# Technical white paper Step-by-Step Guide to Deploying **NNMi**



### Network Node Manager i Software 10.00

May 2014

## Contents

Purpose	3
The Basic Steps: A Roadmap	3
Apply the License	5
Back up the Original Configuration	5
Sign in to NNMi and Create Users	5
Initial Sign In	5
Create User Accounts and Roles	6
Set up Communication Configuration	8
Configure Discovery	11
Configure Monitoring	16
Create an Interface Group for Monitoring	
Apply Monitoring to an Interface Group	20
Test the Monitoring Settings	24
Monitoring Exceptions	26
Configure Incidents, Traps, and Automatic Actions	27
Configure Incidents	27
Configure Traps	29
Configure Automatic Actions	
Configure the NNMi Console	35
Configure Node Groups	
Configure the Node Group Maps	42
Maintain NNMi	46
Back up and Restore NNMi Data	46
Export and Import NNMi Configurations	
Trim Traps from the Database	
Check NNMi Health	47
Best Practices	

Example Usage Scenarios	.49
Management by Exception	.49
Map-Based Management	. 50
List-Based Management	.51
Conclusion	. 52
We appreciate your feedback!	. 53
Legal Notices	.54
Warranty	.54
Restricted Rights Legend	.54
Copyright Notices	.54
Trademark Notices	.54
Oracle Technology — Notice of Restricted Rights	.54
Acknowledgements	.54
Support	.54

### Purpose

This document describes deploying a new NNMi 10.00 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.

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

### 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.

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

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:

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

To install the NNMi iSPIs, see the following documents, available http://h20230.www2.hp.com/selfsolve/manuals:

- NNM iSPI Performance for Metrics Interactive Installation Guide
- NNM iSPI Performance for Traffic Interactive Installation Guide
- NNM iSPI Performance for QA Interactive Installation Guide
- NNM iSPI Performance for QA Intelligent Response Agent Interactive Installation Guide

To deploy the NNMi iSPIs, see the following documents, available http://h20230.www2.hp.com/selfsolve/manuals:

- NNM iSPI Performance for Metrics Deployment Reference
- NNM iSPI Performance for Traffic Deployment Reference
- NNM iSPI Performance for QA Deployment Reference

### **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 is for NNMi Ultimate and enables NNMi for 250 nodes. If you install NNMi Premium at a later date, some functionality is lost. For information about NNMi Ultimate and NNMi Premium features, see the *HP Network Node Manager i Software Release Notes*, available at http://h20230.www2.hp.com/selfsolve/manuals.

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.
- 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

<b>(p</b> )	Network Node Manager		
	User Name	system	
	Password		
		Sign In Clear	
Java		© Copyright 1990-2014 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.

You should see the **Security Wizard Welcome Page**.

Figure 2: Security Wizard: Welcome Page

Metwork Node Manager		User Name: system NNMi Role: Administrator Sign Out
<u>File T</u> ools <u>H</u> elp		
🕐 Dashboards 🛛 😵	Security Wizard *	
👌 Incident Management 🛛 🕹 🕹	a Welcome	Welcome to the Configuring Security Wizard
A. Topology Maps      Second State S	Map User Accounts and Map User Groups and S Assign Nodes to Securi	The Configuring Security Wizard enables you to configure User Accounts, User Groups, and Security Groups.
Security Security Wizard Wiser Accounts User Groups Security Groups Security Groups Security Group Mappings MBs Device Profiles	< <u> </u>	NNMI provides a Default Tenant and Default Security Group. Unless the NNMI administrator changes the default configuration, each time Sprind 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 Witzard 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 User Groups** and click the \* icon.

### Figure 3: Security Wizard: Create User Account

Metwork Node Manager					User Name: system	NNMi Role: Administra	tor Sign Out
File Tools Help							
Dashboards	≈	Security Wizard *					
👌 Incident Management	≈	🔉 Welcome	Use this page to do any of Create and Delete User Acco		te User Groups, Assign	User Accounts to Us	er Groups, Assign
🛧 Topology Maps	岽	🎄 Map User Accounts and User Groups	User Groups to User Accoun User Accounts	ts, Remove User Acco User Account Map		User Groups	
Monitoring	≈	🔉 Map User Groups and Security Groups	* 🗙 🗟	×	Jinga	* 🗙 🗟	
Troubleshooting	*	lacktrian Assign Nodes to Security Groups		User Account	User Group	Name	Display Name
Inventory	*	🖇 View Summary of Changes	Create User Account		outri droup		NNMi
Management Mode	≈					admin	Administrators
lncident Browsing	*					level1	NNMi Level 1 Operators
Integration Module Configuration	*					level2	NNMi Level 2
Configuration     Status Configuration	*						Operators
Global Network Management						client	NNMi Web Service Clients
+ 🗀 User Interface	11					guest	NNMi Guest Users
🖃 🗁 Security						globalops	NNMi Global Operators
🗳 Security Wizard							
User Accounts							
User Groups			L				
III User Account Mappings		۰			<previo< th=""><th>us Next&gt; Can</th><th>cel Save &amp; Close</th></previo<>	us Next> Can	cel Save & Close
Conuche Ocourse	1	Analysis - Summary - No Objects Selected	I				

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 Use	r Account	х
Name	Administrator	
Password		
	<u></u>	Add Close

- 6. Click the new account name in the **User Accounts** column, and then click the <a> icon next to the appropriate User Group to create the **User Account Mapping**.</a>
- 7. Click **Close**, and then click **OK > OK** to accept the changes. See Figure 5.

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

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

Network Node Manager					ystem NNMiR	lole: Administrator	Sign Ou
e Tools Help							
Dashboards 3	Security Wizard *	_					
Incident Management	🕹 Welcome	Use this page to do any of the Create and Delete User Accounts		ser Groups, Assign User Acco	ounts to User G	roups, Assign Use	er Groups to User
Topology Maps	Map User Accounts and User Gr	Accounts, Remove User Account User Accounts	s Mappings. User Account Map	nings	User Gro	uns	
Monitoring	🔉 🔊 Map User Groups and Security G		×		* 🗙	·	
Troubleshooting	Assign Nodes to Security Groups 🔊	Name	User Account	User Group		Name	Display Name
Inventory	View Summary of Changes	Administrator	Administrator	NNMi Administrators	6		NNMi
Management Mode					Jh	admin	Administrators
Incident Browsing					Assign U	ser Group to Sele	ected User Acco
Integration Module Configuration							NNMiLevel 2
Configuration /						level2	Operators
Global Network Management						client	NNMi Web Service Clients
					$\bigcirc$	guest	NNMi Guest Users
Recurity Wizard					$\bigcirc$	globalops	NNMi Global Operators
User Accounts							
User Groups							
User Account Mappings					<previous< td=""><td>Next&gt; Cancel</td><td>Save &amp; Close</td></previous<>	Next> Cancel	Save & Close
Security Groups	Analysis - Summary - No Objects Sel						

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.

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.

Tip: Configuring only default community strings works best when the number of community strings is low.

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

Figure 6: Communication Configuration

Ø	Netw	ork No	ode Man	ager
File	View	Tools	Actions	Help
🕐 Da	shboard	ls		
💧 In	cident M	anagem	ent	ÿ
🔥 To	pology I	Maps		- <
🙅 M	onitoring	1		
_	oublesh	ooting		
	ventory			- 5
	anageme			
	cident Bi		e Configura	ation
	onfigurat		comgun	ation
/ CC	Jingura	lion		
	Comr	nunicatio	n Configurat	tion
± (	🛅 Disco	very	45	
± (	🛅 Monito	-		5
-	🛅 Incide			
	📑 Statu	-		$\langle \cdot \rangle$
			k Managem	ent
	🛅 Userl			
	🛅 Secur 🛅 MIBs	nty		
±		1		post -

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

Communication Configuration           Image: Save and Close         Image:	
✓ 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.	Read Community String
* SNMP Retries Count 2	
* SNMP Port 161	
SNMP Proxy Address	
SNMP Proxy Port	
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

<u>File View Tools Ag</u>	<u>e</u> tions <u>H</u> elp	
Default Read Community Stri	ring	
😼 📄 🎦 🖓 Save	and Close 🛛 🥔 💢 Delete Default Read Community String 🛛 🔛	
(j) Changes are not con ▼	ommitted until the top-level form is saved!	
<ul> <li>Read Community String Ordering</li> </ul>	commstr1	
Analysis		8

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

File View Tools Ac	tions Help		
🖙   🖺 🔮 Save and C	lose 🞜   🖾		
✓ Default SNMP Settings		Â	Default SNMPv1/v2 Community Strings     Default SNMPv3 Setting
For more information, click	iere.		✓ Read Community Strings
Enable SNMP Address Rediscovery			For more information, click here.
Enable SNMP GetBulk		E	* 🖻   🞜   🗙 🔯 🗟 1-2 of 2
* SNMP Timeout	5.00 Seconds v		Read Community String
attempts to communicate u for an answer. Each additi	in, trying at 6, 9, and 12 for a total		commstr1 commstr2
* SNMP Retries Count	2		
* SNMP Port	161		45
SNMP Proxy Address			
SNMP Proxy Port SNMP Minimum Security Level	Community 💌		
▼ Management Address Se	lection		
		-	and and the second second

### **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 IP addresses as input and only discovers the nodes contained in that list. NNMi discovers no additional nodes or IP 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 (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



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

Figure 11: Discovery Configuration: Auto-Discovery Rules

File View Tools	Actions Help								
Discovery Configuration									
😼 📔 🎦 Save and	Close   🧭   🔛								
		4	Schedu	le Settings	Auto-Discove	ry Rules Su	bnet Connection	Rules	Unnumbered
Enable Discovery of ATM/Frame Relay Interfaces for Performance Monitorin	<b>—</b>		Default Ter				discovered node itional nodes. If r		
	Sweep Control (IPv4 only)				information, clie		luonarnouca. In r	io ruic ap	plics to all add
This control can override Auto-Discovery Rules.	the Enable Ping Sweep choice for all		*	🞜   🖻	×   ×	×	Ø	of 0 🖒	
Ping Sweep	None 👻		0 New	)iscover Matching Nodes	Enable Ping Sweep	Discover Any SNMP Device	Discover Non-SNMP Devices	Name	Notes
Sweep Interval	24.00 Hours -			loues	змеер	Device	Devices		
Node Name Resolutio	n								-
* First Choice	Short DNS Name 💌								
* Second Choice	Short sysName 👻								
* Third Choice	IP Address 💌								
Layer 2 Connection S	ource								
Node-Grownto-dientie	- Andrew All Stranger Ar		A					\	

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

Auto-Discovery Rule * 🛛 🗟 📔 🎦 Save and Close   🞜	Delete Auto-Discovery Ru	ıle 🛛 🔛		
(i) Changes are not committed until the t	op-level form is saved!			
	A	IP Ranges	System Object ID Ranges	4
Auto Discovery Rules apply only to Default	Tenant.		overy Starting Point for this Rule	4
Vame MyNetwork     Ordering 10 Notes      Purpose of this Auto-Discovery Rule		(/16) of the n Auto-Discov	weep Instead of or In Addition to D	nore information about i
	E	▼ IP Address	Ranges for this Rule	
If enabled, NNMi discovers any Node that co criterion. If disabled, NNMi rejects any Node Rule's criterion. Click <b>here</b> from more informa	that complies with this		P Address Ranges for this Rule to includ to ignore (remain available for another R	
Discover Matching Nodes		Tip: Provide (	one seed for each WAN's IP Address Ra	
	and Switches)			0-0of0 🕞 😒
		IF New	<ul> <li>Range Type</li> </ul>	

