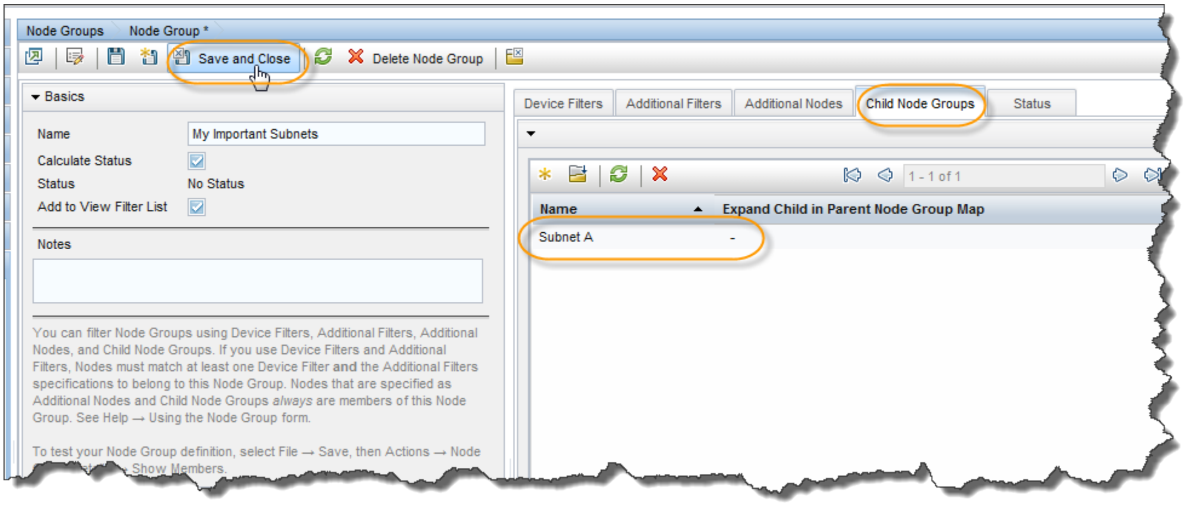
The Node Group Hierarchy relates a parent Node Group with a Child Node Group. In Node Group maps, Child Node Groups will show as a single icon to represent the entire Node Group, unless Expand Child in Parent Node Group Map is enabled. This allows for small, reusable Node Groups. See Help → Using the Node Group Hierarchy form.

Child Node Group: Subnet A

Expand Child in Parent Node Group Map: □

5. Click Save and Close. You just created a Child Node Group, Subnet A, for the My Important Subnets Node Group.

Figure 49: Child Node Groups Tab: Save and Close



Name: My Important Subnets

Calculate Status: ☑

Status: No Status

Add to View Filter List: ☑

Notes

You can filter Node Groups using Device Filters, Additional Filters, Additional Nodes, and Child Node Groups. If you use Device Filters and Additional Filters, Nodes must match at least one Device Filter and the Additional Filters specifications to belong to this Node Group. Nodes that are specified as Additional Nodes and Child Node Groups *always* are members of this Node Group. See Help → Using the Node Group form.

To test your Node Group definition, select File → Save, then Actions → Node Group Details → Show Members.

Name	Expand Child in Parent Node Group Map
Subnet A	-

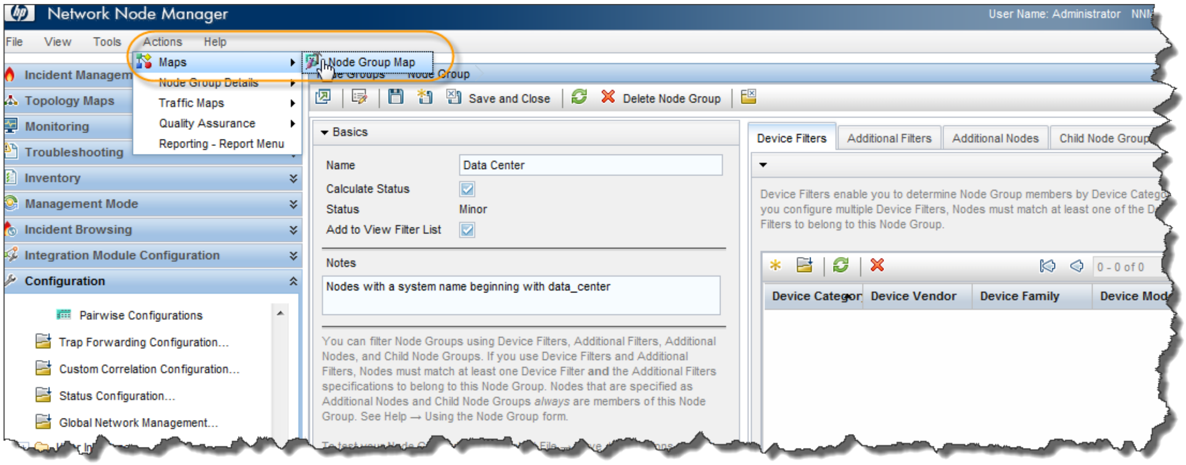
Finally, create the Node Group called My Network that includes the following Child Node Groups: Data Center and My Important Subnets.

Tip: Remember to test the membership after you save each Node Group by clicking **Actions > Node Group Details > Show Members**.

After you test the population of the Node Groups, create an initial instance of a map for each Node Group:

1. Click **Actions > Maps > Node Group Map** to open the map.

Figure 50: Actions: Map: Select Node Group Map



Name: Data Center

Calculate Status ☑

Status: Minor

Add to View Filter List ☑

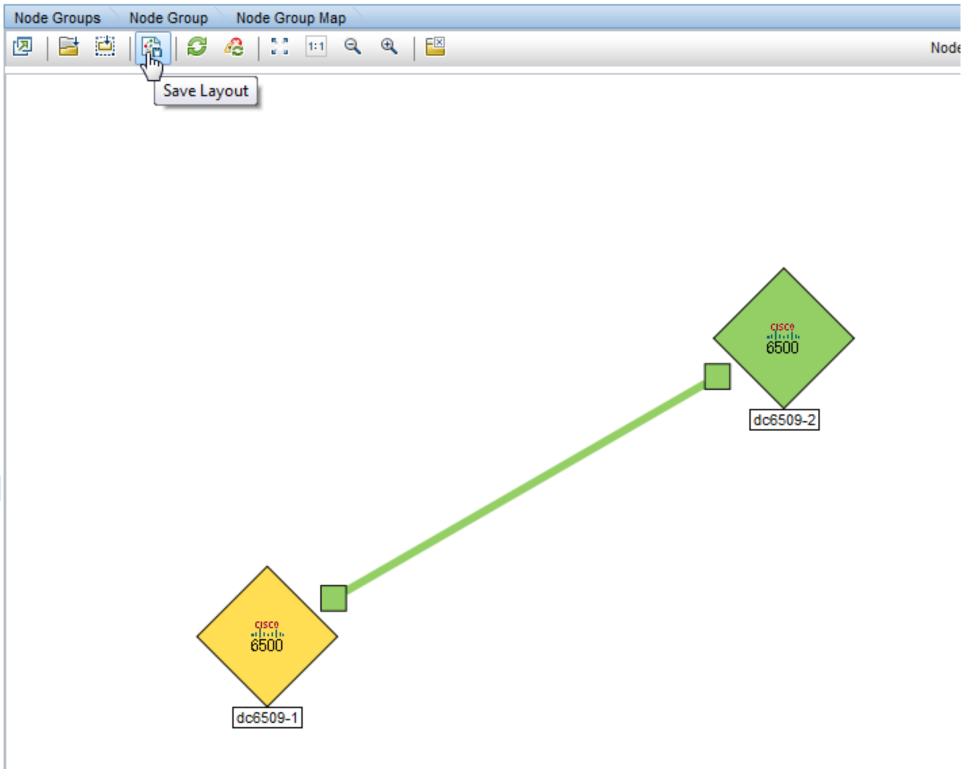
Notes: Nodes with a system name beginning with data_center