- 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

	not committed until the top-level form is saved!	
Basics		
Address ranges c	can be entered in either a wildcard or CIDR notation.	
<pre>/4 examples: 10.2-3.*.1 10.2.120.0/21</pre>		
6 examples: 2001:D88:0:A00-		
S2001:d88:0:a00	J/00	
e Help $\rightarrow$ Using (t	this form) for more examples and important	
		:

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

Metwork Node Manager				User N
File View Tools Actions Help				
Dashboards	*	Seeds		
👌 Incident Management	≈	Ø (*) ⊑   S ⊑   ∽ ∛   ×   ≅		
\Lambda Topology Maps	≈	Hostnar New Initial Discovery Ter Discovery See	ed Results	Last Mo
Monitoring	≈			
Troubleshooting	≈			2
1 Inventory	≈			
🗞 Management Mode	≈			
🏡 Incident Browsing	*			
🐗 Integration Module Configuration	*			
🌽 Configuration	*			1
🖃 🣴 Discovery				
Discovery Configuration				
E Seeds		Updated: 6/11/14 11:12:41 AM	Total: 0	Selected: 0
III Tenants		Analysis		_
, 🛅 Overlapping Address Mappings		Summary 😳		
Lord Lanson Comment	العان	and the second	and the second s	ma l

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

🧑 Network Node Manager	
File View Tools Actions Help	
② Dashboards	Seeds Discovery Seed *
👌 Incident Management	😮 🗵 🛱 🛗 🎦 🚰 Save and Close 🔽 🗶 Delete Discovery Se
\Lambda Topology Maps	× -
Monitoring	* Hostname/IP (10.161.4.3
Troubleshooting	*
Inventory	Initial Discovery Tenant
S Management Mode	Discovery Seed Results
o Incident Browsing	Last Modified June 3, 2014 9:44:21 PM IST     Notes
4 Integration Module Configuration	× My Router
J Configuration	
the second second	and the second s
	14

**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**.



Metwork Node Manager				User Name: Administrator	NNMi Role: Administ
File View Tools Actions Help					
② Dashboards	*	Seeds			
👌 Incident Management	*	💯   * 🖻   🞜 🖷   🔊 🖗	≍   ≝	🔯 🌖 1-1 (	of 1
🛧 Topology Maps	*	Hostname/IP〉 Initial Discovery Te	Discovery Seed Results	Last Modified	Notes
Monitoring	*	10.161.4.3	In progress	Jun 11, 2014 11:17:18 AM	My Router
Troubleshooting	*				
Inventory	*				9
📀 Management Mode	*				
🏡 Incident Browsing	*				
🐗 Integration Module Configuration	*				
J Configuration	*				1
🖃 🗁 Discovery					3
Discovery Configuration					
m Seeds		Updated: 6/11/14 11:18:24 AM	Total: 1	Selected: 0 Filter:	ON
m Tenants		Analysis		-	
Overlapping Address Mappings	r.	Summary Panel 🚭			
	J.	and remained and	and the second strends and a feature of the second strends and the second strends and the second strends and the	Summer and the second second second	

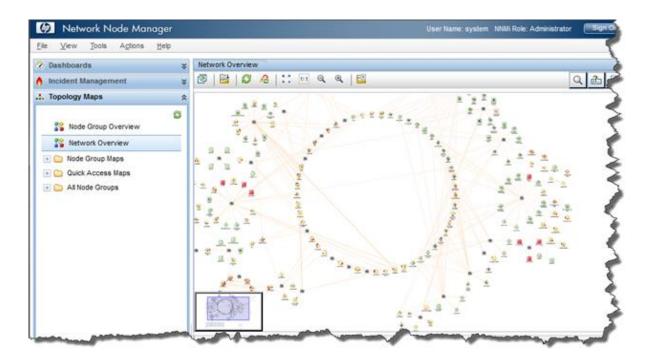
**Tip:** You can also load a list of seeds from a file using the **nnmloadseeds.ovpl** script. This script enables you to load a large number of seed nodes. If you use list-based discovery rather than Auto-Discovery Rules, you can load all of your nodes using the **nnmloadseeds.ovpl** script. See the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



### **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.

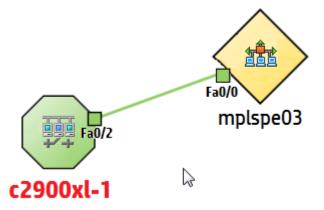
Consider the following scenario:

- 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



<ul> <li>Basics</li> </ul>		Â	4	G	eneral	IP /	Addresses	Interfaces	Chassis	Cards	Ports	
Name	10.1.76.68		•									
Hostname	10.1.76.68		ſ	2		<b>0</b>	භ		00	1 - 10 of 505	001	
Management Address	10.1.76.68								~ ~	1 - 10 01 303		E
Status	Minor			<del>S</del> ta:	Adı	Ope	ifName	ifTyp	е	ifSpeed	ifAlias	I
<ul> <li>Node Management Mode</li> </ul>			17	0	0	0	Fa0/2	others	atCamaa.	100 Mbps	HCDD D4	
Device Profile	nortelCarrierPass	E		<u> </u>	<u> </u>	<u> </u>	Fau/2	emen	letCsmact	TOO MDps	IL SKP DC	-
				Ø	5	3	Nu0	other		10 Gbps		
<ul> <li>Tenant</li> </ul>	Default Tenan 👻 🎬 🔻			0	<b>6</b>	5	VL2	othors	etCsmacc	10 Mbaa	Connect	
<ul> <li>Security Group</li> </ul>	Default Secur 👻 🎲 🔻			÷	<u> </u>	<u> </u>		emen	letusmact	TO MODS	Connect	
SNMP Agent State		·		Ø	5	6	Fa0/11	etherr	etCsmacc	100 Mbps		∢
Agent Enabled		- 🛛		0	<b>6</b>		Fa0/12	etherr	etCemaco	100 Mbps		٦
Agent SNMP State	Normal				_	_		Guich	icito sina ci	roo mopa		4
Management Address ICMP State	Responding			Ø	6	Ê <mark>I</mark>	Fa0/8	etherr	etCsmacc	100 Mbps		1
Management Address				CA.	5	5	Fa0/9			100 Mbps		

Figure 19: Node Form: List of Interfaces

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.

- Basics		Â		General	IP	Addresses	Interfaces Chassis	Cards	Ports
Name	10.1.76.68		-						
Hostname	10.1.76.68		図	1 🖻		2			9 - 16 of 79
Management Address	18.1.76.68							12 2	00000
Status	Minor		Sta	Adı	Оре	ifName	ifType	ifSpeed	ifAlias
<ul> <li>Node Management Mode</li> </ul>	Managed 👻				-				
Device Profile	nortelCarrierPass	E		13	3	Fa3/43	ethernetCsmaco	100 Mbps	connection to
* Tenant	Default Tenan 👻 🏢 💌		0	5	5	Fa3/31	ethernetCsmaco	100 Mbps	connection to
<ul> <li>Security Group</li> </ul>	Default Secur 👻 🎲 🔻		Ø	5	5	Fa3/34	ethernetCsmaco	100 Mbps	monitor port to
SNMP Agent State			Ø	5	5	Tu1	tunnel	9 Kbps	tunnel to demo
Agent Enabled		1	Ø			Tu2	tunnel	9 Kbps	tunnel to demo
Agent SNMP State	Normal			-0		102	turinor	5 Kups	tunner to denie
Management Address ICMP State	Responding		0	5	5	Fa3/25	ethernetCsmaco	100 Mbps	

#### Figure 20: Node Form: Apply Monitoring Settings

### **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

File View Tools Actions Help						
2 Dashboards	×	Interface Groups				/
h Incident Management	×	🗵 (*) 🖻   😂   🄊 🐬	🗙   🔛			🕼 🔇 1 - 6 of 11
🗛 Topology Maps	×	Name	Add to	Add to	Node Group	Notes
Monitoring	×		View Filter List	Filter List (Unlicensed		
Troubleshooting	×	ATM Interfaces	<b>v</b>	~		Interfaces identified as A
Inventory	×					
Management Mode	×	DSx Interfaces	~	~		Interfaces identified as Di
🗞 Incident Browsing	×	FrameRelay Interfaces	~	~		Interfaces identified as Fi
🤣 Integration Module Configuration	*	ISDN Interfaces	~	-		ISDN Interfaces as identi-
Configuration	*	Link Aggregation Interfaces	~	-		Interfaces identified as a
📑 Communication Configuration		Point to Point Interfaces	~	-		Point to Point Interfaces a
🖭 🧰 Discovery						
📧 🚞 Monitoring		Updated: 6/11/12 02:46:58 PM		Total:	11 Selected:	0 Filter: OFF
\pm 🧰 Incidents		Analysis				
📑 Status Configuration		Summary 😳				
📑 Global Network Management						
📧 🚞 User Interface		No Objects Select	ed			
📧 🧰 Security						4
🛨 🧰 MIBs						
Device Profiles						
📄 📂 Object Groups						
Interface Groups						1
RAMS Servers						

- 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
-----------------------------------

Interface Groups Interface Group *		
🙋   🗟 🕕 🛗 🎦 Save and Close   🧭 🗙 Delete Interface Gro	up   🖾	
▼ Basics Save	ifType Filters Additional Filters	
Name Important 9kbs Tunnels	▼	
Add to View Filter List  Node Group Notes	When using the like or not like operators, use an * (asterisk) to match zero or more characters in 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 betw AND 10.10.1.255 For more information, click <b>here</b> .	-
You can filter Interface Groups using ITType Filters and Additional Filters. If you use both iTType Filters and Additional Filters, Interfaces must match at least one iTType 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 $\rightarrow$ Using the Interface Group form.	Filter Editor Attribute Operator Value IfSpeed • F = F 9000	Append Insert Replace
To test your Interface Group definition, select File $\rightarrow$ Save, then Actions $\rightarrow$ Interface Group Details $\rightarrow$ Show Members.		AND
NNM iSPI Performance	AND	OR
Used by NNM iSPI Performance for Metrics and NNM iSPI for Traffic.	ifSpeed = 9000	EXISTS
Add to Filter List		NOT EXISTS
	Filter String (ifAlias like tunnel to* AND ifSpeed = 9000)	Delete

- 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 (include Child Groups)** menu item.

NNMi displays all items that pass the filter criteria.

Figure 23: Actions: Show Interface Group Members

Metwork Node Manager				f
<u>File View Tools Actions H</u> elp				1
⊘ Dashboards Show Members (Inc	lude Child Groups)	ce Group		
👌 Incident Management 🛛 🕹		Save and Close   🥰 🔀 Delete Interface Gro	up p 🔛	
🛧 Topology Maps 🛛 🗧 🗧	- Basics		ifType Filters	Additional Filters
Monitoring ×	* Name	Important 9kbs Tunnels	_	
Troubleshooting ¥	Add to View Filter List		•	
inventory ¥				e: like or not like operation ) to match exactly one or
📀 Management Mode 🛛 🕹 😵	Node Group	- III - IIII - III - IIII - III - II	To orosto on in	clusive IP address range
🏡 Incident Browsing 🛛 🗧 😵	Notes		AND 10.10.1.2	5i5
Section Contraction	Law and	and a state of the	For more inform	mation, 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

File View Tools Actions Help															
2 Dashboards	×	Interf	ace (	Group	os 📏 Interface G	iroup 👌 Inte	rfaces								
👌 Incident Management	×	2	B		3 🖪 🖉	🔊   🔛				Impo	ortant 9kbs Tunnels (Interfaces	) -	🔯 🍳 1 - 21 o	of 21	0 01
🛆 Topology Maps	۲	Sta	Adr	Ope	Hosted On No	ifName	ifType	ifSpeed	ifDescr		ifAlias 🔺	Status	Last Modified	State Last Modified	Notes
Monitoring	*	0	0	0	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	
Troubleshooting	*	0	0	0	peoriapr	Tu3	tunnel	9 Kbps	Tunnel3		tunnel to demorams9 eigrp 10	Apr 19,	2011 9:15:52 PM	May 3, 2011 6:37:45 PM	
Inventory	*	0	63	63	ntc2ext-aw3	Tu1	tunnel	9 Kbps	Tunnel1		tunnel to demorams9 for area	Apr 19.	2011 11:57:30 PM	Apr 19, 2011 11:57:57 PM	
🔄 Management Mode	*	0	ER.	63	ntc2ext-gw3	Tu2	tunnel		Tunnel2		tunnel to demorams9 for area				
http://www.ing	*					Tu3	tunnel	9 Kbps	Tunnel3	8	tunnel to eastcoast-gw1 for				
🗘 Integration Module Configuration	*	ø				Tu2	other		Tunnel2		tunnel to ntc2rams			Apr 20, 2011 12:01:20 AM	
Configuration	*	Ξ.	ŏ	-		Tu1	tunnel	9 Kbps	Tunnel1		tunnel to ntc2rams			Apr 20, 2011 12:06:20 AM	
E Communication Configuration		ŏ	ŏ	Ξ.	-	Tunnel1	other		Tunnel1		tunnel to ntc2rams			May 3, 2011 5:22:11 PM	

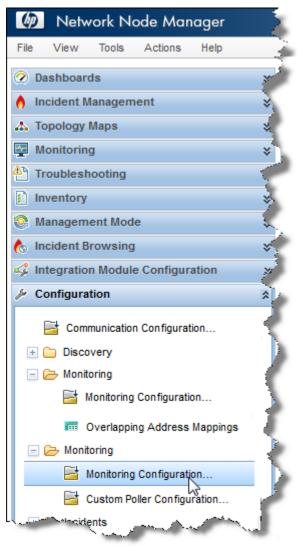
### **Apply Monitoring to an Interface Group**

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



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

nitoring Configuration											
Save and C	lose   🤣   🔛										
Global Control		Interfa	ce Settings Node Settings	Defa	ault Setti	ngs					
f disabled, previous devic for more information, click	e state and status values remain uncha <b>here</b> .				r 11						
Enable State Polling		when	multiple settings are defined, I	vivini ap	oplies the	em acco	raing	to the t	Jraerin	g numb	er (lowest number first).
	e State Polling above, NNMi disables g object types and resets the previous		)⊟   🕫   🗙		K	4	1 - 3	of 3			
states for each.	g object types and resets the previous		Vew	Eng	Ena _	Pol	Ena	Ena I	Ena Er		
Enable Card Polling			. Name	ICN		ol Inte	Inte	Locks 1	SOI A' Inte In	Rel	Notes
Enable Chassis Polling		Ore	IE		Fau Ir Pol	nte IP Ade	Per Pol	Per	Per Po Pol Po	, Per	
Enable Node Sensor Polling						Au		FUL		Pol	
Enable Physical Sensor		100	ISDN Interfaces	-	<b>*</b>		-	-		-	ISDN Interfaces as iden
Polling		200	Point to Point Interfaces	-	<b>~</b> .		-	-		-	Point to Point Interfaces
Enable Router Redundancy Group Polling		300		-	<b>~</b>		-	-		-	VLAN interfaces do no

- 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.

File View Tools Ag		ings. Save and close											
	aona <u>n</u> oip												
Interface Settings *		🕽 💢 Delete Interface Settings   🖥	X	_									_
□ 1 1 Save:	and Close	🖇 🗙 Delete Interface Settings 🛛 🖥											
(i) Changes are not cor	mmitted until the	top-level form is saved!											
				_									
			Â	ŀ	Threshold Settings	Basel	ine Settings						
For more information, click h	iere.				•								
* Ordering	50	)			If the optional NNM i	SPI Per	formance for Me	etrics is er	abled, set ti	he low and	gh values to determine	e Interface	
					Interface performan	ice stat	te.						
* Interface Group	Important 9kb	os Tunnels 🔻 🖼 🔻			* - 🖻 🕯	3   6	o   X				🕼 🥥 0-0 of (		
▼ Fault Monitoring			=		Monitored Attribute	•	Threshold	High	High Value	Low Value	Low Value Rearr	n	
For more information, click h	are		=		Attribute		Setting Type	Value	Rearm	value			
ICMP Fault Monitoring													
Enable IP Address Fault Polling													
SNMP Fault Monitoring													
Enable Interface Fault													
Polling													
* Fault Polling Interval	5.00	Minutes 🔻											
SNMD Darformance Monite	aric					h							
			r			-							- 4
<ul> <li>Extend the Scope of Pollin</li> </ul>	ng Beyond Con	nected Interfaces		Ľ									
		polled. These settings extend the ded to use them with small node or											
Interface Groups.	it is recommen	ded to dae them with sindli hode of											
For more information, click h	nere.												
Poll Unconnected													
Interfaces	_												
Poll Interfaces Hosting IP Addresses													
Poll Link Aggregation Interfaces				F					Total: 0	Selected	1:0 Filter: OFF	Auto refresh: OFF	
Interfaces				-									
Analysis - Summary - No	Objects Sele	cted											

Figure 27: Interface Settings: Save and Close

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

Figure 28: Monitoring Configuration: Save and Close

Poling	e View Tools Actions Help													
• Global Control If disabled, previous device state and status values remain unchanged. For more information, click here. 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 Card Polling Enable Node Sensor Polling Enable Node Sensor Polling Enable Router Redundancy Group Polling Enable Router Redundancy Group Polling Colored Name Colored Name Node Settings Default S														
If disabled, previous device state and status values remain unchanged. For more information, click here. 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 Sensor Polling Enable Node Sensor Polling Enable Router Redundancy Group Polling Enable Router Redundancy Redundancy Redundancy Redundancy Redundancy	I I Save and Close													
For more information, click here.         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 Chassis Polling         Enable Chassis Polling         Enable Chassis Polling         Enable Physical Sensor         Polling         Enable Physical Sensor         Polling         Enable Physical Sensor         Polling         Enable Router         Redundarcy Group         Polling	Global Control	Interface	e Settings	Node Settings	Defaul	t Settir	ngs							
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.       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       Image: Comparison object types and resets the previous states for each.         Enable Card Polling       Image: Comparison object types and resets the previous states for each.         Enable Chassis Polling       Image: Comparison object types and resets the previous states for each.         Enable Chassis Polling       Image: Comparison object types and resets the previous states for each.         Enable Rode Sensor       Image: Comparison object types and resets the previous states for each.         Faule Rable Physical Sensor       Image: Comparison object types and resets the previous states for each.         Sol Important 9kbs Tunnels       Image: Comparison object types and resets the previous states for each.         Sol Important 9kbs Tunnels       Image: Comparison object types and resets the previous states for each.         Sol Important 9kbs Tunnels       Image: Comparison object types and resets the previous states for each.         Sol Important 9kbs Tunnels       Image: Comparison object types and resets and the previous states for each.         Sol Important 9kbs Tunnels       Image: Comparison object types and resets and the previous states for each.         Sol Important 9kbs Tunnels		-												
If you do not select Enable State Polling above, NNMI disables monitoring for the following object types and resets the previous states for each.       Image: Comparison of the following object types and resets the previous states for each.         Enable Card Polling       Image: Comparison of the following object types and resets the previous states for each.       Image: Comparison of the following object types and resets the previous states for each.         Enable Card Polling       Image: Comparison of the following object types and resets the previous states for each.       Image: Comparison of the following object types and resets the previous states for each.         Enable Card Polling       Image: Comparison of the following object types and resets the previous states for each.       Image: Comparison of the following object types and resets the previous states for each.         Enable Card Polling       Image: Comparison of the following object types and resets the previous states for each.       Image: Comparison of the following object types and resets the previous states for each.         Enable Card Polling       Image: Comparison of the following object types and resets the previous states for each.       Image: Comparison of the following object types and resets the previous states for each.         Enable Router Redundancy Group Polling       Image: Comparison of the following object types and resets the previous state for each of the following object types and resets the previous state for each of the following object types and resets the previous state for each of the following object types and resets the previous state for each of the following object types and resets the previous state for each of t	Fachia Chata Dallian	When r	nultiple sett	ings are defined,	NNMi ap	oplies t	hem a	accor	ding t	to the	Orde	ring n	umbe	r (lowest number first).
monitoring for the following object types and resets the previous states for each.         Enable Card Polling         Enable Card Polling         Enable Card Polling         Enable Card Polling         Enable Chassis Polling         Enable Chassis Polling         Enable Chassis Polling         Enable Chassis Polling         Enable Rodes         Enable Physical Sensor         Polling         Enable Router         Redundancy Group         Polling				1.00			~	~						
states for each. Enable Card Polling Enable Chassis Polling Enable Chassis Polling Enable Physical Sensor Polling Enable Router Redundancy Group Polling Enable Router Redundancy Group Enable Router Redundancy Group Enable Router Redundancy Group Enable Router Redundancy Group Enable Router Redundancy Group Enable Router Redundancy Group Polling Enable Router Redundancy Group Enable		*		× .		LS.	9 (	♀ 1	1 - 4 0	of 4				Q Q   <u></u> =
Enable Card Polling       Important 9kbs Tunnels       - <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>Del</th> <th></th> <th>Eng</th> <th>Eng</th> <th>Eng</th> <th>Ena</th> <th></th>								Del		Eng	Eng	Eng	Ena	
Enable Chassis Polling       Intel IP       Per						Ena	Pol	Inte	Ena	DSv		ATI		
Enable Chassis Polling       Pol       P	Enable Card Polling	Orde	Name			Fau	one	noe	Dor	mile		Inte		Notes
Enable Node Sensor Polling       Important 9kbs Tunnels       <	Enable Chassis Polling						mile		Pol	FOI		Per	Per	
Polling       50       Important 9kbs Tunnels       - <t< th=""><th>Enable Node Sensor</th><th></th><th></th><th></th><th></th><th></th><th></th><th>Aut</th><th></th><th>FUI</th><th>FUI</th><th>FUI</th><th>Pol</th><th></th></t<>	Enable Node Sensor							Aut		FUI	FUI	FUI	Pol	
Polling 100 ISDN Interfaces ISDN Interfaces as ide Enable Router Redundancy Group 200 Point to Point Interfaces Point to Point Interface	Poling	50	Important	9kbs Tunnels	-	~	<b>~</b>	~	-	-			-	
Enable Router Redundancy Group 🔽 Polling		100	ISDN Inter	faces		~	-				-	-		ISDN Interfaces as idea
Poling	Enable Router	100	15DN Inter	10003										ISBN Internaces as laci
Polling 300 VLAN Interfaces VLAN interfaces do n		200	Point to Po	pint Interfaces	-	~	-	-	-	-	-	-	-	Point to Point Interfaces
	Polling	300	VLAN Inte	erfaces	-	~	-	-	-	-	-	-	-	VLAN interfaces do no