You can filter Node Groups using Device Filters, Additional Filters, Additional Nodes, and Child Node Groups. If you use Device Filters and Additional Filters, Nodes must match at least one Device Filter **and** the Additional Filters specifications to belong to this Node Group. Nodes that are specified as Additional Nodes and Child Node Groups *always* are members of this Node Group. See Help → Using the Node Group form.

Device Filters enable you to determine Node Group members by Device Categ you configure multiple Device Filters, Nodes must match at least one of the D Filters to belong to this Node Group.

2. Click **Save Layout**.

Figure 51: Node Group Map: Save Node Group Map Layout



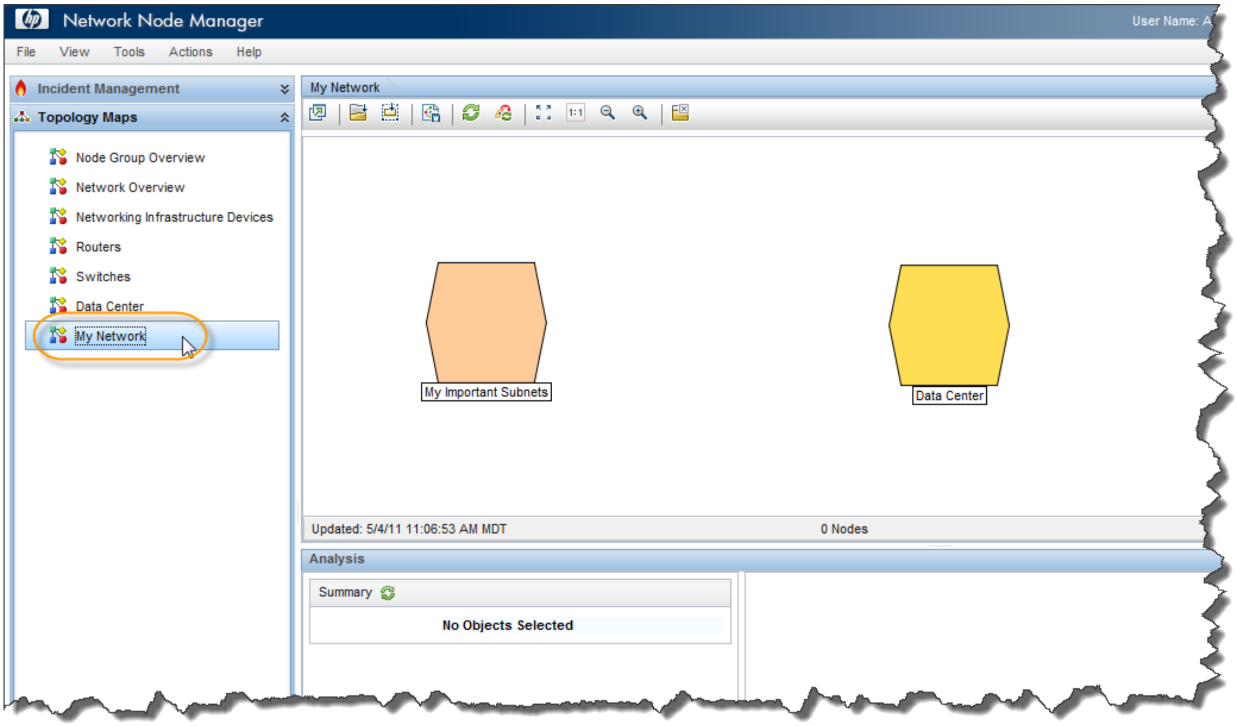
After you save the change, NNMi displays a message informing you that it created a Node Group map.

Repeat this same process for the entire hierarchy. It may take time for status to fully propagate to the Node Groups.

Configure the Node Group Map

You now have a map hierarchy that you can navigate within. From the workspace navigation panel, select the **Topology Maps** workspace. If you do not see the newly created Node Group Maps, try refreshing the browser or signing out and back into NNMi.

Figure 52: My Network Topology Map



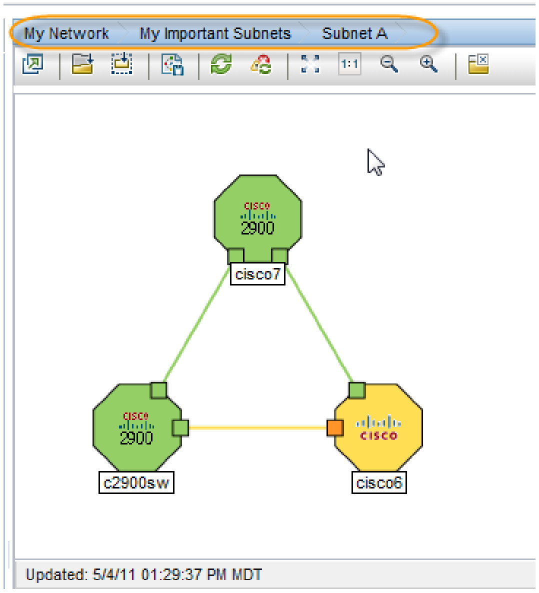
Updated: 5/4/11 11:06:53 AM MDT

0 Nodes

No Objects Selected

The bread crumb trail at the top indicates where you are in the hierarchy.

Figure 53: Bread Crumb Trail



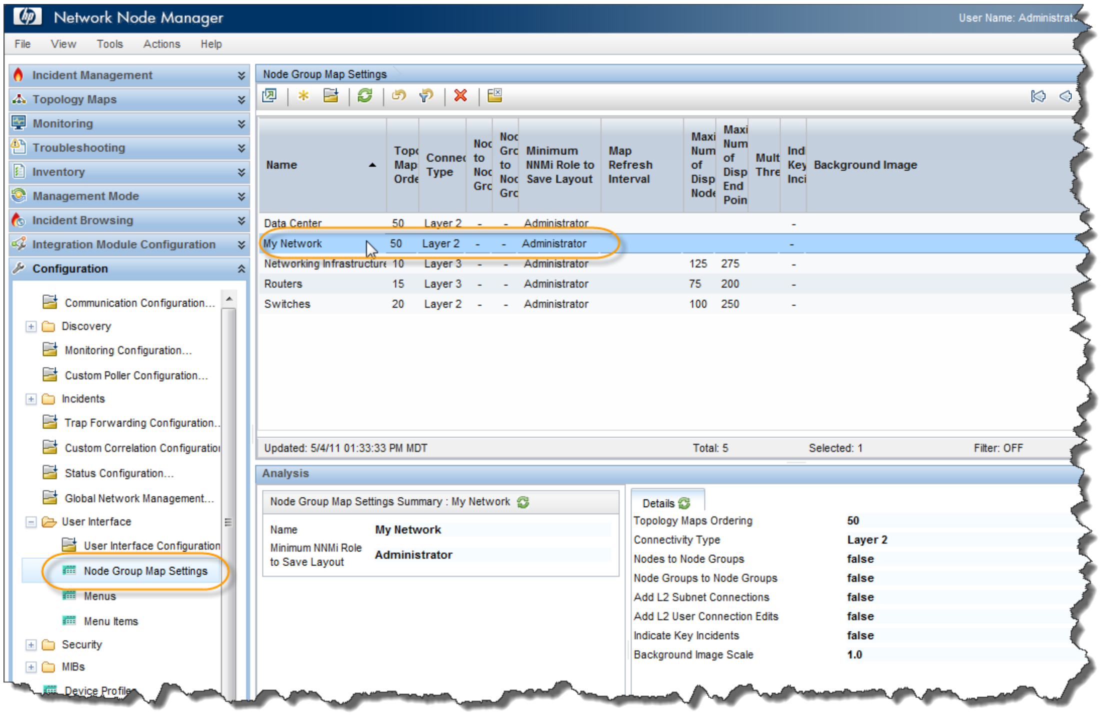
The Node Group Map Settings configuration option enables you to position Node Groups, add background graphics, and change connectivity options.

To place a background graphic on the map:

1. From the workspace navigation panel, select the **Configuration** workspace, expand the **User Interface** folder, and then click **Node Group Map Settings**.

Note the current Topology Map Ordering values. The lowest number currently used is `10`.

Figure 54: Node Group Map Settings



Name	Topc Map Orde	Connec Type	Noc to Noc Grc	Noc Grc to Noc Grc	Minimum NNMi Role to Save Layout	Map Refresh Interval	Maxi Num of Disp Node	Maxi Num of Disp End Poin	Mult Thre	Ind Key Inci	Background Image
Data Center	50	Layer 2	-	-	Administrator					-	
My Network	50	Layer 2	-	-	Administrator					-	
Networking Infrastructure	10	Layer 3	-	-	Administrator		125	275		-	
Routers	15	Layer 3	-	-	Administrator		75	200		-	
Switches	20	Layer 2	-	-	Administrator		100	250		-	

Updated: 5/4/11 01:33:33 PM MDT Total: 5 Selected: 1 Filter: OFF

Node Group Map Settings Summary : My Network

Name	**My Network**
Minimum NNMi Role to Save Layout	**Administrator**

Details

Topology Maps Ordering	**50**
Connectivity Type	**Layer 2**
Nodes to Node Groups	**false**
Node Groups to Node Groups	**false**
Add L2 Subnet Connections	**false**
Add L2 User Connection Edits	**false**
Indicate Key Incidents	**false**
Background Image Scale	**1.0**

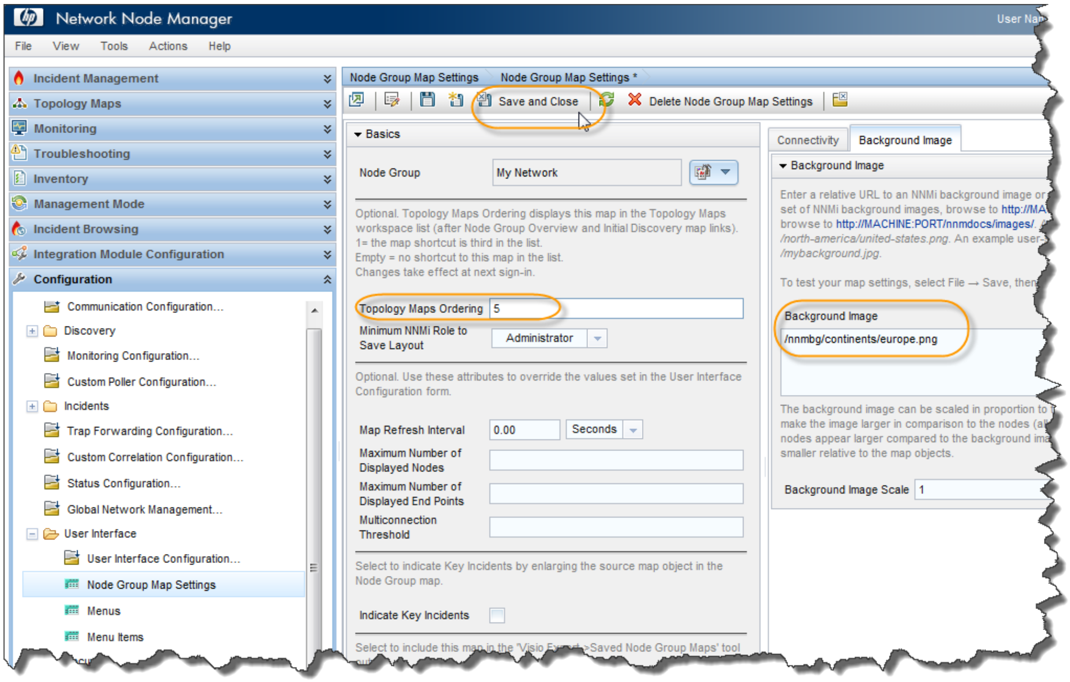
2. Double-click My Network.

3. Add a background image.

Tip: Use the local path, such as `/nnmbg/continents/europe.png`, rather than including `http://<machine name>` in front of the path. This enables the Application Failover feature to function properly.

4. Change the **Topology Maps Ordering** value to 5 so that this value is lower than the lowest value used in the previous example.
5. Click **Save and Close**.

Figure 55: Save Node Group Map Settings



Node Group: My Network

Optional. Topology Maps Ordering displays this map in the Topology Maps workspace list (after Node Group Overview and Initial Discovery map links).
1= the map shortcut is third in the list.
Empty = no shortcut to this map in the list.
Changes take effect at next sign-in.

Topology Maps Ordering: 5

Minimum NNMi Role to Save Layout: Administrator

Optional. Use these attributes to override the values set in the User Interface Configuration form.

Map Refresh Interval: 0.00 Seconds

Maximum Number of Displayed Nodes:

Maximum Number of Displayed End Points:

Multiconnection Threshold:

Select to indicate Key Incidents by enlarging the source map object in the Node Group map.

Indicate Key Incidents □

Select to include this map in the 'Visio Export->Saved Node Group Maps' tool

Background Image

Enter a relative URL to an NNMi background image or set of NNMi background images, browse to http://MA browse to http://MACHINE:PORT/nnmdocs/images/. /north-america/united-states.png. An example user- /mybackground.jpg.