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

ile View Tools Actions Help														
Dashboards	¥	Interf	ace (	Group	is 📏 Interface G	roup 🔪 Inte	rfaces							
Incident Management	×	2			3 🖪   🔊 ·	🔊   🔛			Imp	oortant 9kbs Tunnels (Interfac	ces)	- 10 0 3-21 0	if 21	୦ ରା
L Topology Maps	×	Sta	Adı	Ope	Hosted On No	ifName	ifType	ifSpeed	ifDescr	ifAlias 🔺		Status Last Modified	State Last Modified	Notes
Monitoring	×	0	0	0	ntc2ext-gw3	Tu2	tunnel	9 Kbps	Tunnel2	tunnel to demorams9 for a	re: I	lay 3, 2011 6:59:18 PM	May 3, 2011 6:59:16 PM	
Troubleshooting	*	۲	0	0	core_6509-1	Tu3	tunnel	9 Kbps	Tunnel3	tunnel to eastcoast-gw1 f	or ,	Apr 19, 2011 11:59:03 PM	May 3, 2011 6:58:59 PM	
Management Mode	÷1	0	0	0	wanrouter-1	Tu2	other	9 Kbps	Tunnel2	tunnel to ntc2rams		Apr 19, 2011 11:59:03 PM	May 3, 2011 6:59:09 PM	
Incident Browsing	×	۲	0	0	ntc2ext-gw2	Tu1	tunnel	9 Kbps	Tunnel1	tunnel to ntc2rams		Apr 20, 2011 12:02:22 AM	May 3, 2011 6:58:54 PM	
2 Integration Module Configuration	*	0	0	0	wanrouter-2	Tunnel1	other	9 Kbps	Tunnel1	tunnel to ntc2rams	1	lay 3, 2011 5:37:52 PM	May 3, 2011 6:59:04 PM	
Configuration	*	0	0	0	peoriapr	Tu1	tunnel	9 Kbps	Tunnel1	tunnel to ntc2rams	1	Apr 19, 2011 9:15:52 PM	May 3, 2011 6:58:54 PM	
	-	0	0	0	cisco4k1	Tu5	tunnel	9 Kbps	Tunnel5	tunnel to rams910		lay 3, 2011 6:59:06 PM	May 3, 2011 6:59:04 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

Metwork Node Manage	er					
File View Tools Actions He	elp					
<ul> <li>Dashboards</li> <li>Incident Managem</li> <li>Graphs Poling</li> </ul>		Save and Close 🛛 💋 🛛 🔛				
Topology Maps Configuratio	on Details ، Monitoring Setti	ings	A 4	General	IP Addresses	Ports
Monitoring Custom Attri		Tu1		SNMP Values		4
		Normal Managed Inherited next-gw2		ifName ifAlias ifDescr ifIndex ifSpeed ifType	Tu1 tunnel to Tunnei1 26 9 Kbps tunnel	ntc2rams
🗰 VI ANs	▼ Interface State		-	Input/Output Sp	eed	
📀 Management Mode	*			Input Speed	9000	
🏡 Incident Browsing	Administrative State     Operational State	e Up Up		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.

### Monitoring Settings Report: Interface

Tu1

NNMi Management Station: deploylx1.fc.usa.hp.com

Object Name:

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 S	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 Setting	s Applied
Туре	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

🕼 Network Node Mar	nager			5
<u>File View Tools Actions</u>	<u>H</u> elp			
Dashboards	•	rfaces Interface		
Incident Managem     Polling	s 🕨	😼   💾 💾 Save	and Close   🧭   🖼	
A Topology Maps Config	uration Details 🕨	Basics		
Monitoring Custon	n Attributes	Name	7.4	I GG
Troubleshooting Manag	emen <u>t</u> Mode 🔷 🕨	🖬 Manage	Tu1 Normal	
inventory	*	🚽 Manage (Reset All)	Managed	ifName
m Nodes		Not Managed	Inherited 👻	ifAlias
Interfaces	= -	🔏 Out of Service		ifIndex
IP Addresses		Hosted Un Node	next-gw2	ifSpeed
SNMP Agents	-	Physical Address		ifType

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.

Network Node Manager							ser Nam	ie: syst	em N	NNMi Role: Adminis	trator Sign O
ile ⊻iew <u>T</u> ools A <u>c</u> tions <u>H</u> elp											
Dashboards	×	Management Event Configurations	s								
Incident Management	*	🖉   * 🖻   🞜   🄊 🕇	ፆ│≍│⊑							35 - 46	of 100 🗇 🗐 📘
🖍 Topology Maps	*	Name 🔺	SNMP Object ID	Enabled	Deduplicati		Sev	Cat	Fa	Author	Message Format
Monitoring	≈				on Enabled	Enabl	erit V	_	mil v		
Troubleshooting	∻	FanOutOfRangeOrMalfunctioning	.1.3.6.1.4.1.11.2.17.19.2.0	0.15 🗸	-	-	с С		∙ ∮c	HP Network Nod	Fan on SsourceNode!
Management Mode	*	HostedObjectTrapStorm	.1.3.6.1.4.1.11.2.17.19.2.0	0.49.1 🗸	-	-	Δv	Βίζι Δ	500 T	HP Network Nod	Host \$trapSource ove
Incident Browsing	*	InterfaceDisabled	.1.3.6.1.4.1.11.2.17.19.2.0	0.18 -		~	8 c		Si ir	HP Network Nod	Interface Disabled
C Integration Module Configuration	*	InterfaceDown	.1.3.6.1.4.1.11.2.17.19.2.0	0.19 🗸	-	-	🕴 c		ال	HP Network Nod	Interface Down
Configuration	*	InterfaceFCSLANErrorRateHigh	.1.3.6.1.4.1.11.2.17.19.3.4	4.0.17 -	-	-	🕴 c	🔊 p		HP Network Nod	High FCS LAN error ra
Communication Configuration		InterfaceFCSWLANErrorRateHig	.1.3.6.1.4.1.11.2.17.19.3.4	4.0.29 -	-	-	🕴 c	🕋 p	Fi in	HP Network Nod	High FCS WLAN error
E Discovery		InterfaceInputDiscardRateHigh	.1.3.6.1.4.1.11.2.17.19.3.4	¥.0.1 🖌	-	-	🕴 c	🔊 p	🖧 ir	HP Network Nod	High input discard rate
Control Monitoring     Control Monitoring     Control Monitoring		InterfaceInputErrorRateHigh	.1.3.6.1.4.1.11.2.17.19.3.4	4.0.2 🗸	-	-	8 c	🔊 p	🖧 ir	HP Network Nod	High input error rate o
Incident Configuration		InterfaceInputQueueDropsRateH	.1.3.6.1.4.1.11.2.17.19.3.4	4.0.18 -	-	-	🕴 c	🔊 p	Fi Ir	HP Network Nod	High input queue drop
SNMP Trap Configurations		InterfaceInputUtilizationAbnorma	.1.3.6.1.4.1.11.2.17.19.3.4	4.0.22 🗸	-	-	Δv	🔊 P		HP Network Nod	Abnormal input utilizat
Syslog Message Configurations	- 11	InterfaceInputUtilizationHigh	.1.3.6.1.4.1.11.2.17.19.3.4	4.0.3 🗸	-	-	🕴 c	🔊 p		HP Network Nod	High input utilization o
Management Event Configuration	1S	Updated: 4/22/14 04:38:26 PM		Total: 100	Sel	ected: 1	1	Filter: O	FF		Auto refresh: OFF
Pairwise Configurations	Ì	Analysis									
Custom Correlation Configuration	n	Management Event Configuration	a Summany :	Details 😳							
Chattan Confirmation		InterfaceDown	Enabled true								

#### Figure 33: Configuration: Management Event Configurations

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 Configu 2   😼   🗎 🎽 🛛		nfiguration elete Mana		ent Event	Configu	ratior	🖴			4
Enabled		<b>^</b>	•	Interface	e Setting	s I	Node Setting	s Suppre	ssion Er	nrichment
* Category * Family	Fault    Interface		Ob	ject base	d on the	Sour	ce Object's	ss, Enrich, D participatior Dampen, or	n in an Inter	face Grou
* Severity	Critical	_						de Settings t		ingurution
view. To include Incident in	nessage appears in the Incident formation in the message use hese variables from a set of valid ident attributes. For more			k 📑	Group	•	¥ Ordering	Enabled	4	
Interface Down		=								4
Description This incident indicates the to polls.	at the interface is not responding									
* Author	Customer V	-			~~~~~~		<i></i>	Total: 0	Selected:	0 Filter:
							-			

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

Ope	n Ke	ey Inc	cide	nts								
2		3	Ð	l 🖪   🔊 🖏	🗙   🔛						All	▼ <set filter="" group="" node="">         ▼         1 - 23 of 202         ♥         ♥         ●</set>
Sev	Pr	ic Li	ife	Last Occurren <del>e</del> e	Assigned	Source Node	Source Object	Cat	Fan	Ori	Сог	Message Notes
8	5	2		5/3/11 8:17:07 PM		c2950t	Fa0/1			ъ	₽ <u>¥</u> 4	High input discard rate on interface Fa0/1. The inDiscardRateState transitioned from
0	5	2		5/3/11 8:12:21 PM		nortel5510	ifc3 (Slot: 1 Port:			ъ	₽ <u>¥</u> 4	High input discard rate on interface ifc3 (Slot: 1 Port: 3). The inDiscardRateState tra
8	5	2		5/3/11 8:08:47 PM		core_6509-1	Tu3	*		ъ	14	Interface Down with Alias = tunnel to eastcoast-gw1 for multicast
8	5	2		5/3/11 8:08:47 PM		wanrouter-1	Tu2	*	<b>.</b>	ъ	₽₹¢	Interface Down with Alias = tunnel to ntc2rams
8	5	2		5/3/11 7:26:02 PM		ntc6kgw2	Chassis Fan Tray		1	ъ	₽ <u>¥</u> 4	Fan on ntc6kgw2 is malfunctioning
8	5	2		5/3/11 6:14:16 PM		10.161.4.3	10.161.4.3	*		ъ	₩₫	Non-SNMP Node Unresponsive
۸	5	2		5/3/11 12:29:43 PM		colby	colby.fc.usa.hp.c	*		1	₽ <u>¥</u> 4	SNMP Agent Not responding
	5	2		4/26/11 5:00:36 PM		vwanrouter-1	10.100.100.1	*	RRP	۵	₩ <b>a</b>	Primary device in Router Redundancy Group switched
	5	. 2		4/26/11 5:00:36 PM		ww.aprouter-1	-10,100-100	<u>_</u>	R	<b>b</b>	2	Rate Correlation for BroBailover: Primary divice in Router Redundancy Group swite

### **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.
- 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**.
- 2. Notice the newly loaded Rugged Com MIBs.
- 3. Take note of the traps module (RUGGEDCOM-TRAPS-MIB). You will need this for the next command.