To test your map settings, select File → Save, then

Background Image: /nnmbg/continents/europe.png

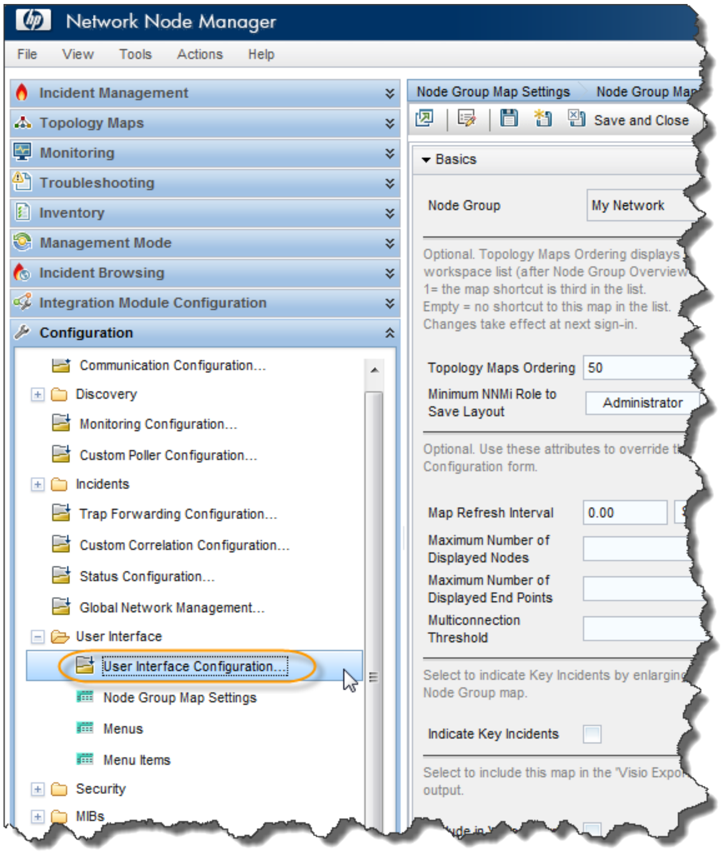
The background image can be scaled in proportion to make the image larger in comparison to the nodes (al nodes appear larger compared to the background ima smaller relative to the map objects.

Background Image Scale: 1

To specify the My Network map as the initial view:

6. Click **User Interface Configuration**.

Figure 56: Configuration: User Interface Configuration



Node Group: My Network

Optional. Topology Maps Ordering displays workspace list (after Node Group Overview 1= the map shortcut is third in the list. Empty = no shortcut to this map in the list. Changes take effect at next sign-in.

Topology Maps Ordering: 50

Minimum NNMi Role to Save Layout: Administrator

Optional. Use these attributes to override t Configuration form.

Map Refresh Interval: 0.00

Maximum Number of Displayed Nodes:

Maximum Number of Displayed End Points:

Multiconnection Threshold:

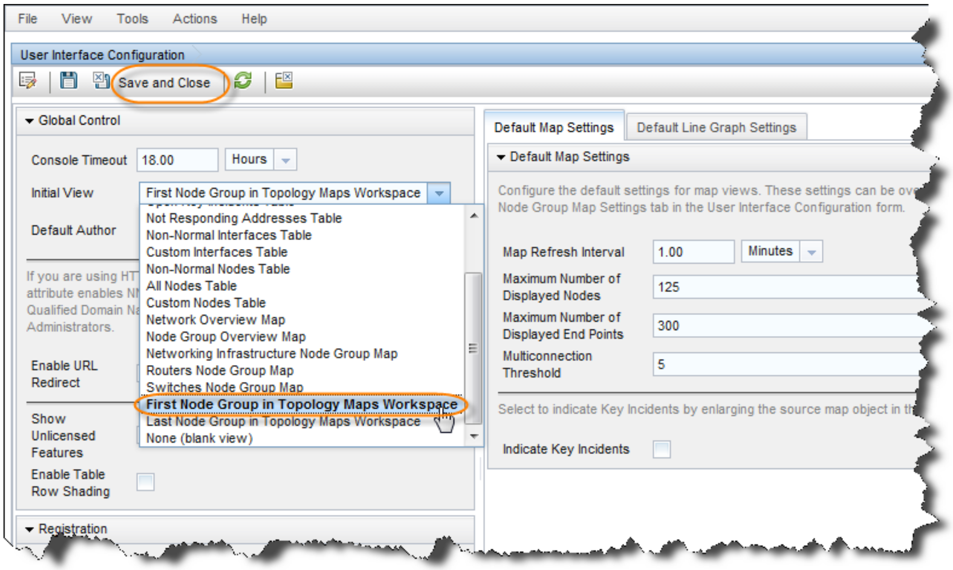
Select to indicate Key Incidents by enlarging Node Group map.

Indicate Key Incidents □

Select to include this map in the 'Visio Expo output.

7. Change the **Initial View** selection to the **First Node Group in Topology Maps Workspace**. This is the My Network map because we set the **Topology Maps Ordering** attribute value to 5.
8. Click **Save and Close**.

Figure 57: Save User Interface Configuration


File View Tools Actions Help
User Interface Configuration
Save and Close
Global Control
Default Map Settings
Default Line Graph Settings
Default Map Settings
Not Responding Addresses Table
Non-Normal Interfaces Table
Custom Interfaces Table
Non-Normal Nodes Table
All Nodes Table
Custom Nodes Table
Network Overview Map
Node Group Overview Map
Networking Infrastructure Node Group Map
Routers Node Group Map
Switches Node Group Map
First Node Group in Topology Maps Workspace
Last Node Group in Topology Maps Workspace
None (blank view)
Registration

Console Timeout: 18.00 Hours

Initial View: First Node Group in Topology Maps Workspace

Default Author

If you are using HT attribute enables N Qualified Domain N Administrators.

Enable URL Redirect

Show Unlicensed Features

Enable Table Row Shading □

Configure the default settings for map views. These settings can be ov Node Group Map Settings tab in the User Interface Configuration form.

Map Refresh Interval: 1.00 Minutes

Maximum Number of Displayed Nodes: 125

Maximum Number of Displayed End Points: 300

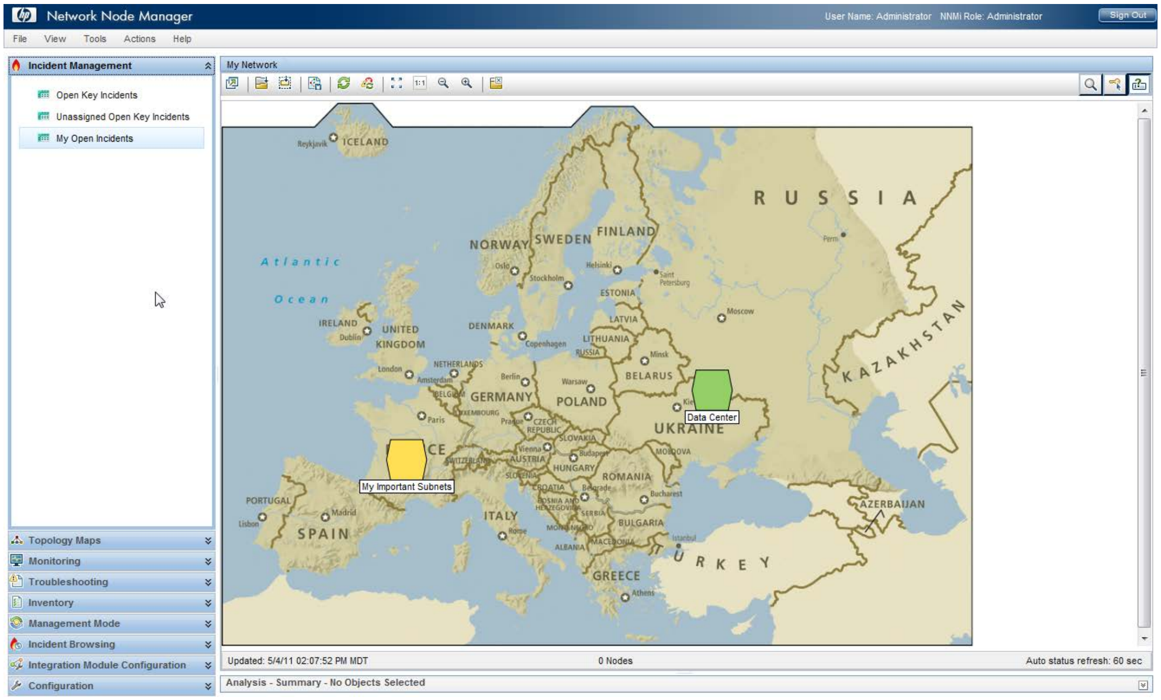
Multiconnection Threshold: 5

Select to indicate Key Incidents by enlarging the source map object in th

Indicate Key Incidents □

9. After you sign out, and then back into NNMi, the initial view is the My Network map.

Figure 58: My Network Map


Network Node Manager
User Name: Administrator NNMi Role: Administrator
Sign Out
File View Tools Actions Help
Incident Management
Open Key Incidents
Unassigned Open Key Incidents
My Open Incidents
Topology Maps
Monitoring
Troubleshooting
Inventory
Management Mode
Incident Browsing
Integration Module Configuration
Configuration
My Network
Data Center
My Important Subnets
Updated: 5/4/11 02:07:52 PM MDT
0 Nodes
Auto status refresh: 60 sec
Analysis - Summary - No Objects Selected

Maintain NNMi

Back up and Restore NNMi Data

NNMi provides backup and restore scripts to help protect your data.

The backup script is `nnmbackup.ovpl`. Use this script either *online* or *offline*. The online option enables you to run the script without stopping NNMi. Running this script generates a backup with a date and time stamp in the file name so you can specify the same target directory each time. This backup contains everything needed to restore your NNMi environment.

The following command shows an example of using the backup script:

```
nnmbackup.ovpl -type online -scope all -force -archive -target /var/tmp/mybackups
```

The previous command creates a file with a name similar to `nnm-bak-20110504145143.tar`.

The associated restore script is `nnmrestore.ovpl`. This command requires the backup file or directory created from the `nnmbackup.ovpl` script. To run this script, you must stop NNMi using the **`ovstop -c`** command.

An example `nnmrestore.ovpl` script usage is:

```
nnmrestore.ovpl -force -source /var/tmp/mybackups/nnm-bak-20110504145143.tar
```

The source directory should contain all of the files from the backup or the single tar file. If the source is a tar file, the script extracts the tar file to a temporary folder in the current working directory. The script removes the temporary folder after it completes the restore.

Caution: Never restore a backup across NNMi patch versions or restore a backup from a previous patch level of NNMi.

For example, in the following scenario, you should not restore the backup from the NNMi management running patch 4 onto the patch 5 code. This will cause fatal errors for NNMi:

- Patch 4 is running on your NNMi management server.
- After you run a backup, you upgrade to patch 5.

Tip: Track the version of the patch you are running in the backups by using a naming convention for the directories. For example, name the backup directory `patch4`.

Export and Import NNMi Configurations

Configuring NNMi is one of the most important tasks you do. Although your configuration is backed up as part of the `nnmbackup.ovpl` and `nnmbackupembdb.ovpl` scripts, consider using the `nnmconfigexport.ovpl` and `nnmconfigexport.ovpl` scripts included in NNMi. These scripts provide flexibility when it comes to restoring NNMi configuration. Using these scripts, you can:

- take a snapshot of the present NNMi configuration
- divide the configuration into small pieces
- restore just one piece of NNMi configuration if you need to revert back to a recent snapshot

For example, to create several Node Groups, use the export script to take a snapshot of the configuration at strategic points along the way so you can revert back if you make a significant mistake.

The export script is `nnmconfigexport.ovpl`. Use the `nnmconfigexport.ovpl` script to specify a configuration area, such as discovery, Node Groups, incidents, and many others. NNMi also provides an `all` option to export all of the configuration information.

See the `nnmconfigexport.ovpl` reference page or the UNIX manpage for details.

An example `nnmconfigexport.ovpl` script usage is listed below:

```
nnmconfigexport.ovpl -c nodegroup -f /tmp
```

In this example, NNMi displays the following message:

```
Successfully exported /tmp/nodegroup.xml.
```

Each exported configuration corresponds to one configuration area in the NNMi console.

Note: The `nnmconfigexport.ovpl` script does not generate a date and time stamp on the files. If you want to automate this command, put the date and time stamp in the directory name.

To restore the configuration, use the `nnmconfigimport.ovpl` script.

Tip: You do not need to specify a configuration area because this is implied by the file contents.

An example `nnmconfigexport.ovpl` script usage is listed below:

```
nnmconfigimport.ovpl -f /tmp/nodegroup.xml
```

As with the `nnmbackup.ovpl` and `nnmbackupembdb.ovpl` scripts, do not use these scripts across patch versions. NNMi validates the configuration file and rejects it during the import if it is invalid for the current version of NNMi.

Caution: The `nnmconfigimport.ovpl` script overrides the current configuration if the format is correct.

Note: NNMi does not support importing configurations from other NNMi management servers. Therefore, you cannot create a configuration export on one NNMi management server and import it on another server. Only a full backup (`nnmbackup.ovpl`) can be transferred between servers.

Trim Traps from the Database

Traps that pass all of the NNMi filters are eventually stored in the NNMi database. Traps can come in high volume and affect NNMi performance.

Tip: Regularly trim traps from your NNMi database using the `nnmtrimincidents.ovpl` script. You can archive these traps if necessary.

An example `nnmtrimincidents.ovpl` script usage is listed below:

```
nnmtrimincidents.ovpl -age 1 -incr weeks -origin SnmpTrap -trimOnly -quiet
```

This example usage trims any traps older than one week. This usage does not archive the traps. See the `nnmtrimincidents.ovpl` reference page or the UNIX manpage for more options.