#### Figure 36: Configuration: Loaded MIBs

Network Node Manager			User Name: A
e View Tools Actions Help			
Dashboards	×	Loaded MIBs	
Incident Management	*	🗵   🔁   🌮 🗳	
Topology Maps	×	Name 🔺	MIB File
Monitoring	×	POWER-ETHERNET-MID	TIIE:///opt/UV/misc/nnm/snmp-mips/Standard/TC3621-PUWER-ETHERNET-MIB.mip
Troubleshooting	×	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
Inventory	×	RFC1155-SMI	jar:file:/opt/OV/nonOV/jboss/nms/server/nms/lib/nms-mib-model.jarl/com/hp/ov/nms/mib/model/hibernate/rfc1155-
Management Mode	×	RFC-1212	jar:file:/opt/OV/nonOV/jboss/nms/server/nms/lib/nms-mib-model.jarl/com/hp/ov/nms/mib/model/hibernate/rfc1212-
Incident Browsing	×	RFC1213-MIB	jar:file:/opt/OV/nonOV/jboss/nms/server/nms/lib/nms-mib-model.jarl/com/hp/ov/nms/mib/model/hibernate/rfc1213-
Integration Module Configuration	×	RFC-1215	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc1215-RFC1215.mib
Configuration	*	RFC1271-MIB	jar:file:/opt/OV/nonOV/jboss/nms/server/nms/lib/nms-mib-model.jarl/com/hp/ov/nms/mib/model/hibernate/rfc1271
comgaration		RFC1315-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc1315-RFC1315-MIB.mib
Communication Configuration		RIPv2-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc1724-RIPv2-MIB.mib
Discovery		RMON2-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc4502-RMON2-MIB.mib
) 🧁 Monitoring		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
Monitoring Configuration		RUGGEDCOM-MIB	file:///var/tmp/rugged/./ruggedcom.mib
📑 Custom Poller Configuration		RUGGEDCOM-SYS-INEO-MIB	file:///var/tmp/rugged/./rcsysinfo.mib
🗀 Incidents	=	RUGGEDCOM-TRAPS-MIB	file:///var/tmp/rugged/./ruggedcomtraps.mib
Status Configuration		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
📑 Global Network Management		SNMP-REPEATER-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc2108-SNMP-REPEATER-MIB.mib
🗀 User Interface		SNMP-TARGET-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc3413-SNMP-TARGET-MIB.mib
) 🧰 Security		SNMPv2-CONF	jar:file:/opt/OV/nonOV/jboss/nms/server/nms/lib/nms-mib-model.jar/com/hp/ov/nms/mib/model/hibernate/rfc1904
) 🧀 MIBs		SNMPv2-MIB	jar:file:/opt/OV/nonOV/jboss/nms/server/nms/lib/nms-mib-model.jarl/com/hp/ov/nms/mib/model/hibernate/rfc3418
📖 Loaded MIBs		SNMPv2-SMI	jar: file:/opt/OV/nonOV/jboss/nms/server/nms/lib/nms-mib-model.jarl/com/hp/ov/nms/mib/model/hibernate/rfc2578
MIB Variables		SNMPv2-TC	jar: file:/opt/OV/nonOV/jboss/nms/server/nms/lib/nms-mib-model.jarl/com/hp/ov/nms/mib/model/hibernate/rfc2579-
		SNMP-VIEW-BASED-ACM-MIB	file:///OV/misc/nnm/snmp-mibs/Standard/rfc3415-SNMP-VIEW-BASED-ACM-MIB.mib
MIB Notifications		SONET-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc3592-SONET-MIB.mib
Textual Conventions		TOKEN-RING-RMON-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/Historic/rfc1513-TOKEN-RING-RMON-MIB.mib
MIB Expressions		TRANSPORT-ADDRESS-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc3419-TRANSPORT-ADDRESS-MIB.mib
MIB OID Types		TUNNEL-MIB	file:///opt/OV/misc/nnm/snmp-mibs/Standard/rfc4087-TUNNEL-MIB.mib
	Ψ.	And the second second	and the state of t

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.

Network Node Manager <u>V</u> iew <u>T</u> ools A <u>c</u> tions <u>H</u> elp											User Name: system NNMi Role: Administra	.or
)ashboards 🏻 🗧	SNMP Trap Configurations											
ncident Management 🛛 😵	, 🗵   * 📑   🞜   🔊	💎   🗙   🔛									🔯 🔇 9 - 29 of 129	
opology Maps 🛛 😵	Name	SNMP Object ID	Ena	Roc D Cai E	ec I	Rat	se (	a Fai	Author	Message Format		
Nonitoring 🗧	STPTOPOlogycnange	1.3.6.1.2.1.1/.9.2	LIIId	CalE	na I	Ena `				vc STP Topology Change		
roubleshooting	4						<u> </u>					
nventory a	RcVrrpStateChange	.1.3.6.1.2.1.46.1.3.0.1	*			- 4	_ ⇒ ^			No RC VRRP State Change		
Nanagement Mode 🛛 😵	letfVrrpStateChange	.1.3.6.1.2.1.68.0.1	~			- 4	_ ⇒	t 76	HP Network N	No IETF VRRP State Chan	ge on ipAddress \$1	
ncident Browsing	SiteScopeAlertEventv1	.1.3.6.1.4.1.11.15.1.4.0.1	~			- (	3 🕸	ŧ \$	HP SiteScope	Alert "\$.1.3.6.1.4.1.11.	15.1.3.1.2" was triggered on monitor "\$.1.3.6	1.4.1.11.15.1.2.1.3
ntegration Module Configuration	SiteScopeAlertEventv2	.1.3.6.1.4.1.11.15.1.4.1	~			. (	3 🕫	ŧ 🖏	HP SiteScope	Alert "\$.1.3.6.1.4.1.11.	15.1.3.1.2" was triggered on monitor "\$.1.3.6	.1.4.1.11.15.1.2.1.3
Configuration A	NetScoutServerAlarm	.1.3.6.1.4.1.141.50.2.0.1	~			- 4	1	1	HP Network N	Nc NetScout Server Alarn	n: Threshold \$3; Value \$5; Interval \$6	
Communication Configuration	NetScoutServerClear	.1.3.6.1.4.1.141.50.2.0.3	~			- (	2 🖪	1	HP Network N	Nc NetScout Clear Alarm		
Discovery	genericTrap	.1.3.6.1.4.1.15004.5.1	~			. (	) î	7 lb	Customer	genericTrap		
C Monitoring	powerSupplyTrap	.1.3.6.1.4.1.15004.5.2	~			- (	9 ř	<u>کا</u> (	Customer	powerSupplyTrap		
➢ Incidents	swUpgradeTrap	1361411500453	~				9 P	2 ib	Customer	swUpgradeTrap	13	
📑 Incident Configuration	cfgChangeTrap	.1.3.6.1.4.1.15004.5.4	~				9 F	5 fin	Customer	cfgChangeTrap		
m SNMP Trap Configurations								_				
📅 Syslog Message Configurations	cfgChangeNoRevTrap	.1.3.6.1.4.1.15004.5.5	*			- (	9 ľ	/ 10	Customer	cfgChangeNoRevTrap		
Management Event Configurations	Rcn2kTemperature	.1.3.6.1.4.1.2272.1.21.0.13	~			- (	3 4	ŧ ()	HP Network N	No Temperature node con	ponent indicates the device is over-heating v	vith a temperature
Pairwise Configurations	RcnChasPowerSupplyUp	.1.3.6.1.4.1.2272.1.21.0.14	~			- (	9 🔹	<b>k</b> (	HP Network N	Nc Power supply \$1 is tra	nsitioning to up	
Custom Correlation Configuration	RcnSmltIstLinkUp	.1.3.6.1.4.1.2272.1.21.0.17	~			- (	o 🤞	k ()(	HP Network N	Nc SMLT IST aggregator li	nk operational state changed from down to u	р
🗉 🧰 Trap Server	RcnSmltIstLinkDown	.1.3.6.1.4.1.2272.1.21.0.18	~			- (	3 🔹	t 11	HP Network N	Nc SMLT IST aggregator li	nk operational state changed from up to dow	n
📑 Status Configuration	RcnChasFanUp	.1.3.6.1.4.1.2272.1.21.0.21	~			- (	o 🔹	ŧ (	HP Network N	Nc Fan \$1 is transitioning	to up	
📴 Global Network Management	RcnAggLinkUp	.1.3.6.1.4.1.2272.1.21.0.41	~			- (	o 🔹	<b>t</b> 11	HP Network N	Nc MLT aggregator link op	erational state changed from down to up	
🗀 User Interface	RcnAaaLinkDown	.1.3.6.1.4.1.2272.1.21.0.42	~			. (	8 s	e 11	HP Network N	No. MLT appregator link op	erational state changed from up to down	
C Security	RcnChasPowerSupplyDown		~					k (1		Nc Power supply \$1 is tra		
🗀 MBs											-	
m Device Profiles	RcnChasFanDown	.1.3.6.1.4.1.2272.1.21.0.7	~			- •	⊌ ⇒	• 1	HP Network N	Nc Fan \$1 is transitioning	to down	
C Object Groups	Updated: 5/3/11 08:36:55 PM M						tal: 12			elected: 1	Filter: OFF	Auto refresh

### **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: %NnmDataDir%\shared\nnm\actions
- Linux: \$NnmDataDir/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

🐌 Network Node Manager			Use	er Name: syster	n NNMiRole: A	dministrator	Sign O	
ile <u>V</u> iew <u>T</u> ools A <u>c</u> tions <u>H</u> elp								
2 Dashboards	*	Management Event Configuration	s					
Incident Management	*	🗵   * 🖻   🞜   🔊 🤉	₽   🗙   🔛	C	🤝 🔷 74 -	83 of 100 🕼	A 1	
🔈 Topology Maps	*	Name 🔺	SNMP Object ID	Enabled	Deduplicati	Rate	Sev Ca	
Monitoring	≈				on Enabled	Enabled	erit eg y q	
Troubleshooting	*	NnmClusterTransfer	1.3.6.1.4.1.11.2.17.19.2.0.31	~	_	-	Ø N 1	
Inventory	≈							
Management Mode	*	NnmHealthOverallStatus	.1.3.6.1.4.1.11.2.17.19.2.0.64	~	-	-	🛇 N 🛒	
Incident Browsing	≈	NodeDeleted	.1.3.6.1.4.1.11.2.17.19.2.0.79	-	-	-	🗢 N 🕅	
Integration Module Configuration	*	NodeDown	.1.3.6.1.4.1.11.2.17.19.2.0.32	~	-	~	🕴 c	
Configuration Configuration	*	NodeOrConnectionDown	.1.3.6.1.4.1.11.2.17.19.2.0.33	*	-	-	🛛 🔁 c 🖈	
Discovery	<b>^</b>	NonSNMPNodeUnresponsive	.1.3.6.1.4.1.11.2.17.19.2.0.35	*	-	-	😣 c 🔹	
🛨 🧰 Monitoring	н	PVCDown	.1.3.6.1.4.1.11.2.17.19.2.0.9999	~	-	-	Δv	
Incidents		PipelineQueueSizeExceeded	.1.3.6.1.4.1.11.2.17.19.2.0.53	~	-	-	V N 6	
Incident Configuration	-	PowerSupplyOutOfRangeOrMal	4 2 6 4 4 4 4 2 47 40 2 0 26	*			🛛 c 🥈	
SNMP Trap Configurations		PowerSupplyOutOrRangeOrMan	.1.3.0.1.4.1.11.2.17.19.2.0.30	•	-	-	• C •	
📰 Syslog Message Configurations		•	III				•	
Management Event Configurations		Updated: 4/23/14 01:43:10 PM	Total: 100	Selected: 1	Filter: OFF	Auto	refresh: OFI	
Pairwise Configurations		Analysis					1	
📑 Custom Correlation Configuration		Management Event Configuratio	n Details 😂					
🖃 🗁 Trap Server		Summary : NodeDown 😂	Enabled	true				
📑 Trap Forwarding Configuration		SNMP 13614112171	Severity	🙁 🔽 Crit	ical			
🛲 Trap Logging Configuration		SNMP Object ID Messa	Family	Fault				

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

Figure 39: Management Event Configuration: Actions	Tab

🖗   💾 🎽	Save and Close 🛛 😂	Delete Management E		n   🖴						
Basics			de Setting	s Suppression	Enrichment	Dampening	Deduplication	Rate	Actions	►
r information about	t troubleshooting Incidents, clie	ck here.	-							
at must appear at nly in OIDs beginnir formation.	NodeDown (OID) attribute accepts one w the end of the OID specified. I ng with .1.3.6.1.4 (private MIB	NNMi permits wildcards s). Click <b>here</b> for more	generated (F operator, NN	re actions to autom kegistered), you mi Mi supports runnin onfigured actions a	ght want to auto g a Jython file, e	matically open executable, or s	a trouble ticket, se cript as an action.	nd email, or p		
SNMP Object ID	.1.3.6.1.4.1.11.2.17.1	9.2.0.32	▼ Lifecycle T	Transition Actions						
cident information in	Fault Fault Node Critical • dent message appears in the the message use S(variable, of valid parameters or Custom k here.	_name). Select these	New	ଟ   🗙 umand Type Co	mmand		0100-0			
escription										
etermined the node ne addresses assig gent installed on thi	Is that NMMS Advanced Proble is down based on the followined to this node are unreaches s machine is not responding. / can be reached and are repo ode.	ing analysis: 1) 100% of able, and 2) The SNMP At least two of the								

- 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  ${}^{\textcircled{}}$ 

Save and Close.