Tip: Use `nnmtrimincidents.ovpl` in a cron job to clear out old unnecessary trap incidents on a regular basis.

Note: NNMi eventually forces you to trim traps from the NNMi database by stopping storage of traps after it reaches a limit of 100,000 traps in the NNMi database.

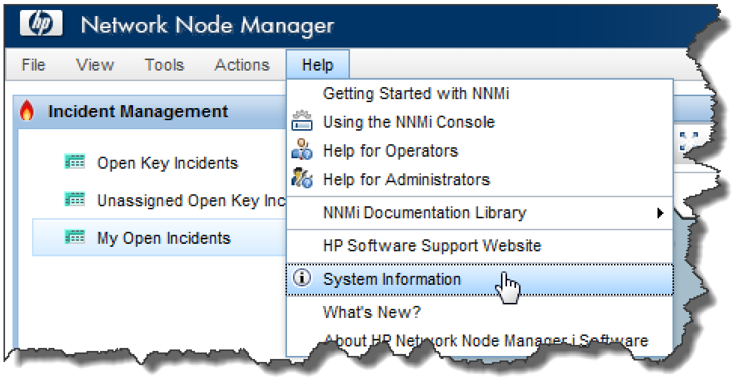
This reference to the NNMi database is not the same as the trap datastore. See the *Step- by-Step Guide to Incident Management*, available at http://h20230.www2.hp.com/selfsolve/manuals, for more information.

Check NNMi Health

You can check the general health of NNMi with a few different tools.

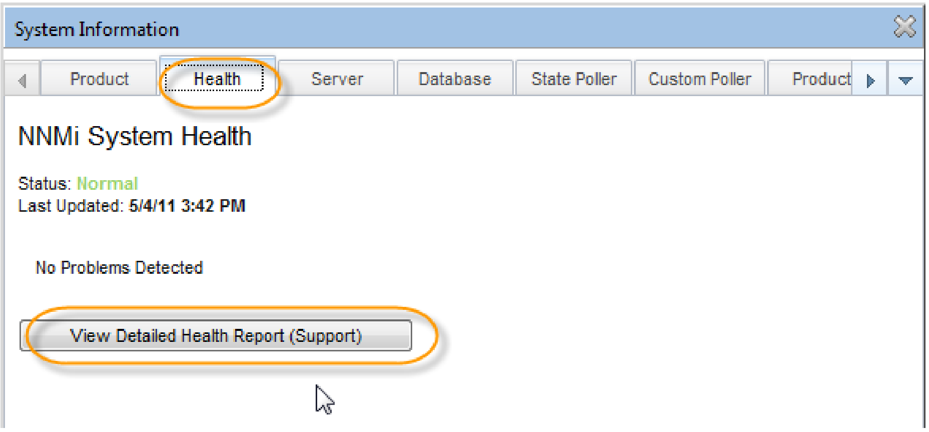
From the NNMi console, click **Help > System Information** for a listing of some important information.

Figure 59: Help: System Information



The best place to view the health of NNMi is in the **Health** tab. If NNMi identifies a health issue, it changes status and presents the reasons for the status in this report.

Figure 60: System Information: Health Tab



NNMi System Health

Status: Normal
Last Updated: 5/4/11 3:42 PM

No Problems Detected

Best Practices

Some additional recommendations that you might want to consider:

- **NNMi Embedded Database**. Use NNMi's embedded database, even for large scale. Tests show that Postgres is highly scalable. You do not need to consider Oracle just because you have a large network. Postgres is highly reliable and is the preferred database for NNMi. Postgres is embedded into NNMi and NNMi provides any required tools you need.
- **SNMP Timeout Configuration**. Use caution when adjusting the SNMP timeout configuration. Timeout values increment with each timeout and can grow quickly beyond your original intention.
- **Node Status**. From the NNMi console, click one of the topology map selections. After you see the resulting display, double-click one of the nodes to open a node form. Click the **Conclusions** tab and review the data to better understand why the current status is set for the node.
- **Node Group Map Settings**. Reduce the number of connections between Node Groups using the `End Points Filter` in the **Node Group Map Settings** form. Highly connected maps display slowly and NNMi drops connections, if necessary, on the map.
- **SNMP Community Strings**. Do not use an @ symbol in your SNMP community strings. This is a reserved character for Cisco devices and causes unpredictable NNMi behavior.

Example Usage Scenarios

This section presents three usage scenarios. These scenarios assume that you have only NNMi available.

Management by Exception

NNMi identifies root cause problems associated with a network fault as Key Incidents.

To view all of the Open Key Incidents:

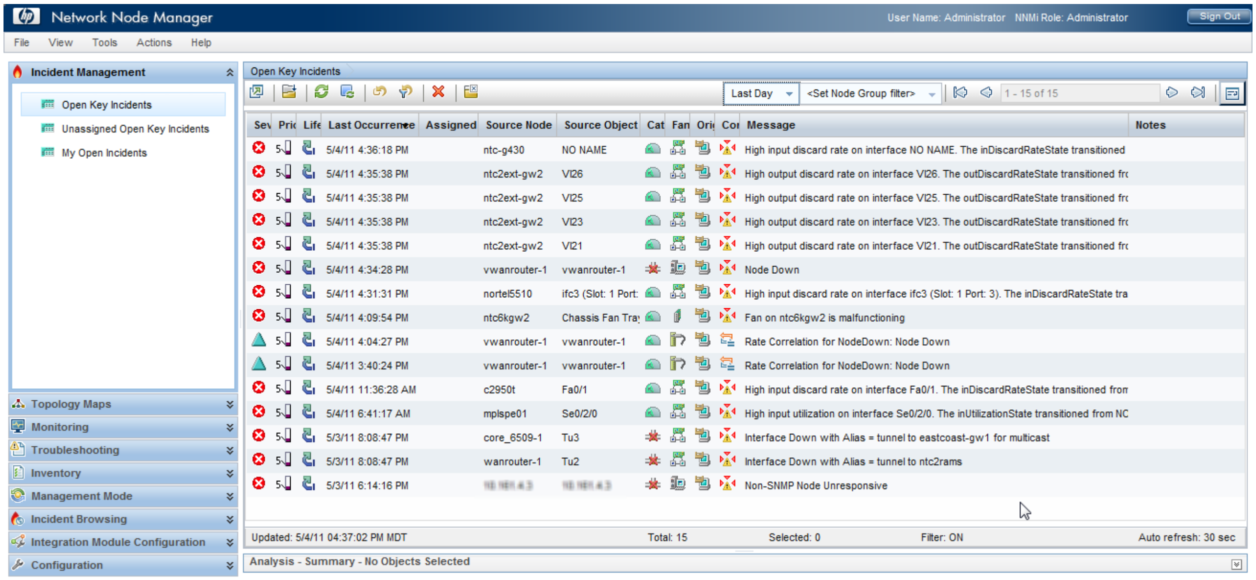
1. From the workspace navigation panel, select the **Incident Management** workspace.
2. Click **Open Key Incidents**.

NNMi displays all of the outstanding key incidents in your network and updates this list every 30 seconds. See "Help for Operators" in the NNMi help for more information about key incidents.

Tip: NNMi filters the Open Key Incidents view by time. Use the drop-down menu to select an appropriate time value.

The following example displays all of the open key incidents that occurred in the last day. Using this example, you can see that one node went down in the last 24 hours.

Figure 61: Open Key Incidents



Sev	Pri	Last Occurrence	Assigned	Source Node	Source Object	Message	Notes
⊗	5	5/4/11 4:36:18 PM		ntc-g430	NO NAME	High input discard rate on interface NO NAME. The inDiscardRateState transitioned	
⊗	5	5/4/11 4:35:38 PM		ntc2ext-gw2	Vl26	High output discard rate on interface Vl26. The outDiscardRateState transitioned frc	
⊗	5	5/4/11 4:35:38 PM		ntc2ext-gw2	Vl25	High output discard rate on interface Vl25. The outDiscardRateState transitioned frc	
⊗	5	5/4/11 4:35:38 PM		ntc2ext-gw2	Vl23	High output discard rate on interface Vl23. The outDiscardRateState transitioned frc	
⊗	5	5/4/11 4:35:38 PM		ntc2ext-gw2	Vl21	High output discard rate on interface Vl21. The outDiscardRateState transitioned frc	
⊗	5	5/4/11 4:34:28 PM		vwanrouter-1	vwanrouter-1	Node Down	
⊗	5	5/4/11 4:31:31 PM		nortel5510	ifc3 (Slot: 1 Port:	High input discard rate on interface ifc3 (Slot: 1 Port: 3). The inDiscardRateState tra	
⊗	5	5/4/11 4:09:54 PM		ntc6kgw2	Chassis Fan Tray	Fan on ntc6kgw2 is malfunctioning	
▲	5	5/4/11 4:04:27 PM		vwanrouter-1	vwanrouter-1	Rate Correlation for NodeDown: Node Down	
▲	5	5/4/11 3:40:24 PM		vwanrouter-1	vwanrouter-1	Rate Correlation for NodeDown: Node Down	
⊗	5	5/4/11 11:36:28 AM		c2950t	Fa0/1	High input discard rate on interface Fa0/1. The inDiscardRateState transitioned from	
⊗	5	5/4/11 6:41:17 AM		mplspe01	Se0/2/0	High input utilization on interface Se0/2/0. The inUtilizationState transitioned from NC	
⊗	5	5/3/11 8:08:47 PM		core_6509-1	Tu3	Interface Down with Alias = tunnel to eastcoast-gw1 for multicast	
⊗	5	5/3/11 8:08:47 PM		wanrouter-1	Tu2	Interface Down with Alias = tunnel to ntc2rams	
⊗	5	5/3/11 6:14:16 PM		[redacted]	[redacted]	Non-SNMP Node Unresponsive	

Updated: 5/4/11 04:37:02 PM MDT Total: 15 Selected: 0 Filter: ON Auto refresh: 30 sec

Analysis - Summary - No Objects Selected

By monitoring the Open Key Incidents view, you can pinpoint the exact cause of a network problem and begin working toward a solution. This is *management by exception* because the incident view shows these *exceptions* (or outages).

The *management by exception* approach includes the following advantages:

- You can quickly see the root cause of the problem.
- You can easily identify the source of the problem as the *source object*, such as an interface, address, node, or other possible sources.
- NNMi can forward Key Incidents to other products, such as HP Operations Manager (HP OM).

Note the following when using the *management by exception* approach:

- A Node Down incident shows only the root cause; however, the node being down could affect connectivity to many other nodes. Check the **Topology Maps** views to assist you in recognizing the scope of an outage. (See the following section, *Map-Based Management*, for more information.)
- Not all Node Down incidents are of equal importance. You will want additional tools, such as the **Topology Maps** view and Node Group names, to assist you in prioritizing these incidents. (See the following section, *Map-Based Management*, for more information.)

Map-Based Management

Another method of network management is to create maps to monitor node status changes. These maps can be arranged in many ways, including geography or building.

All of the maps available from the **Topology Maps** workspace are arranged by Node Groups. Note the following about Node Group maps:

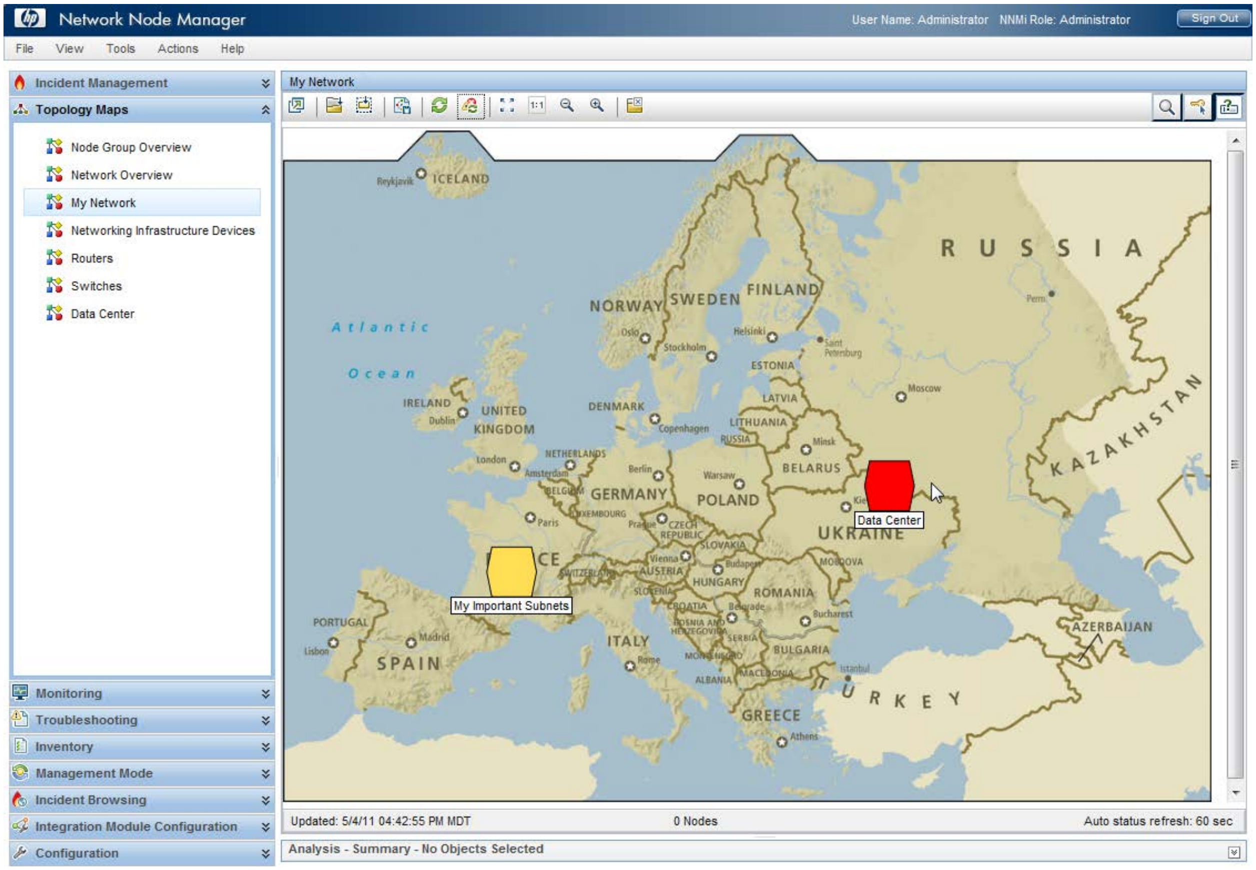
- The status is propagated from the *Child Node Group nodes* up to the parent Node Group maps.
- By default, NNMi propagates the most critical node status in the Node Group up the hierarchy. This enables you to monitor node status from a high level.
- When a top-level Node Group map changes color from green to red, yellow, or orange, you can navigate into the Node Group maps until you find the problem node. After you reach the problem node, you can take actions similar to those described in the previous section to troubleshoot the problem.
- Similar to incidents, nodes and interfaces can be annotated with notes if you want to keep a log of information about the troubleshooting progress.