### Figure 40: Lifecycle Transition Action

fecycle Transition Action *         Image: Save and Close         Image: Save and Close	sition Action	
	Payload Filter	
inter the Java Jython file, executable, or script to run when an Incident changes to the specified Lifecycle State. You can pass Incident attribute ralues as parameters into each. See Help → Using the Lifecycle ransition Action form. Lifecycle State Registered Command Type ScriptOrExecutable Command	A Payload Filter enable participate in an opera pairwise. A Payload F values (ciaValue). For Filter Editor Attribute	tion; for example, fa ilter selects incomita more information, Operator
/var/opt/OV/shared/nnm/actions/writelog.ovol		, <u>i</u> =

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

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

Basics       Ide Settings       Suppression       Enrichment       Dampening       Deduplication       Rate       Actions         You configure actors to subornatically you right wart to automatically you and twart to automatically you right wart automatically you right wart to automatically you right wart automatically you right warth automatit automatically you risth wart to automatica	1   🖗   🗎 🕴	🖞 🔄 Save and Close   😂 🔀 Delete Management	it Event Configuration 🛛 🖼
Name       NodeDown         The SNMP Object D (OD) attribute acoust one wildcard character (*) that must appear at the end of the OD specified. NMM permits wildcards only in ODs beginning with 1.3.6.1.4 (private MBs). Click here for more information.       SNMP Object D 1.3.6.1.4.1.11.2.17.19.2.0.32         Enabled       Image: Category       Fault       Image: Category       Fault       Image: Category       Fault       Image: Category       Fault       Image: Category       Image: Cat	Basics		de Settings Suppression Enrichment Dampening Deduplication Rate Actions
<pre>ration records in the rest of the ODE specified. NHMI permits wildcards in the subject ID (ODE) structure accepts one wildcard character (1) that must appear at the end of the ODE specified. NHMI permits wildcards in the nod be beginning with 1.3.6.1.4 (private MIBs). Click tere for more information. The incident information in the message appears in the incident tributes. For one information, click here.</pre>	or information abo	out troubleshooting Incidents, click here.	
Enabled       Image: Control of the contr	The SNMP Object I that must appear a only in OIDs begin	ID (OID) attribute accepts one wildcard character (*) at the end of the OID specified. NNMi permits wildcards	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.
Category Fault  Fault Fa	SNMP Object ID	.1.3.6.1.4.1.11.2.17.19.2.0.32	▼ Lifecycle Transition Actions
This incident indicates that WWMs Advanced Problem Analyzer has determined the node is down based on the following analysis: 1) 100% of he addresses assigned to this node are unreachable, and 2) The SWWP agent installed on this machine is not responding. At least two of the heighboring devices can be reached and are reporting problems with	Category Family Severity ipecify how the In icident information ariables from a se hore information, c dessage Format	Node  Critical  Critical	Hife Command Type Command
This incident indicates that NUMS 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 heighboring devices can be reached and are reporting problems with			-
Author Customer	Description		

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**.

Metwork Node Manager														: Administrat
File View Tools Actions Help														
② Dashboards	×	Clos	ed Ke	y Inci	idents									
ncident Management	×	2			3   🤊 🧳   🗙							All	✓ <set filter="" group="" node=""> ✓</set>	N 🛛 🧹
🛧 Topology Maps	×	Sev	Pric	Life	Last Occurrence	Assigned	Source Node	Source Object	Cat	Fan	Ori	Co	Message	
Monitoring	×	ø	5	Q	5/3/11 4:10:42 PM		vwanrouter-2	vwanrouter-2	*	Ŀ	Ъ	₽₩₫	Node Down	
Troubleshooting	×	0	5	<b>P</b>	5/3/11 3:39:44 PM		cisco2k1	cisco2k1	*		Ъ	₽ <u>¥</u> 4	Node Down	
1 Inventory	*	•	5	R	5/3/11 3:39:33 PM		hpov2k2	hpov2k2	*		1	₽ <u>¥</u> 4	Node or Connection Down	
S Management Mode	*	•	5	Q	5/3/11 3:39:00 PM		hpov2k1	hpov2k1	*		1	₽ <u>⊼</u> 4	Node Down	
lncident Browsing	×	۲	5	R	5/3/11 3:19:16 PM		hpov2k1	hpov2k1	*		1	<b>₽</b> <u>₹</u> 4	Node or Connection Down	
Closed Key Incidents		۲	5	Q	5/2/11 8:08:19 PM		colby	colby	*		1	₽ <u>⊼</u> 4	Node Down	5
Open Root Cause Incidents	Ξ	0	5	R	5/2/11 2:35:33 PM	2	hpov2k1	hpov2k1	*		1	₽ <u>⊼</u> 4	Node or Connection Down	
E Service Impact Incidents		0	5	Q	4/29/11 1:44:01 PM		nsntc-s3140-2	nsntc-s3140-2	*		1	₽ <u>⊼</u> 4	Node Down	
All Incidents		۲	5	Q	4/27/11 7:05:23 PM		cheese	cheese	*		1	₽ <u>⊼</u> 4	Node Down	
tom Open Acidents		8	5.		4/27/11		tilsit	tist		νũφ/	H.	<u>y</u>		Marcal

Figure 42: Incident Browsing: Closed Key Incidents View

2. Double-click to open the form for 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.

#### Figure 43: Incident Form: Registered Lifecycle State

Closed Key Incidents Incident						
💯   📴 📋 🖺 Save and Close   🧬 🔀 Delete Incident   🔛						
▼ Basics	General	Correlated Par	ents Correlated Children	Custom Attributes	Diagnostics	Registration
Message	✓ Details					
Node Down	Name Category	No	deDown Fault 👻			
* Severity Critical 👻	Family	No	de			
Priority     None     Ifecycle State	Origin Correlation N	NN lature Ro	Mi ot Cause			
Closed Closed Closed Closed Source Node Closed Clos	Duplicate Co RCA Active Correlation N					
Source Object Closed	Time incident Time incident	t detected: Tues	12 seconds, 52 ms day, May 3, 2011 4:10:42 PM day, May 3, 2011 4:12:54 PM p.			
▼ Notes	First Occurre	ence Time Ma	ay 3, 2014 4:10:42 PM MDT			
Notes	Last Occurre	ence Time Ma	ay 3, 2014 4:10:42 PM MDT			
	Origin Occur	rrence Time Ma	ay 3, 2014 4:10:42 PM MDT			
			home		-	

4. Click Save after each Lifecycle State change.

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**

#### **Overview**

NNMi administrators define Node Groups to establish logical groups of devices. These Node Groups are used in a variety of ways. This section explains how they are used to create maps.

When NNMi Administrators create a Node Group:	🛧 Topology Maps 🛛 🛠
<ul> <li>The link to that Node Group's map automatically shows up under the Topology Maps &gt; All Node Groups folder in alphabetical order.</li> <li>The All Node Groups folder is visible only to NNMi Administrators.</li> <li>The Node Group Map icon is grey.</li> </ul>	<ul> <li>Node Group Overview</li> <li>Network Overview</li> <li>Node Group Maps</li> <li>Quick Access Maps</li> <li>Quick Access Maps</li> <li>All Node Groups</li> <li>Important Nodes</li> <li>Microsoft Windows Systems</li> <li>Name</li> <li>Neighbor Connections Filter</li> <li>Networking Infrastructure Devices</li> <li>Non-SNMP Devices</li> <li>Virtual Machines</li> <li>VMware ESX Hosts</li> </ul>
When the NNMi Administrator opens the Node Group Map and clicks the Save Map icon:	🔥 Topology Maps 🛛 🕆
Node Groups       Node Group       Name         Image: Image	<ul> <li>Node Group Overview</li> <li>Network Overview</li> <li>Node Group Maps</li> <li>Name</li> <li>Name</li> <li>Networking Infrastructure Devices</li> <li>Quick Access Maps</li> <li>All Node Groups</li> </ul>
If the the NNMi Administrator wants the new Node Group map to NNMi, use the Configuration > User Interface > User Interface Co	

# **Configure Node Groups**

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

See "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.

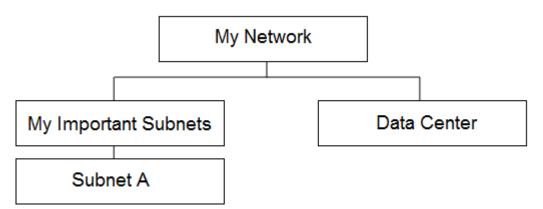
This example creates Node Groups for a few different subnets.

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.
- Click the Configuration workspace > Object Groups > Node Groups.
   On the Node Groups form, click the \* icon.

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

ode Groups 🔷 Node Group *						
] 🛛 🖶 🕈 🏝 Save and Close 🛛 🖉 🗙 Delete Node Group						
Basics	Device Filters	Additional Filters	Additional Nodes	Child Node Groups	Status	
Name Subnet A Calculate Status C Status No Status Add to View Filter List C otes	(question mark cisco*.hp.com	<ul> <li>to match exactly</li> <li>ftc??gs??.*.hp.co</li> <li>nclusive IP address</li> </ul>	one character in a s m	terisk) to match zero o tring. Valid examples f veen operator. Valid ex	or hostname: ci	sco?.hp.com,
u can filter Node Groups using Device Filters, Additional Filters, Additional des, and Child Node Groups. If you use Device Filters and Additional	Filter Editor Attribute		Operator	Value		)
res, Nodes must match at least one Device Filter and the Additional Filters ecifications to belong to this Node Group. Nodes that are specified as didional Nodes and Child Node Groups <i>always</i> are members of this Node oup. See Help $\rightarrow$ Using the Node Group form.	mgmtlPAddr	ess 💌	between	▼ 100:20.41 100:20.20.31		Append Insert Replace
test your Node Group definition, select File $\to$ Save, then Actions $\to$ Node oup Details $\to$ Show Members.						Append AND
NNM iSPI Performance						OR
ed by NNM iSPI Performance for Metrics and NNM iSPI for Traffic.	mgmtlPAdd	ress between	AND	2008.2008		NOT
dd to Filter List						EXISTS
]						NOT EXISTS Delete
aller a second as a second	Filter String mgmtlPAddres	ss between	AND		an dawah darihi	

2. Next, create the Data Center Node Group.

Figure 46: Node Group: Additional Filters Tab

lode Groups Node Group * ■   📴   🛗 🎦 🔛 Save and Close   🥔 🗙 Delete Node Group	<u>य</u>	
To test your Node Group definition, select File → Save, then Actions → Node Group Details → Show Members. NNM ISPI Performance Jsed by NNM ISPI Performance for Metrics and NNM ISPI for Traffic. Add to Filter List	sysName like data_center*	d ND DR OT ISTS EXISTS lete

- 3. 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

Node Groups 🔷 Node Group *	2
😕   📴 🎽 🏝 Save and Close   😂 🗙 Delete Node Group	3
✓ Basics	Device Filters Additional Filters Additional Nodes Child Node Groups Status
* Name My Important Subnets	· .
Calculate Status Vo Status	🔨 🖾 🗴 🕼 🛇 0 - 0 of 0 🖉 📄
Add to View Filter List	New Expand Child in Parent Node Group Map
Notes	Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y
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 <i>always</i> are members of this Node Group. See $Help \rightarrow Using$ the Node Group form.	
To test your Node Group definition, select File $\to$ Save, then Actions $\to$ Node Group Details $\to$ Show Members.	ſ
▼ NNM iSPI Performance	( (
Used by NNM iSPI Performance for Metrics and NNM iSPI for Traffic.	
Add to Filles risk	A second se

# 4. Click **W**, 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

ile View Tools	Actions Help			
Node Group Hierarchy *				1
😼   💾 🎽 (💾 s	ave and Close ) 😂 👂	Celete Node Group I	Hierarchy 🛛 🔛	
				1
Changes are no	ot committed until the top-le	aval form is saved		
() changes are no	t committee antii the top-it	ever form is saved:		
<ul> <li>Basics</li> </ul>				τ
The Node Group Hierar	chy relates a parent Node	e Group with a Child		
	roup maps, Child Node Gr			ļ
	t the entire Node Group, u p is enabled. This allows f		e	1
Groups. See Help $\rightarrow$ U	sing the Node Group Hiera	archy form.		
				4
Child Node Group	Subnet A	<u> </u>		1
Expand Child in Parent				₹
Node Group Map				
				1
Area Area				

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

Node Groups Node Group *	<u>}</u>
🗵   📴   🛅 🎽 🚰 Save and Close 🖉 🗶 Delete Node Group	
▼ Basics	Device Filters Additional Filters Additional Nodes Child Node Groups Status
* Name My Important Subnets	•
Calculate Status 🔽 Status No Status	* 🖻 🞜 🗙 🔯 🗘 1-1of1 🖉 🍳 🖻
Add to View Filter List 🔽	Name Expand Child in Parent Node Group Map
Notes	Subnet A -
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 Show Members.	

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 > Preview Members (Current Group Only).

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

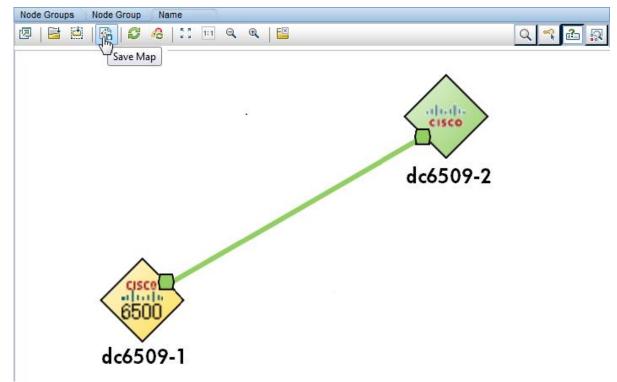
1. Click Actions > Maps > Node Group Map to open the map.

Figure 50: Actions: Map: Select Node Group Map

Metwork Node Manager					User Name:	system NNMi Role: A	dministrator
<u>File View Tool Actions Help</u>							7
Dashboards <u>Maps</u> Node Group Details	Node Group Map						
↑ Incident Managerr Management Mode ▶	🖉 🎝 📋 👔 🖄 Save and Close 🛛 🞜 🗶 Delete No	de Gro	oup 📔				
▲ Topology Maps ¥		Â	Device Filters	Additional Filters	Additional Nodes	Child Node Groups	Status
Monitoring ¥	* Name Data Center		•				
Troubleshooting ¥	Calculate Status		Device Filters	enable you to dete	rmine Node Group m	embers by Device Cat	egory, Vend
Inventory     ×	Status No Status					Nodes must match at	least one of
Management Mode ¥	Add to View Filter List		Filters and pa	iss any Additional P	ilters to belong to thi	is Node Group.	
🇞 Incident Browsing 🛛 🕹 🕹	Notes	=	* 📑	🗗 🔊 🗙			- 0 of 0 🐼
Integration Module Configuration	Modes with a system name beginning with data center			- 1 1			
			Device Cat	egony Device V	endor Device	e Family Dev	vice Model
🗄 🧰 Security	You can filter Node Groups using Device Filters. Additional Filters.						
📧 🧰 MIBs	Additional Nodes, and Child Node Groups. If you use Device						
Device Profiles	Filters and Additional Filters, Nodes must match at least one Device Filter and the Additional Filters specifications to belong to						
🖃 🗁 Object Groups	this Node Group. Nodes that are specified as Additional Nodes and Child Node Groups <i>always</i> are members of this Node Group.						
m Node Groups	See Help $\rightarrow$ Using the Node Group form.						
Interface Groups	To test your Node Group definition, select File → Save, then Actions → Node Group Details → Preview Members (Current	-					
Carlo and and the	Tetechnouellade G	de la constanción de la constanci de la constanción de la constanción de la constanc	No.ma				

2. Optional: You can move the icons around and click 🗟 Save Map (this changes everyone's copy of the map).

Figure 51: Topology Maps > All Node Groups > Node Group Map: Save Map



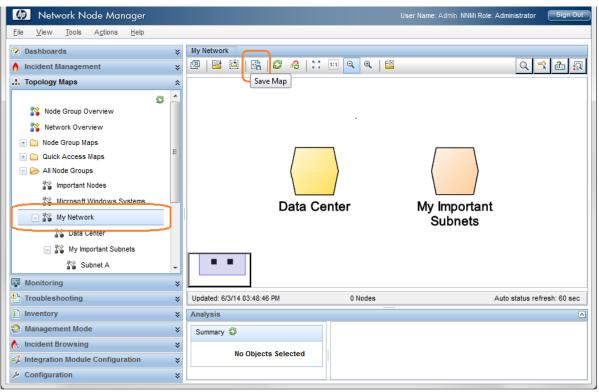
After you save the change, NNMi displays a message informing you that it created a Node Group map.

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 Maps**

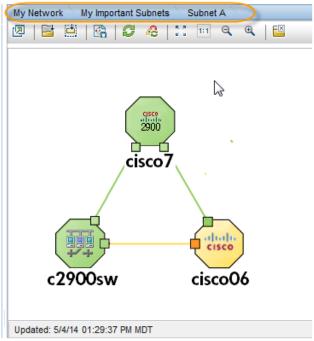
You now have a map hierarchy that you can navigate within. From the workspace navigation panel, select the **Topology Maps** workspace. If you do not see the newly created Node Group Maps, try refreshing the browser or signing out and back into NNMi.





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

#### 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:

- From the workspace navigation panel, select the Topology Maps workspace, expand the All Node Groups folder, and then click My Network to display the map. Click Save Map (this adds the map to the Node Group Maps Settings).
- 2. 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.

e View Tools Actions Help													
Dashboards	≽	Node Group Map Settings	$\geq$ $-$										
Incident Management	×	🗵   * 🖻   🖉	5	🔊   🗙	:   E	×							$\bowtie$
Topology Maps	×									Maxi			
Monitoring	×		Торо	C	Noc	Noc Grc	Minimum	Мар	Maxi Num	Num		Ind	
Troubleshooting	×	Name 🔺	Map Orde	Type	Noc	to Nor	NNMi Role to Save Layout	Refresh Interval	of Disp		Mult Thre		Background Image
Inventory	×		orac		Grc	Grc	ouvo Eujout	interrui	Node	End Poin		mo	inage
Management Mode	≈	Data Center	50	Layer 2		-	Administrator					-	
Incident Browsing	×	My Network	50	Layer 2	-	-	Administrator	$\mathbf{)}$				-	
Integration Module Configuration	×	Networking Infrastructure	10	Layer 3	-	-	Administrator			275		-	
Configuration	*	Routers Switches	15 20	Layer 3 Layer 2	-	-	Administrator Administrator		75 100	200 250		-	
<ul> <li>☐ Monitoring</li> <li>☐ Incidents</li> <li>☐ Status Configuration</li> </ul>		Updated: 5/4/11 01:33:33 Analysis	PM ME	т				Total: 5		Select	ed: 1		Filter: OFF
📑 Global Network Management		-	_										
🗉 🗁 User Interface		Node Group Map Setting	)s Sum	mary : My	Netw	ork i						50	
📑 User Interface Configuration		Name Minimum NNMi Role to S	ave Me		Netw ninis		Connectivi	Maps Orderi ity Type	ing				er 2
m Node Group Map Settings		Minimum NNMI Role to 3	avema	p Adr	ninis	trato		lode Groups	s			fals	e
🗰 Menus								ips to Node	-	8		fals	
🛲 Menu Items								ibnet Conne er Connecti		•		fals fals	
icons								Number of D			es	125	
🗄 🧰 Security							Maximum M	Number of D	isplaye	d End	Points	275	
🗄 🧰 MIBs								ey Incidents				fals	e
m Device Profiles							Backgroun	nd Image Sc	ale			1.0	

Figure 54: Configuration > Node Group Map Settings

- 3. Double-click My Network.
- 4. 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.

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

🧑 Network Node Manager		UserN
<u>File View Tools Actions H</u> elp		
② Dashboards ::	Node Group Map Settings Node Group Map Settings	
👌 Incident Management :	🗴 🖉   📴   🖺 🎽 🎬 Save and Close   🥩 🗙 Delete Node Group Ma	p Settings
\Lambda Topology Maps	✓ Basics	Connectivity Background Image
Monitoring :	×	Background Image
Troubleshooting :	Node Group My Network	
Inventory :	Optional. If it is set, this map is displayed in the Topology Maps workspace	Enter a relative URL to an NNMi background i image. To view the set of NNMi background in
Management Mode :	Quick Access Maps folder according to the ordering number	To view the set of images added to NNMi, bro An example NNM-supplied Background Image
lncident Browsing :	Topology Maps Ordering 5	states.png. An example user-supplied Backg /mybackground.jpg.
💱 UI Extensions Test	Minimum NNMi Role to     Save Map     Administrator	
Integration Module Configuration	Optional. Use these attributes to override the values set in the User Interface	■ To test your map settings, select File → Save
J Configuration	Configuration form.	Background Image
📑 Communication Configuration 📥	Map Refresh Interval 0.00 Seconds	/nnmbg/continents/europe.png
🛨 🧰 Discovery	Maximum Number of	The background image can be scaled in prop
\pm 🧰 Monitoring 😑	Displayed Nodes Maximum Number of	number greater than 1.0 to make the image la nodes). Use a number less than 1.0 to make
\pm 🧰 Incidents	Displayed End Points	background image. For example, a scale value
Status Configuration	Multiconnection Threshold	to the map objects.
Global Network Management	Select to indicate Key Incidents by enlarging the source map object in the Node	* Background Image Scale 1
User Interface	Group map.	
User Interface Configuration	Indicate Key Incidents	
m Node Group Map Settings		·

To specify the **My Network** map as the initial view:

1. Click User Interface Configuration.

# Figure 56: Configuration: User Interface Configuration

Metwork Node Manager	
<u>File View Tools Actions H</u> elp	
② Dashboards	×
👌 Incident Management	*
🛧 Topology Maps	≽
Monitoring	*
Troubleshooting	×
Inventory	×
🚱 Management Mode	*
🇞 Incident Browsing	≽
4 Integration Module Configuration	≽
Ju Configuration	*
🛨 🧰 Discovery	*
🛨 🧰 Monitoring	
🛨 🧰 Incidents	
📑 Status Configuration	
📑 Global Network Management	=
📃 🗁 User Interface	
📑 User Interface Configuration	
🛅 Node Group Map Settings	
🛲 Menus	
🛲 Menu Items	
icons	-

2. Change the **Initial View** selection to the **First Node Group in Quick Access Maps folder**. This is the My Network map because we set the **Topology Maps Ordering** attribute value to **5**.

Click 🕙 Save and Close.



User Interface Configuration	ose 😝   🖾						2		
			Default Map Settings	Defa	ult Line Grap	oh Settings			
Console Timeout     Initial View	18.00 Hours v		✓ Default Map Setting			·			
* Default Author	All Nodes Table Nodes Table (All Attributes)	^		ab in t	ings for map views. These settings can be o the User Interface Configuration form.				
If you are using NNM iSPIs w to redirect URL requests to t "Open the NNMi Console" in	Network Overview Map Node Group Overview Map Networking Infrastructure Node Group Map		<ul> <li>Maximum Number ( Displayed Nodes</li> <li>Maximum Number (</li> </ul>	of	125				
Enable URL Redirect	Routers Node Group Map Switches Node Group Map		<ul> <li>Displayed End Poir</li> <li>Multiconnection Threshold</li> </ul>		5				
Show Unlicensed Features Enable Table Row Shading	First Node Group in Quick Access Maps folder best Node Group in Quick Access Maps folder None (blank view)	Ţ	Select to indicate Key		ents by enlar	rging the sou	rce map object in th		
Last Modified	June 3, 2014 3:26:21 PM MDT								
	and the second se	-		A.,			A Amaral		

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

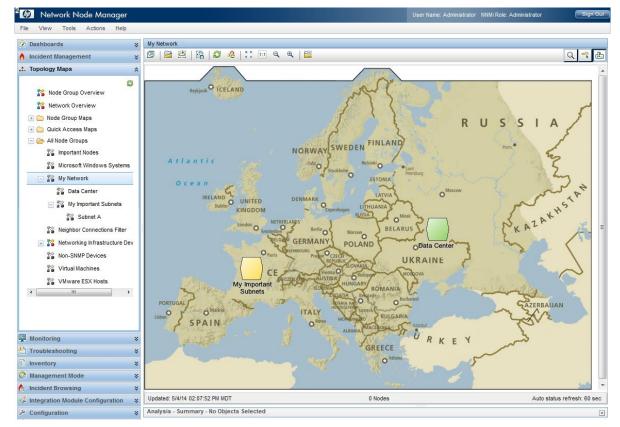


Figure 58: My Network Map

# **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 Linux 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 Linux 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

🕼 Network Node Man	nager	
File View Tools Actions	Help	{
② Dashboards	Getting Started with NNMi	
👌 Incident Management	🖓 Help for Operators	2
Open Key Incidents	Not Help for Administrators	$\geq$
	NNMi Documentation Library	
Unassigned Open Key Inc	HP Software Support Website	Γ.
My Open Incidents	🛈 System Information ျက	1
	What's New?	Ρ.
	About HP Network Node Manager i Software	1

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

System Information						83
Product     Health	Server	Database	State Poller	Custom Poller	►	•
NNMi System Health						
Status: Normal Last Updated: 5/4/14: 3:42 PM						
No Problems Detected						
View Detailed Health Report (	(Support)					
	ß					

# **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.

Tip: NNMi can forward Key Incidents to other products, such as HP Operations Manager (HP OM).

#### **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.

🕼 Network Node Manager			User Name: Administrator NNMi Role: Administrator	Sign O
File View Tools Actions Help				
🕗 Dashboards 🛛 😵	Open Key Incidents			
👌 Incident Management 🛛 🔗	. 🖉   🗃   🞜 🗟   🔊 💎   🗙   🖺	3	Last Day 👻 <set filter="" group="" node=""> 👻 🔯 1 - 15 of 15</set>	
Open Key Incidents	Sev Pric Life Last Occurrentee Assigned	Source Node Source O	bject Cat Fan Orie Cor Message	Notes
Unassigned Open Key Incidents	🔇 5 🖳 🍓 5/4/11 4:36:18 PM	ntc-g430 NO NAME	nterface NO NAME. The inDiscardRateState transitioned 🕺 🚳 🔊	
III My Open Incidents	😒 5 🖳 🍓 5/4/11 4:35:38 PM	ntc2ext-gw2 VI26	n 🔊 🖏 😼 🥻 High output discard rate on interface VI26. The outDiscardRateState transitioned fro	
.Λ. Topology Maps ⇒	😒 5 🖳 🍓 5/4/11 4:35:38 PM	ntc2ext-gw2 VI25	🝙 瑟 ங 🔀 High output discard rate on interface VI25. The outDiscardRateState transitioned fro	
	😒 5 🖳 🍓 5/4/11 4:35:38 PM	ntc2ext-gw2 VI23	🝙 🐉 ங 🔀 High output discard rate on interface VI23. The outDiscardRateState transitioned fro	
	😒 5 🖳 🍓 5/4/11 4:35:38 PM	ntc2ext-gw2 VI21	🝙 🐉 ங 🔀 High output discard rate on interface VI21. The outDiscardRateState transitioned fro	
	😒 5 🖳 🖏 5/4/11 4:34:28 PM	vwanrouter-1 vwanroute	r-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 Fa	n Tra; 🛋 🧃 😼 🔀 Fan on ntc6kgw2 is malfunctioning	
	🛆 5 🗓 🖏 5/4/11 4:04:27 PM	vwanrouter-1 vwanroute	r-1 🔺 р ங 🖳 Rate Correlation for NodeDown: Node Down	
	🛆 5 🖳 🖏 5/4/11 3:40:24 PM	vwanrouter-1 vwanroute	r-1 🛛 🕋 🎁 🖏 🔤 Rate Correlation for NodeDown: Node Down	
	😒 5 🗓 🖏 5/4/11 11:36:28 AM	c2950t Fa0/1	🝙 瑟 ங 🔀 High input discard rate on interface Fa0/1. The inDiscardRateState transitioned from	r
	🖸 🖸 5.0 🖏 5/4/11 6:41:17 AM	mplspe01 Se0/2/0	🝙 🎏 ங 🔀 High input utilization on interface Se0/2/0. The inUtilizationState transitioned from NC	
Troubleshooting \$	S 5. 2 5/3/11 8:08:47 PM	core_6509-1 Tu3	🔹 📰 ங 🔀 Interface Down with Alias = tunnel to eastcoast-gw1 for multicast	
Inventory \$	🐼 5. 🖳 5/3/11 8:08:47 PM	wanrouter-1 Tu2	🔹 📰 ங 🔀 Interface Down with Alias = tunnel to ntc2rams	
Management Mode 🛛 🕹		10.161.4.3 10.161.4.3	🔹 🕮 🛂 🔀 Non-SNMP Node Unresponsive	
Incident Browsing \$			6	
${}^{2}$ Integration Module Configuration $~~st$	Updated: 5/4/11 04:37:02 PM MDT		Total: 15 Selected: 0 Filter: ON	Auto refresh: 30 se
Configuration ¥	Analysis - Summary - No Objects Selected			

#### Figure 61: Open Key Incidents

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.

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:

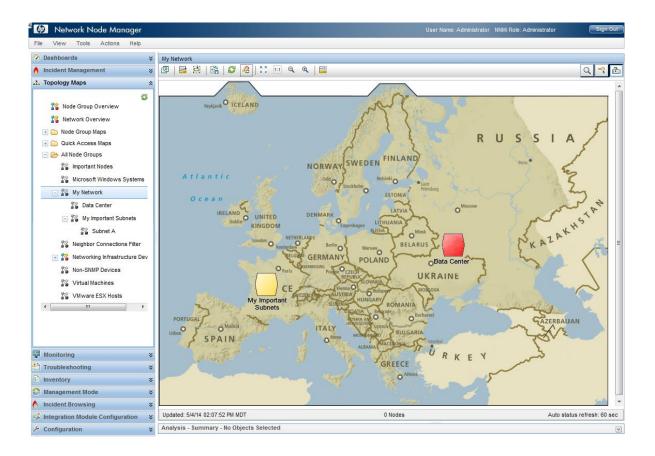
- The status is propagated from the Child Node Group nodes up to the parent Node Group maps.
- By default, NNMi propagates the most critical node status in the Node Group up the hierarchy. This enables you to monitor node status from a high level.
- When a top-level Node Group map changes color from 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.

#### 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

ile View Tools Actions Help										
Dashboards	¥	Non-Norma	I Nodes	>						
h Incident Management 🛛 🕹		🖉   🚰   🞜 尾   🕫 💎   🗙   🔛					<set filter="" group="" node=""> 🗸 🕼 🖓 1 - 6 of 6</set>			
🔈 Topology Maps	*	Status⊽	Device	Name	Hostname	Management Address	Tenant	Security Group	System Location	Device Profile
Monitoring	*	8		mimwin1	mimwin1.sup	10.97.145.168	Default T	Default Security G	SAPro01	microsoftNTWo
Non-Normai Node Sensors		8	<u>101</u>	mimsp-n	mimsp-nec5(	10.97.145.242	Default T	Default Security G	SAPro01	nec5010
Non-Normal Physical Sensors     Non-Normal Chassis	=	<u> </u>	<u>111</u>	mimhp4k	mimhp4k1sw	10.97.145.98	Default T	Default Security G	SAPro01	hp4000M
📅 Non-Normal Cards	- 11	<u> </u>	鏾	mulder	mulder.super	10.97.145.57	Default T	Default Security G	SAPro01	enterasysXP-86
📰 Non-Normal Interfaces		Δ	龤	sp-cp-w	sp-cp-wan-r	10.97.145.80	Default T	Default Security G	SAPro01	hp9308m
Non-Normal Nodes		4	1 <b>1</b> 11	sp-unnu	sp-unnum4.s	10.6.3.4	Default T	Default Security G	SAPro01	cisco3620

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.

# 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.

# We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click <u>here</u>.

If no email client is available, copy the information below to a new message in a web mail client, and then send this message to **ovdoc-nsm@hp.com**.

Product name and version: NNMi 10.00

Document title: Step-by-Step Guide to Deploying NNMi

Feedback:

# **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 2009–2014 Hewlett-Packard Development Company, L.P.

### **Trademark Notices**

Adobe<sup>®</sup> 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.

Intel<sup>®</sup> is a trademark of Intel Corporation in the U.S. and other countries.

Microsoft<sup>®</sup> and Windows<sup>®</sup> are U.S. registered trademarks of Microsoft Corporation.

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

Red Hat<sup>®</sup> Enterprise Linux Certified is a registered trademark of Red Hat, Inc. in the United States and other countries.

UNIX<sup>®</sup> 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