The following screen capture shows an example of the My Network map with a problem that you need to correct. In this example, double-click the Node Group icon to find the faulting node.

Tip: The NNMi administrator can specify the *default map* that NNMi displays after initial sign in.

To navigate to a Node Group map from the NNMi console, click **Topology Maps**, and then select the map name of interest.

Figure 62: My Network Topology Map



The *map-based management* approach includes the following advantages:

- You can easily scope the outage. It becomes obvious quickly if other nodes are affected based on the status of neighboring nodes.
- You can easily identify the affected location. This approach helps you decide what to work on first.

When using the *map-based management* approach note the following:

- To find the source of the problem, open the node and go to the **Conclusions** tab to determine the problem.
- If one node is already down in a Node Group, NNMi does not indicate that one or more additional nodes have gone down in the same Node Group.
- NNMi does not propagate node status to other tools such as HP Operations Manager (HP OM).

List-Based Management

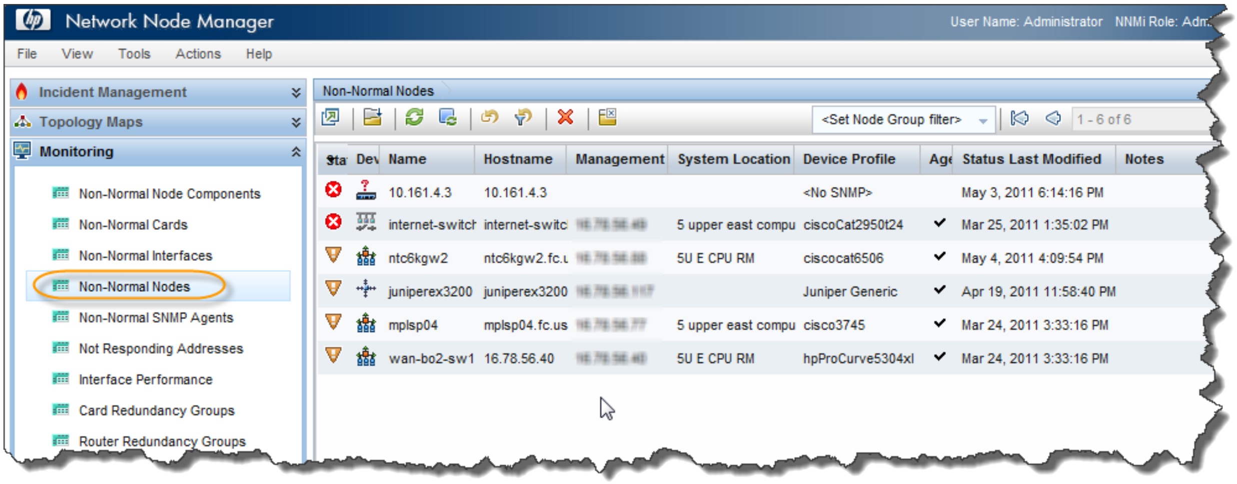
NNMi also enables you to manage your network from a dynamic list. NNMi provides dynamically updated tables that show nodes or interfaces experiencing problems. NNMi usually updates this list every 15 seconds. From this list, you can use tools, as described in the previous sections, to diagnose and fix problems. Because this list is dynamic, NNMi removes the nodes or interfaces from this list as the nodes or interfaces return to a Normal status.

For example, to display all the nodes having a non-normal status:

1. From the workspace navigation panel, select the **Monitoring** workspace.
2. Click **Non-Normal Nodes**.

As shown in the following example, NNMi displays all nodes that have a status other than Normal.

Figure 63: Non-Normal Nodes



Sta	Dev	Name	Hostname	Management	System Location	Device Profile	Age	Status Last Modified	Notes
✖		10.161.4.3	10.161.4.3			<No SNMP>		May 3, 2011 6:14:16 PM	
✖		internet-switch	internet-switc	[redacted]	5 upper east compu	ciscoCat2950t24	✓	Mar 25, 2011 1:35:02 PM	
▽		ntc6kgw2	ntc6kgw2.fc.u	[redacted]	5U E CPU RM	ciscocat6506	✓	May 4, 2011 4:09:54 PM	
▽		juniperex3200	juniperex3200	[redacted]		Juniper Generic	✓	Apr 19, 2011 11:58:40 PM	
▽		mplsp04	mplsp04.fc.us	[redacted]	5 upper east compu	cisco3745	✓	Mar 24, 2011 3:33:16 PM	
▽		wan-bo2-sw1	16.78.56.40	[redacted]	5U E CPU RM	hpProCurve5304xl	✓	Mar 24, 2011 3:33:16 PM	

The *list-based management* approach includes the following advantages:

- You know how many nodes or interfaces you need to investigate.
- You do not need to navigate into NNMi maps to troubleshoot your network.

When using list-based management, note the following:

- NNMi includes up to five entries in the status history.
- NNMi does not assign a Critical status to nodes that are "in the shadow" of a node that is down. See "Help for Operators" in the NNMi help for more information.
- The list-based view does not indicate where the node is physically located.
- NNMi does not propagate node status to other tools such as HP Operations Manager (HP OM).

Conclusion

This document described an NNMi deployment on a small test network. It included information about installing a license, creating users, configuring communication, discovery, incidents, traps, actions, and the NNMi console. This document also explained maintenance tasks for NNMi and how to monitor NNMi health. It also provided some best practices and explained some possible usage scenarios for NNMi.

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

© Copyright 2009–2011 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

For the full Oracle license text, see the license-agreements directory on the NNMi product DVD.

Acknowledgements

This product includes software developed by the Apache Software Foundation.

(http://www.apache.org)

This product includes software developed by the Indiana University Extreme! Lab.

(http://www.extreme.indiana.edu)

Support

Visit the HP Software Support web site at:

www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp