HP Network Node Manager i Software

For the Windows®, HP-UX, Linux, and Solaris operating systems

Software Version: NNMi 9.1x Patch 5

Deployment Reference

Document Release Date: January 2013
Software Release Date: January 2013

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notice

Trademark Notices

Oracle Technology — Notice of Restricted Rights

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)

Available Product Documentation

In addition to this guide, the following documentation is available for NNMi:

- *HP Network Node Manager i Software Documentation List*—Available on the HP manuals web site. Use this file to track additions to and revisions within the NNMi documentation set for this version of NNMi. Click a link to access a document on the HP manuals web site.
- *HP Network Node Manager i Software Installation Guide*—Available for each supported operating system on the product media and the NNMi management server.
- *HP Network Node Manager i Software Upgrade Reference*—Available on the HP manuals web site.
- *HP Network Node Manager i Software Release Notes*—Available on the product media and the NNMi management server.
- *HP Network Node Manager i Software System and Device Support Matrix*—Available on the product media and the NNMi management server.
- *HP Network Node Manager iSPI Network Engineering Toolset Planning and Installation Guide*—Available on the NNM iSPI NET diagnostics server product media.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

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

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online 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 and associated patch documentation
- 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 user ID, go to:

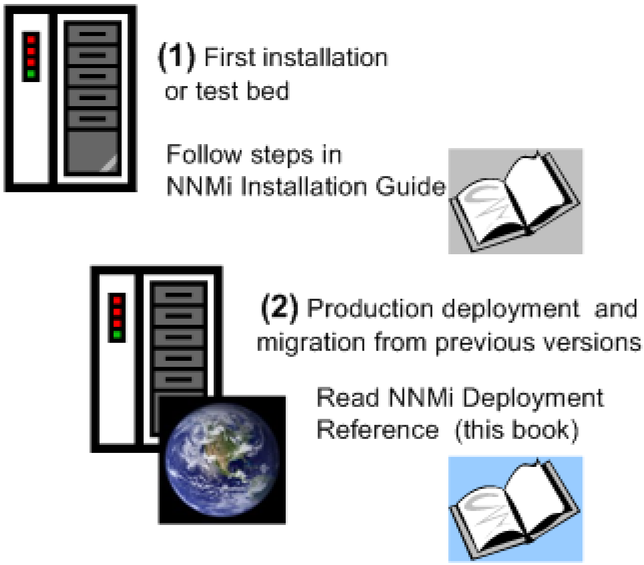
http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

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

Contents

About This Guide



This chapter contains the following topics:

- What Is in This Guide?
- Path Conventions Used in This Document
- Revision History
- For More Information about NNMi

What Is in This Guide?

This guide contains a collection of information and best practices for deploying HP Network Node Manager i Software, including NNMi and NNMi Advanced. This guide is for an expert system administrator, network engineer, or HP support engineer with experience deploying and managing networks in large installations.

This guide assumes that you have already installed NNMi in a limited (test) environment, and that you are familiar with start-up configuration tasks, such as using the Quick Start Configuration wizard to configure community strings, set up discovery for a limited range of network nodes, and create an initial administrator account. To learn more about these tasks, see the *NNMi Installation Guide* (see Available Product Documentation on page 3).

HP updates this guide between product releases, as new information becomes available. For information about retrieving an updated version of this document, see Available Product Documentation on page 3.

Path Conventions Used in This Document

For commands located in the NNMi `bin` directory, this document does not include the command path. The NNMi `bin` directory is located as follows:

- *Windows Server 2008*: `<drive>\Program Files\HP\HP BTO Software\bin`
- *UNIX®*: `/opt/OV/bin`

This document primarily uses the following two NNMi environment variables to reference file and directory locations. This list shows the default values. Actual values depend on the selections that you made during NNMi installation.

- *Windows Server 2008*:
  - `%NnmInstallDir%`: `<drive>\Program Files\HP\HP BTO Software`
  - `%NnmDataDir%`: `<drive>\ProgramData\HP\HP BTO Software`

  On Windows systems, the NNMi installation process creates these system environment variables, so they are always available to all users.

- *UNIX*:
  - `$NnmInstallDir`: `/opt/OV`
  - `$NnmDataDir`: `/var/opt/OV`

  On UNIX systems, you must manually create these environment variables if you want to use them.

Additionally, this document references some of the NNMi environment variables that you can source as part of your user log-on configuration on the NNMi management server. These variables are of the form `NNM_*`. For information about this extended list of NNMi environment variables, see Other Available Environment Variables on page 639.

Revision History

The following table lists the major changes for each new release of this document.

Document Release Date	Description of Major Changes
March 2011 (9.10)	Entirely updated. • Fourth English edition. • Third Japanese edition.
June 2011 (9.1x Patch 1)	• Added HP ArcSight Logger chapter. • Updated HP Network Automation chapter. • Updated Configuring NNMi in a High Availability Cluster chapter. • Added Enabling the Auto-Trim Oldest SNMP Trap Incidents Feature (No Incident Archive) section to Maintaining NNMi chapter.
September 2011 (9.1x Patch 2)	Updated the following: • About This Guide section • Changing the NNMi Management Server chapter • Configuring NNMi for Application Failover chapter • Configuring NNMi in a High Availability Cluster Cluster • Hardware and Software Requirements chapter • HP ArcSight Logger chapter • HP Business Service Management Topology chapter • HP Universal CMDB chapter • Maintaining NNMi chapter • NNMi Northbound Interface chapter • NNMi Security and Multi-Tenancy chapter • Upgrading from NNMi 9.0x section • Working with Certificates for NNMi chapter
January 2012 (9.1x Patch 3)	• Updated the PCM+ chapter • Updated the Additional Upgrade Information chapter • Updated the HP Network Automation chapter
January 2013 (9.1x Patch 5)	Updated the following: • Maintaining NNMi chapter • NNMi Console chapter • NNMi 9.10 and Well-Known Ports appendix Added the following: • NNMi 9.10 iSPI Well-Known Ports appendix

For More Information about NNMi

To obtain a complete set of information about the NNMi product, use this guide along with other NNMi documentation. The table below shows all NNMi documents to date, including both guides and white papers.

➤ All information below can be downloaded from **http://h20230.www2.hp.com/ selfsolve/manuals**. See Available Product Documentation on page 3 for more information.

What do you want to do?	**Where to find more information**
View a list of available documentation for this version of NNMi.	Download the *NNMi Documentation List*. Use this file to track additions to and revisions within the NNMi documentation set for this version of NNMi. Click a link to access a document on the HP manuals web site.
Install NNMi or NNMi Advanced (first time).	Download the *NNMi Installation Guide*. This guide contains basic steps to install and un-install the product, plus how to do an initial configuration using the NNMi Quick Start Configuration Wizard. • *HP Network Node Manager i Software Installation Guide for the Windows Operating System* • *HP Network Node Manager i Software Installation Guide for the HP-UX Operating System* • *HP Network Node Manager i Software Installation Guide for the Linux Operating System* • *HP Network Node Manager i Software Installation Guide for the Solaris Operating System*
Plan for network deployment, including links to system requirements.	See Preparation on page 31 of this guide.
Configure NNMi for a production environment.	See Configuration on page 37 of this guide.
Configure NNMi behind the scenes.	See Advanced Configuration on page 115 of this guide.
Maintain the NNMi configuration.	See Maintaining NNMi on page 351 of this guide.
Upgrade to NNMi from previous versions of Network Node Manager i Software (NNMi 9.0x).	See Upgrading from NNMi 9.0x on page 401 of this guide.
Upgrade to NNMi from previous versions of Network Node Manager (NNM 6.x/7.x).	Download the *NNMi Upgrade Reference*.
Learn more about products that integrate with NNMi.	See Integrations with NNMi on page 417 of this guide.
Reference NNMi environment variables, ports, and messages.	See Additional Information on page 637 of this guide.
Obtain more information about a specific topic.	Download by example documents and white papers.

What do you want to do?	Where to find more information
Print the NNMi help.	Download PDFs of the help content.
Install the HP NNM iSPI NET (NNM iSPI NET) diagnostics server and learn about NNM iSPI NET functionality.	Download the *HP NNM iSPI Network Engineering Toolset Planning and Installation Guide* from the Network Node Manager SPI for NET product category for the Windows operating system.
Obtain documentation about the NNMi Developer Toolkit (SDK).	See Licensing NNMi to review information related to the SDK, obtaining and installing an SDK license, and viewing SDK documentation and samples.

Preparation

This section contains the following chapter:

Hardware and Software Requirements

This chapter contains the following topics:

- Supported Hardware and Software
- Checking for Required Patches
- System Configuration (UNIX)
- Installing NNMi and the NNM iSPIs
- NNMi Coexistence with HP Performance Insight
- NNMi Coexistence with HP Operations Agent
- NNMi 9.1x and NNM iSPI Performance for Metrics Version Requirements

Supported Hardware and Software

Before installing NNMi, read the information about NNMi hardware and software requirements described in Table 1.

For current versions of all documents listed here, go to:

http://h20230.www2.hp.com/selfsolve/manuals

Table 1 Software and Hardware Pre-Installation Checklist

Complete (y/n)	Document to Read
	NNMi Installation Guide • **Filename** = `install-guide_en.pdf` • **Windows Media** = DVD main drive (root) • **UNIX Media** = Root directory • **NNMi console** = **Help > NNMi Documentation Library > Installation Guide**
	NNMi Release Notes • **Filename** = `releasenotes_en.html` • **Windows Media** = DVD main drive (root) • **UNIX Media** = Root directory • **NNMi console** = **Help > NNMi Documentation Library > Release Notes**
	NNMi System and Device Support Matrix • **Filename** = `supportmatrix_en.html` • **Windows Media** = DVD main drive (root) • **UNIX Media** = Root directory • **NNMi console** = Linked from the release notes

➤ HP updates the *NNMi System and Device Support Matrix* as new information becomes available. Before you deploy NNMi, check for the most recent NNMi support matrix for your version of the software at:

http://www.hp.com/go/hpsoftwaresupport/support_matrices

(You must have an HP Passport ID to access this web site.)

➤ If you plan to install NNM Smart Plug-ins (NNM iSPIs), include the system requirements for those products as you plan the NNMi deployment.

Checking for Required Patches

NNMi ships an embedded Java virtual machine and JDK version 1.6. Java requires specific operating system patches to function properly. If you plan to install NNMi on a server running the HP-UX operating system, you can run the **`HPjconfig`** command to see if the server has the required patches installed. When you run **`HPJconfig`**, make the correct selection for JDK version 1.6. See the following URL for more information about installing and running **`HPjconfig`** on HP-UX: **https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPJCONFIG**

If you plan to install NNMi on servers running supported operating systems other than HP-UX, consult the release notes for those operating systems.

System Configuration (UNIX)

If you cannot display NNMi manpages on the NNMi management server, verify that the `MANPATH` variable contains the `/opt/OV/man` location. If it does not, add the `/opt/OV/man` location to the `MANPATH` variable.

NNMi uses a configuration file located in the `/etc/opt/OV` directory. Do not delete this directory.

Installing NNMi and the NNM iSPIs

If you plan to use any of the HP NNM iSPIs along with NNMi, install NNMi before installing any of the HP NNM iSPIs.

NNMi Coexistence with HP Performance Insight

If you plan to install NNMi on the same server as HP Performance Insight, follow this procedure to avoid problems with the installation sequence and port conflicts:

1. Install HP Performance Insight first.

   Do not install NNMi until after you complete step 1 and step 2.

2. Stop all HP Performance Insight processes.
3. Install NNMi. See the *NNMi Installation Guide* for specific instructions.
4. Stop all NNMi processes:

   ```
   ovstop -c
   ```

5. Modify the `nms-local.properties` file to resolve any port conflicts. You can find this file in the following directory:
   - *Windows*: `%NNM_CONF%\nnm\props`
   - *UNIX*: `$NNM_CONF/nnm/props`
6. Start HP Performance Insight processes.

7 Start all NNMi processes:

```
ovstart -c
```

⚠ When NNMi is installed on the same server as HP Performance Insight, uninstalling NNMi causes an exception when running the HP PI MIB Browser. To prevent this exception, complete the following steps:

1 Uninstall NNMi.

2 Recreate the snmpmib MIB database:

   a `mkdir -p /var/opt/OV/shared/nnm/conf/`

   b `/opt/OV/lbin/nnmloadmib -load /usr/OVPI/mibs/GENMIB2IF.mib`

3 Use the `nnmloadmib.ovpl` command to load additional MIBs.

NNMi Coexistence with HP Operations Agent

If you plan to install an HP Operations agent on the NNMi management server (for communicating with HP Operations Manager (HPOM)), install NNMi before installing the HP Operations agent.

NNMi 9.1x and NNM iSPI Performance for Metrics Version Requirements

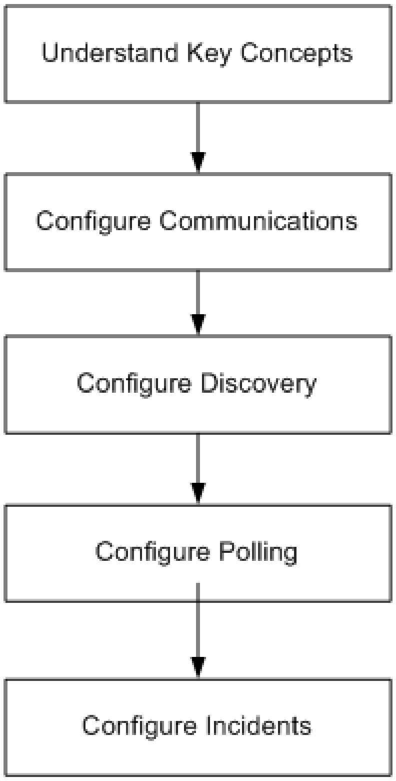
NNMi 9.1x and NNM iSPI Performance for Metrics must have equivalent versions:

- NNM iSPI Performance for Metrics version 9.10 is only supported with NNMi 9.10.
- NNM iSPI Performance for Metrics version 9.11 is only supported with NNMi 9.1x patch 1 (9.11).

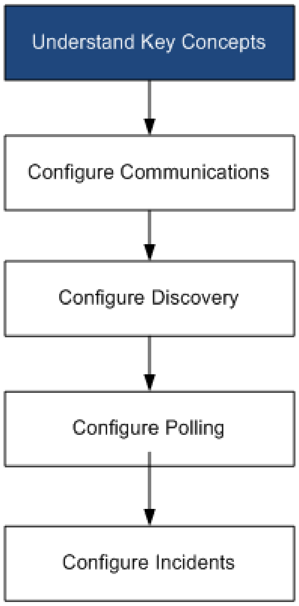
Configuration

This section contains the following chapters:

- General Concepts for Configuration
- NNMi Communications
- NNMi Discovery
- NNMi State Polling
- NNMi Incidents
- NNMi Console



General Concepts for Configuration



Read this chapter for an introduction to concepts that are explained in more detail later in this guide. This chapter also contains some best practices that apply to all HP Network Node Manager i Software (NNMi) configuration areas.

This chapter contains the following topics:

- Task Flow Model
- Best Practice: Save the Existing Configuration
- Best Practice: Use the Author Attribute
- User Interface Model
- Ordering
- Node Groups and Interface Groups
- Node/Interface/Address Hierarchy
- Stop Everything and Start Over Again

Task Flow Model

The chapters in the configuration section of this guide support the following task flow:

1. **Concepts**—Gain a general understanding of the configuration area. The information in this guide supplements the information in the NNMi help.
2. **Plan**—Decide how you want to approach the configuration. This is a good time to begin or update your company's network management documentation.
3. **Configure**—Use a combination of the NNMi console, configuration files, and command line interface to enter the configuration into NNMi. See the NNMi help for specific procedures.

⚠ Writing, amending, or changing configurations in the embedded database using command line interfaces (such as PSQL commands) or external utilities is not supported. Attempting to do so may cause irreparable damage to the database.

4 **Evaluate**—In the NNMi console, examine the results of your configuration. Adjust the configuration as necessary to achieve the desired results.

5 **Tune**—Optional. Adjust the configuration to improve NNMi performance.

Best Practice: Save the Existing Configuration

It is a good idea to save a copy of the existing configuration before you make any major configuration changes. If you do not like the results of your configuration changes, it is easy to revert to your saved configuration.

Use the nnmconfigexport.ovpl command to save the current configuration. To recover a saved configuration, use the nnmconfigimport.ovpl command.

For information about how to use these commands, see the appropriate reference pages, or the UNIX manpages.

The nnmconfigexport.ovpl command does not retain SNMPv3 credentials. For more information, see the *nnmconfigexport.ovpl* reference page, or the UNIX manpage.

Best Practice: Use the Author Attribute

Many NNMi configuration forms include the **Author** attribute.

As you create or modify the configurations on these forms, set the **Author** attribute to a value that identifies your organization. When you export the NNMi configuration, you can specify an author value to pull only those items that your organization has customized.

When you upgrade NNMi, the installer does not overwrite any configurations whose author value is not HP.

User Interface Model

Some NNMi console forms use a transactional approach to updating the database. The changes that you make in the NNMi console forms do not take effect until you save and close the forms all of the way back to the NNMi console. If you close a form that contains unsaved changes (on that form or on a contained form), NNMi warns you about the unsaved changes and gives you a chance to cancel the close.

The **Discovery Seed** form is one exception to the transactional approach. This form is provided on the **Discovery Configuration** form as a convenience, but it is disconnected from the rest of discovery configuration. For this reason, you must save and close the **Discovery Configuration** form to implement your auto-discovery *rules* before you configure any discovery seeds for those rules.

Ordering

Some NNMi console configuration forms include the **Ordering** attribute, which sets the priority for applying the configurations. For one configuration area, NNMi evaluates each item against the configurations from the smallest (lowest) ordering number to the next lowest ordering number, and so on, until NNMi finds a match. At that point, NNMi uses the information from the matching configuration and ceases to look for any more matches. (The communication configuration is an exception. NNMi continues to search for information at other levels to complete the communication settings.)

The **Ordering** attribute plays an important role in NNMi configuration. If you see unexpected discovery or status results, check the ordering of the configurations for that area.

Ordering applies within the local context. The Menus and Menu Items tables contain multiple objects with the same ordering number because of the local context idea.

Ordering numbers are also used in the following places, but with different meanings:

- Ordering on the **Menu** and **Menu Item** forms sets the order of items in the local context of the associated menu.
- Topology maps ordering on the **Node Group Map Settings** form sets the order of items in the **Topology Maps** workspace.

For specific information about how the **Ordering** attribute affects a given configuration area, see the NNMi help for that area.

Best practice

For each configuration area, apply low ordering numbers to the most restrictive configurations, and apply high ordering numbers to the least restrictive configurations.

Best practice

For each configuration area, all ordering numbers must be unique. During initial configuration use ordering numbers with a standard interval to provide flexibility for future modifications to the configuration. For example, give the first three configurations the ordering numbers 100, 200, and 300.

Node Groups and Interface Groups

In NNMi, the primary filtering technique is to group nodes or interfaces, and then applying settings to a group or filtering visualizations by group. Node groups can be used for any or all of the following purposes:

- Monitoring settings
- Incident payload filtering
- Table filtering
- Customizing map views
- Filtering the nodes passed from a regional manager to the global manager for the global network management feature

Interface groups can be used for either or both of the following purposes:

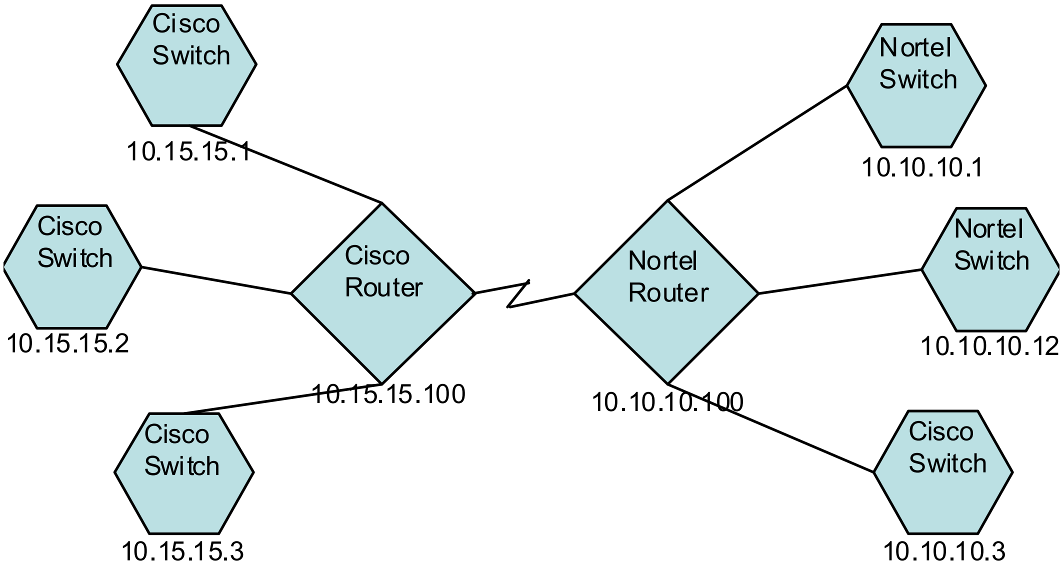
- Excluding interfaces from discovery

- Monitoring settings
- Incident payload filtering
- Table filtering

You can create a hierarchy of node groups based on any filterable attributes to control map view drill-down, monitoring or both settings inheritance.

Group Overlap

Regardless of the intended uses for group definitions, the first step is to define which nodes or interfaces are members of a group. Because you can create groups for different purposes, each object can be included in multiple groups. Consider the following example:



- For monitoring purposes, you might want to set a polling interval of 3 minutes for all switches, regardless of vendor or location. You can do this with a device category filter.
- For maintenance purposes, you might want to group all Cisco switches so that you can place them OUT OF SERVICE together for IOS upgrades. You can do this with a vendor filter.
- For visualization, you might want to group all devices on the 10.10.*.* site into a container with propagated status. You can do this with an IP address filter.

The Cisco switch with IP address 10.10.10.3 would qualify for all three groups.

You want to find the balance between having a usably rich set of groups available for configuration and viewing, and overloading the list with superfluous entries that will never be used.

Node Group Membership

NNMi determines node group membership by comparing each discovered node to each of the configured node groups.

- All nodes specified on the **Additional Nodes** tab are members of the node group.

  Rarely use the **Additional Nodes** tab to add nodes to a node group, as it consumes excessive resources on the NNMi management server.

- All nodes that are members of at least one node group specified on the **Child Node Groups** tab are members of the node group.
- Any node that matches one or more entries (if any exist) on the **Device Filters** tab *and* the filter specified on the **Additional Filters** tab is a member of the node group.

Hierarchies/Containment

You can create simple, reusable, atomic groups and combine them hierarchically for monitoring or visualization. Using hierarchical containers for nodes greatly enhances map views by providing cues about the location or type of object at fault. NNMi gives you complete control of the definition of the groups and their drill-down order.

You can create simple, reusable atomic groups first, and then specify them as child groups as you build up. Alternatively, you can specify your largest parent group first and create child groups as you go.

For example, a network might contain Cisco switches, Cisco routers, Nortel switches, and Nortel routers. You can create parent groups for Cisco devices and for all switches. Because the hierarchy is specified when you create the parent and designate its children, each child group, such as Cisco switches, can have multiple parents.

Hierarchies work well for the following situations:

- Types of nodes with similar monitoring needs
- Geographical locations of nodes
- Types of nodes to be taken OUT OF SERVICE together
- Groups of nodes by operator job responsibility

When you use groups in map views and table views, you see a (configurable) propagated status for the group.

Keep in mind that as you use group definitions to specify monitoring configuration, hierarchy does *not* imply ordering for settings. The settings with the lowest ordering number apply to a node. By carefully incrementing ordering numbers, you can emulate inheritance concepts for settings.

The configuration interface automatically prevents circular hierarchy definitions.

Device Filters

During discovery, NNMi collects direct information through SNMP queries and derives other information from that through device profiles. (For more information, see NNMi Derives Attributes through Device Profiles on page 60.) By gathering the system object ID, NNMi can index through the correct device profile to derive the following information:

- Vendor

- Device category
- Device family within the category

These derived values, in addition to the device profile itself, are available for use as filters.

For example, you can group all objects from a specific vendor, regardless of device type and family. Or you can group all devices of a type such as router, across vendors.

Additional Filters

With the additional filters editor, you can create custom logic to match fields including:

- hostname (Hostname)
- mgmtIPAddress (Management Address)
- hostedIPAddress (Address)
- sysName (System Name)
- sysLocation (System Location)
- sysContact (System Contact)
- capability (Unique Key of the Capability)
- customAttrName (Custom Attribute Name)
- customAttrValue (Custom Attribute Value)

Filters can include the `AND`, `OR`, `NOT`, `EXISTS`, `NOT EXISTS`, and grouping (parentheses) operations. For more information, see *Specify Node Group Additional Filters* in the NNMi help.

Capabilities are primarily intended for other programs that integrate with NNMi. For example, router redundancy and component health add capabilities (fields) to the NNMi database. You can view these capabilities by examining the node details from a device that has already been discovered.

Custom attributes can be added by iSPIs, or you can create your own custom attributes. If you have not purchased the Web Services SDK, you must place values in the field for each node manually. For example, an asset number or serial number might be an attribute that is not a capability.

Additional Nodes

It is better to use **Additional Filters** to qualify nodes for node groups. If the network contains critical devices that are too difficult to qualify using filters, add them to a group by individual hostname. Only add nodes to a node group by individual hostnames as a last resort.

Rarely use the **Additional Nodes** tab to add nodes to a node group, as it consumes excessive resources on the NNMi management server.

Node Group Status

When configured to do so, NNMi determines the status of a node group using one of the following algorithms:

- Set the node group status to match the most severe status of any node in the node group. To use this approach, select the **Propagate Most Severe Status** check box on the **Status Configuration** form.
- Set the node group status using the thresholds set for each target status. For example, the default threshold for the target status of Minor is 20%. NNMi sets the status of the node group to Minor when 20% (or more) of the nodes in the node group have Minor status. To use this approach, clear the **Propagate Most Severe Status** check box on the **Status Configuration** form. You can change the percentage thresholds for the target thresholds on the **Node Group Status Settings** tab of this form.

Because status calculations for large node groups can be resource-intensive, node group status calculation is off by default for new installations of NNMi. (Upgrades from NNMi 8.x retain the prior status calculation settings.) You can enable status calculation with the **Calculate Status** check box on the **Node Group** form for each node group.

Interface Groups

Interface groups filter interfaces within nodes by IFType or by other attributes, such as ifAlias, ifDescr, ifName, ifIndex, IP address, and so forth. Interface groups carry no hierarchy or containment, although you can further qualify membership based on the node group for the node hosting the interface.

Interface groups can be filtered on custom capabilities and attributes similarly to node groups.

Qualifications for interface groups are AND'd together within and across tabs.

Node/Interface/Address Hierarchy

NNMi assigns monitoring settings in the following manner:

1. **Interface Settings**—NNMi monitors each of the node's interfaces and IP addresses based on the first matching **Interface Settings** definition. The first match is the **Interface Settings** definition with the lowest ordering number.
2. **Node Settings**—NNMi monitors each node and each previously unmatched interface or IP address based on the first matching **Node Settings** definition. The first match is the **Node Settings** definition with the lowest ordering number.

   ➤ Child node groups are included in the ordering hierarchy. If the parent node group has a lower ordering number (for example, parent=10, child=20), then the monitoring configuration specified for the parent node group also applies to the nodes in the child node group. To override a parent node group monitoring configuration, set the ordering number for the child node group to a number that is lower than the parent (for example, parent=20, child=10).

3. **Default Settings**—If no match is found for a node, interface, or IP address in step 1 or step 2, NNMi applies the default monitoring configuration settings.

Stop Everything and Start Over Again

If you want to completely restart discovery and redo all of the NNMi configuration, or if the NNMi database has become corrupted, you can reset the NNMi configuration and database. This process deletes *all* of the NNMi configuration, topology, and incidents.

For information about the commands identified in this procedure, see the appropriate reference pages, or the UNIX manpages.

Follow these steps:

1 Stop the NNMi services:

```
ovstop -c
```

2 Optional. Because this procedure deletes the database, you might want to back up the existing database before proceeding:

```
nnmbackup.ovpl -type offline -target <backup_directory>
```

3 Optional. If you want to keep any of the current NNMi configuration, use the `nnmconfigexport.ovpl` command to output the NNMi configuration to an XML file.

The nnmconfigexport.ovpl command does not retain SNMPv3 credentials. For more information, see the *nnmconfigexport.ovpl* reference page, or the UNIX manpage.

4 Optional. Use the `nnmtrimincidents.ovpl` command to archive the NNMi incidents.

5 Drop and recreate the NNMi database.

- For the embedded database, run the following command:

  ```
  nnmresetembdb.ovpl -nostart
  ```

- For an Oracle database, ask the Oracle database administrator to drop and recreate the NNMi database. Maintain the database instance name.

6 If you have installed iSPIs or stand-alone products that integrate with NNMi, reset those products to remove the old topology identifiers. For specific procedures, see the product documentation.

7 Start the NNMi services:

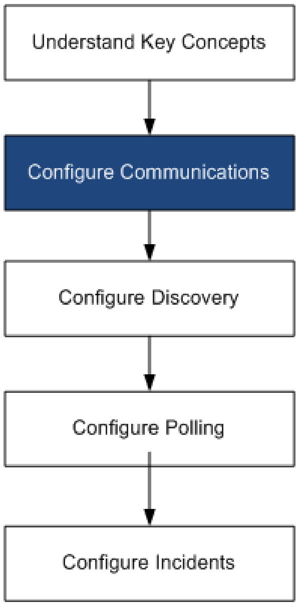
```
ovstart -c
```

NNMi now has only the default configurations as if you had just installed the product on a new system.

8 Start configuring NNMi. Do one of the following:

- Use the Quick Start Configuration Wizard.
- Enter information into the **Configuration** workspace in the NNMi console.
- Use the `nnmconfigimport.ovpl` command to import some or all of the NNMi configuration that you saved in step 3.

NNMi Communications



HP Network Node Manager i Software (NNMi) uses both Simple Network Management Protocol (SNMP) and Internet Control Message Protocol (ICMP ping) to discover devices and to monitor device status and health. To establish viable communication in your environment, you configure NNMi with the access credentials and appropriate timeout and retry values for different devices and areas of your network. You can disable a protocol in some areas of your network to reduce traffic or to respect firewalls.

The communication values that you configure form the foundation of NNMi discovery and state polling. NNMi applies the appropriate values for each device when making queries for discovery or polling. Thus, if you configure NNMi to disallow SNMP communication within some region of your network, neither NNMi discovery nor NNMi state polling can send SNMP requests to that region.

This chapter contains the following topics:

- Concepts for Communications
- Plan Communications
- Configure Communications
- Evaluate Communications
- Tune Communications

Concepts for Communications

NNMi uses SNMP and ICMP primarily in a request-response manner. Responses to ICMP ping requests verify address responsiveness. Responses to SNMP requests for specific MIB objects provide more comprehensive information about a node.

The following concepts apply to NNMi communications configuration:

- Levels of Communication Configuration
- Network Latency and Timeouts
- SNMP Access Control
- SNMP Version Preferences
- Management Address Preferences
- Polling Protocols
- Communication Configuration and the nnmsnmp*.ovpl Commands

Levels of Communication Configuration

NNMi communication configuration provides the following levels:

- Specific nodes
- Regions
- Global defaults

At each level you can configure access credentials, timeout and retry values, ICMP and SNMP protocol enablement, and SNMP access settings. If you leave settings blank at one level, NNMi applies the next level of defaults.

When communicating with a given node, NNMi applies the configuration settings as follows:

1. If the node matches a **specific node** configuration, NNMi uses any communication values in that configuration.
2. If any settings are not yet defined, NNMi determines whether the node belongs to any **regions**. Because regions might overlap, NNMi uses the matching region with the lowest ordering number. NNMi uses the values specified for that region to fill in the blanks left from the applicable specific node setting (if any). The settings for additional regions are not considered.
3. If any settings are still not yet defined, NNMi uses the **global default** settings to fill in the remaining blanks.

The values used for ICMP and SNMP communication with a particular device might be built up cumulatively until all required settings are determined.

Network Latency and Timeouts

Normal network latency influences the amount of time the NNMi management server must wait to get answers to ICMP and SNMP queries. Different areas of a network customarily have different turnaround times. For example, the local network where the NNMi management server resides could provide nearly instantaneous response, while responses from a device in a remote geographical region accessed through a dial-up wide area link would typically take much longer. In addition, heavily-loaded devices might be too busy to respond to ICMP or SNMP queries immediately. When deciding which timeout and retry settings to configure, consider these latency concerns.

You can configure specific timeout and retry settings for both network regions and specific devices. The settings you choose determine how long NNMi waits for an answer and how many times NNMi requests data before abandoning the request when no answer is received.

For each request retry, NNMi adds the configured timeout value to the previous timeout value. Thus, the pause gets longer between each retry. For example, when NNMi is configured to use timeout of 5 seconds and three retries, NNMi waits 5 seconds for a response to the first request, 10 seconds for a response to the second request, and 15 seconds for a response to the third request before giving up until the next polling cycle.

SNMP Access Control

Communication with SNMP agents on managed devices requires access control credentials:

- SNMPv1 and SNMPv2c

  A community string in each NNMi request must match a community string configured in the responding SNMP agent. All communication passes through the network in clear text (no encryption).

- SNMPv3

  Communication with the SNMP agent complies with the user-based security model (USM). Each SNMP agent has a list of configured user names and their associated authentication requirements (the authentication profile). Formatting of all communication is controlled through configuration settings. NNMi SNMP requests must specify a valid user and follow the authentication and privacy controls configured for that user.

  - Authentication protocol uses hash-based message authentication code (HMAC) using your choice of either the message-digest algorithm 5 (MD5) or the secure hash algorithm (SHA).

  - Privacy protocol uses no encryption or the data encryption standard - cipher block chaining (DES-CBC) symmetric encryption protocol.

NNMi supports the specification of multiple SNMP access control credentials for a region of your network (defined through IP address filters or hostname filters). NNMi attempts communication with a device in that region by trying all configured values at a given SNMP security level in parallel. You can specify the minimum SNMP security level that NNMi uses in that region. NNMi uses the first value returned by each node (response from the device’s SNMP agent) for discovery and monitoring purposes.

SNMP Version Preferences

The SNMP protocol itself has evolved over the years from version 1 to version 2(c) and now version 3, with increasing security capabilities (among others). NNMi can handle any or a mix of all versions in your network environment.

The first SNMP response NNMi receives for a particular node determines the communication credentials and SNMP version used by NNMi for communication with that node.

➤ The SNMP version selection for a node plays a role in NNMi accepting traps from that node:

- If the source node or source object of the incoming trap has been discovered by NNMi using SNMPv3, NNMi accepts incoming SNMPv1, SNMPv2c, and SNMPv3 traps.
- If the source node or source object of the incoming trap has been discovered by NNMi using SNMPv1 or SNMPv2c, NNMi discards incoming SNMPv3 traps.

You specify the minimum level of SNMP version and security settings that are acceptable in each area of your network. The options for the SNMP Minimum Security Level field are as follows:

- **Community Only (SNMPv1 only)**—NNMi attempts to communicate using SNMPv1 with the configured values for community strings, timeouts, and retries. NNMi does not try any SNMPv2c or any SNMPv3 settings.
- **Community Only (SNMPv1 or v2c)**—NNMi attempts to communicate using SNMPv2c with the configured values for community strings, timeouts, and retries. If there is no response to any community string using SNMPv2c, NNMi attempts to communicate using SNMPv1 with the configured values for community strings, timeouts, and retries. NNMi does not try any SNMPv3 settings.
- **Community**—NNMi attempts to communicate using SNMPv2c with the configured values for community strings, timeouts, and retries. If there is no response to any community string using SNMPv2c, NNMi attempts to communicate using SNMPv1 with the configured values for community strings, timeouts, and retries. If none work, NNMi tries SNMPv3.
- **No Authentication, No Privacy**—For users with no authentication and no privacy, NNMi attempts to communicate using SNMPv3 with the configured values for timeouts and retries. If none work, NNMi tries users with authentication and no privacy followed by users with authentication and privacy, if necessary.
- **Authentication, No Privacy**—For users with authentication and no privacy, NNMi attempts to communicate using SNMPv3 with the configured values for timeouts and retries. If none work, NNMi tries users with authentication and privacy.
- **Authentication, Privacy**—For users with authentication and privacy, NNMi attempts to communicate using SNMPv3 with the configured values for timeouts and retries.

Management Address Preferences

A node's **management address** is the address NNMi uses to communicate with the node's SNMP agent. You can specify the management address for a node (in the specific node settings), or you can let NNMi choose an address from the IP addresses associated with the node. You can fine-tune this behavior in the discovery configuration settings by excluding certain addresses from discovery. For information about how NNMi determines the management address, see *Node Form* in the NNMi help.

NNMi discovers and monitors devices on an ongoing basis. *After the first NNMi discovery cycle*, the **Enable SNMP Address Rediscovery** field controls NNMi behavior when previously discovered SNMP agents quit responding (for example, when you reconfigure the device's SNMP agent).

- If the **Enable SNMP Address Rediscovery** check box is selected, NNMi retries any configured values in search of one that works.
- If the **Enable SNMP Address Rediscovery** check box is cleared, NNMi reports the device as "Down" and does not attempt to find another communication configuration setting for that device.

The **Enable SNMP Address Rediscovery** check box is available at all levels of communication configuration.

The **Discover Any SNMP Device** and **Non-SNMP Devices** auto-discovery rule configuration fields influence the way NNMi uses SNMP. For more information, see *Configure Basic Settings for the Auto-Discovery Rule* in the NNMi help.

Polling Protocols

You can prevent NNMi from using SNMP or ICMP in portions of your network (for example, when firewalls in your infrastructure prohibit ICMP or SNMP traffic).

Disabling ICMP traffic to the devices in an area of the network has the following results in NNMi:

- The optional auto-discovery rule ping sweep feature cannot locate additional nodes in that region of your network. All nodes must either be seeded or available through answers to MIB object requests, such as neighbor's ARP cache, Cisco Discovery Protocol (CDP), or Extreme Discovery Protocol (EDP). Wide area network devices might be missed unless you seed every one of them.
- The State Poller cannot monitor devices that are not configured to respond to SNMP requests. (However, if the device responds to SNMP, State Poller does not use ICMP.)
- Operators cannot use **Actions > Ping** to check device reachability during troubleshooting.

Disabling SNMP traffic to the devices in an area of the network has the following results in NNMi:

- Discovery cannot gather any information about the devices except that they exist. All devices receive the `No SNMP` device profile.
- Discovery cannot find additional neighboring devices through queries. All devices must be directly seeded.

- Discovery cannot gather connectivity information from the devices, so they appear unconnected on NNMi maps.
- For devices with the `No SNMP` device profile, the State Poller respects the defaults of monitoring that device using only ICMP (ping).
- The State Poller cannot gather component health or performance data from the devices.
- The Causal Engine cannot contact the devices to perform neighbor analysis and locate the root cause of incidents.

Communication Configuration and the nnmsnmp*.ovpl Commands

The `nnmsnmp*.ovpl` commands look up the values for unspecified device communication settings in the NNMi database. This approach requires that the ovjboss process be running. If ovjboss is not running, the `nnmsnmp*.ovpl` commands behave as follows:

- For SNMPv1 and SNMPv2c agents, the commands use default values for any unspecified communication settings.
- For SNMPv3 agents, if you specify a user and password the commands use default values for any unspecified communication settings. If you do not specify a user and password, the commands fail.

Plan Communications

Make decisions in the following areas:

- Default Communication Settings
- Communication Configuration Regions
- Specific Node Configurations
- Retry and Timeout Values
- Active Protocols
- Multiple Community Strings or Authentication Profiles

Default Communication Settings

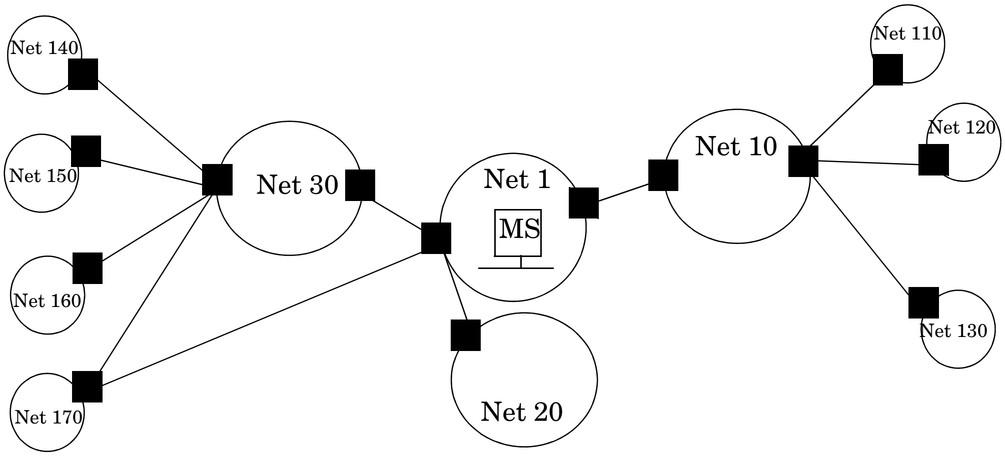
Because NNMi uses default values to complete any configuration settings that were not specified for the applicable region or specific node, set defaults to be reasonable for the majority of your network.

- Are there commonly-used community strings that NNMi should try?
- What default timeout and retry values are reasonable in your network?

Communication Configuration Regions

Regions represent areas of the network where similar communication settings make sense. For example, the local network around the NNMi management server usually returns responses very quickly. Areas of your network that are multiple hops away typically take longer to respond.

You do not need to configure each subnet or area of your network. You can combine areas into one region based on similar lag times. Consider the following network map:



For timeout and retry purposes, you might want to configure the following regions:

- Region A for Net 1
- Region B to include Net 10, Net 20, and Net 30
- Region C for the more distant outlying networks

You would decide how best to group Net 170, depending on whether traffic management configuration is set to prefer the one-hop or two-hop path from the NNMi management server.

Regions are also used to group devices with similar access credentials. If all routers in your network use the same community string (or a small set of possible community strings) and you can identify the routers with a naming convention (for example, `rtr`*`nnn`*`.yourdomain.com`), you can configure a region containing all routers so that they are handled similarly. If you cannot use a wildcard to group the devices, you can configure each as a specific node.

Plan your region configurations so that you can apply the same timeout and retry value and access credential configurations to all nodes in a region.

Region definitions can overlap, and a device might qualify for multiple regions. NNMi applies the settings from the region with the lowest ordering number (and no other matching regions).

Specific Node Configurations

For any device with unique communication configuration requirements, use the specific node settings to specify the communication settings for that node. Example uses of specific node settings include the following:

- A node that might not respond well to SNMPv2c/SNMPv3 GetBulk requests
- A node whose name does not match the name pattern of other similar nodes

Retry and Timeout Values

Configuring longer timeouts and more retries can result in more responses from devices that are busy or distant. This higher response rate eliminates false down messages. However, it also lengthens the time to determine that actual down devices require attention. Finding the balance for each area of your network is important and might require a period of testing and adjusting values in your environment.

To get an idea of current lag time for each hop, do the following:

- *Windows*: Run a `tracert` to a device in each network area.
- *UNIX*: Run a `traceroute` to a device in each network area.

Active Protocols

You have two opportunities to control the type of traffic NNMi generates when communicating with devices in your network: communication and monitoring configuration settings. Use the communication settings when firewalls in your infrastructure prohibit ICMP or SNMP traffic. Use monitoring settings to fine tune protocol usage when you do not need a particular subset of data about devices. If either communication or monitoring settings disable a protocol for a device, NNMi does not generate that type of traffic to the device.

➤ Disabling SNMP communication significantly compromises the NNMi status and health monitoring of your network.

Note whether each region or specific device should receive ICMP traffic.

You do not need to explicitly disable SNMP communication with devices for which you do not supply access credentials. By default, NNMi assigns those devices to the `No SNMP` device profile and monitors them using ICMP only.

Multiple Community Strings or Authentication Profiles

Plan the community strings and authentication profiles to be tried for each area of your network. For the default and region settings, you can configure multiple community strings and authentication profiles to be tried in parallel.

➤ While trying probable community strings, NNMi queries might cause devices to generate authentication failures. Inform your operations department that authentication failures might safely be ignored while NNMi completes its initial discovery. Alternatively, you can minimize the number of authentication failures by configuring your regions (and the associated community strings and authentication protocols to try) as tightly as possible.

If your environment uses SNMPv1 or v2c *and* SNMPv3, determine the minimum acceptable security level for each region.

SNMPv1 and SNMPv2 Community Strings

For regions where SNMPv1 or v2c access is acceptable, gather the community strings in use within the region and any unique community strings required by specific devices.

SNMPv3 Authentication Profiles

For regions containing SNMPv3-accessible devices, determine the minimum acceptable default authentication profiles, the authentication profiles appropriate for each region, and the unique authentication credentials in use on specific devices (if any). Also determine the authentication and privacy protocols in use within your network.

For SNMPv3 communication, NNMi supports the following authentication protocols:

- HMAC-MD5-96
- HMAC-SHA-1

For SNMPv3 communication, NNMi supports the following privacy protocols:

- DES-CBC
- TripleDES
- AES-128
- AES-192
- AES-256

You can specify one (or no) authentication protocol and one (or no) privacy protocol for each specific node or region setting.

Use of the TripleDES, AES-192, or AES-256 privacy protocols requires the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files library For more information, see Preparing NNMi to Use SNMPv3 Privacy Protocols on page 56.

Configure Communications

After reading the information in this section, see *Configuring Communication Protocol* in the NNMi help for specific procedures.

It is a good idea to save a copy of the existing configuration before you make any major configuration changes. For more information, see Best Practice: Save the Existing Configuration on page 40.

Configure the following areas of communication:

- Default settings
- Region definitions and their settings
- Specific node settings

For specific nodes, you can enter node settings through the NNMi console or through a configuration file.

➤ **Save and Close** all **Communication Configuration** forms all of the way back to the NNMi console to implement your changes.

Best practice Double-check the ordering numbers for the defined regions. If a node qualifies for membership in multiple regions, NNMi applies the settings from the region with the lowest ordering number to that node.

Preparing NNMi to Use SNMPv3 Privacy Protocols

You can specify a privacy protocol to use for communication with SNMPv3 devices on the **SNMPv3 Settings** form in the NNMi console. The AES-192, AES-256, and TripleDES protocols are available for selection only when the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files library is installed on the NNMi management server.

To enable NNMi to use the AES-192, AES-256, and TripleDES privacy protocols for SNMPv3 communication, follow these steps:

1. Download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files library from the Oracle Technology Network web site for Java developers (**http://www.oracle.com/technetwork/java/index.html**). A direct link is:
   https://cds.sun.com/is-bin/INTERSHOP.enfinity/WFS/CDS-CDS_Developer-Site/en_US/-/USD/ViewProductDetail-Start?ProductRef=jce_policy-6-oth-JPR@CDS-CDS_Developer
2. Uncompress the download package, and then copy both JAR files (`local_policy.jar` and `US_export_policy.jar`) to the following location:
   - *Windows*: `%NnmInstallDir%\nonOV\jdk\nnm\jre\lib\security`
   - *UNIX*: `$NnmInstallDir/nonOV/jdk/nnm/jre/lib/security`
3. Restart NNMi by running the following commands:
   a. **`ovstop`**
   b. **`ovstart`**

Evaluate Communications

This section lists ways to evaluate the progress and success of the communications settings. Most of these tasks can be completed only after discovery has completed.

Consider the following:

- Are All Nodes Configured for SNMP?
- Is SNMP Access Currently Available for a Device?
- Is the Management IP Address Correct?
- Is NNMi Using the Correct Communications Settings?
- Do the State Poller Settings Agree with the Communication Settings?

Are All Nodes Configured for SNMP?

1. Open the **Nodes** inventory view.
2. Filter the **Device Profile** column to contain the string `No SNMP`.
   - For each of the devices that you want to manage, configure communication settings for the specific node. Alternatively, you can expand a region to include the node and update the access credentials.
   - If the communication settings are correct, verify that the SNMP agent on the device is running and properly configured (including ACLs).

Is SNMP Access Currently Available for a Device?

1. Select the node in an inventory view.
2. Select **Actions > Status Poll** or **Actions > Configuration Poll**.

   If the results show any SNMP values, communication is operational.

You can also test communication from the command line with the `nnmsnmpwalk.ovpl` command. For more information, see the *nnmsnmpwalk.ovpl* reference page, or the UNIX manpage.

Is the Management IP Address Correct?

To determine which management address NNMi has selected for a device, follow these steps:

1. Select the node in an inventory view.
2. Select **Actions > Communication Settings**.
3. In the **Communication Configuration** window, verify that the management address of the SNMP agent listed in the Active SNMP Agent Settings list is correct.

Is NNMi Using the Correct Communications Settings?

Missing or incorrect SNMP community strings can result in incomplete discovery or can negatively affect the discovery performance.

To verify the communication settings configured for a device, use the `nnmcommconf.ovpl` command or follow these steps:

1. Select the node in an inventory view.
2. Select **Actions > Communication Settings**.
3. In the **Communication Configuration** window, verify that the values listed in the SNMP configuration settings table are the settings you want NNMi to use for this node.

   If the communication settings are not correct, use the source information in the SNMP configuration settings table as a starting point for fixing the problem. You might need to change the configuration or the ordering number of a region or specific node.

Do the State Poller Settings Agree with the Communication Settings?

Even if the communication settings permit protocol traffic to an area of your network, that type of traffic might be disabled in the monitoring settings. To determine whether the settings are being overridden:

1. Select the node in an inventory view.
2. Select **Actions > Monitoring Settings**.

If either the Monitoring Settings or the Communication Settings disable a type of traffic to the device, that traffic will not be sent from NNMi.

Tune Communications

Reduce authentication failures

If NNMi is generating too many authentication traps during discovery, configure smaller regions or specific nodes with smaller groups of access credentials for NNMi to try.

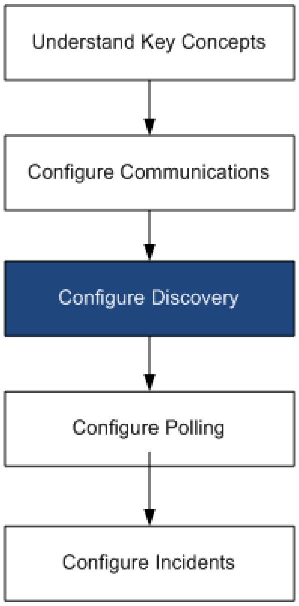
Tune timeouts and retries

When NNMi attempts to contact a device using SNMP during discovery, the communication configuration determines whether NNMi can gather the necessary device information. When the communication configuration does not include the correct SNMP community strings, or if NNMi is discovering non-SNMP devices, NNMi uses the configured settings for SNMP timeouts and retries. In this case, large timeout values or a high number of retries can negatively affect the overall performance of discovery. If your network contains devices that you know respond slowly to SNMP/ICMP requests, consider using the **Regions** or **Specific Node Settings** tabs on the **Communication Configuration** form to fine tune the timeout and retry values for just these devices.

Reduce default community strings

Having a large number of default community strings can negatively affect discovery performance. Instead of entering many default community strings, fine tune the community string configuration for particular areas of your network by using the **Regions** or **Specific Node Settings** tabs on the **Communication Configuration** form.

NNMi Discovery



One of the most important network management tasks is keeping your view of the network topology current. HP Network Node Manager i Software (NNMi) discovery populates the topology inventory with information about the nodes in your network. NNMi maintains this topology information through ongoing spiral discovery, which ensures that root cause analysis and the troubleshooting tools provide accurate information regarding incidents.

This chapter provides information to help you configure NNMi discovery. For an introduction to how discovery works and for detailed information about how to configure discovery, see *Discovering Your Network* in the NNMi help.

This chapter contains the following topics:

- Concepts for Discovery
- Plan Discovery
- Configure Discovery
- Evaluate Discovery
- Tune Discovery

Concepts for Discovery

The NNMi default behavior of discovering only routers and switches enables you to focus your network management on the critical or most important devices. In other words, target the backbone of the network first. Generally, you should avoid managing end nodes (for example, personal computers or printers) unless the end node is identified as a critical resource. For example, database and application servers might be considered critical resources.

NNMi provides several ways to control what devices to discover and include in the NNMi topology. Your discovery configuration can be very simple, quite complex, or anywhere in between, depending on how your network is organized and what you want to manage with NNMi.

NNMi does not perform any default discovery. You must configure discovery before any devices appear in the NNMi topology.

Each discovered node (physical or virtually hosted) counts toward the license limit, regardless of whether NNMi is actively managing that node. The capacity of your NNMi license might influence your approach to discovery.

Status monitoring considerations might also influence your choices. By default, the State Poller only monitors interfaces connected to devices NNMi has discovered. You can override this default for some areas of your network, and you can discover the devices beyond the edge of your responsibility. (For information about the State Poller, see NNMi State Polling on page 77.)

NNMi provides two primary discovery configuration models:

- **List-based discovery**—Explicitly tell NNMi exactly which devices should be added to the database and monitored through a list of seeds.
- **Rule-based discovery**—Tell NNMi which areas of your network and device types should be added to the database, give NNMi a starting address in each area, and then let NNMi discover the defined devices.

You can use any combination of list-based and rule-based discovery to configure what NNMi should discover. Initial discovery adds these devices to the NNMi topology, and then spiral discovery routinely rediscovers the network to ensure that the topology remains current.

If you plan to configure multi-tenancy, configure tenants before initiating network discovery.

NNMi Derives Attributes through Device Profiles

As NNMi discovers devices, it uses SNMP to gather some attributes directly. One of the key attributes is the MIB II system object ID (`sysObjectID`). From the system object ID, NNMi derives additional attributes, such as vendor, device category, and device family.

During discovery, NNMi collects the MIB II system capabilities and stores them in the topology portion of the database. System capabilities are visible on the **Node** form. However, these capabilities are not used by any other portion of NNMi (specifically, monitoring configuration). NNMi uses the device category (from the device profile for the system object ID) to match devices into node groups. In node view tables, the **Device Category** column identifies the device category for each node.

NNMi ships with thousands of device profiles for system object IDs that were available at the time of release. You can configure custom device profiles for the unique devices in your environment to map these devices to category, vendor, and so forth.

Plan Discovery

Make decisions in the following areas:

- Select Your Primary Discovery Approach
- Auto-Discovery Rules
- Node Name Resolution
- Subnet Connection Rules
- Discovery Seeds
- Rediscovery Interval
- Do Not Discover Objects

Select Your Primary Discovery Approach

Decide whether to do entirely list-based discovery, entirely rule-based discovery, or a combination of both approaches.

List-Based Discovery

With list-based discovery, you explicitly specify (as a discovery seed) each node that NNMi should discover.

If you plan to configure multi-tenancy, list-based discovery is the recommended discovery approach.

Benefits of using only list-based discovery include:

- Provides very tight control over what NNMi manages.
- Supports the specification of a non-default tenant at discovery time.
- Simplest configuration.
- Good for fairly static networks.
- A good way to start using NNMi. You can add auto-discovery rules over time.

Disadvantages of using only list-based discovery include:

- NNMi does not discover new nodes as they are added to the network.
- You must provide the complete list of nodes to be discovered.

Rule-Based Discovery

With rule-based discovery, you create one or more auto-discovery rules to define the areas of the network that NNMi should discover and include in the NNMi topology. For each rule, you must provide one or more discovery seeds (by explicitly naming seeds or by enabling ping sweep), and then NNMi discovers the network automatically.

Benefits of using rule-based discovery include:

- Good for large networks. NNMi can discover a large number of devices based on minimal configuration input.

- Good for networks that change frequently. New devices that are added to the network are discovered without administrator intervention (assuming that each device is covered by an auto-discovery rule).
- Ensures that any new device added to your network is discovered to comply with service level agreements for managing new devices in a timely manner or security guidelines to flag unauthorized new devices.

Disadvantages of using rule-based discovery include:

- It is easier to run into license limitations.
- Depending on the structure of your network, tuning auto-discovery rules can be complex.
- If auto-discovery rules are very broad and NNMi discovers many more devices than you want to manage, you might want to delete the unneeded devices from NNMi topology. Node deletion can be time consuming.
- All non-seeded nodes receive the default tenant at discovery. If you want to use NNMi multi-tenancy, you must update the tenant assignment after discovery.

Rule-based discovery only

Auto-Discovery Rules

Auto-Discovery Rule Ordering

The value of an auto-discovery rule's **Ordering** attribute affects discovery ranges in the following ways:

- IP address ranges

  If a device falls within two auto-discovery rules, the settings in the auto-discovery rule with the lowest ordering number applies. For example, if an auto-discovery rule excludes a set of IP addresses, then no other auto-discovery rules with higher ordering numbers process those nodes and the nodes within that range of addresses are not discovered unless they are listed as discovery seeds.

- System object ID ranges
  - If no IP address range is included in an auto-discovery rule, then the system object ID settings apply to all auto-discovery rules with higher ordering numbers.
  - If an IP address range is included in an auto-discovery rule, the system object ID range applies only within the auto-discovery rule.

Exclude Devices from Discovery

- To prevent discovery of certain object types, create an auto-discovery rule with a low ordering number that ignores the system object IDs that you do not want discovered. Do not include an IP address range in this rule. By giving this auto-discovery rule a low ordering number, the discovery process quickly passes by the objects that match this rule.
- The **Ignored by Rule** setting for an IP address range or a system object ID range affects that auto-discovery rule only. The devices included in an ignored range are available to be included in another auto-discovery rule.

- The addresses listed on the **Excluded IP Addresses** tab of the **Discovery Configuration** form apply to all auto-discovery rules. Unless they are configured as discovery seeds, these addresses are never added to the NNMi topology. (Discovery seeds are always discovered.)

➤ Some networks use routing protocols such as Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP) to provide router redundancy. When routers are configured in an router redundancy group (RRG), as they are when using HSRP, the routers configured in the RRG share a protected IP address (one active and one standby). NNMi does not support the discovery and management of multiple RRGs configured with the same protected IP address. Each RRG must have a unique protected IP address.

Ping Sweep

You can use ping sweep to locate devices within the IP address ranges of the configured auto-discovery rules. For initial discovery, you might want to enable ping sweep for all rules. Doing so provides enough information to NNMi discovery that you do not need to configure discovery seeds.

➤ Ping sweep works for subnets of 16 bits or smaller, for example, `10.10.*.*`.

Ping sweeps are especially useful for discovering devices across a WAN that you do not control, such as an ISP network.

➤ Firewalls often view ping sweeps as attacks on the network, in which case, a firewall might block all traffic from a device that emits ping sweeps.

Best practice

Enable ping sweep for small discovery ranges only.

Discovery Hints from SNMP Traps

As of NNMi 9.01, NNMi processes the source IP address of received SNMP traps as hints to auto-discovery rules. This function is especially useful for discovering devices across a WAN.

Discovery Seeds for Auto-Discovery Rules

Provide at least one discovery seed per auto-discovery rule. The options for providing the seeds are as follows:

- Enter seeds on the **Discovery Seed** form by clicking **Seeds** under **Discovery** in the **Configuration** workspace.
- Use the `nnmloadseeds.ovpl` command to load information from a seed file.
- Enable ping sweep for the rule, at least for initial discovery.
- Configure a device to send SNMP traps to the NNMi management server.

Best Practices for Auto-Discovery Rules

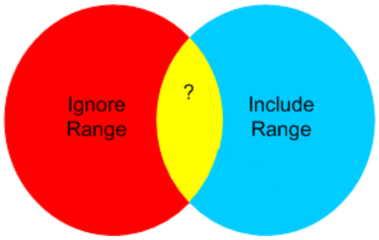
- Because NNMi automatically manages all discovered devices, use IP address ranges that closely match the areas of the network that you want to manage.
  - You can use multiple IP address ranges within an auto-discovery rule to restrict discovery.
  - You can add a large IP address range to an auto-discovery rule and then exclude some IP addresses from discovery within that rule.
- The system object ID range specification is a prefix, not an absolute value. For example, the range 1.3.6.1.4.1.11 is the same as 1.3.6.1.4.1.11.*.

Examples

Discovery Rule Overlap

Figure 1 shows two discovery ranges that overlap. The circle on the left represents an IP address range or a system object ID range to be ignored by NNMi discovery. The circle on the right represents an IP address range or a system object ID range to be discovered and included in the NNMi topology. The overlapping region might be included or ignored by discovery, depending on the ordering of these auto-discovery rules.

Figure 1 Overlapping Discovery Ranges



Limit Device Type Discovery

To discover all HP devices in your network that are not printers, create one auto-discovery rule with a range to include the HP enterprise system object ID (1.3.6.1.4.1.11). In this auto-discovery rule, create a second range to ignore the system object IDs of HP printers (1.3.6.1.4.1.11.2.3 9). Leave the IP address range unset.

Node Name Resolution

By default, NNMi attempts to identify a node in the following order:

1. Short DNS name
2. Short sysName
3. IP Address

➤ If you change a node's hostname, there is a delay before NNMi data reflects the name change, because NNMi caches DNS names to enhance performance.

The following scenarios describe situations in which you might want to change the default order for node name resolution:

- If your organization is dependent on others to update the DNS configuration, you might set a policy of defining the sysName for each new device as it is added to the network. In this case, set select sysName as the first choice for node name resolution so that NNMi can discover the new device as soon as it is deployed in the network. (Maintain the sysName over the life of the device.)
- If your organization does not set or maintain the sysName for managed devices, select sysName as the third option for node name resolution.

Best practice

If you use the full or short DNS name as the primary naming convention, confirm that you have forward and reverse DNS resolution from the NNMi management server to all managed devices.

➤ When the full DNS name is the naming convention, labels on the topology maps can be long.

Best practice

NNMi selects the lowest loopback address as the management address for Cisco devices, so put DNS resolution on the lowest loopback address for each Cisco device. (NNMi 8.0x selects the highest loopback address as the management address.)

Subnet Connection Rules

List-based discovery only

For list-based discovery, NNMi uses the subnet connection rules to detect connections that span a WAN. NNMi evaluates the subnet membership of the device it has discovered on each end of a probable connection (by examining their IP addresses and subnet prefixes) and looks at subnet connection rules for a match.

Rule-based discovery only

When auto-discovery rules are enabled and NNMi finds a device configured with a subnet prefix between /28 and /31:

1. NNMi checks for an applicable subnet connection rule.
2. If a match is found, NNMi uses each valid address in the subnet as a hint and attempts a discovery on that address.

Best practice

Use the default connection rules. Only modify them if you have a problem.

Discovery Seeds

List the devices to use as discovery seeds.

Best practice

One of the NNMi rules for selecting the preferred management IP address specifies using the first discovered IP address as the management address. You can influence NNMi by configuring the preferred IP address as the seed address.

Best practice

For Cisco devices, use a loopback address as the discovery seed because loopback addresses are more reliably reachable than other addresses on a device. Ensure that DNS is correctly configured to resolve the device hostname to the loopback address.

List-based discovery only

For list-based discovery, list all devices that you want NNMi to manage. You might be able to export this list from asset management software or from some other tool.

Because NNMi does not automatically add any devices to this list, ensure that the list includes every device for which you have responsibility or which influences your monitoring and status calculations.

Rule-based discovery only

Discovery seeds are optional for rule-based discovery:

- If ping sweep is enabled for an auto-discovery rule, you do not need to specify a seed for that rule.
- For each auto-discovery rule with ping sweep disabled, identify at least one seed per rule. If a rule includes multiple IP address regions, you might need a seed in each routable region because routers do not keep ARP entries across WAN links.

Best practice

For the most complete rule-based discovery, use routers, not switches, as discovery seeds because routers generally have much larger ARP caches than do switches. A core router connected to a network that you want to discover is an excellent choice for a discovery seed.

Rediscovery Interval

NNMi rechecks the configuration information from each device in the database according to the configured rediscovery interval. In addition, NNMi collects the ARP cache from each router covered by an auto-discovery rule and looks for new nodes on the network.

Any change in the communication-related configuration of a device, such as interface renumbering, automatically triggers NNMi to update its data for that device and its neighbors.

The following changes do not trigger an automatic rediscovery; devices are updated only at the configured rediscovery interval:

- Changes within a node (for example, firmware upgrade or system contact).
- New nodes added to the network.

Select the rediscovery interval to match the level of change in the network. For a highly-dynamic network, you might want to use the minimum interval of 24 hours. For more stable networks, you can safely extend that period.

Do Not Discover Objects

In NNMi, there are three ways that you can configure NNMi to disregard certain objects:

- On the **Communication Configuration** form, you can turn off ICMP communication, SNMP communication, or both at different levels: globally, for communication regions, or for specific hostnames or IP addresses. For information about the impacts of disabling one or both of these protocols, see Polling Protocols on page 51.
- On the **Discovery Configuration** form, you can set up an auto-discovery rule that instructs NNMi to never gather hints from certain IP addresses or SNMP system object IDs. Nodes matching the criteria still appear on the map and in the database, but spiral discovery does not extend to the neighboring devices beyond those IP addresses or object types.
- On the **Discovery Configuration** form, you can set up an auto-discovery rule that instructs NNMi to exclude specific IP address ranges, IP addresses, or both from the database. Spiral discovery does not display those addresses on any node’s list of addresses or use those addresses when establishing connections between devices, so NNMi never monitors the health of those addresses.

Monitoring Virtual IP Addresses with NNMi

NNMi discovers and monitors devices such as clustered servers that share a virtual IP address. After a cluster fails over to a new active node, NNMi associates the virtual IP address with the new active node. This association is not immediate, as some time might pass between failover and NNMi discovering the change.

There are several actions you can take to configure NNMi for your specific situation:

If you want NNMi to monitor a virtual IP address, *use only one of the following options*:

- Option 1: For this option, NNMi manages N+1 non-SNMP devices, where N represents the number of members in the cluster discovered with a non-virtual IP address. NNMi discovers the additional (+1) non-SNMP node, and it is configured with the virtual IP address.

  Do nothing to stop NNMi from discovering a virtual IP address. Using this approach, NNMi discovers the virtual IP address and the physical IP addresses associated with the Network Interface (NIC) cards on devices configured to use this virtual IP address. NNMi discovers and monitors each device as a separate non-SNMP node.

- Option 2: Configure NNMi to use a device's physical IP address as the `Preferred Management Address` of a clustered server. For instructions on how to do this, see the *Specific Node Settings Form (Communication Settings)* topic in the NNMi help.

➤ NNMi might not immediately recognize the transfer of a virtual IP address from one active node to a new active node. NNMi might show the status of a virtual IP address using a node other than the current active node in the cluster.

If you do not want NNMi to monitor a virtual IP address, do the following using the NNMi console:

1. Click **Discovery Configuration** in the **Configuration** workspace.
2. Click the **Excluded IP Addresses** tab.
3. Add the virtual IP address or range of addresses to the list of addresses to be excluded from discovery.
4. Save your work.

Configure Discovery

This section lists configuration tips and provides some configuration examples. After reading the information in this section, see *Configure Discovery* in the NNMi help for specific procedures.

➤ Because NNMi launches discovery from seeds as soon as you **Save and Close** the **Discovery Seed** form, ensure that you do the following before you configure seeds:

- Complete all communication configuration.
- Complete all auto-discovery rules (if any).
- Configure subnet connection rules.
- Configure name resolution preferences.
- **Save and Close** all of the way back to the console.

➤ It is a good idea to save a copy of the existing configuration before you make any major configuration changes. For more information, see Best Practice: Save the Existing Configuration on page 40.

Tips for Configuring Auto-Discovery Rules

- As you define a new auto-discovery rule, check each setting carefully. For a new rule, auto-discovery is enabled by default, IP address ranges are included by default, and system object ID ranges are *ignored* by default.

Tips for Configuring Seeds

- If you already have a file that lists the nodes to be discovered, format this information as a seed file and use the `nnmloadseeds.ovpl` command to import the node list into NNMi.
- In the seed file, specify IP addresses as a way of influencing the IP address that NNMi chooses as the management address. (If you use hostnames, DNS provides the IP address for each node.)
- Good formats for the entries in the seed file are shown here:

  ```
  IP_address1 # node name
  ```

  ```
  IP_address2, <tenant_UUID_or_tenant_name> # node name
  ```

  These formats are easy for both NNMi and human readers.
- For maintenance purposes, it is better to use only one seed file. Add nodes as needed and then rerun the `nnmloadseeds.ovpl` command. NNMi discovers the new nodes but does not re-evaluate the existing nodes.
- Removing a node from the seed file does not remove it from the NNMi topology. Delete the node directly in the NNMi console.
- Deleting a node from a map or inventory view does not delete the seed.
- If you want NNMi to rediscover a node, delete that node from a map or inventory view *and* from the **Seeds** form in the **Discovery** area of the **Configuration** workspace in the NNMi console, and the re-enter the node in the NNMi console, or run the `nnmloadseeds.ovpl` command.

Rule-based discovery only

- Completely configure a discovery rule *before* you specify a seed for that rule. That is, click **Save and Close** on the **Discovery Configuration** form. (The **Discovery Seed** form is a separate form that is not part of the **Discovery Configuration** form in the database model. As a result, when you save the information on the **Discovery Seed** form, NNMi updates the seed configuration immediately.)

Evaluate Discovery

This section lists ways to evaluate the progress and success of discovery.

Follow the Progress of Initial Discovery

NNMi discovery is dynamic and ongoing; it is never complete, so you will never see a "discovery completed" message. The process of initial discovery and connection takes some time. The following items suggest ways to gauge the progress of initial discovery:

- On the **Database** tab of the **System Information** window, watch for the node count to reach the expected level and stabilize. This window does not refresh automatically. During initial discovery, open the **System Information** window several times.
- Under **Discovery** in the **Configuration** workspace, look at the **Seeds** page. Refresh this page until all seeds show the `Node created` results, which indicates that the device has been added to the topology database. This result does *not* indicate that NNMi has gathered all information from the device and processed its connectivity.
- Open the **Node** form for representative nodes. When the **Discovery State** field (located on the **General** tab) transitions to `Discovery Completed`, NNMi has gathered the node's basic characteristics as well as the node's ARP cache and discovery protocol neighbors, if applicable. This state does *not* indicate that NNMi has completed connectivity analysis for the device.
- In the **Nodes** inventory view, scan to see that key devices are present from different areas of your network.
- Open the **Layer 2 Neighbor View** for representative nodes to determine whether connectivity analysis has completed for that area.
- Review the **Layer 2 Connections** and **VLANs** inventory views to gauge the progress of layer 2 processing.

Were All Seeds Discovered?

1. From the **Configuration** workspace, under **Discovery**, click **Seeds**.
2. On the **Seeds** page, sort the list of nodes by the **Discovery Seed Results** column. For any node in an error state, consider the following:
   - Failed discovery due to an unreachable node or unresolved DNS name—For these types of failures, verify network connectivity to the node and check for accurate DNS name resolution. To work around DNS issues, use the IP address to seed the node or include the hostname in a `hostnolookup.conf` file.

- License node count exceeded—This scenario occurs when the number of devices already discovered reached your license limit. You can either delete some discovered nodes or purchase additional node pack licenses.
- Node discovered but no SNMP response—SNMP communication problems can occur for seeded devices as well as devices that are discovered through auto-discovery. For more information, see Evaluate Communications on page 56.

Do All Nodes Have a Valid Device Profile?

1. Open the **Nodes** inventory view.
2. Filter the **Device Profile** column to contain the string `No Device Profile`.
3. If a node is discovered but has no device profile, add a new device profile (from **Configuration > Device Profiles**), and then perform a configuration poll on the node to update its data.

Were All Nodes Discovered Properly?

To avoid discovery problems, NNMi should only manage nodes using a unique IP address that does not appear on any other node in the management domain. For example, if a node suddenly disappears or gets merged with another node in the database, and it is part of a Router Redundancy Group (RRG), there are special requirements. To manage a router that participates in an RRG, you must use a unique IP address (which is not a protected address) as the management address of the router, and SNMP must be enabled on that address. NNMi will not properly manage a router if it tries to use a protected IP address as the management address.

Examine the data in the **Nodes** inventory view. If any nodes do not have a management address, check the communication settings for those nodes as described in Are All Nodes Configured for SNMP? on page 57.

If any expected nodes are missing from the **Nodes** inventory view, check the following:

- On each missing node, verify that the discovery protocol (for example, CDP) is correctly configured.
- If a missing node is on a WAN, enable ping sweep for the auto-discovery rule that includes that node.

List-based discovery only

Auto-Discovery Rules

If you see unexpected discovery results, re-evaluate the auto-discovery rules.

When NNMi discovery finds an address hint, it uses the first matching rule to determine if a node should be created. If no rules are matched, NNMi discovery discards the hint. The ordering number for auto-discovery rules determines the order in which the auto-discovery rule configuration settings are applied.

For each auto-discovery rule, check the following settings:

- **Discover Included Nodes** must be enabled for auto-discovery to occur for the rule.
- Verify that the following settings are correct for the type of nodes you want discovered for the rule:
  - **Discover Any SNMP Device**
  - **Discover Non-SNMP Devices**

  Remember that only routers and switches are discovered by default and non-SNMP nodes are *not* discovered. Enabling these settings without considering your environment can result in NNMi discovering more nodes than intended.

IP Address Ranges

The IP address of a discovery hint must match an **Include in Rule** entry in the IP address range list. If there are no included IP address ranges in an auto-discovery rule, then all address hints are considered a match. (For this case, see Tips for Configuring Auto-Discovery Rules on page 68.) Additionally, the hint must *not* match any entry marked **Ignored by Rule**. If all checks successfully match, this rule's configuration is used for handling the hint.

- If you are not discovering some expected devices, check your configured IP ranges to ensure that the IP addresses for those devices are included in a range and not ignored by a rule with a lower ordering number.
- If you are discovering more devices that you want, modify the include ranges or add ignored ranges for the IP addresses of the devices that you do not want discovered. Also, determine if **Discover Any SNMP Device** is enabled.

System Object ID Ranges

The system object ID (OID) from a discovery hint must match an **Include in Rule** entry in the system object ID ranges list. If there are no included system object ID ranges in an auto-discovery rule, then all object IDs are considered a match. Additionally, the OID must not match any entry marked **Ignored by Rule**. If all checks successfully match, this rule's configuration is used for handling the hint.

- Use the system object ID ranges to either expand auto-discovery to include more than the default routers and switches, or to exclude specific routers and switches.
- Each node must match both the IP address range and the system object ID range specified before it is discovered and added to the topology database.

Are All Connections and VLANs Correct?

NNMi creates Layer 2 connections and VLANs as a separate step after devices are added to the topology. Give NNMi plenty of time for initial discovery before evaluating connections and VLANs.

Evaluate Layer 2 Connectivity

To evaluate Layer 2 connectivity, create a node group for each network area of interest, and then display a topology map for that node group. (In the **Node Groups** inventory, select a node group, and then click **Actions > Node Group Map**.) Look for any nodes that are not connected to the other nodes in this map.

To evaluate VLANs, from the **VLANs** inventory view, open each **VLAN** form, and then examine the list of ports for that VLAN.

NNMi Discovery and Duplicate MAC Addresses

During discovery, NNMi reads the Forwarding Database (FDB) tables from Ethernet switches within a network to help NNMi determine communication paths between network devices. NNMi searches these FDB tables for information about discovered nodes. When an NNMi management server finds FDB references to duplicate Media Access Control (MAC) addresses, it does the following:

- If two or more discovered nodes contain an interface associated with the same MAC address, NNMi disregards the communication paths reported for those duplicate MAC addresses in the FDB. This might result in missing connections on NNMi maps in network areas that include those duplicate MAC addresses.

  NNMi Advanced - Global Network Management feature: If two NNMi management servers discover nodes that contain an interface associated with the same MAC address, the global NNMi management server's maps could be missing connections that are visible on the regional NNMi management server's maps.

- If a single node contains multiple interfaces that have the same MAC address, NNMi gathers all communication path information for those interfaces and displays that information on NNMi maps.

Rediscover a Device

1. Perform a configuration poll of the device.
2. Delete the device.

If the device is a seed, delete the seed, and then re-add the seed.

Tune Discovery

For general discovery performance, fine tune the discovery configuration to discover only critical and important devices.

- Filter by IP address range, system object ID, or both.
- Limit discovery of non-SNMP devices and any SNMP devices (devices that are not switches or routers).

To delete one or more nodes from the NNMi database on the command line, use the `nnmnodedelete.ovpl` command. This command deletes nodes, but not seed definitions, from the NNMi database.

To delete one or more seed definitions from the NNMi database on the command line, use the `nnmseeddelete.ovpl` command.

There are special discovery circumstances that might be remedied by suppressing discovery protocol collections or `VLAN-indexing`. See Suppressing the Use of Discovery Protocols for Specific Nodes on page 375 or Suppressing the Use of VLAN-indexing for Large Switches on page 378 for more information.

Discovery Log File

Look in the nnm.?.0.log file for messages containing the keyword Exception for the classes beginning with the string com.hp.ov.nms.disco. For information about log files, see NNMi Logging on page 383.

Unnumbered Interfaces

Prior to NNMi 9.10 patch 2, NNMi did not discover layer 2 connections for unnumbered interfaces unless you enabled xDP. NNMi 9.10 patch 2, provides an unnumbered interface discovery and monitoring solution that supports devices that use the default MIB-II ipRoutingTable and ipCidrRoutingTable.

The solution described in this section provides a way for NNMi 9.1x Patch 5 to discover and monitor IPv4 unnumbered interfaces and the associated layer 2 connections.

The solution explained in this section functions as follows in a global network management configuration:

- It works normally on a remote NNMi management server.
- It works on a global NNMi management server only for nodes managed on that server.
- It does not work on a global NNMi management server for nodes managed by a remote NNMi management server.

Enabling the Unnumbered Interface Feature

1. Create a node group that includes the devices containing the unnumbered interfaces. Either create a single node group that contains the device identifiers, or create a parent node group that represents multiple child node groups containing the device identifiers.
2. Create the following file:

   Windows: %NNM_DATA%\shared\nnm\conf\disco\UnnumberedNodeGroup.conf

   UNIX: $NNM_DATA/shared/nnm/conf/disco/UnnumberedNodeGroup.conf
3. Add a single node group name to this file. Again, this file must contain the name of a single node group containing the device identifiers, or it can be the name of a parent node group that represents multiple child node groups containing the device identifiers.

   ```
   # This is the name of an node group containing devices with
   unnumbered interfaces.
   Unnumbered Node Group
   ```

   In the example shown above, a node group named Unnumbered Node Group exists in NNMi. Add comment information as a separate line prefaced by a # character.
4. *Optional Step*: Create the following file:

   Windows: %NNM_DATA%\shared\nnm\conf\disco\UnnumberedSubnets.conf

   UNIX: $NNM_DATA/shared/nnm/conf/disco/UnnumberedSubnets.conf

5 *Optional Step*: Add information to this file to show the specific routing address range you need NNMi to discover. You can add multiple lines of IPv4 CIDR subnet entries in random order to this file.

➤ If you do not create and configure this file, NNMi will do a full MIB-II routing table walk against those nodes in the configured node group; by using the `UnnumberedSubnets.conf` file, NNMi requests MIB data from only those routes falling in the specified subnet destinations. It is a good practice to use this file and reduce the amount of discovery traffic and performance effect on the devices.

Below are some example entries to the `UnnumberedSubnets.conf` file.

```
10.1.5.0/18   #This entry filters the following routes: 10.1.0-63.

15.2.126.0/16 #This entry filters the following routes: 15.2.*.*

192.168.1.0/24 #This entry filters the following routes:
192.168.1.0-255
```

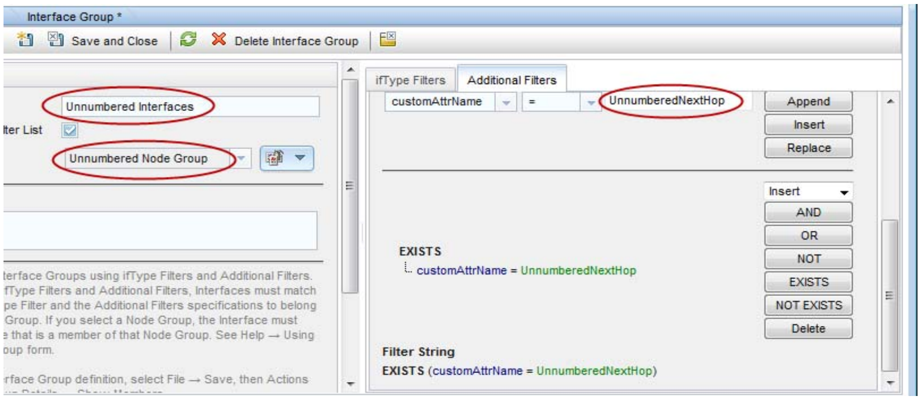
6 Restart the NNMi management server.

a Run the **`ovstop`** command on the NNMi management server.

b Run the **`ovstart`** command on the NNMi management server.

7 Wait for NNMi to complete the next discovery cycle.

8 To find all of the unnumbered interfaces, configure a new interface group to include those interfaces having custom attribute named `UnnumberedNextHop`.



Unnumbered Interfaces

lter List ☑

Unnumbered Node Group

customAttrName = UnnumberedNextHop

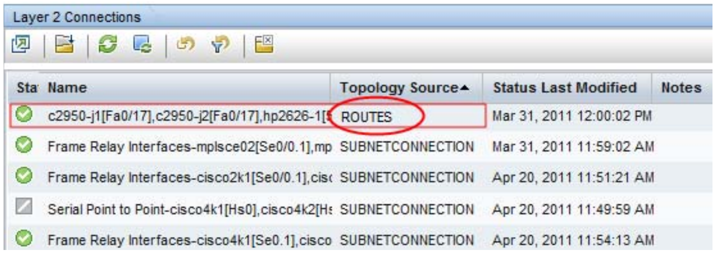
EXISTS
customAttrName = UnnumberedNextHop

Filter String
EXISTS (customAttrName = UnnumberedNextHop)

terface Groups using ifType Filters and Additional Filters.
fType Filters and Additional Filters, Interfaces must match
pe Filter and the Additional Filters specifications to belong
Group. If you select a Node Group, the Interface must
e that is a member of that Node Group. See Help → Using
oup form.

rface Group definition, select File → Save, then Actions

9 To view the layer 2 connections created by this solution, navigate to the **Layer 2 Connections** view; then look for the source from `ROUTES`.


Layer 2 Connections

Sta	Name	Topology Source ▲	Status Last Modified	Notes
✓	c2950-j1[Fa0/17],c2950-j2[Fa0/17],hp2626-1[	ROUTES	Mar 31, 2011 12:00:02 PM	
✓	Frame Relay Interfaces-mplsce02[Se0/0.1],mp	SUBNETCONNECTION	Mar 31, 2011 11:59:02 AM	
✓	Frame Relay Interfaces-cisco2k1[Se0/0.1],cis	SUBNETCONNECTION	Apr 20, 2011 11:51:21 AM	
▨	Serial Point to Point-cisco4k1[Hs0],cisco4k2[H	SUBNETCONNECTION	Apr 20, 2011 11:49:59 AM	
✓	Frame Relay Interfaces-cisco4k1[Se0.1],cisco	SUBNETCONNECTION	Apr 20, 2011 11:54:13 AM	

Disabling the Unnumbered Interface Feature

If you decide to disable the unnumbered interface feature, complete these steps:

1 Remove the following file:

Windows: `%NNM_DATA%\shared\nnm\conf\disco\UnnumberedNodeGroup.conf`

UNIX: `$NNM_DATA/shared/nnm/conf/disco/UnnumberedNodeGroup.conf`

2. Remove the following file if it exists:

   Windows: `%NNM_DATA%\shared\nnm\conf\disco\UnnumberedSubnets.conf`

   UNIX: `$NNM_DATA/shared/nnm/conf/disco/UnnumberedSubnets.conf`

3. Restart the NNMi management server.

   a. Run the **`ovstop`** command on the NNMi management server.

   b. Run the **`ovstart`** command on the NNMi management server.

4. Wait for NNMi to complete the next discovery cycle.

See the `UnnumberedNodeGroup.conf` and `UnnumberedNodeGroup.conf` reference pages, or the UNIX manpage, for more information.

Controlling Deletion of Unresponsive Objects

You can control the deletion of the following unresponsive objects by specifying the number of days to wait after an object has become unresponsive:

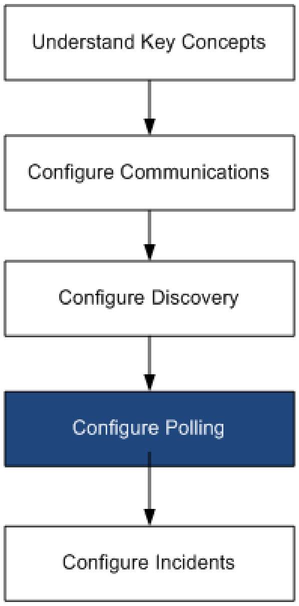
- Unresponsive nodes
- Connections that are down

To control the deletion of unresponsive objects, perform the following steps:

1. In the **Configuration** workspace, click **Discovery Configuration**.
2. In the **Delete Unresponsive Objects Control** area, enter the numbers of days for the system to wait before deleting the applicable objects. Note that a value of zero (0) indicates that the objects should not be deleted.

After the specified waiting period, the unresponsive objects are deleted from the database.

NNMi State Polling



This chapter provides information to help you expand and fine tune network monitoring by configuring the HP Network Node Manager i Software (NNMi) State Poller service. This chapter supplements the information in the NNMi help. For an introduction to how monitoring works and for detailed information about how to configure monitoring, see *Monitoring Network Health* in the NNMi help.

This chapter contains the following topics:

- Concepts for State Polling
- Plan State Polling
- Configure State Polling
- Evaluate State Polling
- Tune State Polling

Concepts for State Polling

This section provides a brief overview of network monitoring, including the order that the State Poller uses to evaluate polling groups. After reading the information in this section, continue to Plan State Polling on page 78 for more specific information.

As with network discovery, you should focus network monitoring on the critical or most important devices in the network. NNMi can only poll devices in the topology database. You control which network devices NNMi monitors, the type of polling to use, and the interval at which to poll.

You can use the interface and node settings on the **Monitoring Configuration** form to refine the status polling of devices, and to set different polling types and intervals for different classes, types of interfaces, and types of nodes.

You can configure State Poller data collection to be based on an ICMP (ping) response, or to be based on SNMP data. NNMi automatically handles the mapping from the type of data collection you enable to the actual MIB objects internally, significantly simplifying configuration.

As you plan polling configuration, you should carefully consider how to set up interface groups and node groups for the State Poller service. If you are new to the concept of *groups*, see Node Groups and Interface Groups on page 41, and Node/Interface/Address Hierarchy on page 45 for overview information.

Order of evaluation

Because an interface or node might qualify for multiple groups, the State Poller applies the configured polling interval and polling type in a well-defined order of evaluation. For each object in the discovered topology:

1. If the object is an interface, State Poller looks for a qualifying interface group. Groups are evaluated from the lowest Order Number to the highest. The first matching group is used and evaluation stops.
2. If no interface group has captured the object, node groups are evaluated from lowest Order Number to highest. The first matching group is used and evaluation stops. Any contained interface that has not qualified for an interface group on its own characteristics inherits the polling settings from its hosting node.
3. For devices that are discovered but not included in any node or interface settings definitions, the global monitoring settings (on the **Default Settings** tab of the **Monitoring Configuration** form) establish the monitoring behavior.

Plan State Polling

This section provides information to plan for State Poller configuration, including a polling configuration checklist; and more detailed information to help you plan for monitoring, decide how to create polling groups, and determine what types of data should be captured during the polling process.

Polling Checklist

You can use the checklist below to plan for State Poller configuration.

□ What can NNMi monitor?

□ What are the logical groups for monitored items, based on object type, location, relative importance, or other criteria?

□ How often should NNMi monitor each grouping?

□ What data should be collected to capture information about the monitored item? This might include:

— ICMP (ping) response

— SNMP fault data

— SNMP performance data if you have a license for one or more NNM Performance iSPIs

— Additional SNMP Component Health data

Example polling configuration

To help you understand the polling configuration process, consider this example. Suppose that your network contains the latest proxy servers from ProximiT. Ensure that these devices can be reached, but you do not require SNMP monitoring of the proxy servers.

1. What can NNMi monitor?

   Because you can only monitor what has been discovered, you configure auto-discovery rules to ensure that NNMi's database contains your ProximiT proxy servers. For more information on configuring discovery, see NNMi Discovery on page 59.

2. What are the logical groups for monitored items?

   It makes sense to group the ProximiT proxy servers together and apply the same monitoring settings to all of them. Because you are not doing interface (SNMP) monitoring for the devices, you do not need any interface groups.

   You can also use this node group to filter views, to check the status of the proxy servers as a group, and to put the group OUT OF SERVICE to update firmware.

3. How often should NNMi monitor each group?

   For your service level agreements, a five minute polling interval for the proxy servers is sufficient.

4. What data should be collected?

   Here's where the monitoring configuration differs from other groups. For our ProximiT proxy server example, you enable ICMP fault monitoring and disable SNMP fault and polling monitoring. Without SNMP fault monitoring for the group, Component Health monitoring will not apply.

For more detailed planning information concerning these configuration choices, see the following topics:

- — What Can NNMi Monitor? on page 79
- — Planning Groups on page 81
- — Planning Polling Intervals on page 83
- — Deciding What Data to Collect on page 84

What Can NNMi Monitor?

By default, the NNMi State Poller uses SNMP polls to monitor the following:

- Interfaces that are connected to another known interface on an NNMi-discovered device.
- Router interfaces that host IP addresses.

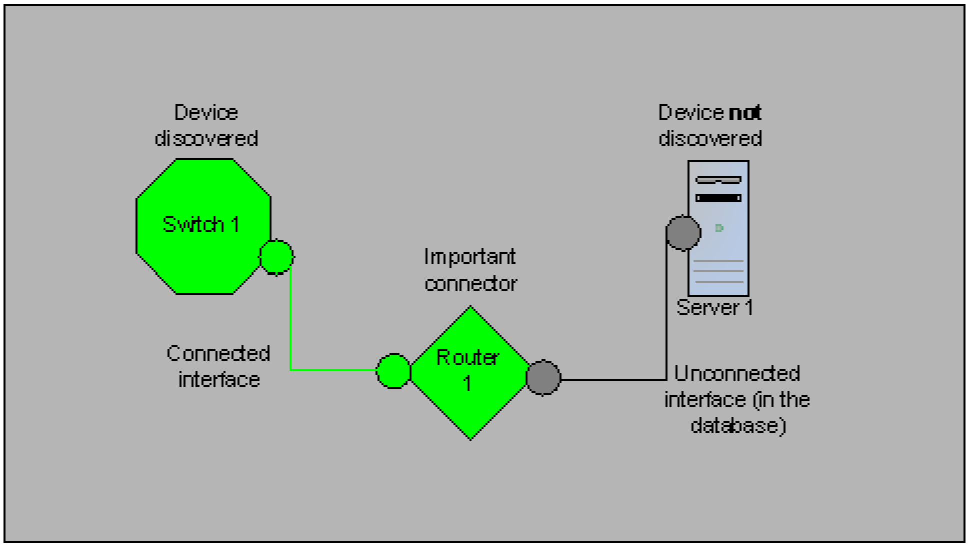
➤ In most cases, polling only connected interfaces provides sufficiently accurate root-cause analysis. Extending the set of monitored interfaces can impact polling performance.

Extend monitoring

You can extend the monitoring to include the following:

- Unconnected interfaces. By default, the only unconnected interfaces that NNMi monitors are those that have IP addresses *and* are included in the **Routers** node group.

➤ NNMi defines an unconnected interface as an interface that is not connected to another device discovered by NNMi, as shown below.



- Interfaces, such as router interfaces, that have an IP address.
- ICMP polling for devices that do not support SNMP. By default, ICMP polling is enabled for the **Non-SNMP Devices** node group.

Interfaces to Unmonitored Nodes

Sometimes, you must know the status of an interface that connects to a device you do not manage directly. For example, you want to know whether the connection to an application or Internet server is up, but you might not be responsible for maintaining that server. If you do not include the server in the discovery rules, NNMi sees the interface that faces the server as unconnected.

There are two ways to monitor the status of an important interface that connects to an unmonitored node.

- Discover the unmonitored node

  When you add an unmonitored node to the NNMi topology, NNMi sees the interfaces connecting the node to the rest of the topology as CONNECTED. Then NNMi can poll these interfaces according to the monitoring configuration. NNMi discovers the node as MANAGED. Unmanage nodes that you do not want NNMi to monitor.

  Each discovered node counts toward the license limit, regardless of whether NNMi is actively managing that node.

- Poll the unconnected interface

  You can create a node group containing the network devices that provide connectivity for undiscovered nodes. Then enable polling of unconnected interfaces for the node group.

  NNMi polls *all* interfaces on the devices in the node group, which can add a lot of traffic for a device with many interfaces.

Stop Monitoring

The NNMi management modes are used to set devices or interfaces to UNMANAGED or OUT OF SERVICE. UNMANAGED is considered to be a permanent situation; you will never care to know the status of the object. OUT OF SERVICE is for temporary situations where one or more objects will be offline and down incidents would be superfluous.

Consider the management mode as an overlay across all group settings. Regardless of its group, polling interval, or type, the State Poller does not communicate with an object when its status is set to UNMANAGED or OUT OF SERVICE.

Best practice

Some of the devices, interfaces, or both you choose to discover and place in the database do not need to be polled. Note those objects that you will permanently set to UNMANAGED. You might want to create one or more node groups to enable you to set management modes more easily.

Planning Groups

You must set up node and interface groups before configuring monitoring settings. Therefore, you must consider polling requirements while configuring node and interface groups. Ideally, node and interface groups are configured so that you can monitor important devices frequently, and you can check on non-critical devices less frequently (if at all).

Best practice

Configure one set of node and interface groups for network monitoring. Configure a different set of node groups for network visualization through maps.

These groups are defined through the **Configuration > Node Groups** or **Configuration > Interface Groups** work spaces and are, by default, the same groups that are used to filter incident, node, interface, and address views. To create a separate set of node or interface filters for configuring monitoring settings, open a node or interface group and select the **Add to View Filter List** check box on the **Node Group** or **Interface Group** form. Click **Save and Close**.

You can set polling types and polling intervals at a node group or interface group level on the **Node Settings** and **Interface Settings** tabs of the **Monitoring Configuration** form.

Determine the criteria by which you want to group interfaces, devices, or both by similar polling needs. Here are some factors to consider in your planning:

- Which area of your network contains these devices? Are there timing constraints?
- Do you want to differentiate polling intervals or data gathered by device type? By interface type?
- Does NNMi provide pre-configured groups you can use?

Best practice

You can create group definitions for objects that are likely to go OUT OF SERVICE at the same time, whether by location or some other criteria. For example, you could put all your Cisco routers into OUT OF SERVICE mode while you apply an IOS upgrade.

Interface Groups

Based on your criteria, determine which Interface groups to create. Remember that interface groups are evaluated first (see Concepts for State Polling on page 77). Interface groups can reference node group membership, so you might end up configuring node groups before interface groups to implement your plan.

Preconfigured interface groups

NNMi has several useful interface groups already configured for you to use. These include:

- All interfaces with an IFType related to ISDN connections
- Interfaces for voice connections
- Interfaces for point-to-point communication
- Software loopback interfaces
- VLAN interfaces
- Interfaces participating in link aggregation protocols

Over time HP might add more default groups to simplify your configuration tasks. You can use existing groups, modify them, or create your own.

Interface groups have two types of qualifiers: node group membership for the hosting node and IFType or other attribute for the interface. You can choose to combine these as follows:

- All interfaces on nodes in a node group are grouped regardless of IFType; do not select any IFTypes or attributes (such as name, alias, description, speed, index, address, or other IFType attributes).
- All interfaces of certain IFTypes or set of attributes are grouped, regardless of the node on which they reside.
- Only interfaces of a certain IFType or attributes that reside on a particular group of nodes are grouped.

Node Groups

After planning interface groups, plan node groups. Not all node groups created for monitoring make sense for filtering views, so you can configure them independently.

Preconfigured node groups

HP provides a default collection of node groups to simplify your configuration tasks. These are based on device categories derived from the system object ID during the Discovery process. The node groups provided by default include:

- Routers
- Networking Infrastructure Devices (such as switches or routers.)
- Microsoft Windows Systems
- Devices for which you do not have the SNMP community string
- Important Nodes. This is used internally by the Causal Engine to provide special handling for devices in the “shadow” of a connector failure. For more information, see *Node Groups As Predefined View Filters* in the NNMi help.

Over time HP might add more default groups to simplify your configuration tasks. You can use existing groups, modify them, or create your own.

You can qualify the definition of related nodes using the following node attributes:

- IP address(es) on the node
- Hostname wildcard convention
- Device Profile derivatives such as category, vendor, and family
- MIB II sysName, sysContact, sysLocation

Best practice

You can create simple, reusable, atomic groups and combine them into hierarchical clusters for monitoring or visualization. Group definitions can overlap, such as “All Routers” and “All systems with IP address ending in .100.” Nodes will probably qualify for multiple groups as well.

Find a balance by creating a rich set of groups for configuration and viewing without overloading the list with superfluous entries that will never be used.

Interaction with Device Profiles

When each device is discovered, NNMi uses its system object ID to index into the list of available Device Profiles. The Device Profile is used to derive additional attributes of the device, such as vendor, product family, and device category.

As you configure node groups, you can use these derived attributes to categorize devices to apply monitoring settings. For example, you might want to poll all switches regardless of vendor throughout your network on a certain polling interval. You can use the derived device category, Switch, as the defining characteristic of your node group. All discovered devices whose system object ID maps to the category, Switches, will receive the configured settings for the node group.

Planning Polling Intervals

For each object group, you select a polling interval that NNMi uses to collect data. The interval can be as short as one minute, or as long as days to best match your Service Level Agreements.

Best practice

Shorter intervals help you become aware of network problems as soon as possible; however, polling too many objects in too short an interval can cause a backlog in the State Poller. Find the best balance between resource use and intervals for your environment.

➤ The Causal Engine performs a Status Poll of each node every 24 hours and updates Status, Conclusion, and Incident information as needed. This Status Poll does not affect the timing of the Polling interval configured for the device.

Deciding What Data to Collect

The State Poller service uses polls to gather state information about the monitored devices in your network. Polling can be done using ICMP, SNMP, or both.

ICMP (ping) ICMP address monitoring uses ping requests to verify the availability of each managed IP address.

SNMP SNMP monitoring verifies that each monitored SNMP agent is responding to SNMP queries.

- The State Poller is highly optimized to collect configured SNMP information from each monitored object with one query at each interval. When you save configuration changes, the State Poller recalculates the group membership of each object and reapplies the configured interval and set of data to collect.
- SNMP monitoring issues SNMP queries for all monitored interfaces and components, requesting the current values from the MIB II interface table, the HostResources MIB, and vendor-specific MIBs. Some values are used for fault monitoring. If you have the NNM iSPI Performance for Metrics installed, some values are used for performance measurement.

SNMP Component Health data You might enable or disable Component Health monitoring at the global level. Component Health monitoring for faults follows the fault polling interval settings for the device.

Gathering additional data at each poll does not affect the time to execute the poll. However, additional data stored for each object can increase the memory requirements for State Poller.

➤ Performance monitoring settings are only used with the NNM iSPI Performance for Metrics. Component Health monitoring for performance follows the performance polling interval settings for the device.

Best practice Batching your monitoring configuration changes is less disruptive to State Poller ongoing operation.

Configure State Polling

This section provides configuration tips and provides some configuration examples. After reading the information in this section, see *Configure Monitoring Behavior* in the NNMi help for specific procedures.

➤ It is a good idea to save a copy of the existing configuration before you make any major configuration changes. For more information, see Best Practice: Save the Existing Configuration on page 40.

Configure Interface Groups and Node Groups

You create interface groups and node groups in the **Configuration** workspace. For more information, see *Creating Groups of Nodes or Interfaces* in the NNMi help.

Examples

For example, to configure a node group for ProximiT proxy servers:

1. Open **Configuration > Node Groups** and click **New**.
2. Name the group `Proxy Servers` and check **Add to View Filter List**.
3. On the **Additional Filters** tab, select the `hostname` attribute, and leave the operator set to `=`.
4. For value, enter the wildcard as `prox*.example.com`.

   If you had configured a device profile and device category for the ProximiT devices, you could use the **Device Filters** tab to access the **Device Category** selector and base the group on the Proxy Server category you created.
5. Click **Save and Close** on the group definition.

➤ You must configure node groups before you can reference them in your interface group configuration.

Configure Interface Monitoring

State Poller analyzes interface group membership before node groups. For each of the interface groups you created, as well as any of the preexisting ones you want to use, open the **Monitoring Configuration** dialog and the **Interface Settings** tab to create a custom set of instructions for how State Poller should handle that group. Your instructions will include:

- Enabling or disabling fault polling
- Setting the fault polling interval
- Enabling or disabling performance polling if you have the NNM iSPI Performance for Metrics
- Setting the performance polling interval if you have the NNM iSPI Performance for Metrics
- Setting performance management thresholds if you have the NNM iSPI Performance for Metrics
- Selecting whether NNMi should monitor unconnected interfaces (or unconnected interfaces hosting IP addresses) in the group

You can configure different settings for each interface group. Remember that the State Poller evaluates the list in order from the lowest ordering number to the highest ordering number.

Best practice

Double-check your order numbers, keeping in mind that an object that qualifies for multiple groups has settings applied from the group with the lowest order number.

Configure Node Monitoring

If an object does not qualify for any configured interface group, State Poller evaluates the object for membership in node groups. Settings are applied to the first node group match from the lowest ordering number to the highest ordering number.

For each node group, open the **Monitoring Configuration** form, and then, open the **Node Settings** tab. Create a custom set of instructions as to how State Poller should handle that group. Your instructions can include:

- Enabling or disabling fault polling
- Setting the fault polling interval
- Enabling or disabling performance polling if you have the NNM iSPI Performance for Metrics
- Setting the performance polling interval if you have the NNM iSPI Performance for Metrics
- Setting performance management thresholds if you have the NNM iSPI Performance for Metrics
- Selecting whether NNMi should monitor unconnected interfaces (or unconnected interfaces hosting IP addresses) in the group

You might configure different settings for each node group.

Best practice

Double-check the order numbers, keeping in mind that an object that qualifies for multiple groups has settings applied from the group with the lowest order number.

Verify Default Settings

State Poller applies the settings from the **Default Settings** tab for any object that does not match a defined interface setting or node setting. Review the settings on this tab to ensure they match your environment at the default level. For example, you would rarely poll all unconnected interfaces as a default setting.

➤ Be sure you **Save and Close** all **Monitoring Configuration** dialog boxes all the way back to the console for your changes to be implemented.

Evaluate State Polling

This section lists ways to evaluate the progress and success of the monitoring settings.

Verify the Configuration for Network Monitoring

You can determine the settings that NNMi uses for monitoring a given node or interface, and you can initiate a status poll of a node at any time.

Is the interface or node a member of the right group?

You can verify which interfaces or nodes belong to a group by selecting one of the following in the **Configuration** workspace:

- Node Groups
- Interface Groups

Follow the instructions in the help to show the members of the group. Keep in mind that an object can be a member of multiple groups, and that another group might have a lower ordering number.

Alternatively, you can see the full list of groups to which the object belongs by opening the object (interface or node) and clicking the **Node Groups** or **Interface Groups** tab. This list is alphabetical by group name and does not reflect the ordering numbers that determine which settings are applied.

If the object is not a member of a group:

1. Retrieve the device profile for the node in the inventory view.
2. Review the attribute mapping for the device profile under **Configuration > Device Profiles**.
3. Review the attribute requirements for the node group definition.

If you have a mismatch, you can adjust the category derived in the Device Profile to force that type of device to qualify for your node group. You might need to do an **Actions** > **Configuration Poll** to update the attributes for the node so that it qualifies.

Which settings are being applied?

To check the monitoring configuration in effect for a specific node, interface, or address, select that object in the appropriate inventory view, and select **Actions > Monitoring Settings**. NNMi opens the current monitoring settings.

Examine the values for **Fault Polling Enabled** and **Fault Polling Interval**. If these values are not as expected, look at the value for **Node Group** or **Interface Group** to see which ordered group match applied.

You might need to check **Actions** > **Communication Settings** for the object to ensure traffic has not been disable for it.

Which data is being collected?

You can initiate a status poll of a specific device to validate that the expected types of polls (SNMP, ICMP) are being performed for that device. Select a node, and then click **Actions > Status Poll**. NNMi performs a real-time status check of the device. The output shows the types and results of the polls being performed. If the types of polls are not what you expect, check the monitoring settings for the node and the respective global, interface, or node settings of the monitoring configuration.

Evaluate the Performance of Status Polling

Evaluate the performance of status polling in your environment by using the information in the state poller health check to quantify and assess the operation of the state poller service.

Is the State Poller keeping up?

At any time, you can check the current health statistics about the state poller service on the **State Poller** tab of the **System Information** window, as described in Table 2.

Table 2 State Poller Health Information

Information	Description
Status	Overall status of the state poller service
Poll counters	• Collections requested in last minute • Collections completed in last minute • Collections in process
Time to execute skips in last minute	The number of regularly scheduled polls that did not complete within the configured polling interval. A non-zero value indicates that the polling engine is not keeping up or that targets are being polled faster than they can respond. • What to watch for: If this value continues to increase, there are problems communicating with the target or NNMi is overloaded. • Action to take: Look in the `nnm.?.0.log` file for messages for the classes beginning with the string `com.hp.ov.nms.statepoller` to determine the targets for the skipped polls. — If the skipped polls are for the same targets, change the configuration to poll these targets at a less frequent rate or to increase the timeout for these targets. — If the skipped polls are for different targets, check the NNMi system performance, especially the available memory for ovjboss.
Stale collections in last minute	A stale collection is a collection that has not received a response from the polling engine for at least 10 minutes. A healthy system should never have any stale collections. • What to watch for: If this value increases consistently, there is a problem with the polling engine. • Action to take: Look in the `nnm.?.0.log` file for messages for the classes beginning with the string `com.hp.ov.nms.statepoller` to determine the targets for the stale collections. — If the stale collections are for a single target, unmanage the target until you can resolve the problem. — If the stale collections are for different targets, check the performance of the NNMi system and the NNMi database. Stop and restart NNMi.
Poller result queue length	• What to watch for: This value should be close to 0 most of the time. • Action to take: If this queue size is very large, ovjboss might be running out of memory.
State mapper input queue length	• What to watch for: This value should be close to 0 most of the time. • Action to take: If this queue size is very large, then check the performance of the NNMi system and the NNMi database.
State updater queue time length	• What to watch for: This value should be close to 0 most of the time. • Action to take: If this queue size is very large, then check the performance of the NNMi system and the NNMi database.

Tune State Polling

The performance of state polling is affected by the following key variables:

- The number of devices/interfaces to be polled
- The type of polling configured
- The frequency of polling each device

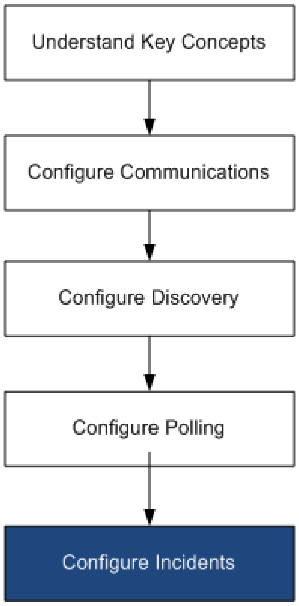
These variables are driven by your network management needs. If you are experiencing performance issues with status polling, consider the following configurations:

- Because polling settings for individual nodes are controlled through their membership in node groups and interface groups, make sure that the groups contain nodes or interfaces with similar polling requirements.
- If you are polling unconnected interfaces or interfaces that host IP addresses, check the configurations to make sure you are only polling the interfaces that are necessary. Enable these polls on the **Node Settings** or **Interface Settings** form (not as a global setting on the **Monitoring Configuration** form) to maintain the most specific control and to select the smallest subset of interfaces to poll.
- Remember that polling unconnected interfaces monitors *all* unconnected interfaces. To monitor only those unconnected interfaces that have IP addresses, enable polling of interfaces that host IP addresses.

Regardless of the monitoring configuration, status polling is dependent on network responsiveness and might be impacted by overall system performance. Although status polling with default polling intervals does not introduce much network load, if the performance of the network link between the server and the polled device is poor, status polling performance is poor. You can configure larger time-outs and a smaller number of retries to reduce the network load, but these configuration changes only go so far. Timely polling requires adequate network performance and sufficient system resources (CPU, memory).

Enabling or disabling the Component Health monitoring has no effect on timeliness of polling. It simply gathers additional MIB objects at the schedule time. However, disabling Component Health monitoring might reduce the amount of memory used by the State Poller.

NNMi Incidents



HP Network Node Manager i Software (NNMi) provides a large number of default incidents and correlations that filter incoming SNMP traps to provide a workable number of incidents in the NNMi console. This chapter provides information to help you fine tune network management by configuring the NNMi incidents. This chapter supplements the information in the NNMi help. For an introduction to NNMi incidents and for detailed information about how to configure incidents, see *Configuring Incidents* in the NNMi help.

This chapter contains the following topics:

- Concepts for Incidents
- Plan Incidents
- Configure Incidents
- Evaluate Incidents
- Tune Incidents

Concepts for Incidents

NNMi collects network status information from the following sources:

- The NNMi Causal Engine analyzes the health of your network and provides the ongoing health status reading for each device. The Causal Engine also extensively evaluates and determines the root cause of network problems whenever possible.
- SNMP traps from network devices. The NNMi Causal Engine uses this information as symptoms during its analysis.
- NNM 6.x/7.x events forwarded from one or more NNM 6.x/7.x management stations.

NNMi converts this network status information into incidents that provide useful information for managing the network. NNMi provides many default incident correlations that reduce the number of incidents for network operators to consider. You can customize the default incident correlations and create new incident correlations to match the network management needs of your environment.

The incident configurations in the NNMi console define the incident types that NNMi can create. If no incident configuration matches a received SNMP trap or NNM 6.x/7.x event, that information is discarded. If the management mode of the source object is set to NOT MANAGED or OUT OF SERVICE in the NNMi database, NNMi always discards the incoming trap.

`nnmtrapconfig.ovpl -dumpBlockList` outputs information about the current incident configuration, including SNMP traps that were not passed into the incident pipeline because of non-existent or disabled incident configurations.

Additionally, NNMi discards SNMP traps from network devices that are not in the NNMi topology. For information about changing this default behavior, see *Handle Unresolved Incoming Traps* in the NNMi help.

For more information, see the following:

- *About the Event Pipeline* in the NNMi help
- *The NNMi Causal Engine and Incidents* in the NNMi help
- *NNMi Causal Analysis White Paper*, available from **http://h20230.www2.hp.com/selfsolve/manuals**

Incident Lifecycle

Table 3 describes the stages of an incident's lifecycle.

Table 3 NNMi Incident Lifecycle

Lifecycle State	Description	State Set By	Incident Used By
none	The NNMi event pipeline receives input from all sources and creates incidents as needed.	not applicable	• NNMi
Dampened	The incident is in a holding place waiting to be correlated with another incident. The purpose of this waiting period is incident reduction in the incident viewers. The dampening interval can vary per incident type. For more information, see Incident Suppression, Enrichment, and Dampening on page 97.	NNMi	• NNMi
Registered	The incident is visible in incident views. The incident is forwarded to any configured destinations (northbound or global manager).	NNMi A user can also set this state in an incident view.	• Users • Lifecycle transition actions • Integrations that forward incidents

Table 3 NNMi Incident Lifecycle (cont'd)

Lifecycle State	Description	State Set By	Incident Used By
In Progress	The incident has been assigned to someone who is investigating the problem. The network administrator defines the specific meaning of this state.	User	• Users • Lifecycle transition actions • Integrations that forward incidents
Completed	Investigation of the problem indicated by the incident is complete, and a solution is in place. The problem that the incident identifies The network administrator defines the specific meaning of this state.	User	• Users • Lifecycle transition actions • Integrations that forward incidents
Closed	Indicates that NNMi determined the problem reported by this Incident is no longer a problem. For example, when you remove an interface from a device, all incidents related to the interface are automatically closed.	User or NNMi	• Users • Lifecycle transition actions • Integrations that forward incidents

Trap and Incident Forwarding

Table 4 summarizes the ways to forward traps and incidents from the NNMi management server to another destination. The text following the table compares the NNMi SNMP trap forwarding mechanism with the NNMi northbound interface SNMP trap forwarding mechanism.

Table 4 Supported Ways to Forward Traps and NNMi Incidents

	NNMi Trap Forwarding	NNMi Northbound Interface Trap Forwarding	Global Network Management Trap Forwarding
What to forward	• SNMP traps from network devices	• SNMP traps from network devices • NNMi management events	• SNMP traps from network devices • NNM 6.x/7.x events from NNM management stations
Forwarding format	SNMPv1, v2c, or v3 traps, as received (SNMPv3 traps can be converted to SNMPv2c traps)	SNMPv2c traps created from NNMi incidents	NNMi incidents
Added information	In most cases, NNMi adds varbinds to identify the original source object. NNMi does not ever modify SNMPv1 traps.	NNMi adds varbinds to identify the original source object.	Any information added to the incident by the regional manager processes is retained in the forwarded incident.

Table 4 Supported Ways to Forward Traps and NNMi Incidents (cont'd)

	NNMi Trap Forwarding	NNMi Northbound Interface Trap Forwarding	Global Network Management Trap Forwarding
Where to configure	**Trap Forward Configuration** in the **Configuration** workspace	**HPOM**, **Northbound Interface**, or **Netcool** in the **Integration Module Configuration** workspace	**Forward to Global Managers** tab on an **SNMP Trap Configuration** form or a **Remote NNM 6.x/7.x Event Configuration** form
Notes		NNMi provides several integrations built on the NNMi northbound interface: • NNMi Northbound Interface on page 543 • HP NNMi—HPOM Integration (Agent Implementation) on page 577 • HP NNMi Integration Module for Netcool Software on page 615	Forward the remote incidents that should be visible in the global manager incident views. Forwarded incidents participate in correlations on the global manager.
For more information	*Configuring Trap Forwarding* in the NNMi help	Using the NNMi Northbound Interface on page 546	• *Configure Forward to Global Manager Settings for an SNMP Trap Incident* in the NNMi help • *Configure Forward to Global Managers Settings for a Remote 6.x/7.x Event Incident* in the NNMi help

Comparison: Forwarding Third-Party SNMP Traps to Another Application

If you want to forward the SNMP traps that NNMi receives from managed devices to another application, you can use either of the following approaches:

- Use the NNMi SNMP trap forwarding mechanism. For information about how to configure NNMi SNMP trap forwarding, see *Configuring Trap Forwarding* in the NNMi help.
- Use the NNMi northbound interface SNMP trap forwarding mechanism. For information about configuring the NNMi northbound interface to forward received SNMP traps, see Incidents in Table 58 on page 554.

The approach to trap identification by the receiving application varies with the SNMP trap forwarding mechanism:

- *Windows (all) and UNIX without original trap forwarding*

  This description applies to the default and SNMPv3 to SNMPv2c conversion forwarding options.

The NNMi SNMP trap forwarding mechanism on a Windows NNMi management server enriches each SNMP trap before forwarding it to the trap destination. The trap appears to originate from the NNMi management server. (This information also applies to a UNIX NNMi management server for which the original trap forwarding option is not selected on the **Trap Forwarding Destination** form.)

To ensure the correct association between the trap-sending device and the event in the receiving application, the rules for these traps must be customized for the enriched varbinds. Interpret the value from the originIPAddress (.1.3.6.1.4.1.11.2.17.2.19.1.1.3) varbind. The originIPAddress value is a byte string of generic type InetAddress, either InetAddressIPv4 or InetAddressIPv6 as determined by the value of originIPAddressType (.1.3.6.1.4.1.11.2.17.2.19.1.1.2) varbind. The rule must read the originIPAddressType varbind to determine the type of Internet address (ipv4(1), ipv6(2)) value in the originIPAddress varbind. The rule might also need to convert the originIPAddress value to a display string.

For more information about the varbinds that NNMi adds to forwarded traps, see *Trap Varbinds Provided by NNMi* in the NNMi help, RFC 2851, and the following file:

— *Windows*: `%NNM_SNMP_MIBS\Vendor\Hewlett-Packard\hp-nnmi.mib`

— *UNIX*: `$NNM_SNMP_MIBS/Vendor/Hewlett-Packard/hp-nnmi.mib`

- *UNIX with original trap forwarding*

  The NNMi SNMP trap forwarding mechanism on a UNIX NNMi management server can forward the traps in the same format as NNMi receives them. Each trap appears as if the managed device sent it directly to the trap destination, so existing trap processing configured in the receiving application should work without modification.

  For more information, see the original trap forwarding option in *Trap Forwarding Destination Form* in the NNMi help.

- *NNMi northbound interface (all operating systems)*

  The NNMi northbound interface enriches each SNMP trap before forwarding it to the trap destination. The trap appears to originate from the NNMi management server. To ensure the correct association between the trap-sending device and the event in the receiving application, the rules for these traps must be customized for the enriched varbinds. The IncidentNodeHostname (1.3.6.1.4.1.11.2.17.19.2.2.21) and IncidentNodeMgmtAddr (1.3.6.1.4.1.11.2.17.19.2.2.24) varbinds identify the original source object.

MIBs

NNMi requires that the following management information base (MIB) files be loaded into the NNMi database:

- All MIB variables used in MIB expressions for the Custom Poller feature, line graphs, or both
- Node components that NNMi monitors for health (for example fan or power supply)
- (NNM iSPI Performance for Metrics) All MIB variables used in threshold monitoring

NNMi requires that the following management information base (MIB) files, or the traps defined in the MIB files, be loaded into the NNMi database:

- All SNMP traps that you want to forward to a northbound destination
- (NNM iSPI NET) All MIB variables accessed from Trap Analytics reports

Custom Incident Attributes

NNMi uses custom incident attributes (CIAs) to attach additional information to incidents.

- For an SNMP trap incident, NNMi stores the original trap varbinds as CIAs for the incident.
- For a management event incident, NNMi adds pertinent information (for example, com.hp.ov.nms.apa.symptom) as CIAs for the incident.

You can use incident CIAs to narrow the scope of configurations such as incident lifecycle transition actions, suppression, deduplication, and enrichment. You can also use CIAs to narrow the availability of the menu items on the Actions menu for an incident view or form.

To determine which CIAs NNMi adds for any given incident, open a sample incident from an incident view, and look at the information on the Custom Attributes tab.

CIAs Added to Closed Management Event Incidents

When the NNMi Causal Engine determines that the conditions that caused a management event incident no longer apply, NNMi sets that incident's lifecycle state to CLOSED and adds the CIAs listed in Table 5 to the incident. NNMi console users can see this information in the **Correlation Notes** field of the **Incident** form. Lifecycle transition actions can use the values of the CIAs directly.

Table 5 Custom Incident Attributes for a Closed Incident

Name	Description
cia.reasonClosed	The reason that NNMi cancelled or closed the incident. This reason is also the conclusion name, for example NodeUp or InterfaceUp. If this field is not set, an NNMi console user closed the incident. To determine the NNMi expected values of the cia.reasonClosed CIA, see *How NNMi Closes Incidents* in the NNMi help.
cia.incidentDurationMs	The duration, in milliseconds, of the outage, as measured by NNMi from when the status goes down and comes back up. This value is the difference of the cia.timeIncidentDetectedMs and cia.timeIncidentResolvedMs CIAs. It is a more accurate measurement than comparing the timestamps of down and up incidents.
cia.timeIncidentDetectedMs	The timestamp, in milliseconds, when the NNMi Causal Engine first detected the problem.
cia.timeIncidentResolvedMs	The timestamp, in milliseconds, when the NNMi Causal Engine detected that the problem has been resolved.

NNMi adds the CIAs listed in Table 5 to most primary and secondary root cause incidents. For example, a NodeDown incident can have InterfaceDown and AddressDown incidents as secondary root causes. When NNMi closes the NodeDown incident, NNMi also closes the secondary incidents and adds the CIAs with values for each incident context to the secondary incidents.

NNMi does not add the CIAs listed in Table 5 to the following default management event incident types:

- Incidents that an NNMi console user closes manually
- Incidents that NNMi closes in response to an object being deleted from the NNMi database
- IslandGroupDown incidents
- NnmClusterFailover, NnmClusterLostStandby, NnmClusterStartup, and NnmClusterTransfer incidents
- Incidents in the following families:
  - Correlation
  - License
  - NNMi Health
  - Trap Analysis

Incident Reduction

NNMi provides the following customizable correlations for reducing the number of incidents that network operators see in the NNMi console:

- Pairwise correlation—One incident cancels another incident.
- Deduplication correlation—When multiple copies of an incident are received within the specified time window, correlate the duplicates under a deduplication incident. The time window restarts for each newly received duplicate incident. In this way, NNMi correlates the duplicate incidents until it has not received any duplicates for the entire duration of the correlation time window.
- Rate correlation—When the specified number of copies on an incident are received within the specified time window, correlate the duplications under a rate incident. NNMi generates the rate incident when the specified number of incidents has been received, regardless of how much time remains in the time window.

Incident Suppression, Enrichment, and Dampening

NNMi provides a rich feature set for getting the most value from incidents. For each incident type, you can specifically define when an incident is of interest with the following incident configuration options:

- Suppression—When an incident matches the suppression configuration, that incident does not appear in the NNMi console incident views. Incident suppression is useful for incidents (for example, SNMPLinkDown traps) that are important for some nodes (for example routers and switches) but not others.

- Enrichment—When an incident matches the enrichment configuration, NNMi changes one or more incident values (for example, severity or message) according to the contents of the incident. Incident enrichment is useful for processing traps (for example, RMONFallingAlarm) that carry the distinguishing information in the trap varbinds (payload).
- Dampening—When an incident matches the dampening configuration, NNMi delays activity for that incident for the duration of the dampen interval. Incident dampening provides time for the NNMi Causal Engine to perform root cause analysis on the incident, which is useful for providing fewer, more meaningful incidents in the NNMi console.

For each incident type NNMi provides the following levels of configuration for suppression, enrichment, and dampening:

- Interface group settings—Specify incident behavior when the source object is a member of an NNMi interface group. You can specify different behavior for each interface group.
- Node group settings—Specify incident behavior when the source object is a member of an NNMi node group. You can specify different behavior for each node group.
- Default settings—Specify default incident behavior.

For each incident configuration area (suppression, enrichment, and dampening), NNMi uses the following procedure to determine the behavior of a specific incident:

1. Check the interface group settings:
   - If the source object matches any interface group settings, carry out the behavior defined in the match with the lowest ordering number and stop looking for a match.
   - If the source object does not match any interface group settings, continue with step 2.
2. Check the node group settings:
   - If the source object matches any node group settings, carry out the behavior defined in the match with the lowest ordering number and stop looking for a match.
   - If the source object does not match any node group settings, continue with step 3.
3. Carry out the behavior defined in the default settings, if any.

Lifecycle Transition Actions

A lifecycle transition action is an administrator-provided command that runs when an incident lifecycle state changes to match the action configuration. An incident action configuration is specific to one lifecycle state for one incident type. The action configuration identifies the command to run when this incident type transitions to the specified lifecycle state. The command can include arguments that pass incident information to the action code.

The action code can be any Jython file, script, or executable that runs correctly on the NNMi management server. The action code can be specific to one incident type, or it can process many incident types. For example, you might creation action code that pages a network operator when NNMi creates a ConnectionDown, NodeDown, or NodeOrConnectionDown incident. You would configure three incident actions, one for the REGISTERED lifecycle state for each of these incident types.

Similarly, the action code can be specific to one lifecycle state change, or it can respond to several lifecycle state changes. For example, you might create action code that generates a trouble ticket when NNMi creates an InterfaceDown incident and closes the trouble ticket when the InterfaceDown incident is canceled. You would configure two incident actions for the InterfaceDown incident, one for the REGISTERED state and one for the CLOSED state.

Each action configuration can include a payload filter based on CIAs that limits when the action is run. For additional filtering, you can use incident enrichment to add a CIA to the incident. NNMi determines the value of that attribute from the incident source. For example, if you have added a custom attribute to some nodes, you can add this information to the incident as a CIA and then base the payload filter for an incident action on this attribute value.

Plan Incidents

Make decisions in the following areas:

- Which Device Traps Should NNMi Process?
- Which Incidents Should NNMi Display?
- How Should NNMi Respond to Incidents?
- Should NNMi Receive Traps from an NNM Management Station?
- Should NNMi Forward Traps to Another Event Receiver?

Which Device Traps Should NNMi Process?

Identify the device traps that are of interest in your network, and plan an incident configuration for each trap. NNMi can process traps without the MIB being loaded into NNMi. If the MIB contains TRAP-TYPE or NOTIFICATION-TYPE macros, you can create skeleton incident configurations for the traps defined in the MIB.

Decide whether you want to see traps from devices that are not in the NNMi topology.

Which Incidents Should NNMi Display?

The default set of incidents is a good place to start. You can expand and reduce the incident set over time.

Plan which incidents can be reduced though deduplication, rate configuration, and pairwise correlation.

How Should NNMi Respond to Incidents?

What actions (for example, sending an email message to a network operator) should NNMi take when certain incidents occur? At what lifecycle state should each action run?

Should NNMi Receive Traps from an NNM Management Station?

If your environment includes one or more NNM 6.x/7.x management stations that will continue managing areas of the network in conjunction with NNMi, identify the NNM 6.x/7.x events that will help NNMi operators manage the network. Plan an incident configuration for each NNM 6.x/7.x event that should be available in the NNMi console.

Should NNMi Forward Traps to Another Event Receiver?

If your environment includes a third-party trap consolidator, decide whether to use the NNMi SNMP trap forwarding mechanism with the NNMi northbound interface SNMP trap forwarding mechanism.

If you choose the NNMi northbound interface SNMP trap forwarding mechanism, load the MIBs for all traps that NNMi will forward to the event receiver.

Configure Incidents

This section lists configuration tips and provides some configuration examples. After reading the information in this section, see *Configuring Incidents* in the NNMi help for specific procedures.

➤ It is a good idea to save a copy of the existing configuration before you make any major configuration changes. For more information, see Best Practice: Save the Existing Configuration on page 40.

- Configure the incident types that you planned. If possible, start with the skeleton incident configurations from the traps defined in the MIB.
- Load any MIBs that are required for trap forwarding.
- Verify that devices are configured to send traps to the NNMi management server.

Configuring Incident Suppression, Enrichment, and Dampening

While configuring incident suppression, enrichment, and dampening, note the following:

- For each interface group, node group, or default setting, you can specify a payload filter that further refines when the configuration is applicable.
- Configure interface group settings on the **Interface Settings** tab of an incident configuration form.
- Configure node group settings on the **Node Settings** tab of an incident configuration form.
- Configure default settings on the **Suppression**, **Enrichment**, and **Dampening** tabs of an incident configuration form.

Configuring Lifecycle Transition Actions

While configuring lifecycle transition actions, note the following:

- By default, NNMi runs actions in the following location:
  - *Windows*: `%NnmDataDir%\shared\nnm\actions`
  - *UNIX*: `$NNM_DATA/shared/nnm/actions`

  If an action is not in this location, specify the absolute path to the action in the **Command** field of the **Lifecycle Transition Action** form.

  ➤ Jython files must be placed in the `actions` directory.

- Each time you make a change to the action configuration, NNMi rereads the actions directory for Jython files and loads them into NNMi.
- Actions are enabled as a group for an incident type.
- For information about the NNMi information that you can pass to an action, see *Valid Parameters for Configuring Incident Actions* in the NNMi help.

Evaluate Incidents

This section lists ways to evaluate the incident configuration.

- Verify that NNMi receives traps from all managed devices in the network.

  If NNMi is not receiving traps, verify the configuration of the firewall on the NNMi management server.

  ➤ Some anti-virus software includes a firewall that is configured separately from the system firewall.

- Verify that the most important traps are converted to incidents.
- Verify that incident actions run at the correct lifecycle state transitions.
- Verify that NNMi is handling incidents as expected.

  The **Actions > Incident Configuration Reports** menu contains several options for testing an existing incident against the current configuration of that incident type. Using one of these menu items does not change the incidents currently in the NNMi console.

Tune Incidents

Reduce the number of incidents in the NNMi console incident views. Use any of the following methods:

- Disable the incident configuration for any incident types that are not needed in the NNMi console.
- Set the management mode of the network objects that you do not need to monitor to NOT MANAGED or OUT OF SERVICE. NNMi discards most incoming traps from these nodes and their interfaces.
- Set NNMi to not monitor some network objects. NNMi discards most incoming traps from the source objects that are not monitored.
- Identify additional criteria for or relationships between incoming incidents. When these criteria or relationships occur, NNMi modifies the flow of incidents by recognizing the criteria or patterns of incoming management events or SNMP traps and nesting related incidents as correlated children.

Enabling and Configuring Incidents for Undefined Traps

NNMi drops undefined traps silently by default. As of NNMi 9.01, NNMi can identify any undefined SNMP traps that might be dropped.

If you have NNM iSPI NET licensed on the NNMi management server, use the `Total Traps Received (by OID)` report to research the dropped SNMP traps. See *Analyze Trap Information (NNM iSPI NET)* in the NNMi help for more information.

If you do not have NNM iSPI NET licensed on the NNMi management server, and want to see the missing traps as an incident, configure the Undefined SNMP Trap incident as follows:

1. Edit the following file:
   - *Windows*: `%NNM_PROPS%\nms-jboss.properties`
   - *UNIX*: `$NNM_PROPS/nms-jboss.properties`
2. Look for look for a section in the file that resembles the following line:

   ```
   #!com.hp.nnm.events.allowUndefinedTraps=false
   ```

   Change this line as follows:

   ```
   com.hp.nnm.events.allowUndefinedTraps=true
   ```
3. *Optional*. Specify the incident severity using the values explained within the `nms-jboss.properties` file. Look for a section in the file that resembles the following line:

   ```
   #!com.hp.nnm.events.undefinedTrapsSeverity=NORMAL
   ```

   Change this line as follows, substituting a defined severity value for *YourSpecifiedSeverity*.

   ```
   com.hp.nnm.events.undefinedTrapsSeverity=YourSpecifiedSeverity
   ```

4. *Optional*. Specify the incident nature using the values explained within the `nms-jboss.properties` file. Look for a section in the file that resembles the following:

   ```
   #!com.hp.nnm.events.undefinedTrapsNature=INFO
   ```

   Change this line as follows, substituting a defined nature value for *YourSpecifiedNature*.

   ```
   com.hp.nnm.events.undefinedTrapsNature=YourSpecifiedNature
   ```

5. Restart NNMi by running the following commands:

   a. **`ovstop`**

   b. **`ovstart`**

6. Review the list of undefined traps and create new incident configurations for those traps that you want to control. Enable the new incident if you want NNMi to display it and disable the new incident if you want NNMi to ignore it. See *Configuring SNMP Trap Incidents* in the NNMi help for more information.

NNMi Console

Use the information in this chapter to understand how to use the NNMi console to configure NNMi to function in specific ways.

This chapter contains the following topics:

A Practical Example of Using Node Groups

The following shows a practical example for configuring node groups.

My Network: A top level *container* node group containing other node groups.

> **USA**: An intermediate *container* node group containing other node groups.
>
> > **Colorado**: A node group containing nodes located in Colorado.

Note the following:

- It is a best practice to design your node group map layout ahead of time.
- It is a best practice to configure one set of node and interface groups for network monitoring. Configure a different set of node groups for network visualization through maps.
- In this example, **Colorado** is the only node group that contains nodes.

- NNMi provides more than one way to configure node groups and node group maps. After you become familiar with the steps described in this document, you might find more efficient ways to create subsequent node groups and node group maps.

This document guides you through the following steps for configuring node groups and node group maps, and then deleting node groups:

Create Node Groups

- Step 1: Create the My Network Node Group
- Step 2: Create the USA Node Group
- Step 3: Create the Colorado Node Group Using Filters
- Step 4: View the Node Group Members to Check the Node Group Filter Results
- Step 5: Set Up the Node Group Hierarchy for the My Network Node Group
- Step 6: Establish the Node Group Hierarchy for the USA Node Group

➤ Parent node groups might not contain any nodes. Instead they contain only child node groups in the definition. In this example, the `My Network` and `USA` node groups are parent node groups that contain only child node groups.

Configure the Node Group Maps

- Step 1: Create the Node Group Maps
- Step 2: View the Node Group Maps
- Step 3: Configure Node Group Status
- Step 4: Configure Node Group Map Ordering
- Step 5: Add a Background Image to a Node Group Map

Remove Node Groups

- Step 1: Navigate to the Node Group
- Step 2: Delete the Node Group

Create Node Groups

We begin by creating the Node Groups to include in our Node Group maps.

Step 1: Create the My Network Node Group

To create the **My Network** Node Group:

1. Navigate to the **Configuration** workspace.
2. Select **Node Groups**.
3. Click the **New** icon.
4. In the **Name** attribute, enter: **`My Network`**.
5. In the **Notes** attribute, enter: **`This is the top level Node Group`**.
6. Click **Save and Close** to save this configuration.

Step 2: Create the USA Node Group

1 Navigate to the **Configuration** workspace.

2 Select **Node Groups**.

3 Click the **New** icon.

4 In the **Name** attribute, enter: **`USA`**.

5 Click **Save and Close** to save this configuration.

Step 3: Create the Colorado Node Group Using Filters

To create the **Colorado** node group, use the Filter Editor to establish a filter to select the nodes.

When possible, use the **Additional Filters** tab rather than specifying a list of nodes using the **Additional Nodes** tab. Using a node group filter enables NNMi to automatically place a node into the correct node group as new nodes are added to the network.

1 Navigate to the **Configuration** workspace.

2 Select **Node Groups**.

3 Click the **New** icon.

4 In the **Name** attribute, enter: **`Colorado`**.

5 Select the **Additional Filters** tab.

6 Click **OR** to specify that you want NNMi to match a node if the node matches either of the hostname values you enter.

7 In the Filter Editor **Attribute** field, select `hostname`.

Selecting `hostname` specifies that NNMi should match hostname values when determining whether a node belongs to this node group.

8 In the **Operator** field, select `like`.

Selecting `like` enables you to use wildcard characters in the search.

9 In the **Value** field, enter a value that represents the devices you want the node group to contain. For example, **`cisco*.ntc.example.com`** represents devices named `cisco`*<replace with this text>.<network_domain>*.

10 Click **Append**.

11 In the **Attribute** field, select `hostname`.

12 In the **Operator** field, select `like`.

13 In the **Value** field, enter a wildcard that represents the remaining device names you want to add to the `Colorado` node group. For this example, use **`cisco?*`**.

14 Click **Append.**

15 Click **Save** to save the node group without closing the window.

Step 4: View the Node Group Members to Check the Node Group Filter Results

To test the node group filter, you can view the members of the node group you just created.

Select **Actions->Node Group Details->Show Members** to launch a view containing all of the nodes in the node group.

Examine the node group filter definition results until you are confident the node group filter is correct.

Step 5: Set Up the Node Group Hierarchy for the My Network Node Group

Establish a hierarchy for the node groups, starting with the top level node group, **My Network**.

1 Return to the **Node Groups** option in the **Configuration** workspace to view a list of the node groups you created.

2 Navigate to the **My Network** Node Group; then click **Open**.

3 Click the **Child Node Groups** tab.

4 Click the **New**. icon.

5 In the **Child Node Group** attribute, click the **Lookup** icon and select **Quick Find**.

Use **Quick Find** to select an object, such as a node group, when it already exists.

6 Select **USA** as the child node group.

7 Click **OK**.

8 Click **Save and Close** to save your changes and close the **Node Group Hierarchy** form.

9 Click **Save and Close** to save your changes and close the **Node Group** form.

Step 6: Establish the Node Group Hierarchy for the USA Node Group

Next, establish **Colorado** as a child node group of the **USA** node group. Repeat the same steps described in Step 5: Set Up the Node Group Hierarchy for the My Network Node Group to make the Colorado node group a child of the USA Node Group.

You are ready to create the node group maps for each node group that you created.

Configure the Node Group Maps

Step 1: Create the Node Group Maps

To create node group maps for each node group, use the **Actions** menu.

1 Open the node group for which you want to create a map:

   a Return to the **Node Groups** option in the **Configuration** workspace to view a list of the node groups you created.

   b Navigate to the node group you want and click the **Open** icon.

2 Select the **Actions->Maps-> Node Group Map** to display a node group map.

3 Position the nodes and node group map icons.

4 Click the **Save Layout** icon to create the node group map.

Always use **Save Layout** to create the node group map, even if you do not change the node positions. **Save Layout** creates the node group map.

A dialog box appears confirming you successfully created the node group map.

5 Click **OK**.

6 Repeat steps 1 through 5 for each node group you created.

Step 2: View the Node Group Maps

Now that you have created the node group maps, view the maps to check the contents.

1 Navigate to the **Topology Maps** workspace.

2 Select **Node Group Overview.**

3 Select the top level map: **My Network**.

4 Navigate to the child node group maps by double-clicking its icon.

5 Use the breadcrumb trail above the toolbar to return to the previous map.

Step 3: Configure Node Group Status

NNMi enables you to configure how status is calculated for a node group. When you configure node group status, you determine which of the following method NNMi should use:

- Use the most severe status of the nodes in the node group.
- Specify the percentage calculation NNMi should use.

Status Configuration is a global configuration. By default, NNMi uses the most severe status of the nodes in the node group.

1 Navigate to the **Configuration** workspace.

2 Select **Status Configuration**.

3 Examine the **Status Configuration** form to become familiar with the default percentages. To use percentages, you must deselect the **Propagate Most Severe Status** option, then save your changes.

Step 4: Configure Node Group Map Ordering

Node group map ordering is used to help determine in what order a map opens under the **Topology Maps** workspace.

In this example, use node group map ordering to specify that the **My Network** node group map should appear first in the list in the **Topology Maps** workspace.

1 Navigate to the **Configuration** workspace.

2 Select **User Interface > Node Group Map Settings**.

The

As shown in the following example, the default **Topology Maps Ordering** value is `50` for all user-defined maps.

To indicate that NNMi should list **My Network** as the first map under the **Topology Maps** workspace, change the **Topology Maps Ordering** value to a number that is less than the **Topology Maps Ordering** value for any other maps in the list; for example **5**.

3 Open the **My Network** Node Group map.

4 In the **Topology Maps Ordering** attribute, change the value to **5**.

5 Click **Save and Close** to save your changes and close the form.

You can also specify whether the map is initially displayed in the NNMi console. To do so, use the **User Interface Configuration** option from the **Configuration** workspace.

1 Navigate to the **Configuration** workspace.

2 Click **User Interface Configuration**.

3 In the **Initial View** attribute, use the drop-down menu to select **First Node Group in Topology Maps** workspace.

4 Click **Save and Close** to save your changes and close the form.

This will make the **My Network** map the initial view.

To verify the initial view, sign out of NNMi and sign back in. The **My Network** map should be the view you see in the NNMi console.

Step 5: Add a Background Image to a Node Group Map

To include a background graphic on a map, use the **Node Group Map Settings** form for the selected node group map.

1 Navigate to the **Configuration** workspace.

2 Click **User Interface > Node Group Map Settings**.

3 Open the **My Network** node group map.

4 Navigate to the **Background Image** tab.

5 Click **http://MACHINE:PORT/nnmdocs/images/.**

NNMi opens a list of HP supplied graphics.

6 Right-click the **world.png** link.

7 Select **Copy Link Location**.

8 Close the directory listing window.

Paste the copied link into the `Background Image` attribute.

Note the `Background Image Scale` value in case you want to change it later.

9 Click **Save and Close** to save your changes.

10 Navigate to the **Topology Maps** workspace and select **My Network** to view your new map with the background graphic.

Remove Node Groups

Suppose we want to remove a node group. Say, for example, we would like to delete the Colorado node group created earlier in this example.

Step 1: Navigate to the Node Group

1 In the **Configuration** workspace, click **Node Groups**.

2 Select the **Colorado** node group in the list and click the **Open** button.

Step 2: Delete the Node Group

1. Click the **Delete Node Group** button.
2. A dialog box appears, warning you that all contained objects and references will also be deleted by deleting the node group.
3. Click **OK** to delete the node group.

Disabling the Analysis Pane

NNMi permits you to disable the analysis pane from the NNMi console by performing the following steps:

1. Edit the following file:
   - *Windows*: `%NNM_PROPS%\nms-ui.properties`
   - *UNIX*: `$NNM_PROPS/nms-ui.properties`
2. Append the following text to the end of the file:

```
# Disables the analysis pane from being shown by default.

# The analysis pane can still be shown by toggling it open

# or using the "Show Analysis Pane" menu item.

#com.hp.nnm.ui.analysisPaneDisabled = true
```

3. Uncomment the property (the last line) to disable the analysis pane.
4. Save your changes.

Reducing the Maximum Number of Nodes Displayed in a Network Overview Map

The **Network Overview** map opens a map containing up to 250 of the most highly connected nodes in the layer 3 network. If this map contains too many nodes, the map might respond slowly when moving nodes or become too complex for practical viewing. You can increase or reduce the maximum number of nodes displayed in the **Network Overview** map as shown in the following example.

Suppose you want to change the maximum number of nodes displayed in the **Network Overview** map from 250 to 100. To do this, follow these steps:

1. Edit the following file:
   - *Windows*: `%NNM_PROPS%\nms-ui.properties`
   - *UNIX*: `$NNM_PROPS/nms-ui.properties`
2. Look for text similar to following line:

```
#!com.hp.nnm.ui.networkOverviewMaxNodes = 250
```

Change the line as follows:

```
com.hp.nnm.ui.networkOverviewMaxNodes = 100
```

➤ Make sure to remove the **#!** characters located at the beginning of the line.

3 Save your changes.

Reducing the Number of Displayed Nodes on a Node Group Map

If you configure a node group map to contain hundreds of nodes, the map showing the node group might show many small node icons instead of the detailed node icons you expect. To view the map with better detail, you would need to use the zoom feature. Using the zoom feature might slow the NNMi console performance when displaying maps.

The remedy is to limit the number of displayed nodes, displayed end points, or both, by doing the following:

1 In the NNMi console, click **Configuration**.

2 Click **User Interface Configuration** located beneath **User Interface**.

3 Select the **Default Map Settings** tab.

4 Modify the value shown in the `Maximum Number of Displayed Nodes` field.

5 Modify the value shown in the `Maximum Number of Displayed End Points` field.

6 Click **Save and Close**.

See *Define Default Map Settings* in the NNMi help for more information.

Setting the Maximum Number of Gauges in the Analysis Pane

The Gauges tab in the Analysis Pane shows real-time SNMP gauges that display State Poller and Custom Poller SNMP data. These gauges display data for nodes, interfaces, custom node collections, custom node instances, and for node components of type CPU, Memory, Buffers, or Backplane.

Set the maximum number of gauges to be displayed in the Analysis Pane as follows:

1 Edit the following file:

- *Windows*: `%NNM_PROPS%\nms-ui.properties`
- *UNIX*: `$NNM_PROPS/nms-ui.properties`

2 Look for text similar to following line:

```
#!com.hp.nnm.ui.maxGaugePerAnalysisPanel = 24
```

Change the line as follows:

```
com.hp.nnm.ui.maxGaugePerAnalysisPanel = 12
```

➤ Make sure to remove the **#!** characters located at the beginning of the line.

3 Save your changes.

A higher number of gauges affects performance when the Analysis Pane opens. A fewer number of gauges results in larger size gauges.

Setting the Refresh Rate for Gauges in the Analysis Pane

Set the refresh interval (in seconds) for gauges displayed in the Analysis Pane as follows:

1 Edit the following file:

- *Windows*: `%NNM_PROPS%\nms-ui.properties`
- *UNIX*: `$NNM_PROPS/nms-ui.properties`

2 Look for text similar to following line:

```
#!com.hp.nnm.ui.analysisGaugeRefreshSecs = 15
```

Change the line as follows:

```
com.hp.nnm.ui.analysisGaugeRefreshSecs = 10
```

Make sure to remove the **#!** characters located at the beginning of the line.

3 Save your changes.

Setting the value to “0” results in gauges never refreshing. A refresh rate faster than 10 seconds causes some SNMP agents to cache their values for short periods of time, causing repeated results.

Advanced Configuration

This section contains the following chapters:

Licensing NNMi

If you do not have a permanent license key installed, the NNMi product includes a temporary Instant-On license key that is valid for 60 days after you install NNMi. This temporary Instant-On license key enables you to use NNMi Advanced features. You should obtain and install a permanent license key as soon as possible.

To view a list of the features included with an NNMi Advanced license, see the licensing section of the *HP NNMi Software Release Notes*.

Preparing to Install a Permanent License Key

The temporary Instant-On license has a 250 node limit. If you have been running NNMi with the Instant-On license key, you might be managing more nodes than your permanent license supports. When the permanent license takes effect, NNMi automatically unmanages nodes of its choosing to achieve the license limit.

If you want to control which nodes are no longer managed with the permanent license, use the NNMi console to delete less important nodes before installing your new license key.

Checking the License Type and the Number of Managed Nodes

To determine the type of license that NNMi is using, follow these steps:

1. In the NNMi console, click **Help > About Network Node Manager.**
2. In the **About Network Node Manager** window, click **View Licensing Information**.

   (**View Licensing Information** is also available on the NNMi console sign-in page.)
3. Look for the value shown in the **Consumption** field. This is the number of nodes that NNMi is currently managing.
4. If your permanent license supports fewer nodes than NNMi is currently managing, use the NNMi console to delete less important nodes. For more information, see *Delete a Node* in the NNMi help.

Obtaining and Installing a Permanent License Key

To request a permanent license key, gather the following information:

- The Entitlement Certificate, which contains the HP product number and order number
- The IP address of one of the NNMi management servers
- If the license is for NNMi running under HA, the virtual IP address of the NNMi HA resource group
- Your company or organization information

Using Autopass and your HP Order Number (not possible behind a firewall)

To obtain and install a permanent license key, follow these steps:

1. At a command prompt, enter the following command to open the Autopass user interface:

   ```
   nnmlicense.ovpl NNM -gui
   ```

2. On the left side of the Autopass window, click **License Management**.
3. Click **Install License Key**.
4. Click **Retrieve/Install License Key**.
5. Enter your HP Order Number and follow the Autopass prompts to complete the license key retrieval process.
6. NNMi automatically completes the installation.

From the Command Line

If the automated process does not run to completion (for example, if the NNMi management server is behind a firewall), follow these steps:

1. To obtain a license key, go to the HP password delivery service at

   https://webware.hp.com/welcome.asp

2. At a command prompt on the NNMi management server, enter the following command to update the system and to store license data files:

   ```
   nnmlicense.ovpl NNM -f license_file
   ```

   (The product license ID (NNM) is case-sensitive.)

   See the *nnmlicense.ovpl* reference page, or the UNIX manpage, for more information.

3. NNMi automatically completes the installation.

Obtaining Additional License Keys

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

See *Extend a Licensed Capacity* in the NNMi help for more information.

Note to Developers: With the NNMi Developer Toolkit, you can enhance the capabilities of NNMi by integrating custom web-service clients. After you install an NNMi Developer license, NNMi creates the `sdk-dev-kit.jar` file located in the `doc` folder. Unpack the `sdk-dev-kit.jar` file to view the NNMi Developer Toolkit documentation and samples.

Working with Certificates for NNMi

A certificate identifies the web server to the browser. This certificate can be self-signed or signed by a CA (Certificate Authority). The `nnm.keystore` file stores private keys and certificates with their corresponding public keys. The `nnm.truststore` file contains certificates from other parties that you expect to communicate with, or from Certificate Authorities that you trust to identify other parties. NNMi includes a self-signed certificate in both of the `nnm.keystore` and `nnm.truststore` files.

To use certain NNMi features, NNMi management servers need to share their certificates with one another. This chapter contains configuration instructions for copying these certificates among NNMi management servers and using the `nnmcertmerge.ovpl` script to merge these certificates into the `nnm.keystore` and `nnm.truststore` files.

This chapter contains the following topics:

- Putting it All Together
- Generating a Certificate Authority Certificate
- Configuring Application Failover to use Self-Signed Certificates
- Configuring Application Failover to use a Certificate Authority
- Configuring High Availability to use Self-Signed or Certificate Authority Certificates
- Configuring the Global Network Management Feature to use Self-Signed Certificates
- Configuring the Global Network Management Feature to use a Certificate Authority
- Configuring Global Network Management with Application Failover to use Self-Signed Certificates
- Configuring an SSL Connection to the Directory Service
- Configuring an SSL Connection to HP BSM Version 9.xx

Putting it All Together

Use the following information to guide you in configuring certificates for your special needs:

- If you are using CA certificates, follow the instructions shown in Generating a Certificate Authority Certificate on page 123.
- If you configured your global, regional, or both NNMi management servers to use the application failover feature there are some additional configuration steps. Merge the NNMi management servers' `nnm.keystore` and `nnm.truststore` files for each cluster before completing the global network management configuration, as described in the Configuring Application Failover to use Self-Signed Certificates on page 126.
- If you must use a Certificate Authority, and you configured your global, regional, or both NNMi management servers to use the application failover feature, there are some additional configuration steps. First, follow the instructions shown in Generating a Certificate Authority Certificate on page 123; then merge the NNMi management servers' `nnm.keystore` and `nnm.truststore` files for each cluster before completing the global network management configuration, as described in the Configuring Application Failover to use a Certificate Authority on page 128.
- If you configured your global, regional, or both NNMi management servers to use High Availability, create the self-signed certificate in the `nnm.keystore` and `nnm.truststore` files for the virtual hostname before completing the global network management configuration, as described in Configuring High Availability to use Self-Signed or Certificate Authority Certificates on page 130.
- After you have each HA or application failover cluster properly configured, enable the global network management feature by copying the `nnm.truststore` file from the active regional node to the active global node, then merging the truststore. You must do this for each active regional node. Review the information shown in Configuring Global Network Management with Application Failover to use Self-Signed Certificates on page 133. If the NNMi management servers use CA certificates generated using the procedure shown in Generating a Certificate Authority Certificate on page 123, then those CA certificates are the only certificates you must merge into the global truststore.
- If you configure your NNMi management servers in a global network management configuration, then decide later to change the regional, global, or both to be in an application failover cluster, follow the instructions shown in Configuring Application Failover to use Self-Signed Certificates on page 126. Use the commands shown in that section to configure your `nnm.keystore` and `nnm.truststore` files correctly; then copy the modified `nnm.truststore` file to the global NNMi management server and merge it into its `nnm.truststore` file.
- If you configure your NNMi management servers in a global network management configuration, then decide later to change the regional, global, or both to use HA, follow the instructions shown in Configuring High Availability to use Self-Signed or Certificate Authority Certificates on page 130.
- After directory service communications are enabled, NNMi uses the LDAP protocol for retrieving data from a directory service. If the directory service requires an SSL connection, follow the instructions show in Configuring an SSL Connection to the Directory Service on page 134.

Generating a Certificate Authority Certificate

If you plan to use a CA (Certificate Authority), complete the following steps to generate a CA certificate.

If you plan to use a CA with NNMi, sign the certificate using the RSA algorithm. The DSA algorithm is not supported.

1 Change to the directory on the NNMi management server that contains the `nnm.keystore` and `nnm.truststore` files:

- *Windows*:`%NNM_DATA%\shared\nnm\certificates`
- *UNIX*: `$NNM_DATA/shared/nnm/certificates`

2 Save a backup copy of the `nnm.keystore` file.

3 Generate a private key from your system. Use the *keytool* command to generate this private key:

a Run the following command *exactly as shown*:

— *Windows*: **`%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool.exe -genkeypair -validity 3650 -keyalg rsa -keystore nnm.keystore -storepass nnmkeypass -alias`** ***`myserver.mydomain`***

— *UNIX*: **`$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -genkeypair -validity 3650 -keyalg rsa -keystore nnm.keystore -storepass nnmkeypass -alias`** ***`myserver.mydomain`***

The alias, referred to as *myserver.mydomain* in this example, identifies this newly-created key. Although the alias can be any string, HP recommends you use the fully-qualified domain name of your system for the *myserver.mydomain* alias variable.

Linux operating systems have a keytool command that is not compatible with the keytool command or command options used in this step.

b Enter the requested information.

Important: When prompted for your first and last name, enter the FQDN (fully-qualified domain name) of your system.

4 Run the following command *exactly as shown* to create a CSR (Certificate Signing Request) file:

— *Windows*:**`%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool.exe -keystore nnm.keystore -certreq -storepass nnmkeypass -alias`** ***`myserver.mydomain`*** **`-file CERTREQFILE`**

— *UNIX*: **`$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -keystore nnm.keystore -certreq -storepass nnmkeypass -alias`** ***`myserver.mydomain`*** **`-file CERTREQFILE`**

For more information about the `keytool` command, search for “Key and Certificate Management Tool” at **http://www.oracle.com/technetwork/java/index.html**.

5 Send the CSR to your CA signing authority. They should provide you with one of the following:

- A signed certificate, referred to as `myserver.crt`. The `myserver.crt` file contains both the server certificate (the top certificate contained in the file) and one or more CA (Certified Authority) certificates (the last certificates contained in the file). Copy the CA certificate into a new file, the `myca.crt` file. Use the `myserver.crt` file when importing the server certificate into the `nnm.keystore` file and the `myca.crt` file when importing the CA certificate into the `nnm.truststore` file.
- Two files, referred to `myserver.crt` and `CA.crt` in this procedure. Add the `CA.crt` file content to the end of the `myserver.crt` file. Use the `myserver.crt` file when importing the server certificate into the `nnm.keystore` file and the `myca.crt` file when importing the CA certificate into the `nnm.truststore` file.

The following examples show you what the files you receive from your CA signing authority might look like:

Separate server and CA certificate files:

```
-----BEGIN CERTIFICATE-----
Sample/AVQQKExNQU0EgQ29ycG9yYXRpb24gTHRkMRAwDgYDVQQLEwdOZXR3b3Js
eGVSZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlw
................................................................
................................................................
TZImiZPyLGQBGRYDaW50MRIwEAYKCZImiZPyLGQBGRYCc2cxEzARBgNVBAMTCmNb
pSo6o/76yShtT7Vrlfz+mXjWyEHaIy/QLCpPebYhejHEg4dZgzWWT/lQt==
-----END CERTIFICATE-----
```

Combined server and CA certificates in one file:

```
-----BEGIN CERTIFICATE-----
Sample1/VQQKExNQU0EgQ29ycG9yYXRpb24gTHRkMRAwDgYDVQQLEwdOZXR3b3Js
eGVSZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlw
................................................................
................................................................
TZImiZPyLGQBGRYDaW50MRIwEAYKCZImiZPyLGQBGRYCc2cxEzARBgNVBAMTCmNb
pSo6o/76yShtT7Vrlfz+mXjWyEHaIy/QLCpPebYhejHEg4dZgzWWT/lQt==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Sample2/Gh0dHA6Ly9jb3JwMWRjc2cyLnNnLmludC5wc2FnbG9iYWwuY29tL0Nlc
RaOCApwwggKYMB0GA1UdDgQWBBSqaWZzCRcpvJWOFPZ/Be9b+QSPyDAfBgNVHSMC
................................................................
................................................................
Wp5Lz1ZJAOu1VHbPVdQnXnlBkx7V65niLoaT90Eqd6laliVlJHj7GBriJ90uvVGu
BQagggEChoG9bGRhcDovLy9DTj1jb3JwMWRjc2cyL==
-----END CERTIFICATE-----
```

6 Copy the files containing these certificates to a location on the NNMi management server. For this example, copy the files to the following location:

- *Windows*: `%NNM_DATA%\shared\nnm\certificates`
- *UNIX*: `$NNM_DATA/shared/nnm/certificates`

Use the certificates you generated in the previous steps to replace the self-signed certificate:

1 Change to the directory on the NNMi management server that contains the `nnm.keystore` and `nnm.truststore` files:

- *Windows*:`%NNM_DATA%\shared\nnm\certificates`
- *UNIX*: `$NNM_DATA/shared/nnm/certificates`

2 Run the following command to import the server certificate and the CA certificate into the NNMi `nnm.keystore` file:

Windows:

- **`%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool.exe -importcert -trustcacerts -keystore nnm.keystore -storepass nnmkeypass -alias`** *myserver.mydomain* **`-file myserver.crt`**

UNIX:

- **`$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -importcert -trustcacerts -keystore nnm.keystore -storepass nnmkeypass -alias`** *myserver.mydomain* **`-file myserver.crt`**

If you use the **`-storepass`** option and provide the password, the keystore program does not prompt you for the keystore password. If you do not use the **`-storepass`** option, enter **`nnmkeypass`** when prompted for the keystore password.

3 When prompted to trust the certificate, enter: **`y`**

Example output for importing a certificate into the keystore

The output from this command is of the form:

```
Owner: CN=NNMi_server.example.com
Issuer: CN=NNMi_server.example.com
Serial number: 494440748e5
Valid from: Tue Oct 28 10:16:21 MST 2008 until: Thu Oct 04
11:16:21 MDT 2108
Certificate fingerprints:
MD5:  29:02:D7:D7:D7:D7:29:02:29:02:29:02:29:02:29:02
SHA1: C4:03:7E:C4:03:7E:C4:03:7E:C4:03:7E:C4:03:7E:C4:03
Trust this certificate? [no]:  y
Certificate was added to keystore
```

4 Run the following commands to import the CA certificate into the NNMi `nnm.truststore` file:

— *Windows*:

`%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool.exe -import -alias` ***myca*** **`-keystore nnm.truststore -file myca.crt`**

— *UNIX*:

`$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -import -alias` ***myca*** **`-keystore nnm.truststore -file myca.crt`**

5 When prompted for the truststore password, enter: **`ovpass`**.

6 Examine the contents of the trust store:

- *Windows*:
  `%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool -list \`
  `-keystore nnm.truststore`
- *UNIX*:
  `$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -list \`
  `-keystore nnm.truststore`

When prompted for the truststore password, enter: **`ovpass`**

Example trust store output

The trust store output is of the form:

```
Keystore type: jks
Keystore provider: SUN
Your keystore contains 1 entry
nnmi_ldap, Nov 14, 2008, trustedCertEntry,
Certificate fingerprint (MD5):
29:02:D7:D7:D7:D7:29:02:29:02:29:02:29:02:29:02
```

The trust store can include multiple certificates.

7 Edit the following file:

- *Windows*: `%NNM_CONF%\nnm\props\nms-local.properties`
- *UNIX*: `$NNM_CONF/nnm/props/nms-local.properties`

8 Update the `com.hp.ov.nms.ssl.KEY_ALIAS` variable to the value you used for *myserver.mydomain*. Make sure to save your work.

9 Restart NNMi by running these commands:

a **`ovstop`**

b **`ovstart`**

10 Test HTTPS access to the NNMi console using the following syntax: **https://<fully_qualified_domain_name>:<port_number>/nnm/.** If the browser trusts the CA, it will trust the HTTPS connection to the NNMi console.

Configuring Application Failover to use Self-Signed Certificates

Figure 2 Using Self-Signed Certificates with Application Failover

Active NNMi Management Server (Server X)
Standby NNMi Management Server (Server Y)

When configuring the application failover feature, you must merge the `nnm.keystore` *and* `nnm.truststore` *file content for both nodes into a single* `nnm.keystore` *and* `nnm.truststore` *file. Complete the following steps to configure the application failover feature to use self-signed certificates based on the above diagram.*

If you are using self-signed certificates with NNMi along with the application failover feature, and do not complete the following steps, NNMi processes will not start correctly on the standby NNMi management server (`Server Y` in this example).

1 Change to the following directory on `Server Y` before completing step 2:

- *Windows*:`%NNM_DATA%\shared\nnm\certificates`
- *UNIX*: `$NNM_DATA/shared/nnm/certificates`

2 Copy the `nnm.keystore` and `nnm.truststore` files from `Server Y` to some temporary location on `Server X`. The remaining steps refer to these file locations as <*keystore*> and <*truststore*>.

3 Run the following command on `Server X` to merge `Server Y`'s certificates into `Server X`'s `nnm.keystore` and `nnm.truststore` files.

Windows:

```
nnmcertmerge.ovpl -keystore <keystore> -truststore
<truststore>
```

UNIX:

```
nnmcertmerge.ovpl -keystore <keystore> -truststore
<truststore>
```

4 Copy the merged `nnm.keystore` and `nnm.truststore` files from `server X` to `server Y`, so that both nodes have the merged files. The location of these files is as follows:

- *Windows*:`%NNM_DATA%\shared\nnm\certificates`
- *UNIX*: `$NNM_DATA/shared/nnm/certificates`

5 Run the following command on both `Server X` and `Server Y`. Verify that the displayed results from both servers, including the fully-qualified-domain names, match. If they do not match do not continue, rather redo step 1 through step 7.

Windows:

```
%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool.exe -list
-keystore %NnmDataDir%\shared\nnm\certificates\nnm.keystore
-storepass nnmkeypass
```

UNIX:

```
$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -list -keystore
$NnmDataDir/shared/nnm/certificates/nnm.keystore -storepass
nnmkeypass
```

6 Run the following command on both `Server X` and `Server Y`. Verify that the displayed results from both servers, including the fully-qualified-domain names, match. If they do not match do not continue, rather redo step 1 through step 7.

Windows:

```
%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool.exe -list
-keystore
%NnmDataDir%\shared\nnm\certificates\nnm.truststore
-storepass ovpass
```

UNIX:

```
$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -list -keystore
$NnmDataDir/shared/nnm/certificates/nnm.truststore
-storepass ovpass
```

7 Continue configuring the application failover feature at step 6 on page 277 .

➤ Although you manually completed the following automatic action during step 4, after you start the application failover feature, NNMi automatically replicates the merged keystore and truststore information from NNMi_active to NNM_standby.

Configuring Application Failover to use a Certificate Authority

Figure 3 Using CA Certificates with Application Failover

Active
NNMi
Management
Server
(Server X)
Standby
NNMi
Management
Server
(Server Y)

When configuring the application failover feature, you must merge the `nnm.keystore` *and* `nnm.truststore` *file content for both nodes into a single* `nnm.keystore` *and* `nnm.truststore` *file.* Complete the following steps to configure the application failover feature to use CA certificates based on the above diagram.

⚠ If you are using CA certificates with NNMi along with the application failover feature, and do not complete the following steps, NNMi processes will not start correctly on the standby NNMi management server (`Server Y` in this example).

1 Follow the instructions shown in Generating a Certificate Authority Certificate on page 123 for NNMi_standby.

2 Change to the following directory on `Server Y` before completing step 3:

- *Windows*:`%NNM_DATA%\shared\nnm\certificates`
- *UNIX*: `$NNM_DATA/shared/nnm/certificates`

3 Copy the `nnm.keystore` and `nnm.truststore` files from `Server Y` to some temporary location on `Server X`. The remaining steps refer to these file locations as <*keystore*> and <*truststore*>.

4 Run the following command on `Server X` to merge `Server Y`'s certificates into `Server X`'s `nnm.keystore` and `nnm.truststore` files.

Windows:

```
nnmcertmerge.ovpl -keystore <keystore> -truststore
<truststore>
```

UNIX:

```
nnmcertmerge.ovpl -keystore <keystore> -truststore
<truststore>
```

5 Copy the merged `nnm.keystore` and `nnm.truststore` files from `server X` to `server Y`, so that both nodes have the merged files. The location of these files is as follows:

- *Windows*:`%NNM_DATA%\shared\nnm\certificates`
- *UNIX*: `$NNM_DATA/shared/nnm/certificates`

6 Run the following command on both `Server X` and `Server Y`. Verify that the displayed results from both servers, including the `hp.com` fully-qualified-domain name, match. If they do not match do not continue, rather redo step 1 through step 7.

Windows:

```
%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool.exe -list
-keystore %NnmDataDir%\shared\nnm\certificates\nnm.keystore
-storepass nnmkeypass
```

UNIX:

```
$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -list -keystore
$NnmDataDir/shared/nnm/certificates/nnm.keystore -storepass
nnmkeypass
```

7 Run the following command on both `Server X` and `Server Y`. Verify that the displayed results from both servers, including the `hp.com` fully-qualified-domain name, match. If they do not match do not continue, rather redo step 1 through step 7.

Windows:

```
%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool.exe -list
-keystore
%NnmDataDir%\shared\nnm\certificates\nnm.truststore
-storepass ovpass
```

UNIX:

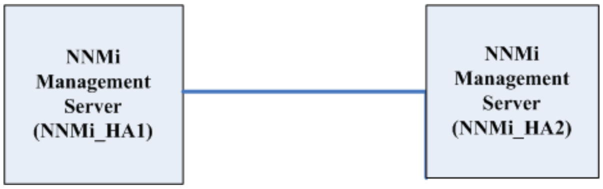
```
$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -list -keystore
$NnmDataDir/shared/nnm/certificates/nnm.truststore
-storepass ovpass
```

8 Continue configuring the application failover feature at step 6 on page 277 .

➤ Although you manually completed the following automatic action during step 5 on page 129, after you start the application failover feature, NNMi automatically replicates the merged keystore and truststore information from Server X to Server Y

Configuring High Availability to use Self-Signed or Certificate Authority Certificates

Figure 4 Using Certificates with HA


NNMi Management Server (NNMi_HA1)
NNMi Management Server (NNMi_HA2)

Configuring High Availability to use Self-Signed Certificates

The process for configuring NNMi for HA correctly shares the self-signed certificate among the primary and secondary cluster nodes. You do not need to take any extra steps to use the default certificate with NNMi running under HA.

Configuring High Availability for a New Certificate

Suppose you create a new self-signed or CA certificate, referred to as `newcert`. Complete the following steps to configure HA with this new CA or self-signed certificate.

You can complete this procedure before or after configuring NNMi for HA, as described in Configuring HA on page 309.

1 Change to the following directory on `NNMi_HA1` before completing step 2:

- *Windows*:`%NNM_DATA%\shared\nnm\certificates`
- *UNIX*: `$NNM_DATA/shared/nnm/certificates`

2 On `NNMi_HA1`, run the following commands to import `newcert` into the `nnm.keystore` file:

- *Windows*: **`%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool -import -alias newcert_Alias -keystore nnm.keystore -file newcert`**
- *UNIX*: **`$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -import -alias newcert_Alias -keystore nnm.keystore -file newcert`**

3 Edit the following file on both the active `(NNMi_HA1)` and the standby `(NNMi_HA2)` `nodes:`

- *Windows*: `%NNM_DATA%\conf\nnm\props\nms-local.properties`
- *UNIX*: `$NNM_DATA/conf/nnm/props/nms-local.properties`

4 Change the following line in the `nms-local.properties` file on both `NNMi_HA1` and `NNMi_HA2`.

```
com.hp.ov.nms.ssl.KEY_ALIAS = newcert_Alias
```

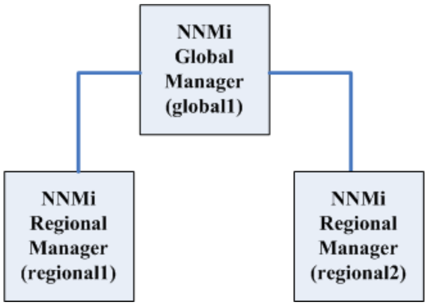
5 Save your changes.

Configuring the Global Network Management Feature to use Self-Signed Certificates

During NNMi installation, the installation script creates a self-signed certificate for the NNMi management server. This certificate contains an alias that includes the fully-qualified domain name of the node. The installation script adds this self-signed certificate to the NNMi management server's `nnm.keystore` and `nnm.truststore` files.

Suppose you want your global network management configuration to model Figure 5.

Figure 5 Global Network Management


NNMi Global Manager (global1)
NNMi Regional Manager (regional1)
NNMi Regional Manager (regional2)

Complete the following steps to configure the global network management feature to use self-signed certificates based on Figure 5.

1 Change to the following directory on `regional1` and `regional2` before completing step 2:

- *Windows*:`%NNM_DATA%\shared\nnm\certificates`
- *UNIX*: `$NNM_DATA/shared/nnm/certificates`

2 Copy the `nnm.truststore` files from the above locations on `regional1` and `regional2` to some temporary location on `global1`.

3 Run the following command on `global1` to merge the `regional1` and `regional2` certificates into `global1`'s `nnm.truststore` file.

Windows:

a **`nnmcertmerge.ovpl -truststore`** ***`regional1_nnm.truststore_location`***

b **`nnmcertmerge.ovpl -truststore`** ***`regional2_nnm.truststore_location`***

UNIX

a **`nnmcertmerge.ovpl -truststore`** ***`regional1_nnm.truststore_location`***

b **`nnmcertmerge.ovpl -truststore`** ***`regional2_nnm.truststore_location`***

4 Run the following command sequence on `global1`:

a **`ovstop`**

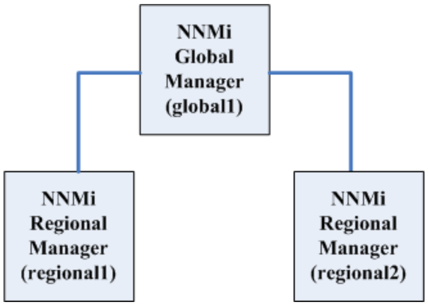
b **`ovstart`**

Configuring the Global Network Management Feature to use a Certificate Authority

During NNMi installation, the installation script creates a self-signed certificate for the NNMi management server. This certificate contains an alias that includes the fully-qualified domain name of the node. The installation script adds this self-signed certificate to the NNMi management server's `nnm.keystore` and `nnm.truststore` files.

Suppose you want your global network management configuration to model Figure 6.

Figure 6 Using Certificates with Global Network Management


NNMi Global Manager (global1)
NNMi Regional Manager (regional1)
NNMi Regional Manager (regional2)

1 Follow the instructions shown in Generating a Certificate Authority Certificate on page 123 for `regional1` and `regional2`.

2 Change to the following directory on `regional1` and `regional2` before completing step 3.

- *Windows*:`%NNM_DATA%\shared\nnm\certificates`
- *UNIX*: `$NNM_DATA/shared/nnm/certificates`

3 Copy the `nnm.truststore` files from the above locations on `regional1` and `regional2` to some temporary location on `global1`.

4 Run the following command on `global1` to merge the `regional1` and `regional2` certificates into `global1`'s `nnm.truststore` file.

Windows:

a **`nnmcertmerge.ovpl -truststore`** ***`regional1_nnm.truststore_location`***

b **`nnmcertmerge.ovpl -truststore`** ***`regional2_nnm.truststore_location`***

UNIX

a **`nnmcertmerge.ovpl -truststore`** ***`regional1_nnm.truststore_location`***

b **`nnmcertmerge.ovpl -truststore`** ***`regional2_nnm.truststore_location`***

5 Run the following command sequence on `global1`:

a **`ovstop`**

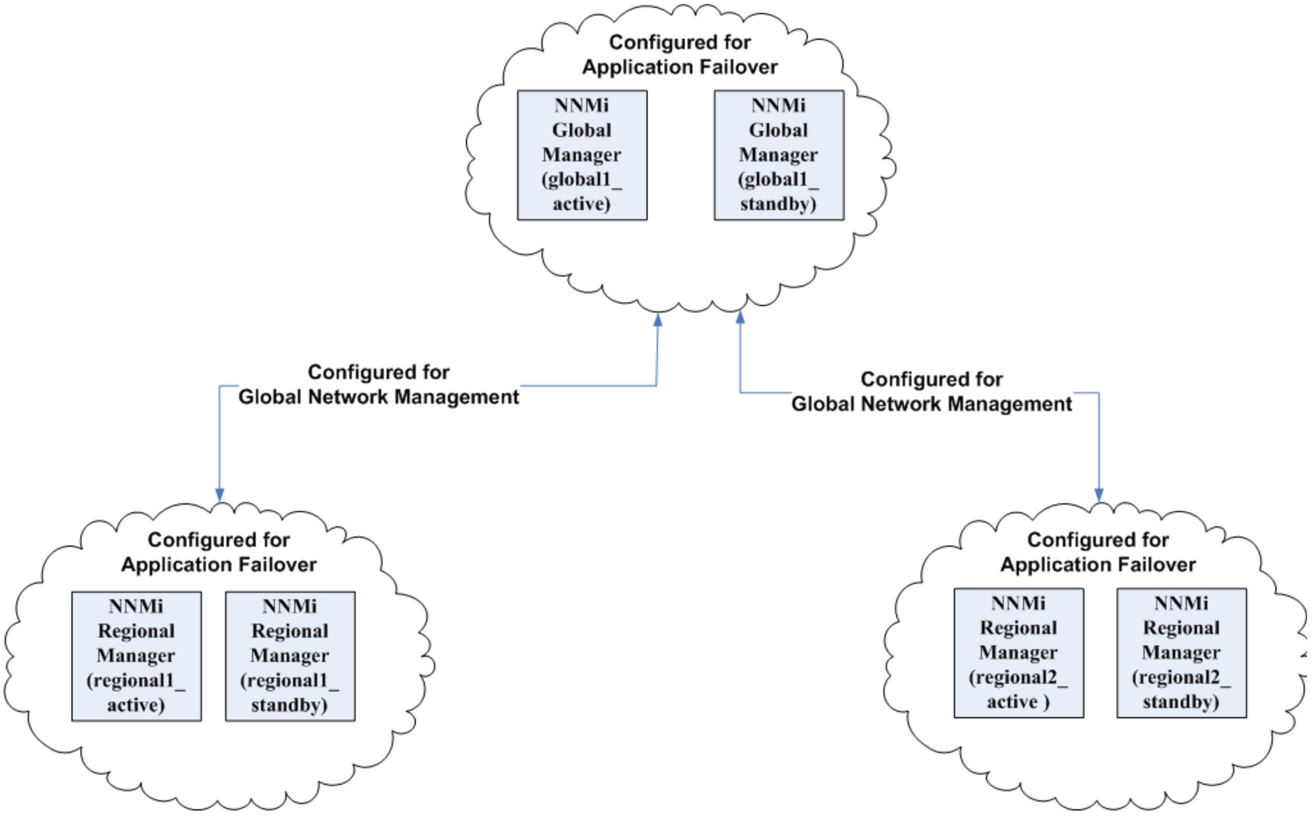
b **`ovstart`**

Configuring Global Network Management with Application Failover to use Self-Signed Certificates

As discussed above, during NNMi installation the installation script creates a self-signed certificate for the NNMi management server. This certificate contains an alias that includes the fully-qualified domain name of the node. The installation script adds this self-signed certificate to the NNMi management server's `nnm.keystore` and `nnm.truststore` files.

Suppose you want your global network management configuration to model the application failover feature as shown in Figure 7.

Figure 7 Global Network Management with Application Failover


Configured for Application Failover
NNMi Global Manager (global1_ active)
NNMi Global Manager (global1_ standby)
Configured for Global Network Management
Configured for Global Network Management
Configured for Application Failover
NNMi Regional Manager (regional1_ active)
NNMi Regional Manager (regional1_ standby)
Configured for Application Failover
NNMi Regional Manager (regional2_ active)
NNMi Regional Manager (regional2_ standby)

Complete the following steps to configure the global network management feature to work with application failover based on the above diagram:

1 Follow the instructions shown in Configuring Application Failover to use Self-Signed Certificates on page 126 for each application failover cluster shown in the above diagram.

2 Complete the configuration for application failover shown in Application Failover Basic Setup on page 274.

3 Follow the instructions shown in Configuring the Global Network Management Feature to use Self-Signed Certificates on page 131 for `regional1_active and regional2_active`.

Configuring an SSL Connection to the Directory Service

By default, when directory service communications are enabled, NNMi uses the LDAP protocol for retrieving data from a directory service. If your directory service requires an SSL connection, you must enable the SSL protocol to encrypt the data that flows between NNMi and the directory service.

SSL requires a trust relationship between the directory service host and the NNMi management server. To create this trust relationship, add a certificate to the NNMi trust store. The certificate confirms the identity of the directory service host to the NNMi management server.

To install a trust store certificate for SSL communications, follow these steps:

1. Obtain your company's trust store certificate from the directory server. The directory service administrator should be able to give you a copy of this text file.

2. Change to the directory that contains the NNMi trust store:
   - *Windows*: `%NNM_DATA%\shared\nnm\certificates`
   - *UNIX*: `$NNM_DATA/shared/nnm/certificates`

   Run all commands in this procedure from the `certificates` directory.

3. Import your company's trust store certificate into the NNMi trust store:
   a. Run the following command:
      - *Windows*:
        ```
        %NnmInstallDir%\nonOV\jdk\b\bin\keytool -import
        -alias nnmi_ldap -keystore nnm.truststore
        -file <Directory_Server_Certificate.txt>
        ```
      - *UNIX*:
        ```
        $NnmInstallDir/nonOV/jdk/b/bin/keytool -import \
        -alias nnmi_ldap -keystore nnm.truststore \
        -file <Directory_Server_Certificate.txt>
        ```

      Where *`<Directory_Server_Certificate.txt>`* is your company's trust store certificate.

   b. When prompted for the keystore password, enter: **`ovpass`**

   c. When prompted to trust the certificate, enter: **`y`**

      Example output for importing a certificate into the trust store

      The output from this command is of the form:

      ```
      Owner: CN=NNMi_server.example.com
      Issuer: CN=NNMi_server.example.com
      Serial number: 494440748e5
      Valid from: Tue Oct 28 10:16:21 MST 2008 until: Thu Oct 04
      11:16:21 MDT 2108
      Certificate fingerprints:
      MD5:  29:02:D7:D7:D7:D7:29:02:29:02:29:02:29:02:29:02
      SHA1: C4:03:7E:C4:03:7E:C4:03:7E:C4:03:7E:C4:03:7E:C4:03
      Trust this certificate? [no]:  y
      Certificate was added to keystore
      ```

4 Examine the contents of the trust store:

- *Windows*:
  %NnmInstallDir%\nonOV\jdk\b\bin\keytool.exe -list -keystore nnm.truststore
- *UNIX*:
  $NnmInstallDir/nonOV/jdk/b/bin/keytool -list -keystore nnm.truststore

When prompted for the keystore password, enter: **ovpass**

Example trust store output

The trust store output is of the form:

```
Keystore type: jks
Keystore provider: SUN
Your keystore contains 1 entry
nnmi_ldap, Nov 14, 2008, trustedCertEntry,
Certificate fingerprint (MD5):
29:02:D7:D7:D7:D7:29:02:29:02:29:02:29:02:29:02
```

The trust store can include multiple certificates.

5 Restart NNMi by running these commands:

a **ovstop**

b **ovstart**

For more information about the `keytool` command, search for “Key and Certificate Management Tool” at **http://www.oracle.com/technetwork/java/index.html**.

Configuring an SSL Connection to HP BSM Version 9.xx

To configure an SSL connection to HP BSM, follow these steps:

1 Export the NNMi certificates from the `nnm.keystore` file using the following command:

- *Windows*:
  %NnmInstallDir%\nonOV\jdk\b\bin\keytool.exe -export -alias *hostname*.selfsigned -file C:\temp\cert -keystore %NnmDataDir%\shared\nnm\certificates\nnm.keystore -storepass nnmkeypass
- *UNIX*:
  $NnmInstallDir/nonOV/jdk/b/bin/keytool -export -alias *hostname*.selfsigned -file /tmp/cert -keystore $NnmDataDir/shared/nnm/certificates/nnm.keystore -storepass nnmkeypass

2 Verify that you see the `Certificate stored in file <directory>:\cert` message.

3 Copy the certificate from the `cert` file you created in step 1 to the BSM server.

4 Open a command window on the BSM server.

5 Change directories using the **cd C:\HPBSM\JRE64\bin** command.

6. Run the following command: **keytool.exe -import -keystore *<directory>*:\HPBSM\odb\conf\security\server.keystore -storepass hppass -trustcacerts -file *<directory>*\cert**.

   Make sure you answer `yes` when asked whether to `Trust this certificate?`. The following program listing is an example of what happens after you run this command.

```
Owner: CN=hpbsm_server.example.com
Issuer: CN=hpbsm_server.example.com
Serial number: 4d525d0e
      Valid from: Wed Feb 09 11:23:26 EET 2011 until: Fri Jan 16
11:23:26 EET 2111
Certificate fingerprints:
         MD5:  C2:45:E9:73:07:B3:A8:84:AF:5F:B5:FA:41:D0:AE:D2
         SHA1:
42:84:B1:A8:45:3E:8A:9E:62:3C:7F:A4:76:78:44:C2:35:F3:50:4B
         Signature algorithm name: SHA1withRSA
         Version: 1
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

7. Run the command shown in step 6, substituting `server.truststore` for `server.keystore`: **keytool.exe -import -keystore *<directory>*:\HPBSM\odb\conf\security\server.truststore -storepass hppass -trustcacerts -file *<directory>*:\cert**.

   Make sure you answer `yes` when asked whether to `Trust this certificate?`.The following program listing is an example of what happens after you run this command.

```
Owner: CN=hpbsm_server.example.com
Issuer: CN=hpbsm_server.example.com
Serial number: 4d525d0e
Valid from: Wed Feb 09 11:23:26 EET 2011 until: Fri Jan 16 11:23:26
EET 2111
Certificate fingerprints:
         MD5:  C2:45:E9:73:07:B3:A8:84:AF:5F:B5:FA:41:D0:AE:D2
         SHA1:
42:84:B1:A8:45:3E:8A:9E:62:3C:7F:A4:76:78:44:C2:35:F3:50:4B
         Signature algorithm name: SHA1withRSA
         Version: 1
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

8. To add the NNMi certificate to JRE, run the following command: **keytool.exe -import -file** *<directory>*:**\cert -keystore *<directory>*:\HPBSM\JRE\lib\security\cacerts -trustcacerts -storepass changeit**.

   Make sure you answer `yes` when asked whether to `Trust this certificate?`. The following program listing is an example of what happens after you run this command.

```
Owner: CN=hpbsm_server.example.com
Issuer: CN=hpbsm_server.example.com
Serial number: 4d525d0e
```

```
Valid from: Wed Feb 09 11:23:26 EET 2011 until: Fri Jan 16 11:23:26
EET 2111
Certificate fingerprints:
         MD5:  C2:45:E9:73:07:B3:A8:84:AF:5F:B5:FA:41:D0:AE:D2
         SHA1:
42:84:B1:A8:45:3E:8A:9E:62:3C:7F:A4:76:78:44:C2:35:F3:50:4B
         Signature algorithm name: SHA1withRSA
         Version: 1
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

9 To add the NNMi certificate to JRE64, run the following command:
keytool.exe -import -file *<directory>*:\cert -keystore *<directory>*:\HPBSM\JRE64\lib\security\cacerts -trustcacerts -storepass changeit.

Make sure you answer `yes` when asked whether to `Trust this certificate?` The following program listing is an example of what happens after you run this command.

```
Owner: CN=hpbsm_server.example.com
Issuer: CN=hpbsm_server.example.com
Serial number: 4d525d0e
Valid from: Wed Feb 09 11:23:26 EET 2011 until: Fri Jan 16 11:23:26
EET 2111
Certificate fingerprints:
         MD5:  C2:45:E9:73:07:B3:A8:84:AF:5F:B5:FA:41:D0:AE:D2
         SHA1:
42:84:B1:A8:45:3E:8A:9E:62:3C:7F:A4:76:78:44:C2:35:F3:50:4B
         Signature algorithm name: SHA1withRSA
         Version: 1
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

10 To import the BSM certificates into the NNMi management server, complete the following steps:

a Run the following command on the BSM server:
keytool.exe -export -alias clientcert -file *<directory>*:\truststore -keystore *<directory>*:\HPBSM\odb\conf\security\server.truststore -storepass hppass

After the command finishes, the BSM 9.01 truststore certificate is stored in the *<directory>*:\truststore file.

b Run the following command on the BSM server:
keytool.exe -export -alias hpcert -file *<directory>*:\keystore -keystore *<directory>*:\HPBSM\odb\conf\security\server.keystore -storepass hppass

After the command finishes, the BSM 9.01 keystore certificate is stored in the *<directory>*:\keystore file.

c Copy the `truststore` and `keystore` files to a temporary directory on the NNMi management server. These files are shown as residing on the NNMi management server in the `<directory>:\temp\keystore`, `<directory>:\temp\truststore`, `/tmp/keystore and /tmp/truststore` locations in the remaining commands.

d To merge the keystore certificate, run the following command on the NNMi management server:

— *Windows*:

```
keytool -import -alias hpcert -keystore
%NnmDataDir%\shared\nnm\certificates\nnm.keystore
-storepass nnmkeypass -file <directory>:\temp\keystore
```

— *UNIX*:

```
keytool -import -alias hpcert -keystore $NnmDataDir/
shared/nnm/certificates/nnm.keystore -storepass
nnmkeypass -file
/tmp/keystore
```

e To merge the truststore certificate, run the following command on the NNMi management server:

— *Windows*:

```
keytool -import -alias clientcert -keystore
%NnmDataDir%\shared\nnm\certificates\nnm.truststore
-storepass ovpass -file <directory>:/temp/truststore
```

— *UNIX*:

```
keytool -import -alias clientcert -keystore $NnmDataDir/
shared/nnm/certificates/nnm.truststore -storepass ovpass
-file
/tmp/truststore
```

11 *Optional*: Run the following command sequence on the NNMi management server:

a **ovstop**

b **ovstart**

12 *Optional*: Run the following commands on both the NNMi management server and the BSM server. Compare the outputs to make sure the keystore certificates reside on both servers:

- *NNMi management server*:

  — *Windows*: **keytool.exe -list -keystore %NnmDataDir%\shared\nnm\certificates\nnm.keystore -storepass nnmkeypass**

  — *UNIX*: **keytool -list -keystore $NnmDataDir/shared/nnm/certificates/nnm.keystore -storepass nnmkeypass**

- *BSM server*: **keytool.exe -list -keystore *<directory>*:\HPBSM\odb\conf\security\server.keystore -storepass hppass**

13 *Optional*: Run the following commands on both the NNMi management server and the BSM server. Compare the outputs to make sure the truststore certificates reside on both servers:

- *NNMi management server*:
  - *Windows*: **keytool.exe -list -keystore %NnmDataDir%\shared\nnm\certificates\nnm.truststore -storepass ovpass**
  - *UNIX*: **keytool -list -keystore $NnmDataDir/shared/nnm/certificates/nnm.truststore -storepass ovpass**
- *BSM server*: **keytool.exe -list -keystore *<directory>*:\HPBSM\odb\conf\security\server.truststore -storepass hppass**

Using Single Sign-On with NNMi

You can configure HP Network Node Manager i Software (NNMi) single sign-on (SSO) to facilitate access to NNM iSPIs from the NNMi console. With SSO, when you log on to the NNMi console, you receive access to NNM iSPIs and other HP applications without needing to log on again. SSO provides easier access to NNM iSPIs and other HP applications while maintaining a secure level of access. After you sign out of the NNMi console (or the NNMi console session times out), you must re-enter your sign-in credentials to access NNM iSPI and other HP application URLs outside the NNMi console.

SSO is not enabled during installation. If it was, browsing from one NNMi management server to another logs you out of the first one, providing little benefit. To keep this from happening, SSO is initially disabled so you can coordinate setting the `initString` and `protectedDomains` parameter among the NNMi management servers. as explained in this chapter.

This chapter contains the following topics:

SSO Access for NNMi

To browse among several NNMi management servers, do one of the following:

- Edit the `nms-ui.properties` file and make the parameter values for `com.hp.nms.ui.sso.initString` and `com.hp.nms.ui.sso.protectedDomains` the same among the NNMi management servers. Make sure to set the `com.hp.nms.ui.sso.domain` parameter to match the domain an NNMi management server resides in.
  - If you have NNMi management servers residing in only one network domain, follow the instructions show in Enabling SSO for a Single Domain on page 142.
  - If you have NNMi management servers residing in more than one network domain, follow the instructions shown in Enabling SSO for NNMi Management Servers Located in Different Domains on page 143 for more information.
- Edit the `nms-ui.properties file` and make sure you have SSO disabled. See Disabling SSO on page 150 for more information.

If you choose to not complete one of these actions, each time you browse to a different NNMi management server, you will be automatically signed out of the previous NNMi management server.

There are special considerations for using SSO with the NNMi global network management feature. See SSO and the Actions Menu on page 229 and Configuring Single Sign-On for Global Network Management on page 229 for more information.

If the domain name of the NNMi management server is short, as in `mycompany`, without any period (.), the NNMi console will immediately sign you out. The restrictions for SSO browser cookies require a domain name to contain at least one period, such as `mycompany.com`. To remedy this situation, complete the following steps:

1. Open the following file in a text editor:
   - *Windows*: `%NNM_PROPS%/nms-ui.properties`
   - *UNIX*: `$NNM_PROPS/nms-ui.properties`
2. For this example, search for the following string:

   ```
   com.hp.nms.ui.sso.domain = mycompany
   ```

   and replace it with the following string:

   ```
   com.hp.nms.ui.sso.domain = mycompany.com
   ```
3. Run the following command to commit the changes:

   ```
   nnmsso.ovpl -reload
   ```

Enabling SSO for a Single Domain

To enable SSO for use in a single domain, complete the following steps:

1. Edit the following file:

- *Windows*: `%NNM_PROPS%\nms-ui.properties`
- *UNIX*: `$NNM_PROPS/nms-ui.properties`

2 Look for a section in the file that resembles the following:

```
com.hp.nms.ui.sso.isEnabled = false
```

Change this as follows:

```
com.hp.nms.ui.sso.isEnabled = true
```

3 Look for a section in the file that resembles the following:

```
com.hp.nms.ui.sso.domain = mycompany.com
```

Change *mycompany*`.com` to the domain the NNMi management server resides in. Make sure there is only one domain listed when enabling SSO in a single domain.

4 Look for a section in the file that resembles the following:

```
com.hp.nms.ui.sso.protectedDomains = mycompany.com
```

Change *mycompany*`.com` to the domain the NNMi management server resides in. Make sure there is only one protected domain listed when enabling SSO in a single protected domain.

5 Run the following command to commit the changes:

```
nnmsso.ovpl -reload
```

Enabling SSO for NNMi Management Servers Located in Different Domains

You can configure two or more NNMi management servers for SSO. This example explains how to configure SSO for three NNMi management servers located in different domains. If you must configure two or more NNMi management servers for SSO and these systems reside in different domains, complete the following steps:

1 Edit the following file:

- *Windows*: `%NNM_PROPS%\nms-ui.properties`
- *UNIX*: `$NNM_PROPS/nms-ui.properties`

2 Look for a section in the file that resembles the following:

```
com.hp.nms.ui.sso.isEnabled = false
```

Change this as follows:

```
com.hp.nms.ui.sso.isEnabled = true
```

3 Look for a section in the file that resembles the following:

```
com.hp.nms.ui.sso.domain = group1.mycompany.com
```

Make sure the domain name contains at least one dot.

4 Look for a section in the file that resembles the following:

```
com.hp.nms.ui.sso.protectedDomains=group1.mycompany.com
```

Change this as follows:

```
com.hp.nms.ui.sso.protectedDomains=group1.mycompany.com,
group2.yourcompany.com, group3.yourcompany.com
```

5 Look for a section in the file that resembles the following:

```
com.hp.nms.ui.sso.initString = Initialization String
```

NNMi management servers must share the same initialization string to work in an SSO configuration. Change the initialization string the same value on all NNMi management servers included in the SSO configuration.

6 Run the following command to commit the changes:

`nnmsso.ovpl -reload`

7 Repeat step 1 through step 6 two more times, configuring the remaining two NNMi management servers. For each remaining NNMi management server, substitute *`group2`* or *`group3`* for *`group1`* during step 3.

SSO Access for NNMi and the NNM iSPIs

After SSO is enabled, SSO between NNMi and the NNM iSPIs does *not* require `initString` configuration.

To use SSO, access NNMi as follows:

- Use the correct URL in the following form:
  <protocol>://<fully_qualified_domain_name>:<port_number>/nnm/
  <protocol> represents either http or https.
  <fully_qualified_domain_name> represents the official fully-qualified domain name (FQDN) of the NNMi management server.
  <port_number> is the port for connecting to the NNMi console, is assigned during NNMi installation, and is specified in the following file:
  - — *Windows*: `%NnmDataDir%\conf\nnm\props\nms-local.properties`
  - — *UNIX*: `$NnmDataDir/conf/nnm/props/nms-local.properties`
- Log on to NNMi using a valid account.

For SSO to work, URL access to NNMi and the NNM iSPIs must share a common network domain name. Additionally, the URL must not include an IP address. If you do not have a FQDN for the NNMi management server, you can substitute the IP address of the NNMi management server. However, doing so disables single sign-on for NNM iSPIs, and you must log on again the next time you access any NNM iSPI.

To determine the official FQDN of the NNMi management server, use one of the following methods:

- Use the **`nnmofficialfqdn.ovpl`** command to display the value of the official FQDN set during installation. See the *nnmofficialfqdn.ovpl* reference page, or the UNIX manpage, for more information.
- In the NNMi console, click **Help > System Information**. On the **Server** tab, look for the official FQDN statement.

To change the official FQDN set during installation, use the **nnmsetofficialfqdn.ovpl** command. See the *nnmsetofficialfqdn.ovpl* reference page, or the UNIX manpage, for more information.

➤ After installation, the system account is still valid. Use the system account only for command-line security and for recovery purposes.

SSO to NNM iSPIs require that users access the NNMi console through a URL that contains the official FQDN. You can configure NNMi to redirect NNMi URLs to the official FQDN when the NNMi console is accessed through a non-official domain name, such as an IP address or a shortened version of the domain name. Before configuring NNMi to redirect URLs, an appropriate official FQDN must be configured. For information, see the NNMi help.

After you enable NNMi to redirect URLs, note the following:

- You can log on to the NNMi console using any hostname that is valid for the NNMi management server you want to access. For example, if you request http://localhost/nnm, NNMi redirects you to a URL such as http://host.mydomain.com/nnm.
- If you cannot access the NNMi console using http://host.mydomain.com/nnm, use the following to directly access the NNMi console:
  ***<protocol>*://**
  ***<fully_qualified_domain_name>*:*<port_number>*launch?cmd=showMain.**
  <protocol> represents either http or https.
  <fully_qualified_domain_name> represents the official fully-qualified domain name (FQDN) of the NNMi management server.
  <port_number> is the port for connecting to the NNMi console, is assigned during NNMi installation, and is specified in the following file:
  - *Windows*: `%NnmDataDir%\conf\nnm\props\nms-local.properties`
  - *UNIX*: `$NnmDataDir/conf/nnm/props/nms-local.properties`

Configuring Single Sign-On Between NNMi and HP BSM or HP BAC

Single sign-on is available for all HP enterprise applications that use identical initialization string values and also share a common network domain name.

If the NNMi and HP Business Service Management (BSM) or HP Business Availability Center (BAC) user names are exactly the same for a particular individual, that person can log on to the MyBSM portal and view NNMi portlets without also logging on to NNMi. This single sign-on feature maps user names, but not passwords, between the two products. The passwords for logging on to MyBSM and NNMi can be different. Single sign-on does not map user roles, so the user can have different privileges in each application. For example, a user might have normal privileges in BSM or BAC and administrator privileges in NNMi.

To configure single sign-on access from BSM or BAC to NNMi, make sure that both applications use the same initialization string. You can copy the string from either application to the other. Consider all applications that interact when choosing which initialization string value to use. If necessary, also update the initialization string configuration for other applications.

BSM or BAC initialization string

Locate the BSM or BAC initialization string as follows:

1 Access the JMX console for BSM or BAC at:

   http://<*BSM_BAC_hostname*>:<*BSM_BAC_JMX_port*>/jmx-console/

2 Select **service=LW-SSO Configuration** (under Topaz).

   The initialization string is the value of the **InitString** parameter.

3 If you change the value of the **InitString** parameter, click **Apply Changes**.

NNMi initialization string

Locate the NNMi initialization string as follows:

1 Open the following file in a text editor:

   - *Windows*: `%NNM_PROPS%\nms-ui.properties`
   - *UNIX*: `$NNM_PROPS/nms-ui.properties`

2 Search for the string `initString`.

   The initialization string is the value of the `initString` parameter without the quotation marks.

   For example, if the `nms-ui.properties` file contains the following text:

```
initString=E091F3BA8AE47032B3B35F1D40F704B4
```

   the initialization string is:

```
E091F3BA8AE47032B3B35F1D40F704B4
```

3 If you change the value of the `initString` parameter shown in step 2, run the following command to commit the changes:

```
nnmsso.ovpl -reload
```

Configuring Single Sign-On Between NNMi and HP UCMDB

Single sign-on is available for all HP enterprise applications that use identical initialization string values and also share a common network domain name.

If the NNMi and HP Universal CMDB (UCMDB) user names are exactly the same for a particular individual, that person can log on to the NNMi console and launch UCMDB views without also logging on to UCMDB. This single sign-on feature maps user names, but not passwords, between the two products. The passwords for logging on to NNMi and UCMDB can be different. Single sign-on does not map user roles, so the user can have different privileges in each application. For example, a user might have normal privileges in NNMi and administrator privileges in UCMDB.

To configure single sign-on access from NNMi UCMDB, make sure that both applications use the same initialization string. You can copy the string from either application to the other. Consider all applications that interact when choosing which initialization string value to use. If necessary, also update the initialization string configuration for other applications.

UCMDB initialization string

Locate the UCMDB initialization string as follows:

1 Access the JMX console for UCMDB at:

   http://<*UCMDB_hostname*>:<*UCMDB_JMX_port*>/jmx-console/

2 Select **service=LW-SSO Configuration** (under Topaz).

The initialization string is the value of the **InitString** parameter.

3 If you change the value of the **InitString** parameter, click **Apply Changes**.

NNMi initialization string

Locate the NNMi initialization string as follows:

1 Open the following file in a text editor:

- *Windows*: `%NNM_PROPS%\nms-ui.properties`
- *UNIX*: `$NNM_PROPS/nms-ui.properties`

2 Search for the string `initString`.

The initialization string is the value of the `initString` parameter without the quotation marks.

For example, if the `nms-ui.properties` file contains the following text:

```
initString=E091F3BA8AE47032B3B35F1D40F704B4
```

the initialization string is:

```
E091F3BA8AE47032B3B35F1D40F704B4
```

3 If you change the value of the `initString` parameter, run the following command to commit the changes:

```
nnmsso.ovpl -reload
```

Configuring Single Sign-On Between NNMi and HP NA

Single sign-on is available for all HP enterprise applications that use identical initialization string values and also share a common network domain name.

If the NNMi and HP Network Automation (NA) user names are exactly the same for a particular individual, that person can log on to NNMi and view NA pages without logging on to NA. This single sign-on feature maps user names, but not passwords, between the two products. The passwords for logging on to NNMi and NA can be different. Single sign-on does not map user roles, so the user can have different privileges in each application. For example, a user might have operator level 1 privileges in NNMi and administrator privileges in NA.

To configure single sign-on access from NNMi to NA, make sure that both applications use the same initialization string. You can copy the string from either application to the other. Consider all applications that interact when choosing which initialization string value to use. If necessary, also update the initialization string configuration for other applications.

On the NNMi management server, locate the NNMi initialization string as follows:

1 Open the following file in a text editor:

- *Windows*: `%NNM_PROPS%\nms-ui.properties`
- *UNIX*: `$NNM_PROPS/nms-ui.properties`

Enable SSO

2 Look a section in the file that resembles the following:

```
com.hp.nms.ui.sso.isEnabled = false
```

```
Change this as follows:
```

```
com.hp.nms.ui.sso.isEnabled = true
```

NNMi initialization string

3 Search for the string initString.

The initialization string is the value of the initString parameter without the quotation marks.

For example, if the nms-ui.properties file contains the following text:

```
initString=E091F3BA8AE47032B3B35F1D40F704B4
```

the initialization string is:

```
E091F3BA8AE47032B3B35F1D40F704B4
```

4 If you change the value of the initString parameter, run the following command to commit the changes:

```
nnmsso.ovpl -reload
```

NA initialization string

On the NA server, locate the NA initialization string as follows:

1 Open the following file in a text editor:

- *Windows*:
  %NA_HOME%\server\ext\jboss\server\default\conf\lwssofmconf.xml
- *UNIX*:
  $NA_HOME/server/ext/jboss/server/default/conf/lwssofmconf.xml

The default value of the NA_HOME environment variable is as follows:

- *Windows*: C:/na
- *UNIX*: /opt/NA

2 In the enableLWSSO tag, set the enableLWSSOFramework attribute to true:

```
enableLWSSOFramework="true"
```

3 In the lwssoValidation block, do the following:

- Set the value of the domain tag to the full domain name of the NA server. For example, if the hostname of the NA server is na.location.example.com, set <domain>location.example.com</domain>.

➤ This step assumes that the NNMi management server is in the same domain as the NA server. If it is not, you must add a DNSDomain element for the NNMi management server's domain to the trustedHosts block.

- In the crypto tag, set the initString attribute to the value of the initString property in the NNMi nms-ui.properties file.

➤ The settings in the crypto block must be identical for all applications participating in SSO.

4 In the `trustedHosts` block, set the DNSDomain tag to the value of the domain tag in the `lwssoValidation` block, for example:

```
<DNSDomain>location.example.com</DNSDomain>
```

➤ This step assumes that the NNMi management server is in the same domain as the NA server. If the NA server is in a different domain than the NNMi management server, add `DNSDomain` entries for both domains.

5 Make sure all of the applications participating in SSO have a GMT (Greenwich Mean Time) time difference of less than 15 minutes. Although they can be in different time zones, the time difference, after conversion to GMT, should be the same.

6 Restart the NA jboss server:

- *Windows*: In the NA user interface, on the **Admin > Start/Stop Services** page, restart the Management Engine.
- *UNIX*: Run the following command:

  ```
  /etc/init.d/truecontrol restart
  ```

Disabling SSO

If you have a need to disable SSO, complete the following steps:

1. Edit the following file:
   - *Windows*: `%NNM_PROPS%\nms-ui.properties`
   - *UNIX*: `$NNM_PROPS/nms-ui.properties`
2. Look for a section in the file that resembles the following:

   ```
   com.hp.nms.ui.sso.isEnabled = true
   ```

   Change this as follows:

   com.hp.nms.ui.sso.isEnabled = false
3. Run the following command to commit the changes:

   `nnmsso.ovpl -reload`

SSO Security Notes

1. Confidential `initString` parameter in SSO security.

   SSO uses *Symmetric Encryption* to validate and create an SSO token. The `initString` parameter within the configuration is used for initialization of the secret key. An application creates a token, and each application that uses the same `initString` parameter validates the token.

   The following information is very important:

   — It is not possible to use SSO without setting the `initString` parameter.

   — The `initString` parameter is confidential information and should be treated as such in terms of publishing, transporting, and persistency.

   — Applications that integrate with each other can share the `initString` using SSO.

   — The minimum length of the `initString` is 12 characters.
2. Disable SSO unless it is specifically required.
3. The application that uses the weakest authentication framework, and issues an SSO token that is trusted by other integrated applications, determines the level of authentication security for all the applications.

   HP recommends that only applications using strong and secure authentication frameworks issue an SSO token.
4. Symmetric encryption implication:

   SSO uses symmetric cryptography for issuing and validating SSO tokens. Therefore, any application using SSO can issue a token to be trusted by all other applications sharing the same `initString`.

   This potential risk is relevant when an application sharing the `initString` either resides or is accessible in an untrusted location.

5 User roles:

SSO does not share user roles between integrated applications. Therefore, the integrated application must monitor user roles. HP recommends you share the same user registry (as LDAP/AD) among all integrated applications.

Failure to manage user roles might cause security breaches and negative application behavior. For example, the same user name might be assigned to different roles in the applications.

There could be situations when a user logs on to application A, then accesses application B that uses container or application authentication. The failure to manage the user role will force the user to manually log on to application B and enter a username. If the user enters a different user name than the one used to log on to application A, the following unexpected behavior can arise: If the user subsequently accesses a third application, application C, from application A or application B, then the user will access it using the user names that were used to log on to application A or application B respectively.

6 Identity Manager is used for an authentication:

All unprotected resources in the Identity Manager must be configured as nonsecure URL settings in the SSO configuration.

7 SSO demonstration mode:

- Use the SSO demonstration mode for demonstrative purposes only.
- Only use the demonstration mode in unsecured networks.
- Do not use the demonstration mode in production. Any combination of the demonstration mode with the production mode should not be used.

Integrating NNMi's SSO into Novell Access Manager Enterprise SSO

This chapter contains configuration information on integrating NNMi's SSO with Novell Access Manager using its LW-SSO IdM feature.

NNMi User Access Configuration Information

The instructions shown below explain how to configure NNMi to use Novell Access Manager's IdM (Identity Management) feature.

How to enable NNMi IdM SSO support

To configure NNMi to accept an inbound call from Novell Access Manager's IdM feature, do the following:

1. From a command prompt, change to the following directory:
   - *Windows*: %NNM_SHARED_CONF%
   - *UNIX*: $NNM_SHARED_CONF
2. Copy the `lwssofmconf.xml` file into the above location.
3. From a command prompt, change to the following directory:
   - *Windows*: %NNM_JBOSS_DEPLOY%
   - *UNIX*: $NNM_JBOSS_DEPLOY
4. Copy the `nms-ui.ear` file into the above location.
5. Edit the following file:
   - *Windows*: `%NNM_PROPS%\nms-ui.properties`
   - *UNIX*: `$NNM_PROPS/nms-ui.properties`

6. Add the following line and save your changes:

   ```
   com.hp.nms.ui.sso.userNameHeaderName=USERID
   ```

   The value you set for the **`com.hp.nms.ui.sso.userNameHeaderName`** parameter (**`USERID`**) is the tag name for the IdM SSO user name. If necessary, change **`USERID`** to the correct user name based on the value required for your environment.

7. Restart the NNMi management server.

   a. Run the **`ovstop`** command on the NNMi management server.

   b. Run the **`ovstart`** command on the NNMi management server.

Configuring the Telnet and SSH Protocols for Use by NNMi

The **Actions > Telnet... (from client)** menu item invokes the telnet command to the selected node (from the web browser in which the NNMi console is currently running). The **Actions > Secure Shell... (from client)** menu item invokes the secure shell (SSH) command to the selected node (from the web browser in which the NNMi console is currently running). By default, neither Microsoft Internet Explorer nor Mozilla Firefox defines the telnet command nor the SSH command, so using either of these menu items produces an error message. You can configure the telnet, SSH, or both protocols for each NNMi user (on a per-system basis), and you can change the NNMi console menu items.

This chapter contains the following topics:

Disable the Telnet or SSH Menu Item

If the NNMi users in your deployment environment do not require telnet or SSH connections from the NNMi console, you can disable the respective menu item to remove it from the NNMi console.

Disabling a menu item in the NNMi console applies to all users who log on to the NNMi console on this NNMi management server. To disable the **Telnet** or **Secure Shell** menu item, follow these steps:

1. In the **Configuration** workspace, expand **User Interface**, and then elect **Menu Items**.
2. In the **Menu Items** view, select the **Telnet... (from Client)** row or the **Secure Shell... (from client)** row, and then click **Open** .

3. On the **Menu Item** form, clear the **Enabled** check box, and then set the **Author** field to an appropriate value.

   Changing the author value ensures that this menu item remains disabled when you upgrade NNMi.

4. Save and close the form.

For more information, see *Control the Actions Menu* in the NNMi help.

Configure a Telnet or SSH Client for the Browser on Windows

Configure the operating-system provided telnet command for an NNMi user's web browser. This procedure must be done for each computer and web browser from which an NNMi user needs to run the **Actions > Telnet... (from Client)** menu item.

Configure a third-party ssh command for an NNMi user's web browser. This procedure must be done for each computer and web browser from which an NNMi user needs to run the **Actions > Secure Shell... (from Client)** menu item.

To complete any of the procedures in this section, you must have administrative privileges on the computer. The specific steps depend on the version (32-bit or 64-bit) of the browser and the operating system.

To determine the version of Internet Explorer, click **Help > About Internet Explorer**. If the version information does not include the text **64-bit Edition**, this Internet Explorer is 32-bit.

Firefox is only available in a 32-bit version.

Table 6 identifies the procedure to use for each browser and operating system combination.

Table 6 Matrix of Telnet and SSH Configuration Procedures on Windows

Web Browser	Windows Operating System Architecture	Applicable Procedures
Internet Explorer 32-bit	32-bit	• Windows Operating System-Provided Telnet Client on page 157 • Third-Party Telnet Client (Standard Windows) on page 159 • Third-Party SSH Client (Standard Windows and Windows on Windows) on page 161
	64-bit Windows 7	• Third-Party Telnet Client (Standard Windows) on page 159 • Third-Party SSH Client (Standard Windows and Windows on Windows) on page 161
	64-bit other than Windows 7	• Third-Party Telnet Client (Windows on Windows) on page 160 • Third-Party SSH Client (Standard Windows and Windows on Windows) on page 161

Table 6 Matrix of Telnet and SSH Configuration Procedures on Windows (cont'd)

Web Browser	Windows Operating System Architecture	Applicable Procedures
Internet Explorer 64-bit	64-bit	• Windows Operating System-Provided Telnet Client on page 157 • Third-Party Telnet Client (Standard Windows) on page 159 • Third-Party SSH Client (Standard Windows and Windows on Windows) on page 161
Firefox	32-bit	• Windows Operating System-Provided Telnet Client on page 157 • Third-Party Telnet Client (Standard Windows) on page 159 • Third-Party SSH Client (Standard Windows and Windows on Windows) on page 161
	64-bit Windows 7	• Third-Party Telnet Client (Standard Windows) on page 159 • Third-Party SSH Client (Standard Windows and Windows on Windows) on page 161
	64-bit other than Windows 7	• Third-Party Telnet Client (Windows on Windows) on page 160 • Third-Party SSH Client (Standard Windows and Windows on Windows) on page 161

Many of the tasks in this section involve editing the Windows registry. Instead of editing the registry directly, you can create a .reg file that each user can run on their system. For example .reg files, see Example Files for Changing the Windows Registry on page 164.

For more information about the tasks described in this section, see the following Microsoft articles:

- Installing the Microsoft-provided telnet client:
  http://technet.microsoft.com/en-us/library/cc771275%28WS.10%29.aspx
- Introduction to the Windows registry:
  http://support.microsoft.com/kb/256986
- Backing up and restoring the Windows registry:
  http://support.microsoft.com/kb/322756

Windows Operating System-Provided Telnet Client

This procedure applies to the following cases:

- 32-bit Internet Explorer on a 32-bit operating system
- 32-bit Firefox on a 32-bit operating system
- 64-bit Internet Explorer on a 64-bit operating system

To configure the operating system-provided telnet client for use by a web browser, follow these steps:

1 (Microsoft Windows 7, Microsoft Vista, or Microsoft Windows Server 2008 only) Install the operating system telnet client on the computer by following the steps appropriate to the operating system.

   Windows 7 or Vista:

   a In the Control Panel, click **Programs**, and then click **Programs and Features**.

   b Under Tasks, click **Turn Windows features on or off**.

   c In the Windows Features dialog box, select the **Telnet Client** check box, and then click **OK**.

   Windows Server 2008:

   a In the Server Manager, under Features Summary, click **Add Features**.

   b In the Add Features Wizard, select the **Telnet Client** check box, click **Next**, and then click **Install**.

2 (Internet Explorer only) Enable Internet Explorer to use the telnet protocol.

   a Back up the Windows registry.

   b Use the Windows registry editor to add the [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_DISABLE_TELNET_PROTOCOL] key with the following values:

Name	Type	Data
iexplore.exe	REG_DWORD	0

3 Set file association for the URL:Telnet Protocol file type.

   a Back up the Windows registry.

   b Use the Windows registry editor to modify the [HKEY_CLASSES_ROOT\telnet\shell\open\command] key with the following value:

Name	Type	Data
(default)	REG_SZ	rundll32.exe url.dll,TelnetProtocolHandler %l

`%l` (with a lowercase L) is the argument passed to telnet, usually an IP address or the fully-qualified domain name of a node.

For tighter control, you can encode the paths to the binaries in the key (as a single line). For example:

```
"C:\Windows\system32\rundll32.exe"
"C:\Windows\system32\url.dll",TelnetProtocolHandler %l
```

4 Restart the web browser, and then, in the browser address bar, enter the telnet command:

```
telnet://<node>
```

<node> is the IP address or fully-qualified domain name of a node that runs the telnet server.

If you are prompted with a security warning, permit the action.

In Firefox, select the **Remember my choice for telnet links** check box.

Third-Party Telnet Client (Standard Windows)

This procedure applies to the following cases:

- 32-bit Internet Explorer on a 32-bit operating system
- 32-bit Internet Explorer on a 64-bit Windows 7 operating system
- 32-bit Firefox on a 32-bit operating system
- 64-bit Internet Explorer on a 64-bit operating system

To configure a third-party telnet client for use by a web browser, follow these steps:

1 Obtain and install a third-party telnet client.

This procedure gives examples for the PuTTY client installed to `C:\Program Files\PuTTY\putty.exe`. The PuTTY client is available from **http://www.putty.org**.

2 (Internet Explorer only) Enable Internet Explorer to use the telnet protocol.

a Back up the Windows registry.

b Use the Windows registry editor to add the [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_DISABLE_TELNET_PROTOCOL] key with the following values:

Name	Type	Data
iexplore.exe	REG_DWORD	0

3 Set file association for the URL:Telnet Protocol file type.

a Back up the Windows registry.

b Use the Windows registry editor to modify the [HKEY_CLASSES_ROOT\telnet\shell\open\command] key with the following value:

Name	Type	Data
(default)	REG_SZ	"C:\Program Files\PuTTY\putty.exe" %l

`%l` (with a lowercase L) is the argument passed to telnet, usually an IP address or the fully-qualified domain name of a node.

In a .reg file, escape each quotation mark (") and backslash (\) character with a backslash (\) character.

4 Restart the web browser, and then, in the browser address bar, enter the telnet command:

```
telnet://<node>
```

<node> is the IP address or fully-qualified domain name of a node that runs the telnet server.

If you are prompted with a security warning, permit the action.

In Firefox, select the **Remember my choice for telnet links** check box.

Third-Party Telnet Client (Windows on Windows)

This procedure applies to the following cases:

- 32-bit Internet Explorer on a 64-bit operating system (other than Windows 7)
- 32-bit Firefox on a 64-bit operating system

To configure a third-party telnet client for use by a web browser, follow these steps:

1 Obtain and install a third-party telnet client.

This procedure gives examples for the PuTTY client installed to `C:\Program Files\PuTTY\putty.exe`. The PuTTY client is available from **http://www.putty.org**.

2 (Internet Explorer only) Enable Internet Explorer to use the telnet protocol.

a Back up the Windows registry.

b Use the Windows registry editor to add the [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_DISABLE_TELNET_PROTOCOL] key with the following values:

Name	Type	Data
iexplore.exe	REG_DWORD	0

3 Set file association for the URL:Telnet Protocol file type.

a Back up the Windows registry.

b Use the Windows registry editor to modify the [HKEY_CLASSES_ROOT\Wow6432Node\telnet\shell\open\command] key with the following value:

Name	Type	Data
(default)	REG_SZ	"C:\Program Files\PuTTY\putty.exe" %l

`%l` (with a lowercase L) is the argument passed to telnet, usually an IP address or the fully-qualified domain name of a node.

In a .reg file, escape each quotation mark (") and backslash (\) character with a backslash (\) character.

4 Restart the web browser, and then, in the browser address bar, enter the telnet command:

`telnet://<node>`

<node> is the IP address or fully-qualified domain name of a node that runs the telnet server.

If you are prompted with a security warning, permit the action.

In Firefox, select the **Remember my choice for telnet links** check box.

Third-Party SSH Client (Standard Windows and Windows on Windows)

This procedure applies to the following cases:

- 32-bit Internet Explorer on a 32-bit or 64-bit operating system
- 32-bit Firefox on a 32-bit or 64-bit operating system
- 64-bit Internet Explorer on a 64-bit operating system

To configure a third-party SSH client for use by a web browser, follow these steps:

1 Obtain and install a third-party SSH client.

This procedure gives examples for the PuTTY client installed to `C:\Program Files\PuTTY\putty.exe`. The PuTTY client is available from **http://www.putty.org**.

2 Because PuTTY cannot correctly parse the "ssh://<node>" input, this example includes a script that strips the "ssh://" from the input argument. The script `C:\Program Files\PuTTY\ssh.js` contains the following commands:

```
host = WScript.Arguments(0).replace(/ssh:/,"").replace(/\//g,"");
shell = WScript.CreateObject("WScript.Shell");
shell.Run("\"c:\\Program Files\\PuTTY\\putty.exe\" -ssh " + host);
```

This script was created for this example and is not included with PuTTY.

3 Define the ssh protocol.

a Back up the Windows registry.

b Use the Windows registry editor to add the [HKEY_CLASSES_ROOT\ssh] key with the following values:

Name	Type	Data
(default)	REG_SZ	URL:ssh Protocol
EditFlags	REG_DWORD	2
FriendlyTypeName	REG_SZ	Secure Shell
URL Protocol	REG_SZ	*no value*

4 Set file association for the URL:ssh Protocol file type.

a Back up the Windows registry.

b Use the Windows registry editor to modify the [HKEY_CLASSES_ROOT\ssh\shell\open\command] key with the following value:

Name	Type	Data
(default)	REG_SZ	"C:\Windows\System32\WScript.exe" "C:\Program Files\PuTTY\ssh.js" %l

`%l` (with a lowercase L) is the complete ssh argument, including the protocol specification. The ssh.js script passes the ssh target to PuTTY.

In a .reg file, escape each quotation mark (") and backslash (\) character with a backslash (\) character.

5 Restart the web browser, and then, in the browser address bar, enter the ssh command:

```
ssh://<node>
```

<node> is the IP address or fully-qualified domain name of a node that runs the telnet server.

If you are prompted with a security warning, permit the action.

In Firefox, select the **Remember my choice for ssh links** check box.

Configure Firefox to use Telnet or SSH on Linux

On the Linux operating system, define the telnet or ssh protocol, and then configure Firefox to use the new protocol.

To complete any of the procedures in this section, you must have administrative privileges on the computer.

For more information, see **http://kb.mozillazine.org/Register_protocol**.

Telnet on Linux

To configure Firefox on the Linux operating system to use the telnet protocol, follow these steps:

1 Define the telnet protocol.

a Create the `/usr/local/bin/nnmtelnet` file with the following contents:

```
#!/bin/bash
#
# Linux shell script called by Firefox in response to
# telnet:// URLs for the NNMi telnet menu.
#
```

```
address=`echo $1 | cut -d : -f 2 | sed 's;/;;g'`
port=`echo $1 | cut -d : -f 3`
exec /usr/bin/xterm -e telnet $address $port
```

b Set the script permissions to be executable by everyone:

```
chmod 755 /usr/local/bin/nnmtelnet
```

2 Configure Firefox preferences for telnet.

a In the Firefox address bar, enter: **`about:config`**

b In the preference list, right-click, click **New**, and then click **Boolean**.

c Enter the preference name: **`network.protocol-handler.expose.telnet`**

d Select the preference value: **`false`**

3 Configure Firefox to use the newly-defined protocol.

a Browse to a telnet link.

You can create a simple HTML file containing the link, or you can use **Actions > Telnet... (from Client)** in the NNMi console. Typing the link directly into the address bar does not have the same effect.

b In the Launch Application window, click **Choose**, and then select `/usr/local/bin/nnmtelnet`.

c Select the **Remember my choice for telnet links** check box.

Secure Shell on Linux

To configure Firefox on the Linux operating system to use the ssh protocol, follow these steps:

1 Define the ssh protocol.

a Create the `/usr/local/bin/nnmssh` file with the following contents:

```
#!/bin/bash
#
# Linux shell script called by Firefox in response to
# ssh:// URLs for the NNMi SSH menu.
#
address=`echo $1 | cut -d : -f 2 | sed 's;/;;g'`
port=`echo $1 | cut -d : -f 3`
exec /usr/bin/xterm -e ssh $address $port
```

b Set the script permissions to be executable by everyone:

```
chmod 755 /usr/local/bin/nnmssh
```

2 Configure Firefox preferences for SSH.

a In the Firefox address bar, enter: **`about:config`**

b In the preference list, right-click, click **New**, and then click **Boolean**.

c Enter the preference name: **`network.protocol-handler.expose.ssh`**

d Select the preference value: **`false`**

3 Configure Firefox to use the newly-defined protocol.

a Browse to an SSH link.

You can create a simple HTML file containing the link, or you can use the new SSH menu item that you defined in the NNMi console. Typing the link directly into the address bar does not have the same effect.

b In the Launch Application window, click **Choose**, and then select `/usr/local/bin/nnmssh`.

c Select the **Remember my choice for ssh links** check box.

Example Files for Changing the Windows Registry

If many NNMi users need to use the telnet or ssh protocols to access managed nodes from the NNMi console, you might be able to automate the Windows registry updates with one or more .reg files. This section contains example .reg files on which you can base the creation of your own .reg files. Note that the registry keys are located in a different path for running 32-bit applications on 64-bit versions of Windows than they are for when the application and operating system match.

For more information, see the Microsoft article at **http://support.microsoft.com/kb/310516**.

Example nnmtelnet.reg

This registry content example applies to Windows Operating System-Provided Telnet Client on page 157.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
Explorer\MAIN\FeatureControl\FEATURE_DISABLE_TELNET_PROTOCOL]
"iexplore.exe"=dword:00000000

[HKEY_CLASSES_ROOT\telnet\shell\open\command]
@="\"C:\\Windows\\system32\\rundll32.exe\"
\"C:\\Windows\\system32\\url.dll\",TelnetProtocolHandler %l"
```

Example nnmputtytelnet.reg

This registry content example applies to Third-Party Telnet Client (Standard Windows) on page 159.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
Explorer\MAIN\FeatureControl\FEATURE_DISABLE_TELNET_PROTOCOL]
"iexplore.exe"=dword:0c0000000

[HKEY_CLASSES_ROOT\telnet\shell\open\command]
@="\"C:\\Program Files\\PuTTY\\putty.exe\" %l"
```

Example nnmtelnet32on64.reg

This registry content example applies to Third-Party Telnet Client (Windows on Windows) on page 160.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet
Explorer\MAIN\FeatureControl\FEATURE_DISABLE_TELNET_PROTOCOL]
"iexplore.exe"=dword:00000000

[HKEY_CLASSES_ROOT\Wow6432Node\telnet\shell\open\command]
@="\"C:\\Program Files\\PuTTY\\putty.exe\" %l"
```

Example nnmssh.reg

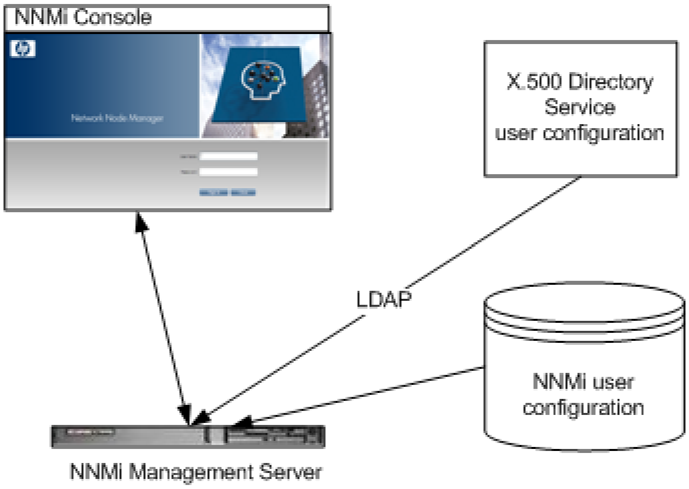
This registry content example applies to Third-Party SSH Client (Standard Windows and Windows on Windows) on page 161.

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\ssh]
@="URL:ssh Protocol"
"EditFlags"=dword:00000002
"FriendlyTypeName"="Secure Shell"
"URL Protocol"=""

[HKEY_CLASSES_ROOT\ssh\shell\open\command]
@="\"C:\\Windows\\System32\\WScript.exe\" \"c:\\Program Files\\PuTTY\\ssh.js\" %l"
```

Integrating NNMi with a Directory Service through LDAP



This chapter contains information about integrating NNMi with a directory service for consolidating the storage of user names, passwords, and, optionally, NNMi user group assignments. It contains the following topics:

NNMi User Access Information and Configuration Options

Together, the following items define an NNMi user:

- The **user name** uniquely identifies the NNMi user. The user name provides access to NNMi and receives incident assignments.
- The **password** is associated with the user name to control access to the NNMi console or NNMi command.
- **NNMi user group** membership controls the information available and the type of actions that a user can take in the NNMi console. User group membership also controls the availability of NNMi commands to the user.

NNMi provides several options for where the NNMi user access information is stored, as described in the following topics. Table 7 indicates the databases that store the NNMi user access information for each configuration option.

Table 7 Options for Storing User Information

Option	User Name	Password	User Group	User Group Membership
1	NNMi	NNMi	NNMi	NNMi
2	Both	Directory Service	NNMi	NNMi
3	Directory Service	Directory Service	Both	Directory Service

When NNMi is integrated with a directory service for some or all of the user access information, the user account and user group definition statement on the **Server** tab of the **System Information** window indicates the type of information that was obtained through LDAP queries.

Single sign-on (SSO) between NNMi and other applications is not dependent on how the NNMi user access information is configured or where this information is stored.

Option 1: All NNMi User Information in the NNMi Database

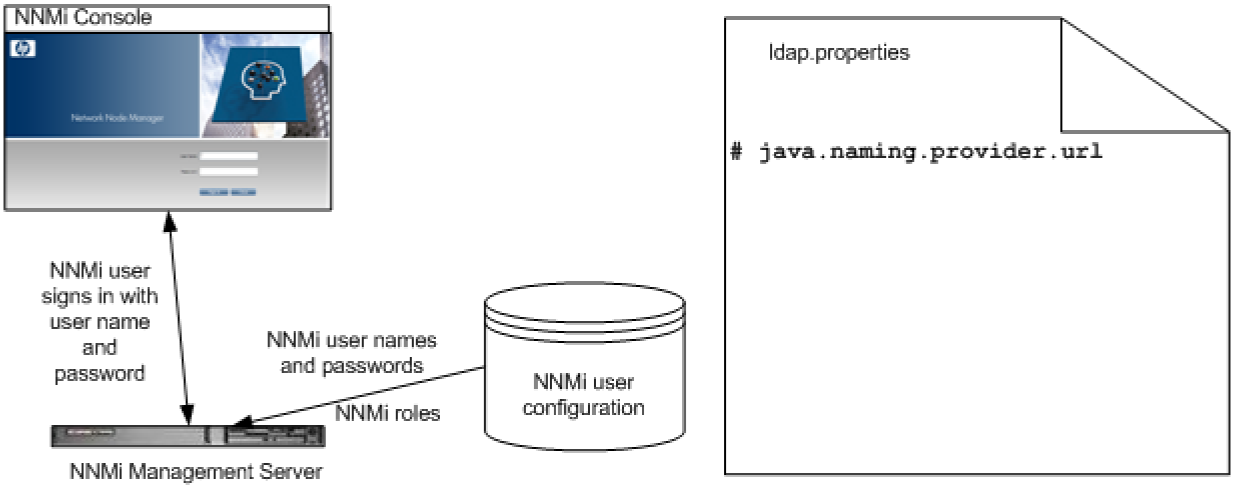
With configuration option 1, NNMi accesses the NNMi database for all user access information, which the NNMi administrator defines and maintains in the NNMi console. The user access information is local to NNMi. NNMi does not access a directory service, and NNMi ignores the `ldap.properties` file (as indicated by the commented line in Figure 8).

Figure 8 shows the information flow for this option, which is appropriate in the following situations:

- The number of NNMi users is small.
- No directory service is available.

For information about setting up all user information in the NNMi database, see *Control Access with NNMi Accounts* in the NNMi help. You do not need to read this chapter.

Figure 8 NNMi User Sign-in Information Flow for Option 1


NNMi Console
NNMi user signs in with user name and password
NNMi user names and passwords
NNMi roles
NNMi user configuration
NNMi Management Server
ldap.properties
# java.naming.provider.url

Option 2: Some NNMi User Information in the NNMi Database and Some NNMi User Information in the Directory Service

With configuration option 2, NNMi accesses a directory service for the user name and password, which are defined externally to NNMi and are also available to other applications. The mapping of users to NNMi user groups is maintained in the NNMi console. The configuration and maintenance of NNMi user access information is a joint effort as described here:

- The directory service administrator maintains the user names and password in the directory service.
- The NNMi administrator enters the user names (as defined in the directory service), user group definitions, and the user group mappings in the NNMi console.
- The NNMi administrator configures the NNMi `ldap.properties` file to describe the directory service database schema for user names to NNMi. (In Figure 9, the commented line indicates that NNMi does not pull user group information from the directory service.)

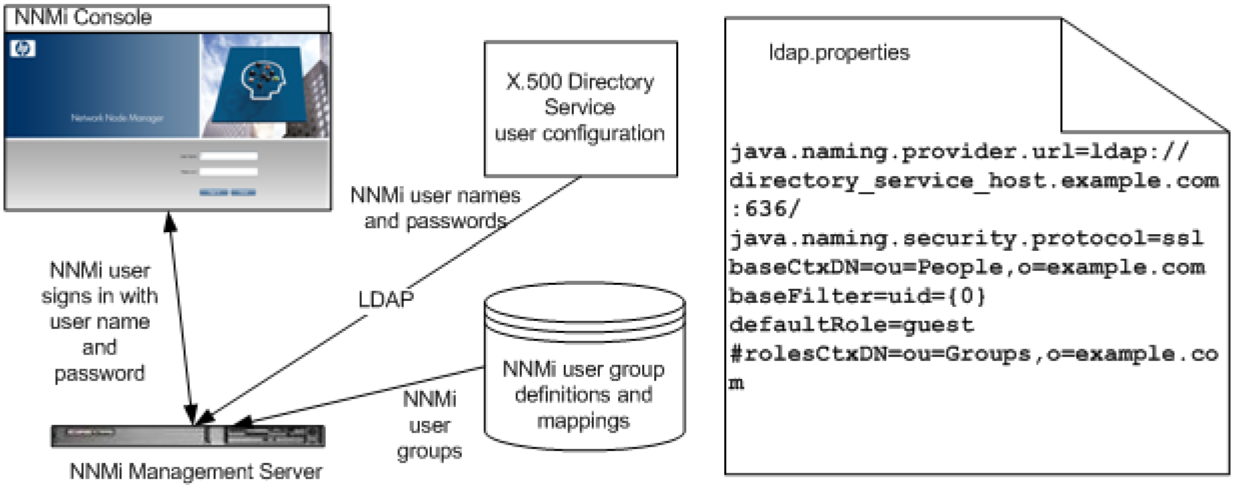
Because user names must be entered in two places, user name maintenance must be performed in both places.

Figure 9 shows the information flow for this option, which is appropriate in the following situations:

- The number of NNMi users is small, and a directory service is available.
- The NNMi administrator wants to control the user groups instead of requiring a directory service change for each user group change.
- The directory service group definitions are not easily expandable.

For information about integrating with a directory service for the user name and password, see the rest of this chapter and *Control Access Using Both Directory Service and NNMi* in the NNMi help.

Figure 9 NNMi User Sign-in Information Flow for Option 2


NNMi Console
X.500 Directory Service user configuration
ldap.properties
NNMi user names and passwords
LDAP
NNMi user signs in with user name and password
NNMi user group definitions and mappings
NNMi user groups
NNMi Management Server

```
java.naming.provider.url=ldap://
directory_service_host.example.com
:636/
java.naming.security.protocol=ssl
baseCtxDN=ou=People,o=example.com
baseFilter=uid={0}
defaultRole=guest
#rolesCtxDN=ou=Groups,o=example.co
m
```

Option 3: All NNMi User Information in the Directory Service

With configuration option 3, NNMi accesses a directory service for all user access information, which is defined externally to NNMi and is available to other applications. Membership in one or more directory service groups determines the NNMi user groups for the user.

The configuration and maintenance of NNMi user access information is a joint effort as described here:

- The directory service administrator maintains the user names, passwords, and group membership in the directory service.
- The NNMi administrator maps the directory service groups to NNMi user groups in the NNMi console.
- The NNMi administrator configures the NNMi `ldap.properties` file to describe the directory service database schema for user names and groups to NNMi.

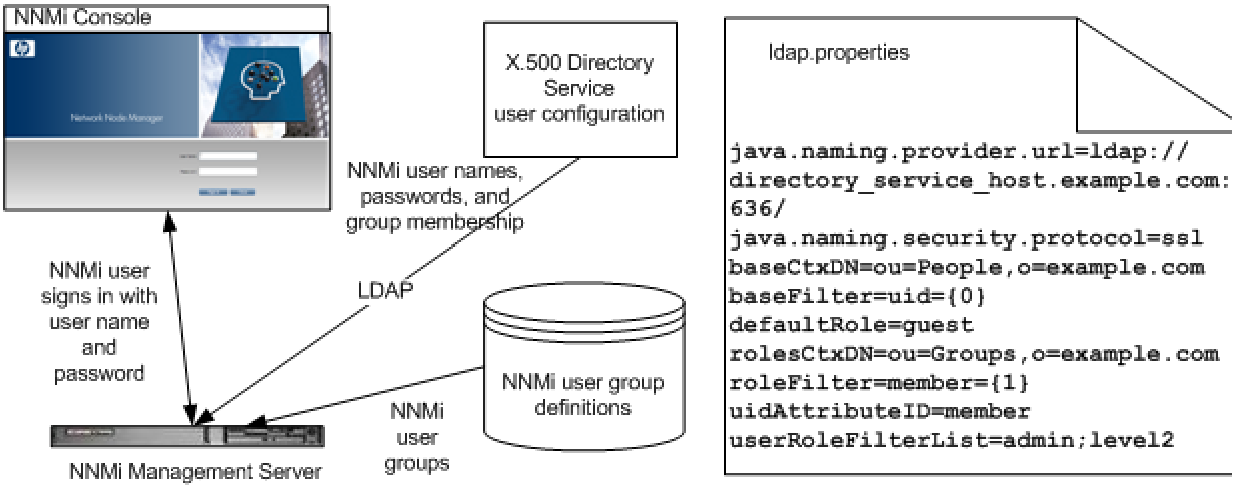
Figure 10 shows the information flow for this option, which is appropriate for environments where the directory service can be modified to include user groups that align with the people who need access to NNMi.

Because this option is an expansion of the option 2 scenario, HP recommends the following configuration process:

1. Configure and verify NNMi user name and password retrieval from the directory service.
2. Configure NNMi user group retrieval from the directory service.

For information about integrating with a directory service for all user information, see the rest of this chapter and *Control Access with a Directory Service* in the NNMi help.

Figure 10 NNMi User Sign-in Information Flow for Option 3


NNMi Console
X.500 Directory Service user configuration
ldap.properties
NNMi user names, passwords, and group membership
NNMi user signs in with user name and password
LDAP
NNMi user group definitions
NNMi user groups
NNMi Management Server

```
java.naming.provider.url=ldap://
directory_service_host.example.com:
636/
java.naming.security.protocol=ssl
baseCtxDN=ou=People,o=example.com
baseFilter=uid={0}
defaultRole=guest
rolesCtxDN=ou=Groups,o=example.com
roleFilter=member={1}
uidAttributeID=member
userRoleFilterList=admin;level2
```

Configuring NNMi to Access a Directory Service

Directory service access is configured in the following file:

- *Windows*: `%NNM_SHARED_CONF%\ldap.properties`
- *UNIX*: `$NNM_SHARED_CONF/ldap.properties`

For information about this file, see ldap.properties Configuration File Reference on page 192. Also see Examples on page 197.

For information about the general structure of a directory service, see Directory Service Queries on page 180.

For configuration option 2, complete the following tasks:

- Task 1: Back up the Current NNMi User Information
- Task 2: Optional. Configure Secure Communications to the Directory Service
- Task 3: Configure User Access from the Directory Service
- Task 4: Test the User Name and Password Configuration
- Task 9: Clean up to Prevent Unexpected Access to NNMi
- Task 10: Optional. Map the User Groups to Security Groups

For configuration option 3, complete the following tasks:

- Task 1: Back up the Current NNMi User Information
- Task 2: Optional. Configure Secure Communications to the Directory Service
- Task 3: Configure User Access from the Directory Service
- Task 4: Test the User Name and Password Configuration
- Task 5: (Configuration Option 3 only) Configure Group Retrieval from the Directory Service

  ➤ If you plan to store NNMi user groups in the directory service, the directory service must be configured with the NNMi user groups. For more information, see Directory Service Configuration for Storing NNMi User Groups on page 190.

- Task 6: (Configuration Option 3 only) Map the Directory Service Groups to NNMi User Groups
- Task 7: (Configuration Option 3 only) Test the NNMi User Group Configuration
- Task 8: (Configuration Option 3 only) Configure NNMi User Groups for Incident Assignment
- Task 9: Clean up to Prevent Unexpected Access to NNMi
- Task 10: Optional. Map the User Groups to Security Groups

Task 1: Back up the Current NNMi User Information

Back up the user information in the NNMi database:

```
nnmconfigexport.ovpl -c account -u <user> \
-p <password> -f NNMi_database_accounts.xml
```

Task 2: Optional. Configure Secure Communications to the Directory Service

If the directory service requires the use of secure sockets layer (SSL), import your company's certificate into the NNMi trust store as described in Configuring an SSL Connection to the Directory Service on page 134.

Task 3: Configure User Access from the Directory Service

Complete this task for configuration options 2 and 3. Follow the appropriate procedure for your directory service. This task includes the following sections:

- Simple Approach for Microsoft Active Directory
- Simple Approach for Other Directory Services

(For detailed configuration instructions, see User Identification on page 185.)

Simple Approach for Microsoft Active Directory

1 Back up the `ldap.properties` file that was shipped with NNMi, and then open the file in any text editor.

2 Overwrite the file contents with the following text:

```
java.naming.provider.url=ldap://<myldapserver>:389/

bindDN=<mydomain>\\<myusername>
bindCredential=<mypassword>

baseCtxDN=CN=Users,DC=<myhostname>,DC=<mycompanyname>,DC=<mysuffix>
baseFilter=CN={0}

defaultRole=guest

#rolesCtxDN=CN=Users,DC=<myhostname>,DC=<mycompanyname>,DC=<mysuffix>
roleFilter=member={1}
uidAttributeID=member
userRoleFilterList=admin;level2;level1
```

3 Specify the URL for accessing the directory service. In the following line:

```
java.naming.provider.url=ldap://<myldapserver>:389/
```

Replace *`<myldapserver>`* with the fully-qualified hostname of the Active Directory server (for example: `myserver.example.com`).

To specify multiple directory service URLs, separate each URL with a single space character ( ).

4 Specify credentials for a valid directory service user. In the following lines:

```
bindDN=<mydomain>\\<myusername>
bindCredential=<mypassword>
```

Make the following substitutions:

- Replace *`<mydomain>`* with the name of the Active Directory domain.

- Replace *<myusername>* and *<mypassword>* with a user name and password for accessing the Active Directory server.
  If you plan to add the password in plain text, specify a user name with read-only access to the directory service.
  If you plan to specify an encrypted password, use the following command to encrypt the plain text password before adding it to the `ldap.properties` file:
  `nnmldap.ovpl -encrypt <mypassword>`

  This encrypted password only works for the NNMi instance you create it for. Do not attempt to use it for a different NNMi instance.

  For more information see the *nnmldap.ovpl* reference page, or the UNIX manpage.

5 Specify the portion of the directory service domain that stores user records. In the following line:

```
baseCtxDN=CN=Users,DC=<myhostname>,DC=<mycompanyname>,
  DC=<mysuffix>
```

Replace *<myhostname>*, *<mycompanyname>*, and *<mysuffix>* with the components of the fully-qualified hostname of the Active Directory server (for example, for the hostname `myserver.example.com`, specify: `DC=myserver,DC=example,DC=com`).

Simple Approach for Other Directory Services

1 Back up the `ldap.properties` file that was shipped with NNMi, and then open the file in any text editor.

2 Specify the URL for accessing the directory service. In the following line:

```
#java.naming.provider.url=ldap://<myldapserver>:389/
```

Do the following:

- Uncomment the line (by deleting the `#` character).
- Replace *<myldapserver>* with the fully-qualified hostname of the directory server (for example: `myserver.example.com`).

  To specify multiple directory service URLs, separate each URL with a single space character ( ).

3 Specify the portion of the directory service domain that stores user records. In the following line:

```
baseCtxDN=ou=People,o=myco.com
```

Replace `ou=People,o=myco.com` with the portion of the directory service domain that stores user records.

4 Specify the format of user names for signing in to NNMi. In the following line:

```
baseFilter=uid={0}
```

Replace `uid` with the user name attribute from the directory service domain.

Task 4: Test the User Name and Password Configuration

1 In the `ldap.properties` file, set `defaultRole=guest` for testing purposes. (You can change this value at any time.)

2 Save the `ldap.properties` file.

3 Force NNMi to re-read the ldap.properties file by running the following command:

```
nnmldap.ovpl -reload
```

4 Log on to the NNMi console with a user name and password that are defined in the directory service.

Run this test with a user name that is not already defined in the NNMi database.

5 Verify the user name and NNMi role (Guest) in the title bar of the NNMi console.

- If user signin works correctly, continue with step 8 of this task.
- If user signin does not work correctly, continue with step 6, next.

After each test, sign out of the NNMi console to clear the session credentials.

6 Test the configuration for one user by running the following command:

```
nnmldap.ovpl -diagnose <NNMi_user>
```

Replace *<NNMi_user>* with the sign-in name of an NNMi user as defined in the directory service.

Examine the command output and respond appropriately. Suggestions include:

- Verify that you completed Task 3 on page 172 correctly.
- Follow the detailed configuration process in User Identification on page 185.

7 Repeat step 1 through step 5 until you see the expected result when signing in to the NNMi console.

8 After you can log on, choose your strategy:

- If you plan to store NNMi user group membership in the NNMi database (configuration option 2), continue with Task 9 on page 177.
- If you plan to store NNMi user group membership in the directory service (configuration option 3), continue with Task 5, next.

Task 5: (Configuration Option 3 only) Configure Group Retrieval from the Directory Service

Complete this task for configuration option 3. Follow the appropriate procedure for your directory service. This task includes the following sections:

- Simple Approach for Microsoft Active Directory
- Simple Approach for Other Directory Services

(For detailed configuration instructions, see User Group Identification on page 188.)

Simple Approach for Microsoft Active Directory

1 Back up the ldap.properties file, and then open the file in any text editor.

2 Specify the portion of the directory service domain that stores group records. In the following line:

```
#rolesCtxDN=CN=Users,DC=<myhostname>,DC=<mycompanyname>,
  DC=<mysuffix>
```

Do the following:

- Uncomment the line (by deleting the # character).

- Replace *<myhostname>*, *<mycompanyname>*, and *<mysuffix>* with the components of the fully-qualified hostname of the Active Directory server (for example, for the hostname `myserver.example.com`, specify: `DC=myserver,DC=example,DC=com`).

Simple Approach for Other Directory Services

1. Back up the `ldap.properties` file, and then open the file in any text editor.
2. Specify the portion of the directory service domain that stores group records. In the following line:

   ```
   #rolesCtxDN=ou=Groups,o=myco.com
   ```

   Do the following:

   - Uncomment the line (by deleting the # character).
   - Replace `ou=Groups,o=myco.com` with the portion of the directory service domain that stores group records.
3. Specify the format of group member names in the directory service group definitions. In the following line:

   ```
   roleFilter=member={1}
   ```

   Replace `member` with the name of the group attribute that stores the directory service user ID in the directory service domain.

Task 6: (Configuration Option 3 only) Map the Directory Service Groups to NNMi User Groups

1. In the NNMi console, map the predefined NNMi user groups to their counterparts in the directory service:
   1. Open the **User Groups** view.

      In the **Configuration** workspace, expand **Security**, and then **click User Groups**.
   2. Double-click the **admin** row.
   3. In the **Directory Service Name** field, enter the full distinguished name of the directory service group for NNMi administrators.
   4. Click **Save and Close**.
   5. Repeat step b through step d for each of the **guest**, **level1**, and **level2** rows.

   These mappings provide NNMi console access. Every user who will access the NNMi console must be in a directory service group that is mapped to one of the predefined NNMi user groups named in this step.

2. For other groups containing one or more NNMi users in the directory service, create a new user group in the NNMi console:
   1. Open the **User Groups** view.

      In the **Configuration** workspace, expand **Security**, and then **click User Groups**.
   2. Click **New**, and then enter the information for the group:
      - Set **Unique Name** to any unique value. Short names are recommended.
      - Set **Display Name** to the value users should see.
      - Set **Directory Service Name** to the full distinguished name of the directory service group.

— Set **Description** to text that describes the purpose of this NNMi user group.

c Click **Save and Close**.

d Repeat step b and step c for each additional directory service group of NNMi users.

These mappings provide topology object access in the NNMi console. Each directory service group can be mapped to multiple NNMi user groups.

Task 7: (Configuration Option 3 only) Test the NNMi User Group Configuration

1 Save the `ldap.properties` file.

2 Force NNMi to re-read the `ldap.properties` file by running the following command:

```
nnmldap.ovpl -reload
```

3 Log on to the NNMi console with a user name and password that are defined in the directory service.

Run this test with a user name that is not already defined in the NNMi database and is a member of a directory service group that is mapped to the admin, level1, or level2 NNMi user group.

4 Verify the user name and NNMi role (as configured in the **Display Name** field in the **User Group** view) in the title bar of the NNMi console.

- If user signin works correctly, continue with Task 8 on page 176.
- If user signin does not work correctly, continue with step 5, next.

After each test, sign out of the NNMi console to clear the session credentials.

5 Test the configuration for one user by running the following command:

```
nnmldap.ovpl -diagnose <NNMi_user>
```

Replace *<NNMi_user>* with the sign-in name of an NNMi user as defined in the directory service.

Examine the command output and respond appropriately. Suggestions include:

- Verify that you completed Task 5 on page 174 correctly.
- Verify that you completed Task 6 on page 175 correctly for each of the predefined NNMi user groups.
- Follow the detailed configuration process in User Group Identification on page 188.

6 Repeat step 1 through step 4 until you see the expected result when signing in to the NNMi console.

Task 8: (Configuration Option 3 only) Configure NNMi User Groups for Incident Assignment

1 Back up the `ldap.properties` file, and then open the file in any text editor.

2 Modify the `userRoleFilterList` parameter value to specify the NNMi roles to which NNMi operators can assign incidents.

The format is a semicolon-separated list of the unique names for one or more of the predefined NNMi user group names (as defined in Table 10 on page 188).

3 Save the `ldap.properties` file.

4 Force NNMi to re-read the `ldap.properties` file by running the following command:

```
nnmldap.ovpl -reload
```

5 Log on to the NNMi console with a user name and password that are defined in the directory service.

6 In any incident view, select an incident, and then click **Actions > Assign > Assign Incident**. Verify that you can assign the incident to a user in each of the NNMi roles specified by the `userRoleFilterList` parameter.

7 Repeat step 1 through step 6 until you can assign an incident to each configured NNMi role.

Task 9: Clean up to Prevent Unexpected Access to NNMi

1 Optional. Change the value of, or comment out, the `defaultRole` parameter in the `ldap.properties` file.

2 (Configuration Option 2 only) To store user group membership in the NNMi database, reset the user access information in the NNMi database as follows:

a Remove any pre-existing user access information. (Delete all rows in the **User Accounts** view.)

For instructions, see *Delete a User Account* in the NNMi help.

b For each NNMi user, create a new object in the **User Accounts** view for the user name.

— For the **Name** field, enter the user name as defined in the directory service.

— Select the **Directory Service Account** check box.

— Do not specify a password.

For more information, see *User Account Tasks* in the NNMi help.

c For each NNMi user, map the user account to one or more NNMi user groups.

For instructions, see *User Account Mapping Tasks* in the NNMi help.

d Update incident ownership so that each assigned incident is associated with a valid user name.

For instructions, see *Manage Incident Assignments* in the NNMi help.

3 (Configuration Option 3 only) To rely on the user group membership in the directory service, reset the user access information in the NNMi database as follows:

a Remove any pre-existing user access information. (Delete all rows in the **User Accounts** view.)

For instructions, see *Delete a User Account* in the NNMi help.

b Update incident ownership so that each assigned incident is associated with a valid user name.

For instructions, see *Manage Incident Assignments* in the NNMi help.

Task 10: Optional. Map the User Groups to Security Groups

For instructions, see *Security Group Mapping Tasks* in the NNMi help.

Changing the Directory Service Access Configuration to Support the NNMi Security Model

The information in this section describes how to revise an `ldap.properties` file from NNMi 8.1x or 9.0x to support multiple NNMi user groups per user. This revision is necessary under *both* of the following conditions:

- The `ldap.properties` file currently enables NNMi user access configuration option 3 (all NNMi user information in the directory service).
- NNMi has been or will be configured with custom security groups.

In NNMi 8.1x and 9.0x, NNMi users were assigned to one of the predefined NNMi roles. Each user had access to all objects in the NNMi topology.

In NNMi 9.10, the predefined NNMi user groups replace NNMi roles. Each NNMi user must belong to at least one predefined NNMi user group, which defines what an NNMi user can do in the NNMi console. Additional user groups, if they exist, limit access to NNMi topology objects as follows:

- If no custom user groups exist, all NNMi console users can access all topology objects.
- If one or more custom user groups exist, each of these user groups provide access to a subset of objects in the NNMi topology.

NNMi 8.1x and 9.0x required each directory service group definition to include a group attribute that named the NNMi role. In the `ldap.properties` configuration file, the following parameters specified this group attribute:

- `roleAttributeID`
- `roleAttributeIsDN`
- `roleNameAttributeID`

NNMi 9.10 deprecates these parameters. They will become unsupported in a future release.

In NNMi 9.10, each user group must be defined in the NNMi console. The user group definition includes an external name, which is the distinguished name of the group in the directory service.

To change the directory service access configuration to support the NNMi security model, follow these steps:

1 Back up the user information in the NNMi database:

```
nnmconfigexport.ovpl -c account -u <user> \
-p <password> -f NNMi_database_accounts.xml
```

2 Back up the `ldap.properties` file, and then open the file in any text editor.

For information about the `ldap.properties` file, see ldap.properties Configuration File Reference on page 192. For information about the deprecated parameters, see the *NNMi Deployment Reference* for the previous version of NNMi.

3 Comment out or delete the following parameters (if they exist):

- `roleAttributeID`
- `roleAttributeIsDN`
- `roleNameAttributeID`

The `roleAttributeID` parameter is the flag that tells NNMi which method to use for identifying NNMi user groups. When `roleAttributeID` is set, NNMi uses the NNMi 8.1x and 9.0x approach. When `roleAttributeID` is not set, NNMi uses the NNMi 9.10 approach.

4 In the NNMi console, map the predefined NNMi user groups to their counterparts in the directory service:

a Open the **User Groups** view.

In the **Configuration** workspace, expand **Security**, and then **click User Groups**.

b Double-click the **admin** row.

c In the **Directory Service Name** field, enter the full distinguished name of the directory service group for NNMi administrators.

d Click **Save and Close**.

e Repeat step b through step d for each of the **guest**, **level1**, and **level2** rows.

These mappings provide NNMi console access. Every user who will access the NNMi console must be in a directory service group that is mapped to one of the predefined NNMi user groups named in this step.

5 In the directory service, identify additional groups of NNMi users. Define new groups as needed.

6 For each new group added in step 5, create a new user group in the NNMi console:

a Open the **User Groups** view.

In the **Configuration** workspace, expand **Security**, and then **click User Groups**.

b Click **New**, and then enter the information for the group:

— Set **Unique Name** to any unique value. Short names are recommended.

— Set **Display Name** to the value users should see.

— Set **Directory Service Name** to the full distinguished name of the directory service group.

— Set **Description** to text that describes the purpose of this NNMi user group.

c Click **Save and Close**.

d Repeat step b and step c for each new directory service group of NNMi users.

These mappings provide topology object access in the NNMi console. Each directory service group can be mapped to multiple NNMi user groups.

7 Optional. Map the user groups to security groups.

For information, see *Configuring Security* in the NNMi help.

Directory Service Queries

NNMi uses LDAP to communicate with a directory service. NNMi sends a request, and the directory service returns stored information. NNMi cannot alter the information that is stored in the directory service.

This section contains the following topics:

- Directory Service Access
- Directory Service Content
- Information Owned by the Directory Service Administrator
- User Identification
- User Group Identification

Directory Service Access

LDAP queries to a directory service use the following format:

ldap://<*directory_service_host*>:<*port*>/<*search_string*>

- `ldap` is the protocol indicator. Use this indicator for both standard connections and SSL connections to the directory service.
- <*directory_service_host*> is the fully-qualified name of the computer that hosts the directory service.
- <*port*> is the port that the directory service uses for LDAP communication. The default port for non-SSL connections is 389. The default port for SSL connections is 636.
- <*search_string*> contains the information request. For more information, see Directory Service Content and RFC 1959, *An LDAP URL Format*, which is available at:
  labs.apache.org/webarch/uri/rfc/rfc1959.txt

You can enter an LDAP query as a URL in a web browser to verify that you have the correct access information and the correct structure for the search string.

If the directory service (for example, Active Directory) does not permit anonymous access, the directory service denies LDAP queries from a web browser. In this case, you can use a third-party LDAP browser (for example, the LDAP browser included in Apache Directory Studio) to validate your configuration parameters.

Directory Service Content

A directory service stores information such as user names, passwords, and group membership. To access the information in a directory service, you must know the distinguished name that references the storage location of the information. For sign-in applications, the distinguished name is a combination of variable information (such as a user name) and fixed information (such as the storage location of user names). The elements that make up a distinguished name depend on the structure and content of the directory service.

The following examples show possible definitions for a group of users called USERS-NNMi-Admin. This group lists the directory service user IDs that have administrative access to NNMi. The following information pertains to these examples:

- The Active Directory example is for the Windows operating system.
- The other directory services example is for UNIX operating systems.
- The file shown in each example is a portion of a lightweight directory interchange format (LDIF) file. LDIF files provide for sharing directory service information.
- The figure shown in each example is a graphical representation of the directory service domain that provides an expanded view of the information in the LDIF file excerpt.

Example content structure for Active Directory

In this example, the following items are of interest:

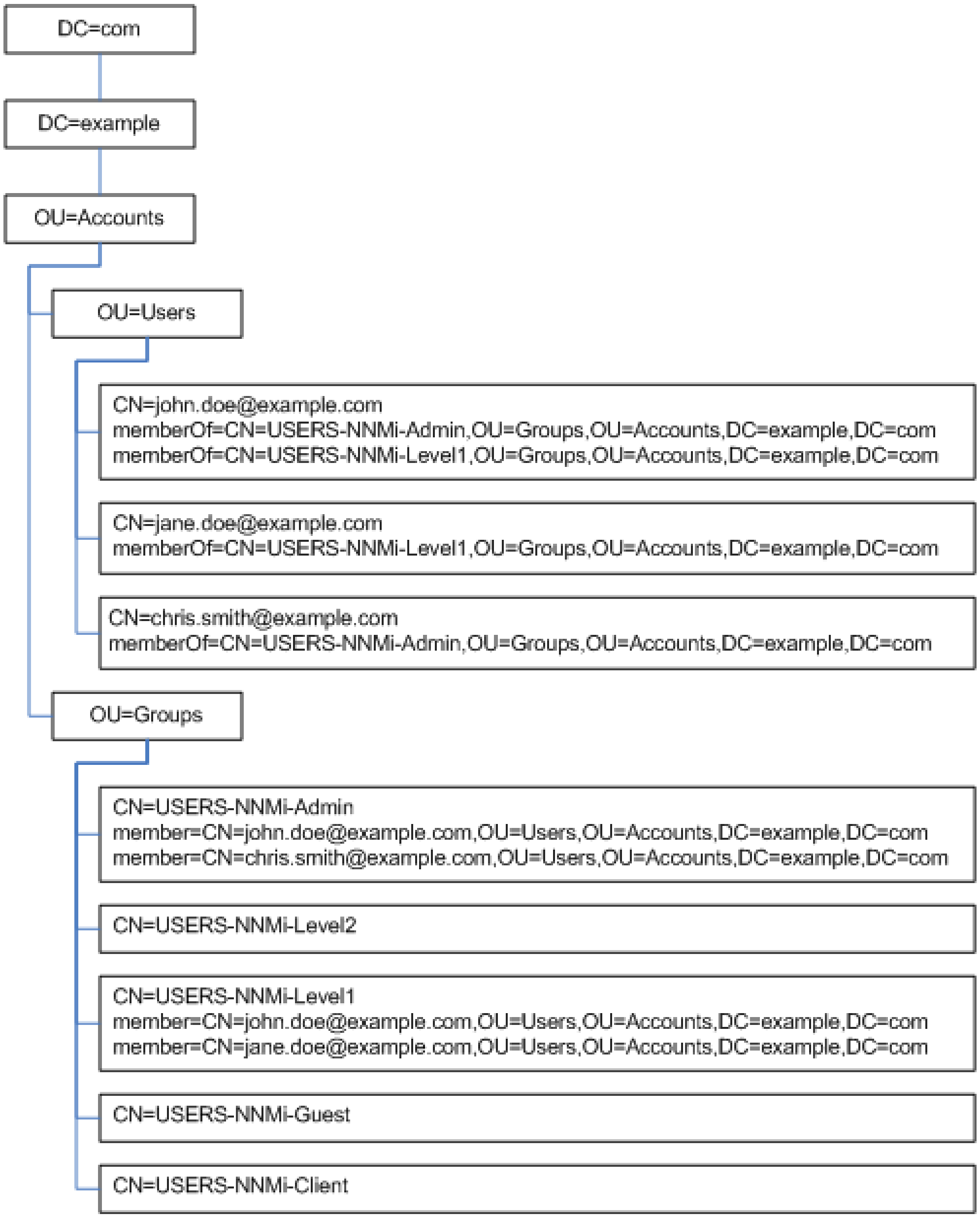
- The distinguished name of the user John Doe is: `CN=john.doe@example.com,OU=Users,OU=Accounts,DC=example,DC=com`
- The distinguished name of the group USERS-NNMi-Admin is: `CN=USERS-NNMi-Admin,OU=Groups,OU=Accounts,DC=example,DC=com`
- The group attribute that stores the directory service user ID is: `member`

Example LDIF file excerpt:

```
groups |USERS-NNMi-Admin
dn: CN=USERS-NNMi-Admin,OU=Groups,OU=Accounts,DC=example,DC=com
cn: USERS-NNMi-Admin
description: Group of users for NNMi administration.
member: CN=john.doe@example.com,OU=Users,OU=Accounts,
  DC=example,DC=com
member: CN=chris.smith@example.com,OU=Users,OU=Accounts,
  DC=example,DC=com
```

Figure 11 on page 182 illustrates this directory service domain.

Figure 11 Example Domain for Active Directory


DC=com
DC=example
OU=Accounts
OU=Users
CN=john.doe@example.com
memberOf=CN=USERS-NNMi-Admin,OU=Groups,OU=Accounts,DC=example,DC=com
memberOf=CN=USERS-NNMi-Level1,OU=Groups,OU=Accounts,DC=example,DC=com
CN=jane.doe@example.com
memberOf=CN=USERS-NNMi-Level1,OU=Groups,OU=Accounts,DC=example,DC=com
CN=chris.smith@example.com
memberOf=CN=USERS-NNMi-Admin,OU=Groups,OU=Accounts,DC=example,DC=com
OU=Groups
CN=USERS-NNMi-Admin
member=CN=john.doe@example.com,OU=Users,OU=Accounts,DC=example,DC=com
member=CN=chris.smith@example.com,OU=Users,OU=Accounts,DC=example,DC=com
CN=USERS-NNMi-Level2
CN=USERS-NNMi-Level1
member=CN=john.doe@example.com,OU=Users,OU=Accounts,DC=example,DC=com
member=CN=jane.doe@example.com,OU=Users,OU=Accounts,DC=example,DC=com
CN=USERS-NNMi-Guest
CN=USERS-NNMi-Client

Example content structure for other directory services

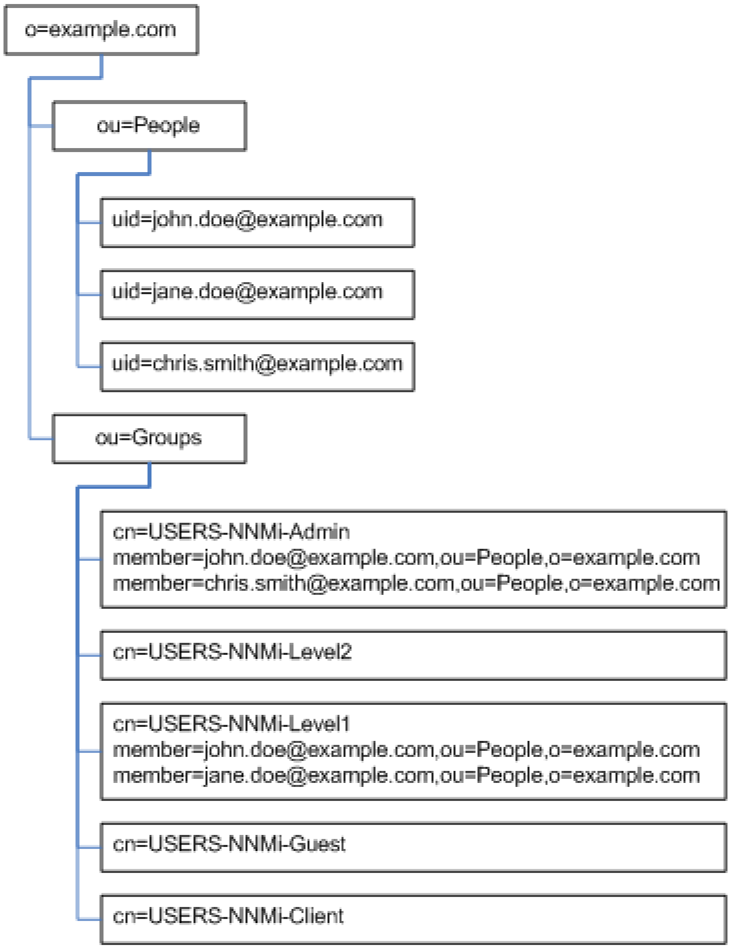
In this example, the following items are of interest:

- The distinguished name of the user John Doe is: `uid=john.doe@example.com,ou=People,o=example.com`
- The distinguished name of the group USERS-NNMi-Admin is: `cn=USERS-NNMi-Admin,ou=Groups,o=example.com`
- The group attribute that stores the directory service user ID is: `member`

Example LDIF file excerpt:

```
groups |USERS-NNMi-Admin
dn: cn=USERS-NNMi-Admin,ou=Groups,o=example.com
cn: USERS-NNMi-Admin
description: Group of users for NNMi administration.
member: uid=john.doe@example.com,ou=People,o=example.com
member: uid=chris.smith@example.com,ou=People,o=example.com
```

Figure 12 Example Domain for Other Directory Services


o=example.com
ou=People
uid=john.doe@example.com
uid=jane.doe@example.com
uid=chris.smith@example.com
ou=Groups
cn=USERS-NNMi-Admin
member=john.doe@example.com,ou=People,o=example.com
member=chris.smith@example.com,ou=People,o=example.com
cn=USERS-NNMi-Level2
cn=USERS-NNMi-Level1
member=john.doe@example.com,ou=People,o=example.com
member=jane.doe@example.com,ou=People,o=example.com
cn=USERS-NNMi-Guest
cn=USERS-NNMi-Client

Information Owned by the Directory Service Administrator

Table 8 and Table 9 list the information to obtain from the directory service administrator before configuring NNMi for LDAP access to a directory service.

- If you plan to use the directory service for user names and passwords only (configuration option 2), gather the information for Table 8.
- If you plan to use the directory service for all NNMi access information (configuration option 3), gather the information for Table 8 and Table 9.

Table 8 Information for Retrieving User Names and Passwords from a Directory Service

Information	Active Directory Example	Other Directory Services Example
The fully-qualified name of the computer that hosts the directory service	`directory_service_host.example.com`	
The port that the directory service uses for LDAP communication	• 389 for non-SSL connections • 636 for SSL connections	
Does the directory service require an SSL connection?	If yes, obtain a copy of your company's trust store certificate and see Configuring an SSL Connection to the Directory Service on page 134.	
The distinguished name for one user name that is stored in the directory service (to demonstrate the directory service domain)	`CN=john.doe@example.com, OU=Users,OU=Accounts, DC=example,DC=com`	`uid=john.doe@example.com, ou=People,o=example.com`

Table 9 Information for Retrieving Group Membership from a Directory Service

Information	Active Directory Example	Other Directory Services Example
The distinguished name for identifying the groups to which a user is assigned	The `memberOf` user attribute identifies the groups.	• `ou=Groups,o=example.com` • `cn=USERS-NNMi-*, ou=Groups,o=example.com`
The method of identifying a user within a group	• `CN=john.doe@example.com, OU=Users,OU=Accounts, DC=example,DC=com` • `CN=john.doe@example.com`	• `cn=john.doe@example.com, ou=People,o=example.com` • `cn=john.doe@example.com`
The group attribute that stores the directory service user ID	`member`	`member`

Table 9 Information for Retrieving Group Membership from a Directory Service (cont'd)

Information	Active Directory Example	Other Directory Services Example
The names of the groups in the directory service that apply to NNMi access	• `CN=USERS-NNMi-Admin, OU=Groups,OU=Accounts, DC=example,DC=com` • `CN=USERS-NNMi-Level2, OU=Groups,OU=Accounts, DC=example,DC=com` • `CN=USERS-NNMi-Level1, OU=Groups,OU=Accounts, DC=example,DC=com` • `CN=USERS-NNMi-Client, OU=Groups,OU=Accounts, DC=example,DC=com` • `CN=USERS-NNMi-Guest, OU=Groups,OU=Accounts, DC=example,DC=com`	• `cn=USERS-NNMi-Admin, ou=Groups,o=example.com` • `cn=USERS-NNMi-Level2, ou=Groups,o=example.com` • `cn=USERS-NNMi-Level1, ou=Groups,o=example.com` • `cn=USERS-NNMi-Client, ou=Groups,o=example.com` • `cn=USERS-NNMi-Guest, ou=Groups,o=example.com`

User Identification

User identification applies to configuration options 2 and 3.

The distinguished name for user identification is the fully-qualified method of locating one user in the directory service. NNMi passes the user distinguished name in an LDAP request to the directory service.

In the `ldap.properties` file, the user distinguished name is the concatenation of the `baseFilter` value and the `baseCtxDN` value. If the password returned by the directory service matches the sign-in password the user entered into the NNMi console, user signin continues.

For configuration option 2, the following information applies:

- For NNMi console access, NNMi examines the following information and grants the user the highest possible privileges:
  - The value of the `defaultRole` parameter in the `ldap.properties` file
  - This user's membership in the predefined NNMi user groups in the NNMi console
- For NNMi topology object access, NNMi grants access according to the security group mappings for the NNMi user groups to which this user belongs in the NNMi console.

For configuration option 3, the following information applies:

- For NNMi console access, NNMi examines the following information and grants the user the highest possible privileges:
  - The value of the `defaultRole` parameter in the `ldap.properties` file
  - This user's membership in the directory service groups that are mapped (with the **Directory Service Name** field) to the predefined NNMi user groups in the NNMi console

- For NNMi topology object access, NNMi grants access according to the security group mappings for the groups to which this user belongs in the directory service (as mapped to NNMi user groups in the NNMi console).

Active Directory user identification example

If `baseFilter` is set to `CN={0}`, `baseCtxDN` is set to `OU=Users,OU=Accounts,DC=example,DC=com`, and a user signs in to NNMi as `john.doe`, the string passed to the directory service is:

```
CN=john.doe,OU=Users,OU=Accounts,DC=example,DC=com
```

Other directory services user identification example

If `baseFilter` is set to `uid={0}@example.com`, `baseCtxDN` is set to `ou=People,o=example.com`, and a user signs in to NNMi as `john.doe`, the string passed to the directory service is:

```
uid=john.doe@example.com,ou=People,o=example.com
```

Configuring NNMi User Access from the Directory Service (Detailed Approach)

If the simple approach described in Task 3 on page 172 did not work correctly, follow these steps:

1 Obtain the information listed in Table 8 on page 184 from the directory service administrator.

2 Verify the format of user names in the directory service by completing the appropriate procedure:

  - *LDAP browser approach for Active Directory and other directory services*: See Determining How the Directory Service Identifies a User (LDAP Browser Approach) on page 187.
  - *Web browser approach for other directory services*: See Determining How the Directory Service Identifies a User (Web Browser Approach) on page 187.

3 Open the `ldap.properties` file in any text editor.

For information about the `ldap.properties` file, see ldap.properties Configuration File Reference on page 192.

4 Set the `java.naming.provider.url` parameter to the URL for accessing the directory service through LDAP.

  - *LDAP browser approach*: Obtain this information from the LDAP browser configuration.
  - *Web browser approach*: Include the values of <*directory_service_host*> and <*port*> from Determining How the Directory Service Identifies a User (Web Browser Approach) on page 187.

To specify multiple directory service URLs, separate each URL with a single space character.

5 If you configured secure communications to the directory service, uncomment (or add) the following line:

```
java.naming.security.protocol=ssl
```

6 (Active Directory only) Set the `bindDN` and `bindCredential` parameters as follows:

- Replace *<mydomain>* with the name of Active Directory domain.
- Replace *<myusername>* and *<mypassword>* with a user name and password for accessing the Active Directory server.
  If you plan to add the password in plain text, specify a user name with read-only access to the directory service.
  If you plan to specify an encrypted password, use the following command to encrypt the plain text password before adding it to the `ldap.properties` file:
  `nnmldap.ovpl -encrypt <`*`mypassword`*`>`

  This encrypted password only works for the NNMi instance you create it for. Do not attempt to use it for a different NNMi instance.

  For more information see the *nnmldap.ovpl* reference page, or the UNIX manpage.

7 Set the `baseCtxDN` parameter to the elements of the distinguished user name that are the same for multiple users.

8 Set the `baseFilter` parameter to correlate user names as they are entered for NNMi signin to the way user names are stored in the directory service.

This value is the element of the distinguished user name that changes for each user. Replace the actual user name with the expression `{0}`.

9 Test the configuration as described in Task 4 on page 173.

Determining How the Directory Service Identifies a User (LDAP Browser Approach)

In a third-party LDAP browser, do the following:

1 Navigate to the portion of the directory service domain that stores group information.

2 Identify a group of users, and then examine the format of the distinguished names for the users associated with that group.

Determining How the Directory Service Identifies a User (Web Browser Approach)

1 In a supported web browser, enter the following URL:

ldap://*<directory_service_host>*:*<port>*/*<user_search_string>*

- *<directory_service_host>* is the fully-qualified name of the computer that hosts the directory service.
- *<port>* is the port that the directory service uses for LDAP communication.
- *<user_search_string>* is the distinguished name for one user name that is stored in the directory service.

2 Evaluate the results of the directory service access test.

- If the request times out or you see a message that the directory service could not be reached, verify the values of *<directory_service_host>* and *<port>*, and then repeat step 1.
- If you see a message that the directory service does not contain the requested entry, verify the value of *<user_search_string>*, and then repeat step 1.
- If you see the appropriate user record, the access information is correct. The value of *<user_search_string>* is the distinguished user name.

User Group Identification

User group identification applies to configuration option 3.

NNMi determines the user groups for an NNMi user as follows:

1 NNMi compares the values of the external names of all user groups configured in the NNMi console with the names of the directory service groups.

2 For any user group match, NNMi then determines whether the NNMi user is a member of that group in the directory service.

In the NNMi console, short text strings identify the unique names of the predefined NNMi user groups that grant NNMi console access. These text strings are also required by the `defaultRole` and `userRoleFilterList` parameters in the `ldap.properties` configuration file. Table 10 maps the unique names of these groups to their display names.

Table 10 NNMi User Group Name Mappings

NNMi Role Name in the NNMi Console	User Group Unique Name and Text String in NNMi Configuration Files
Administrator	`admin`
Operator Level 2	`level2`
Operator Level 1	`level1`
Guest	`guest`
Web Service Client	`client`

Configuring User Group Retrieval from the Directory Service (Detailed Approach)

If the simple approach described in Task 5 on page 174 did not work correctly, follow these steps:

1 Obtain the information listed in Table 9 on page 184 from the directory service administrator.

2 Verify the format of group names and group members in the directory service by completing the appropriate procedure:

- *LDAP browser approach for Active Directory*: See Determining How the Directory Service Identifies a Group and Group Membership (LDAP Browser Approach for Active Directory) on page 189.
- *LDAP browser approach for other directory services*: See Determining How the Directory Service Identifies a Group and Group Membership (LDAP Browser Approach for Other Directory Services) on page 189.
- *Web browser approach for other directory services*: See Determining How the Directory Service Identifies a Group (Web Browser Approach) on page 189.

3 Open the `ldap.properties` file in any text editor.

For information about the `ldap.properties` file, see ldap.properties Configuration File Reference on page 192.

4 Set the `rolesCtxDN` parameter to the elements of the distinguished group name that are the same for multiple groups.

5 Set the `roleFilter` parameter to correlate user names to the way user names are stored for groups in the directory service. Replace the actual user name with one of the following expressions:

- Use `{0}` to denote the user name entered for signin (for example, `john.doe`).
- Use `{1}` to denote the distinguished name of the authenticated user as returned by the directory service (for example, `uid=john.doe@example.com,ou=People,o=example.com`).

6 Set the `uidAttributeID` parameter to the name of the group attribute that stores the user ID.

7 Test the configuration as described in Task 7 on page 176.

Determining How the Directory Service Identifies a Group and Group Membership (LDAP Browser Approach for Active Directory)

In a third-party LDAP browser, do the following:

1 Navigate to the portion of the directory service domain that stores user information.

2 Identify a user who requires access to NNMi, and then examine the format of the distinguished names for the groups associated with that user.

3 Navigate to the portion of the directory service domain that stores group information.

4 Identify the groups that correspond to NNMi user groups, and then examine the format of the names for the users associated with a group.

Determining How the Directory Service Identifies a Group and Group Membership (LDAP Browser Approach for Other Directory Services)

In a third-party LDAP browser, do the following:

1 Navigate to the portion of the directory service domain that stores group information.

2 Identify the groups that correspond to NNMi user groups, and then examine the format of the distinguished names for those groups.

3 Also examine the format of the names for the users associated with a group.

Determining How the Directory Service Identifies a Group (Web Browser Approach)

1 In a supported web browser, enter the following URL:

ldap://<*directory_service_host*>:<*port*>/<*group_search_string*>

- <*directory_service_host*> is the fully-qualified name of the computer that hosts the directory service.
- <*port*> is the port that the directory service uses for LDAP communication.
- <*group_search_string*> is the distinguished name for a group name that is stored in the directory service, for example: `cn=USERS-NNMi-Admin,ou=Groups,o=example.com`

2 Evaluate the results of the directory service access test.

   - If you see a message that the directory service does not contain the requested entry, verify the value of <*group_search_string*>, and then repeat step 1.
   - If you see the appropriate list of groups, the access information is correct.

3 Examine the group properties to determine the format of the names for the users associated with that group.

Directory Service Configuration for Storing NNMi User Groups

If you plan to store NNMi user groups in the directory service (configuration option 3), the directory service must be configured with NNMi user group information. Ideally, the directory service already contains appropriate user groups. If this is not the case, the directory service administrator can create new user groups specifically for NNMi user group assignment.

Because directory service configuration and maintenance procedures depend on the specific directory service software and your company's policies, those procedures are not documented here.

Troubleshooting the Directory Service Integration

1 Verify the NNMi LDAP configuration by running the following command:

```
nnmldap.ovpl -info
```

If the reported configuration is not as expected, verify the settings in the `ldap.properties` file.

2 Force NNMi to re-read the `ldap.properties` file by running the following command:

```
nnmldap.ovpl -reload
```

3 Test the configuration for one user by running the following command:

```
nnmldap.ovpl -diagnose <NNMi_user>
```

Replace <*NNMi_user*> with the sign-in name of an NNMi user as defined in the directory service.

Examine the command output and respond appropriately.

4 Verify that the directory service contains the expected records. Use a web browser or a third-party LDAP browser (for example, the LDAP browser included in Apache Directory Studio) to examine the directory service information.

Information about the format of a query to a directory service can be found in RFC 1959, *An LDAP URL Format*, which is available at:

http://labs.apache.org/webarch/uri/rfc/rfc1959.txt

5 View the `%NnmDataDir%\log\nnm\jbossServer.log` or (*Windows*) or `/var/opt/OV/log/nnm/jbossServer.log` (*UNIX*) log file to verify that the sign-in request is correct, and to determine if any errors occurred:

- A message similar to the following line indicates that the directory service requires HTTPS communication. In this case, enable SSL as described in Configuring an SSL Connection to the Directory Service on page 134.

  ```
  javax.naming.AuthenticationNotSupportedException: [LDAP:
  error code 13 - confidentiality required]
  ```

- A message similar to the following line indicates that a timeout occurred while communicating with the directory service. In this case, increase the value of `searchTimeLimit` in the `nms-ldap.properties` file.

  ```
  javax.naming.TimeLimitExceededException: [LDAP: error code 3
  - Timelimit Exceeded]
  ```

ldap.properties Configuration File Reference

The ldap.properties file contains the settings for communicating with and building LDAP queries to the directory service. This file is located as follows:

- *Windows*: %NNM_SHARED_CONF%\ldap.properties
- *UNIX*: $NNM_SHARED_CONF/ldap.properties

In the ldap.properties file, the following conventions apply:

- To comment out a line, begin that line with a number sign character (#).
- The following rules apply to special characters:
  - To specify a backslash character (\), comma (,), semicolon (;), plus sign (+), less than sign (<), or greater than sign (>), escape the character with a backslash character. For example: \\ or \+
  - To include a space character ( ) as the *first* or *last* character in a string, escape the space character with a backslash character (\).
  - To include a number sign character (#) as the *first* character in a string, escape the number sign character with a backslash character (\).

  Characters not mentioned here do not need to be escaped or quoted.

After editing the ldap.properties file, force NNMi to re-read the LDAP configuration by running the following command:

```
nnmldap.ovpl -reload
```

Table 11 describes the parameters in the ldap.properties file.

The initial ldap.properties file might not include all parameters that are listed in Table 11. Add the parameters you need.

Table 11 Parameters in the ldap.properties File

Parameter	Description

java.naming.provider.url	Specifies the URL for accessing the directory service.
	The format is the protocol (ldap), followed by the fully-qualified host name of the directory server, optionally followed by the port number. For example:
	`java.naming.provider.url=ldap://ldap.example.com:389/`
	If the port number is omitted the following defaults apply:
	• For non-SSL connections, the default port is 389.
	• For SSL connections, the default port is 636.
	If you specify multiple directory service URLs, NNMi uses the first directory service when possible. If that directory service is not accessible, NNMi queries the next directory service in the list, and so forth. Separate each URL with a single space character. For example:
	`java.naming.provider.url=ldap://ldap1.example.com/ ldap://ldap2.example.com/`
	Configuring this parameter enables LDAP communication between NNMi and the directory service. To disable LDAP communication, comment out this parameter, and then save the file. NNMi ignores the configuration in the ldap.properties file.

Table 11 Parameters in the ldap.properties File (cont'd)

Parameter	Description
java.naming.security.protocol	Specifies the connection protocol specification. • If the directory service is configured to use LDAP over SSL, set this parameter to `ssl`. For example: `java.naming.security.protocol=ssl` • If the directory service does not require SSL, leave this parameter commented out. For more information, see Configuring an SSL Connection to the Directory Service on page 134.
bindDN	For a directory service (such as Active Directory) that does not permit anonymous access, specify the user name for accessing the directory service. For example: `bindDN=region1\\john.doe@example.com` • If you plan to add the password in plain text, specify a user name with read-only access to the directory service. For example: `bindCredential=PasswordForJohnDoe` • If you plan to specify an encrypted password, use the following command to encrypt the plain text password before adding it to the `ldap.properties` file: **`nnmldap.ovpl -encrypt <mypassword>`** For example: `bindCredential={ENC}uaF22C+0CF9VozBVYj8OAw==` This encrypted password only works for the NNMi instance you create it for. Do not attempt to use it for a different NNMi instance. For more information see the *nnmldap.ovpl* reference page, or the UNIX manpage.
bindCredential	When `bindDN` is set, specifies the password for the user name that `bindDN` identifies. For example: `bindCredential=PasswordForJohnDoe`
baseCtxDN	Specifies the portion of the directory service domain that stores user records. The format is a comma-separated list of directory service attribute names and values. For example: • `baseCtxDN=CN=Users,DC=ldapserver,DC=example,DC=com` • `baseCtxDN=ou=People,o=example.com` For more information, see User Identification on page 185.

Table 11 Parameters in the ldap.properties File (cont'd)

Parameter	Description
baseFilter	Specifies the format of user names for signing in to NNMi. The format is the name of the directory service user name attribute and a string that relates the entered user sign-in name to the format of names in the directory service. The user name string contains the expression `{0}` (to denote the user name entered for signin) and any other characters that are needed to match the directory service formatting of user names. • If the user name entered for NNMi signin is the same as the user name stored in the directory service, the value is the replacement expression. For example: — `baseFilter=CN={0}` — `baseFilter=uid={0}` • If the user name entered for NNMi signin is as subset of the user name stored in the directory service, include the additional characters in the value. For example: — `baseFilter=CN={0}@example.com` — `baseFilter=uid={0}@example.com` For more information, see User Identification on page 185.
defaultRole	Optional. Specifies a default role that applies to any directory service user who signs in to NNMi through LDAP. The value of this parameter applies regardless of where user group mappings are stored (in the NNMi database or in the directory service). If a user is directly configured for a predefined NNMi user group, NNMi grants the user the superset of privileges for the default role and the assigned user group. Valid values are as follows: `admin`, `level2`, `level1`, or `guest`. These names are the unique names of the predefined NNMi user group names (as defined in Table 10 on page 188). For example: `defaultRole=guest` If commented out or omitted, NNMi does not use a default role.

Table 11 Parameters in the ldap.properties File (cont'd)

Parameter	Description
rolesCtxDN	Specifies the portion of the directory service domain that stores group records. The format is a comma-separated list of directory service attribute names and values. For example: • `rolesCtxDN=CN=Users,DC=ldapserver,DC=example,DC=com` • `rolesCtxDN=ou=Groups,o=example.com` In other directory services (not Active Directory), for a faster search, you can identify one or more directory service groups that contain NNMi user groups. If the group names form a pattern, you can specify a wildcard. For example, if the directory service includes groups named `USERS-NNMi-administrators`, `USERS-NNMi-level1Operators`, and so forth, you could use a search context similar to: `rolesCtxDN=cn=USERS-NNMi-*,ou=Groups,o=example.com` Configuring this parameter enables directory service queries for NNMi user group assignments through LDAP. To disable directory service queries for NNMi user group assignments through LDAP, comment out this parameter, and then save the file. NNMi ignores the remaining user group-related values in the `ldap.properties` file. For more information, see User Group Identification on page 188.

roleFilter	Specifies the format of group member names in the directory service group definitions.
	The format is the name of the directory service group attribute for user ID and a string that relates the entered user sign-in name to the format of user IDs in the directory service. The user name string contains one of the following expressions and any other characters that are needed to match the directory service formatting of group member names.
	• The expression `{0}` denotes the user name entered for signin (for example, `john.doe`).
	An example role filter that matches on the (short) user name entered for signin is:
	`roleFilter=member={0}`
	• The expression `{1}` denotes the distinguished name of the authenticated user as returned by the directory service (for example,
	`CN=john.doe@example.com,OU=Users,OU=Accounts,`
	`DC=example,DC=com`
	or
	`uid=john.doe@example.com,ou=People,o=example.com`).
	An example role filter that matches on the (full) authenticated user name is:
	`roleFilter=member={1}`
	For more information, see User Group Identification on page 188.

uidAttributeID	Specifies the group attribute that stores the directory service user ID. For example: `uidAttributeID=member` For more information, see User Group Identification on page 188.

Table 11 Parameters in the ldap.properties File (cont'd)

Parameter	Description
userRoleFilterList	Optional. Limits the NNMi user groups whose associated users can be assigned incidents in the NNMi console. The user groups in this list apply only to directory service user names authenticated through LDAP. This parameter provides functionality that is not available when NNMi user groups are assigned in the NNMi console and stored in the NNMi database. The format is a semicolon-separated list of the unique names for one or more predefined NNMi user group names (as defined in Table 10 on page 188). `userRoleFilterList=admin;level2;level1`
searchTimeLimit	Optional. Specifies the timeout value in milliseconds. The default value is 10000 (10 seconds). If you are encountering timeouts during NNMi user signin, increase this value. For example: `searchTimeLimit=10000`

Examples

Example ldap.properties file for Active Directory

An example ldap.properties file follows for Active Directory:

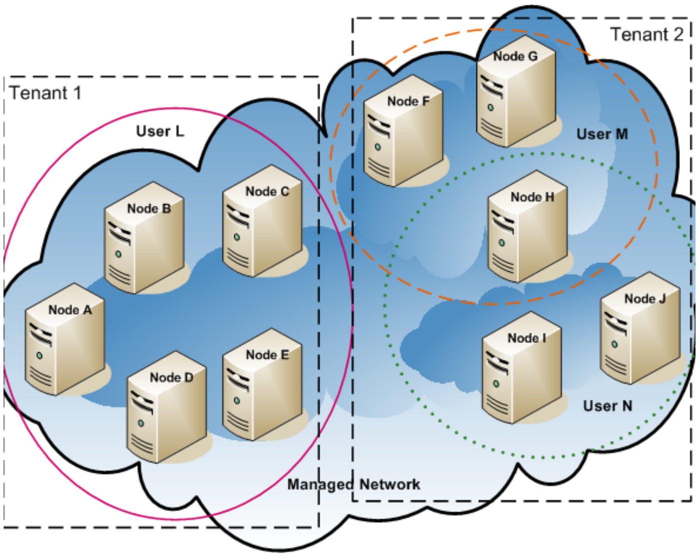
```
java.naming.provider.url=ldap://MYldapserver.example.com:389/
bindDN=MYdomain\\MYusername
bindCredential=MYpassword
baseCtxDN=CN=Users,DC=MYldapserver,DC=EXAMPLE,DC=com
baseFilter=CN={0}
defaultRole=guest
rolesCtxDN=CN=Users,DC=MYldapserver,DC=EXAMPLE,DC=com
roleFilter=member={1}
uidAttributeID=member
userRoleFilterList=admin;level2;level1
```

Example ldap.properties file for other directory services

An example ldap.properties file follows for other directory services:

```
java.naming.provider.url=ldap://MYldapserver.example.com:389/
baseCtxDN=ou=People,o=EXAMPLE.com
baseFilter=uid={0}
defaultRole=guest
rolesCtxDN=ou=Groups,o=EXAMPLE.com
roleFilter=member={1}
uidAttributeID=member
userRoleFilterList=admin;level2;level1
```

NNMi Security and Multi-Tenancy



By default, all NNMi console users can see information for all objects in the NNMi database. If this default configuration is acceptable for your environment, you do not need to read this chapter.

In NNMi, security and multi-tenancy provide for restricting user access to information about the objects in the NNMi database. This restriction is useful for customizing the views of network operators to their areas of responsibility. It also supports service providers with per-organization configuration of NNMi.

This chapter describes the NNMi security and tenant models and gives suggestions for configuration. It contains the following topics:

- Effects of Limiting Object Access on page 200
- The NNMi Security Model on page 201
- The NNMi Tenant Model on page 206
- NNMi Security and Multi-Tenancy Configuration on page 209
- NNMi Security, Multi-Tenancy, and Global Network Management on page 216
- Including Select Interfaces in NPS Reports on page 219

Effects of Limiting Object Access

Configuring NNMi security has the following impacts:

- Topology inventory objects:
  - Each NNMi console user sees only those nodes that match the configuration for their NNMi user account.
  - Sub-node objects, such as interfaces, inherit the access control from the node.
  - Inter-node objects, such as connections, are visible only if the NNMi console user can see at least one of the nodes involved.
  - A NNMi console user sees only those node groups for which they can access at least one node in the group.
  - For Network Performance Server (NPS) reports, the NNMi administrator can selectively override access control inheritance on interfaces. For more information, see Including Select Interfaces in NPS Reports on page 219.
- Maps and path views:
  - Maps show connections for which the NNMi console user has permission to view both of the participating nodes.
  - Path views omit or show as clouds any intermediate nodes to which the NNMi console user does not have access.
  - For the NNM iSPI for MPLS and the NNM iSPI for IP Multicast, when maps and path views include nodes to which the NNMi console user does not have access, the NNM iSPI opens only the connecting interface and the name of the node. The icons for the inaccessible nodes are white to indicate that status and detailed information are not available for these nodes.
  - For the NNM iSPI for IP Telephony, when maps and path views include nodes to which the NNMi console user does not have access, the NNM iSPI opens only the connecting interface and the name of the node. The icons for the inaccessible nodes show the NNMi status, but all attempted actions fail.
- Incidents:
  - For incidents whose source node is in the NNMi topology, an NNMi console user sees only the incidents for which the user has access to tho source node.
  - Incidents that do not have a source node, such as NNMi health and licensing management event incidents, are handled as a group. The NNMi administrator determines which NNMi console users see them (by associating the users with the Unresolved Incidents security group).
  - Incidents that result from traps for which the source node is not in the NNMi topology are handled in the same way as incidents with no source node. If NNMi is configured to generate these incidents, the NNMi administrator determines which NNMi console users see them (by associating the users with the Unresolved Incidents security group).

➤ The incident assignment action does not check user access. It is possible for an NNMi administrator to assign an incident to an NNMi console user who does not have permission to view that incident.

- NNMi console actions:
  - For actions that run without any selections, an NNMi console user sees only those actions they have permission to run.
  - For actions that run against one or more selected objects, an NNMi console user must have the correct access level to the selected objects. Depending on the security configuration, the NNMi console might present actions that are not valid on some of the objects visible in the NNMi console views. Invoking one of these actions results in an error message regarding this limitation.
  - For map views and NNM iSPI table views and forms, NNMi cannot distinguish between unknown nodes and nodes that exist in the NNMi topology but are not accessible by the current user.
- MIB browser and line grapher:
  - An NNMi console user can view MIB data and graphs for nodes to which they have access.
  - An NNMi console user can view MIB data for nodes to which they know the SNMP community string.
- NNMi console URLs:

  Users must log on to NNMi before accessing an NNMi console view from a direct URL. NNMi enforces that user's access according to the NNMi security configuration and limits the available topology accordingly.

The NNMi Security Model

The NNMi security model provides user access control to the objects in the NNMi database. This model is appropriate for use by any network management organization that wants to limit NNMi user access to specific objects and incidents. The NNMi security model has the following benefits:

- Provides a way to limit an NNMi console operator's view of the network. Operators can focus on specific device types or network areas.
- Provides for customizing operator access to the NNMi topology. The level of operator access can be configured per node.
- Provides for filtering the Custom Nodes view and Network Performance Server reports by security group.
- Simplifies the configuration and maintenance of node groups that align with the security configuration.
- Can be used independently of the NNMi tenant model.

Possible use cases for NNMi security include the following:

- Provide NNMi operator focus on equipment type within a site (custom maps).
- Provide NNMi operators at different sites views that show only the nodes at a given site (custom maps).
- Stage nodes during deployment. NNMi administrators see all nodes, while NNMi operators see only the deployed nodes.

- Provide full access to all NOC operators, and limit access to NOC customers.
- Provide full network views to the central NOC operators, and limit the views of the regional NOC operators.

Security Groups

In the NNMi security model, user access to nodes is controlled indirectly though user groups and security groups. Each node in the NNMi topology is associated with only one security group. A security group can be associated with multiple user groups.

Each user account is mapped to the following user groups:

- One or more of the following preconfigured NNMi user groups:
  - NNMi Administrators
  - NNMi Level 2 Operators
  - NNMi Level 1 Operators
  - NNMi Guest Users

  This mapping is required for NNMi console access and determines which actions are available within the NNMi console. If a user account is mapped to more than one of these NNMi user groups, the user receives the superset of the permitted actions.

  ➤ The NNMi Web Services Clients user group does not grant access to the NNMi console; however, it does grant administrator-level access to all NNMi objects.

- Zero or more custom user groups that are mapped to security groups.

  These mappings provide access to objects in the NNMi database. Each mapping includes an object access privilege level that applies to the nodes for a security group. The object access privilege level also applies to the related database objects, such as interfaces and incidents. For example, a user with Object Operator Level 1 access to node A containing interfaces X and Y has Object Operator Level 1 access to all of the following database objects:
  - Node A
  - Interfaces X and Y
  - Incidents whose source object is node A, interface X, or interface Y

NNMi provides the following security groups:

- Default Security Group

  In a new NNMi installation, the Default Security Group is the initial security group assignment for all nodes. By default, all users can see all objects in the Default Security Group. The NNMi administrator can configure which nodes are associated with the Default Security Group and which users can access the objects in the Default Security Group.

- Unresolved Incidents

  The Unresolved Incidents security group provides access to incidents that NNMi creates from received traps whose source node is not in the NNMi topology. By default, all users can see all incidents associated with the Unresolved Incidents security group. The NNMi administrator can configure which users can access the incidents associated with the Unresolved Incidents security group.

All node components inherit the security group assignment of the node.

Best practice

The following best practices apply to NNMi security configuration:

- Map each user account to only one preconfigured NNMi user group.
- Do not map the preconfigured NNMi user groups to security groups.
- Because any user account mapped to the NNMi Administrators user group receives administrator-level access to all objects in the NNMi database, do not map this user account to any other user groups.
- Create a separate user account for the Web Services Client role. Because this user account has access to the entire NNMi topology, map this user account to only the NNMi Web Service Clients user group.

Example Security Group Structure

The three ovals in Figure 13 indicate the primary groupings for which users need to view the nodes in this example NNMi topology. For complete user access control, each of the four unique subgroups corresponds to a unique security group. Each unique security group can be mapped to one or more user groups to represent the available levels of user access to the objects in that security group.

Table 12 on page 204 lists the mappings between the security groups and the possible custom user groups for this topology. (An actual implementation of this security model might not require all of these custom user groups.) Table 13 on page 205 lists the mappings for several user accounts and the user groups for this topology.

Figure 13 Example Topology for User Access Requirements

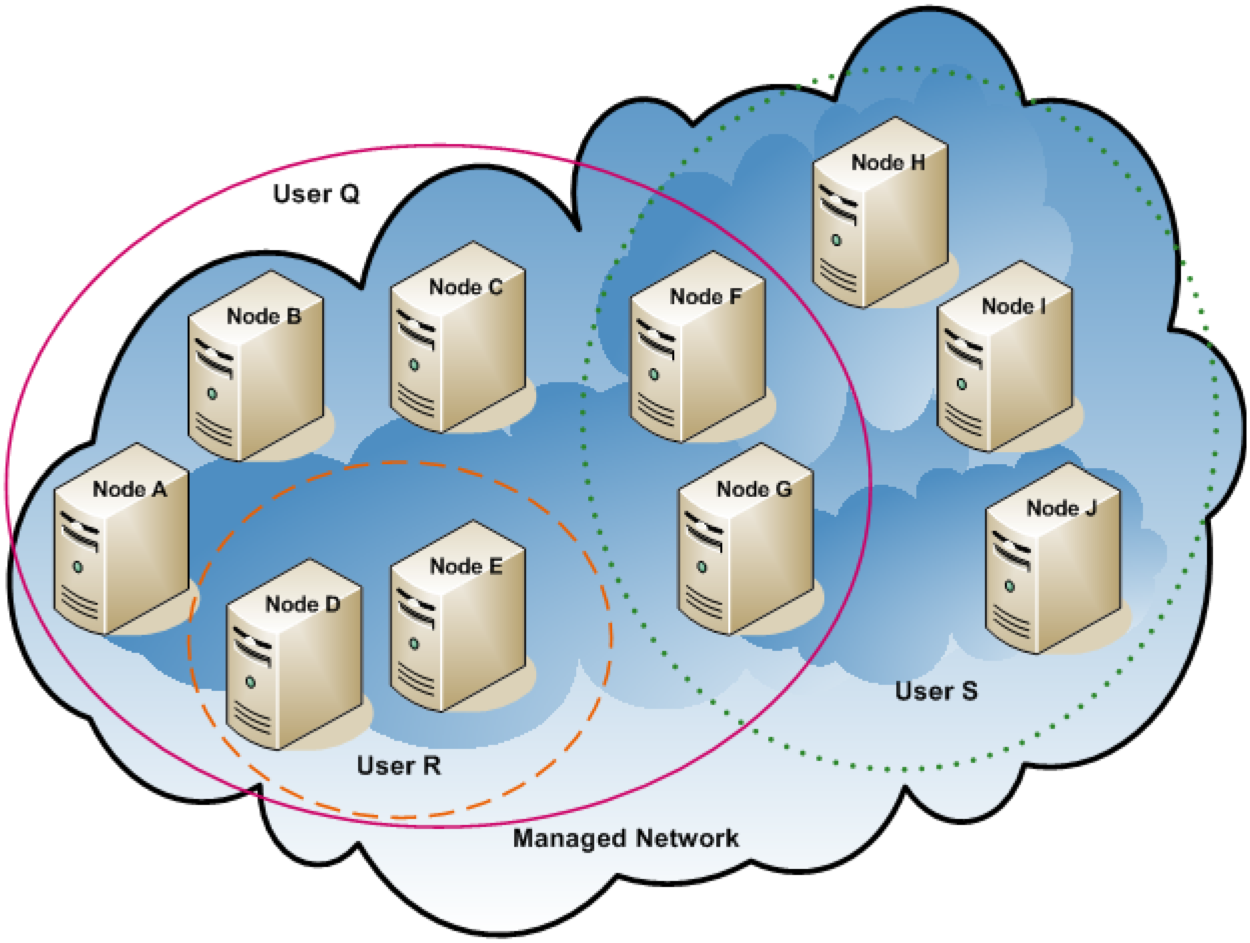


Table 12 Example Security Group Mappings

Security Group	Nodes of Security Group	User Group	Object Access Privilege
SG1	A, B, C	UG1 Administrator	Object Administrator
		UG1 Level 2	Object Operator Level 2
		UG1 Level 1	Object Operator Level 1
		UG1 Guest	Object Guest
SG2	D, E	UG2 Administrator	Object Administrator
		UG2 Level 2	Object Operator Level 2
		UG2 Level 1	Object Operator Level 1
		UG2 Guest	Object Guest

Table 12 Example Security Group Mappings (cont'd)

Security Group	Nodes of Security Group	User Group	Object Access Privilege
SG3	F, G	UG3 Administrator	Object Administrator
		UG3 Level 2	Object Operator Level 2
		UG3 Level 1	Object Operator Level 1
		UG3 Guest	Object Guest
SG4	H, I, J	UG4 Administrator	Object Administrator
		UG4 Level 2	Object Operator Level 2
		UG4 Level 1	Object Operator Level 1
		UG4 Guest	Object Guest

Table 13 Example User Account Mappings

User Account	User Groups	Node Access	Notes
User Q	NNMi Level 2 Operators	none	This user has operator level 2 access to the nodes in the pink oval (solid line).
	UG1 Level 2	A, B, C	
	UG2 Level 2	D, E	
	UG3 Level 2	F, G	
User R	NNMi Level 1 Operators	none	This user has operator level 1 access to the nodes in the orange oval (dashed line).
	UG2 Level 1	D, E	
User S	NNMi Level 2 Operators	none	This user has operator level 2 access to the nodes in the green oval (dotted line).
	UG3 Level 2	F, G	
	UG4 Level 2	H, I, J	
User T	NNMi Level 2 Operators	none	This user has access (with varying privilege levels) to all nodes in the example topology. This user has administrative access to nodes D and E but cannot see the menu items for tools that require administrative access. If this user has access to the NNMi management server, this user can run command-line tools that require administrative access against nodes D and E only.
	UG1 Guest	A, B, C	
	UG2 Administrator	D, E	
	UG3 Level 2	F, G	
	UG4 Level 1	H, I, J	

The NNMi Tenant Model

The NNMi tenant model provides strict segregation of topology discovery and data into tenants, also called organizations or customers. This model is appropriate for use by service providers, especially managed service providers, and large enterprises. The NNMi tenant model has the following benefits:

- Marks the organization to which each node belongs.
- Provides for filtering the Custom Nodes inventory view and Network Performance Server reports by tenant and security group.
- Meets regulatory requirements for separating operator access to customer data.
- Simplifies the configuration and maintenance of node groups that align with the tenant configuration.
- Simplifies configuration of NNMi security.

Use NNMi multi-tenancy to provide different customer views for a service provider that has multiple customers (tenants) managed from the same NNMi management server.

Tenants

The NNMi tenant model adds the idea of an organization to the security configuration. Each node in the NNMi topology belongs to only one tenant. The tenant provides logical separation in the NNMi database. Object access is managed through security groups.

For each node, the initial discovery tenant assignment occurs when the node is first discovered and added to the NNMi database. For seeded nodes, you can specify the tenant to assign to each node. NNMi assigns all other discovered nodes (those included in an auto-discovery rule but not seeded directly) to the Default Tenant. An NNMi administrator can change the tenant for a node at any time after discovery.

Each tenant definition includes an initial discovery security group. NNMi assigns this initial discovery security group to the node along with the initial discovery tenant. An NNMi administrator can change the security group for a node at any time after discovery.

Changing the tenant assignment of a node does not automatically change the security group assignment.

NNMi provides the Default Tenant. By default, all NNMi users have access (through the Default Security Group) to all objects associated with this tenant.

All node components inherit the tenant and security group assignments of the node.

Best practice

The following best practices apply to NNMi tenant configuration:

- For a small organization, a single security group per tenant is probably sufficient.
- You might want to subdivide a large organization into multiple security groups.
- To prevent users from accessing nodes across organizations, ensure that each security group includes nodes for only one tenant.

Example Tenant Structure

Figure 14 shows an example NNMi topology containing two tenants, represented by the rectangles. The three ovals indicate the primary groupings for which users need to view the nodes. The topology for Tenant 1 is managed as a single group, so it needs only one security group. The topology for Tenant 2 is managed in overlapping sets, so it is separated into three security groups.

Table 14 on page 208 lists the mappings between the security groups and the possible custom user groups for this topology. (An actual implementation of this security model might not require all of these custom user groups.) Table 15 on page 208 lists the mappings for several user accounts and the user groups for this topology.

Figure 14 Example Topology for Multiple Tenants

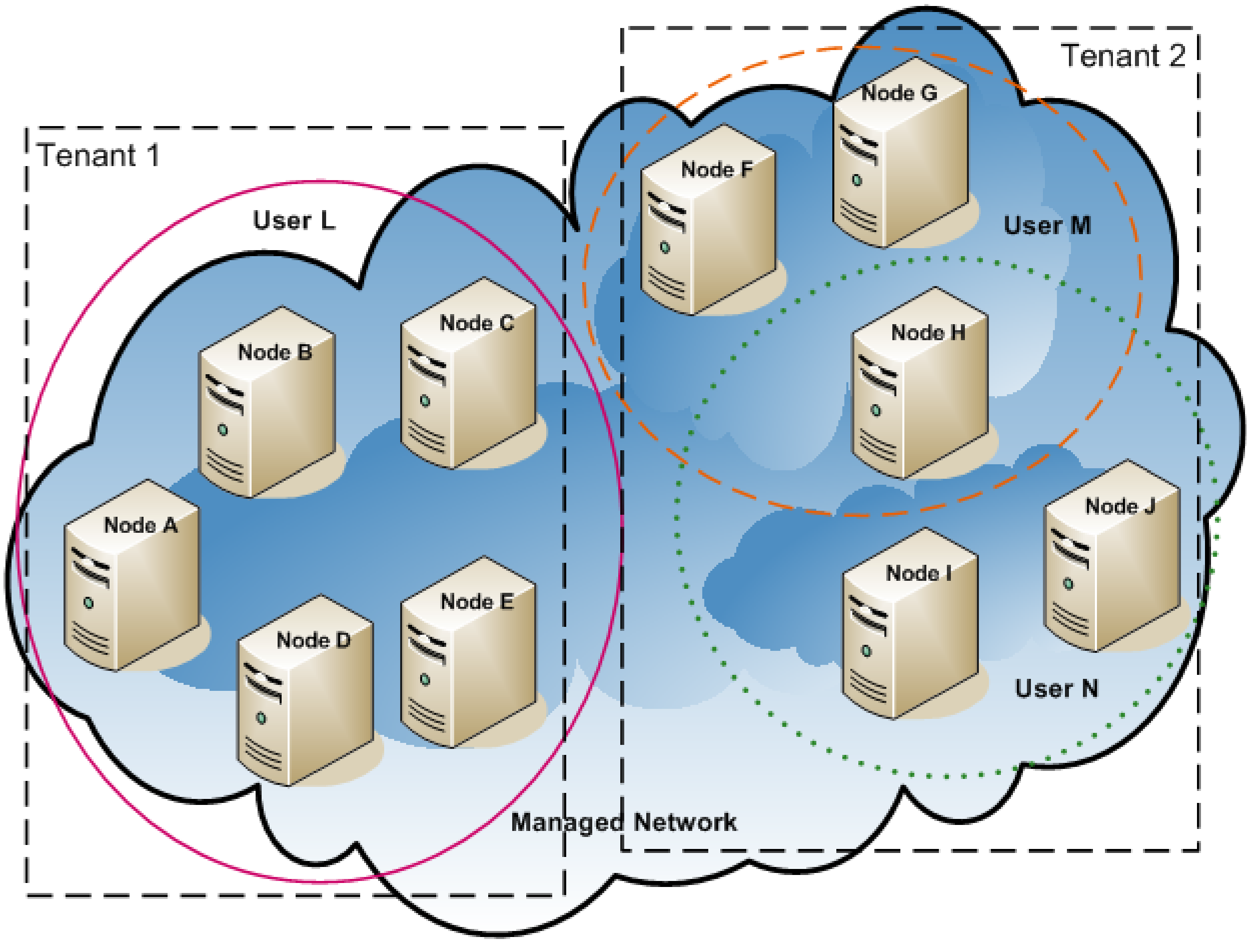


Table 14 Example Security Group Mappings for Multiple Tenants

Security Group	Nodes of Security Group	User Group	Object Access Privilege
T1 SG	A, B, C, D, E	T1 Administrator	Object Administrator
		T1 Level 2	Object Operator Level 2
		T1 Level 1	Object Operator Level 1
		T1 Guest	Object Guest
T2 SGa	F, G	T2_a Administrator	Object Administrator
		T2_a Level 2	Object Operator Level 2
		T2_a Level 1	Object Operator Level 1
		T2_a Guest	Object Guest
T2 SGb	H	T2_b Administrator	Object Administrator
		T2_b Level 2	Object Operator Level 2
		T2_b Level 1	Object Operator Level 1
		T2_b Guest	Object Guest
T2 SGc	I, J	T2_c Administrator	Object Administrator
		T2_c Level 2	Object Operator Level 2
		T2_c Level 1	Object Operator Level 1
		T2_c Guest	Object Guest

Table 15 Example User Account Mappings for Multiple Tenants

User Account	User Groups	Node Access	Notes
User L	NNMi Level 2 Operators	none	This user has operator level 2 access to the nodes in the pink oval (solid line), which groups all nodes in Tenant 1.
	T1 Level 2	A, B, C, D, E	
User M	NNMi Level 1 Operators	none	This user has operator level 1 access to the nodes in the orange oval (dashed line), which groups a subset of the nodes in Tenant 2.
	T2_a Level 1	F, G	
	T2_b Level 1	H	
User N	NNMi Level 2 Operators	none	This user has operator level 2 access to the nodes in the green oval (dotted line), which groups a subset of the nodes in Tenant 2.
	T2_b Level 2	H	
	T2_c Level 2	I, J	

NNMi Security and Multi-Tenancy Configuration

NNMi security and multi-tenancy configuration applies to the entire NNMi database. Any NNMi administrator can view and configure operator access to all objects for all tenants.

After an NNMi administrator has defined at least one custom security group, the **Security Group** field is visible on all **Node** forms and as a column in the **Nodes** and **Custom Nodes** inventory views.

After an NNMi administrator has defined at least one custom tenant, the **Tenant** field is visible on all **Node** forms and as a column in the **Nodes** and **Custom Nodes** inventory views.

Node groups

To create a node group that aligns with part of the security or multi-tenancy configuration, specify a node group additional filter based on security group UUID, security group name, tenant UUID, or tenant name. Use these node groups to configure per-security group or per-tenant polling cycles for monitoring and incident lifecycle transition actions.

Best practice

Because security group and tenant names can change, specify the security group or tenant UUID in additional filters. This information is available on the configuration forms and in the `nnmsecurity.ovpl` command output.

User groups: NNMi console access

The user account mapping to one of the predefined NNMi user groups sets the NNMi role and the visibility of menu items in the NNMi console. It is recommended to grant each user account the NNMi role that matches the highest object access privilege for that user's topology objects.

The exception to this recommendation is at the administration level because NNMi administrators can access all topology objects. To configure an NNMi console user as an administrator of only some nodes in the NNMi topology, assign that user to the NNMi Level 2 Operators or NNMi Level 1 Operators user group (note that Level 1 Operators have less access privileges than Level 2 Operators). Also assign that user to a custom user group mapped with the Object Administrator object access privilege to a security group containing a subset of the nodes in the topology.

User groups: directory service

If you are if storing user group membership in the NNMi database, all object access configuration occurs in the NNMi configuration areas through user groups, user account mappings, security groups, and security group mappings.

If you are storing user group membership in a directory service, object access configuration is shared between NNMi configuration (security groups and security group mappings) and the directory service content (user group membership). Do not create user accounts or user account mappings in the NNMi database. For each applicable group in the directory service, create one or more user groups in the NNMi database. In NNMi, set the **Directory Service Name** field of each user group definition to the distinguished name of that group in the directory service.

For more information, see Integrating NNMi with a Directory Service through LDAP on page 167.

Configuration Tools

NNMi provides several tools for configuring multi-tenancy and security.

Security Wizard

The **Security Wizard** in the NNMi console is useful for visualizing the security configuration. It is the easiest way to assign nodes to security groups within the NNMi console. The **View Summary of Changes** page presents a list of unsaved changes from the current wizard session. It also identifies potential problems with the security configuration.

➤ The **Security Wizard** is for NNMi security configuration only. It does not include tenant information.

For information about using the **Security Wizard**, click the NNMi help links within the wizard.

NNMi console forms

The forms for individual security and multi-tenancy objects in the NNMi console are useful for concentrating on one aspect of the configuration at a time. For information about using these forms, see the NNMi help for each form.

The **Tenants** view contains NNMi multi-tenancy configuration information. This view is available under **Discovery** in the **Configuration** workspace. Each **Tenant** form describes one NNMi tenant and shows the nodes currently assigned to that tenant. The node assignment information is read-only.

To change the tenant or security group assignment for a node, use the **Node** form or the `nnmsecurity.ovpl` command.

The following NNMi console views are available under **Security** in the **Configuration** workspace. These views contain NNMi security configuration information:

- **User Accounts**
  - Each **User Account** form describes one NNMi user and shows the user groups to which that user belongs. The membership information is read-only.
  - If you are storing user group membership in a directory service, user accounts are not visible in the NNMi console.
- **User Groups**

  Each **User Group** form describes one NNMi user group and shows the user accounts and security groups mapped to the user group. The mapping information is read-only.
- **User Account Mappings**
  - Each **User Account Mapping** form shows one user account-to-user group association.
  - Changes to user account mappings do not affect the current NNMi console users. These users receive any changes the next time they log on to the NNMi console.
  - If you are storing user group membership in a directory service, user account mappings are not visible in the NNMi console.
- **Security Groups**

  Each **Security Group** form describes one NNMi security group and shows the nodes currently assigned to that security group. The node assignment information is read-only.

- **Security Group Mappings**
  - Each **Security Group Mapping** form shows one user group-to-security group association.
  - After initial configuration, the object access privilege associated with a security group mapping is read-only. To change the object access privilege for a security group mapping, delete that mapping and recreate it.

Command line

The nnmsecurity.ovpl command-line interface is useful for automation and bulk operations. The tool also provides reports of potential problems with the security configuration.

Many of the nnmsecurity.ovpl options support loading input data from comma-separated values (CSV) files. You can maintain configuration data in a file or system that can generate CSV output for consumption by the nnmsecurity.ovpl command. The command can also accept UUIDs generated outside of NNMi.

Best practice

Because security group and tenant names do not need to be unique, specify the security group or tenant UUID as input to the nnmsecurity.ovpl command.

The following example script uses the nnmsecurity.ovpl command to create the security configuration for two user accounts and five nodes.

```
#!/bin/sh
# create two users
nnmsecurity.ovpl -createUserAccount user1 -password password -role level1
nnmsecurity.ovpl -createUserAccount user2 -password password -role level2

# create two user groups
nnmsecurity.ovpl -createUserGroup local1
nnmsecurity.ovpl -createUserGroup local2

# assign the user accounts to the new user groups
nnmsecurity.ovpl -assignUserToGroup -user user1 -userGroup local1
nnmsecurity.ovpl -assignUserToGroup -user user2 -userGroup local2

# create two security groups
nnmsecurity.ovpl -createSecurityGroup secgroup1
nnmsecurity.ovpl -createSecurityGroup secgroup2

# assign the new user groups to the new security groups
nnmsecurity.ovpl -assignUserGroupToSecurityGroup -userGroup local1 \
  -securityGroup secgroup1 -role level1
nnmsecurity.ovpl -assignUserGroupToSecurityGroup -userGroup local2 \
  -securityGroup secgroup2 -role level2

# assign nodes to security groups
nnmsecurity.ovpl -assignNodeToSecurityGroup -node mplspe01 -securityGroup secgroup1
nnmsecurity.ovpl -assignNodeToSecurityGroup -node vwan_router-1 -securityGroup secgroup1
nnmsecurity.ovpl -assignNodeToSecurityGroup -node vwan_router-2 -securityGroup secgroup1
nnmsecurity.ovpl -assignNodeToSecurityGroup -node data_center_1 -securityGroup secgroup2
nnmsecurity.ovpl -assignNodeToSecurityGroup -node mplspe03 -securityGroup secgroup2
```

Configuring Tenants

NNMi provides the following ways to configure multi-tenancy:

- The **Tenant** form in the NNMi console is useful for working with individual tenants.
- The nnmsecurity.ovpl command-line interface is useful for automation and bulk operations. The tool also provides reports of potential problems with the tenant configuration.

The process of defining and configuring NNMi multi-tenancy to assign each NNMi topology object to a tenant (organization) is a cyclical process. This high-level procedure describes one approach to configuring NNMi multi-tenancy.

Note the following about configuring NNMi multi-tenancy:

- The security group that NNMi assigns to a discovered node is set by the value of the Initial Discovery Security Group for the tenant associated with that node.
- When you use the NNMi security model without also configuring NNMi tenants, all nodes are assigned to the Default Tenant.
- When you seed a node for NNMi discovery, you can specify the tenant to which that node belongs. When NNMi discovers a node through an auto-discovery rule, NNMi assigns that node to the Default Tenant. After discovery, you can change the tenant assignment for the node.

One high-level approach to planning and configuring NNMi multi-tenancy is as follows:

1. Analyze your customer requirements to determine how many tenants are required in the NNMi environment.

   It is recommended that tenants be used only when managing multiple separate networks with a single NNMi management server.

2. Analyze the managed network topology to determine which nodes belong to each tenant.
3. Analyze the topology of each tenant to determine the groups of nodes to which NNMi users need access.
4. Remove the default associations between the predefined NNMi user groups and the Default Security Group and the Unresolved Incidents security group.

   Doing this step assures that users do not inadvertently obtain access to nodes they should not be managing. At this point, only NNMi administrators can access objects in the NNMi topology.

5. Configure the identified tenants.
   a. Create the identified security groups.
   b. Create the identified tenants.

      For each tenant, set the Initial Discovery Security Group to either the Default Security Group or a tenant-specific security group with restricted access. This approach ensures that new nodes for the tenant are not generally visible until the NNMi administrator configures access.

6. Prepare for discovery by assigning tenants to seeds.

   After discovering a group of nodes, you can change the value of the Initial Discovery Security Group. Using this approach limits the manual re-assignment of nodes to security groups.

7. After discovery completes, do the following:
   - Verify the tenant for each node and make changes as necessary.
   - Verify the security group for each node and make changes as necessary.
8. Continue with step 4 on page 214.

Configuring Security Groups

If you plan to integrate NNMi with a directory service for consolidating the storage of user names, passwords, and, optionally, NNMi user group assignments, complete that configuration before configuring NNMi security.

NNMi provides the following ways to configure security:

- The **Security Wizard** in the NNMi console is useful for visualizing the security configuration. The **View Summary of Changes** page presents a list of unsaved changes from the current wizard session. It also identifies potential problems with the security configuration.
- The forms in the NNMi console for individual security objects are useful for concentrating on one aspect of the security configuration at a time.
- The `nnmsecurity.ovpl` command-line interface is useful for automation and bulk operations. The tool also provides reports of potential problems with the security configuration.

The process of defining and configuring NNMi security to limit users' access to objects in the NNMi topology is a cyclical process. This high-level procedure describes one approach to configuring NNMi security.

This example moves from security groups to user accounts. For examples of configuring NNMi security from user accounts to security groups, search for "Configure Security Example" in the NNMi help.

Note the following about configuring NNMi security:

- The security group that NNMi assigns to a discovered node is set by the value of the Initial Discovery Security Group for the tenant associated with that node.
- When you use the NNMi security model without also configuring NNMi tenants, all nodes are assigned to the Default Tenant.

One high-level approach to planning and configuring NNMi security is as follows:

1. Analyze the managed network topology to determine the groups of nodes to which NNMi users need access.
2. Remove the default associations between the predefined NNMi user groups and the Default Security Group and the Unresolved Incidents security group.

   Doing this step assures that users do not inadvertently obtain access to nodes they should not be managing. At this point, only NNMi administrators can access objects in the NNMi topology.
3. Configure a security group for each subset of nodes. Remember that a given node can belong to only one security group.

   a. Create the security groups.

   b. Assign the appropriate nodes to each security group.

4 Configure custom user groups.

   a For each security group, configure a user group for each level of NNMi user access.

      — If you are if storing user group membership in the NNMi database, no users are mapped to these user groups yet.

      — If you are storing user group membership in a directory service, set the Directory Service Name field for each user group to the distinguished name of that group in the directory service.

   b Map each custom user group to the correct security group. Set the appropriate object access privilege for each mapping.

5 Configure user accounts.

   - If you are storing user group membership in the NNMi database, do the following:

      — Create a user account object for each user who can access the NNMi console. (The process of configuring user accounts depends on whether you are using a directory service for NNMi console logon.)

      — Map each user account to one of the predefined NNMi user groups (for access to the NNMi console).

      — Map each user account to one or more custom NNMi user groups (for access to topology objects).

   - If you are storing user group membership in a directory service, verify that each user belongs to one of the predefined NNMi user groups and one or more custom user groups.

6 Verify the configuration as described in Verifying the Configuration on page 214.

7 Maintain the security configuration.

   - Watch for nodes added to the Default Security Group, and move these nodes to the correct security groups.

   - Add new NNMi console users to the correct user groups.

Verifying the Configuration

To verify that the security configuration is correct, verify each aspect of the configuration separately. This section describes some approaches to verifying the configuration. Other approaches are possible.

NNMi provides reports of possible security configuration errors. Access these reports with **Tools > Security Reports** in the NNMi console and with the `-displayConfigReport` option to the `nnmsecurity.ovpl` command.

Verify security group-to-node assignments

One approach to verifying that each node is assigned to the correct security group is to sort the **Nodes** or **Custom Nodes** inventory view by security group, and then examine the groupings.

Another approach is to use the `-listNodesInSecurityGroup` option to the `nnmsecurity.ovpl` command.

Verify user group-to-security group assignments

One approach to verifying which user groups are mapped to each security group is to sort the **Security Group Mappings** view by user group or security group, and then examine the groupings. Also verify the object access privilege for each mapping.

Alternatively, on the **Map User Groups and Security Groups** page of the **Security Wizard**, select one user group or security group at a time to see the current mappings for that object.

Another approach is to use the `-listUserGroupsForSecurityGroup` option to the `nnmsecurity.ovpl` command.

Verify that each user has NNMi console access

For NNMi console access, ensure that each user is assigned to one of the predefined NNMi user groups (listed from highest to lowest):

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

All other user group assignments provide access to objects in the NNMi database.

Users without NNMi console access are listed on the **View Summary of Changes** page of the **Security Wizard**. The **Tools > Security Reports** menu item and the `-displayConfigReport usersWithoutRoles` option to the `nnmsecurity.ovpl` command also provide this information.

➤ Each **Tools** and **Action** menu item provided in the NNMi Console is associated with a default NNMi role. (To determine the default NNMi Role assigned to each Action menu item, see *Actions Provided by NNMi* in the NNMi help.) If you change the setting for a menu item provided by NNMi to a role that is a lower level role than the default NNMi role assigned to the menu item, NNMi ignores that change. Any User Group with the lower level role than the default NNMi role cannot access the menu item.

Verify user-to-user group assignments

One approach to verifying user group membership is to sort the **User Account Mappings** view by user account or user group, and then examine the groupings.

Alternatively, on the **Map User Accounts and User Groups** page of the **Security Wizard**, select one user account or user group at a time to see the current mappings for that object.

Another approach is to use the `-listUserGroups` and `-listUserGroupMembers` options to the `nnmsecurity.ovpl` command.

Verify tenant-to-node assignments

One approach to verifying that each node is assigned to the correct tenant is to sort the **Nodes** or **Custom Nodes** inventory view by tenant, and then examine the groupings.

Verify current user settings

To verify the NNMi console access for the currently logged-on user, click **Help > System Information**. The **User Information** section on the **Product** tab lists the following information for the current NNMi session:

- User name as defined for the user account in the NNMi database or the accessed directory service.
- NNMi role, which corresponds to the most privileged of the predefined NNMi user groups (NNMi Administrators, NNMi Level 2 Operators, NNMi Level 1 Operators, and NNMi Guest Users) to which the user is mapped. This mapping determines which actions are available within the NNMi console.

- User groups mapped to this user name. This list includes predefined NNMi user group that sets the NNMi role and any other user groups that provide access to objects in the NNMi database.

Exporting the NNMi Security and Multi-Tenancy Configuration

Table 16 describes the configuration areas (available with `nnmconfigexport.ovpl -c`) for exporting the NNMi security and multi-tenancy configuration. These export areas are beneficial for maintaining the configuration across multiple NNMi management servers, especially in a Global Network Management environment.

Table 16 NNMi Security and Multi-Tenancy Configuration Export Areas

Configuration Area	Description
account	Exports user accounts, user groups, and user account-to-user group mappings. Useful for sharing user definitions across multiple NNMi databases.
security	Exports tenants and security groups. Useful for sharing security definitions across multiple NNMi databases. Importing this information creates new objects and updates existing objects but does not delete objects not included in the current export. Therefore, this option is safe to use with an NNMi database containing locally-defined objects.
securitymappings	Exports user group-to-security group mappings. For a complete export of the security and multi-tenancy configuration, perform a concurrent export of the `account`, `security`, and `securitymappings` configuration areas.

NNMi Security, Multi-Tenancy, and Global Network Management

In a Global Network Management (GNM) environment, a node's tenant is set on the NNMi management server that manages that node. The tenant UUID for a given node is the same on each global and regional manager in the GNM environment.

A node's security group is set on each NNMi management server whose topology contains that node. Thus, user access to objects in the topology is configured separately on each NNMi management server in the GNM environment. The global and regional managers might use the same or different security group definitions.

If you want user access to be similar on the global manager and regional managers, you can employ some configuration tricks, but you probably cannot completely avoid custom configuration on each NNMi management server.

Best practice

Define all tenants and security groups on the global manager. Use `nnmconfigexport.ovpl -c security` to export the tenant and security group definitions. On each regional manager, use `nnmconfigimport.ovpl` to import the tenant and security group definitions. Alternatively, you can use the `nnmsecurity.ovpl` command to create tenants and security group with the same UUID as on another NNMi management server. Following this recommendation ensures that each tenant and security group has the same UUID within the GNM environment.

➤ This best practice becomes a *required* part of the configuration if users will be launching NPS reports from the global manager.

➤ Tenant UUIDs must be unique, but tenant names can be reused. NNMi considers two tenants with the same name and different UUIDs to be two distinct tenants with no shared configuration.

Best practice

If you are setting up one regional manager per organization, all nodes on a regional manager can be in a single tenant. However, configure a unique tenant on each regional manager to ensure separation of the topology data on the global manager.

Incidents forwarded from a regional manager to a global manager might include some additional custom incident attributes (CIAs) to convey security and tenant information.

If the incident's source object belongs to a tenant other than the Default Tenant, the forwarded incident contains the following CIAs:

- cia.tenant.name
- cia.tenant.uuid

If the incident's source object belongs to a security group other than the Default Security Group, the forwarded incident contains the following CIAs:

- cia.securityGroup.name
- cia.securityGroup.uuid

This section contains the following topics:

- Initial GNM Configuration on page 217
- GNM Maintenance on page 219

Initial GNM Configuration

After GNM is first configured, the regional manager updates the global manager with information about the nodes in the regional topology (according to the GNM configuration).

Topology synchronization with the Default Tenant only

For GNM environments with custom security groups and the Default Tenant, on the global manager, all nodes managed remotely are added to the global manager topology with the following configuration:

- Default Tenant
- The security group that is set as the Initial Discovery Security Group for the Default Tenant.

Topology synchronization with custom tenants

For GNM environments with custom security groups and custom tenants, on the global manager, all nodes managed remotely are added to the global manager topology with the UUID of the tenant assigned to the node. If that tenant UUID does not exist on the global manager, the GNM processes create that tenant in the NNMi configuration of the global manager as follows:

- The tenant UUID is the same value as on the regional manager.
- The tenant name is the same value as on the regional manager.
- The value of the Initial Discovery Security Group is set to the security group with the same name as the tenant. (NNMi creates this security group if it does not already exist on the global manager.)

As the node is added to the topology on the global manager, it is assigned to the Initial Discovery Security Group for the tenant UUID as configured on the global manager. That is, the security group association on the global manager is independent of the security group association on the regional manager.

Best practice

Suggestions for simplifying security configuration on the global manager include:

- Maintain a spreadsheet or other record of the nodes managed by each regional manager. For each node, note the expected security group on the regional manager and that on the global manager. After GNM configuration completes, use the `nnmsecurity.ovpl` command to verify and update the security group assignments.
- If the GNM environment will include multiple regional managers updating a single global manager, enable the GNM configuration from one regional manager at a time to the global manager.

  If appropriate, you can change the value of the Initial Discovery Security Group of the Default Tenant (or a custom tenant) before adding each regional manager to the GNM configuration. Note that this approach can have mixed results if new nodes are being added to the topology on the previously configured regional managers.
- Before enabling GNM, on the global manager, set the Initial Discovery Security Group of each tenant used on the regional manager to be a private security group that operators cannot access. An administrator on the global manager then needs to explicitly move the nodes to the appropriate security groups for other NNMi console operators.

GNM Maintenance

Table 17 describes how changes to a node's tenant or security group assignment on a regional manager affect the global manager.

Table 17 Global Manager Impact of Configuration Changes on a Regional Manager

Action	Effect
On the regional manager, assign a node to a different tenant.	The node on the global manager is changed to be assigned to the different tenant. If this tenant UUID does not exist on the global manager, it is created.
On the regional manager, assign a node to a different security group.	No change on the global manager. The NNMi administrator can choose to replicate the change manually.
On the regional manager, change the configuration (name, description, or Initial Discovery Security Group) of a tenant.	No change on the global manager. The NNMi administrator can choose to replicate the change manually.
On the regional manager, change the configuration (name or description) of a security group.	No change on the global manager. The NNMi administrator can choose to replicate the change manually.

Including Select Interfaces in NPS Reports

By default, all components of a node are in the same security group as the node. For individual interfaces, you can override this default behavior and assign an interface to a different security group. The purpose of this override is to generate tenant-specific reports that include the appropriate interfaces for that tenant (customer) on shared devices. In this way, each customer can see the interface information for their interfaces but cannot see the other interfaces on the device.

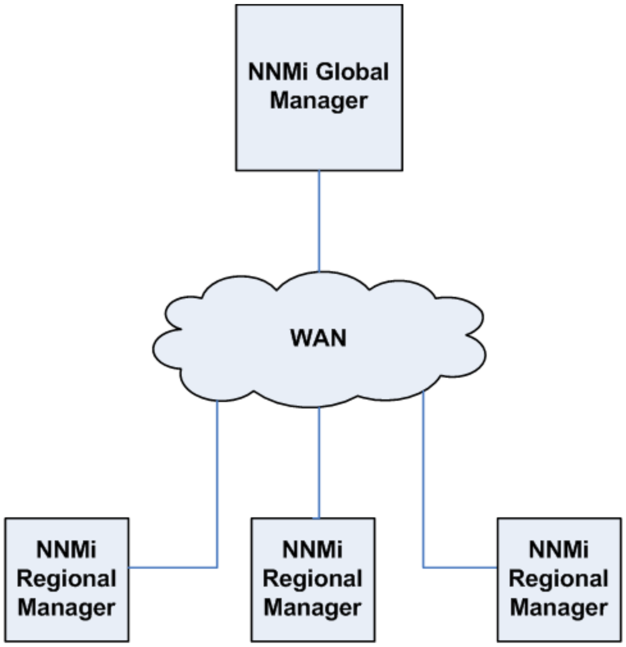
➤ The security group override only affects NPS reports. It has no impact on what users can see and do in the NNMi console.

To change the security group assignment for an interface, on the **Custom Attributes** tab of an **Interface** form or with the `nnmloadattributes.ovpl` command, add the `InterfaceSecurityGroupOverride` custom attribute to that interface. Set the value of this custom attribute to the UUID of the security group. For example:

```
InterfaceSecurityGroupOverride=0826c95c-5ec8-4b8c-8998-301e0cf3c1c2
```

➤ An interface can belong to only one security group at a time. Setting the `InterfaceSecurityGroupOverride` custom attribute on an interface breaks the association between that interface and the security group to which its node belongs.

Global Network Management



This chapter contains the following topics:

Global Network Management Benefits

Suppose you have HP Network Node Manager i Software (NNMi) deployed on multiple NNMi management servers in several geographic locations. You have each NNMi management server discovering and monitoring the network to meet your discovery and monitoring needs. Using these existing NNMi management servers and configurations, you can designate specific NNMi management servers as global managers to display combined node object data without additional discovery or monitoring configuration changes.

The NNMi global network management feature enables multiple NNMi management servers to work together while managing different geographic areas of the network. You designate specific NNMi management servers as global managers to display combined node object data from 2 or more regional managers.

The NNMi global network management feature offers the following benefits:

- A central big-picture view of your corporate-wide network from the global manager.
- Easy to set up:
  - Each regional manager administrator specifies all node object data or a specific node group for participation at the global manager level.
  - Each global manager administrator specifies which regional managers are allowed to contribute information.
- Generates and manages incidents independently on each server (generated within the context of topology available on each server).

See *NNMi's Global Network Management Feature* in the NNMi help for additional details.

Is Global Network Management a Good Tool for Managing my Network?

Ask the following questions to determine if NNMi's global network management feature can help you better manage your network.

Do I Need Continuous Multi-Site Network Monitoring?

Does your information technology group manage network equipment located at multiple sites on a 24 by 7 basis? If so, your group can use NNMi's global network management feature to observe combined topology and incident views.

Can my Critical Devices be Visible?

From one NNMi management server, can I view device status and incidents for critical devices located at multiple locations? Yes. You configure forwarding filters on the regional managers. This enables you to select the node object data you want regional managers to send to global managers. For example, you can set up forwarding filters on the regional managers so that they only forward information about critical devices to the global manager.

Licensing Considerations

For information about obtaining and installing NNMi license keys, see Licensing NNMi on page 117.

Do I need an NNMi Advanced license on both the global and regional managers? You must purchase and install an NNMi Advanced license on the NNMi management server you plan to use as a global manager. NNMi management servers do not need an NNMi Advanced license to function as regional managers.

I currently have adequate NNMi licenses for single geographies. Can I use the global network management feature and limit the new licenses I need on the global manager? Yes. If your information technology group needs to monitor critical equipment located at multiple sites, you can configure a forwarding filter on the regional manager to make sure you only forward information about critical devices to the global manager. This enables you to wisely use your NNMi investment and control your use of the license capacity you have on the global manager.

I increased the NNMi licenses for the regional managers such that the total number of licensed nodes is larger than the NNMi Advanced licenses on the global manager. Now the global manager does not have a complete inventory of all nodes in all regions. After I purchase and install enough licenses for the global manager, how can I get the global manager to synchronize with all of the regional managers in order for it to find and create the nodes it formerly skipped due to insufficient licenses? You must purchase and install enough NNMi Advanced licenses on the global manager to meet or exceed the number of total licenses you have installed on the regional managers. After you have enough licenses installed, do one of the following:

- Wait for all of the configured rediscovery intervals on all of the regional managers to elapse so that all of the nodes in all of the regions are rediscovered. After the regional managers rediscover all of the nodes in all of the regions, the regional managers send this rediscovered node information to the global manager. The global manager receives this node information and creates global nodes for each node in each region.
- Run the **`nnmnoderediscover.ovpl -all`** script on each regional manager.

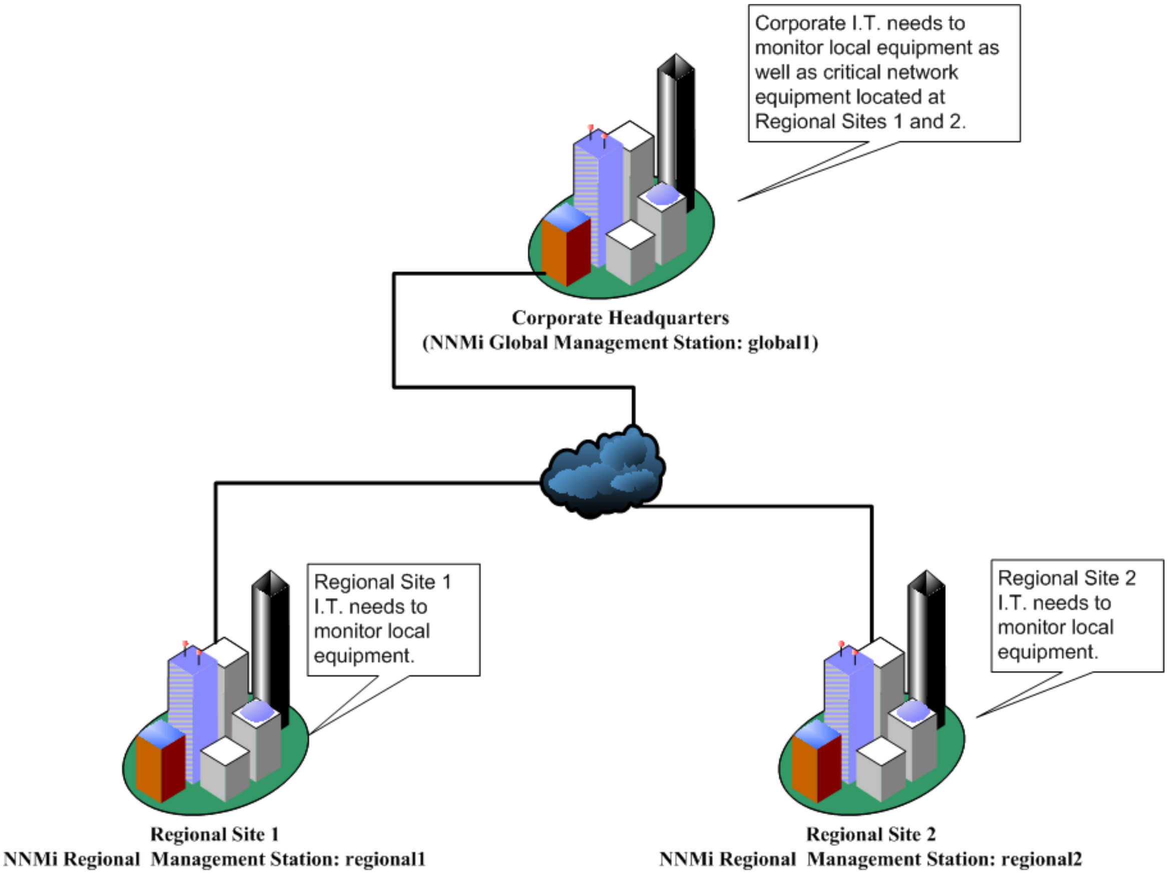
➤ The second option causes both a lot of traffic on your network and consumes a lot of NNMi resources from the entire set of NNMi managers. This option is not as resource intensive as the initial NNMi discovery, but it is similar to doing the first discovery. The best approach is to space the running of the script for each region by some amount of time or by waiting for the current regional manager's workload to drop to normal before starting the next regional manager's rediscovery.

Practical Global Network Management Examples

See Figure 15 on page 224. Suppose your company has 2 operating sites in different geographic locations. Your company’s headquarters is located in a third geographic area. There are NNMi management servers functioning at all 3 locations.

From a network perspective, information technologists located at corporate headquarters need to monitor local network equipment as well as critical network equipment located at both regional sites 1 and 2. Information technologists from both regional sites 1 and 2 need to monitor the local critical network equipment located at their sites.

Figure 15 Example Network.


Corporate I.T. needs to monitor local equipment as well as critical network equipment located at Regional Sites 1 and 2.
Corporate Headquarters
(NNMi Global Management Station: global1)
Regional Site 1 I.T. needs to monitor local equipment.
Regional Site 2 I.T. needs to monitor local equipment.
Regional Site 1
NNMi Regional Management Station: regional1
Regional Site 2
NNMi Regional Management Station: regional2

Review the Requirements

Suppose the NNMi management servers at corporate headquarters, regional site 1, and regional site 2 manage several routers and switches located at their individual sites. For this example, refer to the NNMi management servers as `global1`, `regional1` and `regional2` respectively. Suppose you configured these NNMi management servers to discover and monitor critical switches and routers located at their own locations. There is no need to reconfigure discovery for NNMi management servers at any of these sites to use the global network management feature.

➤ During global network management configuration, you might be tempted to use the **`nnmbackup.ovpl`** script to back up one NNMi management server, use the **`nnmrestore.ovpl`** script to restore this backup to a second NNMi management server, then connect both of these NNMi management servers to a regional NNMi management server. Do not do this. Placing the backup data from one NNMi management server onto a second NNMi management server means that both servers have the same database UUID. After you restore NNMi on the second NNMi management server, you would need to uninstall NNMi from the original NNMi management server.

The information technology group at your corporate site wants to monitor critical equipment located at regional sites 1 and 2, but they do not want to manage every device. The following table summarizes the monitoring needs:

Table 18 Network Requirements for Global Network Management

Site	NNMi Management Servers	Critical Switches	Regional Equipment to Manage
Corporate Headquarters	`global1`	15 Model 3500yl HP Procurve Switches	All model 3500yl HP Procurve Switches from each regional site
Regional Site 1	`regional1`	15 Model 3500yl HP Procurve Switches	not applicable
Regional Site 2	`regional2`	15 Model 3500yl HP Procurve Switches	not applicable

To summarize, you have an NNMi management server, `global1`, monitoring the corporate headquarters. You have NNMi management servers, `regional1` and `regional2`, monitoring each of the regional sites. From corporate headquarters, you must view incidents and device information for the Model 3500yl Procurve switches located at regional sites 1 and 2. Suppose that, for this example, `regional1` and `regional2` both manage several common switches located at regional site 1.

Regional Manager and Global Manager Connections

When you configure global network management connections, consider the following information:

- NNMi enables you to configure more than one global manager to communicate with a regional manager. For example, if you need a second global manager, `global2`, to communicate with `regional1`, NNMi enables you to configure both `global1` and `global2` to communicate with `regional1`. For more information see the *HP Network Node Manager i Software System and Device Support Matrix*.
- Global network management works with one connection layer. For example, the examples in this chapter discuss one connection layer: `global1` communicating with `regional1` and `global1` communicating with `regional2`. Do not configure NNMi for multiple connection levels. For example, do not configure `global1` to communicate with `regional1`, then configure `regional1` to communicate with `regional2`. The global network management feature is not designed for this three layer configuration.
- Do not configure two NNMi management servers to communicate both ways with each other. For example, do not configure `global1` to communicate with `regional1`, then configure `regional1` to communicate with `global1`.

Initial Preparation

Port Availability: Configuring the Firewall

For the global network management feature to function properly, verify that certain well-known ports are open for TCP access from `global1` to `regional1`, and `regional2`. The NNMi installation script sets ports 80 and 443 as defaults; however, you can change these values during installation.

In the example discussed in this section, `global1` establishes TCP access to `regional1` and `regional2`. Firewalls are usually configured based on the server initiating the connection. After global1 establishes the connection to regional1 and regional2, traffic flows in both directions.

Edit the following file to see the current values or to make port configuration changes:

- *Windows*: `%NNM_CONF%\nnm\props\nms-local.properties`
- *UNIX*: `$NNM_CONF/nnm/props/nms-local.properties`

The following table shows the well-know ports that need to be accessible:

Table 19 Required Accessible Sockets

Security	Parameter	TCP Port
non-SSL	jboss.http.port	80
	jboss.bisocket.port	4457
	jboss.jmsControl.port	4458
SSL	jboss.https.port	443
	jboss.sslbisocket.port	4459
	jboss.ssljmsControl.port	4460

See NNMi 9.10 and Well-Known Ports for more information.

Configuring Self-Signed Certificates

If you plan to use the global network management feature with SSL (Secure Sockets Layer) between `global1` and the two regional NNMi management servers (`regional1` and `regional2`), you must do some additional work. During NNMi installation, the NNMi installation script creates a self-signed certificate on the NNMi management server so it can identify itself to other entities. Configure the NNMi management servers you plan to use with the global network management feature with the correct certificates. Complete the steps shown in Configuring the Global Network Management Feature to use Self-Signed Certificates on page 131.

Configuring Global Network Management for Application Failover

During NNMi installation, the NNMi installation script creates a self-signed certificate on the NNMi management server so it can identify itself to other entities. If you plan to use the application failover along with the global network management feature, you must do some additional configuration. Complete the steps shown in

Configuring Global Network Management with Application Failover to use Self-Signed Certificates on page 133.

NNMi Management Server Sizing Considerations

This example assumes you plan to use existing NNMi management servers in a global network management configuration. The global network management feature is different than the distributed solution used in earlier NNM products. The global network management feature avoids polling nodes being managed by regional systems, so you do not need to be as concerned about network bandwidth and computer resources.

Review the *NNMi Installation Guide*, the *NNMi Release Notes*, and the *NNMi System and Device Support Matrix*, for specific information about the size of server required to house NNMi.

Synchronizing System Clocks

It is important for you to synchronize the NNMi management server clocks for `global1`, `regional1`, and `regional1` before you connect these servers in a global network management configuration. All NNMi management servers in your network environment that participate in global network management (global managers and regional managers) or single sign-on (SSO) must have their internal time clocks synchronized in universal time. Use a Time Synchronization program, for example, the UNIX (HP-UX / Linux / Solaris) tool Network Time Protocol Daemon (NTPD) or one of the available Window operating system tools. See *Clock Synchronization Issues* or *Troubleshoot Global Network Management* in the NNMi help and Clock Synchronization on page 254 for more information.

> NNMi opens a warning message at the bottom of the NNMi Console if there is a connection problem with a regional manager, such as a server clock synchronization problem.

Using the Application Failover Feature with Self-Signed Certificates in Global Network Management

If you plan to use the global network management feature using self-signed certificates in an application failover configuration, you must complete some additional steps. See Configuring Global Network Management with Application Failover to use Self-Signed Certificates on page 133.

Using Self-Signed Certificates in Global Network Management

If you plan to use the global network management feature using self-signed certificates, you must complete some additional steps. See Configuring the Global Network Management Feature to use Self-Signed Certificates on page 131.

Using a Certificate Authority in Global Network Management

If you plan to use the global network management feature using a Certificate Authority, you must complete some additional steps. See Configuring the Global Network Management Feature to use a Certificate Authority on page 132.

List the Critical Equipment you Want to Monitor

Make a list of the equipment managed by `regional1` and `regional2` that you want to monitor from `global1`. You will use this information in a forwarding filter (to be discussed later). Carefully consider the possible outcomes of limiting the information forwarded to `global1` from `regional1` and `regional2`. Below are some things to consider during your planning:

- Be careful not to exclude too many devices, as `global1` needs a complete topology from `regional1` and `regional2` to do a complete analysis to generate accurate incidents.
- Excluding non-critical devices helps you to reduce license costs on `global1`.
- Excluding non-critical devices helps you to improve the solution's overall scalability, and reduce the network traffic required by NNMi.

Review the Global and Regional Managers' Management Domains

NNMi management servers `global1`, `regional1`, and `regional2` manage their own set of nodes. Later in this example, you will configure `regional1` and `regional2` to forward information about equipment they manage to `global1`.

Use the following procedure to understand the equipment that `global1`, `regional1`, and `regional2` currently monitor. This helps you select the critical equipment you want `regional1` and `regional2` to forward to `global1`.

For this example, complete the following steps to review this information:

1. Point your browser to `global1's`, NNMi console.
2. Sign in.
3. Click **Inventory** workspace.
4. From here you can review the discovered inventory `global1` currently monitors.
5. Point your browser to `regional1`'s, NNMi console.
6. Sign in.
7. Click **Inventory** workspace.
8. Review the nodes that `regional1` monitors and make a list of the devices you want to monitor from `global1`.
9. Point your browser to `regional2`'s, NNMi console.
10. Sign in.
11. Click **Inventory** workspace.
12. Review the nodes that `regional2` monitors and make a list of the devices you want to monitor from `global1`.

Review NNMi Help Topics

To review all of the help topics related to global network management, complete the following steps:

1 From the NNMi help, click **Search**.

2 Type **"Global Network Management"** in the `Search` field.

3 Click **Search**.

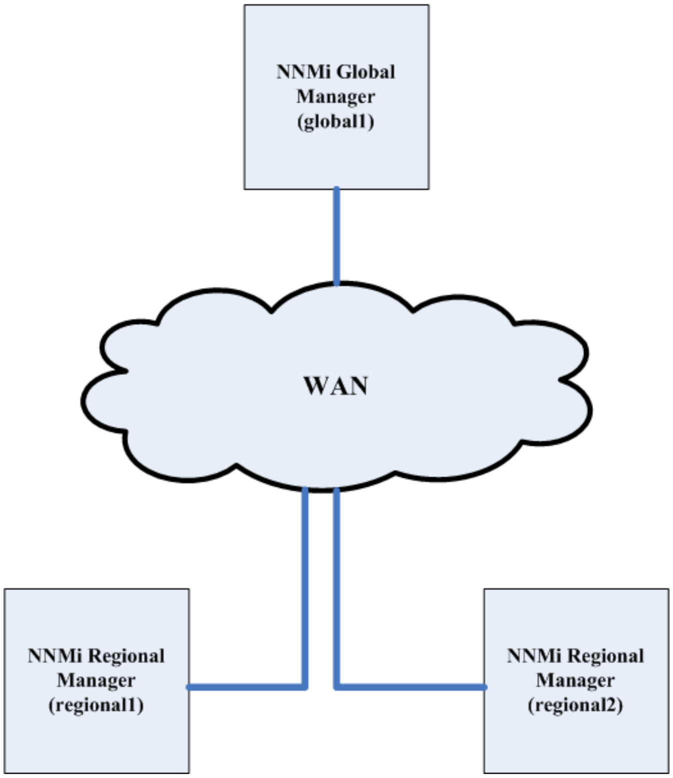
This search results in more than 50 topics related to global network management.

SSO and the Actions Menu

From an NNMi console on a global manager, suppose you select a node managed by a regional manager, then use the **Actions** menu to initiate an action on the selected node. Without having the `initString` and `domain` parameters the same among the NNMi management servers, the session information from the global manager does not get passed on to the new session and the action does not get initiated. To avoid this problem, follow the configuration steps shown in Configuring Single Sign-On for Global Network Management on page 229.

Configuring Single Sign-On for Global Network Management

You can configure NNMi single sign-on (SSO) to facilitate access to NNMi regional managers from an NNMi global manager. Complete this step before connecting regional managers from a global manager. See Using Single Sign-On with NNMi on page 141 for more information.


NNMi Global Manager (global1)
WAN
NNMi Regional Manager (regional1)
NNMi Regional Manager (regional2)

The SSO feature communicates a user name among NNMi management servers, but not passwords or roles. For example, NNMi associates the same username on one NNMi management server (`global1`) with a different role on other NNMi management servers (`regional1` or `regional2`). Any of these three NNMi management servers could associate a different password with the same username.

If a global and regional manager resides in the same management domain, and you do not copy the *Initialization String* value from the global NNMi management server to the regional NNMi management server as shown in step 4 on page 230, you could have NNMi console access problems. To avoid this, either configure SSO correctly using the following steps, or disable SSO as described in Disabling SSO on page 150.

To configure SSO to work with the global network management feature, complete the following steps:

1 Edit the following file on `global1, regional1, and regional2`:

- *Windows*: `%NNM_PROPS%\nms-ui.properties`
- *UNIX*: `$NNM_PROPS/nms-ui.properties`

2 On `global1`, `regional1, and regional2`, look for a section in the file that resembles the following:

```
com.hp.nms.ui.sso.isEnabled = false
```

Change this as follows:

```
com.hp.nms.ui.sso.isEnabled = true
```

3 Locate the SSO NNMi initialization string for `global1`. Look for a section in the `nms-ui.properties` file that resembles the following:

com.hp.nms.ui.sso.initString = *Initialization String*

4 Copy the value of *Initialization String* from the `nms-ui.properties` file on `global1` to the `nms-ui.properties` files on `regional1` and `regional2`. All of the servers must use the same value for *Initialization String*. Save your changes.

NNMi supports copying the *Initialization String* value from the global NNMi management server to the regional NNMi management servers. In this step, you copied the *Initialization String* value from the global manager to the two regional managers. Always copy the *Initialization String* value from the global manager to the regional managers if you want to use SSO with the global network management feature.

If a global and regional manager resides in the same management domain, and you do not copy the *Initialization String* value from the global NNMi management server to the regional NNMi management server, disable SSO to avoid NNMi console access problems. See Disabling SSO on page 150 for more information.

5 If `global1`, `regional1`, and `regional2` are in different domains, modify the `protectedDomains` content. To do this, look in the `nms-ui.properties` file for a section that resembles the following:

```
com.hp.nms.ui.sso.protectedDomains=group1.mycompany.com
```

Suppose `global1` is in `global1.company1.com`, `regional1` is in `regional1.company2.com` and `regional2` is in `regional2.company3.com`. Modify the `protectedDomains` section of the `nms-ui.properties` file on `global1`, `regional1` and `regional2` as follows:

```
com.hp.nms.ui.sso.protectedDomains=regional1.company1.com,
regional2.company2.com,regional3.company3.com
```

6 Save your changes.

7 Run the following command sequence on `global1`, `regional1`, and `regional2`:

   a `ovstop`

   b `ovstart`

There are no manual configuration steps to perform to enable single sign-on in an application failover configuration. For example, If you plan to configure single sign-on in an application failover configuration, NNMi replicates the above changes from the active NNMi management server to the standby NNMi management server.

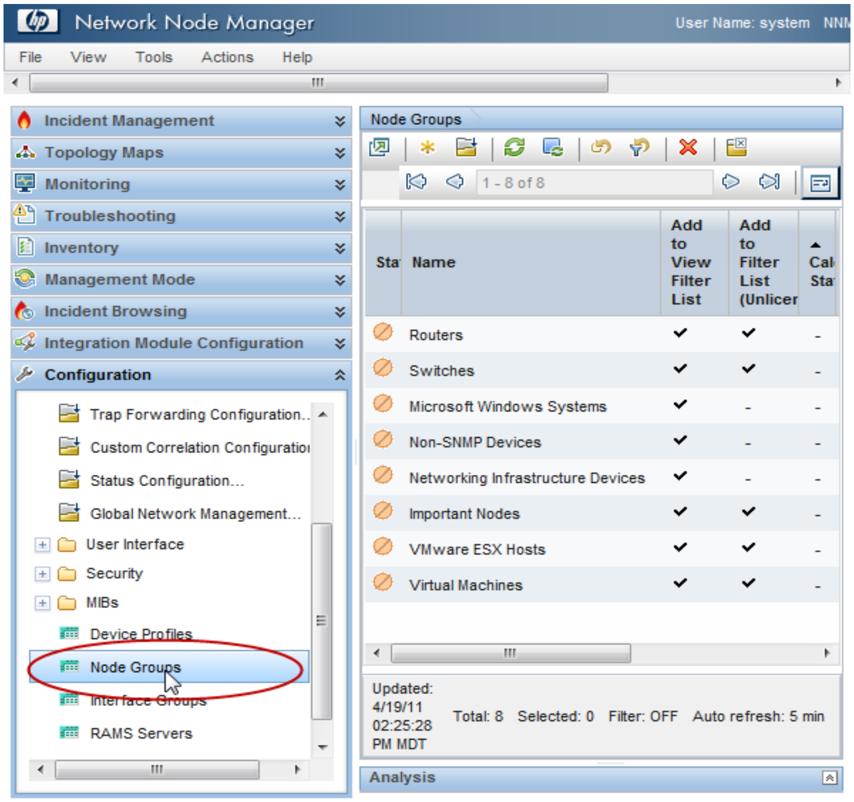
Configuring Forwarding Filters on the Regional Managers

In this example, `global1` communicates with both `regional1` and `regional2`. To control the node object data you want the global manager, `global1`, to receive from regional managers `regional1` and `regional2`, configure forwarding filters on both `regional1` and `regional2`.

Configuring a Forwarding Filter to Limit Forwarded Nodes

Suppose you want to set up a node group to enable `regional1` to only forward node information for Procurve Model 3500yl switches to `global1`. To create a new node group and set these limits, complete the following steps:

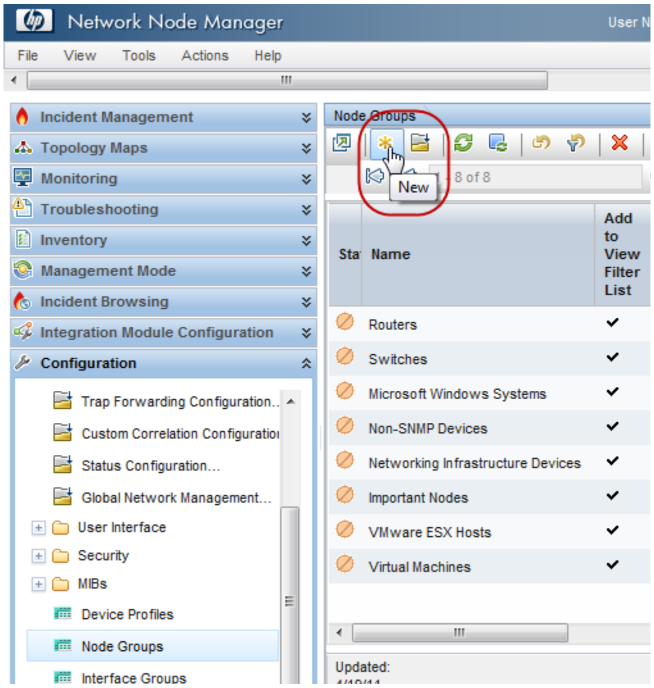
1 From `regional1`'s **Configuration** workspace in the NNMi console, click **Node Groups.**



Sta	Name	Add to View Filter List	Add to Filter List (Unlicer	Cal Sta
	Routers	✓	✓	-
	Switches	✓	✓	-
	Microsoft Windows Systems	✓	-	-
	Non-SNMP Devices	✓	-	-
	Networking Infrastructure Devices	✓	-	-
	Important Nodes	✓	✓	-
	VMware ESX Hosts	✓	✓	-
	Virtual Machines	✓	✓	-

Updated: 4/19/11 02:25:28 PM MDT Total: 8 Selected: 0 Filter: OFF Auto refresh: 5 min

2 Click **New**.



Sta	Name	Add to View Filter List
	Routers	✓
	Switches	✓
	Microsoft Windows Systems	✓
	Non-SNMP Devices	✓
	Networking Infrastructure Devices	✓
	Important Nodes	✓
	VMware ESX Hosts	✓
	Virtual Machines	✓

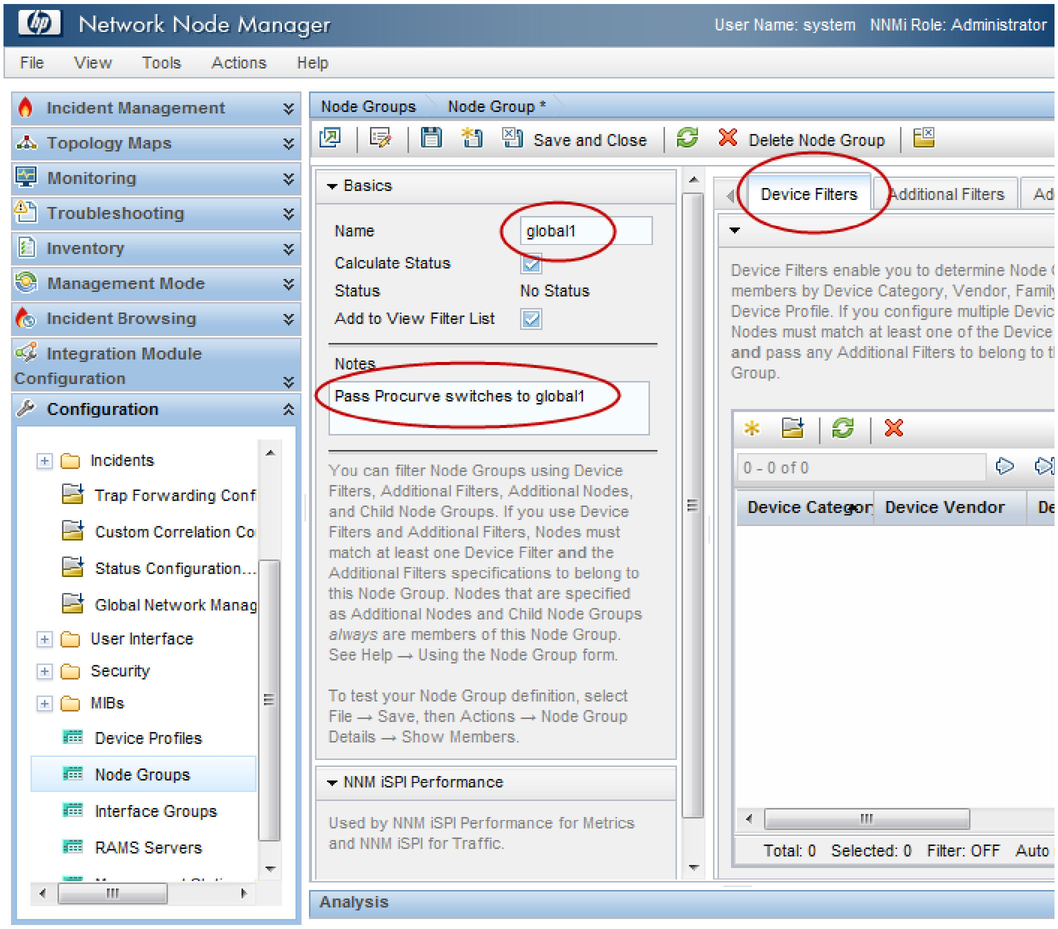
Updated:

Although this example explains how to create a new node filter, then use it to create a forwarding filter from regional1 and regional2, you can use any of these existing filters to set up forwarding filters from a regional NNMi management server to a global NNMi management server.

You can create a *container* node group that contains no devices or filters of its own; then use this node group to specify child node groups. Using this approach, you can forward node object data to global NNMi management servers using one *container* node group.

3 Click the **Device Filters** tab. Type `global1` as the filter name and make any notes you need about the filter you are creating in the notes field.

.



Name: global1

Calculate Status: ☑

Status: No Status

Add to View Filter List: ☑

Notes: Pass Procurve switches to global1

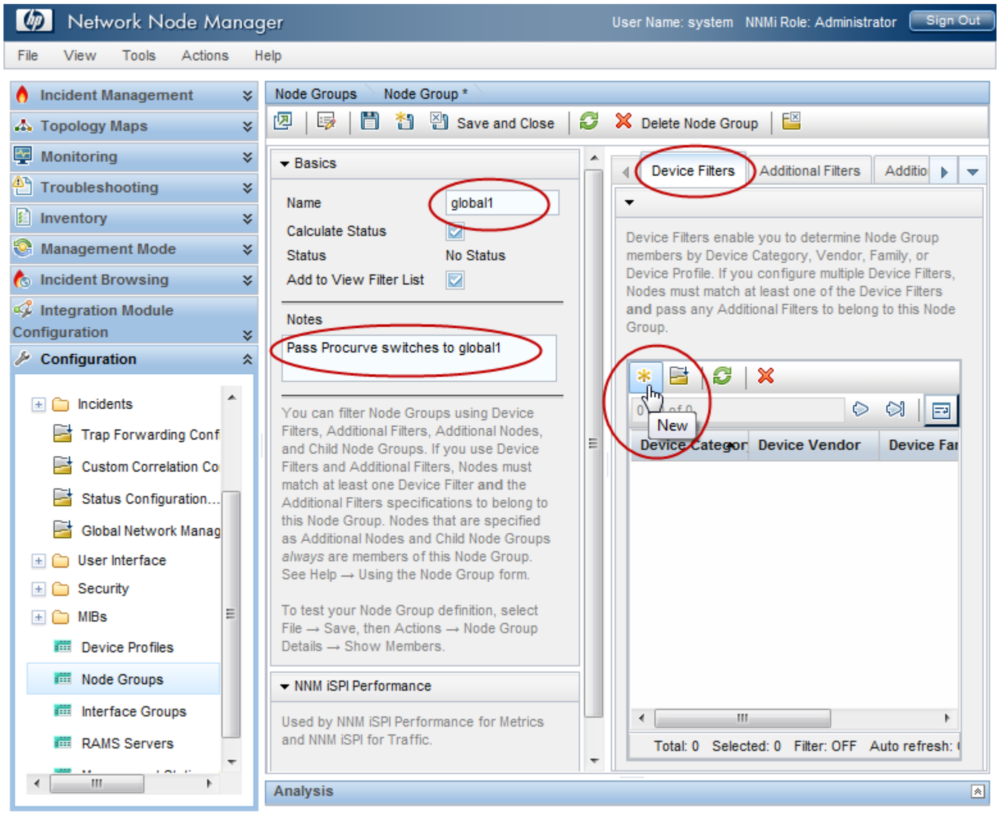
You can filter Node Groups using Device Filters, Additional Filters, Additional Nodes, and Child Node Groups. If you use Device Filters and Additional Filters, Nodes must match at least one Device Filter and the Additional Filters specifications to belong to this Node Group. Nodes that are specified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

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

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

Device Filters enable you to determine Node (members by Device Category, Vendor, Family Device Profile. If you configure multiple Devic Nodes must match at least one of the Device and pass any Additional Filters to belong to t Group.

4 Click the **New** icon to open a `Node Device Filter` form.



Name: global1
Calculate Status ☑
Status: No Status
Add to View Filter List ☑

Notes: Pass Procurve switches to global1

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

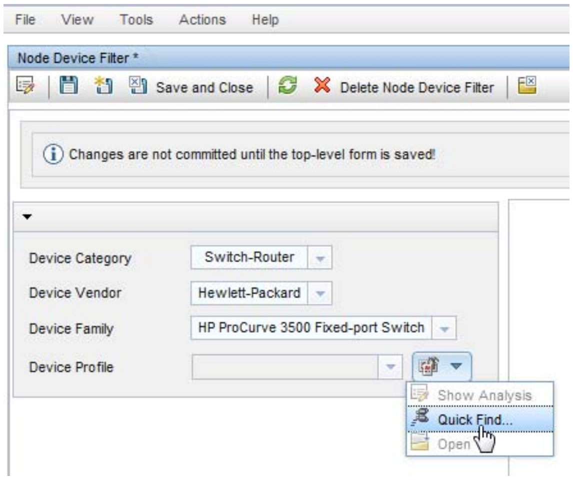
To test your Node Group definition, select File → Save, then Actions → Node Group Details → Show Members.

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

Device Filters enable you to determine Node Group members by Device Category, Vendor, Family, or Device Profile. If you configure multiple Device Filters, Nodes must match at least one of the Device Filters and pass any Additional Filters to belong to this Node Group.

5 Using the pull-down, select the `Switch Router` Device Category`,` the `Hewlett-Packard` Device Vendor, and the `HP Procurve 3500 Fixed-port Switch` Device Family.

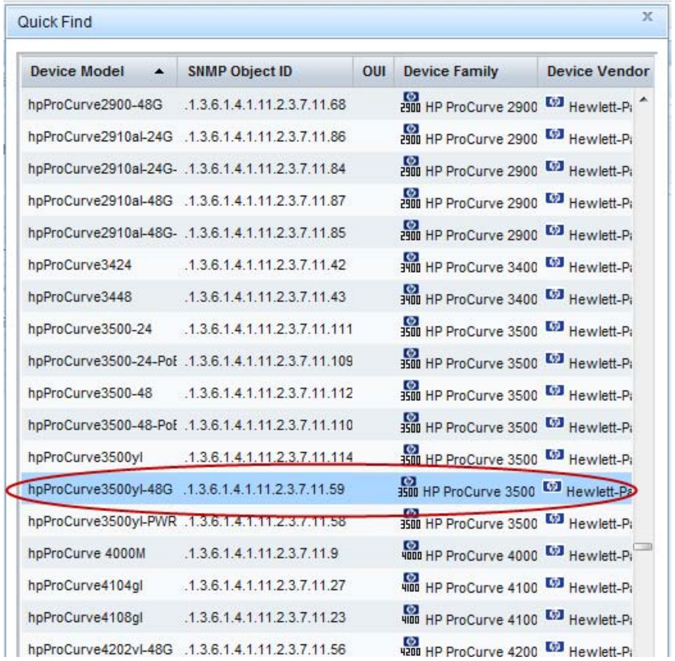
6 Using the pull-down, click **Quick Find** to open a `Device Profile` form.



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

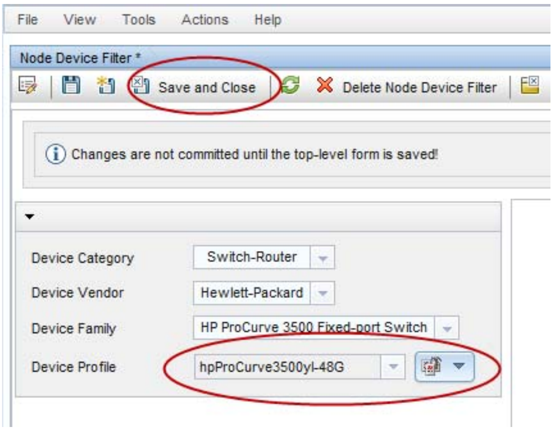
Device Category: Switch-Router
Device Vendor: Hewlett-Packard
Device Family: HP ProCurve 3500 Fixed-port Switch
Device Profile:

7 Find and select the profile for the HP Procurve 3500yl Switch; then click **OK**.



Device Model	SNMP Object ID	OUI	Device Family	Device Vendor
hpProCurve2900-48G	.1.3.6.1.4.1.11.2.3.7.11.68		HP ProCurve 2900	Hewlett-Pa
hpProCurve2910al-24G	.1.3.6.1.4.1.11.2.3.7.11.86		HP ProCurve 2900	Hewlett-Pa
hpProCurve2910al-24G-	.1.3.6.1.4.1.11.2.3.7.11.84		HP ProCurve 2900	Hewlett-Pa
hpProCurve2910al-48G	.1.3.6.1.4.1.11.2.3.7.11.87		HP ProCurve 2900	Hewlett-Pa
hpProCurve2910al-48G-	.1.3.6.1.4.1.11.2.3.7.11.85		HP ProCurve 2900	Hewlett-Pa
hpProCurve3424	.1.3.6.1.4.1.11.2.3.7.11.42		HP ProCurve 3400	Hewlett-Pa
hpProCurve3448	.1.3.6.1.4.1.11.2.3.7.11.43		HP ProCurve 3400	Hewlett-Pa
hpProCurve3500-24	.1.3.6.1.4.1.11.2.3.7.11.111		HP ProCurve 3500	Hewlett-Pa
hpProCurve3500-24-PoE	.1.3.6.1.4.1.11.2.3.7.11.109		HP ProCurve 3500	Hewlett-Pa
hpProCurve3500-48	.1.3.6.1.4.1.11.2.3.7.11.112		HP ProCurve 3500	Hewlett-Pa
hpProCurve3500-48-PoE	.1.3.6.1.4.1.11.2.3.7.11.110		HP ProCurve 3500	Hewlett-Pa
hpProCurve3500yl	.1.3.6.1.4.1.11.2.3.7.11.114		HP ProCurve 3500	Hewlett-Pa
hpProCurve3500yl-48G	.1.3.6.1.4.1.11.2.3.7.11.59		HP ProCurve 3500	Hewlett-Pa
hpProCurve3500yl-PWR	.1.3.6.1.4.1.11.2.3.7.11.58		HP ProCurve 3500	Hewlett-Pa
hpProCurve 4000M	.1.3.6.1.4.1.11.2.3.7.11.9		HP ProCurve 4000	Hewlett-Pa
hpProCurve4104gl	.1.3.6.1.4.1.11.2.3.7.11.27		HP ProCurve 4100	Hewlett-Pa
hpProCurve4108gl	.1.3.6.1.4.1.11.2.3.7.11.23		HP ProCurve 4100	Hewlett-Pa
hpProCurve4202vl-48G	.1.3.6.1.4.1.11.2.3.7.11.56		HP ProCurve 4200	Hewlett-Pa

8 Click **Save and Close** two times.

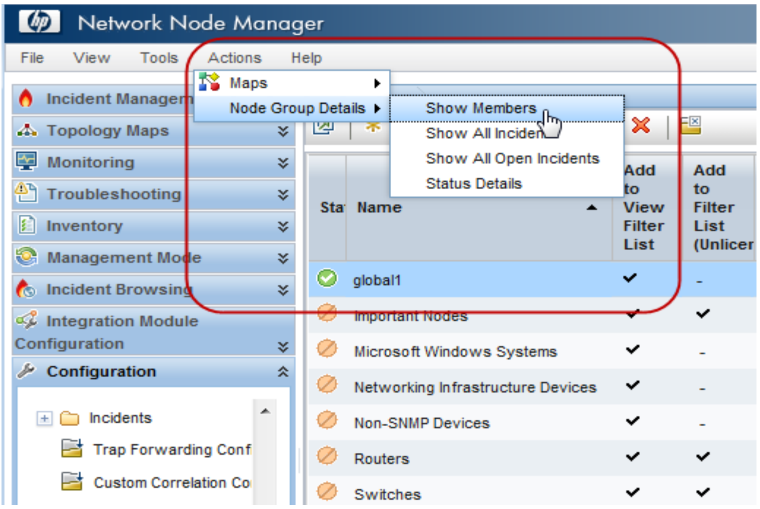


Changes are not committed until the top-level form is saved!

Device Category	Switch-Router
Device Vendor	Hewlett-Packard
Device Family	HP ProCurve 3500 Fixed-port Switch
Device Profile	hpProCurve3500yl-48G

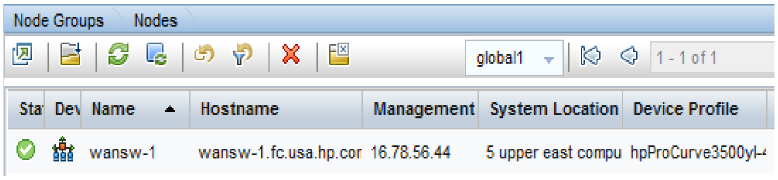
9 To test this filter, select **global1**.

10 Using the pull-down, click **Show Members**.



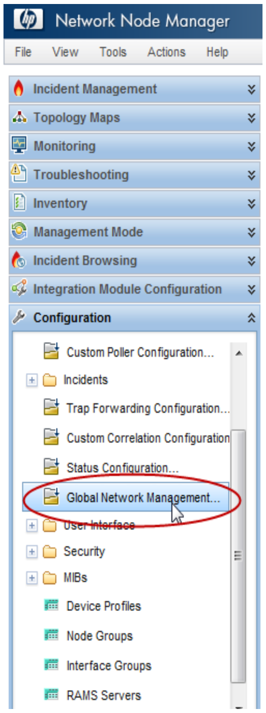
Sta	Name	Add to View Filter List	Add to Filter List (Unlicer
✓	global1	✓	-
	Important Nodes	✓	✓
	Microsoft Windows Systems	✓	-
	Networking Infrastructure Devices	✓	-
	Non-SNMP Devices	✓	-
	Routers	✓	✓
	Switches	✓	✓

11 Notice that NNMi discovered 1 HP 3500yl switch already. This shows you that the filter you created is finding the specific switch models you configured it for. The next step is to configure the forwarding filter using this node filter you just created.

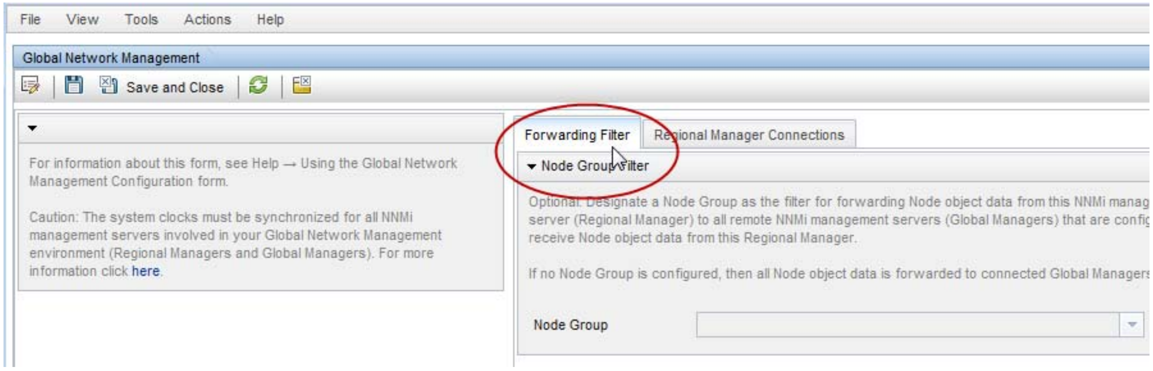


Sta	Dev	Name	Hostname	Management	System Location	Device Profile
✓		wansw-1	wansw-1.fc.usa.hp.cor	16.78.56.44	5 upper east compu	hpProCurve3500yl-4

12 From regional1's **Configuration** workspace in the NNMi console, click **Global Network Management**.



13 Click the **Forwarding Filter** tab.



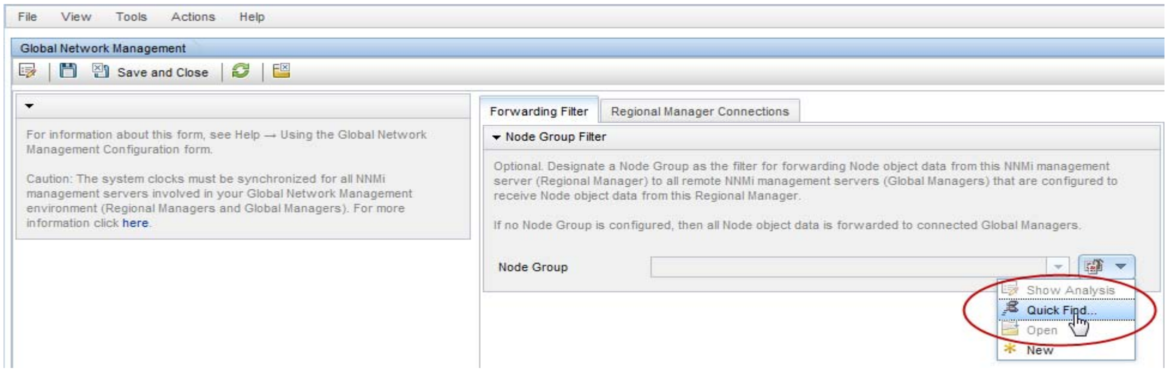
For information about this form, see Help → Using the Global Network Management Configuration form.

Caution: The system clocks must be synchronized for all NNMi management servers involved in your Global Network Management environment (Regional Managers and Global Managers). For more information click here.

Optional. Designate a Node Group as the filter for forwarding Node object data from this NNMi manag server (Regional Manager) to all remote NNMi management servers (Global Managers) that are config receive Node object data from this Regional Manager.

If no Node Group is configured, then all Node object data is forwarded to connected Global Managers

14 Click **Quick Find**.



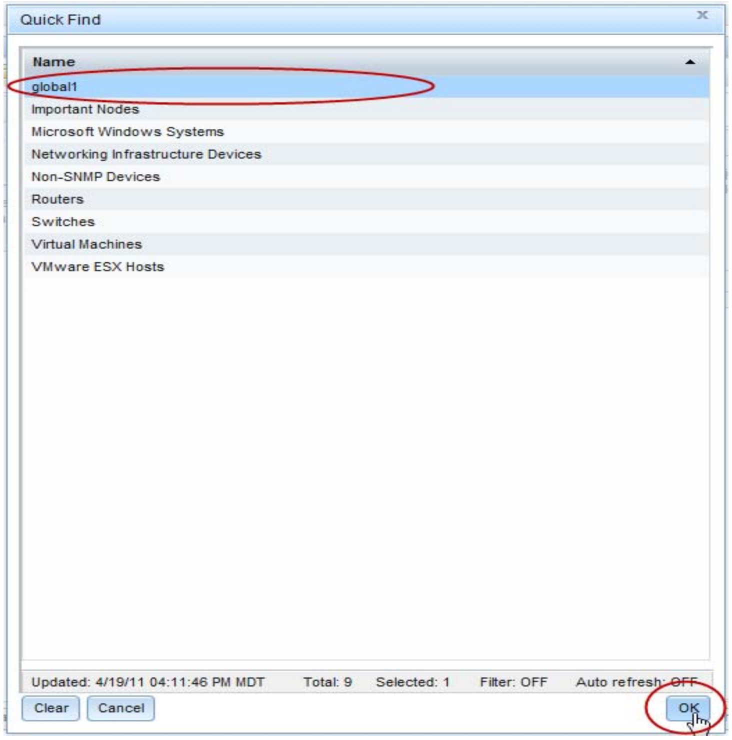
For information about this form, see Help → Using the Global Network Management Configuration form.

Caution: The system clocks must be synchronized for all NNMi management servers involved in your Global Network Management environment (Regional Managers and Global Managers). For more information click here.

Optional. Designate a Node Group as the filter for forwarding Node object data from this NNMi management server (Regional Manager) to all remote NNMi management servers (Global Managers) that are configured to receive Node object data from this Regional Manager.

If no Node Group is configured, then all Node object data is forwarded to connected Global Managers.

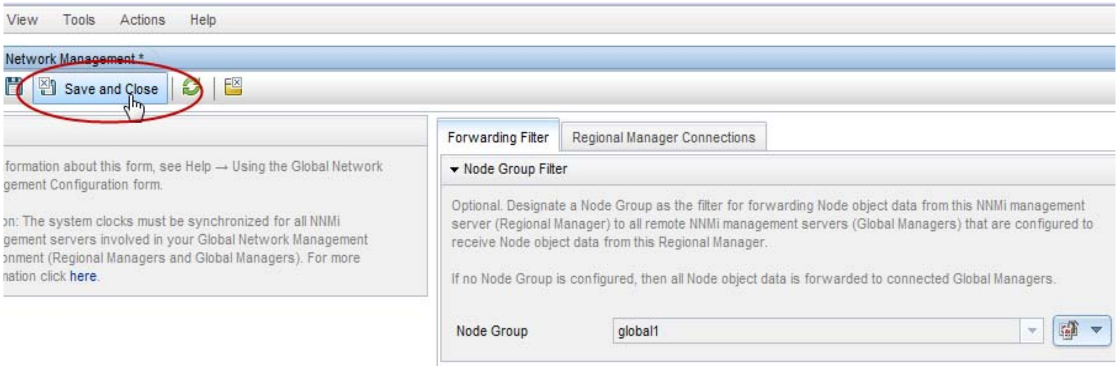
15 Select the **global1** filter; then click **OK**.



Name
global1
Important Nodes
Microsoft Windows Systems
Networking Infrastructure Devices
Non-SNMP Devices
Routers
Switches
Virtual Machines
VMware ESX Hosts

Updated: 4/19/11 04:11:46 PM MDT Total: 9 Selected: 1 Filter: OFF Auto refresh: OFF

16 Click **Save and Close**.



formation about this form, see Help → Using the Global Network gement Configuration form.

on: The system clocks must be synchronized for all NNMi gement servers involved in your Global Network Management onment (Regional Managers and Global Managers). For more nation click here.

Optional. Designate a Node Group as the filter for forwarding Node object data from this NNMi management server (Regional Manager) to all remote NNMi management servers (Global Managers) that are configured to receive Node object data from this Regional Manager.

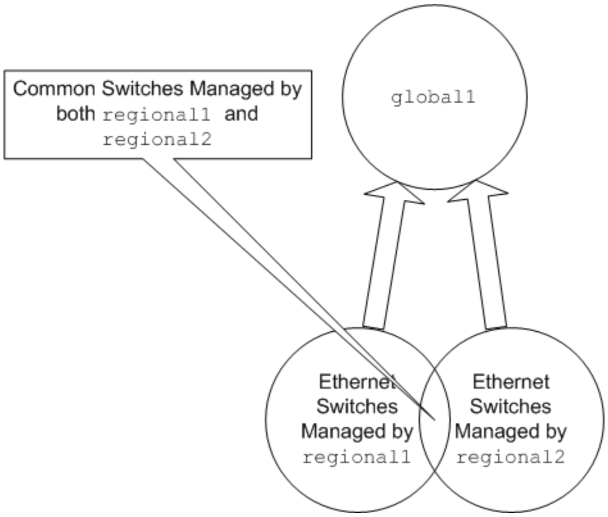
If no Node Group is configured, then all Node object data is forwarded to connected Global Managers.

Node Group: global1

This completes the task of setting up a forwarding filter on `regional1`. After you complete step 1 through step 16 for `regional2`, move on to the next section to connect `global1` to `regional1` and `regional2`.

Connecting a Global Manager with a Regional Manager

As mentioned earlier, suppose that `regional1` and `regional2` both manage several common switches. Suppose that you want this common switch information forwarded to `global1` from `regional1`.


Common Switches Managed by both regional1 and regional2
global1
Ethernet Switches Managed by regional1
Ethernet Switches Managed by regional2

To make that happen you must connect `global1` to `regional1` before connecting it to `regional2`. By using that connection sequence, `global1` considers `regional1` to be the NNMi management server monitoring these common switches. `Global1` also ignores information about these common switches that it receives from `regional2`.

➤ HP recommends you use this feature on a small scale to better understand how it works, then expand it to meet your network management needs.

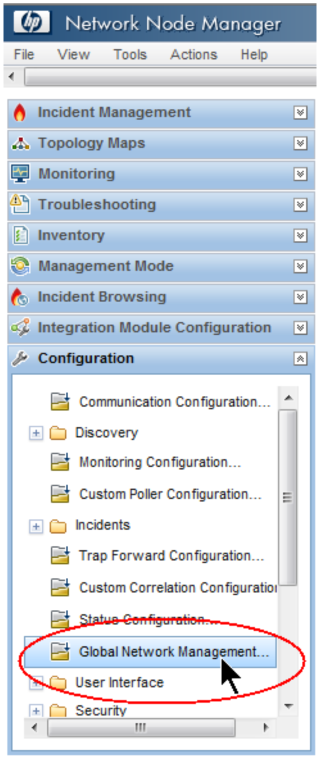
To connect `global1` first to `regional1`, then to `regional2`, complete the following steps:

1 As mentioned earlier, synchronize the NNMi management server clocks for `global1`, `regional1`, and `regional2` before you connect these servers in a global network management configuration. See *Clock Synchronization Issues* in the NNMi help for more information.

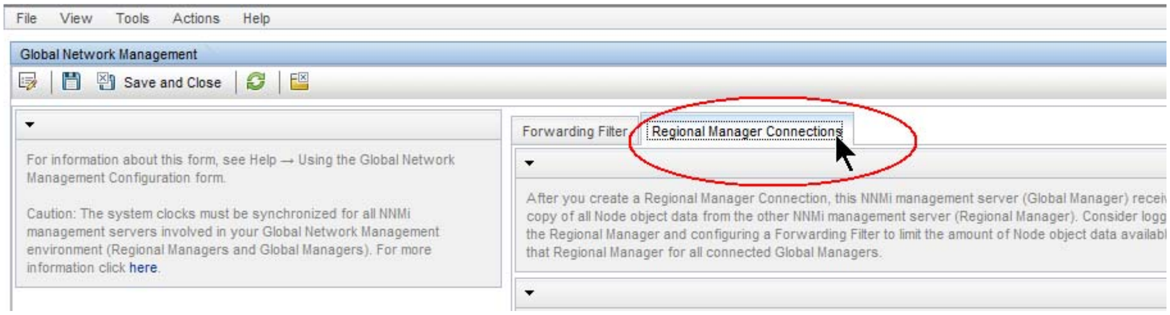
➤ NNMi opens a warning message if there is a connection problem with a regional manager, such as a server clock synchronization problem.

2 Set up a connection from `global1` to `regional1`.

a From the `global1` NNMi console, click **Global Network Management** in the **Configuration** workspace.


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

b Click **Regional Manager Connections**.

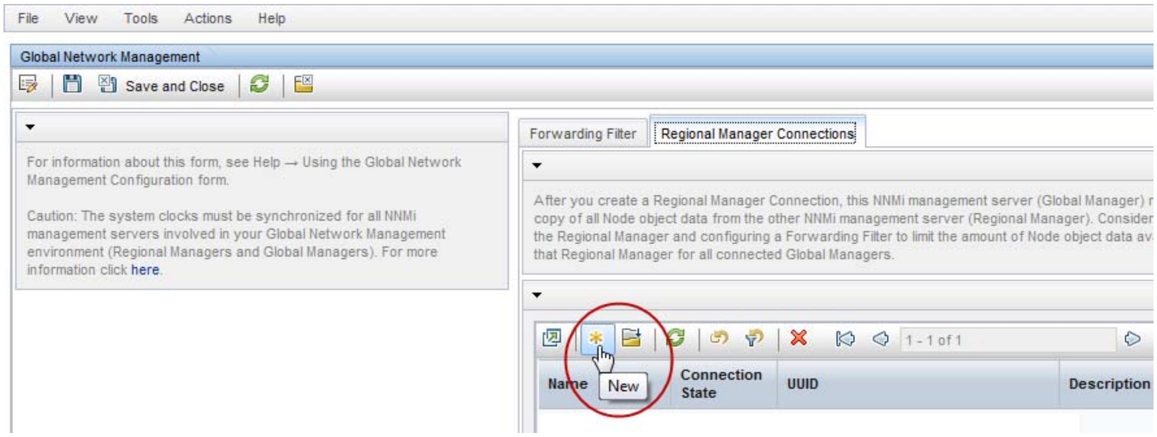

File View Tools Actions Help
Global Network Management
Save and Close
Forwarding Filter
Regional Manager Connections

For information about this form, see Help → Using the Global Network Management Configuration form.

Caution: The system clocks must be synchronized for all NNMi management servers involved in your Global Network Management environment (Regional Managers and Global Managers). For more information click here.

After you create a Regional Manager Connection, this NNMi management server (Global Manager) recei copy of all Node object data from the other NNMi management server (Regional Manager). Consider logg the Regional Manager and configuring a Forwarding Filter to limit the amount of Node object data availabl that Regional Manager for all connected Global Managers.

c Click the **New** icon to create a new regional manager.



For information about this form, see Help → Using the Global Network Management Configuration form.

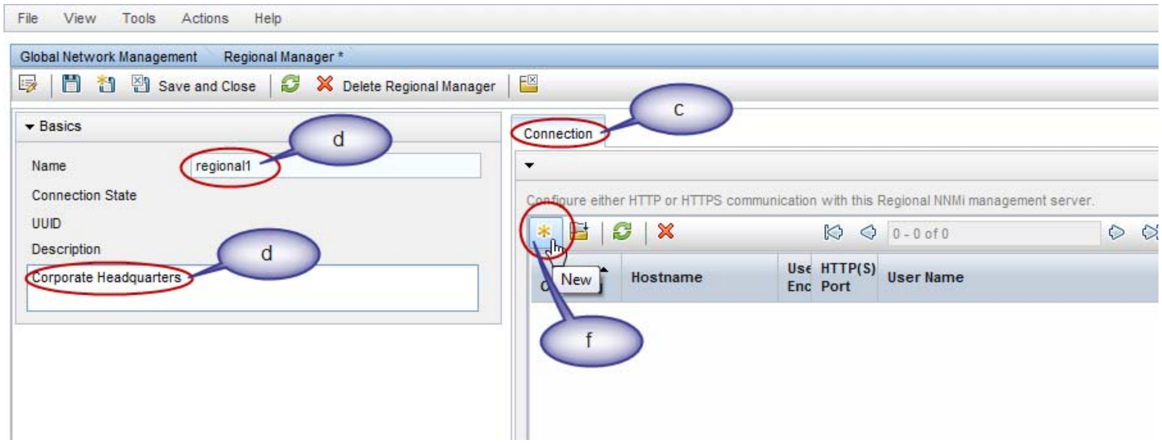
Caution: The system clocks must be synchronized for all NNMi management servers involved in your Global Network Management environment (Regional Managers and Global Managers). For more information click here.

After you create a Regional Manager Connection, this NNMi management server (Global Manager) r copy of all Node object data from the other NNMi management server (Regional Manager). Consider the Regional Manager and configuring a Forwarding Filter to limit the amount of Node object data av that Regional Manager for all connected Global Managers.

d Add the name and description information for `regional1`.

e Click the **Connection** Tab.

f Click the **New** icon.



Name: regional1

Connection State

UUID

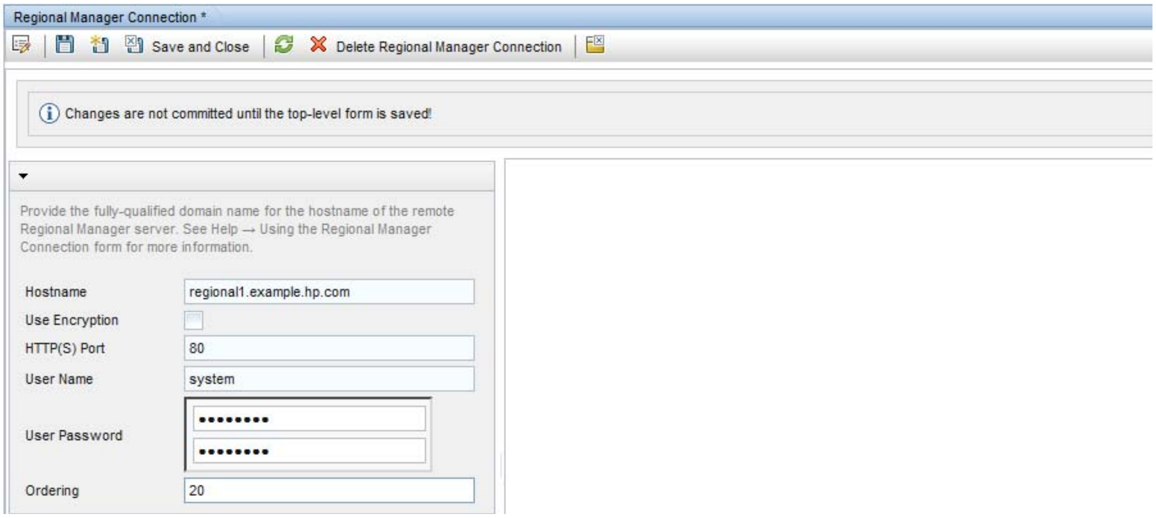
Description: Corporate Headquarters

Configure either HTTP or HTTPS communication with this Regional NNMi management server.

g Add the connection information for `regional1`

➤ See **Help->Using the Regional Manager Connection Form** in the NNMi help for specific information about the entries to make in this form

.


Regional Manager Connection *
Save and Close
Delete Regional Manager Connection

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

Provide the fully-qualified domain name for the hostname of the remote Regional Manager server. See Help → Using the Regional Manager Connection form for more information.

Hostname	regional1.example.hp.com
Use Encryption	□
HTTP(S) Port	80
User Name	system
User Password	•••••••• ••••••••
Ordering	20

h Click **Save and Close** two times to save your work.

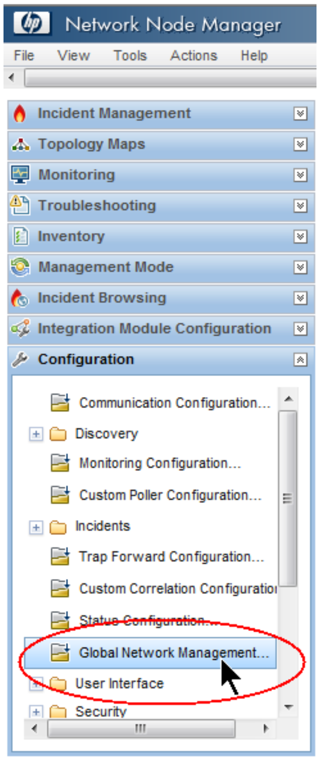
3 Complete step a on page 239 through step g on page 241 to establish a connection from `global1` to `regional2`.

Determining the Connection States from global1 to regional1 and regional2

To check the connection states from global1 to `regional1` and `regional2`, complete the following steps:

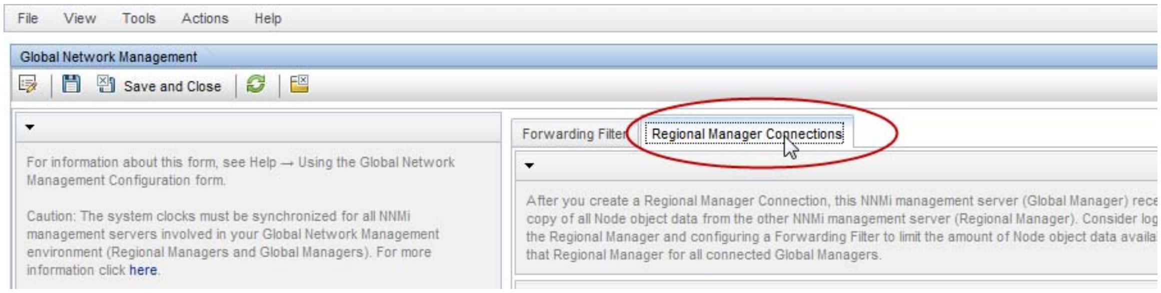
1 From the `global1` NNMi console, click **Global Network Management** in the **Configuration** workspace.

.



2 Click the **Regional Managers Connections** tab.

.



For information about this form, see Help → Using the Global Network Management Configuration form.

Caution: The system clocks must be synchronized for all NNMi management servers involved in your Global Network Management environment (Regional Managers and Global Managers). For more information click here.

After you create a Regional Manager Connection, this NNMi management server (Global Manager) rece copy of all Node object data from the other NNMi management server (Regional Manager). Consider log the Regional Manager and configuring a Forwarding Filter to limit the amount of Node object data availa that Regional Manager for all connected Global Managers.

3 Check the status of regional1 and regional2 by checking their connection states. Notice that the connection states are shown as Connected, which means they are functioning properly.

See *Determine the State of the Connection to a Regional Manager* in the NNMi help for more information.

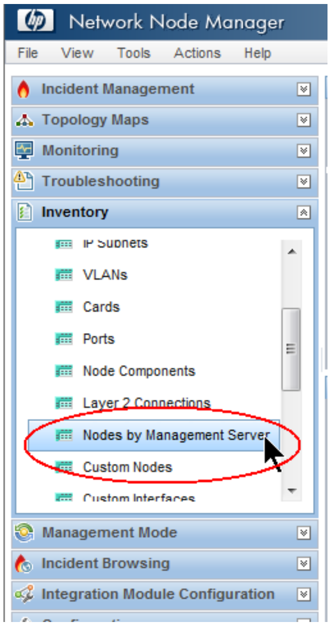
Do not continue to the next section until NNMi completes a good discovery. See *Checking Discovery Progress* in the *NNMi Installation Guide* for more information.

Reviewing global1 Inventory

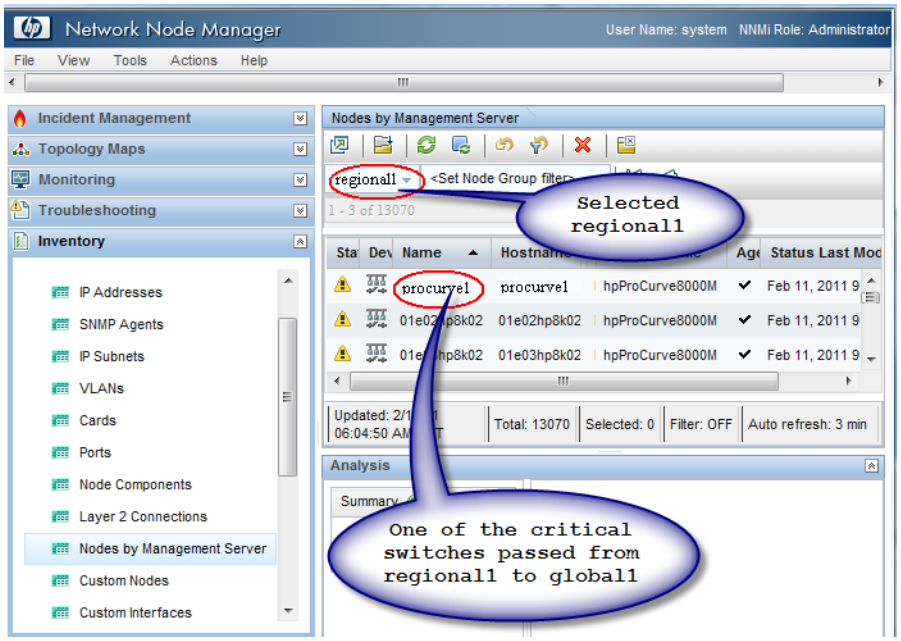
Do not complete this section until NNMi completes a good discovery. See *Checking Discovery Progress* in the *NNMi Installation Guide* for more information.

To view the node information regional1 forwarded to global1, complete the following steps:

1 From the global1 NNMi console, navigate to the **Nodes by Management Server** form located in the **Inventory** workspace.



2 Assume that `regional1` passed information about switch `procurve1.x.y.z` to `global1`. After selecting **regional1**, the inventory might look as follows:



Sta	Dev	Name	Hostname		Age	Status Last Mod
⚠		procurve1	procurve1	hpProCurve8000M	✓	Feb 11, 2011 9
⚠		01e02hp8k02	01e02hp8k02	hpProCurve8000M	✓	Feb 11, 2011 9
⚠		01e hp8k02	01e03hp8k02	hpProCurve8000M	✓	Feb 11, 2011 9

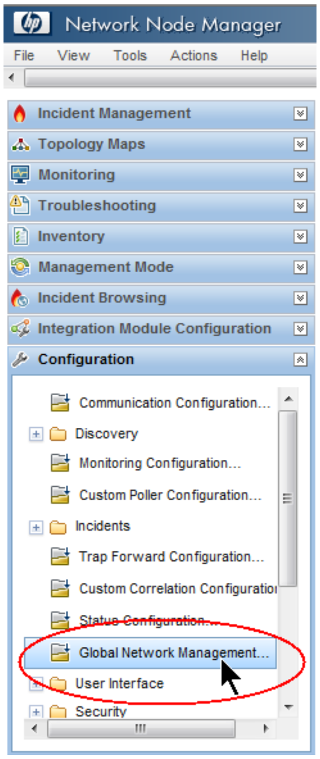
Updated: 2/1 1 06:04:50 AM T | Total: 13070 | Selected: 0 | Filter: OFF | Auto refresh: 3 min

Complete step 1 through step 2 to look at the device inventory passed to global1 from other connected regional managers.

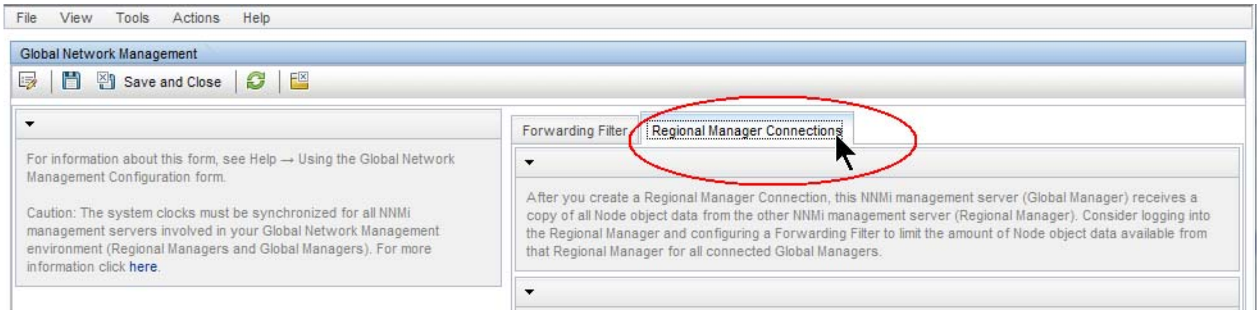
Disconnecting Communication between global1 and regional1

Suppose you plan to permanently shut down global1 or to shut it down for a number of days. Assume for this example that global1 still has active subscriptions to regional1. You must complete some additional steps to complete the shutdown:

1 From the global1 NNMi console, click **Global Network Management** in the **Configuration** workspace.


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

2 Click Regional Manager Connections.

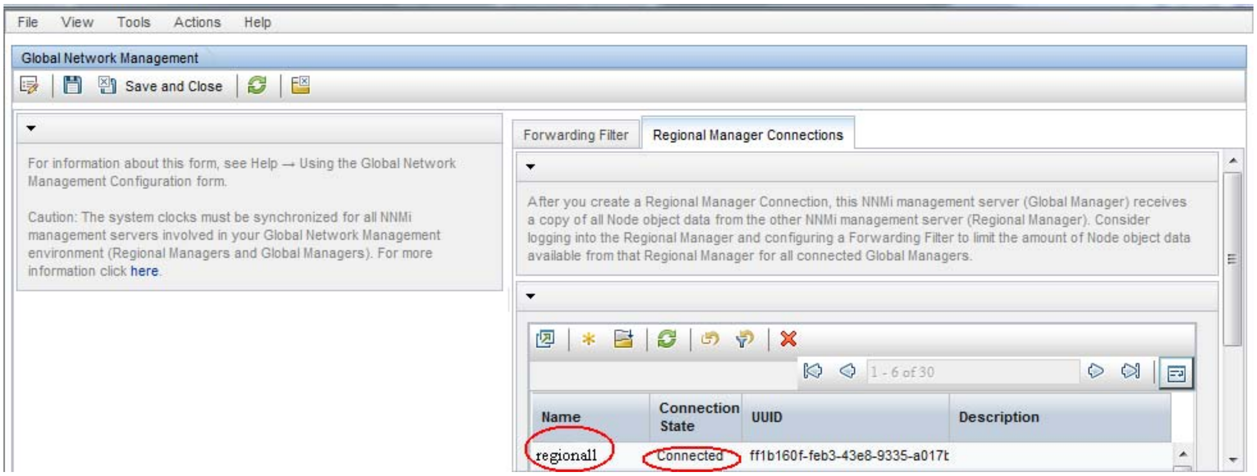

File View Tools Actions Help
Global Network Management
Save and Close
Forwarding Filter
Regional Manager Connections

For information about this form, see Help → Using the Global Network Management Configuration form.

Caution: The system clocks must be synchronized for all NNMi management servers involved in your Global Network Management environment (Regional Managers and Global Managers). For more information click here.

After you create a Regional Manager Connection, this NNMi management server (Global Manager) receives a copy of all Node object data from the other NNMi management server (Regional Manager). Consider logging into the Regional Manager and configuring a Forwarding Filter to limit the amount of Node object data available from that Regional Manager for all connected Global Managers.

3 Check to make sure the status is `Connected`. If the status is not `Connected`, diagnose the problem using information from the *Troubleshoot Global Network Management* topic in the NNMi help before continuing.


File View Tools Actions Help
Global Network Management
Save and Close
Forwarding Filter
Regional Manager Connections
1 - 6 of 30

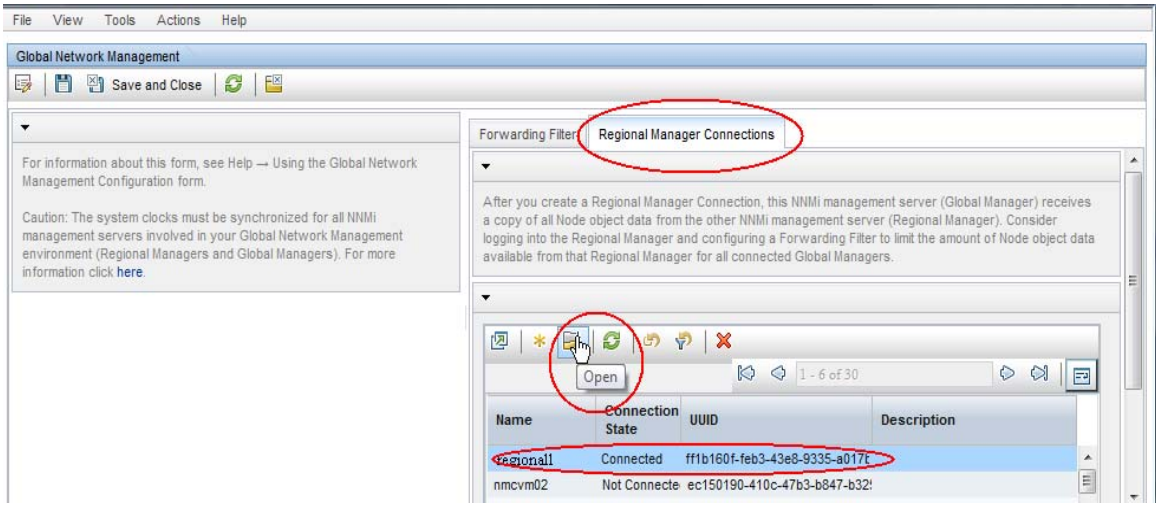
For information about this form, see Help → Using the Global Network Management Configuration form.

Caution: The system clocks must be synchronized for all NNMi management servers involved in your Global Network Management environment (Regional Managers and Global Managers). For more information click here.

After you create a Regional Manager Connection, this NNMi management server (Global Manager) receives a copy of all Node object data from the other NNMi management server (Regional Manager). Consider logging into the Regional Manager and configuring a Forwarding Filter to limit the amount of Node object data available from that Regional Manager for all connected Global Managers.

Name	Connection State	UUID	Description
regional1	Connected	ff1b160f-feb3-43e8-9335-a017t	

4 Select `regional1`, then click the `Open` icon.


File View Tools Actions Help
Global Network Management
Save and Close
Forwarding Filter
Regional Manager Connections
Open
1 - 6 of 30

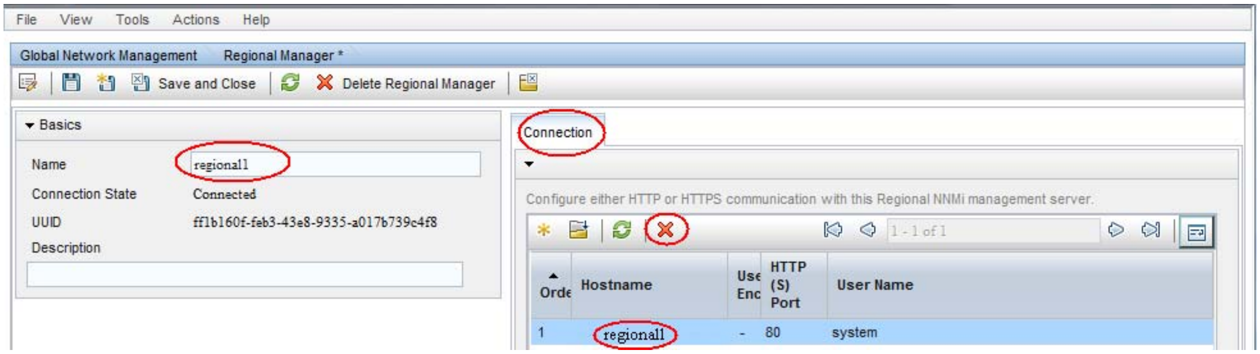
For information about this form, see Help → Using the Global Network Management Configuration form.

Caution: The system clocks must be synchronized for all NNMi management servers involved in your Global Network Management environment (Regional Managers and Global Managers). For more information click here.

After you create a Regional Manager Connection, this NNMi management server (Global Manager) receives a copy of all Node object data from the other NNMi management server (Regional Manager). Consider logging into the Regional Manager and configuring a Forwarding Filter to limit the amount of Node object data available from that Regional Manager for all connected Global Managers.

Name	Connection State	UUID	Description
regional1	Connected	ff1b160f-feb3-43e8-9335-a017t	
nmcvm02	Not Connecte	ec150190-410c-47b3-b847-b32!	

5 Click **Connection**, select **regional1.x.y.z**, then click the **Delete** icon.



Name	regional1
Connection State	Connected
UUID	ff1b160f-feb3-43e8-9335-a017b739c4f8
Description	

Configure either HTTP or HTTPS communication with this Regional NNMi management server.

Orde	Hostname	Use Enc	HTTP (S) Port	User Name
1	regional1	-	80	system

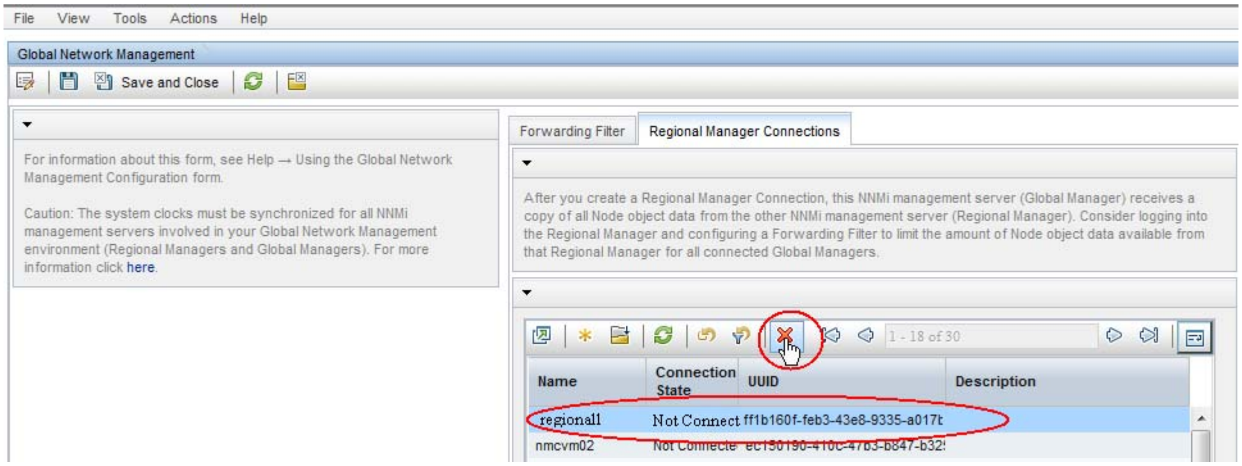
6 Click **Save and Close**.

7 In the `Regional Manager Connections` tab, note the `Name` attribute value for `regional1` (case-sensitive). You need this text string for the `RemoteNNMiServerName` variable in a later step.

8. Click **Save and Close** again.
9. On `global1`, at the command line, type the following command:

   `nnmnodedelete.ovpl -rm regional1 -u` *NNMiadminUserName* **`-p`** *NNMiadminPassword*

10. These commands remove the node records from `global1` that `regional1` forwarded to it. The commands also close incidents associated with the nodes forwarded to `global1` from `regional1`. For detailed information, see *Disconnect Communication with a Regional Manager* in the NNMi help.
11. To remove the configuration records for `regional1`, do the following.
    - a Click the **Configuration** workspace.
    - b Select the **Global Network Management** form.
    - c Select the **Regional Manager Connections** tab.
    - d Select `regional1`, then click the `Delete` icon.



For information about this form, see Help → Using the Global Network Management Configuration form.

Caution: The system clocks must be synchronized for all NNMi management servers involved in your Global Network Management environment (Regional Managers and Global Managers). For more information click here.

After you create a Regional Manager Connection, this NNMi management server (Global Manager) receives a copy of all Node object data from the other NNMi management server (Regional Manager). Consider logging into the Regional Manager and configuring a Forwarding Filter to limit the amount of Node object data available from that Regional Manager for all connected Global Managers.

Name	Connection State	UUID	Description
regional1	Not Connect	ff1b160f-feb3-43e8-9335-a017t	
nmcvm02	Not Connecte	ec150190-410c-47b3-b847-b32!	

    - e Click **Save and Close** to save your deletions.

12. Complete step 1 through step 11 for other regional NNMi management servers, such as `regional2`, that are connected to `global1`.

Additional Information

Discovery and Data Synchronization

As network administrators add, delete, or modify devices on a network, regional servers, such as `regional1` and `regional2`, discover those changes and update global servers, such as `global1` in the example in this chapter, `regional1` and `regional2` also notify `global1` of changes that administrators make to the management mode of a node it manages.

> ➤ To maintain consistency, as `regional1` and `regional2` discover device state changes, they continuously update `global1`, thereby maintaining identical node states on both the global and regional servers.

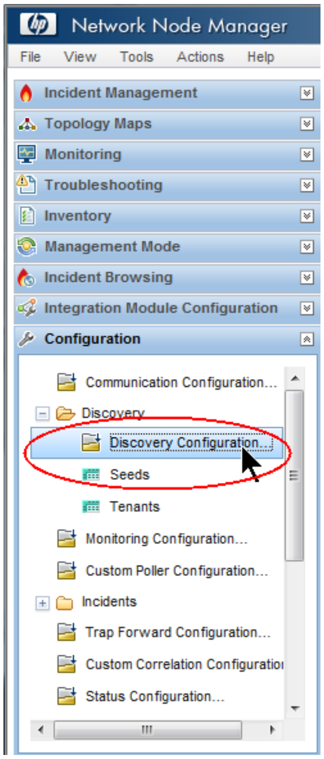
Any time global1 requests information about a node that is managed by regional1 or regional2, regional1 or regional2 responds to global1 with the requested information. global1 never talks directly to a node. There will not be duplicate SNMP queries to devices when global1 performs a discovery.

global1 synchronizes with regional1 and regional2 each time regional1 or regional2 completes a discovery. NNMi uses FDB (Forwarding Database) data to calculate layer 2 connections. FDB data is very dynamic, and varies a lot between discoveries, especially if there are multiple regionals connected to a global.

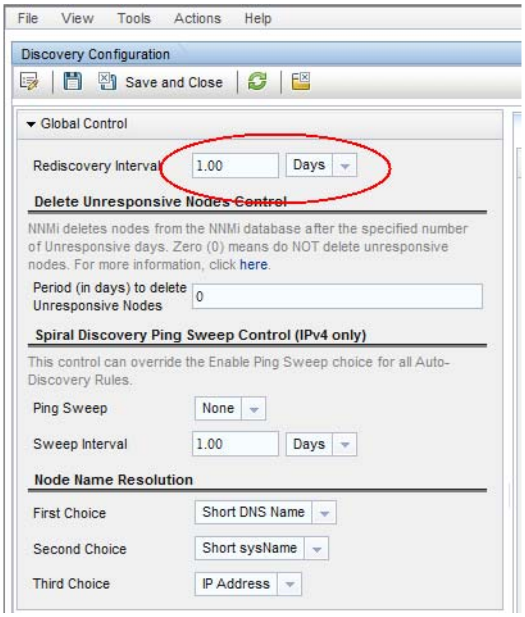
Changes to user-modified or application-modified attributes are not updated on the global during a synchronization.

The Rediscovery Interval is adjustable on each regional, and can make a difference in the discovery accuracy between global1 and the regional managers. The shorter the Rediscovery Interval, the more accurate the discovery, and the more NNMi-generated network traffic. The longer the Rediscovery Interval, the less accurate the discovery, and the less NNMi-generated network traffic. This means that the larger your network grows, the less frequently you might want to rediscover. To set the Rediscovery Interval, do the following steps:

From the regional1or regional2 NNMi console, click **Discovery Configuration** in the **Configuration** workspace.



13 Adjust the `Rediscovery Interval` according to your how often you want the regionals to initiate a discovery. The global will initiate a discovery immediately after a regional completes a discovery.



Rediscovery Interval: 1.00 Days

Delete Unresponsive Nodes Control

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

Period (in days) to delete Unresponsive Nodes: 0

Spiral Discovery Ping Sweep Control (IPv4 only)

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

Ping Sweep: None

Sweep Interval: 1.00 Days

Node Name Resolution

First Choice: Short DNS Name

Second Choice: Short sysName

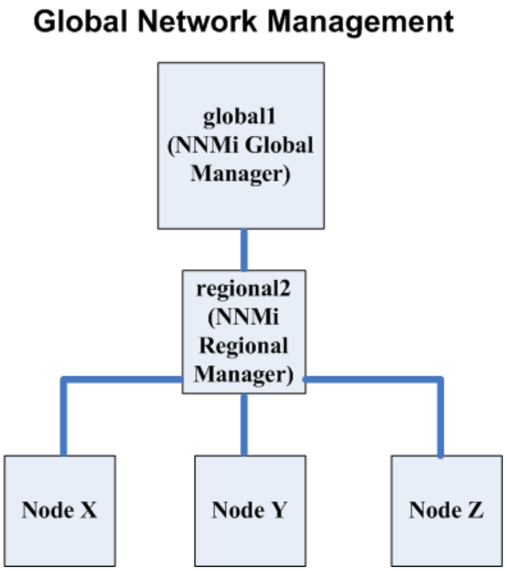
Third Choice: IP Address

14 Click **Save and Close**.

Status Poll or Configuration Poll a Device

Suppose regional NNMi management server `regional2` discovers and manages `Node X` and global NNMi management server `global1` connects with regional NNMi management server `regional2`.

Figure 16 Status Poll or Configuration Poll a Node


Global Network Management
global1 (NNMi Global Manager)
regional2 (NNMi Regional Manager)
Node X
Node Y
Node Z

To status poll `Node X` from `global1`, do the following:

1. From `global1`, click **Nodes** in the **Inventory** workspace.
2. Select `Node X` from the nodes inventory.
3. Request a status poll of `Node X` using the **Actions > Status Poll** menu item.
4. NNMi management server `global1` requests a status poll from regional NNMi management server `regional2` and shows the results on your screen. It does not matter if you initiate the status poll request from either `global1` or `regional2`. You still see the same status poll results.

If you want `global1` to have the most current discovery information for `Node X`, do the following to configuration poll `Node X` from `global1`.

1. From `global1`, click **Nodes** in the **Inventory** workspace.
2. Select `Node X` from the nodes inventory.
3. Request a configuration poll of `Node X` using the **Actions > Configuration Poll** menu item.
4. NNMi management server `global1` requests a configuration poll from regional NNMi management server `regional2` and shows the results on your screen. It does not matter if you initiate the configuration poll request from either `global1` or `regional2`. You still see the same configuration poll results.

Determining Device Status and NNMi Incident Generation using a Global Manager

NNMi management server global1 listens for state changes coming from regional managers regional1 and regional2 and updates the states in its local database.

The NNMi StatePoller services on NNMi management servers regional1 and regional2 calculate state values for the devices it monitors. global1 receives state value updates from regional1 and regional2. global1 polls nodes that it discovers, and does not poll nodes being managed by regional1 and regional2.

After you change the management mode of a node being managed by regional1, you see that management mode change on global1 as well. As network administrators add, remove, or modify network equipment being managed by regional1 or regional2, regional1 or regional2 updates global1 of these network device changes.

global1 generates incidents using its own causal engine and topology, including the node object data forwarded to it by regional1 and regional2. This means that the incidents it generates might be slightly different from the regional1 and regional2 incidents if there are differences in topology.

It is better to avoid using a forwarding filter on regional1 or regional2, as filtering might affect the connectivity on global1 . The result could be a difference in the root cause analysis between global1 and the two regionals (regional1 and regional2). In most cases, if you choose to avoid using forwarding filters, a global NNMi management server will have a larger topology. This helps it draw more accurate root cause analysis conclusions.

Without additional configuration, regional1 does not forward traps to global1. To do this, you must configure regional1 to forward specific traps to global1. HP recommends you only configure regional managers to forward low-volume, important traps to avoid excessive burden on the global manager. NNMi drops forwarded traps if the forwarded traps result in a TrapStorm incident. See the TrapStorm Management Event details in the NNMi console.

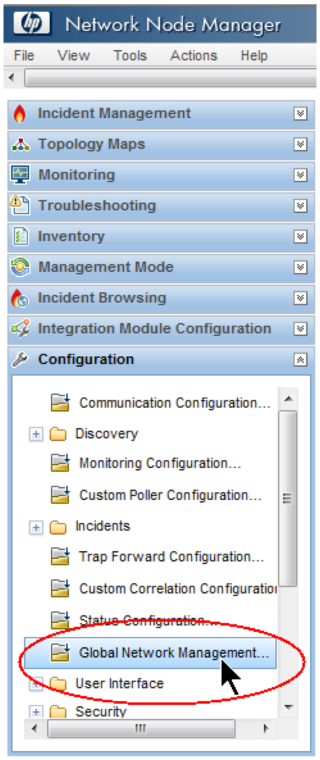
Configuring Application Failover for Global Network Management

You can configure both global and regional managers to use application failover. The global or regional manager automatically detects and connects to the active system.

Configuring Application Failover on a Global Manager

To configure global1 to recognize the application failover do the following:

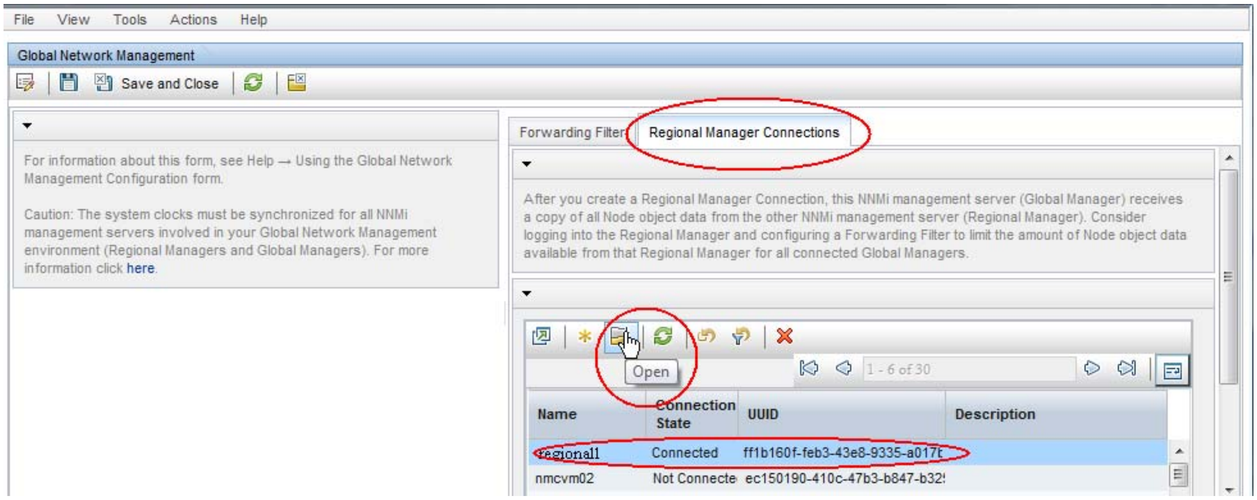
1 From the global1 NNMi console, click **Global Network Management** in the **Configuration** workspace.


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

Suppose you configured regional1 for application failover, and regional1_backup. as the secondary server.

2 Click **Regional Manager Connections**.

3 Select `regional1`, then click the **Open** icon.


File View Tools Actions Help
Global Network Management
Save and Close
Forwarding Filter
Regional Manager Connections
Open
1 - 6 of 30

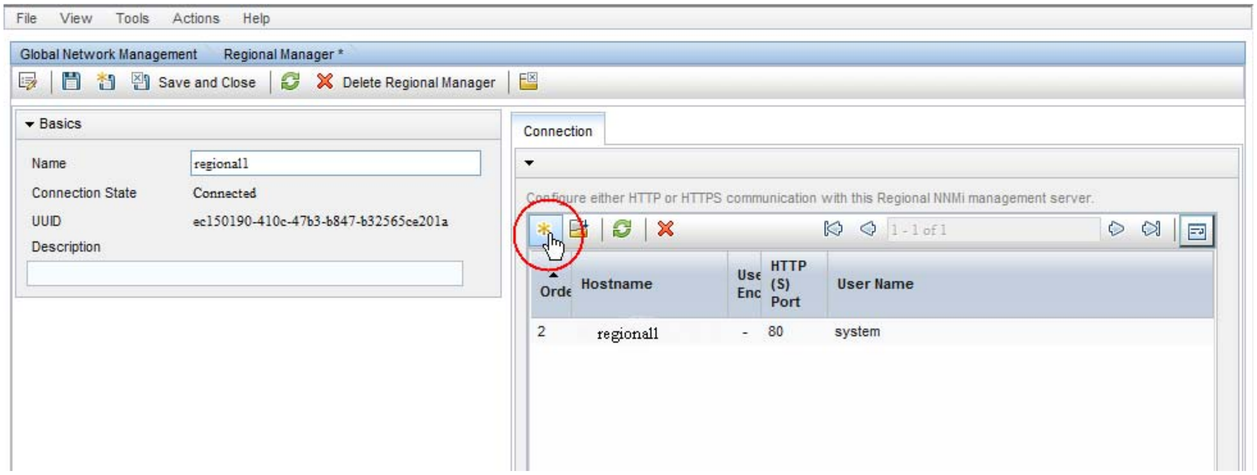
For information about this form, see Help → Using the Global Network Management Configuration form.

Caution: The system clocks must be synchronized for all NNMi management servers involved in your Global Network Management environment (Regional Managers and Global Managers). For more information click here.

After you create a Regional Manager Connection, this NNMi management server (Global Manager) receives a copy of all Node object data from the other NNMi management server (Regional Manager). Consider logging into the Regional Manager and configuring a Forwarding Filter to limit the amount of Node object data available from that Regional Manager for all connected Global Managers.

Name	Connection State	UUID	Description
regional1	Connected	ff1b160f-feb3-43e8-9335-a017t	
nmcvm02	Not Connecte	ec150190-410c-47b3-b847-b32!	

4 Click the **New** icon.

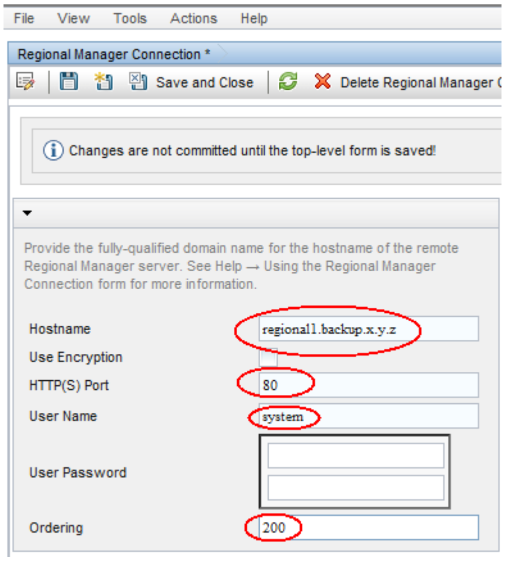


Name	regional1
Connection State	Connected
UUID	ec150190-410c-47b3-b847-b32565ce201a
Description	

Configure either HTTP or HTTPS communication with this Regional NNMi management server.

Orde	Hostname	Use Enc	HTTP (S) Port	User Name
2	regional1	-	80	system

5 Add the **Hostname**, **HTTP or HTTPS Port**, **User Name**, and **Ordering** value. Set the ordering value to a value greater than the `regional1` value.


File View Tools Actions Help
Regional Manager Connection *
Save and Close
Delete Regional Manager (

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

Provide the fully-qualified domain name for the hostname of the remote Regional Manager server. See Help → Using the Regional Manager Connection form for more information.

Hostname	regional1.backup.x.y.z
Use Encryption	□
HTTP(S) Port	80
User Name	system
User Password	
Ordering	200

6 Click **Save and Close** three times to save your work.

If a regional manager fails, the global manager does the following:

a It contacts the primary.

b If the primary does not respond, it contacts the secondary.

If the global system detects that the active system is not responding, it tries to reconnect starting with the lowest order number.

Troubleshooting Tips for Global Network Management

Troubleshooting Information in the NNMi Help

See the *Troubleshoot Global Network Management* topic in the NNMi help for global network management troubleshooting information.

Clock Synchronization

All NNMi management servers in your network environment that participate in global network management (global managers and regional managers) or single sign-on (SSO) must have their internal time clocks synchronized in universal time. Use a Time Synchronization program, for example, the UNIX (HP-UX / Linux / Solaris) tool Network Time Protocol Daemon (NTPD) or one of the available Windows operating system tools.

If you see the following message at the bottom of the NNMi console:

```
NNMi is not connected to 1 Regional Manager(s). See Help ? System
Information, Global Network Management.
```

Check the `nnm.0.0.log` file on the Global Manager for the following message:

```
WARNING: Not connecting to system <serverName> due to clock
difference of <number of seconds>. Remote time is <date/time>.
```

Perhaps the clocks have drifted apart and need to be resynchronized. Check the `nnm.0.0.log` file on the Global Manager for the following message:

```
WARNING: Not connecting to system <serverName> due to clock
difference of <number of seconds>. Remote time is <date/time>.
```

Within a few minutes of this warning, NNMi disconnects the Regional Manager Connection. And the following message appears at the bottom of the NNMi console:

```
NNMi is not connected to 1 Regional Manager(s). See Help ? System
Information, Global Network Management.
```

Global Network Management System Information

Select **Help > System Information**, then click the **Global Network Management** tab to view information about your global network management connections.

Synchronize Regional Manager Discovery from a Global Manager

Suppose you notice an information inconsistency between `global1` and `regional2`. To fix that, run the **`nnmnoderediscover.ovpl`** script from `global1`, causing `global1` and `regional2` to synchronize. This also results in the `regional2` updating `global1` with any new discovery results.

Consider the network shown in Figure 16 on page 250. Suppose you want `regional2` to synchronize its entire set of nodes, nodes: X, Y and Z, with `global1`. Run the following command to synchronize nodes X, Y, and Z with `global1`: **`nnmnoderediscover.ovpl -u`** ***`username`*** **`-p`** ***`password`*** **`-rm regional2`**. For more information, see the *nnmnoderediscover.ovpl* reference page, or the UNIX manpage.

Remedying a Destroyed Database on global1

If you take `global1` out of service and need to restore its database, you face several scenarios:

1. If you restore `global1`'s database successfully, `regional1` and `regional2` synchronize their cached information with `global1`. There are no manual steps to perform after bringing `global1` back online.
2. If `global1` is out of service for an extended period of time, step 1 might not work successfully. To remedy this, run the **`nnmnoderediscover.ovpl`** script on `global1` to initiate a new discovery on `global1`, `regional1` and `regional2`. In this case you could run status polls on key devices to more quickly get updated status information.
3. If you cannot recover `global1`'s database then submit a support call to clear out the old `global1` data from the `regional1` and `regional2` databases using the **`nnmsubscription.ovpl`** script.

Upgrading from NNMi 9.0x to NNMi 9.10

NNMi Versions Supported by Global Network Management

If a global manager is connected to a regional manager running NNMi 9.0x patch 2 or earlier, SNMP queries between the global and regional manager do not work. To remedy this, upgrade the regional manager to NNMi 9.0x patch 3 or later. To achieve the best results, the global manager should be the same version and NNMi patch level as the regional manager. HP supports an NNMi 9.10 global manager connected to an NNMi 9.0x regional manager.

Global Network Management Upgrade Steps

To upgrade NNMi management servers configured in a global network management environment, upgrade the NNMi management servers in the following order:

1. Upgrade the global manager from NNMi 9.0x to NNMi 9.10.
2. Upgrade the regional managers from NNMi 9.0x to NNMi 9.10.

The global network management feature continues to function while you complete the upgrades, but some of the new NNMi 9.10 features might not work on the global NNMi management server until you complete the upgrades on the regional NNMi management servers.

Global Network Management and NNM iSPIs or Third-Party Integrations

Each NNM iSPI or third-party integration has its own unique deployment guideline. For the examples in this chapter, you can deploy some NNM iSPIs on `regional1` only, `global1` only, or on both `regiona1` and `global1`. For other NNM iSPIs or third-party integrations, you must have them installed on both `regional1` and `global1`. See the documentation for the NNM iSPI or third-party integration for more information.

Configuring NNMi Advanced for IPv6

You must purchase and install an NNMi Advanced license to use the IPv6 management feature. References to NNMi in this chapter refer to NNMi with an NNMi Advanced license installed.

IPv6 management in NNMi enables the discovery and monitoring of IPv6 addresses, including their interfaces, nodes and subnets. To provide a seamless integration, NNMi extends its IP Address model to include both IPv4 and IPv6 addresses. Whenever possible, NNMi treats all IP Addresses equally; most of the features associated with an IPv4 address are also available for IPv6 addresses. However, there are some exceptions. See the NNMi help for more information about IPv6 information displayed in the NNMi console.

This chapter contains the following topics:

Feature Description

The NNMi IPv6 management feature provides the following:

- IPv6 inventory discovery for IPv6-only and dual-stacked devices
  - IPv6 addresses
  - IPv6 subnets
  - Associations between IPv6 Addresses, Subnets, Interfaces and Nodes

- Native IPv6 SNMP communication for the following:
  - Node discovery
  - Interface monitoring
  - Trap and inform reception and forwarding
- Automatic selection of IPv4 or IPv6 communication (management address) for dual-stacked devices. Use the NNMi console to set the SNMP management address preference to IPv4 or IPv6 using **Communication Configuration** located in the **Configuration** workspace.
- Native ICMPv6 communication for IPv6 Address fault monitoring.
- Seeded device discovery using an IPv6 address or hostname
- Automatic IPv6 device discovery using IPv6 Layer 3 neighbor discovery hints
- Automatic IPv6 device discovery using layer 2 neighbor discovery hints using LLDP (Link Layer Discovery Protocol) IPv6 neighbor information
- Consolidated presentation of IPv4 and IPv6 information
  - Inventory views for nodes, interfaces, addresses, subnets, and associations
  - Layer 2 Neighbor View and Topology Maps for IPv4 and IPv6 devices
  - Layer 3 Neighbor View and Topology Maps for IPv4 and IPv6 devices
  - Incidents, conclusions, root-cause analysis
- NNMi console actions: ping and traceroute for IPv6 addresses and nodes
- NNMi configuration using IPv6 addresses and address ranges
  - Communication configuration
  - Discovery configuration
  - Monitoring configuration
  - Node & Interface Groups
  - Incident configuration
- SDK Web-services support for IPv6 inventory and incidents
- NNM iSPI Performance for Metrics support for IPv6 interfaces

The NNMi IPv6 management feature excludes the following:

- Discovery of IPv6 subnet connections
- Use of IPv6 ping sweep for discovery
- IPv6 Network Path View (Smart Path)
- IPv6 Link Local Address fault monitoring
- Using IPv6 Link Local Addresses as discovery seeds

Prerequisites

Review the *NNMi Deployment Reference*, *NNMi Release Notes*, and *NNMi System and Device Support Matrix* for details on management server specifications and NNMi installation.

To use native IPv6 communication, the NNMi management server must be a dual-stacked system, meaning that it communicates using both IPv4 and IPv6.

IPv6 is not supported on Windows operating systems. See the *NNMi System and Device Support Matrix* for information about the supported operating systems for IPv6. There are other requirements listed below:

- You must enable and configure IPv4 on at least one network interface.
- You must enable IPv6 and have a global unicast address or a unique local unicast address configured on at least one network interface that is connected to the IPv6 network you must manage.
- You must configure IPv6 routes on the NNMi management server to enable NNMi to communicate with any devices you want NNMi to discover and monitor using IPv6.

➤ You can use an IPv4-only NNMi management server, but doing so will limit NNMi from fully managing IPv4/IPv6 dual-stacked devices. For example, if you use an IPv4-only management server, NNMi cannot discover IPv6-only devices, cannot discover using IPv6 seeds and hints, and cannot monitor for faults on devices having IPv6 addresses.

The DNS server used by the NNMi management server must resolve hostnames to and from IPv6 addresses. For example, it must be able to resolve to and from an AAAA DNS record. That means the DNS server must map a hostname to a 128-bit IPv6 address. If an IPv6-capable DNS server is not available, NNMi will still function correctly; however NNMi does not determine nor display DNS hostnames for nodes using IPv6 addresses.

Licensing

As mentioned earlier, you must purchase and install an NNMi Advanced license to use the IPv6 management feature. For information about obtaining and installing your NNMi Advanced license, see Licensing NNMi on page 117.

The NNMi product includes a temporary Instant-On license password. This is a temporary, but valid NNMi Advanced license. You should obtain and install a permanent license password as soon as possible.

Supported Configuration

See the *NNMi System and Device Support Matrix* for additional information about the supported operating system configurations for NNMi.

Management Server

The following table shows the capabilities of both the IPv4-only and dual-stacked NNMi management server.

Table 20 Management Server Capabilities

Feature/Capability	IPv4-Only	Dual-Stack
IPv4 Communication (SNMP, ICMP)	Supported	Supported
IPv6 Communication (SNMP, ICMPv6)	Not Supported	Supported
Dual-Stack Managed Node	Supported	Supported
Discovery using IPv4 Seed	Supported	Supported
Discovery using IPv6 Seed	Not Supported	Supported
IPv4 Address and Subnet Inventory	Supported	Supported
IPv6 Address and Subnet Inventory	Supported	Supported
Interface Status and Performance using SNMP	Supported	Supported
IPv4 Address Status using ICMP	Supported	Supported
IPv6 Address Status using ICMPv6	Not Supported	Supported
IPv6-only Managed Node	Not Supported	Supported
Discovery using IPv6 Seed	Not Supported	Supported
IPv6 Address and Subnet Inventory	Not Supported	Supported

Table 20 Management Server Capabilities (cont'd)

Feature/Capability	IPv4-Only	Dual-Stack
Interface Status and Performance using SNMP	Not Supported	Supported
IPv6 Address Status using ICMPv6	Not Supported	Supported
IPv4-only Managed Node	Supported	Supported
Node Discovery using IPv4 Seed	Supported	Supported
Node Discovery using IPv4 Seed	Supported	Supported
Interface Status and Performance using SNMP	Supported	Supported
Interface Status and Performance using SNMP	Supported	Supported
IPv4 Address and Subnet Inventory	Supported	Supported

Supported SNMP MIBs for IPv6

NNMi supports the following SNMP MIBs for IPv6:

- RFC 4293 (current IETF standard)
- RFC 2465 (original IETF proposal)
- Cisco IP-MIB

Installing NNMi

During NNMi installation, the installation script includes IPv6 features; however, you must manually enable these IPv6 features. First, you must purchase and apply an NNMi Advanced license to enable the IPv6 features. Then you must manually configure IPv6 to work by editing the `nms-jboss.properties`. file.

Activating IPv6 Features

Features requiring IPv6 communication, such as the discovery and of IPv6 only devices and the monitoring of IPv6 address status, require an NNMi management server to have an IPv6 global unicast address configured and operational.

The procedure shown below explains how to enable IPv6 features by doing the following:

- Install an NNMi Advanced license
- Enable the IPv6 Master Switch in the `nms-jboss.properties` file

➤ Review and verify all of the prerequisites described in the preceding section before continuing.

1. Use the temporary Instant-on license that comes with NNMi, or install an NNMi Advanced license. For information about obtaining and installing NNMi licenses, see Licensing NNMi on page 117. IPv6 features are not available with the basic NNMi license.
2. Edit the `nms-jboss.properties` file. Look in the following location:
   - *UNIX*: `$NNM_PROPS/nms-jboss.properties`
3. Locate the text that begins with `# Enable NNMi IPv6 Management`.

   ➤ NNMi provides a complete description of each property, showing them as comments in the `nms-jboss.properties` file.

   a. To enable IPv6 communication in NNMi, un-comment the property:

      `java.net.preferIPv4Stack=false`

      ➤ To un-comment a property, remove the `#!` characters from the beginning of a line.

   b. To enable overall IPv6 management in NNMi, un-comment the property:

      `com.hp.nnm.enableIPv6Mgmt=true`

   c. Save and close the `nms-jboss.properties` file.
4. Optionally set the SNMP management address preference for dual-stacked managed nodes. Dual-stacked managed nodes are those nodes that can communicate using either IPv4 or IPv6. To do this, complete the following steps:

   a. From the NNMi console, click **Communication Configuration** located in the **Configuration** workspace.

   b. Select `IPv4`, `IPv6`, or `Any` in the `IP Version Preference` field.

   c. Save your changes.
5. Restart the NNMi management server.

   a. Run the **`ovstop`** command on the NNMi management server.

   b. Run the **`ovstart`** command on the NNMi management server.
6. Check the NNMi processes using the following command:

   ```
   ovstatus -v ovjboss
   ```

Successful startup should look something like the following:

```
object manager name: ovjboss
 state:               RUNNING
 PID:                 <Process ID #>
 last message:        Initialization complete.
 exit status:         -
 additional info:
            SERVICE                                 STATUS
            CommunicationModelService               Service is started
            CommunicationParametersStatsService     Service is started
            EventsCustomExportService               Service is started
            ExtensionDeployer                       Service is started
            IslandSpotterService                    Service is started
            KeyManager                              Service is started
            ManagedNodeLicenseManager           Service is started
            ModelChangeNotificationAdapter   Service is started
            MonitoringSettingsService              Service is started
            NMSLogManager                           Service is started
            NamedPoll                               Service is started
            NetworkApplication                      Service is started
            NmsApa                                  Service is started
            NmsDisco                                Service is started
            NmsEvents                               Service is started
            NmsEventsConfiguration                Service is started
            NmsExtensionNotificationService   Service is started
            NmsModel                                Service is started
            NmsWorkManager                          Service is started
            NnmTrapService                         Service is started
            RbaConfig                               Service is started
            RbaManager                              Service is started
            SpmdjbossStart                          Service is started
            StagedIcmp                              Service is started
            StagedSnmp                              Service is started
            StatePoller                             Service is started
            TrustManager                            Service is started
```

7 After you enable IPv6, NNMi views immediately include the IPv6 inventory for newly discovered nodes. During the next discovery cycle, NNMi views show the IPv6 inventory associated with previously discovered nodes.

To speed things up, select nodes that you know are dual-stack nodes, and then use the **Actions** > **Configuration Poll** command located in the NNMi console. You can also use the `nnmnoderediscover.ovpl` script to add nodes to the NNMi discovery queue. See the *nnmnoderediscover.ovpl* reference page, or the UNIX manpage, for more information.

After you enable IPv6 communication on the NNMi management server, NNMi begins monitoring nodes for IPv6 address faults using ICMPv6.

Deactivating IPv6 Features

You can administratively disable IPv6 features using one of the following methods:

1. Turn off the IPv6 master switch in the `nms-jboss.properties` file, then restart NNMi.
2. Let the NNMi Advanced license expire, or replace it with a basic NNMi license.

   For information about changing the NNMi license, see Licensing NNMi on page 117.

The following sections describe NNMi behavior and inventory cleanup after you disable IPv6.

IPv6 Monitoring Following Deactivation

If IPv6 management or IPv6 communication becomes completely disabled, the `StatePoller` service immediately stops monitoring IPv6 addresses with ICMPv6. NNMi sets the IP address state of these addresses to `Not Polled`. If you select an address, then use the **Actions** > **Monitoring Settings** for this address, NNMi opens `Fault ICMP Polling enabled: false` even though the associated `Monitoring Configuration` rule has the `IP Address Fault Polling` enabled.

IPv6 Inventory Following Deactivation

Once NNMi completely discovers your IPv6 inventory, you can enable NNMi to clean it up automatically in the following scenarios:

- You turned on the master IPv6 switch, then turned it off and restarted NNMi.

  NNMi does not immediately remove the IPv6 inventory. NNMi removes the IPv6 inventory for SNMP nodes during the next discovery cycle. NNMi does not remove non-SNMP IPv6 nodes. Manually delete IPv6 nodes from the NNMi inventory.

- Your NNMi Advanced license expired or someone removed the license. NNMi begins using the NNMi basic license, and the basic license has enough capacity to continue managing all of the discovered nodes.

  NNMi immediately removes all of the non-SNMP IPv6 nodes from its inventory. NNMi rediscovers all of the SNMP nodes and removes all of the IPv6 data.

- Your NNMi Advanced license expired or someone removed the license. NNMi begins using the NNMi basic license, and the basic license does not have enough capacity to continue managing all of the discovered nodes. NNMi immediately removes all non-SNMP IPv6 nodes. The `Licensing` service marks the SNMP nodes that exceed the licensed inventory capacity with an `unmanaged` state. NNMi immediately removes IPv6 data from the managed SNMP nodes.

For the unmanaged SNMP nodes, complete these steps:

a Install additional license capacity.

b Use the **Actions > Management Mode > Manage** command located in the NNMi console to change the management mode for the nodes marked as `unmanaged` by the `Licensing` service. You can use the `nnmmanagementmode.ovpl` script to manage these nodes as well. See the *nnmmanagementmode.ovpl* reference page, or the UNIX manpage, for more information.

c Use the **Actions** > **Configuration Poll** command located in the NNMi console to enable NNMi to discover them. You can use the `nnmnoderediscover.ovpl` script to discover these nodes as well. See the *nnmnoderediscover.ovpl* reference page, or the UNIX manpage, for more information.

- Your NNMi Advanced license expired or someone removed the license; you neglected to install an NNMi basic license.

  NNMi immediately removes all non-SNMP IPv6 nodes and automatically unmanages the remaining nodes. To remedy this situation, complete these steps:

a Install a valid license.

b Use the **Actions > Management Mode > Manage** command located in the NNMi console to change the management mode for the nodes marked as `unmanaged` by the `Licensing` service. You can use the `nnmmanagementmode.ovpl` script to manage these nodes as well. See the *nnmmanagementmode.ovpl* reference page, or the UNIX manpage, for more information.

c Use the **Actions** > **Configuration Poll** command located in the NNMi console to enable NNMi to discover the nodes you changed from `unmanaged` to `managed`.You can use the `nnmnoderediscover.ovpl` script to discover these nodes as well. See the *nnmnoderediscover.ovpl* reference page, or the UNIX manpage, for more information

d To create an IPv6 list, then remove the IPv6 inventory, use the **Actions** > **Configuration Poll** command to obtain configuration information from each managed node.

Known Issues When Cleaning Up IPv6 Inventory

You could experience leftover IPv6 inventory in the following situation: Suppose that NNMi successfully uses SNMP to manage an IPv6 node, then the node becomes inaccessible before the next discovery. Due to the design of the existing discovery system, the discovery process cannot update a node that loses its ability to communicate using SNMP. To remove these remaining nodes, fix the communication problem, then use the **Actions** > **Configuration Poll** command located in the NNMi console to obtain configuration information from these nodes. For native IPv6 nodes, delete the node directly from the NNMi console.

Running NNMi in a Solaris Zones Environment

For the supported versions of the Solaris operating system, HP Network Node Manager i Software (NNMi) runs without special configuration in a Solaris Zones environment.

This chapter contains the following topics:

- Installing NNMi in a Solaris Zone
- Trap Forwarding in a Solaris Zone
- Running NNMi Application Failover in a Solaris Zones Environment
- Running NNMi under HA in a Solaris Zones Environment

Installing NNMi in a Solaris Zone

If you plan to implement NNMi application failover in a Solaris Zones environment, see Running NNMi Application Failover in a Solaris Zones Environment on page 268.

If you plan to run the Solaris Zone under high availability (HA), see Running NNMi under HA in a Solaris Zones Environment on page 268.

For all other deployment models, install NNMi as described in the *NNMi Installation Guide*.

Trap Forwarding in a Solaris Zone

Suppose you want to forward the SNMP traps that NNMi receives from managed devices to another application. To do this, navigate to the **Trap Forward Configuration** in the **Configuration** workspace. See the NNMi help for more information.

Because the Solaris Zones environment does not support raw trap forwarding, do not select the **Original Trap** forwarding option. Choose one of the other forwarding options when running NNMi in a Solaris Zones environment.

Running NNMi Application Failover in a Solaris Zones Environment

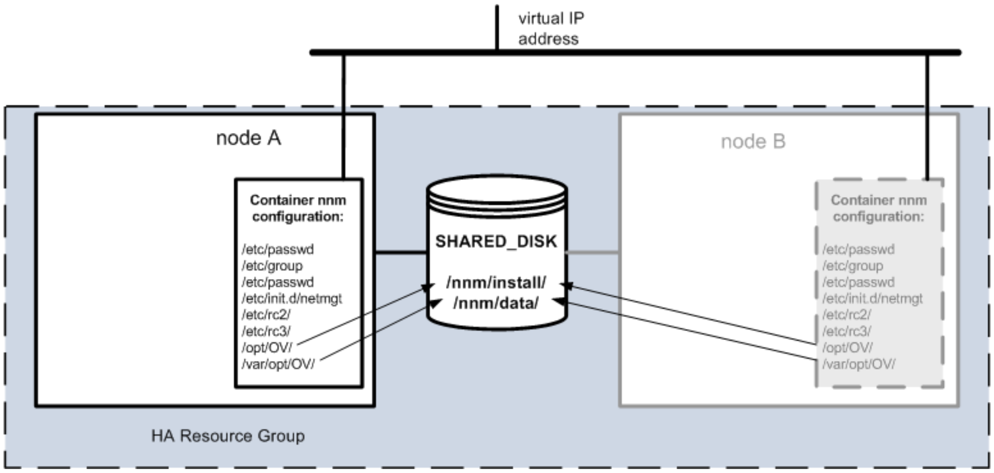
If you want to use the NNMi application failover feature in a Solaris Zones environment, install NNMi in its own zone on each of two physical systems.

Configure application failover as described in Configuring NNMi for Application Failover on page 273. Throughout the procedure, “server X” refers to one zone and “server Y” refers to the other zone.

Running NNMi under HA in a Solaris Zones Environment

In a Solaris Zones environment, you do not need to implement the NNMi-provided solution for running NNMi in an HA cluster. Because Veritas Cluster Server (VCS) is zone-aware, configure the HA resource group for the zone, as shown in Figure 17.

Figure 17 NNMi in a Solaris Zone Running under HA



The configuration to run NNMi in this environment is minimal. The NNMi installation process creates the nmsdbmgr user in the nmsdb group and adds startup configuration to the host system. Replicate this setup to the second node in the HA cluster.

To install NNMi to run in a zone inside an HA resource group, follow these steps:

1 On the shared disk, create the NNMi installation folders:

- `/nnm/install`
- `/nnm/data`

2 On node A, create and prepare a new zone called **nnm**:

a Create zone **nnm**, as described in the Solaris zone documentation.

Note all configuration parameters set during zone creation.

b Start zone **nnm**.

c. Log on to zone **nnm**, and then create the following symbolic links:
   - `/opt/OV/` pointing to `/nnm/install/` on the shared disk
   - `/var/opt/OV/` pointing to `/nnm/data/` on the shared disk

d. Log off from and then shut down zone **nnm**.

3. On node B, create an identical new zone called **nnm**, and then install NNMi:

   a. Create zone **nnm** with identical properties (including IP address) as zone **nnm** on node A.

   b. Start zone **nnm**.

   c. Log on to zone **nnm**, and then create the following symbolic links:
      - `/opt/OV/` pointing to `/nnm/install/` on the shared disk
      - `/var/opt/OV/` pointing to `/nnm/data/` on the shared disk

   d. Instruct the NNMi installer to follow the symbolic links by entering the following command:

      `PKG_NONABI_SYMLINKS=true`

   e. Install NNMi inside the **nnm** zone.

      NNMi installs into the `/nnm/install/` and `/nnm/data/` directories on the shared disk.

   f. Copy the following files to a temporary location (such as the shared disk) that is accessible from outside the **nnm** zone:
      - `/etc/passwd`
      - `/etc/group`
      - `/etc/shadow`
      - `/etc/init.d/netmgt`

   g. Log off from and then shut down zone **nnm**.

4. On node A, copy the NNMi-modified system files, and then start NNMi:

   a. Start zone **nnm**.

   b. Log on to zone **nnm**, and then copy the files from the temporary location identified in step 3 to the correct location in the zone:
      - `/etc/passwd`
      - `/etc/group`
      - `/etc/shadow`
      - `/etc/init.d/netmgt`

c Create the following symbolic links (to duplicate the configuration created during NNMi installation on node B):

— `/etc/rc0.d/K01netmgt` pointing to `/etc/init.d/netmgt`

— `/etc/rc1.d/K01netmgt` pointing to `/etc/init.d/netmgt`

— `/etc/rc2.d/K01netmgt` pointing to `/etc/init.d/netmgt`

— `/etc/rc3.d/S98netmgt` pointing to `/etc/init.d/netmgt`

— `/etc/rcS.d/K01netmgt` pointing to `/etc/init.d/netmgt`

d Start NNMi by running the following command:

```
ovstart
```

5 Configure Veritas Cluster Server to create a resource group containing zone **nnm** on both node A and node B.

For more information, see the VCS documentation.

Resilience

HP Network Node Manager i Software (NNMi) supports two different approaches to protecting the NNMi data in case of hardware failure:

- NNMi application failover provides for disaster recovery by maintaining a copy of the embedded NNMi database transaction logs on an identically configured system. (If NNMi uses an Oracle database, the two systems connect to the same database at different times.)
- Running NNMi in a high availability (HA) cluster provides for nearly one hundred percent availability of the NNMi management server by maintaining the embedded NNMi database and configuration files on a shared disk. (If NNMi uses an Oracle database, the shared disk contains the NNMi configuration files, and the two systems connect to the same database at different times.)

In both approaches, if the current NNMi management server fails, the second system automatically becomes the NNMi management server.

Table 21 compares several aspects of these two approaches to NNMi data resilience.

Table 21 NNMi Data Resilience Comparison

Item for Comparison	NNMi Application Failover	NNMi Running in an HA Cluster
Required software products	NNMi or NNMi Advanced	• NNMi or NNMi Advanced • A separately purchased HA product
Time to fail over	Embedded NNMi database: Time to process the transaction logs (under normal conditions, 10-60 minutes for NNMi without any NNM iSPIs). Oracle NNMi database: Almost instantaneous.	Under normal conditions, 5-30 minutes for NNMi without any NNM iSPIs.
Transparency of failover	Partial. The IP address of the NNMi management server changes to the physical address of what was the standby server. Users must connect to the NNMi console using the new IP address. Some applications follow the movement of the NNMi management server, but most (including the NNM iSPIs) do not.	Complete. All connections use the virtual IP address of the HA cluster, which does not change on failover.
Relative proximity of active and standby servers	LAN or WAN	LAN or WAN (some HA products only)
Licenses purchased	For each feature: • A production license tied to the IP address of the initial active server. • A non-production license tied to the IP address of the initial standby server.	For each feature: A production or non-production license tied to the virtual IP address of the NNMi HA resource group.

Table 21 NNMi Data Resilience Comparison

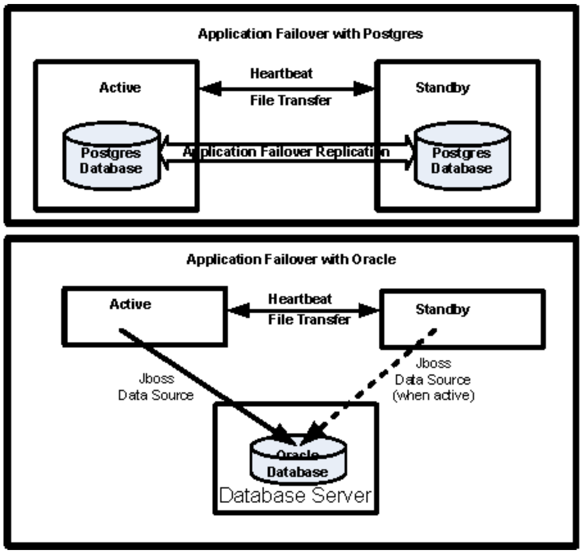
Item for Comparison	NNMi Application Failover	NNMi Running in an HA Cluster
Licenses installed	• Production license keys on the initial active server. • Non-production license keys on the initial standby server.	• Non-production license keys on the initial active server and managed on the shared disk.
Support for NNM iSPIs	Support varies. See the documentation for each NNM iSPI.	
Interaction with Global Network Management	• Can configure each global manager for application failover or HA. • Can configure each regional manager for application failover or HA. • Each of these configurations requires two physical or virtual systems.[a] • If a global manager or regional manager fails over, NNMi re-establishes the connections between the global managers and regional managers.	
NNMi maintenance	NNMi must be taken out of the application failover cluster before applying a patch or upgrading.	NNMi can be patched and upgraded without unconfiguring HA.

[a] Virtual machine support for HA is dependent on HA software vendors' support of virtual systems.

This section contains the following chapters:

- Configuring NNMi for Application Failover
- Configuring NNMi in a High Availability Cluster

Configuring NNMi for Application Failover



Many information technology professionals depend on HP Network Node Manager i Software (NNMi) to notify them when critical network equipment fails and to provide them with a root cause for the failure. They also need NNMi to continue to notify them of network equipment failures, even when the NNMi management server fails. **NNMi application failover** meets this need, transferring application control of NNMi processes from an active NNMi management server to a standby NNMi management server, providing continuance of NNMi functionality.

This chapter contains the following topics:

- Application Failover Overview
- Application Failover Basic Setup
- Configuring NNMi for Application Failover
- Using the Application Failover Feature
- Returning to the Original Configuration Following a Failover
- NNM iSPIs and Application Failover
- Integrated Applications
- Disabling Application Failover
- Administrative Tasks and Application Failover
- Network Latency/Bandwidth Considerations

Application Failover Overview

The application failover feature is available for NNMi installations that use either the embedded or Oracle databases. After configuring your systems to use the application failover feature, NNMi detects an NNMi management server failure and triggers a secondary server to assume NNMi functionality.

The following terms and definitions apply to configuring NNMi for application failover:

- **Active**: The server running the NNMi processes.
- **Standby**: The system in the NNMi cluster that is waiting for a failover event; this system is not running NNMi processes.
- **Cluster Member**: A Java process running on a system that is using JGroups technology to connect to a cluster; you can have multiple members on a single system.
- **Postgres**: The embedded database NNMi uses to store information such as topology, incidents, and configuration information.
- **Cluster Manager**: The `nnmcluster` process and tool used to monitor and manage the servers for the application failover feature.

Application Failover Basic Setup

To deploy the application failover feature, install NNMi on two servers. This chapter refers to these two NNMi management servers as the **active** and **standby** servers. During normal operation, only the active server is running NNMi services.

The active and standby NNMi management servers are part of a cluster that monitors a heartbeat signal from both of the NNMi management servers. If the active server fails, resulting in the loss of its heartbeat, the standby server becomes the active server.

For application failover to work successfully, the NNMi management servers must meet the following requirements:

- Both NNMi management servers must be running the same type of operating system. For example, if the active server is running an HP-UX operating system, the standby server must also be running an HP-UX operating system.
- Both NNMi management servers must be running the same NNMi version. For example, if NNMi 9.10 is running on the active server, the identical NNMi version, NNMi 9.10, must be on the standby server. The NNMi patch levels must also be the same on both servers.
- The system password must be the same on both NNMi management servers.
- For NNMi installations on Windows operating systems, the `%NnmDataDir%` and `%NnmInstallDir%` system variables must be set to identical values on both servers.

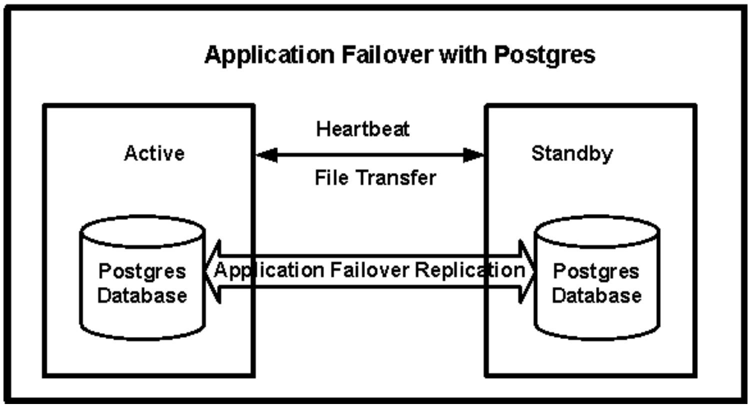
- Both NNMi management servers must be running the same database. For example, both NNMi management servers must be running Oracle or both NNMi management servers must be running the embedded database. You cannot mix the two database types if you plan to use the application failover feature.
- Both NNMi management servers must have identical licensing attributes. For example, the node counts and licensed features must be identical.
- Do not enable application failover until NNMi is in an advanced stage of initial discovery. For more information see Evaluate Discovery on page 69.

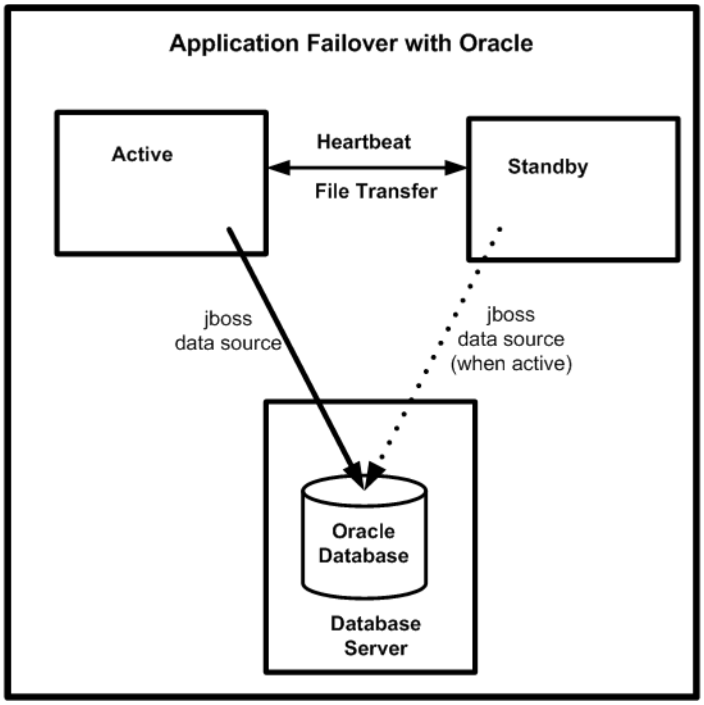
For application failover to function correctly, the active and standby servers must have unrestricted network access to each other. After meeting this condition, complete the steps shown in Configuring NNMi for Application Failover on page 276. For more information see NNMi 9.10 and Well-Known Ports on page 643.

➤ Any software that locks files or restricts network access can cause NNMi communication problems. Configure these applications to ignore the files and ports used by NNMi.

Configuring NNMi for Application Failover

1 Install NNMi on the active server, server X, and the standby server, server Y, as described in the *NNMi Installation Guide*.





2 For each license on server X, obtain a similar non-production license for server Y and install it onto server Y as described in Licensing NNMi on page 117.

3 Run the **`ovstop`** command on each server to shut down NNMi.

➤ If you are using application failover with Oracle as your database, your NNMi processes on the standby server should already be stopped.

4 Configure server X (active) and server Y (standby) for the application failover feature using guidance from the detailed instructions contained in the `nms-cluster.properties` file. Use the following procedure:

➤ **Edit** in the following steps means to uncomment the lines in the text block within the file and to modify the text.

a Edit the following file:

- *Windows*: `%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties`
- *UNIX*: `$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties`

b Declare a unique name for the NNMi cluster. Use the same name when configuring both the active and standby servers.

```
com.hp.ov.nms.cluster.name=MyCluster
```

c Add the hostnames of all nodes in the cluster to the `com.hp.ov.nms.cluster.member.hostnames` parameter in the nms-cluster.properties file:

```
com.hp.ov.nms.cluster.member.hostnames = fqdn_for_active,
fqdn_for_standby
```

In NNMi 9.0x, the application failover feature supported a UDP solution where cluster hosts were automatically discovered on the network. Beginning with NNMi 9.10, HP eliminated the UDP solution and only supports the TCP solution. If you are migrating from NNMi 9.0x you must define the cluster hostnames by completing step c for application failover to work.

d *Optional*. Define other com.hp.ov.nms.cluster* parameters within the `nms-cluster.properties` file. Follow the instructions contained within the `nms-cluster.properties` file for modifying each parameter

If you are using application failover with Oracle as your database, NNMi ignores the database parameters contained in the `nms-cluster.properties` file.

5 Depending on the approach you take, complete the instructions shown in Configuring Application Failover to use Self-Signed Certificates on page 126 or the instructions shown in Configuring Application Failover to use a Certificate Authority on page 128.

When configuring the application failover feature, you must merge the `nnm.keystore` and `nnm.truststore` file content for both nodes into a single `nnm.keystore` and `nnm.truststore` file. *You must choose your approach and complete one set of instructions from* step 5

6 Copy the following file from server X to server Y:

- *Windows*: `%NnmDataDir%\shared\nnm\conf\nnmcluster\cluster.keystore`
- *UNIX*: `$NnmDataDir/shared/nnm/conf/nnmcluster/cluster.keystore`

7. Run the following command on both server X and server Y: **nnmcluster**
   Each server should display something similar to the following:

```
=============================== Current cluster state ===============================
State ID: 000000001000000005
Date/Time: 15 Mar 2011 - 09:37:58 (GMT-0600)
Cluster name: ThisCluster (key CRC:626,187,650)
Automatic failover: Enabled
NNM database type: Embedded
NNM configured ACTIVE node is: NO_ACTIVE
NNM current ACTIVE node is: NO_ACTIVE
Cluster members are:

  Local?    NodeType  State                     OvStatus     Hostname/Address
  ------    --------  -----                     --------     ----------------------------
* REMOTE    ADMIN     n/a                       n/a          serverX.xxx.yyy.yourcompany.com/
16.78.61.68:7800
  (SELF)    ADMIN     n/a                       n/a          serverY.xxx.yyy.yourcompany.com/
16.78.61.71:7800
```

The display should list both server X and server Y. If information about both nodes are not displayed, the nodes are not communicating with each other. Here are some things to check for and correct before continuing:

- The Cluster names might be different on server X and server Y.
- The key CRCs might be different on server X and server Y. Check the contents of the following files on both server X and server Y:

  Windows:
  `%NnmDataDir%\shared\nnm\conf\nnmcluster\cluster.keystore`

  UNIX: `$NnmDataDir/shared/nnm/conf/nnmcluster/cluster.keystore`
- A firewall on server X or server Y might be preventing the nodes from communicating.
- Make sure you merged the `nnm.keystore` and `nnm.truststore` files. You should see this error displayed after running the **nnmcluster** command.
- Server X and server Y are running different operating systems. For example, suppose server X is running a Linux operating system and server Y is running a Windows operating system. You should see this error displayed after running the **nnmcluster** command.
- Server X and server Y are running different NNMi versions. For example, suppose server X is running NNMi 9.10 and server Y is running NNMi 9.10 patch 1 (after it is available). You should see this error displayed after running the **nnmcluster** command.

8 On server X, start the NNMi cluster manager:

```
nnmcluster -daemon
```

After you run the **nnmcluster -daemon** command on NNMi management server X, the NNMi cluster manager goes through the following startup routine:

- Connects NNMi management server X to the cluster.
- Detects that there are no other NNMi management servers present.
- NNMi management server X assumes the active state.
- Starts the NNMi services on NNMi management server X (the active server).
- Creates a database backup.

For more information, see the *nnmcluster* reference page, or the UNIX manpage.

9 Wait a few minutes for server X to become the first active node in the cluster. Run the **nnmcluster -display** command on server X and search the displayed results for the term ACTIVE as in ACTIVE_NNM_STARTING or ACTIVE_*SomeOtherState*. Do not continue with step 10 until you know that server X is the active node.

10 On server Y, start the NNMi cluster manager:

```
nnmcluster -daemon
```

After you run the **nnmcluster -daemon** command on NNMi management server Y, the NNMi cluster manager goes through the following startup routine:

- Connects NNMi management server Y to the cluster.
- Detects that NNMi management server X is present and is in the active state. The display shows STANDBY_INITIALIZING.
- Compares the database backup on NNMi management server Y to the backup on NNMi management server X. If these do not match, a new database backup is sent from NNMi management server X (active) to NNMi management server Y (standby). The display shows STANDBY_RECV_DBZIP.
- NNMi management server Y receives a minimal set of transaction logs, which is the minimum necessary for the backup to be applicable for its standby state. The display shows STANDBY_RECV_TXLOGS.
- NNMi management server Y goes into a waiting state, continuously receiving new transaction logs and heartbeat signals from NNMi management server X. The display shows STANDBY_READY.

For more information, see the *nnmcluster* reference page, or the UNIX manpage.

11 If a failover occurs, the NNMi console for server X no longer functions. Close the NNMi console session for server X and log on to server Y (the new active server). Instruct NNMi users to store two bookmarks in their browsers, one to server X (the active NNMi management server) and one to server Y (the standby NNMi management server). If a failover occurs, users can connect to server Y (the standby NNMi management server).

12 Instruct network operations center (NOC) personnel to configure their devices to send traps to both server X and server Y. While server X (active) is running, it processes the forwarded traps and server Y (standby) ignores the forwarded traps.

Using the Application Failover Feature

Now that you have both NNMi management servers running the cluster manager, with one active node and one standby node, you can use the cluster manager to view the cluster status. The cluster manager has three modes:

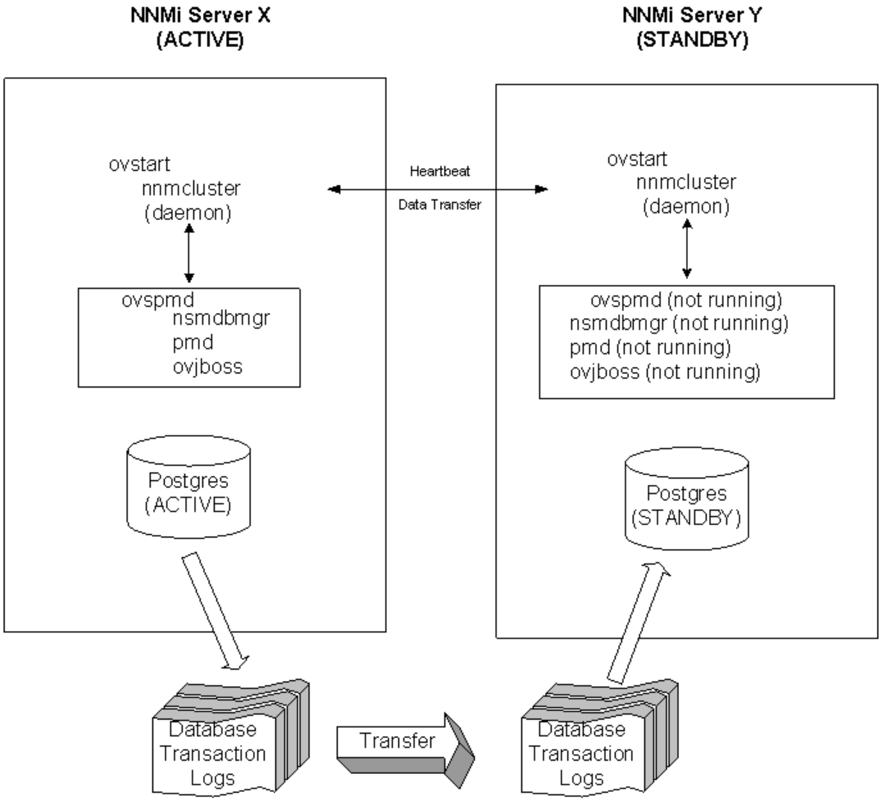
- **daemon mode**: The cluster manager process runs in the background, and uses the **`ovstop`** and **`ovstart`** commands to start and stop the NNMi services.
- **interactive mode**: The cluster manager runs an interactive session in which the NNMi administrator can view and change cluster attributes. For example, the NNMi administrator can use this session to enable or disable the application failover feature or shut down the daemon processes.
- **command line mode**: The NNMi administrator views and changes cluster attributes at the command prompt.

For more information, see the *nnmcluster* reference page, or the UNIX manpage.

Application Failover Behavior Using the Embedded Database

Figure 18 shows the application failover configuration for two NNMi management servers using the embedded database. See this figure while reading the rest of this chapter.

Figure 18 Application Failover Configuration (embedded database)



After you start both the active and standby nodes, the standby node detects the active node, requests a database backup from the active node, but does not start NNMi services. This database backup is stored as a single Java-ZIP file. If the standby node already has a ZIP file from a previous cluster-connection, and NNMi finds that the file is already synchronized with the active server, the file is not retransmitted.

While both the active and standby nodes are running, the active node periodically sends database transaction logs to the standby node. You can modify the frequency of this data transfer by changing the value of the `com.hp.ov.nms.cluster.timeout.archive` parameter in the `nms-cluster.properties` file. These transaction logs accumulate on the standby node, and are available on the standby node any time it needs to become active.

When the standby node receives a full database backup from the active node, it places the information into its embedded database. It also creates a `recovery.conf` file to inform the embedded database that it should consume all received transaction logs before it becomes available to other services.

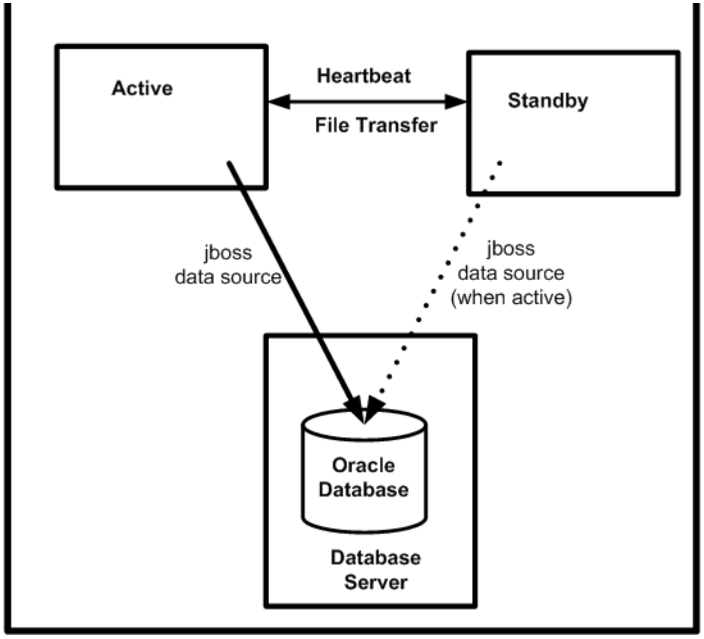
If the active node becomes unavailable for any reason, the standby node becomes active by running an **`ovstart`** command to start the NNMi services. The standby NNMi management server imports the transaction logs before starting the remaining NNMi services.

If the active NNMi system fails, the standby system begins discovery and polling activities. This transition keeps NNMi monitoring and polling your network while you diagnose and repair the failed system.

Application Failover Behavior Using an Oracle Database

Figure 19 shows the application failover configuration for two NNMi management servers using an Oracle database. See this figure while reading the rest of this chapter.

Figure 19 Application Failover Configuration (Oracle database)



If the active node becomes unavailable for any reason, the standby node becomes active by running an **`ovstart`** command to start the NNMi services.

If the active NNMi system fails, the standby system begins discovery and polling activities. This transition keeps NNMi monitoring and polling your network while you diagnose and repair the failed system.

Application Failover Scenarios

There are several possible problems that can cause the active NNMi management server to stop sending heartbeats, and to initiate a failover:

- Scenario 1: The active NNMi management server fails.
- Scenario 2: The system administrator shuts down or reboots the active NNMi management server.
- Scenario 3: The NNMi administrator shuts down the cluster.
- Scenario 4: The network connection between the active and the standby NNMi management servers fails.

  In scenario 4, both NNMi management servers run in the active state. When the network device comes back online, the two NNMi management servers automatically negotiate which node should become the new active node.

Additional ovstart and ovstop Options

When you use the **ovstop** and **ovstart** commands on NNMi management servers configured for application failover, NNMi runs the following commands:

- `ovstart`: **nnmcluster -daemon**
- `ovstop`: **nnmcluster -disable -shutdown**

If you run an **ovstop** command, NNMi does not failover to the standby node. HP designed the **ovstop** command to support temporary maintenance stoppages. To manually initiate a failover, use the **-failover** option with the **ovstop** command. For more information, see the *ovstop* reference page, or the UNIX manpage.

The following options to the **ovstop** command apply to NNMi management servers configured in an application failover cluster:

- **ovstop -failover**: This command stops the local daemon-mode cluster process and forces a failover to the standby NNMi management server. If the failover mode was previously disabled, it is re-enabled. This command is equivalent to: **nnmcluster -enable -shutdown**
- **ovstop -nofailover**: This command disables failover mode and then stops the local daemon-mode cluster process. No failover occurs. This command is equivalent to: **nnmcluster -disable -shutdown**
- **ovstop -cluster**: This command stops both the active and standby nodes, removing them both from the cluster. This command is equivalent to: **nnmcluster -halt**

If you run the **shutdown** command on NNMi management servers running UNIX operating systems, the **ovstop** command runs automatically and disables application failover. That might not be your desired result. To control application failover during maintenance windows, use the **nnmcluster -acquire** and **nnmcluster -relinquish** commands to set the active and standby nodes the way you want them before running the shutdown command. For more information see the *nnmcluster* reference page, or the UNIX manpage.

Application Failover Incidents

Any time the `nnmcluster` process or someone using the **nnmcluster** command starts a node as active, NNMi generates one of the following incidents:

- *NnmClusterStartup*: The NNMi cluster was started, and no active node was present. Therefore the node was started in the active state. This incident has a NORMAL severity.
- *NnmClusterFailover*: The NNMi cluster detected a failure of the active node. The standby node was then enabled and NNMi services started on the new active node. This incident has a MAJOR severity.

Returning to the Original Configuration Following a Failover

Suppose the active node fails and the standby node is functioning as the active node. After you fix the problem with the former active node, run the following command on the desired active node to return to the original configuration: **`nnmcluster -acquire`**. For more information, see the *nnmcluster* reference page, or the UNIX manpage.

NNM iSPIs and Application Failover

You can use the application failover feature for a Smart Plug-in (iSPI) that you deploy along with NNMi if the deployment meets the following requirements:

- The NNM iSPI runs on the NNMi management server.
- The NNM iSPI uses the same embedded database instance as NNMi.

The NNM iSPI Performance for Metrics and the NNM iSPI Performance for Traffic are exceptions to this description. If you plan to configure the NNMi application failover feature, you must install these iSPIs on dedicated servers. In this case, the iSPIs automatically connect to the new NNMi management server after failover occurs. As part of NNMi application failover configuration, run the enablement script for the NNM iSPI Performance for Metrics or the NNM iSPI Performance for Traffic on each NNMi management server in the cluster.

For more information, see *Support for Application Failover* in the NNM iSPI Performance for Metrics or the NNM iSPI Performance for Traffic help.

NNM iSPI Installation Information

To install an NNM iSPI on an NNMi management server that is already part of an application failover cluster, do the following:

1. As a precaution, run the **`nnmconfigexport.ovpl`** script on both the active and standby NNMi management servers before proceeding. For information, see Best Practice: Save the Existing Configuration on page 40.
2. As a precaution, back up the NNMi data on both the active and standby NNMi management servers before proceeding. For information, see Backup Scope on page 355.
3. Embedded database only: As a precaution, on the active NNMi management server run the **`nnmcluster -dbsync`** command and wait for the command to complete.
4. On the standby NNMi management server, run the following command:

   `nnmcluster -shutdown`
5. Edit the following file on the standby NNMi management server:
   - *Windows*: `%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties`
   - *UNIX*: `$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties`

6 Comment out the com.hp.ov.nms.cluster.name option and save the file.

7 Run the **ovstart** command on the standby NNMi management server. This brings up NNMi services in the standalone (unclustered) state.

8 Install the NNM iSPI on the standby NNMi management server as described in the iSPI installation guide.

9 Run the **nnmcluster -halt** command on the active NNMi management server.

10 Edit the following file on the active NNMi management server:

- *Windows*: `%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties`
- *UNIX*: `$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties`

11 Comment out the com.hp.ov.nms.cluster.name option and save the file.

12 Run the **ovstart** command on the active NNMi management server. This brings up NNMi services in the standalone (unclustered) state.

13 Install the NNM iSPI on the active NNMi management server as described in the iSPI installation guide.

14 Edit the following file on **both** the active and standby NNMi management servers:

- *Windows*: `%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties`
- *UNIX*: `$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties`

15 Uncomment the com.hp.ov.nms.cluster.name option and save each file.

16 Run the **ovstart** command on the active NNMi management server.

17 Wait a few minutes for the active NNMi management server to become the first active node in the cluster. Run the **nnmcluster -display** command on the active NNMi management server and search the displayed results for the term `ACTIVE` as in `ACTIVE_NNM_STARTING` or `ACTIVE_`*SomeOtherState*. Do not continue with step 18 until you know that the active NNMi management server is the active node.

18 Run the **ovstart** command on the standby NNMi management server.

Integrated Applications

When other HP Software or third-party products are integrated with NNMi, the affect of NNMi application failover on an integration depends on how a product communicates with NNMi. For more information, see the appropriate chapter in the Integrations with NNMi section.

If an integrated product must be configured with information about the NNMi management server, the following information applies:

- If long-term, you can update the NNMi management server information within the integrating product configuration. For more information, see the appropriate chapter in the Integrations with NNMi section.

- If the outage appears to be temporary, you can resume using the integrating product after server X returns to service. To return server X to service, follow these steps:

1. On server X, run the following command:

   ```
   nnmcluster -daemon
   ```

   Server X joins the cluster and assumes a standby state.

2. On server X, run the following command:

   ```
   nnmcluster -acquire
   ```

   Server X changes to the active state.

If you anticipate that the original server X will be out of service for a longer time, you can update the NNMi management server IP address within the integrating product. For instructions on how to modify the IP address field, see the integrating product documentation.

Disabling Application Failover

Suppose you configure application failover, use it for a few days, then decide to completely disable it. The following information explains how to completely disable application failover. Complete the following instructions, including actions on both the active and standby NNMi management servers configured in the application failover cluster.

1. Run **`nnmcluster -enable`** command on the *active* NNMi management server.
2. Run the **`nnmcluster -shutdown`** command on the *active* NNMi management server.
3. Wait a few minutes for the old standby NNMi management server to become the new active NNMi management server.
4. Run the **`nnmcluster -display`** command on the new active (old standby) NNMi management server.
5. Search the displayed results for the `ACTIVE_NNM_RUNNING` status. Repeat step 4 until you see the `ACTIVE_NNM_RUNNING` status.
6. Run the **`nnmcluster -shutdown`** command on the new active (old standby) NNMi management server.
7. Run the **`nnmcluster -display`** command repeatedly on the new active (old standby) until you no longer see a `DAEMON` process.
8. Edit the following file both NNMi management servers configured in the cluster:
   - *Windows*: `%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties`
   - *UNIX*: `$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties`
9. Comment out the com.hp.ov.nms.cluster.name option on both NNMi management servers and save each file.

10 Edit the following file on both NNMi management servers:

- *Windows*: `%NnmDataDir%\shared\nnm\databases\Postgres\postgresql.conf`
- *UNIX*: `$NnmDataDir/shared/nnm/databases/Postgres/postgresql.conf`

11 Remove the following lines that begin with `archive_command` and `archive_timeout` in each file. This is an example of what these lines could look like on a Windows NNMi management server. These lines might look slightly different on your server.

```
archive_command = 'nnmcluster.exe -archive "%p" "C:/Documents 
and Settings/All Users/Application Data/HP/HP BTO Software/
shared/nnm/databases/Postgres_standby/TxWALs_send"/%f'
```

```
archive_timeout = 900
```

Make sure to save your changes.

12 If these are Windows NNMi management servers, navigate to the `Services (Local)` console and do the following on each server:

a Set the `Startup type` for the `HP NNM Cluster Manager` to `Disabled`.

b Set the `Startup type` for the `HP OpenView Process Manage`r to `Automatic`.

13 Run the **`ovstart`** command on the former active NNMi management server only. In the application failover configuration, this is the NNMi management server that has a permanent NNMi license.

14 If you were using a non-production license on the former standby server. Do not run the **`ovstart`** command on the former standby NNMi management server. In the application failover configuration, this is the NNMi management server that has a non-production license. To run this NNMi management server as a standalone server, you must purchase and install a permanent license. For more information, see Licensing NNMi on page 117.

15 If both NNMi management servers start successfully, then remove the following directory from both the standby and active NNMi management servers:

- *Windows*: `%NnmDataDir%\shared\nnm\databases\Postgres_standby`
- *UNIX*: `$NnmDataDir/shared/nnm/databases/Postgres_standby`

➤ This directory is a default directory and is the value of the `com.hp.ov.nms.cluster.archivedir` parameter located in the `nms-cluster.properties` file. These instructions assume you did not change this value. If you changed the value of the `com.hp.ov.nms.cluster.archivedir` parameter in the `nms-cluster.properties` file, then remove the directory that equates to the new value.

16 Remove the following directory from both the standby and active NNMi management servers:

- *Windows*: `%NnmDataDir%\shared\nnm\databases\Postgres.OLD`
- *UNIX*: `$NnmDataDir/shared/nnm/databases/Postgres.OLD`

Administrative Tasks and Application Failover

The following information explains how to effectively manage application failover when doing administrative tasks such as patching and restarting NNMi management servers.

Application Failover and Upgrading to NNMi 9.10

If you plan to upgrade an earlier version of NNMi 9.0x that is running in an NNMi application failover configuration, the supported upgrade path is to temporarily unconfigure application failover, upgrade each of the NNMi management servers to NNMi 9.10, then reconfigure application failover.

To upgrade NNMi management servers configured for application failover, follow these steps:

1. As a precaution, run the **nnmconfigexport.ovpl** script on both the active and standby NNMi management servers before proceeding. For information, see Best Practice: Save the Existing Configuration on page 40.
2. As a precaution, back up your NNMi data on both the active and standby NNMi management servers before proceeding. For information, see Backup Scope on page 355.
3. *Embedded database only*: Complete the following steps on the active NNMi management server. Completing these steps will speed up the standby NNMi management server startup shown in step 7 on page 289:
   a. Run the **nnmcluster** command.
   b. After NNMi prompts you, type **dbsync**, then press Enter. Review the displayed information to make sure it includes the following messages:

      ACTIVE_DB_BACKUP: This means that the active NNMi management server is performing a new backup.
      ACTIVE_NNM_RUNNING: This means that the active NNMi management server completed the backup referred to by the previous message.
      STANDBY_RECV_DBZIP: This means that the standby NNMi management server is receiving a new backup from the active NNMi management server.
      STANDBY_READY: This means that the standby NNMi management server is ready to perform if the active NNMi management server fails.
4. Run the **nnmcluster -shutdown** command on the standby NNMi management server. This shuts down all nnmcluster processes on the standby NNMi management server.
5. To verify there are no nnmcluster nodes running on the standby NNMi management server, *complete the following steps on the standby NNMi management server*.
   a. Run the **nnmcluster** command.
   b. Verify that there are no (LOCAL) nnmcluster nodes present except the one marked (SELF). There might be one or more (REMOTE) nodes present.
   c. Run **exit** or **quit** to stop the interactive nnmcluster process you started in step a.

6 *Complete the following steps on the standby NNMi management server* to temporarily disable application failover:

a Edit the following file:

- *Windows*: `%NNM_SHARED_CONF%\props\nms-cluster.properties`
- *UNIX*: `$NNM_SHARED_CONF/props/nms-cluster.properties`

b Comment out the `com.hp.ov.nms.cluster.name` parameter.

c Save your changes.

7 Start, then stop processes on the standby NNMi management server.

a Run the **`ovstart`** command on the standby NNMi management server. Running the **`ovstart`** command causes the standby NNMi management server to import the transaction logs from the active NNMi management server.

b After the **`ovstart`** command completes, run the **`ovstatus -v`** command. All NNMi services should show the state `RUNNING`.

c Run the **`ovstop`** command on the standby NNMi management server.

8 Upgrade the standby NNMi management server to NNMi 9.1x Patch 5 using the instructions located in the *NNMi Installation Guide*.

You must upgrade all of the iSPIs that you have installed on the standby NNMi management server to iSPI versions that support NNMi 9.1x Patch 5.

You now have the former active NNMi management server running NNMi 9.0x and the former standby NNMi management server running NNMi 9.10. You have both of these NNMi management servers running independently with no database synchronization. That means you have both NNMi management servers monitoring the network in parallel. Do not leave these NNMi management servers in this configuration for more than a few hours, as this configuration is a violation of the non-production license installed on the former standby node.

To complete the upgrade, and remedy this situation, select a time to upgrade the former active node to NNMi 9.1x Patch 5. Have the operators temporarily use the former standby node to monitor the network while you complete the upgrade.

The remainder of this procedure assumes you plan to retain the database information from the former active node and discard the database information from the former standby node.

9 Run the **`nnmcluster -halt`** command on the former active NNMi management server.

10 To verify there are no nnmcluster nodes running on the former active NNMi management server, *complete the following steps on the former active NNMi management server*.

a Run the **`nnmcluster`** command.

b Verify that there are no (LOCAL) nnmcluster nodes present except the one marked `(SELF)`. There might be one or more (REMOTE) nodes present.

c Run **`exit`** or **`quit`** to stop the interactive `nnmcluster` process you started in step a.

11 *Complete the following steps on the former active NNMi management server* to temporarily disable application failover:

   a Edit the following file:

   - *Windows*: `%NNM_SHARED_CONF%\props\nms-cluster.properties`
   - *UNIX*: `$NNM_SHARED_CONF/props/nms-cluster.properties`

   b Comment out the `com.hp.ov.nms.cluster.name` parameter.

Upgrade the former active NNMi management server to NNMi 9.1x Patch 5 using the instructions located in the *NNMi Installation Guide*.

> You must upgrade all of the iSPIs that you have installed on the former active NNMi management server to iSPI versions that support NNMi 9.1x Patch 5.

Now you have two servers running NNMi 9.10, but they are still independent since the databases are not synchronized.

12 Complete the following steps on the former active NNMi management server:

   a Run the **`ovstop`** command.

   b Edit the following file:

   — *Windows*: `%NNM_SHARED_CONF%\props\nms-cluster.properties`

   — *UNIX*: `$NNM_SHARED_CONF/props/nms-cluster.properties`

   c Type in the value of the `com.hp.ov.nms.cluster.name` parameter.

   d Uncomment the `com.hp.ov.nms.cluster.name` parameter.

   e Save your changes.

13 Run either the **`ovstart`** or **`nnmcluster -daemon`** command on the former active NNMi management server. It is now the active node.

14 Instruct the operators to begin using the active node to monitor the network.

> The former standby NNMi management server discards all of the database activity occurring during the maintenance window, from step step 9 on page 289 through step 13 on page 290

15 Complete the following steps on the former standby NNMi management server:

   a Run the **`ovstop`** command.

   b Edit the following file:

   — *Windows*: `%NNM_SHARED_CONF%\props\nms-cluster.properties`

   — *UNIX*: `$NNM_SHARED_CONF/props/nms-cluster.properties`

   c Uncomment the `com.hp.ov.nms.cluster.name` parameter.

   d Save your changes.

16 Run either the **`ovstart`** or **`nnmcluster -daemon`** command on the former standby NNMi management server.

   This NNMi management server becomes the standby node, and receives a copy of the database from the active node.

17 If you installed the NNM iSPI Performance for QA, the NNM iSPI Performance for Metrics, or the NNM iSPI Performance for Traffic; are using the application failover feature; and completed the ugrade process shown above, run the NNM iSPI enablement script for each NNM iSPI on both the active and standby NNMi management servers.

18 If you are using Linux NNMi management servers, run the following command on both the active and standby NNMi management servers:
`chmod 777 /var/opt/OV/shared/perfSpi/datafiles/nnm_details.xml`

Application Failover and NNMi Patches

Both NNMi management servers must be running the same NNMi version and patch level. To add patches to the active and standby NNMi management servers, use one of the following procedures:

- Applying Patches for Application Failover (Shut Down Both Active and Standby)
  Use this procedure when you are not concerned with an interruption in network monitoring.
- Applying Patches for Application Failover (Keep One Active NNMi Management Server)
  Use this procedure when you must avoid any interruptions in network monitoring.

Applying Patches for Application Failover (Shut Down Both Active and Standby)

This procedure results in both NNMi management servers being non-active for some period of time during the patch process. To apply patches to the NNMi management servers configured for application failover, follow these steps:

1 As a precaution, run the **`nnmconfigexport.ovpl`** script on both the active and standby NNMi management servers before proceeding. For information, see Best Practice: Save the Existing Configuration on page 40.

2 As a precaution, back up your NNMi data on both the active and standby NNMi management servers before proceeding. For information, see Backup Scope on page 355.

3 As a precaution, on the active NNMi management server, do the following steps:

   a Run the **`nnmcluster`** command.

   b Embedded database only: After NNMi prompts you, type **`dbsync`**, then press `Enter`. Review the displayed information to make sure it includes the following messages:

   `ACTIVE_DB_BACKUP`: This means that the active `NNMi management server is performing a new backup.`
   `ACTIVE_NNM_RUNNING`: This means that the active NNMi management server completed the backup referred to by the previous message.
   `STANDBY_READY`: This shows the previous status of the standby NNMi management server.
   `STANDBY_RECV_DBZIP`: This means that the standby NNMi management server is receiving a new backup from the active NNMi management server.
   `STANDBY_READY`: This means that the standby NNMi management server is ready to perform if the active NNMi management server fails.

4. Run the **nnmcluster -halt** command on the active NNMi management server. This shuts down all `nnmcluster` processes on both the active and standby NNMi management servers.
5. To verify there are no nnmcluster nodes running on either server, *complete the following steps on both the active and standby NNMi management servers*.
   a. Run the **nnmcluster** command.
   b. Verify that there are no nnmcluster nodes present except the one marked `(SELF)`.
   c. Run **exit** or **quit** to stop the interactive `nnmcluster` process you started in step a.
6. On the active NNMi management server, comment out the `com.hp.ov.nms.cluster.name` parameter in the `nms-cluster.properties` file.
   a. Edit the following file:
      — *Windows*: `%NNM_SHARED_CONF%\props\nms-cluster.properties`
      — *UNIX*: `$NNM_SHARED_CONF/props/nms-cluster.properties`
   b. Comment out the `com.hp.ov.nms.cluster.name` parameter.
   c. Save your changes.
7. Apply the NNMi patch to the active NNMi management server using the instructions provided with the patch.
8. On the active NNMi management server, uncomment the `com.hp.ov.nms.cluster.name` parameter in the `nms-cluster.properties` file.
   a. Edit the following file:
      — *Windows*: `%NNM_SHARED_CONF%\props\nms-cluster.properties`
      — *UNIX*: `$NNM_SHARED_CONF/props/nms-cluster.properties`
   b. Uncomment the `com.hp.ov.nms.cluster.name` parameter.
   c. Save your changes.
9. Run the **ovstart** command on the active NNMi management server.
10. Verify that the patch installed correctly on the active NNMi management server by viewing information on the **Product** tab of the **Help > System Information** window in the NNMi console.
11. Run the **nnmcluster -dbsync** command to create a new backup.
12. On the standby NNMi management server, comment out the `com.hp.ov.nms.cluster.name` parameter in the `nms-cluster.properties` file as shown in step a on page 292 through step c on page 292
13. Apply the NNMi patch to the standby NNMi management server.
14. On the standby NNMi management server, uncomment the `com.hp.ov.nms.cluster.name` parameter in the `nms-cluster.properties` file as shown in step a on page 292 through step c on page 292.
15. Run the **ovstart** command on the standby NNMi management server.

16 If you installed the NNM iSPI Performance for QA, the NNM iSPI Performance for Metrics, or the NNM iSPI Performance for Traffic; are using the application failover feature; and completed the patch process shown above, run the NNM iSPI enablement script for each NNM iSPI on both the active and standby NNMi management servers.

17 If you are using Linux NNMi management servers, run the following command on both the active and standby NNMi management servers:
`chmod 777 /var/opt/OV/shared/perfSpi/datafiles/nnm_details.xml`

Applying Patches for Application Failover (Keep One Active NNMi Management Server)

This procedure results in one NNMi management server always being active during the patch process.

➤ This process results in continuous monitoring of the network, however NNMi loses the transaction logs occurring during this patch process.

To apply NNMi patches to the NNMi management servers configured for application failover, follow these steps:

1 As a precaution, run the **`nnmconfigexport.ovpl`** script on both the active and standby NNMi management servers before proceeding. For information, see Best Practice: Save the Existing Configuration on page 40.

2 As a precaution, back up your NNMi data on both the active and standby NNMi management servers before proceeding. For information, see Backup Scope on page 355.

3 To synchronize the two databases, run the following command on either of the NNMi management servers:
`nnmcluster -dbsync`

➤ The **`dbsync`** option works on an NNMi management server using the embedded database. Do not use the **`dbsync`** option on an NNMi management server configured to use an Oracle database.

4 To monitor the progress, run the following command on both the active and standby NNMi management servers:
`nnmcluster -display`
Wait until the active NNMi management server reverts to `ACTIVE_NNM_RUNNING` and the standby NNMi management server reverts to `STANDBY_READY`. before continuing.

5 To disable the cluster, run the following command on the active NNMi management server:
`nnmcluster -disable`

6 Stop the cluster on the standby NNMi management server by running the following command on the standby NNMi management server:
`nnmcluster -shutdown`

7 Make sure the following processes and services terminate before continuing:

- `postgres`
- `ovjboss`

8 Make sure the `nnmcluster` process terminates before continuing. If the `nnmcluster` process will not terminate, manually kill the `nnmcluster` process only as a last resort.

9 Edit the following file on the standby NNMi management server:

Windows: `%nnmDataDir%\shared\nnm\conf\props\nms-cluster.properties`

UNIX: `$nnmDataDir/shared/nnm/conf/props/nms-cluster.properties`

10 Comment out the cluster name by placing a **#** at the front of the line, then save your changes:

```
#com.hp.ov.nms.cluster.name = NNMicluster
```

11 Install the NNMi patch on the standby NNMi management server.

12 Shut down the cluster on the active NNMi management server by running the following command on the activeNNMi management server:

```
nnmcluster -halt
```

13 Make sure the `nnmcluster` process terminates. If it does not terminate within a few minutes, manually kill the `nnmcluster` process.

14 On the standby NNMi management server, uncomment the cluster name from the `nms-cluster.properties` file.

15 Start the cluster on the standby NNMi management server by running the following command on the standby NNMi management server:

```
nnmcluster -daemon
```

16 Install the NNMi patch on the active NNMi management server.

17 Uncomment the entry in the `nms-cluster.properties` file on the active NNMi management server.

18 Start the active NNMi management server using the following command:

```
nnmcluster -daemon
```

19 To enable the cluster, run the following command on the active NNMi management server:

```
nnmcluster -enable
```

20 To monitor the progress, run the following command on both the active and standby NNMi management servers:

```
nnmcluster -display
```

Wait until the active NNMi management server finishes retrieving the database from the standby NNMi management server.

21 After the active NNMi management server opens `STANDBY_READY`, run the following command on the active NNMi management server:

```
nnmcluster -acquire
```

22 If you installed the NNM iSPI Performance for QA, the NNM iSPI Performance for Metrics, or the NNM iSPI Performance for Traffic; are using the application failover feature; and completed the patch process shown above, run the NNM iSPI enablement script for each NNM iSPI on both the active and standby NNMi management servers.

23 If you are using Linux NNMi management servers, run the following command on both the active and standby NNMi management servers:

```
chmod 777 /var/opt/OV/shared/perfSpi/datafiles/nnm_details.xml
```

Application Failover and Restarting the NNMi Management Servers

You can restart the standby NNMi management server at any time with no special instructions. If you restart both the standby and active NNMi management servers, restart the active NNMi management server first.

To restart either the active or the standby NNMi management server, do the following.

1. Run the **`nnmcluster -disable`** command on the NNMi management server to disable the application failover feature.
2. Restart the NNMi management server.
   a. Run the **`ovstop`** command on the NNMi management server.
   b. Run the **`ovstart`** command on the NNMi management server.
3. Run the **`nnmcluster -enable`** command on the NNMi management server to enable the application failover feature.

Application Failover Control after a Communication Failure

When there is a communication failure between the two nodes, both nodes will become an active node and, therefore, a controller of its new group. After a communication failure between two remote nodes is resolved, JGroups determines which member of the new single cluster becomes the controller based on the lowest IP address. The controller determines which node is the Active member (this node is always the node on which the controller is running). NNMi starts on the Active member. This functionality is subject to change in future releases.

Application Failover and Recovery from a Previous Database Backup (Embedded Database Only)

To restore your NNMi database from an original backup when active and standby NNMi management servers are configured for application failover, follow these steps:

1. Run the **`nnmcluster -halt`** command on the active NNMi management server.
2. Delete or move the following directory on both the active and standby NNMi management servers:
   - *Windows*: `%NnmDataDir%\shared\nnm\databases\Postgres_standby`
   - *UNIX*: `$NnmDataDir/shared/nnm/databases/Postgres_standby`
3. Restore the database on the active NNMi management server:
   a. Modify the following file to comment out the cluster name:
      — *Windows*: `%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties`
      — *UNIX*: `$NnmDataDir/shared/nnm/conf/props\nms-cluster.properties`
   b. Restore the database as normal. See Same System Restore on page 358.
   c. Run the **`ovstop`** command on the active NNMi management server.

d Modify the following file to uncomment the cluster name:

— *Windows*:
`%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties`

— *UNIX*: `$NnmDataDir/shared/nnm/conf/props/nms-cluster.properties`

4 Run the **`ovstart`** command on the active NNMi management server.

5 Wait until the active NNMi management server generates a new backup. To verify that this step is complete, run the **`nnmcluster -display`** command and look for an `ACTIVE_NNM_RUNNING` message.

6 Run the **`ovstart`** command on the standby NNMi management server. The standby NNMi management server copies and extracts the new backup. To verify that this step is complete, run the **`nnmcluster -display`** command and look for a `STANDBY_READY` message.

Network Latency/Bandwidth Considerations

NNMi application failover works by exchanging a continuous heartbeat signal between the nodes in the cluster. It uses this same network channel for exchanging other data files such as the NNMi embedded database, database transaction logs, and other NNMi configuration files. HP recommends using a high performance, low latency connection for NNMi application failover when implementing it over a WAN (wide area network).

The NNMi embedded database can become quite large, and can grow to 1GB or more even though this file is always compressed. Also, NNMi generates hundreds, or even thousands, of transaction logs during the built-in backup interval (a configuration parameter that defaults to six hours). Each transaction log can be several megabytes, up to a maximum size of 16 MB. (These files are also compressed). Example data collected from an HP test environments is shown here:

```
Number of nodes managed: 15,000

Number of interfaces: 100,000

Time to complete spiral discovery of all expected nodes: 12 hours

Size of database: 850MB (compressed)

During initial discovery: ~10 transaction logs per minute (peak of ~15/
min)

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

10 TxLogs/minute X 12 hours = 7200 TxLogs @ ~10MB = ~72GB
```

This is a lot of data to send over the network. If the network between the two nodes is unable to keep up with the bandwidth demands of NNMi application failover, the standby node can fall behind in receiving these database files. This could result in a larger window of potential data loss if the active server fails.

Similarly, if the network between the two nodes has a high latency or poor reliability, this could result in a *false* loss-of-heartbeat between the nodes. For example, this can happen when the heartbeat signal does not respond in a timely manner, and the standby node assumes that the active node has failed. There are several factors involved in detecting loss-of-heartbeat. NNMi avoids false failover notification as long as the network keeps up with the application failover data transfer needs.

In HP's verification of multi-subnet NNMi application failover, the active and standby servers resided in the United States, one in Colorado and another in Houston. This provided acceptable bandwidth and latency, with no false failovers.

Application Failover and the NNMi Embedded Database

Application failover works with both the embedded and the Oracle database for NNMi 9.10. However, with Oracle, the database resides on a server that is separate from any NNMi management server, When you configure NNMi to work with an Oracle database, there is no database replication. This results in reduced network demands for application failover using an Oracle database. When using application failover with Oracle, the network uses less than 1% of the network demands as compared to using application failover with the embedded database. The information contained in this section explains NNMi traffic information related to application failover using the embedded database.

After you configure NNMi using the embedded database for application failover, NNMi does the following:

1. The active node performs a database backup, storing the data in a single ZIP file.
2. NNMi sends this ZIP file across the network to the standby node.
3. The standby node expands the ZIP file, and configures the embedded database to import transaction logs on the first startup.
4. The embedded database on the active node generates transaction logs, depending on database activity.
5. Application failover sends the transaction logs across the network to the standby node, where they accumulate on the disk.
6. When the standby node becomes active, NNMi starts, and the database imports all transaction logs across the network. The amount of time this takes depends on the number of files and complexity of the information stored within those files (some files take longer to import than other files of comparable size).
7. After the standby node imports all of the transaction logs, the database becomes available, and the standby node starts the remaining NNMi processes.
8. The original standby node is now active, and the procedure starts over at step 1.

Network Traffic in and Application Failover Environment

NNMi transfers many items across the network from the active node to the standby node in an application failover environment:

- Database Activity: the database backup, as a single ZIP file.
- Transaction logs.
- A periodic *heartbeat* so that each application failover node verifies that the other node is still running.
- File comparison lists so that the standby node can verify that its files are in synchronization with those on the active node.
- Miscellaneous events, such as changes in parameters (enable/disable failover and others) and nodes joining or node leaving the cluster,

The first two items generate 99% of the network traffic used by application failover. This section explores these two items in more detail.

Database Activity: NNMi generates transaction logs for all database activity. Database activity includes everything in NNMi. This activity includes, but is not limited to, the following database activities:

- Discovering new nodes.
- Discovering attributes about nodes, interfaces, VLANs, and other managed objects.
- State polling and status changes.
- Incidents, events, and root cause analysis.
- Operator actions in the NNMi console.

Database activity is outside of your control. For example, an outage on the network results in NNMi generating many incidents and events. These incidents and events trigger state polling of devices on the network, resulting in updates to device status in NNMi. When the outage is restored, additional *node up* incidents result in further status changes. All of this activity updates entries in the database.

Although the embedded database itself grows with database activity, it reaches a stable size for your environment, with only moderate growth over time.

Database Transaction Logs: The embedded database works by creating an empty 16 MB file, then writing database transaction information to that file. NNMi closes this file, then makes it available to application failover after 15 minutes, or after writing 16 MB of data to the file, whichever comes first. That means that a completely idle database will generate one transaction log file every 15 minutes, and this file will be essentially *empty*. Application failover compresses all transaction logs, so an empty 16 MB file compresses down to under 1MB. A *full* 16MB file compresses to about 8 MB. Keep in mind that during periods of higher database activity, application failover generates more transaction logs in a shorter period of time, since each file gets full faster.

An Application Failover Traffic Test

The following test resulted in an average of about 2 transaction log files per minute, with an average file size of 7 MB per file. This is due to the database activity associated with discovery of the additional 5000 nodes added with each failover event. The database in this test case eventually stabilized at about 1.1GB (as measured by the size of the backup ZIP file), with 31,000 nodes and 960,000 interfaces.

Testing Method: During the first 4 hours, test personnel seeded NNMi with 5,000 nodes and waited until discovery stabilized. After 4 hours, test personnel induced failover (the standby node became active, and the previous-active node became standby). Immediately after failover, test personnel added approximately 5,000 more nodes, waited another 4 hours to let the NNMi discovery process stabilize, then induced another failover (failed back to t previous active node). Test personnel repeated this cycle several times with some variation in the time between failover (4 hours, then 6 hours, then 2 hours). After each failover event, test personnel measure the following:

- The size of the database backup ZIP file (created when the node first became active).
- The transaction logs: the total number of files and disk space use.
- The number of nodes and interfaces in the NNMi database immediately before inducing failover.
- Time to complete failover. This included the time from the initial `ovstop` command on the active node until the standby node became fully active with NNMi running.

Table 22 summarizes the results:

Table 22 Application Failover Test Results

Hours	DB.zip Size (MB)	No. of Tx Logs	Tx Logs (GB)	Nodes	Interfaces	Failover Time (Minutes)
4	6.5	50	.3	5,000	15,000	5
8	34	500	2.5	12,000	222,000	10
12	243	500	2.5	17,000	370,000	25
16	400	500	3.5	21,500	477,000	23
20	498	500	3.5	25,500	588,000	32
26	618	1100	7.5	30,600	776,000	30
28	840	400	2.2	30,600	791,000	31
30	887	500	2.5	30,700	800,000	16

Observations: When NNMi transferred files from the active node to the standby node, the transfer averaged about 5 GB every 4 hours, which is a continuous throughput of approximately 350KB/s (kilobytes per second) or 2.8 Mb/S (megabits per second).

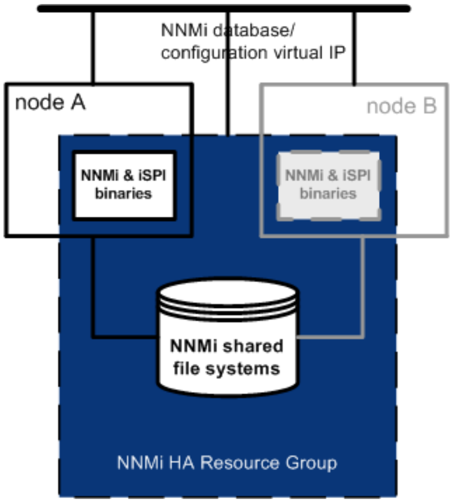
This data does not include any other application failover traffic, such as the heartbeat, file consistency checks, or other application failover communication. This data also excludes the overhead of network I/O, such as packet headers. This data only included the actual network payload of each file's contents moving across the network.

The traffic generated by NNMi application failover environment is very bursty. Application failover identifies new transaction logs on the active node every five minutes and sends these logs to the standby node. Depending on network speed, the standby node should receive all of the new files in a short time, resulting in a relatively idle network for the remainder of that 5-minute interval.

Every time the active and standby nodes switch roles (the standby node becomes active and the active node becomes standby), the new active node will generate a complete database backup and send this across the network to the new standby node. This database backup also occurs periodically, backing up every 24 hours by default. Every time NNMi generates a new backup, it sends this backup to the standby node. Having this new backup available on the standby node reduces the failover time, as all of the transaction logs NNMi generated in that 24 hour interval are already in the database, and do not need to be imported at failover time.

The information provided in the above section will help you understand how the network might perform after a failover when using NNMi with application failover using the embedded database.

Configuring NNMi in a High Availability Cluster



High availability (HA) refers to a hardware and software configuration that provides for uninterrupted service should some aspect of the running configuration fail. An HA cluster defines a grouping of hardware and software that works together to ensure continuity in functionality and data when failover occurs.

NNMi provides support for configuring NNMi to run in an HA cluster under one of several separately purchased HA products. Most of the NNM Smart Plug-ins (iSPIs), but not the NNM iSPI NET diagnostics server, can also run under HA.

This chapter provides a template for configuring NNMi to run in an HA environment. This chapter does not provide end-to-end instructions for configuring your HA product. The HA configuration commands that NNMi provides are wrappers around the commands for the supported HA products. If you prefer, you can substitute the HA product-specific commands where these instructions specify NNMi-provided commands.

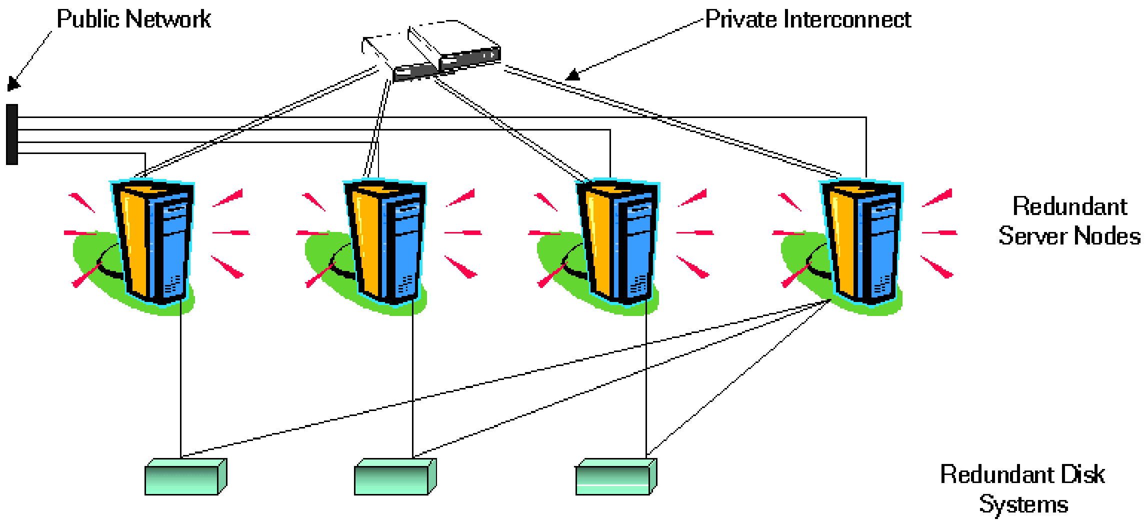
If you plan to install any NNM iSPIs on the NNMi management server, also see the documentation for those NNM iSPIs.

This chapter contains the following topics:

HA Concepts

Cluster architecture provides a single, globally coherent process and resource management view for the multiple nodes of a cluster. Figure 20 shows an example of a cluster architecture.

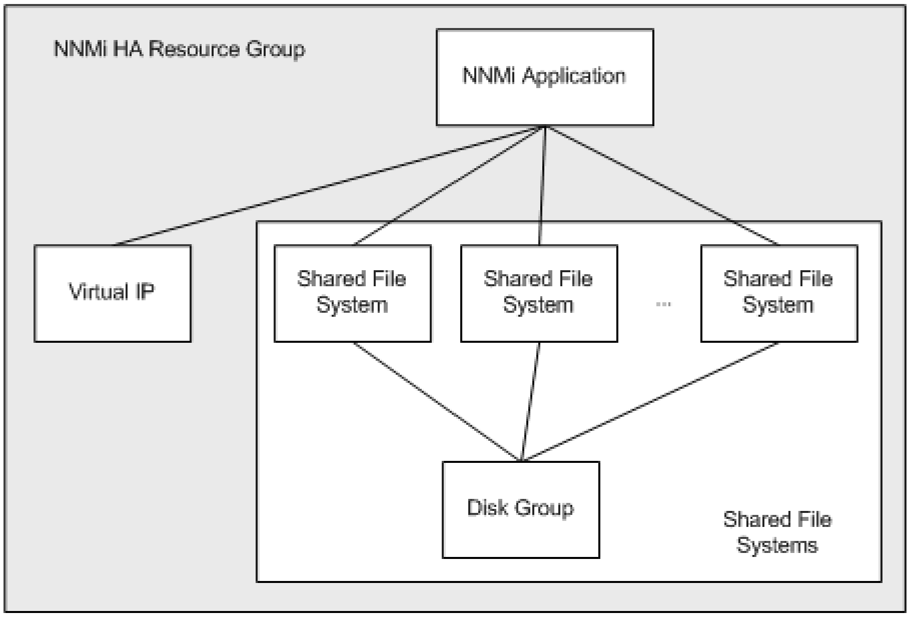
Figure 20 Architecture of a High Availability Cluster



Each node in a cluster connects to one or more public networks and also connects to a private interconnect, representing a communication channel for transmitting data between cluster nodes.

In modern cluster environments such as HP Serviceguard, Veritas Cluster Server, Microsoft Failover Clustering, or Microsoft Cluster Services, applications are represented as compounds of resources, which are simple operations that enable applications to run in a cluster environment. The resources construct an **HA resource group**, which represents an application running in a cluster environment. Figure 21 shows an example HA resource group.

Figure 21 Typical HA Resource Group Layout



This document uses the term *HA resource group* to designate a set of resources in any cluster environment. Each HA product uses a different name for the HA resource group. Table 23 lists the term for each supported HA product that equates to *HA resource group* for this document. (For the specific supported versions of each HA product, see the *NNMi System and Device Support Matrix*.)

Table 23 Terminology for HA Resource Group in the Supported HA Products

HA Product	Abbreviation	Equivalent Term for HA Resource Group
Microsoft Failover Clustering	MSFC	Resource Group
HP Serviceguard	SG	Package
Veritas Cluster Server	VCS	Service Group
Red Hat Cluster Suite	RHCS	Service

HA Terms

Table 24 lists and defines some common HA terms.

Table 24 Common HA Terms

Term	Description
HA resource group	An application running in a cluster environment (under an HA product). An HA resource group can simultaneously be a cluster object that represents an application in a cluster.
Volume group	One or more disk drives that are configured to form a single large storage area.
Logical volume	An arbitrary-size space in a volume group that can be used as a separate file system or as a device swap space.

Table 24 Common HA Terms (cont'd)

Term	Description
Primary cluster node	The first system on which the software product is installed, *and* the first system on which HA is configured. The shared disk is mounted on the primary cluster node for initial set up. The primary cluster node generally becomes the first active cluster node, but you do not need to maintain the primary designation after HA configuration is complete. The next time you update the HA configuration, another node might become the primary cluster node.
Secondary cluster node	Any system that is added to the HA configuration after the primary cluster node has been fully configured for HA.
Active cluster node	The system that is currently running the HA resource group.
Passive cluster node	Any system that is configured for HA but is not currently running the HA resource group. If the active cluster node fails, the HA resource group fails over to one of the available passive cluster nodes, which then becomes the active cluster node for that HA resource group.

NNMi HA Cluster Scenarios

For NNMi HA configuration, NNMi is installed on each system that will become part of an HA resource group. The NNMi database is located on a separate disk that is accessed by the NNMi programs running on each system. (Only one system, the active cluster node, accesses the shared disk at any given time.)

This approach is valid for the embedded and third-party database solutions.

➤ Run the NNMi database backup and restore scripts on the active cluster node only.

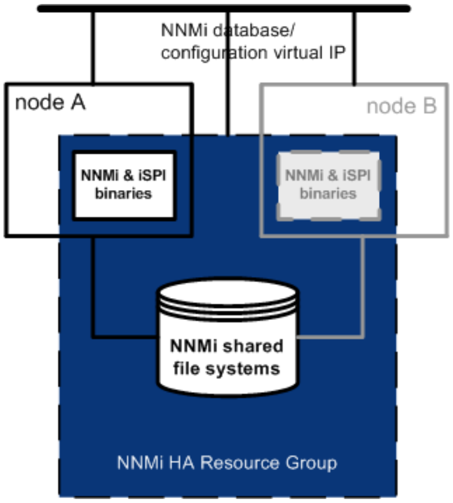
NNMi-only scenario

Figure 22 shows a graphical representation of the NNMi HA cluster scenario. In this figure the NNMi HA resource group is synonymous with the NNMi HA cluster.

Node A and node B are each a fully installed NNMi management server that contains the NNMi program and any NNM iSPIs that run on that system. The active cluster node accesses the shared disk for runtime data. Other products connect to NNMi by the virtual IP address of the HA resource group.

If the cluster contains more than two NNMi nodes, additional nodes are configured similarly to node B in Figure 22.

Figure 22 Basic Scenario for NNMi HA Cluster

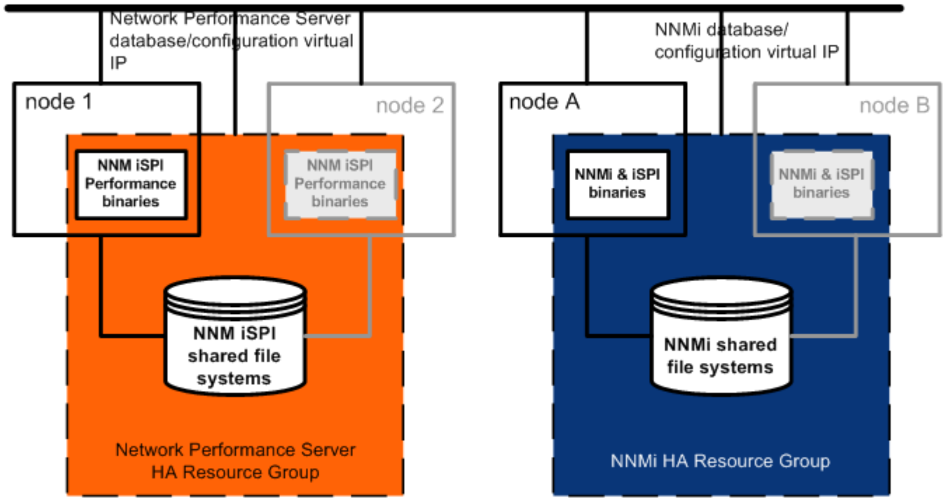


For information about how to implement this scenario, see Configure NNMi for HA on page 309 and Configure NNM iSPIs for HA on page 315.

NNMi and NNM Performance iSPIs on a standalone server scenario

If you are running any of the NNM Performance iSPIs on a standalone server, you can configure these NNM iSPIs to run as a separate HA resource group within the NNMi HA cluster, as shown in Figure 23. The NNMi HA resource group is the same as that described for the NNMi-only scenario.

Figure 23 HA for NNMi and NNM Performance iSPIs on a Standalone Server


Network Performance Server
database/configuration virtual
IP
node 1
node 2
NNM iSPI Performance binaries
NNM iSPI Performance binaries
NNM iSPI shared file systems
Network Performance Server
HA Resource Group
NNMi database/
configuration virtual IP
node A
node B
NNMi & iSPI binaries
NNMi & iSPI binaries
NNMi shared file systems
NNMi HA Resource Group

For information about how to implement this scenario, see Configure NNMi for HA on page 309 and Configure NNM iSPIs for HA on page 315.

Other options for the NNM Performance iSPIs on a standalone server are as follows:

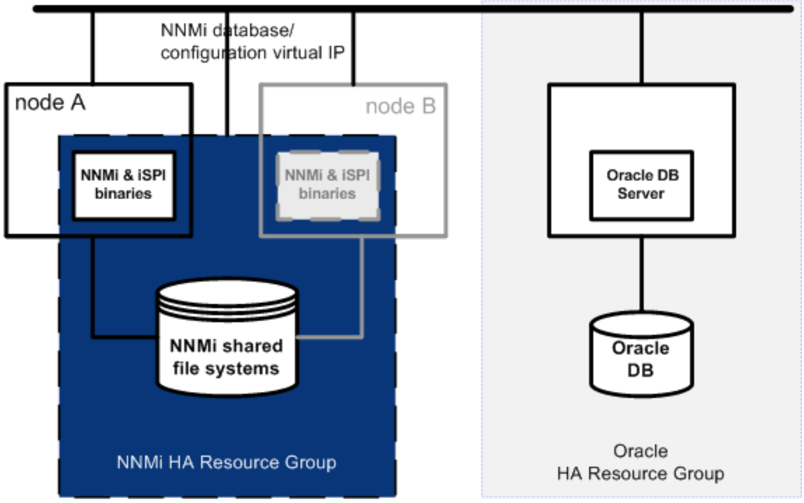
- Run the NNM Performance iSPIs on a single system with no HA. Use this approach while evaluating the NNM iSPIs and for environments where it is not critical for performance data to be always available.
- Configure the NNM Performance iSPIs to run under a different HA cluster than that for NNMi. In this case, you must manage the NNM Performance iSPIs' dependency on NNMi manually.

NNMi with an Oracle database scenario

If your NNMi implementation uses Oracle for the main NNMi database, the Oracle database should be on a separate server, as shown in Figure 24, for performance reasons. Therefore, you must configure two HA resource groups within the NNMi HA cluster:

- The NNMi HA resource group includes the NNMi nodes and a shared disk for NNMi data that is not stored in the Oracle database.
- The Oracle HA resource group contains the Oracle database server and the database disk.

Figure 24 HA for NNMi with an Oracle Database

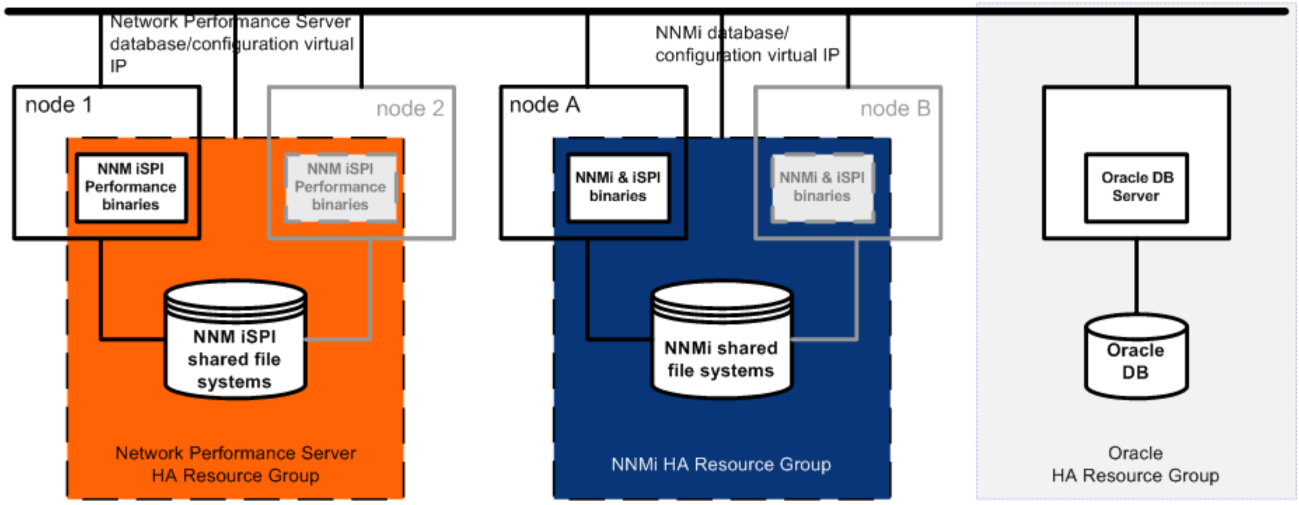


For information about how to implement this scenario, see Configure NNMi for HA in an Oracle Environment on page 316 and Configure NNM iSPIs for HA on page 315.

NNMi with an Oracle database and NNM Performance iSPIs on a standalone server scenario

If your NNMi implementation uses Oracle for the main NNMi database and you are running any of the NNM Performance iSPIs on a standalone server, you can configure three HA resource groups within the NNMi HA cluster, as shown in Figure 25.

Figure 25 HA for NNMi with an Oracle Database and NNM Performance iSPIs on a Standalone Server



For information about how to implement this scenario, see Configure NNMi for HA in an Oracle Environment on page 316 and Configure NNM iSPIs for HA on page 315.

Manpages

With regard to HA configuration, the NNMi manpages contain the following topics:

- nnm-ha
- nnmhaconfigure.ovpl
- nnmhaunconfigure.ovpl
- nnmhadisk.ovpl
- nnmhaclusterinfo.ovpl
- nnmhastartrg.ovpl
- nnmhastoprg.ovpl

On the Windows operating system, these manpages are available as text files.

Verifying the Prerequisites to Configuring NNMi for HA

Successful configuration of NNMi for HA depends on a number of factors:

- Appropriate hardware
- Understanding of the HA product
- A methodical approach to configuration

Before you begin to configure NNMi for HA, complete the following preparation:

1. Verify that NNMi supports your HA product by checking the information in the *NNMi System and Device Support Matrix*.
2. Read the documentation for your HA product to familiarize yourself with the capabilities of that product and to make design decisions.

   HA product documentation changes frequently. Be sure you have the most recent versions available.

3. Verify that each system to be included as a node in an NNMi HA cluster meets the following requirements:
   - Meets all requirements described in the documentation for the HA product.
   - Includes at least two network interface cards (NIC cards).

     Review the HA product, operating system, and NIC card documentation to verify that these products can all work together.

   - Supports the use of a virtual IP address for the HA resource group. This IP address is the IP address used for the NNMi license.

     MSFC requires multiple virtual IP addresses, one for the HA cluster and one for each HA resource group. In this case, the virtual IP address of the NNMi HA resource group is the IP address used for the NNMi license.

- Supports the use of a shared disk or disk array

  Review the HA product, operating system, and disk manufacturer documentation to verify that these products, including the related SCSI cards, can all work together.

- Meets all requirements for NNMi as described in the *NNMi System and Device Support Matrix*.

4 If you plan to run any NNM iSPIs in the NNMi HA cluster, read the appropriate NNM iSPI documentation for additional HA configuration prerequisites.

5 Allocate the following virtual IP addresses and hostnames:

- One virtual IP address for the HA cluster (MSFC only)
- One virtual IP address for each HA resource group to be configured

6 From any system, use the `nslookup` command to validate correct DNS response for all of the IP addresses and hostnames you allocated in step 5.

7 Verify that operating system of each system is at the correct version and patch level for the HA product and NNMi.

8 If necessary, install the HA product.

In a Solaris Zones environment, install the HA product in the global zone.

9 Prepare the shared disk as described in Prepare the Shared Disk Manually on page 319.

10 Use the commands for your HA product to configure (if necessary) and test an HA cluster.

The HA cluster provides such functionality as checking the application heartbeat and initiating failover. The HA cluster configuration must, at a minimum, include the following items:

- (UNIX only) ssh, remsh, or both
- (Windows only) Virtual IP address for the HA cluster that is DNS-resolvable
- Virtual hostname for the HA cluster that is DNS-resolvable
- A resource group that is unique and specific to NNMi.

  NNMi expects that the NNMi HA resource group includes all required resources. If this is not the case, use the HA product functionality to manage dependencies between the NNMi HA resource group and the other HA resource groups. For example, if Oracle is running in a separate HA resource group, configure the HA product to ensure that the Oracle HA resource group is fully started before the HA product starts the NNMi HA resource group.

- *MSFC*: Use the create cluster wizard of Failover Cluster Management for Windows Server 2008.
- *ServiceGuard*:
  - Add .rhosts entries or .ssh entries for nodes.
  - Configure the HA product (cmgetconf, cmcheckconf, cmapplyconf). See the most recent documentation for your HA product on setting up a cluster.
- *VCS*: Not necessary. Product installation created an HA cluster.

- *RHCS*: Add services (cman, rgmanager) as described in the RHCS documentation.

For information about testing the resources that you will place into the NNMi HA resource group, see HA Resource Testing on page 338.

Configuring HA

This section describes the procedures for configuring a new HA configuration for NNMi. It contains the following topics:

- Configure NNMi Certificates for HA on page 309
- Configure NNMi for HA on page 309
- Configure NNM iSPIs for HA on page 315
- Configure NNMi for HA in an Oracle Environment on page 316

➤ If you are running NNMi in a Solaris Zones environment, you do not need to follow the configuration process described in this chapter. See Running NNMi under HA in a Solaris Zones Environment on page 268.

➤ RHCS configuration requires a complete restart of the HA cluster daemons, including all applications, on each node in the HA cluster. Plan your configuration effort accordingly.

Configure NNMi Certificates for HA

The NNMi installation process configures a self-signed certificate for secure communications between the NNMi console and the NNMi database. The process for configuring NNMi for HA correctly shares the self-signed certificate among the primary and secondary cluster nodes. You do not need to take any extra steps to use the default certificate with NNMi running under HA.

If you want to use a different self-signed certificate or a Certificate Authority (CA)-signed certificate for NNMi communications, you must do some additional work. After obtaining the new certificate, complete the steps shown in Configuring High Availability for a New Certificate on page 130. You can complete this procedure before or after configuring NNMi for HA.

Configure NNMi for HA

The two distinct phases of configuring NNMi for HA are as follows:

1 Copy the NNMi data files to the shared disk.

   - Do this task on the primary node, as described in step 1 through step 9 of Configuring NNMi on the Primary Cluster Node on page 312.

2 Configure NNMi to run under HA.

   - Do this task on the primary node, as described in step 10 through step 15 of Configuring NNMi on the Primary Cluster Node on page 312.
   - Also do this task on the secondary node, as described in Configuring NNMi on the Secondary Cluster Nodes on page 314.

Designate one HA cluster node as the primary NNMi management server. This is the node you expect to be active most of the time. Configure the primary node, and then configure all other nodes in the HA cluster as secondary nodes.

⚠ You *cannot* configure NNMi for HA simultaneously on multiple cluster nodes. After the HA configuration process is completed on one cluster node, proceed with the HA configuration on the next node, and so forth until NNMi is configured for HA on all nodes in the cluster environment.

➤ During failover, the NNMi console is unresponsive. After failover completes, NNMi users must log on to continue their NNMi console sessions.

NNMi HA Configuration Information

The HA configuration script collects information about the NNMi HA resource group. Table 25 lists the information that you will need for configuring the primary node. Gather this information before you begin the configuration procedure.

Table 25 NNMi HA Primary Node Configuration Information

HA Configuration Item	Description
HA resource group	The name of the resource group for the HA cluster that contains NNMi. This name must be unique, specific to NNMi, and not currently in use. For example: nnmtest1
Virtual host short name	The short name for the virtual host. This hostname must map to the virtual IP address for the HA resource group. The `nslookup` command must be able to resolve the virtual host short name and the virtual IP address. **NOTE:** If NNMi is unable to resolve the virtual host short name or the virtual host IP address, the HA configuration script could leave the system in an unstable state. Therefore, HP recommends that you implement a secondary naming strategy (such as entering the information in the `%SystemRoot%\system32\drivers\etc\hosts` file on the Windows operating system or `/etc/hosts` file on UNIX operating systems) in case DNS is not available during NNMi HA configuration.
Virtual host netmask	The subnet mask that is used with the virtual host IP address, which must be an IPv4 address.
Virtual host network interface	The network interface on which the virtual host IP address is running. For example: • *Windows*: Local Area Connection • *HP-UX*: lan0 • *Linux*: eth0 • *Solaris*: bge0

Table 25 NNMi HA Primary Node Configuration Information (cont'd)

HA Configuration Item	Description
Shared file system type	The type of shared disk configuration being used for the HA resource group. Possible values are: • `disk`—The shared disk is a physically attached disk that uses a standard file system type. The HA configuration script can configure the shared disk. For more information, see the File system type entry in this table. • `none`—The shared disk uses a configuration other than that described for the `disk` option, such as NFS. After running the HA configuration script, configure the shared disk as described in Prepare the Shared Disk Manually on page 319.
File system type	(UNIX only) The file system type of the shared disk (if the shared file system type is `disk`). The HA configuration scripts pass this value to the HA product so that it can determine how to validate the disk. HP has tested the following shared disk formats: • *Windows*: Basic (see A Note about Shared Disk Configuration on Windows Server on page 321); SAN • *HP-UX*: vxfs • *Linux*: ext2, ext3, and vxfs for VCS and RHCS • *Solaris*: vxfs **NOTE**: HA products support other file system types. If you use a shared disk format that HP has not tested, prepare the disk before configuring NNMi to run under HA, and then specify `none` for the shared file system type while running the NNMi HA configuration script.
Disk group	(UNIX only) The name of the disk group for the NNMi shared file system. This name is based on the name of the HA resource group. For example: nnmtest1-dg
Volume group	(UNIX only) The name of the volume group for the NNMi shared file system. This name is based on the name of the HA resource group. For example: nnmtest1-vol
Mount point	The directory location for mounting the NNMi shared disk. This mount point must be consistent between systems. (That is, each node must use the same name for the mount point.) For example: • *Windows*: `S:\` **NOTE**: Specify the drive completely. `S` and `S:` are unacceptable formats and do not provide access to the shared disk. • *UNIX*: `/nnmmount`

Configuring NNMi on the Primary Cluster Node

Complete the following procedure on the primary cluster node.

➤ If you are using Oracle for the main NNMi database, see Configure NNMi for HA in an Oracle Environment on page 316 first.

➤ If you are running NNMi in a Solaris Zones environment, you do not need to follow the configuration process described in this chapter. See Running NNMi under HA in a Solaris Zones Environment on page 268.

1. If you have not already done so, complete the procedure for Verifying the Prerequisites to Configuring NNMi for HA on page 307.
2. If you have not already done so, install NNMi (including the latest consolidated patch, if any), and then verify that NNMi is working correctly.
3. If you expect to run any NNM iSPIs on this NNMi management server, see Configure NNM iSPIs for HA on page 315 before continuing with this procedure.
4. Use the `nnmbackup.ovpl` command, or another database command, to back up all NNMi data. For example:

   ```
   nnmbackup.ovpl -type offline -scope all -target nnmi_backups
   ```

   For more information about this command, see NNMi Backup and Restore Tools on page 353.
5. Define the disk device group (and logical volume), consisting of at least one shared disk for the NNMi HA resource group. For example:

   - *MSFC*: Use Disk Management to configure the disk mount point and format the disk.
   - *Serviceguard*:

     Use LVM commands such as `pvcreate`, `vgcreate`, and `lvcreate` to initialize the disk, create the volume group, and create the logical volume.
   - *VCS*:

     Use VSF commands such as `vxdiskadm`, `vxassist`, and `mkfs` to add and initialize the disk, allocate disks by space, and create the logical volume.
   - *RHCS*:

     Use LVM commands such as `pvcreate`, `vgcreate`, and `lvcreate` to initialize the disk, create the volume group, and create the logical volume.

   For UNIX operating systems, a reference web site is:
   http://www.unixguide.net/unixguide.shtml

6 Create the directory mount point (for example, `S:\` or `/nnmmount`), and then mount the shared disk:

⚠ After configuration, the HA product manages disk mounting. Do *not* update the file system table with this mount point.

- *Windows*: Use Windows Explorer and Disk Management.
- *UNIX*:
  - — Use the `mkdir` and `mount` commands.
  - — Verify that the shared disk directory mount point has been created with `root` as the user, `sys` as the group, and the permissions set to `555`. For example:

```
ls -l /nnmmount
```

7 Stop NNMi:

```
ovstop -c
```

➤ If NNMi is already installed on a node that you will include in this HA resource group, also run `ovstop -c` on that node at this time.

8 Copy the NNMi database to the shared disk:

- *Windows*:

```
%NnmInstallDir%\misc\nnm\ha\nnmhadisk.ovpl NNM \
-to <HA_mount_point>
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhadisk.ovpl NNM \
-to <HA_mount_point>
```

⚠ To prevent database corruption, run this command (with the `-to` option) only one time. For information about alternatives, see Re-Enable NNMi for HA after All Cluster Nodes are Unconfigured on page 342.

9 (UNIX only) Unmount the shared disk and deactivate the disk group:

```
umount <HA_mount_point>

vgchange -a n <disk_group>
```

10 Verify that NNMi is not running:

```
ovstop -c
```

11 (RHCS only) Copy the NNMi custom script into place, and then restart the HA cluster daemons.

a Copy the `/opt/OV/misc/nnm/ha/NNMscript.sh` file to the following location:

```
/usr/share/cluster/NNMscript.sh
```

b Stop and then restart the `/sbin/ccsd` process.

12 Configure the NNMi HA resource group:

- *Windows*:

```
%NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhaconfigure.ovpl NNM
```

Table 25 on page 310 describes the information that this command requests.

13 (UNIX only) By default NNMi starts in the locale of the user who ran the `nnmhaconfigure.ovpl` command. To change the NNMi locale, run the following command:

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl \
-config NNM -set HA_LOCALE <locale>
```

14 In step 12, what value did you specify for the shared file system type (as described for Shared file system type and File system type in Table 25 on page 310)?

- For type `disk`, the `nnmhaconfigure.ovpl` command configured the shared disk. Continue with step 15.
- For type `none`, prepare the shared disk as described in Prepare the Shared Disk Manually on page 319, and then continue with step 15.

15 Start the NNMi HA resource group:

- *Windows*:

```
%NnmInstallDir%\misc\nnm\ha\nnmhastartrg.ovpl NNM \
<resource_group>
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhastartrg.ovpl NNM \
<resource_group>
```

If NNMi does not start correctly, see Troubleshooting the HA Configuration on page 337.

⚠ Now that NNMi is running under HA, *do not* use the `ovstart` and `ovstop` commands for normal operation. Use these commands only when instructed to do so for HA maintenance purposes.

Configuring NNMi on the Secondary Cluster Nodes

Complete the following procedure on one secondary cluster node at a time.

1 If you have not already done so, complete the procedure for Configuring NNMi on the Primary Cluster Node on page 312.

2 If you have not already done so, complete the procedure for Verifying the Prerequisites to Configuring NNMi for HA on page 307.

3 If you have not already done so, install NNMi (including the latest consolidated patch, if any), and then verify that NNMi is working correctly.

4 Install the NNM iSPIs that you installed in step 3 of Configuring NNMi on the Primary Cluster Node on page 312.

5 Stop NNMi:

```
ovstop -c
```

6 Create a mount point for the shared disk (for example, `S:\` or `/nnmmount`).

This mount point must use the same name as the mount point you created in step 6 of the procedure Configuring NNMi on the Primary Cluster Node.

7 (RHCS only) Copy the NNMi custom script into place, and then restart the HA cluster daemons.

a Copy the `/opt/OV/misc/nnm/ha/NNMscript.sh` file to the following location:

```
/usr/share/cluster/NNMscript.sh
```

b Stop and then restart the `/sbin/ccsd` process.

8 Configure the NNMi HA resource group:

- *Windows*: **`%NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM`**
- *UNIX*: **`$NnmInstallDir/misc/nnm/ha/nnmhaconfigure.ovpl NNM`**

Supply the HA resource group name when the command requests this information.

9 Verify that the configuration was successful:

- *Windows*:

```
%NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl \
-group <resource_group> -nodes
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl \
-group <resource_group> -nodes
```

The command output lists all configured nodes for the specified HA resource group.

10 Optionally, test the configuration by taking the NNMi HA resource group on the primary node offline and then bringing the NNMi HA resource group on the secondary node online.

Configure NNM iSPIs for HA

If you expect to run any NNM iSPIs on the NNMi management server, read this section before configuring NNMi to run under HA.

NNM iSPI Performance for Metrics, NNM iSPI Performance for QA, and NNM iSPI Performance for Traffic

The NNM Performance iSPIs (NNM iSPI Performance for Metrics, NNM iSPI Performance for QA, and NNM iSPI Performance for Traffic) can be installed on the NNMi management server or on a standalone server, but not on a combination of these two options.

- If the NNM Performance iSPIs will be located on the NNMi management server, install the products before configuring NNMi to run under HA.
- If the NNM Performance iSPIs will be located on a standalone server, configure NNMi to run under HA before installing the products. During the NNM iSPI installation process, supply the NNMi HA resource group virtual hostname as the NNMi management server name.

NNM iSPI for MPLS, NNM iSPI for IP Multicast, and NNM iSPI for IP Telephony

The NNM iSPI for MPLS, NNM iSPI for IP Multicast, and NNM iSPI for IP Telephony can be installed on the NNMi management server only. Install these products before configuring NNMi to run under HA.

For information about configuring the NNM iSPIs to run under HA, see the documentation for the appropriate NNM iSPI.

NNM iSPI Network Engineering Toolset Software and NNMi Running under HA

The NNM iSPI Network Engineering Toolset Software SNMP trap analytics and Microsoft Visio export functionality are automatically installed with NNMi. No extra work is needed to run these tools under HA.

The NNM iSPI NET diagnostics server cannot be included in the NNMi HA resource group. Do not install this component on the NNMi management server. To run the NNM iSPI NET diagnostics server on a system that is outside the NNMi HA resource group, follow these steps:

1. Completely configure the NNMi HA resource group.
2. Install the NNM iSPI NET diagnostics server on a system that is outside the NNMi HA resource group. During the NNM iSPI NET diagnostics server installation process, supply the NNMi HA resource group virtual hostname as the NNM Server Hostname.

   For more information, see the *NNM iSPI Network Engineering Toolset Software Planning and Installation Guide*.

If the NNM iSPI NET diagnostics server is already installed on an NNMi management server that will run under HA, uninstall the NNM iSPI NET diagnostics server before configuring NNMi to run under HA.

Uninstalling the NNM iSPI NET diagnostics server removes all existing reports.

It might be possible to save existing reports, as described here, but the following procedure is untested:

1. Use MySQL Workbench to perform a backup of the existing `nnminet` database.

   MySQL Workbench is available in the downloads area at **dev.mysql.com**.
2. Uninstall the NNM iSPI NET diagnostics server.
3. Configure NNMi to run under HA.
4. Install the NNM iSPI NET diagnostics server on a separate system.
5. Before running any flows, use MySQL Workbench to recover the `nnminet` database onto the new installation.

Configure NNMi for HA in an Oracle Environment

This sections presents a high-level overview of the process for configuring NNMi with an Oracle database to run under HA. The number of possible Oracle configurations is large, and the configuration process can vary according to the Oracle release. For the most accurate information about configuring Oracle to run under HA and creating an NNMi dependency on the Oracle HA resource group, see the HA product documentation. You can also go to the Oracle web site (**www.oracle.com**) for information about the appropriate Oracle configuration for your HA product.

NNMi Dependency on Oracle

When Oracle and NNMi both run under HA, the NNMi HA resource group must include a shared disk for the NNMi data that is not stored in the Oracle database. Additionally, consider the following information:

- If the HA product supports dependencies, the recommended approach is to configure each product to run in a separate HA resource group. The Oracle HA resource group must be fully started before the NNMi HA resource group starts. If both HA resource groups are in the same HA cluster, you can modify the cluster configuration to set resource group ordering. If the HA resource groups are in different HA clusters, make sure that the NNMi HA resource group dependency on the Oracle HA resource group is met.
- If the HA product does not support dependencies, include the Oracle systems and the NNMi systems in the NNMi HA resource group.

Configuring NNMi for HA in an Oracle Environment

1. If you plan to run Oracle under HA, complete that configuration first.
2. Create an empty Oracle database instance for NNMi.
3. On the primary NNMi node, install NNMi (including the latest consolidated patch, if any). During installation, do the following:
   a. Select the **Oracle** database type, and then select **Primary Server Installation**.
   b. Specify the virtual IP address or hostname for the Oracle HA resource group (if applicable).
4. On the primary NNMi node, configure NNMi to run under HA as described in Configuring NNMi on the Primary Cluster Node on page 312.
5. Set up the NNMi dependency on the Oracle HA resource group.

   For specific instructions, see the HA product documentation.
6. On the secondary NNMi node, install NNMi (including the latest consolidated patch, if any). During installation, do the following:
   - Select the **Oracle** database type, and then select **Secondary Server Installation**.
   - Specify the virtual IP address or hostname for the Oracle HA resource group (if applicable).
7. On the secondary NNMi node, configure NNMi to run under HA described in Configuring NNMi on the Secondary Cluster Nodes on page 314.
8. For each additional secondary NNMi node, repeat step 6 and step 7.

Shared NNMi Data

This implementation of NNMi running under HA requires the use of a separate disk for sharing files between all NNMi nodes in the HA cluster.

➤ NNMi implementations that use Oracle as the primary database also require the use of a separate disk for shared data.

Data on the NNMi Shared Disk

This section lists the NNMi data files that are maintained on the shared disk when NNMi is running under HA.

The locations are mapped to the shared disk location as follows:

- *Windows*:
  - `%NnmInstallDir%` maps to `%HA_MOUNT_POINT%\NNM\installDir`
  - `%NnmDataDir%` maps to `%HA_MOUNT_POINT%\NNM\dataDir`
- *UNIX*:
  - `$NnmInstallDir` maps to `$HA_MOUNT_POINT/NNM/installDir`
  - `$NnmDataDir` maps to `$HA_MOUNT_POINT/NNM/dataDir`

The directories that are moved to the shared disk are as follows:

- *Windows*:
  - `%NnmDataDir%\shared\nnm\databases\Postgres`
    The embedded database; not present when using an Oracle database.
  - `%NnmDataDir%\log\nnm`
    The NNMi logging directory.
  - `%NnmDataDir%\shared\nnm\databases\eventdb`
    The pmd events database.
  - `%NnmInstallDir%\nonOV\jboss\nms\server\nms\data`
    The transactional store used by ovjboss.
- *UNIX*:
  - `$NnmDataDir/shared/nnm/databases/Postgres`
    The embedded database; not present when using an Oracle database.
  - `$NnmDataDir/log/nnm`
    The NNMi logging directory.
  - `$NnmDataDir/shared/nnm/databases/eventdb`
    The pmd events database.
  - `$NnmInstallDir/nonOV/jboss/nms/server/nms/data`
    The transactional store used by ovjboss.

The `nnmhadisk.ovpl` command copies these files to and from the shared disk. Run this command as the instructions in this chapter indicate. For a summary of the command syntax, see the *nnm-ha* manpage.

Replication of Configuration Files

The NNMi HA implementation uses file replication to maintain copies of the NNMi configuration files on all NNMi nodes in the HA cluster. By default, NNMi manages file replication, copying NNMi configuration files from the active node to a passive node during the failover process. The `nnmdatareplicator.conf` file specifies the NNMi folders and files included in data replication.

Disabling Data Replication

You can disable data replication as follows:

1. Edit the following file:
   - *Windows*: `%NnmDataDir%\shared\nnm\conf\ov.conf`
   - *UNIX*: `$NnmDataDir/shared/nnm/conf/ov.conf`
2. Include the following line:

   ```
   DISABLE_REPLICATION=DoNotReplicate
   ```
3. Save your changes.

When you change files (for example, configuration files) on the Active node, these files are automatically replicated to the Standby node on failover.

Re-enabling Data Replication

After disabling data replication, you can re-enable data replication as follows:

1. Edit the following file:
   - *Windows*: `%NnmDataDir%\shared\nnm\conf\ov.conf`
   - *UNIX*: `$NnmDataDir/shared/nnm/conf/ov.conf`
2. Comment out the following line (by adding the # symbol) as shown:

   ```
   #DISABLE_REPLICATION=DoNotReplicate
   ```
3. Save your changes.

Prepare the Shared Disk Manually

If the shared disk is of a format that HP has tested (as listed in Table 25 on page 310), the HA configuration script prepares the shared disk, and you can ignore this section.

If the shared disk uses a non-tested configuration, such as disk formats supported by the HA product, you must prepare the disk manually. Enter the value `none` for the file system type during HA configuration, and then configure the shared disk and the NNMi HA resource group's use of the shared disk.

You can configure the disk before or after configuring the NNMi HA resource group.

To prepare the shared disk manually, follow these steps:

1. Configure the shared disk as described in Configuring a SAN or a Physically Connected Disk on page 320.

2. Configure the NNMi HA resource group to recognize the disk by completing both of the following procedures:
   - Setting the HA Variables in the ov.conf File on page 320
   - Moving the Shared Disk into the NNMi HA Resource Group on page 321

Configuring a SAN or a Physically Connected Disk

Connecting and formatting a disk that disk into a vxfs or ext3 file system. To configure a SAN or a physically-connected disk, follow these steps:

1. Verify that the shared disk is *not* configured to be mounted at system boot time.

   The resource group is responsible for mounting the shared disk.

2. Connect the device:
   - For a SAN disk, add the SAN device to the network.

     The logical volume on the SAN disk should be in exclusive mode, if that mode is available.

   - For a physically-connected disk, attach the disk using a Y cable.

3. Add operating system entries to all cluster nodes (disk group, logical volume, volume group, and disk):
   - For a SAN disk, the entries reference the SAN.
   - For a physically-connected disk, the entries reference the disk hardware.

4. Format the disk using a disk format listed in Table 25 on page 310.

5. Ensure that the SAN mounts.

   For UNIX systems, a reference web site is: **http://www.unixguide.net/unixguide.shtml**

6. Unmount and deport the disk.

7. To test the configuration, add the disk to a resource group and initiate failover.

Setting the HA Variables in the ov.conf File

The NNMi HA resource group uses the following variables to access the shared disk:

- `HA_POSTGRES_DIR=<HA_mount_point>/NNM/dataDir/shared/nnm/databases/Postgres`
- `HA_EVENTDB_DIR=<HA_mount_point>/NNM/dataDir/shared/nnm/eventdb`
- `HA_NNM_LOG_DIR=<HA_mount_point>/NNM/dataDir/log`
- `HA_JBOSS_DATA_DIR=<HA_mount_point>/NNM/installDir/nonOV/jboss/nms/server/nms/data`
- `HA_MOUNT_POINT=<HA_mount_point>`
- `HA_CUSTOMPOLLER_DIR=<HA_mount_point>/NNM/dataDir/shared/nnm/databases/custompoller`

If you plan to run any NNM iSPIs in the NNMi HA resource group, also set the ov.conf variables for each of those NNM iSPIs. For more information, see the documentation for the appropriate NNM iSPI.

To set the product variables for accessing the shared disk in the `ov.conf` file, run the following command for each of the preceding variables:

- *Windows*:

```
%NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl \
-config NNM -set <variable> <value>
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl \
-config NNM -set <variable> <value>
```

Moving the Shared Disk into the NNMi HA Resource Group

Modify the disk configuration file according to the product documentation to move the shared disk into the NNMi HA resource group. For example:

You can also use this process to add other resources, such as a NIC card or a backup disk to the NNMi HA resource group.

- *MSFC*: Use Failover Management to add resources to the resource group.
- *ServiceGuard*:

  `/etc/cmcluster/<resource_group>/<resource_group>.cntl`
- *VCS*: Add disk entries and links to the HA configuration file by using the `/opt/VRTSvcs/bin/hares` command. For example:
- *RHCS*:

  `/etc/cluster/cluster.conf`

A Note about Shared Disk Configuration on Windows Server

According to Microsoft Knowledge Base article 237853, dynamic disks are not supported for clustering with Windows Server 2008. To ensure the correct disk configuration, review the information located on the following web sites:

- **http://support.microsoft.com/kb/237853**
- **http://www.petri.co.il/difference_between_basic_and_dynamic_disks_in_windows_xp_2000_2003.htm**

Licensing NNMi in an HA Cluster

NNMi requires two licenses to run NNMi in an HA cluster:

- one production license tied to the IP address of one of the physical cluster nodes
- one non-production license tied to the virtual IP address of the NNMi HA resource group

The NNMi license keys are managed on the shared disk. Therefore, each NNMi HA resource group requires only the non-production license keys for each separately licensed product.

When licensing NNMi in an HA cluster, you must update the `licenses.txt` *file on the shared disk with the new information from the license file on the active node. Complete the following procedure to correctly license NNMi in an HA cluster.*

To correctly license NNMi in an HA cluster, perform these steps on the active NNMi cluster node:

1. Obtain and install a permanent non-production license key for each of your ordered products as described in Licensing NNMi on page 117. When prompted for the IP address of the NNMi management server, provide the virtual IP address of the NNMi HA resource group.
2. Update the `licenses.txt` file on the shared disk with the new information from the `LicFile.txt` file on the active node. Do one of the following:
   - If the `licenses.txt` file exists in the `NNM` directory on the shared disk, append the new license keys in `LicFile.txt` on the active node to `licenses.txt` on the shared disk.
   - If the `licenses.txt` file does not exist on the shared disk, copy `LicFile.txt` from the active node to `licenses.txt` in the `NNM` directory on the shared disk.

   On the active node, the `LicFile.txt` file is in the following location:

   - *Windows*:
     `<`*`drive`*`>:\ProgramData\Hewlett-Packard\HPOvLIC\data\LicFile.txt`
   - *UNIX*: `/var/opt/OV/HPOvLIC/LicFile.txt`

   On the shared disk, example locations of the `licenses.txt` file are as follows:

   - *Windows*: `S:\NNM\licenses.txt`
   - *UNIX*: `/nnmount/NNM/licenses.txt`

Maintaining the HA Configuration

Maintenance Mode

When you must apply NNMi patches or update to a newer version of NNMi, put the NNMi HA resource group into maintenance mode to prevent failover during the process. When the NNMi HA resource group is in maintenance mode, you (or an installation script) can run the ovstop and ovstart commands as needed on the primary (active) cluster node.

Never run the ovstart or ovstop commands on a secondary (backup) cluster node.

Putting an HA Resource Group into Maintenance Mode

Putting an HA resource group into maintenance mode disables HA resource group monitoring. When an HA resource group is in maintenance mode, stopping and starting the products in that HA resource group do not cause failover.

To put an HA resource group into maintenance mode, on the active cluster node, create the following file:

- *Windows*: `%NnmDataDir%\hacluster\<resource_group>\maintenance`
- *UNIX*: `$NnmDataDir/hacluster/<resource_group>/maintenance`

The `maintenance` file contents are as follows:

- To disable monitoring of the HA resource group, create the `maintenance` file. The file can be empty or can contain the keyword `NORESTART`.
- To prevent NNMi from starting during a configuration procedure, the first line of the `maintenance` file must contain only the single word:
  `NORESTART`

Removing an HA Resource Group from Maintenance Mode

Taking an HA resource group out of maintenance mode re-enables HA resource group monitoring. Stopping the products in that HA resource group causes the HA resource group to fail over to a passive cluster node.

To remove an HA resource group from maintenance mode, follow these steps:

1 Verify that NNMi is running correctly:

```
ovstatus -c
```

All NNMi services should show the state RUNNING.

2 Delete the `maintenance` file from the node that was the active cluster node before maintenance was initiated. This file is described in Putting an HA Resource Group into Maintenance Mode.

Maintaining NNMi in an HA Cluster

Starting and Stopping NNMi

While NNMi is running under HA, *do not* use the `ovstart` and `ovstop` commands unless instructed to do so for HA maintenance purposes. For normal operation, use the NNMi-provided HA commands or the appropriate HA product commands for starting and stopping HA resource groups.

Changing NNMi Hostnames and IP Addresses in a Cluster Environment

A node in a cluster environment can have more than one IP address and hostname. If a node becomes a member of another subnet, you might need to change its IP addresses. As a result, the IP address or fully-qualified domain name might change.

For example, on UNIX systems, the IP address and the related hostname are generally configured in one of the following:

- /etc/hosts
- Domain Name Service (DNS)
- Network Information Service (NIS on HP-UX or Linux, NIS+ on Solaris)

NNMi also configures the hostname and IP address of the management server for the managed node in the NNMi database.

If you are moving from a non-name-server environment to a name-server environment (that is, DNS or BIND), make sure that the name server can resolve the new IP address.

Hostnames work within IP networks to identify a managed node. While a node might have many IP addresses, the hostname is used to pinpoint a specific node. The system hostname is the string returned when you use the `hostname` command.

When changing the virtual hostname or IP address of the NNMi HA resource group, you must update the `licenses.txt` *file on the shared disk with the new information from the license file on the active node. Complete the following procedure to correctly update the HA configuration.*

To change the virtual hostname or IP address of the NNMi HA resource group, perform these steps on the active NNMi cluster node:

1. Convert and the permanent non-production license keys for the prior virtual IP address of the NNMi HA resource group to the new virtual IP address of the NNMi HA resource group.

   ⚠ Do *not* install the new license keys at this time.

2. Put the NNMi HA resource group into maintenance mode as described in Putting an HA Resource Group into Maintenance Mode on page 323.

3 Stop the NNMi HA resource group:

- *Windows*:

```
%NnmInstallDir%\misc\nnm\ha\nnmhastoprg.ovpl NNM \
<resource_group>
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhastoprg.ovpl NNM \
<resource_group>
```

4 Change the IP address or node name of the NNMi HA resource group:

a In the `ov.conf` file, edit the `NNM_INTERFACE` entry to be the new hostname or IP address.

b In the `ovspmd.auth` file, edit any lines containing the old hostname to contain the new hostname.

The `ov.conf` and `ovspmd.auth` files are available in the following location:

- *Windows*: `%NnmDataDir%\shared\nnm\conf`
- *UNIX*: `$NnmDataDir/shared/nnm/conf`

5 If you changed the node name of the NNMi HA resource group, set NNMi to use the new fully-qualified domain name of the NNMi HA resource group with the `nnmsetofficialfqdn.ovpl` command. For example:

```
nnmsetofficialfqdn.ovpl newnnmi.servers.example.com
```

For more information, see the *nnmsetofficialfqdn.ovpl* reference page, or the UNIX manpage.

6 Change the cluster configuration to use the new IP address:

- *MSFC*:

  In Failover Cluster Management, open ***<resource_group>***.

  Double-click ***<resource_group>*-ip**, select **Parameters**, and the enter the new IP address.

- *Serviceguard*:

  On the active HA cluster node, edit the `/etc/cmcluster/<resource_group>/<resource_group>.cntl` file to replace `IP[0]=<old_IP_address>` with `IP[0]=<new_IP_address>`. (If you moved the NNMi HA resource group to a different subnet, also replace `SUBNET[0]=<old_subnet_mask>` with `SUBNET[0]=<new_subnet_mask>`.) Then use `cmapplyconf` to update all other systems.

- *VCS*:

```
$NnmInstallDir/misc/nnm/ha/nnmhargconfigure.ovpl NNM \
<resource_group> -set_value <resource_group>-ip \
Address <new_IP_address>
```

- *RHCS*:

  On the active HA cluster node, edit the `/etc/cluster/cluster.conf` file to replace `ip address="<old_IP_address>"` with `ip address="<new_IP_address>"`. Then run `ccs_tool update /etc/cluster/cluster.conf` to update all other systems.

7 Install the permanent non-production license keys for the new virtual IP address of the NNMi HA resource group as described in Licensing NNMi on page 117.

8 Update the `licenses.txt` file on the shared disk with the new information from the `LicFile.txt` file on the active node. Do one of the following:

- If the `licenses.txt` file exists in the `NNM` directory on the shared disk, append the new license keys in `LicFile.txt` on the active node to `licenses.txt` on the shared disk.
- If the `licenses.txt` file does not exist on the shared disk, copy `LicFile.txt` from the active node to `licenses.txt` in the `NNM` directory on the shared disk.

On the active node, the `LicFile.txt` file is in the following location:

- *Windows*:
  `<drive>:\ProgramData\Hewlett-Packard\HPOvLIC\data\LicFile.txt`
- *UNIX*: `/var/opt/OV/HPOvLIC/LicFile.txt`

On the shared disk, example locations of the `licenses.txt` file are as follows:

- *Windows*: `S:\NNM\licenses.txt`
- *UNIX*: `/nnmount/NNM/licenses.txt`

9 Start the NNMi HA resource group:

- *Windows*:

```
%NnmInstallDir%\misc\nnm\ha\nnmhastartrg.ovpl NNM \
<resource_group>
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhastartrg.ovpl NNM \
<resource_group>
```

10 Verify that NNMi started correctly:

```
ovstatus -c
```

All NNMi services should show the state RUNNING.

11 Take the NNMi HA resource group out of maintenance mode as described in Removing an HA Resource Group from Maintenance Mode on page 323.

Stopping NNMi Without Causing Failover

When you must perform NNMi maintenance, you can stop NNMi on the active cluster node without causing failover to a currently passive node. Follow these steps on the active cluster node:

1 Put the NNMi HA resource group into maintenance mode as described in Putting an HA Resource Group into Maintenance Mode on page 323.

2 Stop NNMi:

```
ovstop -c
```

Restarting NNMi after Maintenance

If you have stopped NNMi in the manner that prevents failover, follow these steps to restart NNMi and HA monitoring:

1. Start NNMi:

   ```
   ovstart -c
   ```

2. Verify that NNMi started correctly:

   ```
   ovstatus -c
   ```

   All NNMi services should show the state RUNNING.

3. Take the NNMi HA resource group out of maintenance mode as described in Removing an HA Resource Group from Maintenance Mode on page 323.

Maintaining Add-on NNM iSPIs in an NNMi HA Cluster

The NNM iSPIs are closely linked to NNMi. When add-on NNM iSPIs are installed on the nodes in the NNMi HA cluster, use the NNMi HA cluster maintenance procedures as written.

Unconfiguring NNMi from an HA Cluster

Unconfiguring NNMi from an HA Cluster

The process of removing an NNMi node from an HA cluster involves undoing the HA configuration for that instance of NNMi. You can then run that instance of NNMi as a standalone management server, or you can uninstall NNMi from that node.

If you want to keep NNMi configured for high availability, the HA cluster must contain one node that is actively running NNMi and at least one passive NNMi node. If you want to completely remove NNMi from the HA cluster, unconfigure the HA functionality on all nodes in the cluster.

To completely unconfigure NNMi from an HA cluster, follow these steps:

1. Determine which node in the HA cluster is active. On any node, run the following command:

   - *Windows*:

     ```
     %NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl \
     -group <resource_group> -activeNode
     ```

   - *UNIX*:

     ```
     $NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl \
     -group <resource_group> -activeNode
     ```

2. On each passive node, unconfigure any add-on NNM iSPIs from the HA cluster.

   For information, see the documentation for each NNM iSPI.

3 On any node in the HA cluster, verify that the add-on NNM iSPIs on all passive nodes have been unconfigured from the HA cluster:

- *Windows*:

```
%NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl \
-config NNM -get NNM_ADD_ON_PRODUCTS
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl \
-config NNM -get NNM_ADD_ON_PRODUCTS
```

The command output lists the add-on iSPI configurations in the format `<iSPI_PM_Name>[hostname_list]`. For example:

```
PerfSPIHA[hostname1, hostname2]
```

At this time, only the active node hostname should appear in the output. If a passive node hostname appears in the output, repeat step 2 until this command output includes only the active node hostname.

4 On each passive node, unconfigure NNMi from the HA cluster:

- *Windows*:

```
%NnmInstallDir%\misc\nnm\ha\nnmhaunconfigure.ovpl NNM \
<resource_group>
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhaunconfigure.ovpl NNM \
<resource_group>
```

This command removes access to the shared disk but does not unconfigure the disk group or the volume group.

5 On each passive node, move the NNMi HA resource group-specific files to a separate location for safe-keeping:

If you do not plan to reconfigure the NNMi HA resource group, you do not need to save a copy of these files, and you can delete them at this time.

- *MSFC*: In Windows Explorer, delete the `%NnmDataDir%\hacluster\<resource_group>\` folder.
- *Serviceguard*:

```
rm -rf /var/opt/OV/hacluster/<resource_group>
rm -rf /etc/cmcluster/<resource_group>
```

- *VCS*:

```
rm -rf /var/opt/OV/hacluster/<resource_group>
```

- *RHCS*:

```
rm -rf /var/opt/OV/hacluster/<resource_group>
```

6 On the active node, unconfigure any add-on NNM iSPIs from the HA cluster.

For information, see the documentation for each NNM iSPI.On any node in the HA cluster, verify that the add-on NNM iSPIs on all nodes have been unconfigured from the HA cluster:

- *Windows*:

```
%NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl \
-config NNM -get NNM_ADD_ON_PRODUCTS
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl \
-config NNM -get NNM_ADD_ON_PRODUCTS
```

If any hostname appears in the output, repeat step 6 until this command output indicates that no iSPIs are configured.

7 On the active node, stop the NNMi HA resource group:

- *Windows*:

```
%NnmInstallDir%\misc\nnm\ha\nnmhastoprg.ovpl NNM \
<resource_group>
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhastoprg.ovpl NNM \
<resource_group>
```

This command does not remove access to the shared disk. Nor does it unconfigure the disk group or the volume group.

8 On the active node, unconfigure NNMi from the HA cluster:

- *Windows*:

```
%NnmInstallDir%\misc\nnm\ha\nnmhaunconfigure.ovpl NNM \
<resource_group>
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhaunconfigure.ovpl NNM \
<resource_group>
```

This command removes access to the shared disk but does not unconfigure the disk group or the volume group.

9 On the active node, move the NNMi HA resource group-specific files to a separate location for safe-keeping:

If you do not plan to reconfigure the NNMi HA resource group, you do not need to save a copy of these files, and you can delete them at this time.

- *MSFC*: In Windows Explorer, delete the `%NnmDataDir%\hacluster\`*`<resource_group>`*`\` folder.
- *Serviceguard*:

```
rm -rf /var/opt/OV/hacluster/<resource_group>
rm -rf /etc/cmcluster/<resource_group>
```

- *VCS*:

```
rm -rf /var/opt/OV/hacluster/<resource_group>
```

- *RHCS*:

  ```
  rm -rf /var/opt/OV/hacluster/<resource_group>
  ```

10 Unmount the shared disk.

- If you want to reconfigure the NNMi HA cluster at some point, you can keep the disk in its current state.
- If you want to use the shared disk for another purpose, copy all data that you want to keep (as described in Running NNMi with the Existing Database Outside HA on page 330), and then use the HA product commands to unconfigure the disk group and volume group.

Running NNMi with the Existing Database Outside HA

If you want to run NNMi outside HA on any node with the existing database, follow these steps:

1 On the active node (if one still exists), ensure that NNMi is not running:

```
ovstop
```

Alternatively, check the status of the ovspmd process by using Task Manager (Windows) or the ps command (UNIX).

2 On the current node (where you want to run NNMi outside HA), verify that NNMi is not running:

```
ovstop
```

⚠ To prevent data corruption, make sure that no instance of NNMi is running and accessing the shared disk.

3 (UNIX only) Start the disk group:

```
vgchange -a e <disk_group>
```

4 Use the appropriate operating system commands to mount the shared disk. For example:

- *Windows*: Use Windows Explorer.
- *UNIX*: `mount /dev/vgnnm/lvnnm /nnmmount`

5 Copy the NNMi files from the shared disk to the node:

- *Windows*:

  ```
  %NnmInstallDir%\misc\nnm\ha\nnmhadisk.ovpl NNM \
  -from <HA_mount_point>
  ```

- *UNIX*:

  ```
  $NnmInstallDir/misc/nnm/ha/nnmhadisk.ovpl NNM \
  -from <HA_mount_point>
  ```

6 Use the appropriate operating system commands to unmount the shared disk. For example:

- *Windows*: Use Windows Explorer.
- *UNIX*: `umount /nnmmount`

7 (UNIX only) Deactivate the disk group:

```
vgchange -a n <disk_group>
```

8 Obtain and install the permanent production license keys for the physical IP address of this NNMi management server as described in Licensing NNMi on page 117.

9 Start NNMi:

```
ovstart -c
```

NNMi is now running with a copy of the database that was formerly used by the NNMi HA resource group. Manually remove from the NNMi configuration any nodes that you do not want to manage from this NNMi management server.

Patching NNMi under HA

To apply a patch for NNMi, work in HA maintenance mode. Follow these steps:

1 Determine which node in the HA cluster is active:

- *Windows*:

```
%NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl \
-group <resource_group> -activeNode
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl \
-group <resource_group> -activeNode
```

2 On the active node, put the NNMi HA resource group into maintenance mode as described in Putting an HA Resource Group into Maintenance Mode on page 323.

Include the NORESTART keyword.

3 On all passive nodes, put the NNMi HA resource group into maintenance mode as described in Putting an HA Resource Group into Maintenance Mode on page 323.

Include the NORESTART keyword.

4 On the active node, follow these steps:

a Stop NNMi:

```
ovstop -c
```

b Back up the shared disk by performing a disk copy.

c *Optional*. Use the nnmbackup.ovpl command, or another database command, to back up all NNMi data. For example:

```
nnmbackup.ovpl -type offline -scope all -target nnmi_backups
```

For more information about this command, see NNMi Backup and Restore Tools on page 353.

d Apply the appropriate NNMi and NNM iSPI patches to the system.

e Start NNMi:

```
ovstart -c
```

f Verify that NNMi started correctly:

```
ovstatus -c
```

All NNMi services should show the state RUNNING.

5 On each passive node, apply the appropriate patches to the system.

⚠ Never run the ovstart or ovstop commands on a secondary (backup) cluster node.

6 On all passive nodes, take the NNMi HA resource group out of maintenance mode as described in Removing an HA Resource Group from Maintenance Mode on page 323.

7 On the active node, take the NNMi HA resource group out of maintenance mode as described in Removing an HA Resource Group from Maintenance Mode on page 323.

Upgrading NNMi under HA from NNMi 9.0x to NNMi 9.10

Follow the appropriate procedure for your environment:

- Upgrade NNMi with the Embedded Database on the Windows, Linux, or Solaris Operating System on page 332
- Upgrade NNMi with the Embedded Database on the HP-UX Operating System on page 335
- Upgrade NNMi with Oracle on All Supported Operating Systems on page 336

Upgrade NNMi with the Embedded Database on the Windows, Linux, or Solaris Operating System

➤ As of NNMi 9.10, Serviceguard is no longer supported on the Linux operating system. If NNMi is currently running under Serviceguard HA, you cannot follow the procedure in this section. Instead, unconfigure NNMi from HA as described in Unconfiguring NNMi from an HA Cluster on page 327, upgrade NNMi on all nodes, and then configure NNMi to run under a supported HA product as described in Configure NNMi for HA on page 309. Alternatively, you can configure NNMi for NNMi application failover as described in Configuring NNMi in a High Availability Cluster on page 301.

On the Windows, Linux, or Solaris operating system, to upgrade from NNMi 9.0x under HA to NNMi 9.10 under HA, upgrade the passive node, fail over from the active node to the passive node, and then upgrade the second node. Follow these steps:

1 Ensure that the NNMi 9.0x configuration is consistent across all HA nodes by forcing a failover, in turn, to each of the passive nodes.

2 Determine which node in the NNMi 9.0x HA cluster is active:

   - *Windows*:

     ```
     %NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl \
     -group <resource_group> -activeNode
     ```

   - *UNIX*:

     ```
     $NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl \
     -group <resource_group> -activeNode
     ```

   The remainder of this procedure refers to the currently active node as server X and the currently passive node as server Y.

Each resource shown in the cluster manager must use a separate resource monitor:

a Using the cluster manager, right-click each service displayed beneath **Services and applications**.

b Select **Properties**.

c Select **Advanced Policies**.

d Select **Run this resource in a separate Resource Monitor**.

e Click **OK** to save your work.

3 On server Y, upgrade NNMi:

a Disable HA resource group monitoring by creating the following maintenance file:

— *Windows*: `%NnmDataDir%\hacluster\<resource_group>\maintenance`

— *UNIX*: `$NnmDataDir/hacluster/<resource_group>/maintenance`

The file can be empty.

b Upgrade NNMi to the current version as described in Upgrading from NNMi 9.0x on page 401.

c Verify that the upgrade completed without error.

d Upgrade all add-on NNM iSPIs to version 9.10.

To complete an offline upgrade on Network Performance Server (NPS) or NNM iSPI Performance for Metrics HA nodes, unconfigure the node from the HA cluster.

In *addon* mode (where the NNMi management server and the NNM iSPI operate in the same HA cluster), run the following command:
`$NnmInstallDir/misc/nnm/ha/nnmhaunconfigure.ovpl NNM -addon PerfSPIHA`

In *standalone* mode, run the following command
`$NnmInstallDir/misc/nnm/ha/nnmhaunconfigure.ovpl PerfSPIHA`
After this script completes, follow the instructions for upgrading the NPS or NNM iSPI Performance for Metrics in a non-HA environment.

After completing the upgrade, stop all NPS processes; from a newly opened command shell, run the following script:
`$NnmInstallDir/opt/OV/NNMPerformanceSPI/bin/stopALL.ovpl`

‼ When completing step d, do NOT reconfigure HA until after you finish upgrading the primary node.

For more information, see the documentation for each NNM iSPI.

➤ If your environment includes standalone NNM iSPIs, you must also upgrade those products to version 9.10 for correct functionality. You can complete those upgrades after completing this procedure.

4 If the HA cluster includes multiple passive nodes, repeat step 3 for each passive node.

5 On server X, upgrade NNMi:

NNMi will be unavailable for approximately 20 to 60 minutes while the database is upgraded during the failover to server Y. You can schedule this step to occur at a convenient time for system maintenance.

a If you are upgrading NPS or NNM iSPI Performance for Metrics HA nodes, do the following:

- Disable resource group monitoring by creating the following maintenance file:
  Windows: `%NnmDataDir%\hacluster\<`*`resource_group`*`>\maintenance`
  Linux: `$NnmDataDir/hacluster/<`*`resource_group`*`>/maintenance`
  The file can be empty.
- Complete the NPS upgrade
- Enable resource group monitoring by removing the `maintenance` file.

b Force a failover to server Y.

The NNMi database on the shared disk is upgraded to the format of the new NNMi product version at this time.

c Run the following command and view the displayed results. Check that all of the displayed NNMi and ovjboss processes are running without error.

- **`ovstatus -c`**
- **`ovstatus -v ovjboss`**

NNMi might not be fully up since the maintenance file will report the resource <resource group>-APP as being online. To verify that the startup completed successfully, make sure that the `ovstart` process is no longer running.
To do this, use Task Manager on Windows NNMi management servers or run the **`ps -ef | grep ovstart`** command on UNIX NNMi management servers.

If the displayed NNMi and ovjboss processes show errors, check the latest additions to the Release Notes at sg-pro-ovweb.austin.hp.com/nnm/NNM9.10/releasenotesupdate.htm for possible solutions.

d Disable HA resource group monitoring by creating the following maintenance file on server X:

- *Windows*: `%NnmDataDir%\hacluster\<`*`resource_group`*`>\maintenance`
- *UNIX*: `$NnmDataDir/hacluster/<`*`resource_group`*`>/maintenance`

The file can be empty.

e Upgrade NNMi to the current version as described in Upgrading from NNMi 9.0x on page 401.

f Verify that the upgrade completed without error.

g Upgrade all add-on NNM iSPIs to version 9.10. This step does not apply to NNM iSPI Performance for Metrics, as you completed that upgrade in step a on page 334.

For information, see the documentation for each NNM iSPI.

h Delete the maintenance file on server Y:

- *Windows*: `%NnmDataDir%\hacluster\<`*`resource_group`*`>\maintenance`
- *UNIX*: `$NnmDataDir/hacluster/<`*`resource_group`*`>/maintenance`

6 Optional. Complete step b and step c on server X to force a failover from server Y to server X so that the node that was active before the upgrade process is again the active node.

7 Delete the maintenance file on server X:

- *Windows*: `%NnmDataDir%\hacluster\<resource_group>\maintenance`
- *UNIX*: `$NnmDataDir/hacluster/<resource_group>/maintenance`

Upgrade NNMi with the Embedded Database on the HP-UX Operating System

On the HP-UX operating system, upgrading NNMi includes migrating the Postgres database from the 32-bit version to the 64-bit version. For this reason, NNMi must be taken out of operation for the duration of the upgrade process.

NNMi will be unavailable for approximately 30 to 60 minutes during this upgrade procedure.

On the HP-UX operating system, to upgrade from NNMi 9.0x under HA to NNMi 9.10 under HA, upgrade the active node to update the embedded database, and then upgrade the passive node while NNMi is still in maintenance mode. Follow these steps:

1 Ensure that the NNMi 9.0x configuration is consistent across all HA nodes by forcing a failover, in turn, to each of the passive nodes.

2 Ensure that all nodes are running NNMi 9.0x Patch 2 (9.01) or a higher version of NNMi 9.0x.

If necessary, upgrade each system to the latest NNMi 9.0x consolidated patch. Follow the instructions in the “Upgrading NNMi under HA from NNMi 8.1x to NNMi 9.01” section of the “Configuring NNMi in a High Availability Cluster” chapter in the most recent NNMi 9.0x version of the *NNMi Deployment Reference*.

3 Determine which node in the NNMi 9.0x HA cluster is active:

```
$NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl \
-group <resource_group> -activeNode
```

The remainder of this procedure refers to the currently active node as server X and the currently passive node as server Y.

4 On server X, disable HA resource group monitoring by creating the following maintenance file:

```
$NnmDataDir/hacluster/<resource_group>/maintenance
```

The file can be empty.

5 On server X, upgrade NNMi:

a Upgrade NNMi to the current version as described in Upgrading from NNMi 9.0x on page 401.

The database upgrade occurs during this step.

b To verify that the upgrade completed correctly, enter the following command:

```
ovstart
```

All NNMi services should show the state RUNNING.

c. Upgrade all add-on NNM iSPIs to version 9.10.

   For information, see the documentation for each NNM iSPI.

   ➤ If your environment includes standalone NNM iSPIs, you must also upgrade those products to version 9.10 for correct functionality. You can complete those upgrades after completing this procedure.

6. On server Y, upgrade NNMi:

   a. Upgrade NNMi to the current version as described in Upgrading from NNMi 9.0x on page 401.

   b. Verify that the upgrade completed without error.

   c. Upgrade all add-on NNM iSPIs to version 9.10.

      For information, see the documentation for each NNM iSPI.

7. If the HA cluster includes multiple passive nodes, repeat step 6 for each passive node.

8. On server X, delete the maintenance file:

```
$NnmDataDir/hacluster/<resource_group>/maintenance
```

Upgrade NNMi with Oracle on All Supported Operating Systems

To upgrade NNMi for HA in an Oracle environment, follow the procedure described in Upgrade NNMi with the Embedded Database on the Windows, Linux, or Solaris Operating System on page 332.

Troubleshooting the HA Configuration

This section includes the following topics:

Common Configuration Mistakes

Some common HA configuration mistakes are listed here:

- Incorrect disk configuration
  - VCS: If a resource cannot be probed, the configuration is somehow wrong. If a disk cannot be probed, the disk might no longer be accessible by the operating system.
  - Test the disk configuration manually and confirm against HA documentation that the configuration is appropriate.
- The disk is in use and cannot be started for the HA resource group.

  Always check that the disk is not activated before starting the HA resource group.
- MSFC: Bad network configuration

  If network traffic is flowing across multiple NIC cards, RDP sessions fail when activating programs that consume a large amount of network bandwidth, such as the NNMi ovjboss process.
- Some HA products do not automatically restart at boot time.

  Review the HA product documentation for information about how to configure automatic restart on boot up.
- Adding NFS or other access to the OS directly (resource group configuration should be managing this).
- Being in the shared disk mount point during a failover or offlining of the HA resource group.

  HA kills any processes that prevent the shared disk from being unmounted.
- Reusing the HA cluster virtual IP address as the HA resource virtual IP address (works on one system and not the other)
- Timeouts are too short. If the products are misbehaving, HA product might time out the HA resource and cause a failover.

  MSFC: In Failover Cluster Management, check the value of the **Time to wait for resource to start** setting. NNMi sets this value to 15 minutes. You can increase the value.

- Not using maintenance mode

  Maintenance mode was created for debugging HA failures. If you attempt to bring a resource group online on a system, and it fails over shortly afterwards, use the maintenance mode to keep the resource group online to see what is failing.

- Not reviewing cluster logs (cluster logs can show many common mistakes).

HA Resource Testing

This section describes the general approach for testing the resources that you will place into the NNMi HA resource group. This testing identifies hardware configuration problems. It is recommended to perform this testing *before* configuring NNMi to run under HA. Note the configuration values that generate positive results, and use these value when performing the complete configuration of the NNMi HA resource group.

For specific details regarding any of the commands listed here, see the most recent documentation for your HA product.

To test HA resources, follow these steps:

1. If necessary, start the HA cluster.
2. (Windows only) Verify that the following virtual IP addresses have been defined for the HA cluster:
   - A virtual IP address for the HA cluster
   - A virtual IP address for each HA resource group

   Each of these IP addresses should not be used elsewhere.
3. Add an HA resource group to the HA cluster.

   Use a non-production name, such as `test`, for this HA resource group.
4. Test the connection to the HA resource group:

   a. Add the virtual IP address and corresponding virtual hostname for the resource group as a resource to the HA resource group.

      Use the values that you will later associate with the NNMi HA resource group.

   b. Fail over from the active cluster node to the passive cluster node to verify that the HA cluster correctly fails over.

   c. Fail over from the new active cluster node to the new passive cluster node to verify failback.

   d. If the resource group does not fail over correctly, log on to the active node, and then verify that the IP address is properly configured and accessible. Also verify that no firewall blocks the IP address.v
5. Configure the shared disk as described in Configuring a SAN or a Physically Connected Disk on page 320.
6. Test the connection to the shared disk:

   a. Add the shared disk as a resource to the HA resource group as described in Moving the Shared Disk into the NNMi HA Resource Group on page 321.

   b. Fail over from the active cluster node to the passive cluster node to verify that the HA cluster correctly fails over.

c. Fail over from the new active cluster node to the new passive cluster node to verify failback.

d. If the resource group does not fail over correctly, log on to the active node, and then verify that the disk is mounted and available.

7. Keep a record of the commands and inputs that you used to configure the shared disk. You might need this information when configuring the NNMi HA resource group.

8. Remove the resource group from each node:

   a. Remove the IP address entry.

   b. Offline the resource group, and then remove resource group from the node.

   At this point, you can use the NNMi-provided tools to configure NNMi to run under HA.

General HA Troubleshooting

The topics in this section apply to HA configuration for NNMi and the NNM iSPIs. They include:

- Error: Wrong Number of Arguments
- Resource Hosting Subsystem Process Stops Unexpectedly (Windows Server 2008 R2)
- Product Startup Times Out (Solaris)
- Log Files on the Active Cluster Node Are Not Updating
- Cannot Start the NNMi HA Resource Group on a Particular Cluster Node

Error: Wrong Number of Arguments

The name of the product Perl module is a required parameter to most of the NNMi HA configuration commands.

- For NNMi, use the value `NNM`.
- To determine what value to use for an NNM iSPI, see the documentation for that NNM iSPI.

Resource Hosting Subsystem Process Stops Unexpectedly (Windows Server 2008 R2)

Starting an HA cluster resource on a computer running the Windows Server 2008 R2 operating system stops the Resource Hosting Subsystem (`Rhs.exe`) process unexpectedly.

For information about this known problem, see the Microsoft Support web site article *The Resource Hosting Subsystem (Rhs.exe) process stops unexpectedly when you start a cluster resource in Windows Server 2008 R2*, which is available from **http://support.microsoft.com/kb/978527**.

Always run the NNMi resource in a separate resource monitor (rhs.exe) specific to the resource group.

Product Startup Times Out (Solaris)

One or more of the /var/adm/messages* files contains a message similar to the following example:

```
VCS ERROR V-16-1-13012 Thread(…) Resource(<resource group>-app):
online procedure did not complete within the expected time.
```

This message indicates that the product did not start completely within the Veritas timeout value. The NNMi-provided HA configuration scripts define this timeout to be 15 minutes.

To change the Veritas timeout value on the Solaris operating system, run the following commands in order:

```
/opt/VRTSvcs/bin/haconf -makerw
/opt/VRTSvcs/bin/hares -modify <resource_group>-app OnlineTimeout <value in seconds>
/opt/VRTSvcs/bin/haconf -dump -makero
```

Log Files on the Active Cluster Node Are Not Updating

This situation is normal. It occurs because the log files have been redirected to the shared disk.

For NNMi, review the log files in the location specified by HA_NNM_LOG_DIR in the ov.conf file.

Cannot Start the NNMi HA Resource Group on a Particular Cluster Node

If the nnmhastartrg.ovpl or nnmhastartrg.ovpl command does not correctly start, stop, or switch the NNMi HA resource group, review the following information:

- *MSFC*:
  - In Failover Cluster Management, review the state of the NNMi HA resource group and underlying resources.
  - Review the Event Viewer log for any errors.
- *Serviceguard:*

  Review the *<resource_group>*.cntl.log file and the syslog files for errors. The most common problems are leaving the system in a state where a resource cannot be added, for example, having a disk group misconfigured such that it cannot be activated.

  /etc/cmcluster/*<resource_group>*/*<resource_group>*.cntl.log
- *VCS*:
  - Run **/opt/VRTSvcs/bin/hares -state** to review the resource state.
  - For failed resources, review the /var/VRTSvcs/log/*<resource>*.log file for the resource that is failing. Resources are referenced by the agent type, for example: IP*.log, Mount*.log, and Volume*.log.
- *RHCS:*

  Review the *<resource_group>*.cntl.log file and the syslog files for errors. The most common problems are leaving the system in a state where a resource cannot be added, for example, having a disk group misconfigured such that it cannot be activated.

  /etc/cmcluster/*<resource_group>*/*<resource_group>*.cntl.log

If you cannot locate the source of the problem, you can manually start the NNMi HA resource group by using the HA product commands:

1 Mount the shared disk.

2 Assign the virtual host to the network interface:

- *MSF*:
    - — Start Failover Cluster Management.
    - — Expand the resource group.
    - — Right-click ***<resource_group>*-ip**, and then click **Bring Online**.
- *Serviceguard:* Run `/usr/sbin/cmmodnet` to add the IP address.
- *VCS*: **`/opt/VRTSvcs/bin/hares -online <resource_group>-ip \ -sys <local_hostname>`**
- *RHCS:* Run `/usr/sbin/cmmodnet` to add the IP address.

3 Start the NNMi HA resource group. For example:

- *Windows*:

```
%NnmInstallDir%\misc\nnm\ha\nnmhastartrg.ovpl NNM \
-start <resource_group>
```

- *UNIX*:

```
$NnmInstallDir/misc/nnm/ha/nnmhastartrg.ovpl NNM \
-start <resource_group>
```

The return code `0` indicates that NNMi started successfully.

The return code `1` indicates that NNMi did not start correctly.

NNMi-Specific HA Troubleshooting

The topics in this section apply to HA configuration for NNMi only. They include:

- Re-Enable NNMi for HA after All Cluster Nodes are Unconfigured
- NNMi Does Not Start Correctly Under HA
- Changes to NNMi Data are Not Seen after Failover
- nmsdbmgr Does Not Start after HA Configuration
- pmd Does Not Start after HA Configuration
- NNMi Runs Correctly on Only One HA Cluster Node (Windows)
- Disk Failover Does Not Occur
- Shared Disk is Not Accessible (Windows)
- Shared Disk Does Not Contain Current Data
- Shared Disk Files Are Not Found by the Secondary Node after Failover

Re-Enable NNMi for HA after All Cluster Nodes are Unconfigured

When all NNMi HA cluster nodes have been unconfigured, the `ov.conf` file no longer contains any mount point references to the NNMi shared disk. To re-create the mount point reference without overwriting the data on the shared disk, follow these steps on the primary node:

1. If NNMi is running, stop it:

   ```
   ovstop -c
   ```

2. Reset the reference to the shared disk:

   - *Windows*:

     ```
     %NnmInstallDir%\misc\nnm\ha\nnmhadisk.ovpl NNM \
     -setmount <HA_mount_point>
     ```

   - *UNIX*:

     ```
     $NnmInstallDir/misc/nnm/ha/nnmhadisk.ovpl NNM \
     -setmount <HA_mount_point>
     ```

3. In the `ov.conf` file, verify the entries related to HA mount points.

   For the location of the `ov.conf` file, see NNMi HA Configuration Files on page 347.

NNMi Does Not Start Correctly Under HA

When NNMi does not start correctly, it is necessary to debug whether the issue is a hardware issue with the virtual IP address or the disk, or whether the issue is some form of application failure. During this debug process, put the system in maintenance mode *without* the `NORESTART` keyword.

1. On the active node in the HA cluster, disable HA resource group monitoring by creating the following maintenance file:

   - *Windows*: `%NnmDataDir%\hacluster\`*`<resource_group>`*`\maintenance`
   - *UNIX*: `$NnmDataDir/hacluster/`*`<resource_group>`*`/maintenance`

2. Start NNMi:

   ```
   ovstart
   ```

3. Verify that NNMi started correctly:

   ```
   ovstatus -c
   ```

   All NNMi services should show the state RUNNING. If this is not the case, troubleshoot the process that does not start correctly.

4. After completing your troubleshooting, delete the maintenance file:

   - *Windows*: `%NnmDataDir%\hacluster\`*`<resource_group>`*`\maintenance`
   - *UNIX*: `$NnmDataDir/hacluster/`*`<resource_group>`*`/maintenance`

Changes to NNMi Data are Not Seen after Failover

The NNMi configuration points to a different system than where NNMi is running. To fix the problem, verify that the `ov.conf` file has appropriate entries for the following items:

- `NNM_INTERFACE=<virtual_hostname>`
- `HA_RESOURCE_GROUP=<resource_group>`
- `HA_MOUNT_POINT=<HA_mount_point>`
- `NNM_HA_CONFIGURED=YES`
- `HA_POSTGRES_DIR=<HA_mount_point>/NNM/dataDir/shared/nnm/databases/Postgres`
- `HA_EVENTDB_DIR=<HA_mount_point>/NNM/dataDir/shared/nnm/eventdb`
- `HA_CUSTOMPOLLER_DIR=<HA_mount_point>/NNM/dataDir/shared/nnm/databases/custompoller`
- `HA_NNM_LOG_DIR=<HA_mount_point>/NNM/dataDir/log`
- `HA_JBOSS_DATA_DIR=<HA_mount_point>/NNM/installDir/nonOV/jboss/nms/server/nms/data`
- `HA_LOCALE=C`

For the location of the `ov.conf` file, see NNMi HA Configuration Files on page 347.

nmsdbmgr Does Not Start after HA Configuration

This situation usually occurs as a result of starting NNMi after running the `nnmhaconfigure.ovpl` command but without the `nnmhadisk.ovpl` command with the `-to` option having been run. In this case, the `HA_POSTGRES_DIR` entry in the `ov.conf` file specifies the location of the embedded database on the shared disk, but this location is not available to NNMi.

To fix this problem, follow these steps:

1. On the active node in the HA cluster, disable HA resource group monitoring by creating the following maintenance file:
   - *Windows*: `%NnmDataDir%\hacluster\<resource_group>\maintenance`
   - *UNIX*: `$NnmDataDir/hacluster/<resource_group>/maintenance`
2. Copy the NNMi database to the shared disk:
   - *Windows*:

     ```
     %NnmInstallDir%\misc\nnm\ha\nnmhadisk.ovpl NNM \
     -to <HA_mount_point>
     ```
   - *UNIX*:

     ```
     $NnmInstallDir/misc/nnm/ha/nnmhadisk.ovpl NNM \
     -to <HA_mount_point>
     ```

   ⚠ To prevent database corruption, run this command (with the `-to` option) only one time. For information about alternatives, see Re-Enable NNMi for HA after All Cluster Nodes are Unconfigured on page 342.

3 Start the NNMi HA resource group:

- *Windows*:

  ```
  %NnmInstallDir%\misc\nnm\ha\nnmhastartrg.ovpl NNM \
  <resource_group>
  ```

- *UNIX*:

  ```
  $NnmInstallDir/misc/nnm/ha/nnmhastartrg.ovpl NNM \
  <resource_group>
  ```

4 Start NNMi:

```
ovstart
```

5 Verify that NNMi started correctly:

```
ovstatus -c
```

All NNMi services should show the state RUNNING.

6 After completing your troubleshooting, delete the maintenance file:

- *Windows*: `%NnmDataDir%\hacluster\<resource_group>\maintenance`
- *UNIX*: `$NnmDataDir/hacluster/<resource_group>/maintenance`

pmd Does Not Start after HA Configuration

This situation usually occurs after a configuration error such as not setting up the shared disk correctly. The failure of the `pmd` process occurs when the `ovjboss` process does not fully start.

Review the following log file:

- *Windows*: `%HA_MOUNT_POINT%\NNM\dataDir\log\nnm\jbossServer.log`
- *UNIX*: `$HA_MOUNT_POINT/NNM/dataDir/log/nnm/jbossServer.log`

NNMi Runs Correctly on Only One HA Cluster Node (Windows)

The Windows operating system requires two different virtual IP addresses, one for the HA cluster and one for the HA resource group. If the virtual IP address of the HA cluster is the same as that of the NNMi HA resource group, NNMi only runs correctly on the node associated with the HA cluster IP address.

To correct this problem, change the virtual IP address of the HA cluster to a unique value for the network.

Disk Failover Does Not Occur

This situation can happen when the operating system does not support the shared disk. Review the HA product, operating system, and disk manufacturer documentation to determine whether these products can all work together.

If disk failure occurs, NNMi does not start on failover. Most likely, `nmsdbmgr` fails because the `HA_POSTGRES_DIR` directory does not exist. Verify that the shared disk is mounted and that the appropriate files are accessible.

Shared Disk is Not Accessible (Windows)

The command `nnmhaclusterinfo.ovpl -config NNM -get HA_MOUNT_POINT` returns nothing.

The drive of the shared disk mount point must be fully specified (for example, `S:\`) during HA configuration.

To correct this problem, run the `nnmhaconfigure.ovpl` command an each node in the HA cluster. Fully specify the drive of the shared disk mount point.

Shared Disk Does Not Contain Current Data

Responding to the `nnmhaconfigure.ovpl` command question about disk type with the text none bypasses the code for setting the disk-related variables in the `ov.conf` file. To fix this situation, follow the procedure in Prepare the Shared Disk Manually on page 319.

Shared Disk Files Are Not Found by the Secondary Node after Failover

The most common cause of this situation is that the `nnmhadisk.ovpl` command was run with the `-to` option when the shared disk was not mounted. In this case, the data files are copied to the local disk, so the files are not available on the shared disk.

To fix this problem, follow these steps:

1. On the active node in the HA cluster, disable HA resource group monitoring by creating the following maintenance file:
   - *Windows*: `%NnmDataDir%\hacluster\`*`<resource_group>`*`\maintenance`
   - *UNIX*: `$NnmDataDir/hacluster/`*`<resource_group>`*`/maintenance`
2. Log on to the active node, and then verify that the disk is mounted and available.
3. Stop NNMi:

   ```
   ovstop
   ```

4. Copy the NNMi database to the shared disk:
   - *Windows*:

     ```
     %NnmInstallDir%\misc\nnm\ha\nnmhadisk.ovpl NNM \
     -to <HA_mount_point>
     ```

   - *UNIX*:

     ```
     $NnmInstallDir/misc/nnm/ha/nnmhadisk.ovpl NNM \
     -to <HA_mount_point>
     ```

⚠ To prevent database corruption, run this command (with the `-to` option) only one time. For information about alternatives, see Re-Enable NNMi for HA after All Cluster Nodes are Unconfigured on page 342.

5 Start the NNMi HA resource group:

- *Windows*:

  ```
  %NnmInstallDir%\misc\nnm\ha\nnmhastartrg.ovpl NNM \
  <resource_group>
  ```

- *UNIX*:

  ```
  $NnmInstallDir/misc/nnm/ha/nnmhastartrg.ovpl NNM \
  <resource_group>
  ```

6 Start NNMi:

```
ovstart
```

7 Verify that NNMi started correctly:

```
ovstatus -c
```

All NNMi services should show the state RUNNING.

8 After completing your troubleshooting, delete the maintenance file:

- *Windows*: `%NnmDataDir%\hacluster\<resource_group>\maintenance`
- *UNIX*: `$NnmDataDir/hacluster/<resource_group>/maintenance`

NNM iSPI-Specific HA Troubleshooting

For information about troubleshooting an NNM iSPI running under HA, see the documentation for that NNM iSPI.

HA Configuration Reference

NNMi HA Configuration Files

Table 26 lists the NNMi HA configuration files. These files apply to NNMi and add-on NNM iSPIs on the NNMi management server. These files are installed to the following location:

- *Windows*: `%NnmDataDir%\shared\nnm\conf`
- *UNIX*: `$NnmDataDir/shared/nnm/conf`

Table 26 NNMi HA Configuration Files

File Name	Description
ov.conf	Updated by the `nnmhaclusterinfo.ovpl` command to describe the NNMi HA implementation. NNMi processes read this file to determine the HA configuration.
nnmdatareplicator.conf	Used by the `nnmdatareplicator.ovpl` command to determine which NNMi folders and files are included in data replication from the active node to the passive nodes. If you implement a different method of replicating the NNMi configuration, see this file for a list of the data to include. For more information, see the comments in the file.

NNMi-Provided HA Configuration Scripts

Table 27 and Table 28 list the HA configuration scripts that are included with NNMi. The NNMi-provided scripts listed in Table 27 are convenience scripts that can be used to configure HA for any product that has a customer Perl module. If you prefer, you can use the HA product-provided commands to configure HA for NNMi.

On the NNMi management server, the NNMi-provided HA configuration scripts are installed to the following location:

- *Windows*: `%NnmInstallDir%\misc\nnm\ha`
- *UNIX*: `$NnmInstallDir/misc/nnm/ha`

Table 27 NNMi HA Configuration Scripts

Script Name	Description
nnmhaconfigure.ovpl	Configures NNMi or an NNM iSPI for an HA cluster. Run this script on all nodes in the HA cluster.
nnmhaunconfigure.ovpl	Unconfigures NNMi or an NNM iSPI from an HA cluster. Optionally, run this script on one or more nodes in the HA cluster.
nnmhaclusterinfo.ovpl	Retrieves cluster information regarding NNMi. Run this script as needed on any node in the HA cluster.

Table 27 NNMi HA Configuration Scripts (cont'd)

Script Name	Description
nnmhadisk.ovpl	Copies NNMi and NNM iSPI data files to and from the shared disk. During HA configuration, run this script on the primary node. At other times, run this script per the instructions in this chapter.
nnmhastartrg.ovpl	Starts the NNMi HA resource group in an HA cluster. During HA configuration, run this script on the primary node.
nnmhastoprg.ovpl	Stops the NNMi HA resource group in an HA cluster. During HA unconfiguration, run this script on the primary node.

The NNMi-provided scripts listed in Table 28 are used by the scripts listed in Table 27 on page 347. Do not run the scripts listed in Table 28 directly.

Table 28 NNMi HA Support Scripts

Script Name	Description
nnmdatareplicator.ovpl	Checks the `nnmdatareplicator.conf` configuration file for changes and copies files to remote systems.
nnmharg.ovpl	Starts, stops, and monitors NNMi in an HA cluster. For Serviceguard configurations, used by `<`*`resource_group`*`>.cntl`. For VCS configurations, used by the VCS start, stop, and monitor scripts. (`nnmhargconfigure.ovpl` configures this usage.) Also used by `nnmhastartrg.ovpl` to enable and disable tracing.
nnmhargconfigure.ovpl	Configures HA resources and resource groups. Used by `nnmhaconfigure.ovpl` and `nnmhaunconfigure.ovpl`.
nnmhastart.ovpl	Starts NNMi in an HA cluster. Used by `nnmharg.ovpl`.
nnmhastop.ovpl	Stops NNMi in an HA cluster. Used by `nnmharg.ovpl`.
nnmhamonitor.ovpl	Monitors NNMi processes in an HA cluster. Used by `nnmharg.ovpl`.
nnmhamscs.vbs	Is a template for creating a script to start, stop, and monitor NNMi processes in a MSFC HA cluster. The generated script is used by MSFC and is stored in the following location: `%NnmDataDir%\hacluster\<`*`resource_group`*`>\hamscs.vbs`

NNMi HA Configuration Log Files

The following log files apply to the HA configuration for NNMi and add-on NNM iSPIs on the NNMi management server:

- *Windows* configuration:
  - `%NnmDataDir%\tmp\HA_nnmhaserver.log`
  - `%NnmDataDir%\log\haconfigure.log`
- *UNIX* configuration:
  - `$NnmDataDir/tmp/HA_nnmhaserver.log`
  - `$NnmDataDir/log/haconfigure.log`
- *Windows* runtime:
  - Event Viewer log
  - `%HA_MOUNT_POINT%\NNM\dataDir\log\nnm\ovspmd.log`
  - `%HA_MOUNT_POINT%\NNM\dataDir\log\nnm\public\postgres.log`
  - `%HA_MOUNT_POINT%\NNM\dataDir\log\nnm\public\nmsdbmgr.log`
  - `%HA_MOUNT_POINT%\NNM\dataDir\log\nnm\jbossServer.log`
  - `%SystemRoot%\Cluster\cluster.log`
    This is the log file for cluster runtime issues including: adding and removing resources and resource groups; other configuration issues; starting and stopping issues.
- *HP-UX* runtime:
  - `/etc/cmcluster/`*`<resource_group>`*`/`*`<resource_group>`*`.cntl.log`
    This is the log file for the resource group.
  - `/var/adm/syslog/syslog.log`
  - `/var/adm/syslog/OLDsyslog.log`
  - `$HA_MOUNT_POINT/NNM/dataDir/log/nnm/ovspmd.log`
  - `$HA_MOUNT_POINT/NNM/dataDir/log/nnm/public/postgres.log`
  - `$HA_MOUNT_POINT/NNM/dataDir/log/nnm/public/nmsdbmgr.log`
  - `$HA_MOUNT_POINT/NNM/dataDir/log/nnm/jbossServer.log`

- *Linux or Solaris* runtime for VCS:

Table 29 Linux or Solaris Runtime for VCS

Resource	Log File
<resource_group>-app	• /var/VRTSvcs/log/Application_A.log • $HA_MOUNT_POINT/NNM/dataDir/log/nnm/ovspmd.log • $HA_MOUNT_POINT/NNM/dataDir/log/nnm/public/postgres.log • $HA_MOUNT_POINT/NNM/dataDir/log/nnm/public/nmsdbmgr.log • $HA_MOUNT_POINT/NNM/dataDir/log/nnm/jbossServer.log • /var/adm/messages*
<resource_group>-dg *<resource_group>*-volume *<resource_group>*-mount	• /var/VRTSvcs/log/DiskGroup_A.log • /var/VRTSvcs/log/Volume_A.log • /var/VRTSvcs/log/Mount_A.log • /var/adm/messages*
<resource_group>-ip	• /var/VRTSvcs/log/IP_A.log • /var/adm/messages*
For operating system-specific issues related to the HA resources, review the /var/adm/messages* files. For *<resource_group>*-app, look for messages regarding unable to start process.	

- *Linux* runtime for RCHS:
  - /var/adm/syslog/syslog.log
  - $HA_MOUNT_POINT/NNM/dataDir/log/nnm/ovspmd.log
  - $HA_MOUNT_POINT/NNM/dataDir/log/nnm/public/postgres.log
  - $HA_MOUNT_POINT/NNM/dataDir/log/nnm/public/nmsdbmgr.log
  - $HA_MOUNT_POINT/NNM/dataDir/log/nnm/jbossServer.log

Maintaining NNMi

This section contains the following chapters:

NNMi Backup and Restore Tools

A good backup and restore strategy is key to ensuring the uninterrupted operations of any business. HP Network Node Manager i Software (NNMi) is an important asset for network operations and should be backed up regularly.

The two types of critical data related to an NNMi installation are as follows:

- Files in the file system
- Data in the relational database (embedded or external)

This chapter explains the tools that NNMi provides for backing up and restoring important NNMi files and data.

This chapter contains the following topics:

- Backup and Restore Commands
- Backing up NNMi Data
- Same System Restore
- Backup and Restore Strategies
- Backing up and Restoring the Embedded Database Only

Backup and Restore Commands

NNMi provides the following scripts for backing up and restoring NNMi data:

- nnmbackup.ovpl—Backs up all necessary file system data (including configuration information) and any data stored in the NNMi embedded database.
- nnmrestore.ovpl—Restores a backup that was created by using the nnmbackup.ovpl script.
- nnmbackupembdb.ovpl—Creates a complete backup of the NNMi embedded database (but not the file system data) while NNMi is running.
- nnmrestoreembdb.ovpl—Restores a backup that was created by using the nnmbackupembdb.ovpl script.
- nnmresetembdb.ovpl—Drops the NNMi embedded database tables. Run the ovstart command to recreated the tables.

For command syntax, see the appropriate reference page, or the UNIX manpage.

Backing up NNMi Data

The NNMi backup command (nnmbackup.ovpl) copies key NNMi file system data and some or all of the tables in the NNMi Postgres database to the specified target directory. The NNMi backup command can create a tar archive of the backup data, or you can compress the backup files using your own tools. You can then use any appropriate tool to save a copy of the backup.

⚑ If your NNMi implementation uses Oracle for the main NNMi database, the NNMi backup and restore commands work with the NNMi file system data only. External database maintenance should be handled as part of the existing database backup and restore procedures.

The back up and restore data might or might not include data from any NNM iSPIs installed in your network environment. Check the documentation that came with each NNM iSPI for details.

⚠ Any software that locks files (for example, anti-virus or system backup software), can interrupt NNMi access to the NNMi database. This can cause problems such as an inability to read from or write to a file that is being used by another process, such as an anti-virus application. For the NNMi Postgres database, configure these applications to exclude the NNMi database directory (%NNM_DB% and Windows, $NNM_DB on UNIX). Use nnmbackup.ovpl to back up the NNMi database regularly.

Backup Type

The NNMi backup command supports two types of backups:

- Online backups occur while NNMi is running. NNMi ensures that the database tables are synchronized in the backed up data. Operators can be actively using the NNMi console and other processes can be interacting with the NNMi database during an online backup. With an online backup, you can back up all NNMi data or only some of the data according to function, as described in Backup Scope. For the embedded NNMi database, the `nmsdbmgr` service must be running. For an external database, the backup includes NNMi file system data. NNMi processes do not have to be running to back up an external database.

- Offline backups occur while NNMi is completely stopped. With an offline backup, the backup scope applies to the file system files only. An offline backup always includes the complete NNMi database regardless of the backup scope. For the embedded NNMi database, the backup copies the Postgres database files. For an external database, the backup includes NNMi file system data only.

Backup Scope

The NNMi backup command provides several scopes that define how much NNMi is backed up.

Configuration scope

The configuration scope (`-scope config`) loosely aligns to the information in the **Configuration** workspace of the NNMi console.

The configuration scope includes the following data:

- For online backups, only those embedded database tables that store NNMi configuration information.
- For offline backups, the entire embedded database.
- For all backups, the NNMi configuration information in the file system as listed in Table 30.

Topology scope

The topology scope (`-scope topology`) loosely aligns to the information in the **Inventory** workspace of the NNMi console. Because the network topology is dependent on the configuration that was used for discovering that topology, the topology scope includes the configuration scope.

The topology scope includes the following data:

- For online backups, only those embedded database tables that store NNMi configuration and network topology information.
- For offline backups, the entire embedded database.
- For all backups, the NNMi configuration information in the file system as listed in Table 30. Currently, there are no file system files associated with the topology scope.

Event scope

The event scope (`-scope event`) loosely aligns to the information in the **Incident Browsing** workspace of the NNMi console. Because events are dependent on the network topology related to those events, the event scope includes the configuration and topology scopes.

The event scope includes the following data:

- For online backups, only those embedded database tables that store NNMi configuration, network topology, and event information.
- For offline backups, the entire embedded database.
- For all backups, the NNMi configuration information in the file system as listed in Table 30 and the NNMi event information as listed in Table 31.

All scope

The complete backup (`-scope all`) includes all important NNMi files and the complete embedded database.

Table 30 Configuration Scope Files and Directories

Directory or File name	Description
`%NnmInstallDir%/conf` (Windows only)	Configuration information
`%NnmInstallDir%\misc\nms\lic` `$NnmInstallDir/misc/nms/lic`	Miscellaneous license information
`%NnmInstallDi%r\nonOV\jboss\nms\server\nms\conf` `$NnmInstallDir/nonOV/jboss/nms/server/nms/conf`	jboss configuration
`%NnmDataDir%\conf` `$NnmDataDir/conf`	Configuration that might be shared by other HP products
`%NnmDataDir%\conf\nnm\props` `$NnmDataDir/conf/nnm/props`	Local NNMi configuration properties files
• *Windows Server 2008*: *<drive>*`:\ProgramData\Hewlett-Packard\HPOvLIC\data\LicFile.txt` • *UNIX*: `$NnmDataDir/HPOvLIC/LicFile.txt`	License information
`%NnmDataDir%\NNMVersionInfo` `$NnmDataDir/NNMVersionInfo`	NNMi version information file
`%NnmDataDir%\shared\nnm\user-snmp-mibs` `$NnmDataDir/shared/nnm/user-snmp-mibs`	Shared user-added SNMP MIB information
`%NnmDataDir%\shared\nnm\actions` `$NnmDataDir/shared/nnm/actions`	Shared lifecycle transition actions
`%NnmDataDir%\shared\nnm\certificates` `$NnmDataDir/shared/nnm/certificates`	Shared NNMi SSL certificates
`%NnmDataDir%\shared\nnm\conf` `$NnmDataDir/shared/nnm/conf`	Shared NNMi configuration information
`%NnmDataDir%\shared\nnm\conf\licensing` `$NnmDataDir/shared/nnm/conf/licensing`	Shared NNMi license configuration information
`%NnmDataDir%\shared\nnm\lrf` `$NnmDataDir/shared/nnm/lrf`	Shared NNMi component registration files
`%NnmDataDir%\shared\nnm\conf\props` `$NnmDataDir/shared/nnm/conf/props`	Shared NNMi configuration properties files
`%NnmDataDir%\shared\nnm\www\htdocs\images` `$NnmDataDir/shared/nnm/www/htdocs/images`	Shared background images for NNMi node group maps

In this context, files in the shared directories are those shared with another NNMi management server in an NNMi application failover or high availability environment.

Table 31 Event Scope Files and Directories

Directory or File name	Description
$NnmDataDir/log/nnm/signin.0.0.log	NNMi console sign-in log

Restoring NNMi Data

The NNMi restore script (`nnmrestore.ovpl`) places the backup data on the NNMi management server. The type and scope of the backup determines what NNMi can restore.

➤ If you use the `nnmrestore.ovpl` script to place database records on a second NNMi management server, both NNMi management servers must have the same type of operating system and NNMi version and patch level.

Placing the backup data from one NNMi management server onto a second NNMi management server means that both servers have the same database UUID. After you restore NNMi on the second NNMi management server, uninstall NNMi from the original NNMi management server.

- To restore an online backup, NNMi copies the file system data to the correct locations and overwrites the contents of the database tables that were included in the backup. Objects that have been deleted since the backup are restored, and objects that have been created since the backup are deleted. Additionally, any objects that were changed after the backup was taken revert to their state at the time of the backup. For the embedded NNMi database, the `nmsdbmgr` service must be running. For an external database, the restore includes NNMi file system data only and no NNMi processes must be running.
- To restore an offline backup, NNMi overwrites the Postgres files in the file system, completely replacing the database files with the contents of the backup. For an external database, the backup includes NNMi file system data only.

With the `-force` option, the `nnmrestore.ovpl` command stops all NNMi processes, starts the `nmsdbmgr` service (if restoring from an online backup of the NNMi embedded database), restores the data, and then restarts all NNMi processes.

If the provided source is a tar file, the NNMi restore command extracts the tar file to a temporary folder in the current working directory. In this case, either ensure that the current working directory has adequate storage to support the temporary folder, or extract the archive before running the restore command.

➤ Because the database schema might change from one version of NNMi to the next, data backups cannot be shared across versions of NNMi.

Same System Restore

You can use the backup and restore commands on a single system for data recovery. The following items must not have changed between the time of the backup and time of the restore:

- NNMi version (including any patches)
- Operating system type
- Character set (language)
- Hostname
- Domain

Different System Restore

You can use the backup and restore commands to transfer data from one NNMi management server to another. The intended uses of different system restoration include recovering from system failure and transferring NNMi to a different system during an operating system upgrade.

Best practice

Because the NNMi UUID is copied to the target system during the database restore, both source and target systems now appear to be running the same instance of NNMi. Uninstall NNMi from the source system.

To create multiple functional NNMi management servers with similar configurations, such as while deploying global network management, use the `nnmconfigexport.ovpl` and `nnmconfigimport.ovpl` commands.

For a different system restore, the following items must be identical on both systems:

- NNMi version (including any patches)
- Operating system type and version
- Character set (language)

The following items can differ between the two systems:

- Hostname
- Domain

For a different system restore, the `nnmrestore.ovpl` command does not copy the license information to the new system. Obtain and apply a new license for the new NNMi management server. For more information, see Licensing NNMi on page 117.

Backup and Restore Strategies

Back up All Data Periodically

Your disaster recovery plan should include a regularly scheduled complete backup of all NNMi data. You do not need to shut down NNMi to create this backup. If you incorporate the backup into a script, use the `-force` option to ensure that NNMi is on the correct state before the backup begins. For example:

```
nnmbackup.ovpl -force -type online -scope all -archive
  -target nnmi_backups\periodic
```

To recover your NNMi data after a hardware failure, follow these steps:

1 Rebuild or acquire new hardware.

2 Install NNMi to the same version and patch level as were in place for the backup.

3 Restore the NNMi data:

- If the recovery NNMi management server meets the requirements listed in Same System Restore on page 358, run a command similar to the following example:

  ```
  nnmrestore.ovpl -force -lic
  -source nnmi_backups\periodic\newest_backup
  ```

- If the recovery NNMi management server does not qualify for a same-system restore but meets the requirements listed in Different System Restore on page 358, run a command similar to the following example:

  ```
  nnmrestore.ovpl -force
    -source nnmi_backups\periodic\newest_backup
  ```

  Update the licensing as needed.

Back up Data Before Changing the Configuration

Perform scoped backups (as described in Backup Scope on page 355) as needed before beginning configuration changes. In this way, if your configuration changes do not have the expected effect, you will be able to revert to a known working configuration. For example:

```
nnmbackup.ovpl -type online -scope config
-target nnmi_backups\config
```

To restore this backup to the same NNMi management server, stop all NNMi processes, and then run a command similar to the following example:

```
nnmrestore.ovpl -force -source nnmi_backups\config\newest_backup
```

Back up Data Before Upgrading NNMi or the Operating System

Before making major system changes (including upgrading NNMi or the operating system), perform a complete backup of all NNMi data. To ensure that no changes are made to the NNMi database after the backup is made, stop all NNMi processes and create an offline backup. For example:

```
nnmbackup.ovpl -type offline -scope all
-target nnmi_backups\offline
```

If NNMi does not run correctly after the system change, roll back the change or set up a different NNMi management server and ensure that the requirements listed in Different System Restore on page 358 are met. Then run a command similar to the following example:

```
nnmrestore.ovpl -lic -source nnmi_backups\offline\newest_backup
```

Restore File System Files Only

To overwrite NNMi files without affecting the database tables, run a command similar to the following example:

```
nnmrestore.ovpl -partial
-source nnmi_backups\offline\newest_backup
```

The command is useful when the NNMi implementation uses Oracle for the main NNMi database.

Backing up and Restoring the Embedded Database Only

NNMi provides the `nnmbackupembdb.ovpl` and `nnmrestoreembdb.ovpl` commands to back up and restore the NNMi embedded database only. This functionality is useful for creating a snapshot of the data as you experiment with NNMi configuration settings. The `nnmbackupembdb.ovpl` and `nnmrestoreembdb.ovpl` commands perform online backups only. At a minimum, the `nmsdbmgr` service must be running.

Best practice

Run the`nnmresetembdb.ovpl` command before restoring data to the embedded database. This command ensures that the database does not contain any errors, thereby eliminating the possibility of encountering database constraint violations. For information about running the embedded database reset command, see the *nnmresetembdb.ovpl* reference page, or the UNIX manpage.

Maintaining NNMi

After you have your NNMi management server functioning, there are maintenance tasks you can perform to optimize several of the NNMi features.

This chapter contains the following topics:

Administering a Custom Poller Collection Export

The **Custom Poller feature** enables you to take a proactive approach to network management by using SNMP MIB expressions to specify additional information that NNMi should poll. A **Custom Poller collection** defines the information you want to gather (poll) as well as how NNMi reacts to the gathered data. See *Create a Custom Poller Collection* and *Configure Custom Polling* in the NNMi help for more detailed information.

The Custom Poller feature relies on you to remove files from the export directory as you process them. Do not use the exported files for long term storage; if they consume more than the configured maximum disk space, NNMi removes the older files and creates new ones. Unless you process these files and store them in a different location, you will lose them.

Changing the Custom Poller Collections Export Directory

NNMi writes the data from the collections you export into the following directory:

- *Windows*: `%NNM_DATA%\shared\nnm\databases\custompoller\export`
- *UNIX*: `$NNM_DATA/shared/nnm/databases/custompoller/export`

To change the directory that NNMi writes its custom poller files into, follow these steps:

1. Edit the following file:
   - *Windows*: `%NNM_PROPS%\nms-custompoller.properties`
   - *UNIX*: `$NNM_PROPS/nms-custompoller.properties`
2. Look for the `exportdir` entry, which is similar to the following line:

   ```
   #!com.hp.nnm.custompoller.exportdir=<base directory to export
   custom poller metrics>
   ```

   To configure NNMi to write Custom Poller collection information into the `C:\CustomPoller` directory, change the line as follows:

   ```
   com.hp.nnm.custompoller.exportdir=C:\CustomPoller
   ```
3. Restart the NNMi management server.
   a. Run the **`ovstop`** command on the NNMi management server.
   b. Run the **`ovstart`** command on the NNMi management server.

Changing the Maximum Amount of Disk Space for Custom Poller Collections Export

To change the maximum amount of disk space that NNMi uses when exporting data to *`collection_name`*`.csv` files, follow these steps:

1. Edit the following file:
   - *Windows*: `%NNM_PROPS%\nms-custompoller.properties`
   - *UNIX*: `$NNM_PROPS/nms-custompoller.properties`

2 Look for the `maxdiskspace` entry, which is similar to the following line:

```
#!com.hp.nnm.custompoller.maxdiskspace=1000
```

To configure NNMi to reserve up to 2000 MB (2 GB) of storage space for each *collection_name*.csv file, change the line as follows:

```
#!com.hp.nnm.custompoller.maxdiskspace=2000
```

3 Restart the NNMi management server.

a Run the **ovstop** command on the NNMi management server.

b Run the **ovstart** command on the NNMi management server.

Changing the Custom Poller Metric Accumulation Interval

NNMi sets the length of time, in minutes, that it accumulates Custom Poller Collection metrics before it writes data into a file.

To change the custom poller metric accumulation interval, follow these steps:

1 Edit the following file:

- *Windows*: `%NNM_PROPS%\nms-custompoller.properties`
- *UNIX*: `$NNM_PROPS/nms-custompoller.properties`

2 Look for a line the resembles the following:

```
#!com.hp.nnm.custompoller.accumulationinterval=5
```

To configure NNMi to collect metrics for ten minutes instead of the default value of five minutes, change the line as follows:

```
com.hp.nnm.custompoller.accumulationinterval=10
```

3 Restart the NNMi management server.

a Run the **ovstop** command on the NNMi management server.

b Run the **ovstart** command on the NNMi management server.

Administering Incident Actions

You can configure actions to automatically run at any point in the incident lifecycle. For example, you might want to configure an action to occur when an incident of the type you are configuring is generated. See *Configure an Action for an Incident* in the NNMi Help for more information.

To adjust action parameters, follow the steps shown in the following sections.

To avoid undesirable results (such as unintended memory growth, slower event action processing time), HP recommends that you do not change the default property values for event action processing.

Setting the Number of Simultaneous Actions

Increasing the number of simultaneous actions on a Solaris NNMi management server causes NNMi performance degradation.

To modify the number of simultaneous actions that NNMi can run, follow these steps:

1 Edit the following file:

- *Windows*: `%NNM_PROPS%\shared\nnmaction.properties`
- *UNIX*: `$NNM_PROPS/shared/nnmaction.properties`

2 Look for a line the resembles the following:

```
#!com.hp.ov.nms.events.action.numProcess=10
```

To configure NNMi to enable 20 simultaneous actions instead of the default value, change the line as follows:

```
com.hp.ov.nms.events.action.numProcess=20
```

Make sure to remove the **`#!`** characters located at the beginning of the line.

3 Restart the NNMi management server.

a Run the **`ovstop`** command on the NNMi management server.

b Run the **`ovstart`** command on the NNMi management server.

Setting the Number of Threads for Jython Actions

To modify the number of threads the action server uses to run jython scripts, follow these steps:

1 Edit the following file:

- *Windows*: `%NNM_PROPS%\shared\nnmaction.properties`
- *UNIX*: `$NNM_PROPS/shared/nnmaction.properties`

2 Look for a line that resembles the following:

```
#!com.hp.ov.nms.events.action.numJythonThreads=10
```

To configure NNMi to enable 20 threads for running jython scripts instead of the default value, change the line as follows:

```
com.hp.ov.nms.events.action.numJythonThreads=20
```

➤ Make sure to remove the **#!** characters located at the beginning of the line.

3 Restart the NNMi management server.

a Run the **ovstop** command on the NNMi management server.

b Run the **ovstart** command on the NNMi management server.

Setting the Action Server Name Parameter

If you have an NNMi management server running on a Windows operating system, the HP NNM Action Server runs as a windows service with a Local System account. That means you must use the Local System account to run action server actions.

To modify the user name that runs the HP NNM Action Server windows service on a Windows NNMi management server, change the LogOn property of the HP NNM Action Server service.

If you have an NNMi management server running on a HP-UX, Solaris, or Linux operating system, the action server runs with a bin user name. To modify the user name that runs the action server on these operating systems, complete the following steps:

1 Edit the following file:

```
$NNM_PROPS/nnmaction.properties
```

2 Look for a line the resembles the following:

```
#!com.hp.ov.nms.events.action.userName=bin
```

To configure NNMi to have *root* run the action server instead of the default value, change the line as follows:

```
com.hp.ov.nms.events.action.userName=root
```

➤ Make sure to remove the **#!** characters located at the beginning of the line.

3 Save your changes.

4 Restart the action server:

a Run the **ovstop nnmaction** command on the NNMi management server.

b Run the **ovstart nnmaction** command on the NNMi management server.

Changing the Action Server Queue Size

For actions that use a long action command string at a high execution rate, such as responding to a trap storm, the action server can use up a lot of memory. To provide better action server performance, HP places limits on the memory size that the action server can grow to.

➤ For Solaris NNMi management servers, if the NNMi health information shows that action queue sizes are growing, reduce the maximum memory size to improve performance.

To modify these limits, follow these steps:

1. Edit the following file:
   - `%NNM_PROPS%\shared\nnmaction.properties`
   - `$NNM_PROPS/shared/nnmaction.properties`
2. Look for two lines that resemble the following:

   ```
   com.hp.ov.nms.events.action.jvmargs.minMemsize=-Xms6m
   ```

   ```
   com.hp.ov.nms.events.action.jvmargs.maxMemsize=-Xmx30m
   ```
3. The above parameters show the minimum memory size set to 6MB and the maximum set to 30MB. Adjust these parameters to meet your needs.
4. Save your changes.
5. Restart the NNMi management server.
   a. Run the **ovstop** command on the NNMi management server.
   b. Run the **ovstart** command on the NNMi management server.

Incident Actions Log

When an action runs, output is logged to the associated Incident Actions Log file. To view the contents of the log for a selected incident, use the **Tools > Incident Actions Log** menu option. Below are descriptions of the items contained in the log:

Table 32 Incident Actions Log Items

Item	Description
Command	Script to run when incident occurs
Incident Name	Name of incident as defined in incident configuration
Incident UUID	The UUID of the incident (from **Registration** tab)
Command Type	Type of command (**Jython** or **ScriptOrExecutable**)
Lifecycle State	Lifecycle state of the incident (**Registered**, **In Process**, **Completed**, or **Closed**)
Exit Code	Return code of the command (similar to an error code)
Standard Output	Standard output of the action
Standard Error	Standard error output
Execution Status	The determined status per the action

Blocking Incidents using the trapFilter.conf File

Suppose the number of incidents flowing through your NNMi management server reaches a rate that causes NNMi to block newly arriving incidents.

When this happens, NNMi generates a `TrapStorm` incident, indicating that incidents are blocked. NNMi might also generate a major health message indicating that the incident rate is high and incidents are being blocked.

To remedy this, you might try to use the `nnmtrapd.conf` file to block incidents from entering NNMi in an attempt to reduce the incident traffic. However, if you use the `nnmtrapd.conf` file approach, NNMi still uses these incidents to calculate the trap rate and to write to the trap binary store. By using the `nnmtrapd.conf` file approach, you only stop incidents from being created or stored in the database. See the *nnmtrapd.conf* reference page, or the UNIX manpage for more information.

There is a better solution to this problem than using the `nnmtrapd.conf` file. NNMi provides a filtering mechanism that blocks incidents earlier in the NNMi event pipeline, preventing these incidents from being analyzed for trap rate calculations or from being stored in the NNMi trap binary store. By adding device IP addresses or OIDs to the `trapFilter.conf` file, you can block these high-volume incidents and avoid incident volume problems. See the *trapFilter.conf* reference page, or the UNIX manpage for more information.

Configuring HTTPS-Only Communication with the NNMi Console

The most effective method of preventing HTTP access to the NNMi console is to place the NNMi management server behind a firewall that permits only HTTPS access to the protected systems.

Firewall configuration to prevent HTTP access can cause problems for integrations that use web services to communicate with NNMi and only support HTTP. See the documentation for the integrating product to find out if it supports HTTPS.

For a less secure approach, redirect NNMi console access requests from the HTTP port to the HTTPS port by completing the following steps:

1 Edit the following file:

- *Windows*: `%NNM_PROPS\nms-ui.properties`
- *UNIX*: `$NNM_PROPS/nms-ui.properties`

2 Search for the string `https` to locate the text block containing the following line:

```
#! com.hp.ov.nms.ui.https.only=false
```

3 Uncomment and edit the following line to read as follows:

```
com.hp.ov.nms.ui.https.only=true
```

4 Restart NNMi by running these commands:

a **`ovstop`**

b **`ovstart`**

Setting this property to redirect HTTP requests to HTTPS for the NNMi console can cause problems with some applications that cross-launch back to NNMi. If you experience these problems, disable this HTTPS redirect.

Configuring the Auto-Trim Oldest SNMP Trap Incidents Feature

To keep NNMi performing at a high level, NNMi drops incoming SNMP traps (including syslog messages) after storing a specific number of SNMP traps in its database. You can use the auto-trim oldest SNMP trap incidents feature to control the number of SNMP traps stored in the NNMi database and to retain important incoming SNMP traps.

The auto-trim oldest SNMP trap incidents feature defaults to being disabled. After enabling the auto-trim oldest SNMP trap incidents feature, NNMi removes the oldest SNMP trap incidents from the NNMi database.

To manually trim SNMP trap incidents from the NNMi database, use the `nnmtrimincidents.ovpl` script. See the *nnmtrimincidents.ovpl* reference page, or the UNIX manpage, for more information.

Enabling the Auto-Trim Oldest SNMP Trap Incidents Feature (No Incident Archive)

Suppose you want to enable the auto-trim oldest SNMP trap incidents feature to trim 30,000 SNMP trap incidents (including syslog messages) after the number of SNMP trap incidents in the NNMi database exceeds 60,000. For this example, you do not want NNMi to archive the SNMP trap incidents before trimming them. Complete the following steps:

1. Edit the following file:
   - *Windows*: `%NNM_PROPS\nms-jboss.properties`
   - *UNIX*: `$NNM_PROPS/nms-jboss.properties`
2. Locate the text block containing the following line:
   `#!com.hp.nnm.events.snmpTrapAutoTrimStartPercentage=50`
3. Uncomment and edit the line to read as follows:
   `com.hp.nnm.events.snmpTrapAutoTrimStartPercentage=60`
4. Locate the text block containing the following line:
   `#!com.hp.nnm.events.snmpTrapAutoTrimPercentageToDelete=25`
5. Uncomment and edit the line to read as follows:
   `com.hp.nnm.events.snmpTrapAutoTrimPercentageToDelete=50`
6. Locate the text block containing the following line:
   `#!com.hp.nnm.events.snmpTrapAutoTrimSetting=Disabled`
7. Uncomment and edit the line to read as follows:
   `com.hp.nnm.events.snmpTrapsAutoTrimSetting=TrimOnly`
8. Restart NNMi:
   a. Run the **`ovstop`** command on the NNMi management server.
   b. Run the **`ovstart`** command on the NNMi management server.

The default value of **`com.hp.nnm.events.snmpTrapMaxStoreLimit`** is 100,000. With this configuration, after NNMi stores 60,000 SNMP trap incidents (including syslog messages) from the NNMi database, it trims 30,000 SNMP trap incidents from the NNMi database using the following formula:
(**`com.hp.nnm.events.snmpTrapAutoTrimStartPercentage X`**
`com.hp.nnm.events.snmpTrapMaxStoreLimit X`
`com.hp.nnm.events.snmpTrapAutoTrimPercentageToDelete`

Enabling the Auto-Trim Oldest SNMP Trap Incidents Feature (Incident Archive Enabled)

Suppose you want to enable the auto-trim oldest SNMP trap incidents feature to trim 60,000 SNMP trap incidents (including syslog messages) after the number of SNMP trap incidents in the NNMi database exceeds 80,000. For this example, you want NNMi to archive the SNMP trap incidents before trimming them. Complete the following steps:

1. Edit the following file:
   - *Windows*: `%NNM_PROPS\nms-jboss.properties`
   - *UNIX*: `$NNM_PROPS/nms-jboss.properties`

2. Locate the text block containing the following line:
   `#!com.hp.nnm.events.snmpTrapAutoTrimStartPercentage=50`
3. Uncomment and edit the line to read as follows:
   `com.hp.nnm.events.snmpTrapAutoTrimStartPercentage=80`
4. Locate the text block containing the following line:
   `#!com.hp.nnm.events.snmpTrapAutoTrimPercentageToDelete=25`
5. Uncomment and edit the line to read as follows:
   `com.hp.nnm.events.snmpTrapAutoTrimPercentageToDelete=75`
6. Locate the text block containing the following line:
   `#!com.hp.nnm.events.snmpTrapAutoTrimSetting=Disabled`
7. Edit the line to read as follows:
   `com.hp.nnm.events.snmpTrapsAutoTrimSetting=TrimAndArchive`
8. Restart NNMi:

   a. Run the **`ovstop`** command on the NNMi management server.

   b. Run the **`ovstart`** command on the NNMi management server.

The default value of **`com.hp.nnm.events.snmpTrapMaxStoreLimit`** is 100,000. With this configuration, after NNMi stores 80,000 SNMP trap incidents (including syslog messages) from the NNMi database, it archives, then trims 60,000 SNMP trap incidents from the NNMi database using the following formula:

```
(com.hp.nnm.events.snmpTrapAutoTrimStartPercentage X
com.hp.nnm.events.snmpTrapMaxStoreLimit X
com.hp.nnm.events.snmpTrapAutoTrimPercentageToDelete
```

Reducing the Number of Stored SNMP Trap Incidents

If you do not need NNMi to keep SNMP trap incidents for a long time period, you might consider reducing the number of SNMP trap incidents stored in the NNMi database.

NNMi begins dropping SNMP traps (including syslog messages) after the number of SNMP trap incidents in its database reaches 100,000. Setting this limit to a higher number is not supported, as doing so can cause NNMi performance degradation.

Suppose you want to reduce the maximum number of stored SNMP trap incidents (including syslog messages) to 50,000 SNMP trap incidents. To do this, complete the following steps:

1. Edit the following file:
   - *Windows*: `%NNM_PROPS\nms-jboss.properties`
   - *UNIX*: `$NNM_PROPS/nms-jboss.properties`
2. Locate the text block containing the following line:

   `#!com.hp.nnm.events.snmpTrapMaxStoreLimit=100000`
3. Uncomment and edit the line to read as follows:

   `com.hp.nnm.events.snmpTrapMaxStoreLimit=50000`
4. Restart NNMi:

   a. Run the **`ovstop`** command on the NNMi management server.

   b. Run the **`ovstart`** command on the NNMi management server.

Monitoring the Auto-Trim Oldest SNMP Trap Incidents Feature

From the **NNMi console**, click **Help > System Information > Health** to check the health of the auto-trim oldest SNMP trap incidents feature. NNMi also generates the following alarms regarding the auto-trim oldest SNMP trap incidents feature.

- NNMi generates a critical alarm after the number of stored SNMP trap incidents (including syslog messages) reaches 100% of the **`com.hp.nnm.events.snmpTrapMaxStoreLimit`** value.
- NNMi generates an `snmpTrapLimitMajorAlarm` alarm after the number of stored SNMP trap incidents (including syslog messages) reaches 95% of the **`com.hp.nnm.events.snmpTrapMaxStoreLimit`** value.
- NNMi generates an `snmpTrapLimitWarningAlarm` alarm after the number of stored SNMP trap incidents (including syslog messages) reaches 90% of the **`com.hp.nnm.events.snmpTrapMaxStoreLimit`** value.

Disabling the Auto-Trim Oldest SNMP Trap Incidents Feature

To disable the auto-trim oldest incidents feature, complete the following steps:

1. Edit the following file:
   - *Windows*: `%NNM_PROPS\nms-jboss.properties`
   - *UNIX*: `$NNM_PROPS/nms-jboss.properties`
2. Locate the text block containing the following:

   `com.hp.nnm.events.snmpTrapAutoTrimSetting`
3. Uncomment and edit the line to read as follows:

   `com.hp.nnm.events.snmpTrapAutoTrimSetting=Disabled`
4. Restart NNMi:
   a. Run the **`ovstop`** command on the NNMi management server.
   b. Run the **`ovstart`** command on the NNMi management server.

Controlling the Times that APA Accepts Traps

When large areas of a network are unavailable at regular and predictable hours during the day, NNMi can help you moderate the APA analysis load by inhibiting delivery of unnecessary traps to APA. NNMi permits users to configure times that APA stops accepting traps from the event system during the day. This feature does not interfere with traps delivered to the NNMi console.

➤ APA does not use traps as part of its analysis rules. APA reaches the same conclusion with or without traps by using state flows from the NNMi State Poller. Traps that are controlled by inhibiting delivery of traps to APA are used to trigger State Poller to poll a node sooner than the schedule dictated by the State Poller Polling Policy.

To configure times that APA stops accepting traps, follow these steps:

1 Create the following file:

- *Windows*: `%NNM_PROPS%\shared\nms-apa.properties`
- *UNIX*: `$NNM_PROPS/shared/nms-apa.properties`

2 Add the following content to the file:

PROPERTY NAME: com.hp.ov.nms.apa.trapGateSchedule

3 Add the right property value to the file to meet the needs of your network. Use the following examples as a guideline:

— Suppose you want to have traps flow at midnight, inhibit them at 8:30 a.m, let them flow again at 10:00 a.m., then turn them off again at 4:30pm. To do this, add the following entry:

```
com.hp.ov.nms.apa.trapGateSchedule = ENABLE_APA_TRAPS  08:30
10:00 16:30
```

— Suppose you want to have traps inhibited at midnight, let them flow again at 8:30 a.m, inhibit them at 10:00 a.m., then let them flow again at 4:30pm. To do this, add the following entry:

```
com.hp.ov.nms.apa.trapGateSchedule = DISABLE_APA_TRAPS  08:30
10:00 16:30
```

4 Restart NNMi:

a Run the **`ovstop`** command on the NNMi management server.

b Run the **`ovstart`** command on the.NNMi management server

Modifying NNMi Normalization Properties

NNMi stores both hostnames and node names in case-sensitive form. This means that all searches, sorts, and filters that the NNMi console provides return case-sensitive results. If the DNS servers you use return a variety of case-preserving node names and hostnames, including all uppercase, all lowercase, and a mixture of uppercase and lowercase, this can cause less-than-optimal results.

You can change several NNMi normalization properties to meet your specific needs. A good practice is to make these changes before seeding NNMi for its initial discovery. HP recommends that you adjust the settings in this section during deployment, but before running the initial discovery.

If you run an initial discovery, then decide to change the normalization properties later, you can run the **`nnmnoderediscover.ovpl -all`** script to initiate a full discovery. See the *nnmnoderediscover.ovpl* reference page, or the UNIX manpage, for more information.

You can change the following properties:

- Normalize discovered node names to `UPPERCASE`, `LOWERCASE`, or `OFF`.
- Normalize discovered hostnames to `UPPERCASE`, `LOWERCASE`, or `OFF`.

To change normalization properties follow these steps:

1. Edit the following file:
   - *Windows*: `%NNM_PROPS%\nms-topology.properties`
   - *UNIX*: `$NNM_PROPS/nms-topology.properties`
2. To configure NNMi to normalize discovered names, look for a line the resembles the following:

   ```
   #!com.hp.ov.nms.topo.NAME_NORMALIZATION=OFF
   ```

   a. Un-comment the property:

      ```
      com.hp.ov.nms.topo.NAME_NORMALIZATION=OFF
      ```

      To un-comment a property, remove the `#!` characters from the beginning of a line.

   b. Change `OFF` to `LOWERCASE` or `UPPERCASE`.

   c. Save your changes.
3. To configure NNMi to normalize discovered hostnames, look for a line the resembles the following:

   ```
   #!com.hp.ov.nms.topo.NAME_NORMALIZATION=OFF
   ```

   a. Un-comment the property:

      ```
      com.hp.ov.nms.topo.HOSTNAME_NORMALIZATION=OFF
      ```

   b. Change `OFF` to `LOWERCASE` or `UPPERCASE`.

   c. Save your changes.
4. Restart the NNMi management server.

   a. Run the **`ovstop`** command on the NNMi management server.

   b. Run the **`ovstart`** command on the NNMi management server.

Changing Normalization Properties Following an Initial Discovery

Changing normalization properties following an initial discovery causes NNMi to be inconsistent with the property changes until the next discovery. To remedy this, run the **`nnmnoderediscover.ovpl -all`** script to initiate a full discovery after changing NNMi normalization properties.

After NNMi completes a full discovery, the behaviors shown below should return to normal. These examples are not exhaustive, and are intended to provide a few examples of things to consider when changing NNMi normalization properties.

Modifying Simultaneous SNMP Requests

NNMi maintains a limit of three simultaneous SNMP requests to a node. This reduces the risk of a node's SNMP agents dropping responses.

You can adjust this value higher, resulting in increased discovery speed. However, if you set the value too high, you increase the risk of dropped responses and reduced discovery accuracy.

To modify this limit, follow these steps:

1. Edit the following file:
   - *Windows*: `%NNM_PROPS%\nms-communication.properties`
   - *UNIX*: `$NNM_PROPS/nms-communication.properties`
2. To increase the current number of simultaneous SNMP requests to a node, do the following:

   a. Look for a line the resembles the following:
   `#!com.hp.ov.nms.comm.snmp.maxConcurrentRequests=3`

   b. Un-comment the property:
   `com.hp.ov.nms.comm.snmp.maxConcurrentRequests=3`

   To un-comment a property, remove the `#!` characters from the beginning of a line.

   c. Change the existing value to the number of desired simultaneous SNMP requests to a node.

   d. Save your changes.
3. Restart the NNMi management server.

   a. Run the **`ovstop`** command on the NNMi management server.

   b. Run the **`ovstart`** command on the NNMi management server.

NNMi Self Monitoring

NNMi performs self-monitoring checks, including memory, CPU, and disk resources. NNMi generates an incident after the NNMi management server becomes low on resources or detects a serious condition.

To view NNMi health information, use one of the following methods:

- From the NNMi console, click **View** > **System Information**; then click the **Health** tab.
- For a detailed self-monitoring report, select **Tools** > **NNMi System Health Report**
- Run the **`nnmhealth.ovpl`** script.

NNMi opens a status message at the bottom of the NNMi console and on the top of forms after an NNMi detects a self-monitoring heath exception. You can disable this warning message by completing the following steps:

1 Edit the following file:
   - *Windows*: `%NNM_PROPS\nms-ui.properties`
   - *UNIX*: `$NNM_PROPS/nms-ui.properties`

2 Locate the text block containing the following line:

```
#!com.hp.nms.ui.health.disablewarning=false
```

3 Uncomment and edit the following line to read as follows:

```
    com.hp.nms.ui.health.disablewarning==true
```

4 Restart NNMi by running these commands:

   a **`ovstop`**

   b **`ovstart`**

Suppressing the Use of Discovery Protocols for Specific Nodes

NNMi uses several protocols to discover layer 2 connectivity between and among network devices. There are many defined discovery protocols. For example, *Link Layer Discovery Protocol* (LLDP) is an industry standard protocol, while there are many vendor-specific protocols like *Cisco Discovery Protocol* (CDP) for Cisco devices.

You can configure NNMi to suppress discovery protocol collections for devices you specify. There are special circumstances that might be remedied by suppressing discovery protocol collections.

Here are some examples:

- *Enterasys devices*: Using SNMP to collect information from the *Enterasys Discovery Protocol* (EnDP) and LLDP tables on some Enterasys devices might cause issues with NNMi running out of memory. You could prevent this by configuring NNMi to skip EnDP and LLDP processing on these devices. To do this, add the management address of the devices to the `disco.SkipXdpProcessing` file as shown in Suppressing the Use of Discovery Protocol Collections.

  ➤ New operating system versions on some Enterasys devices support the **`set snmp timefilter break`** command. On those Enterasys devices, run the **`set snmp timefilter break`** command. If you configure the device using this command, you do not need to list the device in the `disco.SkipXdpProcessing` file.

- *Nortel devices*: Many Nortel devices use *SynOptics Network Management Protocol* (SONMP) to discover layer 2 layout and connectivity. Some of these devices use the same MAC address on multiple interfaces, and do not work well with this protocol. You might experience this problem if two interconnected Nortel devices show a layer 2 connection between the wrong set of interfaces and the connection shows a connection source of `SONMP`.
  For this example, it is best to configure NNMi to not use the SONMP protocol to derive layer 2 connections for the devices shown as participating in the wrong connection. To do this, add the management address of the two devices to the `disco.SkipXdpProcessing` file as shown in Suppressing the Use of Discovery Protocol Collections.

Suppressing the Use of Discovery Protocol Collections

To suppress this collection, follow these steps:

1. Create the following file:
   - *Windows*: `%NnmDataDir%\shared\nnm\conf\disco\disco.SkipXdpProcessing`
   - *UNIX*: `$NnmDataDir/shared/nnm/conf/disco/disco.SkipXdpProcessing`

   The `disco.SkipXdpProcessing` file is case-sensitive .
2. Add the device IP addresses to the `disco.SkipXdpProcessing` file for all of the devices you want to suppress protocol collection for. Follow the instructions show in the *disco.SkipXdpProcessing* reference page, or the UNIX manpage.
3. Restart the NNMi management server.
   a. Run the **`ovstop`** command on the NNMi management server.
   b. Run the **`ovstart`** command on the NNMi management server.

➤ Suppressing the discovery protocol processing of a node or nodes might cause some inaccuracies in the layer 2 layout of the managed network. HP is not responsible for these inaccuracies.

➤ The `ovjboss` service reads the `disco.SkipXdpProcessing` file on startup. If you make any changes after starting NNMi, restart NNMi as shown in this step.

➤ If you ran the **`set snmp timefilter break`** command on any Enterasys devices, remove the device addresses from the `disco.SkipXdpProcessing` file, then restart NNMi as shown in this step. NNMi opens more accurate layer 2 maps when it uses discovery protocols.

See the *disco.SkipXdpProcessing* reference page, or the UNIX manpage, for more information.

Administering ICMP Polling of the Management Address in a NAT Environment

The information in this section is not included in the published version of the *NNMi Deployment Reference* for HP NNMi 9.0x patch 2. You can share this information with customers that need to use the new feature.

In a Network Address Translation (NAT) environment, a firewall blocks NNMi from communicating with NAT nodes using the IP addresses on the nodes (the private IP addresses). To remedy this, use the NAT address (the public IP address) for communication with NNMi.

In a NAT environment, a node's management address might be different from the IP addresses hosted on the node. For NNMi to discover a node in a NAT environment, you must add the NAT address to NNMi as a discovery seed. NNMi uses this NAT address for SNMP communication, even though it is not in the node's `ipAddressTable`.

After applying NNMi 9.0x patch 2, you can configure a new NNMi feature to ICMP poll a node's SNMP address. The result is a more reliable and accurate analysis. Using this new feature avoids false node down incidents and a better root cause analysis.

Enabling ICMP Polling of the Management Address in a NAT Environment

To enable ICMP management address polling in a NAT environment, do the following:

1. Enable `ICMP Management Address Polling`. See Default Monitoring in the NNMi help.
2. Set a system property as follows:
   - a. Change to the following directory:

     Windows: `%NNM_PROPS%`

     UNIX: `$NNM_PROPS`
   - b. Create the following property file: *mypropertyfile*`.properties`. Substitute any file name for *mypropertyfile*, however you must use the `.properties` file extension.
   - c. Add the following line to the *mypropertyfile*`.properties` file:

     ```
     com.hp.ov.nnm.useSnmpAgentManagementAddressState = true
     ```
   - d. Restart the NNMi management server.

     ```
     ovstop -c
     ```

     ```
     ovstart -c
     ```

View the information NNMi opens after performing **Actions->Monitoring Settings** for SNMP Agents. The displayed information indicates whether NNMi has the management address polling enabled.

How this Changes NNMi

After you complete the steps shown in Enabling ICMP Polling of the Management Address in a NAT Environment on page 377, NNMi changes as follows:

- The Agent ICMP State field appears in the following forms:
  - — Node form
  - — SNMP Agent form
  - — SNMP Agent table views
- NNMi changes the display location of the management address ICMP state. NNMi also changes the way it determines the SNMP agent status.

Table 33 shows the Agent ICMP and IP Address state polling actions that NNMi takes for the ICMP Management Address Polling and ICMP Fault Polling settings. The shaded first row in Table 33 shows the default configuration.

Table 33 ICMP Configurations and Resulting State Polling

ICMP Management Address Polling	ICMP Fault Polling	Agent ICMP State	IP Address State
Enabled	Disabled	Polled	Not Polled
Enabled	Enabled	Polled	Polled
Disabled	Disabled	Not Polled	Not Polled
Disabled	Enabled	Not Polled	Polled

Table 34 shows changes to the SNMP Agent Status determined by APA for the SNMP agent and ICMP responses.

Table 34 Determining SNMP Agent Status

SNMP Agent Response	Management Address ICMP Response	SNMP Agent Status
Responding	Responding	Normal
Responding	Not Responding	Minor
Not Responding	Responding	Critical
Not Responding	Not Responding	Critical

With ICMP polling of the management address enabled, APA now considers the management address ICMP response and the SNMP agent response when generating conclusions and generating incidents.

Suppressing the Use of VLAN-indexing for Large Switches

One of the methods NNMi uses to learn layer 2 connectivity between and among switch devices in a managed network is to retrieve the `dot1dTpFdbTable` (FDB) from the switches. However, for Cisco switches, NNMi must use a `VLAN-indexing` method to retrieve the entire FDB. If there is a large number of VLANs configured on each device, retrieving the FDB with `VLAN-indexing` might take hours to complete.

Cisco switches are often configured to use the Cisco Discovery Protocol (CDP). CDP is considered to be a superior method for learning layer 2 connectivity. Large switches located in the in the core of the network might contain many VLANs. These switches typically do not have end nodes connected directly to them. If the switches you want to manage do not have end nodes connected directly to them, you might want to suppress the collection of the FDB on these large switches. NNMi still completes the layer 2 discovery using data collected from CDP. These large switches are prime candidates for suppression of `VLAN-indexing`. Do not suppress `VLAN-indexing` on smaller switches located at the network's edge (often known as access switches) that have many end nodes attached to them.

You can configure NNMi to suppress `VLAN-indexing`. To do this, the NNMi administrator needs to create and add management addresses or address ranges of the large switches to the `disco.NoVLANIndexing` file as shown in Suppressing the Use of VLAN-indexing on page 379. The `ovjboss` service reads the `disco.NoVLANIndexing` file when it starts. If the NNMi administrator makes changes to the `disco.NoVLANIndexing` file after the `ovjboss` service starts, those changes will not take effect until the next time the `ovjboss` service starts. By default, the `disco.NoVLANIndexing` file does not exist. If the `disco.NoVLANIndexing` does not exist, this feature is disabled and NNMi attempts to use `VLAN-indexing` to collect the entire FDB table on all devices.

Suppressing the Use of VLAN-indexing

To disable this `vlan-indexing`, follow these steps:

1. Create the following file:
   - *Windows*: `%NnmDataDir%\shared\nnm\conf\disco\disco.NoVLANIndexing`
   - *UNIX*: `$NnmDataDir/shared/nnm/conf/disco/disco.NoVLANIndexing`

   The `disco.NoVLANIndexing` file is case-sensitive .
2. Add the device IP addresses or address ranges to the `disco.NoVLANIndexing` file for all of the devices you want to disable `vlan-indexing` for. Follow the instructions show in the *disco.NoVLANIndexing* reference page, or the UNIX manpage.
3. Restart the NNMi management server.
   a. Run the **`ovstop`** command on the NNMi management server.
   b. Run the **`ovstart`** command on the NNMi management server.

➤ Suppressing `vlan-indexing` of a node or nodes might cause some inaccuracies in the layer 2 layout of the managed network. HP is not responsible for these inaccuracies.

➤ The `ovjboss` service reads the `disco.NoVLANIndexing` file on startup. If you make any changes after starting NNMi, restart NNMi as shown in this step.

See the *disco.Disco.NoVLANIndexing* reference page, or the UNIX manpage, for more information.

Understanding ICMP Polling of the Management Address in a NAT Environment

In a network address translation (NAT) environment, a firewall blocks NNMi from communicating with NAT nodes using the IP addresses on the nodes (the private IP addresses). To remedy this, NNMi uses the NAT address (the public IP address) for communication with NNMi.

In a NAT environment, a node's management address might be different from the IP addresses hosted on the node. For NNMi to discover a node in a NAT environment, you must add the NAT address to NNMi as a discovery seed. NNMi uses this NAT address for SNMP communication, even though it is not in the node's `ipAddressTable`.

NNMi provides this feature to avoid generating false node down incidents and a better root cause analysis.

ICMP Polling of the Management Address in a NAT Environment

NNMi automatically enables ICMP management address polling for all nodes, including those nodes residing in a NAT environment. NNMi functions in a NAT environment as shown below.

- The Management Address State field appears in the following forms:
  - Node form
  - SNMP Agent form
  - SNMP Agent table views
- NNMi changes the display location of the management address ICMP state. NNMi also changes the way it determines the SNMP agent status.

Table 35 shows the Management Address ICMP and IP Address state polling actions that NNMi takes for the ICMP Management Address Polling and ICMP Fault Polling settings. The shaded first row in Table 35 shows the default configuration.

Table 35 ICMP Configurations and Resulting State Polling

ICMP Management Address Polling	ICMP Fault Polling	Management ICMP Address State	IP Address State
Enabled	Disabled	Polled	Not Polled
Enabled	Enabled	Polled	Polled
Disabled	Disabled	Not Polled	Not Polled
Disabled	Enabled	Not Polled	Polled

Table 36 shows changes to the SNMP Agent Status and the generated incidents determined by APA for the SNMP agent and ICMP responses. With ICMP polling of the management address, APA considers the management address ICMP response and the SNMP agent response when generating conclusions and incidents.

.

Table 36 Determining SNMP Agent Status and the Generated Incident

SNMP Agent Response	Management Address ICMP Response	SNMP Agent Status	Incident Generated
Responding	Responding	Normal	None
Responding	Not Responding	Minor	There are two possibilities depending on other network issues: - None - `AddressNotResponding`
Not Responding	Responding	Critical	- `SNMPAgentNotResponding`
Not Responding	Not Responding	Critical	There are two possibilities depending on other network issues: - None - `NodeDown`

NNMi Logging

NNMi Log Files

To investigate HP Network Node Manager i Software (NNMi) performance, or to observe how NNMi processes and services are behaving, you can view log files that show a history of process and service activity. These files are available at the following location:

- *Windows*: `%NnmDataDir%\log\nnm\`
- *UNIX*: `$NnmDataDir/log/nnm`

NNMi stores these log files in the form *`name`*`.%g.%u.log`.

- *`name`* is the log file base name, which is `nnm` for most NNMi functions.
- `%g` relates to archived log files. When the `%g` portion of a log file name is zero (`0`), NNMi is actively logging to the *`name`*`.0.%u.log` file. You should also see a *`name`*`.0.%u.log.lck` file.
- `%u` is normally zero (`0`), unless the parent ovjboss failed during a logging session.

A log file can become an archived log file in either of the following ways:

- The ovjboss process is restarted.
- The size of the log file exceeds the configured limit.

When ovjboss is restarted, or a log file size exceeds the configured limit, the last active log file is archived. For example, the file `nnm.0.0.log` is archived as file `nnm.1.0.log`. Then, NNMi begins logging to a new `nnm.0.0.log` file.

NNMi logs messages at the following logging levels:

- SEVERE: Events that relate to abnormal NNMi behavior.
- WARNING: Events that indicate potential problems and all messages included in the SEVERE logging level.
- INFO: Messages written to the NNMi console (or its equivalent) and all messages included in the WARNING logging level.
- CONFIG: Static configuration information and all messages included in the INFO logging level.

Log File Properties

You can control the size of the log file for each service by adjusting the `.limit` property for NNMi log file handler in the `logging.properties` file. You can also control the number of archived files by adjusting the `.count` property for the NNMi log file handler in the `logging.properties` file.

The `logging.properties` file is in the following location:

- *Windows*: `%NnmDataDir%\shared\nnm\conf\ovjboss`
- *UNIX*: `$NnmDataDir/shared/nnm/conf/ovjboss`

For additional information about logging, see the *logging.properties* reference page, or the UNIX manpage.

Changing Logging File Properties

You can configure the number and size of NNMi log files by adjusting the following logging parameters:

- `.count`
- `.limit`

For example, to create fewer, larger `nnm.%g.%u.log` files, follow these steps:

1. Back up the `logging.properties` file, and then open the file in any text editor.
2. Decrease the number of log files to 10 by changing the following line:

   ```
   com.hp.ov.nms.admin.log.NnmMainFileHandler.count = 20
   ```

   to read as follows:

   ```
   com.hp.ov.nms.admin.log.NnmMainFileHandler.count = 10
   ```

3. Increase the amount of logged information for the discovery process by changing the following line:

   ```
   com.hp.ov.nms.admin.log.NnmMainFileHandler.limit = 50000000
   ```

   to read as follows:

   ```
   com.hp.ov.nms.admin.log.NnmMainFileHandler.limit = 100000000
   ```

4 Restart NNMi by running the following commands:

   a **ovstop**

   b **ovstart**

Alternatively, you can run the `nnmrereadlogging.ovpl` command in the NNMi support directory:

- *Windows*: `%NnmInstallDir%\support`
- *UNIX*: `$NnmInstallDir/support`

File Management

You should regularly monitor the log files in `%NnmDataDir%\log\nnm` (Windows) or `$NnmDataDir/log/nnm` (UNIX) because they continue to grow in size. Remove any large archived files.

Changing the NNMi Management Server

You can duplicate the HP Network Node Manager i Software (NNMi) configuration on another system, for example, to move from a test environment to a production environment or to change the hardware of the NNMi management server.

You can change the IP address of the NNMi management server without affecting the NNMi configuration.

This chapter contains the following topics:

Best Practices for Preparing the NNMi Configuration to Be Moved

The following best practices apply to moving the NNMi configuration to a different system:

- If the node group configuration uses hostnames to identify managed nodes, the production and test NNMi management servers must use the same DNS servers. In the case that the production and test systems use different DNS servers, changes in the resolved name for a managed node might result in different polling settings between the two NNMi management servers.
- You can limit the configuration export to a single author. Create a new author value that is unique to your group or company. Specify this author value when you create or modify any of the following items:
  - Device profile
  - Incident configuration
  - URL action
- If you plan to install Smart Plug-ins (iSPIs), see the appropriate chapters in the Integrations with NNMi section.

Moving the NNMi Configuration and Embedded Database

To move the NNMi configuration and the embedded database, for example from a test system to a production system, perform a complete backup of all NNMi data on the source (test) system, and then restore the backup to the target (production) system. To ensure that no changes are made to the NNMi database after the backup is made, stop all NNMi processes and create an offline backup. For example:

```
nnmbackup.ovpl -type offline -scope all \
-target nnmi_backups\offline
```

Ensure that the requirements listed in Different System Restore on page 358 are met on the new system, and then run a command similar to the following example:

```
nnmrestore.ovpl -source nnmi_backups\offline\newest_backup
```

⚠ NNMi uses the same SSL certificate for accessing the database (embedded or external) and supporting HTTPS access to the NNMi console. The certificate for accessing the database was created when the NNMi processes first started on the source system. This certificate is included in the backup and restore data. Without this certificate NNMi cannot access the database from the target system.

However, for HTTPS access to the NNMi console, the SSL certificate must be generated on the target system. Because the current implementation of jboss does not support certificate merging, NNMi does not support HTTPS access to the NNMi console on a system that was set up by restoring data from a different system. If the target system must support HTTPS access to the NNMi console, use the procedure described in Moving the NNMi Configuration on page 389, and then begin data collection fresh on the target system.

Moving the NNMi Configuration

Use the `nnmconfigexport.ovpl` command to output the NNMi configuration to an XML file. Then, use the `nnmconfigimport.ovpl` command to pull this configuration from the XML file into NNMi on the new system.

Do not edit a file exported with the `nnmconfigexport.ovpl` script before using the `nnmconfigimport.ovpl` script to import the file.

For information about these commands, see the appropriate reference pages, or the UNIX manpages.

The nnmconfigexport.ovpl command does not retain SNMPv3 credentials. For more information, see the *nnmconfigexport.ovpl* reference page, or the UNIX manpage.

You can only move the NNMi configuration. HP does not support moving topology or incident data from one NNMi management server to a different NNMi management server. Nor does HP support moving iSPI data, such as performance data that was collected for the NNM iSPI Performance for Metrics.

Restoring the NNMi Public Key Certificate

If the NNMi management server participates in NNMi application failover or is a member of a high availability (HA) cluster, contact your support representative for assistance.

The nnm.keystore file stores the public key certificate that NNMi uses for encryption. The NNMi installation process creates the nnm.keystore file and links the certificate in this file to the nms_sec_key record in the NNMi database (Postgres or Oracle).

If NNMi is subsequently uninstalled, but the Oracle user and database tables for NNMi are not deleted (cascaded delete of the Oracle user) before a subsequent reinstall, the nms_sec_key entry is not valid for the newly created nnm.keystore file.

To restore the NNMi public key certificate, complete the following tasks:

- Task 1: Determine the Status of the KeyManager Service
- Task 2: Back up the Current nnm.keystore File
- Task 3: Attempt to Locate the Original nnm.keystore File
- Task 4: If Available, Restore the Original nnm.keystore File

Task 1: Determine the Status of the KeyManager Service

1 Run the following command:

```
ovstatus -v ovjboss
```

2 In the command output, verify that the KeyManager service is not running, which usually indicates that the nnm.keystore file is corrupt or missing.

If the ovstatus output shows that the KeyManager service is started, contact your support representative for assistance.

Task 2: Back up the Current nnm.keystore File

1. Change to the directory that contains the NNMi trust store:
   - *Windows*: `%NnmDataDir%\shared\nnm\certificates`
   - *UNIX*: `$NnmDataDir/shared/nnm/certificates`
2. For backup purposes, save copies of the following files:
   - `nnm.keystore`
   - `nnm.truststore`

Task 3: Attempt to Locate the Original nnm.keystore File

1. Determine the fingerprint of the security key in the NNMi database:
   - For the embedded Postgres database, enter the following:
     - *Windows*:
       ```
       %NnmInstallDir%\nonOV\Postgres\bin\psql -U postgres \
       -d nnm -c "<database_command>"
       ```
     - *UNIX*:
       ```
       $NnmInstallDir/nonOV/Postgres/bin/psql -U postgres \
       -d nnm -c "<database_command>"
       ```

     Replace *<database_command>* with the following SQL command string:

     ```
     select fingerprint from nms_sec_key;
     ```
   - For an Oracle database, ask the Oracle database administrator to run the *<database_command>* (described for the embedded database earlier in this step) in the appropriate Oracle administration tool.

   The command results should be a single database row. The correct nnm.keystore file also contains this fingerprint.
2. Identify a backup nnm.keystore file to test.

   This file might be in a backup of the NNMi management server in the original installation directory.
3. Test the fingerprint of a backup nnm.keystore file:

   a. Change to the directory that contains the NNMi certificates:
     - *Windows*: `%NnmDataDir%\shared\nnm\certificates`
     - *UNIX*: `$NnmDataDir/shared/nnm/certificates`

   b. Examine the contents of the key store:
     - *Windows*:
       ```
       %NnmInstallDir%\nonOV\jdk\b\bin\keytool -list \
       -keystore nnm.keystore
       ```
     - *UNIX*:
       ```
       $NnmInstallDir/nonOV/jdk/b/bin/keytool -list \
       -keystore nnm.keystore
       ```

     When prompted for the key store password, enter: **`nnmkeypass`**

The key store output is of the form:

```
Keystore type: jks
Keystore provider: SUN
Your keystore contains 1 entry
selfsigned, Oct 28, 2008, keyEntry,
Certificate fingerprint (MD5):
29:02:D7:D7:D7:D7:29:02:29:02:29:02:29:02:29:02
```

c Compare the value of the MD5 fingerprint from this nnm.keystore file with the fingerprint in the NNMi database (from step 1 of this task).

— If the fingerprints match exactly, you have located a good nnm.keystore file for this NNMi database. Continue with Task 4: If Available, Restore the Original nnm.keystore File.

— If the fingerprints do not match exactly, repeat Task 3: Attempt to Locate the Original nnm.keystore File.

If you cannot locate the original nnm.keystore file using the above procedure, contact your support representative for assistance. Do not continue with Task 4: If Available, Restore the Original nnm.keystore File.

Task 4: If Available, Restore the Original nnm.keystore File

If you located the correct nnm.keystore file, restore that file by following these steps:

1 Stop NNMi:

```
ovstop
```

2 Copy the located nnm.keystore file on top of the existing file in the following location:

- *Windows*: `%NnmDataDir%\shared\nnm\certificates`
- *UNIX*: `$NnmDataDir/shared/nnm/certificates`

3 Start NNMi:

```
ovstart
```

4 Run the following command:

```
ovstatus -v ovjboss
```

5 In the command output, verify that the KeyManager service is started.

After you have verified that NNMi is working correctly, you can remove the backup copy of the nnm.keystore file from Task 2: Back up the Current nnm.keystore File.

Changing the IP Address of a Standalone NNMi Management Server

To change the IP address of the NNMi management server, follow these steps:

1. Go to **http://www.webware.hp.com**.
2. Click **Manage Licenses**.
3. Log in; then obtain your new license key by following the procedures to complete the move process.
4. Configure the NNMi management server with the new IP address.
5. Configure the DNS servers to recognize the new IP address of the NNMi management server.
6. Reboot the NNMi management server.
7. At a command prompt, enter the following command:

   ```
   nnmlicense.ovpl NNM -g
   ```

8. In the **Autopass: License Management** dialog box, click **Remove License Key**.
9. Select the license key to remove.
10. Select **Remove Licenses permanently.**
11. Click **Remove**; then close the dialog box.
12. Copy the new license key that you obtained in step 3 into a text file named `license.txt`.
13. At a command prompt, enter the following command:

    ```
    nnmlicense.ovpl NNM -f license.txt
    ```

Licensing Considerations

For information about obtaining and installing NNMi license keys, see Licensing NNMi on page 117.

Changing the Hostname or Domain Name of an NNMi Management Server

If the NNMi management server participates in NNMi application failover or is a member of a high availability (HA) cluster, contact your support representative for assistance.

To change the hostname, the domain name, or both, of the NNMi management server, complete the following tasks:

- Task 1: Prepare the System
- Task 2: Create a New NNMi Public Key Certificate
- Task 3: Change the Fully-Qualified Domain Name of the NNMi Management Server
- Task 4: Update the HTTPS Configuration with the New Certificate
- Task 5: Restart, Update, and Refresh Systems
- Task 6: Back up NNMi

Task 1: Prepare the System

1. Follow your standard procedure to take a complete NNMi backup.

   Clearly label this backup as before changing the name of the NNMi management server.

2. Rename the system.

   If necessary, reboot the system. The ovjboss process might not start completely.

3. If the IP address of the NNMi is also changing, complete the steps in Changing the IP Address of a Standalone NNMi Management Server on page 392.

4. Stop NNMi:

   ```
   ovstop
   ```

5. Change to the directory that contains the NNMi certificates:

   - *Windows*: `%NnmDataDir%\shared\nnm\certificates`
   - *UNIX*: `$NnmDataDir/shared/nnm/certificates`

6. For backup purposes, save copies of the following files:

   - `nnm.keystore`
   - `nnm.truststore`

Task 2: Create a New NNMi Public Key Certificate

Create a new certificate for this NNMi management server in the nnm.keystore file. The next time that the ovjboss process starts successfully, NNMi updates the database access to use the new certificate.

1. Change to the directory that contains the NNMi certificates:
   - *Windows*: `%NnmDataDir%\shared\nnm\certificates`
   - *UNIX*: `$NnmDataDir/shared/nnm/certificates`

   Run all commands in this procedure from the `certificates` directory.

2. Generate a new public/private key pair (certificate) in the keystore by running the following command:
   - *Windows*:
     ```
     %NnmInstallDir%\nonOV\jdk\b\bin\keytool -genkey \
     -alias "<unique_alias>" -keyalg rsa
     -dname "cn=<hostname>, dc=<domain_name_by_parts>" \
     -keypass "nnmkeypass" -validity 36500 \
     -keystore nnm.keystore -storepass "nnmkeypass"
     ```
   - *UNIX*:
     ```
     $NnmInstallDir/nonOV/jdk/b/bin/keytool -genkey \
     -alias "<unique_alias>" -keyalg rsa
     -dname "cn=<hostname>, dc=<domain_name_by_parts>" \
     -keypass "nnmkeypass" -validity 36500 \
     -keystore nnm.keystore -storepass "nnmkeypass"
     ```

   Replace *`<alias>`* with a unique value such as the new hostname of the NNMi management server, for example: `newnnmi`

   Replace *`<hostname>`* with the new fully-qualified domain name of the NNMi management server, for example: `newnnmi.servers.example.com`

   Replace `dc=`*`<domain_name_by_parts>`* with the individual components of the new domain in which the NNMi management server resides. For example, for the NNMi management server `newnnmi.servers.example.com`, specify: `dc=servers, dc=example, dc=com`

For more information about the `keytool` command, search for “Key and Certificate Management Tool” at **java.sun.com**.

Task 3: Change the Fully-Qualified Domain Name of the NNMi Management Server

To set NNMi to use the new fully-qualified domain name of the NNMi management server, use the `nnmsetofficialfqdn.ovpl` command. For example:

```
nnmsetofficialfqdn.ovpl newnnmi.servers.example.com
```

For more information, see the *nnmsetofficialfqdn.ovpl* reference page, or the UNIX manpage.

Task 4: Update the HTTPS Configuration with the New Certificate

Configure the Tomcat server by editing the following file:

```
$jboss.home.dir/server/nms/deploy/jboss-web.deployer/server.xml
```

The default value of `$jboss.home.dir` is as follows:

- *Windows*: `%NnmInstallDir%\nonOV\jboss\nms`
- *UNIX*: `$NnmInstallDir/nonOV/jboss/nms`

If the NNMi web server uses the HTTPS protocol, update the HTTPS configuration by following these steps:

1. Open the `server.xml` file in any text editor.
2. In the uncommented https connector block, change the value of the `keyAlias` parameter to match the alias value you used for the new certificate in Task 2: Create a New NNMi Public Key Certificate.
3. Save the `server.xml` file.

Task 5: Restart, Update, and Refresh Systems

1. Start NNMi:

   ```
   ovstart
   ```

2. Update the connectivity between the NNMi management server and any NNM iSPIs running on dedicated servers to use the new fully-qualified domain name of the NNMi management server.
3. Update the connectivity between the NNMi management server and any integrated applications to use the new fully-qualified domain name of the NNMi management server.

   If necessary, update the single sign-on configuration for the integrated application to trust the new NNMi certificate.

4. If the NNMi database contains any encrypted data (such as SNMPv3 passphrases), this data was encrypted with the old security key. The new security key cannot decrypt the data. Contact your support representative for assistance deleting and recreating these configuration items.

Task 6: Back up NNMi

Follow your standard procedure to take a complete NNMi backup.

⚠ Restoring NNMi from a backup made before changing the name of the NNMi management server overwrites the nnm.keystore file, thereby making the NNMi database inaccessible. To restore NNMi data from an old backup, contact your support representative for assistance.

Changing the Oracle Database Instance Connection Information

NNMi can be connected to one Oracle database instance at a time. You can configure this connection.

Reasons to change the Oracle database instance connection information include the following:

- The Oracle database server name must be changed.
- The port for connecting to the database conflicts with another process, or corporate policies require the use of a non-default port.
- The database instance must be renamed (for example, to meet corporate policies).
- The Oracle database server hardware must be changed.

To change the Oracle database instance that NNMi uses, complete the following tasks:

- Task 1: Update the Oracle Database Instance
- Task 2: Update the NNMi Configuration

Task 1: Update the Oracle Database Instance

1 Stop NNMi:

```
ovstop
```

2 Prepare the Oracle database by moving the database, renaming the Oracle database server, or other necessary changes.

3 Verify that the target Oracle database instance meets the following prerequisites:

- The database instance exists.
- The database instance is populated with current NNMi data.

  Use Oracle tools to copy NNMi data from the working database instance to the target database instance.
- The database instance is running.

Task 2: Update the NNMi Configuration

1 Back up the database connection configuration file:

a Change to the following directory:

— *Windows*: `%NnmInstallDir%\nonOV\jboss\nms\server\nms\`

— *UNIX*: `$NnmInstallDir/nonOV/jboss/nms/server/nms/`

b Within the `nms` directory, create a directory called `deploy.save`.

c Copy the `nms-ds.xml` file from the `deploy` directory to the `deploy.save` directory.

⚠ At startup, the `ovjboss` process reads all files in the `deploy` directory hierarchy. For this reason, save backup copies of the deployed files in a location outside of the `deploy` directory hierarchy, as we do here with the `deploy.save` directory.

2 Edit the database connection configuration file:

a Change to the `deploy` directory.

b. In any text editor, open the `nms-ds.xml` file.

c. Locate the `connection-url` entry.

   For example:

```
<connection-url>jdbc:oracle:thin:@ohost:1521:nnmidb1</connection-url>
```

   The last three parameters in this entry are of interest. They are of the format oracle_hostname:database_port:database_instance_name

d. Change one or more of the fourth, fifth, and sixth parameters in the `connection-url` entry.

   For example:

   — To point to a different Oracle database server, change `ohost` to another hostname.

   — To connect to the Oracle database server on a different port, change `1521` to another port number.

   — To connect to a different Oracle database instance, change `nnmidb1` to another database instance name. (This database instance must already exist!)

e. Save the `nms-ds.xml` file.

3. Start NNMi:

```
ovstart
```

Changing the Password that NNMi Uses to Connect to the Oracle Database Instance

If you change the Oracle configuration to use a different password for connecting to the NNMi database instance, update the NNMi configuration by following these steps:

1. Shut down NNMi:

```
ovstop
```

2. Run the `nnmchangedbpw.ovpl` command and follow the prompts.

3. Start NNMi:

```
ovstart
```

For more information, see the *nnmchangedbpw.ovpl* reference page, or the UNIX manpage.

Copying a Tablespace to a Different Oracle Database

Database administration often requests database changes, creating the need to copy tablespaces to different databases. If you have the need to copy an Oracle tablespace used by NNMi to a different Oracle database, do the following:

1 Point your browser to the following location and use the Oracle 11g documentation to copy the tablespace to the target database.
http://download.oracle.com/docs/cd/B28359_01/server.111/b28310/tspaces013.htm

2 Stop NNMi:

```
ovstop
```

3 Edit the following file:

— Windows: `%NnmInstallDir%\nonOV\jboss\nms\server\nms\nms-ds.xml`

— UNIX: `$NnmInstallDir/nonOV/jboss/nms/server/nms/nms-ds.xml`

4 Locate the following line:

```
<connection-url>jdbc:oracle:thin:@oraclesystem:port:oraclesid</
connection-url>
```

5 Change the line to the new values and save your work.

6 Start NNMi:

```
ovstart
```

7 If the NNMi user password changed, run the **`nnmchangedbpw.ovpl`** script to update the user name and password used to authenticate with the NNMi database. See the *nnmchangedbpw.ovpl* reference page, or the UNIX manpage, for more information.

Running NNMi in a Xen Virtualization Environment

Xen is an OpenSource virtualization environment for Linux. Xen has a low-level hypervisor that permits you to create virtual machines that run operating systems such as Windows or Linux. It also allows snapshots and provides other features similar to VMWare.

If Xen is already present before installing NNMi, then the NNMi installation process automatically fixes issues with the Xen virtual interface.

This chapter contains the following topics:

- Problems after Installing Xen on a Functioning NNMi Management Server

Problems after Installing Xen on a Functioning NNMi Management Server

Suppose you install NNMi 9.10 on a server, and have NNMi functioning correctly in a production environment. If you install Xen on this NNMi management server, Xen changes the network routing tables on the NNMi management server so that all packets, including packets destined for the loopback address, go through the Xen virtual interface. If you run the **`ifconfig -a`** command on the NNMi management server, you see that Xen's virtual address shows up as `virbr0`. The result of installing Xen on the NNMi management server is that NNMi might stop functioning correctly, as several NNMi processes need to communicate using the NNMi management server's loopback address. Now the `virbr0` virtual interface responds instead of the NNMi management server's loopback address, causing communication problems within NNMi.

➤ Do not run NNMi in a virtual machine running inside of Xen, as that is not a supported configuration.

To remedy this issue, do the following:

1 Stop all NNMi processes using the **`kill`** command.

➤ You must use the **`kill`** command. Due to the `virbr0` virtual interface issue you can no longer use the **`ovstop`** command to communicate with NNMi's process manager, `ovspmd`.

2 Run the **ifconfig virbr0** command to display the IP address of the virbr0 interface. The rest of this procedure refers to the displayed IP address as *IP_Address*.

3 Edit the following file: $NNM_SHARED_CONF/ovspmd.auth

4 Add a line at the end of the text, including the IP address from step 2 and the plus + symbol. Use the following example: *IP_Address* +

5 If you plan to use NNMi with the embedded database, do the following:

   a Edit the following file: $NNM_DATA/shared/nnm/databases/Postgres/pg_hba.conf.

   b Add the following line, including the IP address from step 2: host all all IP_Address/32 trust

6 Start the NNMi processes using the **ovstart -c** command. The NNMi management server should run as normal.

Upgrading from NNMi 9.0x

For information about upgrading from NNM 6.x/7.x to NNMi 9.10, see the *NNMi Upgrade Reference*.

You can upgrade NNMi according to the information show in Table 37. The information shown in Table 37 assumes you have NNMi 9.0x or newer installed on the NNMi management server.

Table 37 Supported NNMi Upgrades

NNMi Version	Upgrade to NNMi 9.10
NNMi 9.0x	Supported
NNMi 9.0x Patch 1	Supported
NNMi 9.0x Patch 2 (NNMi 9.01)	Supported
NNMi 9.0x Patch 3	Supported
NNMi 9.0x Patch 4 or newer	Supported

To upgrade from NNMi 9.0x to NNMi 9.10, you must upgrade directly to NNMi 9.10. During an upgrade from NNMi 9.0x to NNMi 9.10, the installation script provides an opportunity to install patches, such as NNMi 9.1x Patch 5 (or newer patch level).

If you plan to upgrade an earlier version of NNMi 9.0x that is running in an NNMi application failover configuration, the supported upgrade path is to temporarily unconfigure application failover, upgrade the NNMi management server to NNMi 9.10,and then reconfigure application failover. For detailed information, see Application Failover and Upgrading to NNMi 9.10 on page 288.

If you plan to upgrade an earlier version of NNMi 9.0x that is running under high availability (HA), see Upgrading NNMi under HA from NNMi 9.0x to NNMi 9.10 on page 332.

If you plan to upgrade NNMi management servers configured in a global network management environment see Upgrading from NNMi 9.0x to NNMi 9.10 on page 255.

If you plan to upgrade a Linux NNMi management server from NNMi 9.0x to NNMi 9.10, you must import the HP public key into the Linux RPM database before installing NNMi 9.10. To do this, point your browser to the following location and follow the instructions:

```
 https://h20392.www2.hp.com/portal/swdepot/
displayProductInfo.do?productNumber=HPLinuxCodeSigning
```

There are several upgrade scenarios you could encounter. This section contains the following chapters:

- Upgrading the NNMi Management Server in Place, which describes the following upgrade scenario:
  - Upgrading from NNMi 9.0x to NNMi 9.10 on the same hardware and operating system.
- Upgrading to a Different NNMi Management Server, which describes the following upgrade scenario:
  - Upgrading from NNMi 9.0x to NNMi 9.10 on the same version operating system.
- Moving NNMi from Windows 2003 to Windows 2008. NNMi 9.10 does not support Windows 2003. You must change the operating system to Windows 2008 before upgrading to NNMi 9.10.
- Migrating NNMi Oracle Data. Explains the steps to take to move the Oracle data used by your NNMi management server from one Oracle database instance to another.
- Additional Upgrade Information. Explains some areas that NNMi 9.10 differs from earlier versions of NNMi.

Upgrading the NNMi Management Server in Place

This chapter describes the process for upgrading an existing NNMi management server to NNMi 9.1x Patch 5.

This chapter contains the following topic:

Upgrade an Existing NNMi Management Server to NNMi 9.1x Patch 5

Read the NNMi 9.1x Patch 5 *Preinstallation Checklist* chapter in the *NNMi Installation Guide* and Additional Upgrade Information on page 413 before continuing. There are notable changes to the *NNMi Installation Guide*. For example, if you use an Oracle database instance instead of the embedded database, you should set the FLASHBACK ANY TABLE permission, as this enables NNMi to create restore points during migration.

Read the *HP Network Node Manager i Software System and Device Support Matrix* for the NNMi software you are upgrading to before continuing. You can obtain a copy of this document at http://h20230.www2.hp.com/selfsolve/manuals. You must have an HP Passport User ID to access this web site.

The following steps explain how to upgrade an NNMi management server to NNMi 9.1x Patch 5. The following steps assume you have NNMi 9.0x running on the NNMi management server.

1 Back up the NNMi management server using the `nnmbackup.ovpl` script. Do this as a precaution, as you would only use this backup in the unlikely event of a failed migration. For more information, see the *nnmbackup.ovpl* reference page, or the UNIX manpage.

2 *Oracle Database Only*: If the NNMi management server uses an Oracle database, have your Oracle database administrator back up the NNMi data. As mentioned earlier, have your Oracle database administrator set the FLASHBACK ANY TABLE permission, as this enables NNMi to create restore points during migration

3 *Oracle Database Only*: Use the `nnmconfigexport.ovpl` script to back up configuration information from the NNMi management server. Do this as a precaution, as you would only use this backup in the unlikely event of a failed migration. For more information, see the *nmconfigexport.ovpl* or *nnmconfigimport.ovpl* reference pages, or the UNIX manpages.

⚠ Never edit a file exported with the `nnmconfigexport.ovpl` script before using the `nnmconfigimport.ovpl` script to import the file.

4 Install NNMi 9.1x Patch 5on the NNMi management server using instructions from the *NNMi Installation Guide*.

➤ *Oracle Database Only*: If your Oracle database administrator does not set the FLASHBACK ANY TABLE permission, you will see a warning about that missing permission after the install completes. You can ignore this warning.

5 Verify that the information from the NNMi management server migrated successfully.

Upgrading to a Different NNMi Management Server

This chapter describes the process for upgrading to NNMi 9.10 on a new system while maintaining the configuration of the existing NNMi management server.

This chapter contains the following topic:

- Upgrade to a Different NNMi Management Server

Upgrade to a Different NNMi Management Server

Read the NNMi 9.10 *Preinstallation Checklist* chapter in the *NNMi Installation Guide* and Additional Upgrade Information on page 413 before continuing. There are notable changes to the *NNMi Installation Guide*. For example, if you use an Oracle database instance instead of the embedded database, you should set the FLASHBACK ANY TABLE permission, as this enables NNMi to create restore points during migration.

The following steps explain how to copy data from an existing NNMi management server to a target NNMi management server. The following steps assume you have NNMi 9.0x running on the existing NNMi management server.

If you want to change the Oracle database server, complete that process before or after the upgrade to NNMi 9.1x Patch 5. For information, see Migrating NNMi Oracle Data on page 411.

1. As a precaution, back up the existing (source) NNMi 9.0x management server using the `nnmbackup.ovpl` script. Label this backup for NNMi 9.0x. For more information, see the *nnmbackup.ovpl* reference page, or the UNIX manpage for NNMi 9.0x.
2. If the existing (source) NNMi management server uses an Oracle database, have your Oracle database administrator back up the NNMi 9.0x data. As mentioned earlier, have your Oracle database administrator set the FLASHBACK ANY TABLE permission, as this enables NNMi to create restore points during migration.

3 Install NNMi 9.10 and the latest consolidated patch (if any) on the source NNMi management server using instructions from the *NNMi Installation Guide*.

➤ *Oracle Database Only*: If your Oracle database administrator does not set the FLASHBACK ANY TABLE permission, you will see a warning about that missing permission after the install completes. You can ignore this warning.

4 Verify that NNMi 9.10 is working correctly on the source NNMi management server.

5 Back up NNMi 9.10 on the source NNMi management server using the `nnmbackup.ovpl` script. Label this backup for NNMi 9.10. You will need it to copy data to the target NNMi management server. For more information, see the *nnmbackup.ovpl* reference page, or the UNIX manpage for NNMi 9.10.

6 Install NNMi 9.10 and the latest consolidated patch (if any) on the target NNMi management server using instructions from the *NNMi Installation Guide*. To migrate the data from step 5, the target NNMi management server must be running the same operating system version. NNMi does not support data migration to an NNMi management server running on a different operating system.

7 Use the `nnmrestore.ovpl` script to copy NNMi database information to the target server. For more information, see the *nnmrestore.ovpl* reference page, or the UNIX manpage.

8 Obtain and install a new license on the target NNMi management server.

For information, see Licensing NNMi on page 117.

9 Verify that the information from the target NNMi management server migrated successfully from the existing NNMi management server.

Moving NNMi from Windows 2003 to Windows 2008

NNMi 9.10 does not support Windows 2003. You must change the operating system to Windows 2008 before migrating to NNMi 9.10.

Use the information in this chapter if you have NNMi 9.0x patch 3 or later running on a Windows 2003 server, and need to change the operating system to Windows 2008.

This chapter contains the following topic:

Changing NNMi from Windows 2003 to Windows 2008

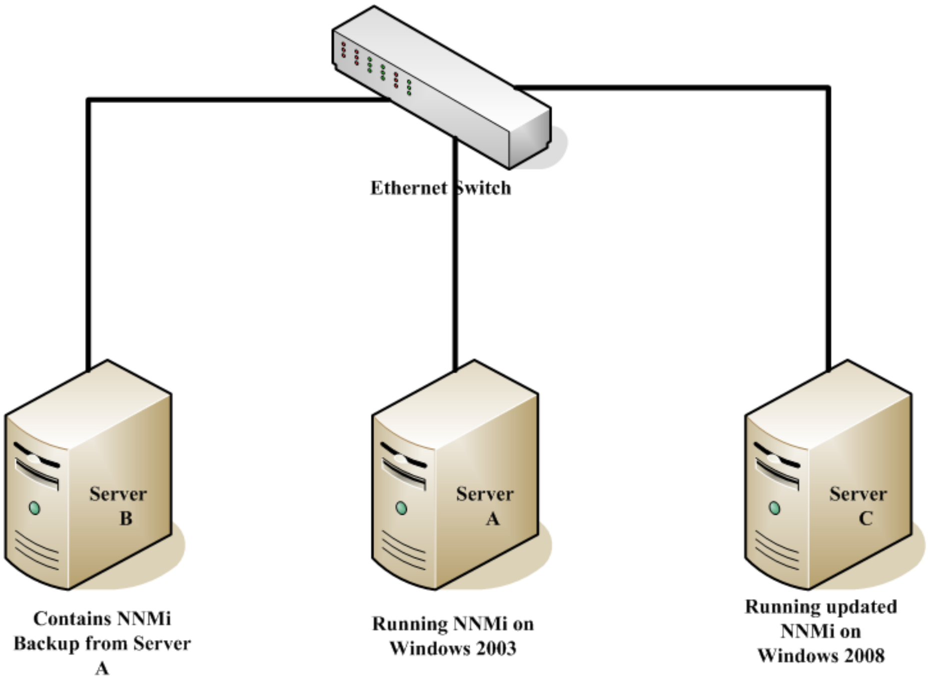
To complete the following steps, you must have NNMi 9.0x patch 3 or later running on a Windows 2003 server. To check the NNMi version number, note the current patch level in the **Help->About HP Network Node Manager i Software** window. Verify that the version is 9.01.003 or later. If the version is earlier than that, do not proceed. Install NNMi 9.0x patch 3 or later before proceeding.

To change an NNMi management server running NNMi 9.0x patch 3 or later from Windows 2003 to Windows 2008, follow these steps:

1 Identify three servers that you will use during this procedure:

- `Server A` is the current NNMi management server running Windows 2003.
- `Server B` will hold the NNMi backup files.
- `Server C` will become the new NNMi management server running Windows 2008. This NNMi management server can be the same hardware as the current `Server A`.

  Make sure the `hosts` file on the new NNMi management server contains the following entry: **`127.0.0.1 localhost`**


Ethernet Switch
Server B
Server A
Server C
Contains NNMi Backup from Server A
Running NNMi on Windows 2003
Running updated NNMi on Windows 2008

2 On `Server A`, run the **`nnmbackup.ovpl -type online -scope all -target`** ***`temporary_location`*** command to complete a full NNMi backup.

For more information about which command options to use, see NNMi Backup and Restore Tools on page 353 and the *nnmbackup.ovpl* reference page, or the UNIX manpage.

3 On `Server A`, copy the backup you completed in step 2 to `Server B`.

4 On `Server C`, install Windows 2008.

As an alternative to using `Server C`, reformat the disk on `Server A` and install Windows 2008. If you do that, substitute `Server A` for `Server C` for the remaining steps.

5 On `Server C`, install NNMi 9.0x patch 3 or later. You must install the same patch level that NNMi `Server A` was at during the backup you completed in step 2.

6 During the NNMi installation on server C, the installation script might assign ports that differ from the server B configuration. During the configuration restore on Server C, this might create port conflicts. To remedy this, do the following:

a On `Server C`, navigate to the following directory: `%$NNM_CONF%\nnm\props\`

b On `Server C`, copy the `nms-local.properties` file to `nms-local.properties.save in` a temporary location.

c On `Server B`, copy the NNMi backup to `Server C`.

d On `Server C`, run the **`nnmrestore.ovpl -force -source`** ***`temporary_location`*** command to complete a full NNMi restore.

For more information about which command options to use, see NNMi Backup and Restore Tools on page 353 and the *nnmrestore.ovpl* reference page, or the UNIX manpage.

Use the command options that match the backup you completed in step 2 e On `Server C`, compare the `nms-local.properties.save` file from the temporary location to the `nms-local.properties` file located in the following directory: `%NNM_CONF%\nnm\props\`

Resolve any port conflicts, making changes to the `nms-local.properties` located in the above directory. Make sure to keep the `jboss.http.port` (NNMi web server port) and `jboss.https.port` (NNMi HTTPS web server port) values that were chosen during the NNMi installation on `Server C`.

f Restart NNMi:

```
ovstop
```

```
ovstart
```

7 NNMi associates its license keys with a server's IP address. If the IP address for `Server C` is different from the IP address of `Server A`, obtain and install new NNMi license keys. See Changing the IP Address of a Standalone NNMi Management Server on page 392.

8 On `Server C`, install NNMi 9.10.

Migrating NNMi Oracle Data

If you plan to move the Oracle data in NNMi to Oracle 11G. The information in this chapter explains the steps to take to complete this work.

Migrating NNMi Oracle Data

Suppose you have NNMi running in one of the following configurations:

- NNMi 9.0x with the latest patch connected to an Oracle 10G database and you must upgrade to NNMi 9.10.
- NNMi 9.0x with the latest patch connected to an Oracle 11G database and you must upgrade to NNMi 9.10.

The Oracle database instance migration you must complete could include combinations of the following requirements:

- The existing Oracle instance running on NNMi 9.10 can be running Oracle 10G or 11G.
- The new Oracle instance running on NNMi 9.10 must be running Oracle 11G.
- The new Oracle instance can be located on the original server or on a different server and hostname.

To complete the migration of the NNMi Oracle data, complete the following steps:

1. As root or administrator, run the following command to stop NNMi: **`ovstop -c`**.
2. Use Oracle tools to move or copy the NNMi data from the existing Oracle server to the new server. See your Oracle documentation for additional information.

   This Oracle data migration can be an in-place upgrade from Oracle 10 to Oracle 11 on the same server. Oracle provides database migration tools for converting Oracle 10 data into the Oracle 11 format.

3. *Only complete this step if the new Oracle server has a different hostname than the previous Oracle server.* On the NNMi management server, reconfigure NNMi to point to the new Oracle server by completing the following steps:

a. Edit the datasource configuration file shown below:

   It is important that you complete the following steps accurately, or jboss will not correctly connect to the Oracle 11G database.

   — *Windows*: `%NNM_JBOSS%\server\nms\deploy\nms-ds.xml`

   — *UNIX*: `$NNM_JBOSS/server/nms/deploy/nms-ds.xml`

b. Change the following attribute to reflect your new server

   OLD:
   <connection-url>jdbc:oracle:thin:@*EXISTING_FQDN*:*EXISTING_ORACLE_PORT*:*EXISTING_SID* </connection-url>

   NEW:
   <connection-url>jdbc:oracle:thin:@NEW_*FQDN*:*NEW_PORT*:*NEW_SID*</connection-url>

4. Complete one of the following actions:

   If you are upgrading from NNMi 9.0x to NNMi 9.10, perform that migration now, following the installation instructions in the *HP Network Node Manager i Software Installation Guide*.

   If you are already using NNMi 9.10, follow these steps to restart NNMi and complete the Oracle database move/migration:

   a. Run the following command on the NNMi management server to restart NNMi: **`ovstart -c`**

   b. Run the following command on the NNMi management server to check if all of the services are started and operating correctly: **`ovstatus -v`**

Additional Upgrade Information

This chapter describes some changes between NNMi 9.10 and earlier NNMi versions. This chapter contains the following topics:

- Configuration Differences
- MIBs
- Functionality Differences

Configuration Differences

- User groups replace NNMi roles for limiting user access within the NNMi console. User accounts can be mapped to multiple user groups.
  - For signing in to the NNMi console, each user account must be mapped to at least one of the NNMi-provided user groups. These groups are equivalent to the function of the NNMi role in previous releases.
  - In a multi-tenancy environment, each user account can be mapped to one or more custom user groups that provide access to a subset of the topology objects.

  For more information, see NNMi Security and Multi-Tenancy on page 199.
- The NNMi integration for retrieving user information from a directory service can now retrieve multiple group names per user.
  - For configuration option 2 (only user names and passwords in the directory service), existing integrations with a directory service continue to work without modification to the `ldap.properties` configuration file.
  - For configuration option 3 (all user information in the directory service), the following information applies:
    - In a single tenant environment (all NNMi console users can access all topology objects), existing integrations with a directory service continue to work without modification to the `ldap.properties` configuration file.

If you add any new NNMi user groups in the directory service, you must update the ldap.properties configuration file to the new model for retrieving user information from a directory service.

    - In a multi-tenancy environment, update the ldap.properties configuration file to the new model for retrieving user information from a directory service.
    - For information about updating the ldap.properties configuration file, see Changing the Directory Service Access Configuration to Support the NNMi Security Model on page 178.
  - NNMi 9.10 deprecates the following ldap.properties configuration file parameters. They will become unsupported in a future release:
    - roleAttributeID
    - roleAttributeIsDN
    - roleNameAttributeID
- After upgrading to NNMi 9.1x Patch 5, the following security and multi-tenancy configuration applies:
  - All nodes are assigned to the Default Tenant and the Default Security Group.
  - All users can access all nodes in the NNMi topology and all incidents.

  This default configuration matches the object access available in NNMi 9.0x. For information about customizing object access, see NNMi Security and Multi-Tenancy on page 199.
- If the HP NNMi—HP NA integration was configured on a NNMi 9.0x management server, the process of upgrading to NNMi 9.10 disables the configuration. For more information, see Integration Configuration Upgraded from NNMi 9.0x on page 486.

Application Failover

NNMi 9.0x supported either a UDP or a TCP solution for the application failover feature. NNMi 9.1x Patch 5 only supports the TCP solution. If you used the UDP application failover solution for NNMi 9.0x, and are upgrading to NNMi 9.1x Patch 5, the upgrade script converts your application failover configuration to the TCP solution. You must add the hostnames of all nodes in the cluster to the `com.hp.ov.nms.cluster.member.hostnames` parameter in the `nms-cluster.properties` file. For more information see Configuring NNMi for Application Failover on page 276.

For the application failover feature to function correctly, the active and standby servers must have unrestricted network access to each other. NNMi 9.10 includes some port changes, so you might need to modify your firewall configuration. For more information see NNMi 9.10 and Well-Known Ports on page 643.

MIBs

If you loaded additional MIBs into earlier versions of NNMi that are not standards compliant or have dependencies on other MIB files, they might not migrate successfully. If a MIB does not migrate successfully, the trap configurations continue to work, however you might not be able to browse that MIB as you could before the migration.

If you suspect that some MIBs did not migrate, check the following directory for a `failed` subdirectory that contains the MIB file or files, failure details, and a log file with a name that associates it with the MIB file or files:

- *Windows*: `%NNM_DATA%\tmp\nnm9xMibMigrate`
- *UNIX*: `$NNM_DATA/tmp/nnm9xMibMigrate`

Use the files contained in the above directories to determine why the MIBs did not migrate, then reload those MIBs.

Functionality Differences

To review information about new features included in NNMi 9.10, see the *What's New In This Version* section of the *NNMi Release Notes*.

Integrations with NNMi

This section contains the following chapters:

- CiscoWorks LAN Management Solution
- Clarus Systems ClarusIPC Plus$^+$
- HP ArcSight Logger
- HP Asset Manager
- HP Business Service Management Topology
- HP Universal CMDB
- HP Business Availability Center My BSM
- HP Network Automation
- PCM+
- HP RAMS MPLS WAN
- HP SiteScope
- HP Systems Insight Manager
- nGenius Performance Manager
- NNMi Northbound Interface
- HP BSM Operations Management
- HP Operations Manager
- HP NNMi Integration Module for Netcool Software
- xMatters (formerly AlarmPoint)

CiscoWorks LAN Management Solution

Cisco Systems CiscoWorks LAN Management Solution (CiscoWorks LMS) is an integrated suite of management tools for configuring, administering, monitoring, and troubleshooting Cisco networks.

This chapter contains the following topics:

HP NNMi–CiscoWorks LMS Integration

The HP NNMi–CiscoWorks LMS integration provides actions for accessing CiscoWorks LMS tools from the NNMi console.

Value

The HP NNMi–CiscoWorks LMS integration adds CiscoWorks LMS information to NNMi, so that NNMi users can detect and investigate potential network problems for Cisco devices.

Integrated Products

The information in this chapter applies to the following products:

- CiscoWorks LMS

  For the list of supported versions, see the *NNMi System and Device Support Matrix*.

- NNMi 9.10

NNMi and CiscoWorks LMS must be installed on separate computers. The NNMi management server and the CiscoWorks LMS server computer can be of the same or different operating systems.

For the most recent information about supported hardware platforms and operating systems for NNMi, see the *NNMi System and Device Support Matrix*.

For the most recent information about supported hardware platforms and operating systems for CiscoWorks LMS, see the documentation for your version. For example:

- CiscoWorks LMS version 3.1:

  http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/3.1/install/guide/prereq.html

- CiscoWorks LMS version 3.2:

  http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/3.2/install/guide1/prereq.html

Documentation

This chapter describes how to configure NNMi to communicate with CiscoWorks LMS and how to use the integration from the NNMi console.

Enabling the HP NNMi–CiscoWorks LMS Integration

On the NNMi management server, configure the connection between NNMi and CiscoWorks LMS by following these steps:

1. In the NNMi console, open the **HP NNMi–CiscoWorks LMS Integration Configuration** form (**Integration Module Configuration > CiscoWorks LMS**).
2. Select the **Enable Integration** check box to make the remaining fields on the form available.
3. Enter the information for connecting to the NNMi management server. For information about these fields, see NNMi Management Server Connection on page 423.
4. Enter the information for connecting to the CiscoWorks LMS server. For information about these fields, see CiscoWorks LMS Server Connection on page 424.

5 Click **Submit** at the bottom of the form.

A new window opens a status message. If the message indicates a problem with connecting to the NNMi management server, click **Return**, and then adjust the values as suggested by the text of the error message.

6 Load the incident definitions for CiscoWorks LMS-managed devices:

a Change to the following directory:

— *Windows*: `%NnmInstallDir%\newconfig\HPOvNmsEvent`

— *UNIX*: `$NnmInstallDir/newconfig/HPOvNmsEvent`

b Import the CiscoWorks LMS incident definitions by entering the following command:

```
nnmconfigimport.ovpl -f nnm-cisco-incidentConfig.xml \
-u <username> -p <password>
```

7 Optional and recommended. Load the MIB definition files for the traps that CiscoWorks LMS-managed devices generate:

a Obtain the appropriate MIB files from the device media or the Cisco web site:

tools.cisco.com/Support/SNMP/do/SearchOID.do?local=en&step=1

b Change to the directory where the MIB files are stored.

c Use the nnmloadmib.ovpl command to load the appropriate MIB files for the managed environment. For example:

```
nnmloadmib.ovpl -load cpqhost.mib -u <username> -p <password>
```

d Verify that the MIBs loaded correctly, by entering the following command:

```
nnmloadmib.ovpl -list -u <username> -p <password>
```

Using the HP NNMi–CiscoWorks LMS Integration

The HP NNMi–CiscoWorks LMS integration provides links from the NNMi console to CiscoWorks LMS. The integration does not provide single sign-on between the products. You must enter your CiscoWorks LMS user credentials to view the CiscoWorks LMS pages.

Enabling the HP NNMi–CiscoWorks LMS integration adds the following actions to the NNMi console:

- **CiscoWorks Device Center**—Opens the CiscoWorks Device Center in the context of the selected node.
- **CiscoWorks CiscoView**—Opens CiscoWorks CiscoView in the context of the selected node.

Changing the HP NNMi–CiscoWorks LMS Integration Configuration

1. In the NNMi console, open the **HP NNMi–CiscoWorks LMS Integration Configuration** form (**Integration Module Configuration > CiscoWorks LMS**).
2. Modify the values as appropriate. For information about the fields on this form, see HP NNMi–CiscoWorks LMS Integration Configuration Form Reference on page 423.
3. Verify that the **Enable Integration** check box at the top of the form is selected, and then click **Submit** at the bottom of the form.

The changes take effect immediately. You do not need to restart `ovjboss`.

Disabling the HP NNMi–CiscoWorks LMS Integration

1. In the NNMi console, open the **HP NNMi–CiscoWorks LMS Integration Configuration** form (**Integration Module Configuration > CiscoWorks LMS**).
2. Clear the **Enable Integration** check box at the top of the form, and then click **Submit** at the bottom of the form. The integration actions are no longer available.

The changes take effect immediately. You do not need to restart `ovjboss`.

Troubleshooting the HP NNMi–CiscoWorks LMS Integration

CiscoWorks LMS Actions Do Not Work

If you have verified the values in the **HP NNMi–CiscoWorks LMS Integration Configuration** form and you are still not able to open a CiscoWorks LMS page from the NNMi console, do the following:

1. Clear the web browser cache.
2. Clear all saved form or password data from the web browser.
3. Close the web browser window completely, and then re-open it.
4. Re-enter the values in the **HP NNMi–CiscoWorks LMS Integration Configuration** form.
5. Verify that CiscoWorks LMS is running.

OID Not Found in the MIB Cache Message in Traps

If the MIB definition files for the traps that CiscoWorks LMS-managed devices generate are not loaded in NNMi, you might see an error similar to the following text:

<Cia .1.3.6.1.4.1.11.5.7.5.2.1.1.1.7.0 with value 1 was not found within the mib cache>

To resolve these errors, load the MIBs as described in step 7 on page 421.

HP NNMi–CiscoWorks LMS Integration Configuration Form Reference

The **HP NNMi–CiscoWorks LMS Integration Configuration** form contains the parameters for configuring communications between NNMi and CiscoWorks LMS. This form is available from the **Integration Module Configuration** workspace.

Only NNMi users with the Administrator role can access the **HP NNMi–CiscoWorks LMS Integration Configuration** form.

The **HP NNMi–CiscoWorks LMS Integration Configuration** form collects information for the following general areas:

- NNMi Management Server Connection
- CiscoWorks LMS Server Connection

To apply changes to the integration configuration, update the values on the **HP NNMi–CiscoWorks LMS Integration Configuration** form, and then click **Submit**.

NNMi Management Server Connection

Table 38 lists the parameters for connecting to the NNMi management server. This is the same information that you use to open the NNMi console. You can determine many of these values by examining the URL that invokes an NNMi console session. Coordinate with the NNMi administrator to determine the appropriate values for this section of the configuration form.

Table 38 NNMi Management Server Information

Field	Description
NNMi SSL Enabled	The connection protocol specification. • If the NNMi console is configured to use HTTPS, select the **NNMi SSL Enabled** check box. This is the default configuration. • If the NNMi console is configured to use HTTP, clear the **NNMi SSL Enabled** check box.
NNMi Host	The fully-qualified domain name of the NNMi management server. This field is pre-filled with the hostname that was used to access the NNMi console. Verify that this value is the name returned by the **`nnmofficialfqdn.ovpl -t`** command run on the NNMi management server.
NNMi Port	The port for connecting to the NNMi console. This field is pre-filled with the port that the jboss application server uses for communicating with the NNMi console, as specified in the following file: • *Windows*: `%NnmDataDir%\conf\nnm\props\nms-local.properties` • *UNIX*: `$NnmDataDir/conf/nnm/props/nms-local.properties` For non-SSL connections, use the value of `jboss.http.port`, which is `80` or `8004` by default (depending on the presence of another web server when NNMi was installed). For SSL connections, use the value of `jboss.https.port`, which is `443` by default.

Table 38 NNMi Management Server Information (cont'd)

Field	Description
NNMi User	The user name for connecting to the NNMi console. This user must have the NNMi Administrator or Web Service Client role.
NNMi Password	The password for the specified NNMi user.

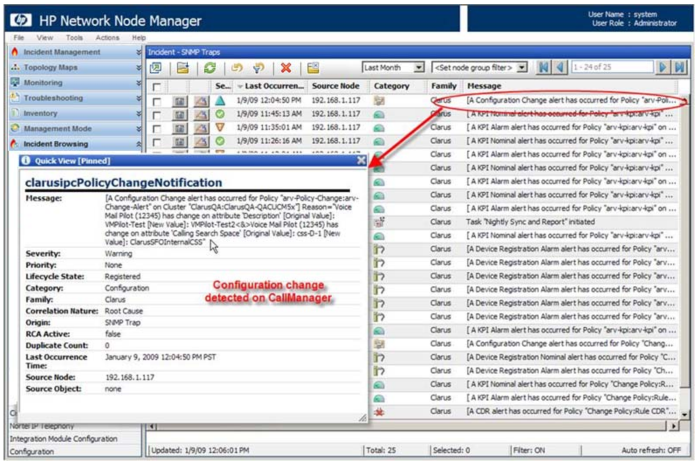
CiscoWorks LMS Server Connection

Table 39 lists the parameters for connecting to the CiscoWorks LMS server to open CiscoWorks LMS pages. Coordinate with the CiscoWorks LMS administrator to determine the appropriate values for this section of the configuration.

Table 39 CiscoWorks LMS Management Server Information

CiscoWorks LMS Server Parameter	Description
CiscoWorks LMS SSL Enabled	The connection protocol specification for connecting to CiscoWorks LMS. • If CiscoWorks LMS is configured to use HTTPS, select the **CiscoWorks LMS SSL Enabled** check box. This is the default configuration. • If CiscoWorks LMS is configured to use HTTP, clear the **CiscoWorks LMS SSL Enabled** check box.
CiscoWorks LMS Host	The fully-qualified domain name of the CiscoWorks LMS server.
CiscoWorks LMS Port	The port for connecting to the CiscoWorks LMS web services. If you are using the default CiscoWorks LMS configuration, use port `1741` (for non-SSL connections to CiscoWorks LMS) or port `443` (for SSL connections to CiscoWorks LMS).

Clarus Systems ClarusIPC Plus+



Se...	Last Occurren...	Source Node	Category	Family	Message
	1/9/09 12:04:50 PM	192.168.1.117		Clarus	[A Configuration Change alert has occurred for Policy "arv-Poli...
	1/9/09 11:45:13 AM	192.168.1.117		Clarus	[A KPI Nominal alert has occurred for Policy "arv-kpi:arv-kpi" ...
	1/9/09 11:35:01 AM	192.168.1.117		Clarus	[A KPI Alarm alert has occurred for Policy "arv-kpi:arv-kpi" on ...
	1/9/09 11:26:16 AM	192.168.1.117		Clarus	[A KPI Nominal alert has occurred for Policy "arv-kpi:arv-kpi" ...
				Clarus	[A KPI Alarm alert has occurred for Policy "arv-kpi:arv-kpi" on ...
				Clarus	[A KPI Nominal alert has occurred for Policy "arv-kpi:arv-kpi" ...
				Clarus	[A KPI Alarm alert has occurred for Policy "arv-kpi:arv-kpi" on ...
				Clarus	[A KPI Nominal alert has occurred for Policy "arv-kpi:arv-kpi" ...
				Clarus	[A KPI Alarm alert has occurred for Policy "arv-kpi:arv-kpi" on ...
				Clarus	Task "Nightly Sync and Report" initiated
				Clarus	[A KPI Nominal alert has occurred for Policy "arv-kpi:arv-kpi" ...
				Clarus	[A Device Registration Alarm alert has occurred for Policy "arv...
				Clarus	[A Device Registration Alarm alert has occurred for Policy "arv...
				Clarus	[A Device Registration Alarm alert has occurred for Policy "arv...
				Clarus	[A Device Registration Alarm alert has occurred for Policy "arv...
				Clarus	[A Device Registration Alarm alert has occurred for Policy "arv...
				Clarus	[A Device Registration Alarm alert has occurred for Policy "arv...
				Clarus	[A KPI Alarm alert has occurred for Policy "arv-kpi:arv-kpi" on ...
				Clarus	[A Configuration Change alert has occurred for Policy "Chang...
				Clarus	[A Device Registration Nominal alert has occurred for Policy "C...
				Clarus	[A Device Registration Alarm alert has occurred for Policy "Ch...
				Clarus	[A KPI Nominal alert has occurred for Policy "Change Policy:R...
				Clarus	[A KPI Alarm alert has occurred for Policy "Change Policy:Rule...
				Clarus	[A CDR alert has occurred for Policy "Change Policy:Rule CDR"...

Updated: 1/9/09 12:06:01 PM | Total: 25 | Selected: 0 | Filter: ON | Auto refresh: OFF

Quick View [Pinned]

clarusipcPolicyChangeNotification

Message:	[A Configuration Change alert has occurred for Policy "arv-Policy-Change:arv-Change-Alert" on Cluster "ClarusQA:ClarusQA-QACUCM5x"] Reason="Voice Mail Pilot (12345) has change on attribute 'Description' [Original Value]: VMPilot-Test [New Value]: VMPilot-Test2<&>Voice Mail Pilot (12345) has change on attribute 'Calling Search Space' [Original Value]: css-D-1 [New Value]: ClarusSFOInternalCSS"
Severity:	Warning
Priority:	None
Lifecycle State:	Registered
Category:	Configuration
Family:	Clarus
Correlation Nature:	Root Cause
Origin:	SNMP Trap
RCA Active:	false
Duplicate Count:	0
Last Occurrence Time:	January 9, 2009 12:04:50 PM PST
Source Node:	192.168.1.117
Source Object:	none

Clarus Systems ClarusIPC Plus+ provides voice service testing; remote diagnostics of IP phone features; call detail record (CDR) based alerting and tracking; and reporting of configurations for Cisco Unified Communications Manager IP telephony systems during new deployments, upgrades, and ongoing operations.

Clarus Systems offers an integration of ClarusIPC Plus+ with HP Network Node Manager i Software (NNMi). HP offers an integration of ClarusIPC Plus+ with the NNM iSPI for IP Telephony. These integrations are mutually exclusive.

This chapter describes the available integrations:

- HP NNMi–Clarus Systems ClarusIPC Plus+ Integration
- HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus+ Integration

HP NNMi–Clarus Systems ClarusIPC Plus+ Integration

This section contains the following topics:

- About the HP NNMi–Clarus Systems ClarusIPC Plus+ Integration on page 426
- Enabling the HP NNMi–Clarus Systems ClarusIPC Plus+ Integration on page 426
- Using the HP NNMi–Clarus Systems ClarusIPC Plus+ Integration on page 427
- Disabling the HP NNMi–Clarus Systems ClarusIPC Plus+ Integration on page 427
- Troubleshooting the HP NNMi–Clarus Systems ClarusIPC Plus+ Integration on page 427

About the HP NNMi–Clarus Systems ClarusIPC Plus$^+$ Integration

Clarus Systems provides and supports the HP NNMi–Clarus Systems ClarusIPC Plus$^+$ integration. In this integration, ClarusIPC Plus$^+$ forwards SNMP traps regarding IP telephony service test results, alerts based on set CDR policies, or alerts based on the Unified Communications Manager Configuration change policies to NNMi, which then generates incidents regarding the status of the IP telephony configuration and devices. NNMi provides a consolidated view of the entire network.

The integration provides for accessing several ClarusIPC Plus$^+$ tools from these incidents in the NNMi console.

Value

The HP NNMi–Clarus Systems ClarusIPC Plus$^+$ integration consolidates IP telephony device management by providing access from the NNMi console to the ClarusIPC Plus$^+$ tools for IP telephony configuration change tracking and reporting.

Integrated Products

The information in this chapter applies to the following products:

- ClarusIPC Plus$^+$

  For the list of supported versions, see the *NNMi System and Device Support Matrix*.

- NNMi 9.10 on the Windows operating system only

Documentation

The HP NNMi–Clarus Systems ClarusIPC Plus$^+$ integration is fully described in the *ClarusIPC Plus$^+$ HP NNMi Software Integration Guide*, which is included in the integration installation package.

The ClarusIPC Plus$^+$ documentation suite contains additional documents that describe the ClarusIPC Plus$^+$ features and capabilities in detail. The documentation suite is available for download from the Clarus Systems web site at:

www.support.clarussystems.com

Enabling the HP NNMi–Clarus Systems ClarusIPC Plus$^+$ Integration

To obtain the HP NNMi–Clarus Systems ClarusIPC Plus$^+$ integration installation package, contact Clarus Systems support.

For information about enabling the integration, see the *ClarusIPC Plus$^+$ HP NNMi Software Integration Guide*, which is included in the integration installation package.

Using the HP NNMi–Clarus Systems ClarusIPC Plus$^+$ Integration

Enabling the HP NNMi–Clarus Systems ClarusIPC Plus$^+$ integration adds several URL actions to the NNMi console. For information about these URL actions, see the *ClarusIPC Plus$^+$ HP NNMi Software Integration Guide*.

ClarusIPC Plus$^+$ requires the use of the Microsoft Internet Explorer web browser. Open the NNMi console in Internet Explorer before launching a URL action that opens a ClarusIPC Plus$^+$ window.

Disabling the HP NNMi–Clarus Systems ClarusIPC Plus$^+$ Integration

For information about disabling the HP NNMi–Clarus Systems ClarusIPC Plus$^+$ integration, contact Clarus Systems support.

Troubleshooting the HP NNMi–Clarus Systems ClarusIPC Plus$^+$ Integration

For information about optimizing and extending the integration, and any currently known issues, see the *ClarusIPC Plus$^+$ HP NNMi Software Integration Guide*.

HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus$^+$ Integration

This section contains the following topics:

About the HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus$^+$ Integration

HP provides and supports the HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus$^+$ integration. With this integration, operators can access the ClarusIPC Plus$^+$ features pertaining to IP telephony service tests and diagnostics; Cisco Unified Communications Manager Configuration change reports; and CDR monitoring policies. ClarusIPC Plus$^+$ forwards SNMP traps regarding IP telephony service test results, alerts based on set CDR policies, or alerts based on the Unified Communications Manager Configuration change policies to NNMi, which then generates incidents regarding the status of the IP telephony configuration and devices. The NNM iSPI for IP Telephony provides the following:

- Workspaces and menus for launching to ClarusIPC Plus$^+$ configuration change reports, policies, test plans, and test results
- Launches to ClarusIPC Plus$^+$ remote diagnostics tools for IP phones in the context of the selected IP phone
- Launches to ClarusIPC Plus$^+$ test results, test details, and CDR policy details in the context of the alert incident selected in an NNMi incident view.

This integration provides access from the NNMi console to more ClarusIPC Plus$^+$ tools than does the integration without the NNM iSPI for IP Telephony.

Value

The HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus$^+$ integration adds advanced IP telephony service testing and diagnostics; CDR monitoring; and configuration change tracking and reporting to the NNM iSPI for IP Telephony.

Integrated Products

The information in this section applies to the following products:

- ClarusIPC Plus$^+$

  For the list of supported versions, see the *NNMi System and Device Support Matrix*.

- NNMi 9.10 with an NNM iSPI Network Engineering Toolset Software license
- NNM iSPI for IP Telephony 9.10

Documentation

The HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus$^+$ integration is fully described in the NNM iSPI for IP Telephony help, which is included with the iSPI.

The help (in PDF format) and additional NNM iSPI for IP Telephony documentation are available at:

http://h20230.www2.hp.com/selfsolve/manuals

Enabling the HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus$^+$ Integration

1 Prepare the NNMi management server:

a If the HP NNMi–Clarus Systems ClarusIPC Plus$^+$ integration (provided by Clarus Systems) is installed on the NNMi management server, uninstall that integration before enabling the integration between the NNM iSPI for IP Telephony and ClarusIPC Plus$^+$.

For information about how to uninstall the ClarusIPC Plus$^+$ integration package, contact Clarus Systems support.

b On the NNMi management server, install the following:

— The most recent NNMi consolidated patch (if any)

— The most recent NNM iSPI for IP Telephony consolidated patch (if any)

Patches are available at:

http://h20230.www2.hp.com/selfsolve/patches

2 On the NNMi management server, enable the HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus$^+$ integration as described in the NNM iSPI for IP Telephony help.

Using the HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus$^+$ Integration

Enabling the HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus$^+$ integration adds several workspaces, incident types, and URL actions to the NNMi console. For information about these URL actions, see the NNM iSPI for IP Telephony help.

ClarusIPC Plus$^+$ requires the use of the Microsoft Internet Explorer web browser. Open the NNMi console in Internet Explorer before launching a URL action that opens a ClarusIPC Plus$^+$ window.

Disabling the HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus$^+$ Integration

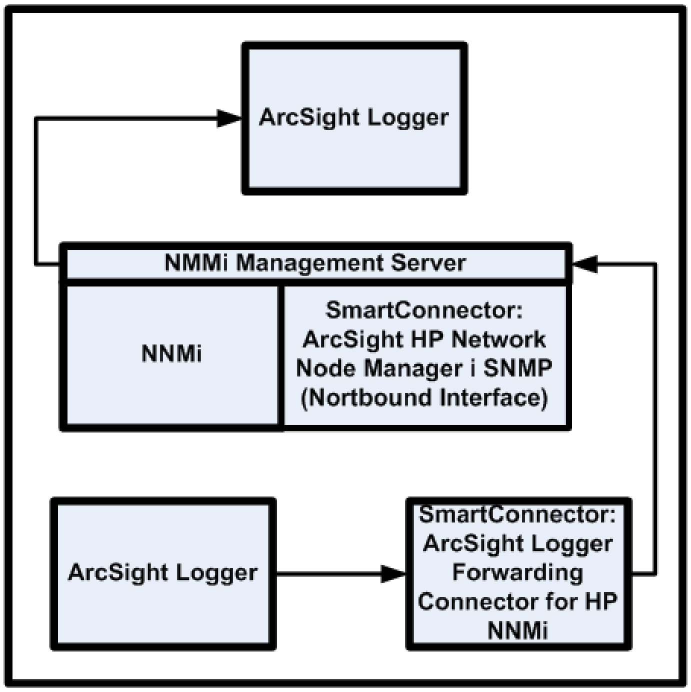
For information about disabling the HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus$^+$ integration, see the NNM iSPI for IP Telephony help.

Troubleshooting the HP NNM iSPI for IP Telephony–Clarus Systems ClarusIPC Plus$^+$ Integration

For information about optimizing and extending the integration, and any currently known issues, see the NNM iSPI for IP Telephony help.

For help troubleshooting problems with ClarusIPC Plus$^+$, contact Clarus Systems support.

HP ArcSight Logger


ArcSight Logger
NMMi Management Server
NNMi
SmartConnector: ArcSight HP Network Node Manager i SNMP (Nortbound Interface)
ArcSight Logger
SmartConnector: ArcSight Logger Forwarding Connector for HP NNMi

HP ArcSight Logger is a universal log management solution that unifies searching, reporting, alerting and analysis across any type of enterprise log data – making it unique in its ability to collect, analyze and store massive amounts of data generated by modern networks.

For information about purchasing HP ArcSight Logger, point your browser to http://www.arcsight.com/products.

.This chapter describes the available integrations:

- HP NNMi–HP ArcSight Logger Integration

HP NNMi–HP ArcSight Logger Integration

About the HP NNMi–HP ArcSight Logger

By using the instructions included in this chapter to configure HP ArcSight Logger (Logger) to forward `ArcSightEvents` to NNMi, a network operations staff can view Syslog incidents in the NNMi console.

Value

The HP NNMi–HP ArcSight Logger integration adds Syslog information to NNMi, so that NNMi users can view these Syslog messages and investigate potential problems.

Integrated Products

The information in this chapter applies to the following products:

- HP ArcSight Logger
- SmartConnector: ArcSight HP Network Node Manager i SNMP
- SmartConnector: ArcSight Logger Forwarding Connector for HP NNMi

For the list of supported Logger versions, see the *NNMi System and Device Support Matrix*.

- NNMi 9.1x Patch 5

For the most recent information about supported hardware platforms and operating systems, see the support matrices for both products.

Customizing the ArcSight Logger Filters

There are Syslog messages that pass the Logger filter and forward to NNMi. Without configuring the Logger filter, Logger forwards large quantities of `ArcSightEvents to` NNMi. This can adversely affect NNMi performance. *It is very important that you configure this filter promptly to limit the quantity of* `ArcSightEvents` *flowing from Logger to NNMi.* From the NNMi console, you can navigate to the Logger Filters configuration page. From there you can add, then maintain a Logger Filter to adjust the messages Logger forwards to NNMi.

It is a good practice to supply non-administrator (search only) credentials to open Logger from NNMi. If you enter administrator credentials, Logger permits NNMi users access to Logger with these administrator privileges, permitting you to make filter configuration changes. If you do not need to make Logger configuration changes, enter non-administrator credentials.

Documentation

Obtain and read to the following manuals to prepare for installing and configuring the NNMi - HP ArcSight Logger integration.

- *SmartConnector Configuration Guide for HP Network Node Manager i SNMP* (NNMi Northbound Interface)
  The SmartConnector for HP Network Node Manager i SNMP forwards NNMi incidents and other information to Logger.
- *SmartConnector Configuration Guide for ArcSight Logger Forwarding Connector for HP NNMi*
  The HP ArcSight Logger Forwarding Connector for HP NNMi forwards Syslog messages in the form of `ArcSightEvents` to NNMi.
- *Logger Administrator's Guide*
  For this integration, HP ArcSight Logger forwards SNMP traps in the form of `ArcSightEvents` to NNMi.

In addition to the *Logger Administrator's Guide*, Logger's integrated online help contains much of the same information as the *Logger Administrator's Guide.*

To obtain copies of HP ArcSight manuals, such as the *SmartConnector Configuration Guides* and the *Logger Administrator's Guide*, point your browser to the following location:
http://www.arcsight.com/supportportal
You must be an HP ArcSight customer (be able to provide user credentials) to access HP ArcSight product documentation.

To view the supported system requirements for HP ArcSight Logger, including the supported operating systems and browsers, point your browser to
http://www.arcsight.com/products/products-logger

Enabling the HP NNMi-HP ArcSight Logger Integration

You might have creatively used existing NNMi features, such as the NNMi northbound interface, to configure a custom integration between HP ArcSight Logger and NNMi. If you plan to install NNMi 9.1x Patch 5, disable this custom NNMi - HP ArcSight Logger integration. After you disable this custom integration, complete the tasks in this section to enable the more robust NNMi - HP ArcSight Logger integration delivered in NNMi 9.1x Patch 5.

Prerequisites

Before Enabling the NNMi - HP ArcSight Logger integration, do the following:

- Install NNMi 9.1x Patch 5. To assist you with this task, point your browser to http://support.openview.hp.com/selfsolve/manuals and download an interactive version of the *Network Node Manager i Installation Guide*.
- Install the SmartConnector for HP Network Node Manager i SNMP using instructions from the *SmartConnector Configuration Guide for HP Network Node Manager i SNMP* manual.

- Install the HP ArcSight Logger Forwarding Connector for HP NNMi using instructions from the *SmartConnector Configuration Guide for ArcSight Logger Forwarding Connector for HP NNMi* manual.

Steps to Enable the HP NNMi HP ArcSight Logger Integration

Complete the following tasks to enable the HP NNMi HP ArcSight Logger integration:

Task 1: Installing NNMi 9.1x Patch 5

Task 2: Loading the ArcSight MIBs

Task 3: Configuring the HP ArcSight Logger Forwarding Connector for HP NNMi

Task 4: Configuring the NNMi–HP ArcSight Integration

Task 5: Configuring the Logger Filter

Task 6: Configuring the SmartConnector for HP Network Node Manager i SNMP (Connector for Northbound Interface, Optional Task)

Task 7: Configuring NNMi to Forward SNMPv1, v2, and v3 Trap Incidents to Logger (Northbound Interface, Optional Task)

Task 1: Installing NNMi 9.1x Patch 5

To obtain and install NNMi 9.1x Patch 5, do the following:

1. Point your browser to http://support.openview.hp.com/selfsolve/patches.
2. Search for NNMi 9.1x Patch 5 for your operating system, then download the patch.
3. Install the patch according to the NNMi 9.1x Patch 5 installation instructions.

Task 2: Loading the ArcSight MIBs

After you complete Task 1 through Task 5, Logger begins forwarding filtered `ArcSightEvents` to NNMi. NNMi resolves interfaces and nodes to the source objects included in these `ArcSightEvents` without requiring you to load the ***hp-arcsight.mib*** *MIB*. However, by manually loading the ***hp-arcsight.mib*** *MIB*, you can use NNMi's **Node Action** > **MIB Information** feature to better understand the OIDs that are present in the `ArcSightEvent`.

During the NNMi 9.1x Patch 5 installation, the **hp-arcsight.mib** MIB is *installed* on the NNMi management server. *You must manually load the* ***hp-arcsight.mib*** *MIB*. Use the **nnmloadmib.ovpl** script to load the **hp-arcsight.mib** MIB into NNMi:

1. Run the following command to import the **hp-arcsight.mib** MIB:

   Windows:

   ```
   nnmloadmib.ovpl -load
   %NNM_SNMP_MIBS%\Vendor\Hewlett-Packard\hp-arcsight.mib -u
   <username> -p <password>
   ```

   UNIX:

   ```
   nnmloadmib.ovpl -load $NNM_SNMP_MIBS/Vendor/Hewlett-Packard/
   hp-arcsight.mib -u <username> -p <password>
   ```

   Verify that the displayed results include the **hp-arcsight.mib** MIB.

2 Verify that the MIBs loaded correctly, by doing one of the following:

   – Enter the following command:

   ```
   nnmloadmib.ovpl -list -u <username> -p <password>
   ```

   – From the NNMi console, navigate to **Configuration** > **MIBs** > **Loaded MIBs**. Verify the presence of the `hp-arcsight.mib` MIB you just loaded

Task 3: Configuring the HP ArcSight Logger Forwarding Connector for HP NNMi

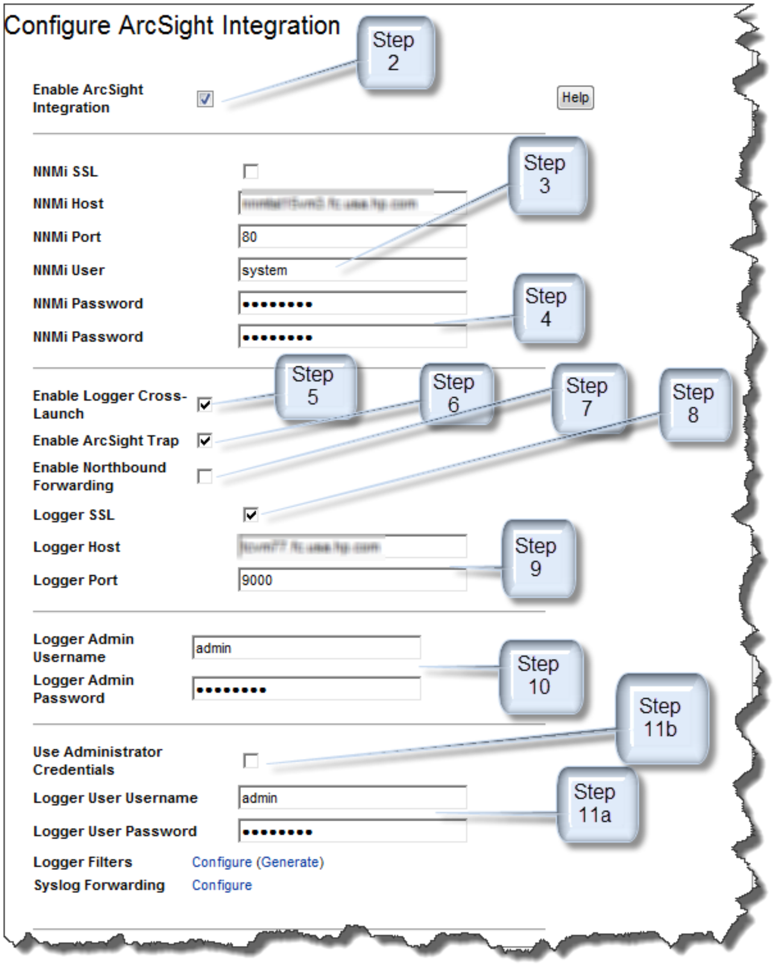
Configure the HP ArcSight Logger Forwarding Connector for HP NNMi using instructions from the *SmartConnector Configuration Guide for ArcSight Logger Forwarding Connector for HP NNMi* manual.

Task 4: Configuring the NNMi–HP ArcSight Integration

By enabling the NNMi - HP ArcSight Logger integration and the `ArcSightEvent`, along with configuring Logger to forward SNMP traps in the form of `ArcSightEvents`, NNMi can evaluate each `ArcSightEvent` content and display it as an SNMP trap or a Syslog message. See To enable the NNMi - HP ArcSight Logger integration complete the following steps:

1 From the NNMi console, click **Integration Module Configuration** > **HP ArcSight**. NNMi opens the **Configure ArcSight Integration** screen show in Figure 26. See Figure 26 while configuring the NNMi - HP ArcSight Logger integration.

Figure 26 Enabling the NNMi-HP ArcSight Logger Integration



Configure ArcSight Integration

Enable ArcSight Integration ☑

NNMi SSL ☐

NNMi Host [redacted]

NNMi Port 80

NNMi User system

NNMi Password ••••••••

NNMi Password ••••••••

Enable Logger Cross-Launch ☑

Enable ArcSight Trap ☑

Enable Northbound Forwarding ☐

Logger SSL ☑

Logger Host [redacted]

Logger Port 9000

Logger Admin Username admin

Logger Admin Password ••••••••

Use Administrator Credentials ☐

Logger User Username admin

Logger User Password ••••••••

Logger Filters Configure (Generate)

Syslog Forwarding Configure

2 Select **Enable ArcSight Integration**.

3 Add or observe the following NNMi integration information:

- `NNMi host`: This field contains the fully qualified domain name of the NNMi management server.
- `NNMi port`: This field contains the HTTP port number used for accessing NNMi. For more information see NNMi 9.10 and Well-Known Ports.
- `NNMi User`: Enter an NNMi username that is mapped to an NNMi administrator user group.

4 `NNMi Password`: Enter the username password. Verify this password with a second entry.

5 Select **Enable Logger Cross-Launch**.

6 Select **Enable ArcSight Trap**.

You can also do the following to enable the ArcSight Trap:

a From the NNMi console, click **Configuration** > **Incidents** > **SNMP Trap Configurations**.

b Click **ArcSightEvent** > **Open**.

c Select **Enabled**.

d Click **Save and Close**.

7 If you want to forward NNMi incidents to Logger, select **Enable Northbound Forwarding**.

8 Not all Logger applications are configured to use SSL. If the Logger application included in this NNMi - HP ArcSight Logger integration is configured to use SSL, select **Logger SSL**.

See the *HP ArcSight Logger v5.1 Administrators Guide* about configuring Logger for SSL.

9 Add the following Logger integration information:

- `Logger Host (the fully qualified domain name of the Logger Host)`
- `Logger Port`

10 Add the following Logger administrator credentials:

- `Logger Admin Username`
- `Logger Admin Password`

11 Complete step a. You can complete step b, however step a is the recommended method.

a Add the following user credentials for read-only cross-launches. Configure these credentials only if you want to use a read-only user within Logger:

- `Logger User Username`
- `Logger User Password`

b Select **Use Administrator Credentials**. This applies the administrator credentials to the Logger User Username and Logger User Password fields. Although this might be useful in some applications, selecting this option does give the NNMi level 1 operator full administrator privileges in Logger. For security purposes, step a is the recommended method.

12 Click **Submit** to save these changes.

13 For the cross-launch menu changes to become visible in the NNMi console, do the following:

a Sign out of NNMi.

b Sign in to NNMi.

Task 5: Configuring the Logger Filter

After completing Task 4, Logger begins forwarding unfiltered `ArcSightEvents to` NNMi. Logger can determine which Syslog messages to forward to NNMi using a filter you configure within Logger. *It is very important that you configure this filter promptly.* You can launch a tool from NNMi that will help you configure these filters.

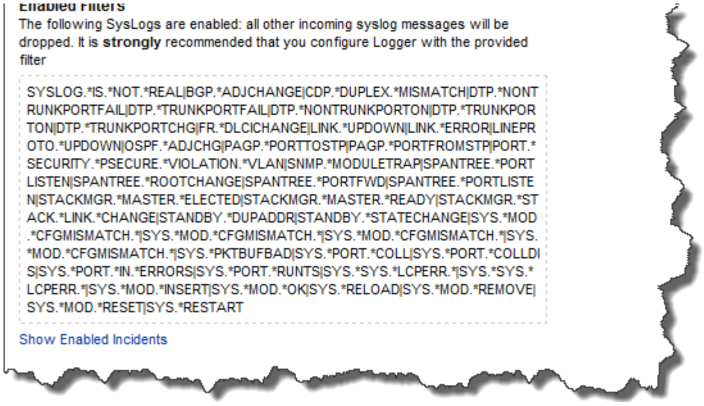
➤ Complete step 1 through step 6 any time you click **Configuration** > **Syslog Message Configurations** and make modifications, such as enabling or disabling Syslog messages.

To access Logger's configuration and add new filter content, do the following

1 From the NNMi console, click **Integration Module Configuration** > **HP ArcSight**.

2 Click **Logger Filters->(Generate)**. NNMi translates the `Enabled` Syslog messages shown in **Configuration** > **Syslog Message Configurations** into a format that you can use in a Logger filter, then opens these translations on the `Enabled Filters` page.

Figure 27 Enabled Filters Page



Enabled Filters

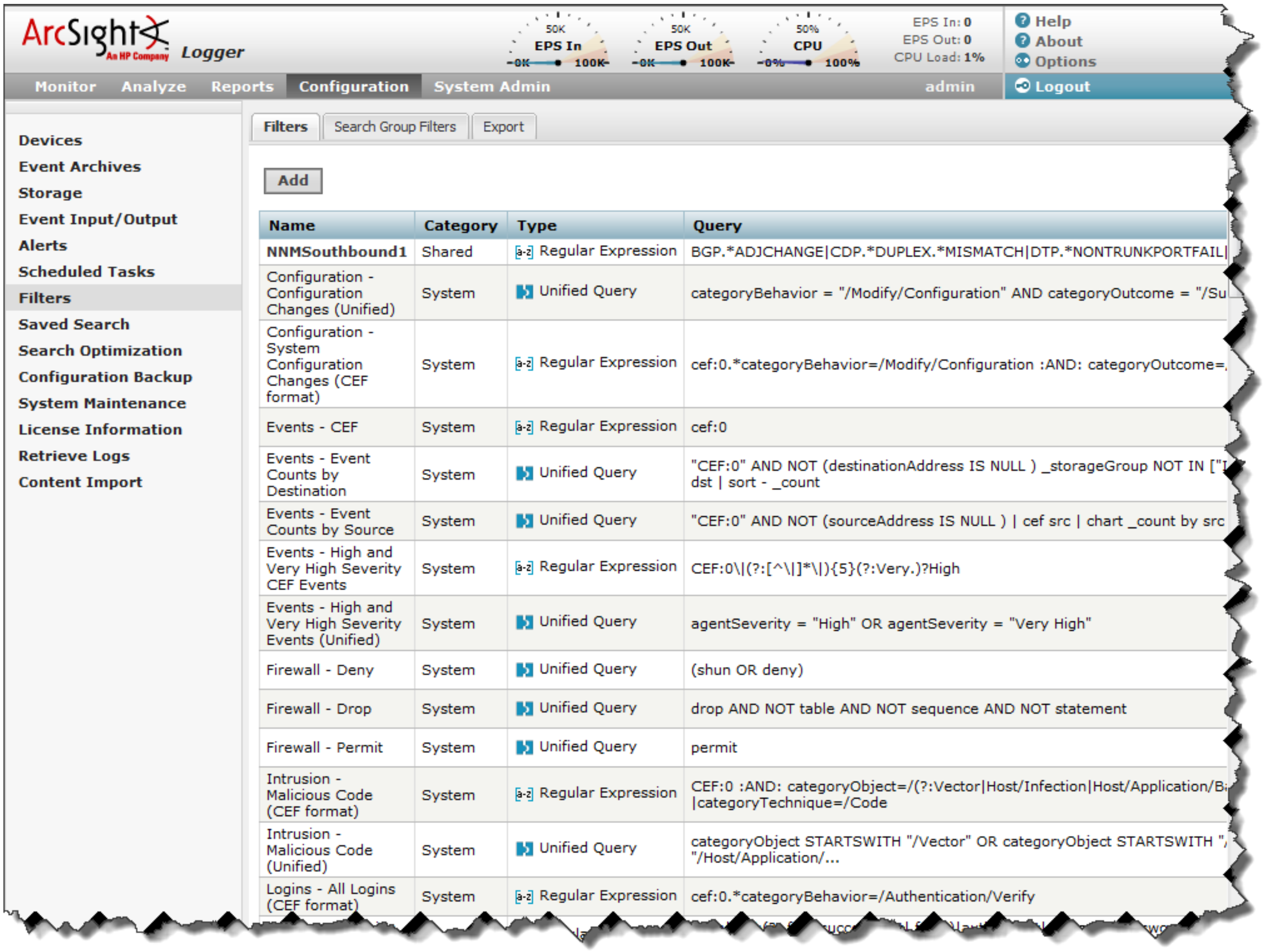
The following SysLogs are enabled: all other incoming syslog messages will be dropped. It is **strongly** recommended that you configure Logger with the provided filter

```
SYSLOG.*IS.*NOT.*REAL|BGP.*ADJCHANGE|CDP.*DUPLEX.*MISMATCH|DTP.*NONT
RUNKPORTFAIL|DTP.*TRUNKPORTFAIL|DTP.*NONTRUNKPORTON|DTP.*TRUNKPOR
TON|DTP.*TRUNKPORTCHG|FR.*DLCICHANGE|LINK.*UPDOWN|LINK.*ERROR|LINEPR
OTO.*UPDOWN|OSPF.*ADJCHG|PAGP.*PORTTOSTP|PAGP.*PORTFROMSTP|PORT.*
SECURITY.*PSECURE.*VIOLATION.*VLAN|SNMP.*MODULETRAP|SPANTREE.*PORT
LISTEN|SPANTREE.*ROOTCHANGE|SPANTREE.*PORTFWD|SPANTREE.*PORTLISTE
N|STACKMGR.*MASTER.*ELECTED|STACKMGR.*MASTER.*READY|STACKMGR.*ST
ACK.*LINK.*CHANGE|STANDBY.*DUPADDR|STANDBY.*STATECHANGE|SYS.*MOD
.*CFGMISMATCH.*|SYS.*MOD.*CFGMISMATCH.*|SYS.*MOD.*CFGMISMATCH.*|SYS.
*MOD.*CFGMISMATCH.*|SYS.*PKTBUFBAD|SYS.*PORT.*COLL|SYS.*PORT.*COLLDI
S|SYS.*PORT.*IN.*ERRORS|SYS.*PORT.*RUNTS|SYS.*SYS.*LCPERR.*|SYS.*SYS.*
LCPERR.*|SYS.*MOD.*INSERT|SYS.*MOD.*OK|SYS.*RELOAD|SYS.*MOD.*REMOVE|
SYS.*MOD.*RESET|SYS.*RESTART
```

3 Select the filter contents located on the `Enabled Filters` page. You will copy and paste this content into a filter within Logger in a later step. Close the window.

4 Click **Logger Filters->Configure**. This launches a view into the Logger **Configuration** page shown in Figure 28.

Figure 28 The Logger Configuration Page



<table>
<tr><th>Name</th><th>Category</th><th>Type</th><th>Query</th></tr>
<tr><td><b>NNMSouthbound1</b></td><td>Shared</td><td>Regular Expression</td><td>BGP.*ADJCHANGE|CDP.*DUPLEX.*MISMATCH|DTP.*NONTRUNKPORTFAIL|</td></tr>
<tr><td>Configuration - Configuration Changes (Unified)</td><td>System</td><td>Unified Query</td><td>categoryBehavior = "/Modify/Configuration" AND categoryOutcome = "/Su</td></tr>
<tr><td>Configuration - System Configuration Changes (CEF format)</td><td>System</td><td>Regular Expression</td><td>cef:0.*categoryBehavior=/Modify/Configuration :AND: categoryOutcome=,</td></tr>
<tr><td>Events - CEF</td><td>System</td><td>Regular Expression</td><td>cef:0</td></tr>
<tr><td>Events - Event Counts by Destination</td><td>System</td><td>Unified Query</td><td>"CEF:0" AND NOT (destinationAddress IS NULL) _storageGroup NOT IN ["I dst | sort - _count</td></tr>
<tr><td>Events - Event Counts by Source</td><td>System</td><td>Unified Query</td><td>"CEF:0" AND NOT (sourceAddress IS NULL) | cef src | chart _count by src</td></tr>
<tr><td>Events - High and Very High Severity CEF Events</td><td>System</td><td>Regular Expression</td><td>CEF:0\|(?:[^\|]*\|){5}(?:Very.)?High</td></tr>
<tr><td>Events - High and Very High Severity Events (Unified)</td><td>System</td><td>Unified Query</td><td>agentSeverity = "High" OR agentSeverity = "Very High"</td></tr>
<tr><td>Firewall - Deny</td><td>System</td><td>Unified Query</td><td>(shun OR deny)</td></tr>
<tr><td>Firewall - Drop</td><td>System</td><td>Unified Query</td><td>drop AND NOT table AND NOT sequence AND NOT statement</td></tr>
<tr><td>Firewall - Permit</td><td>System</td><td>Unified Query</td><td>permit</td></tr>
<tr><td>Intrusion - Malicious Code (CEF format)</td><td>System</td><td>Regular Expression</td><td>CEF:0 :AND: categoryObject=/(?:Vector|Host/Infection|Host/Application/B |categoryTechnique=/Code</td></tr>
<tr><td>Intrusion - Malicious Code (Unified)</td><td>System</td><td>Unified Query</td><td>categoryObject STARTSWITH "/Vector" OR categoryObject STARTSWITH " "/Host/Application/...</td></tr>
<tr><td>Logins - All Logins (CEF format)</td><td>System</td><td>Regular Expression</td><td>cef:0.*categoryBehavior=/Authentication/Verify</td></tr>
</table>

5 Click **Filters**, then wait for the list of filters to load.

6 Complete one of the following actions to configure a filter that determines which Syslog messages to forward to NNMi.

If this is the first time you are creating a filter to determine which Syslog messages to forward to NNMi, do the following:

a Click **Add**.

b After Logger opens the Add Filter form, add a name for the filter, select the **Regex Query** filter type, then select **Next**.

c Copy the contents from step 3 into the `Query` field.

d Save your work.

If you are modifying an existing filter that determines which Syslog messages to forward to NNMi, do the following:

a Edit the existing filter that Logger uses to determine which Syslog messages to forward to NNMi.

b Clear out the existing filter contents.

c Copy the contents from step 3 into the `Query` field.

d Save your work.

Task 6: Configuring the SmartConnector for HP Network Node Manager i SNMP (Connector for Northbound Interface, Optional Task)

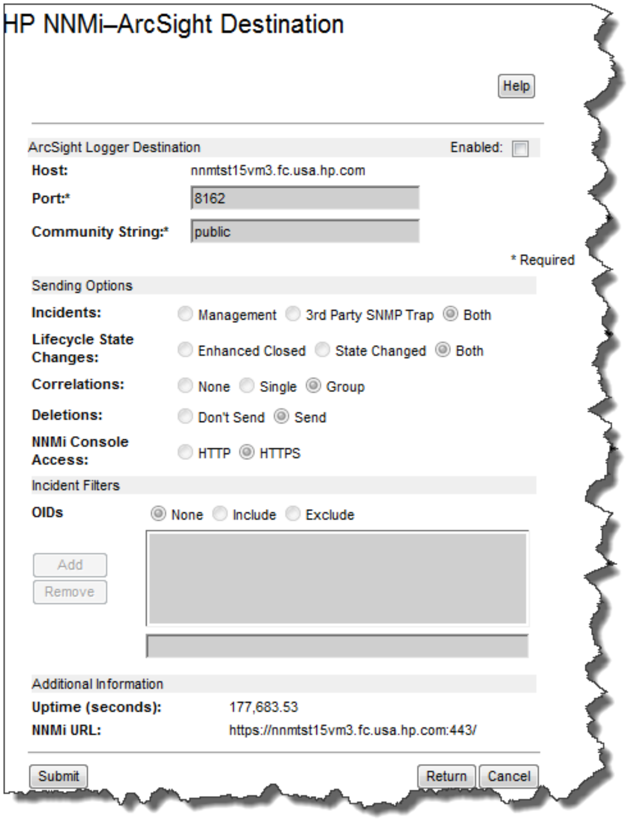
Configure the SmartConnector for HP Network Node Manager i SNMP using instructions from the *SmartConnector Configuration Guide for HP Network Node Manager i SNMP* manual.

Task 7: Configuring NNMi to Forward SNMPv1, v2, and v3 Trap Incidents to Logger (Northbound Interface, Optional Task)

1 From the NNMi console, click **Integration Module Configuration** > **HP ArcSight**.

2 Click **Syslog Forwarding** > **Configure** this launches a view to the **NNMi - Logger Destination** page. See Figure 29 while completing the steps for this task.

Figure 29 Configuring the NNMi - Logger Destination



HP NNMi–ArcSight Destination

ArcSight Logger Destination Enabled: □

Host: nnmtst15vm3.fc.usa.hp.com

Port:* 8162

Community String:* public

* Required

Sending Options

Incidents: ○ Management ○ 3rd Party SNMP Trap ● Both

Lifecycle State Changes: ○ Enhanced Closed ○ State Changed ● Both

Correlations: ○ None ○ Single ● Group

Deletions: ○ Don't Send ● Send

NNMi Console Access: ○ HTTP ● HTTPS

Incident Filters

OIDs ● None ○ Include ○ Exclude

Additional Information

Uptime (seconds): 177,683.53

NNMi URL: https://nnmtst15vm3.fc.usa.hp.com:443/

3 Select **ArcSight Logger Destination** > **Enabled**.

4 Add `8162` as the value of the port field. NNMi forwards to a connector that is installed on theNNMi management server. The port is automatically set to the default for the connector.

5 Enter the `Community String` for the `Logger` host.
If you do not specify a community string, the integration module attempts to use the empty community string.

6 Make sections for the `Sending Options`. Without changes to those values, NNMi forwards everything:

7 For `Incident Filters`, enter the include or exclude **OIDs**.

8 Click **Submit**.

9 NNMi tests for any configuration errors. Fix any displayed errors, then repeat step 8 until the submit is successful.

Using the HP NNMi - HP ArcSight Logger Integration

ArcSightEvent Details

After completing Task 4, enabling the NNMi - HP ArcSight Logger integration and the `ArcSightEvent`, and configuring Logger to forward SNMP traps in the form of `ArcSightEvents`, NNMi evaluates the `ArcSightEvent` content and opens it as an SNMP trap or a Syslog message.

To keep NNMi performing at a high level, NNMi drops incoming SNMP traps (including Syslog messages) after storing a specific number of SNMP traps in its database. You can use the auto-trim oldest SNMP trap incidents feature to control the number of SNMP traps stored in the NNMi database and to retain important incoming SNMP traps. See Configuring the Auto-Trim Oldest SNMP Trap Incidents Feature on page 368 for more information.

The HP NNMi–HP ArcSight Logger Integration supports Syslog messages from the following vendors:

- "*Cisco*: Syslog incident configuration will use the mnemonic identified by event.deviceCustomString5 (.1.3.6.1.4.1.11937.1.54.5)
- "*Juniper*: Syslog incident configuration will use the mnemonic identified by event.deviceEventClassId(.1.3.6.1.4.1.11937.1.46.5)
- "*Nortel*: Syslog incident configuration will use the mnemonic identified by event.deviceEventClassId(.1.3.6.1.4.1.11937.1.46.5). Spaces will be replaced by '_' in the Syslog incident configuration name.
- "*F5*: Syslog incident configuration will use the mnemonic identified by event.deviceEventClassId(.1.3.6.1.4.1.11937.1.46.5) Spaces will be replaced by '_' in the Syslog incident configuration name.

When launching from the NNMi console to Logger, the browser might prompt you to trust the Logger before initiating the cross-launch.

➤ Often when an application attempts to redirect to an untrusted site, it prompts you to trust the site before completing the redirect.

To view `ArcSightEvent` SNMP traps, click **SNMP Traps** in the **Incident Browsing** workspace. To view `ArcSightEvent` Syslog messages, click **Syslog Messages** in the **Incident Browsing** workspace.

After enabling the NNMi - HP ArcSight Logger integration, the `ArcSightEvents` that Logger forwards to NNMi are structured the same as SNMP traps. To view the ArcSightEvent SNMP trap configuration, do the following:

1 From the NNMi console, navigate to **Configuration** > **Incidents** > **SNMP Trap Configurations.**

2 Open the **ArcSightEvent** trap definition.

To view the `ArcSightEvents` that Logger forwards to NNMi 9.10, and that are actual Syslog messages, do the following:

1 From the NNMi console, navigate to **Configuration** > **Incidents** > **Syslog Message Configurations.**

2 NNMi opens the current list of `Syslog Message Configurations`.

Special Pairwise Handling

NNMi applies special pairwise handling, cancelling a down event after an up event occurs, for the following Syslog messages.

- `LINEPROTO-5-UPDOWN`
- `LINK-3-UPDOWN`
- `SNMP-5-MODULETRAP`

Changes to the NNMi Console's Actions Menu

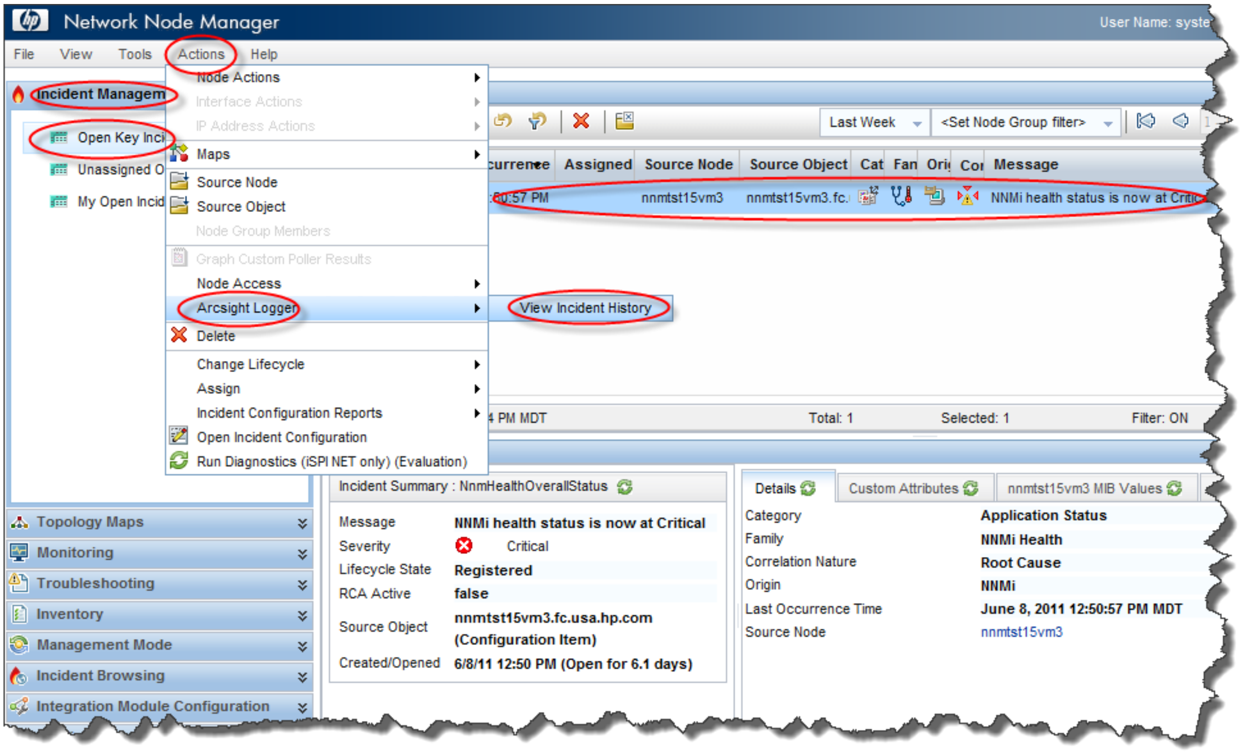
After enabling the NNMi - HP ArcSight Logger integration, the NNMi console provides the following new functionality in the NNMi management server.

Incident Management Workspace

In the **Incident Management** workspace, click **Open Key Incidents**.

Use the NNMi console to open the Logger application from an incident. To do this, select an incident while using the **Incident Management** workspace; then use the NNMi console **Actions** menu to open the Logger application as shown in Figure 30.

Figure 30 Opening Logger from an NNMi Incident in the Incident Management Workspace



:50:57 PM | nnmtst15vm3 | nnmtst15vm3.fc. | NNMi health status is now at Critic

4 PM MDT Total: 1 Selected: 1 Filter: ON

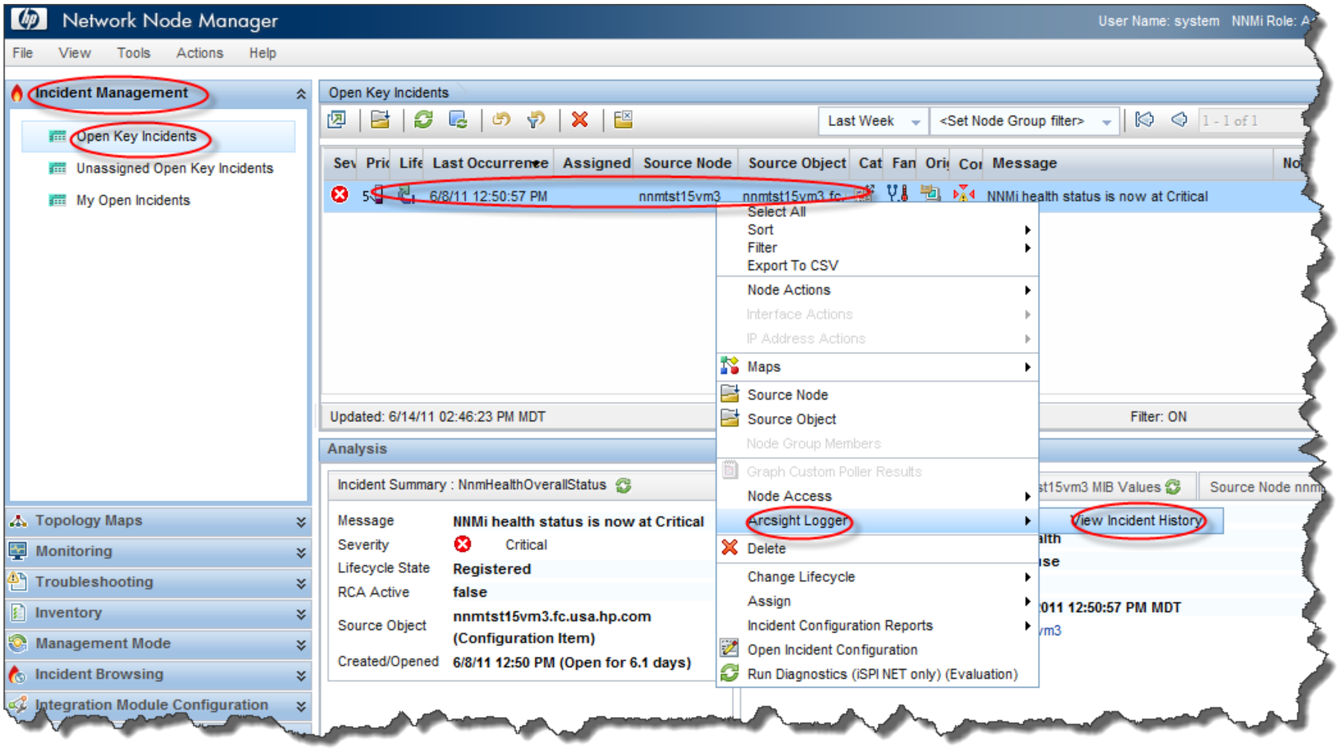
Incident Summary : NnmHealthOverallStatus

Message	NNMi health status is now at Critical
Severity	Critical
Lifecycle State	Registered
RCA Active	false
Source Object	nnmtst15vm3.fc.usa.hp.com (Configuration Item)
Created/Opened	6/8/11 12:50 PM (Open for 6.1 days)

Category	Application Status
Family	NNMi Health
Correlation Nature	Root Cause
Origin	NNMi
Last Occurrence Time	June 8, 2011 12:50:57 PM MDT
Source Node	nnmtst15vm3

You can also right-click an incident; then use the menu to open the Logger application as shown in Figure 31.

Figure 31 Opening Logger by Right-Clicking on an Incident in the Incident Management Workspace



Sev	Pric	Life	Last Occurrence	Assigned	Source Node	Source Object	Cat	Fan	Ori	Cor	Message	No
	5		6/8/11 12:50:57 PM		nnmtst15vm3	nnmtst15vm3.fc					NNMi health status is now at Critical	

Incident Summary : NnmHealthOverallStatus

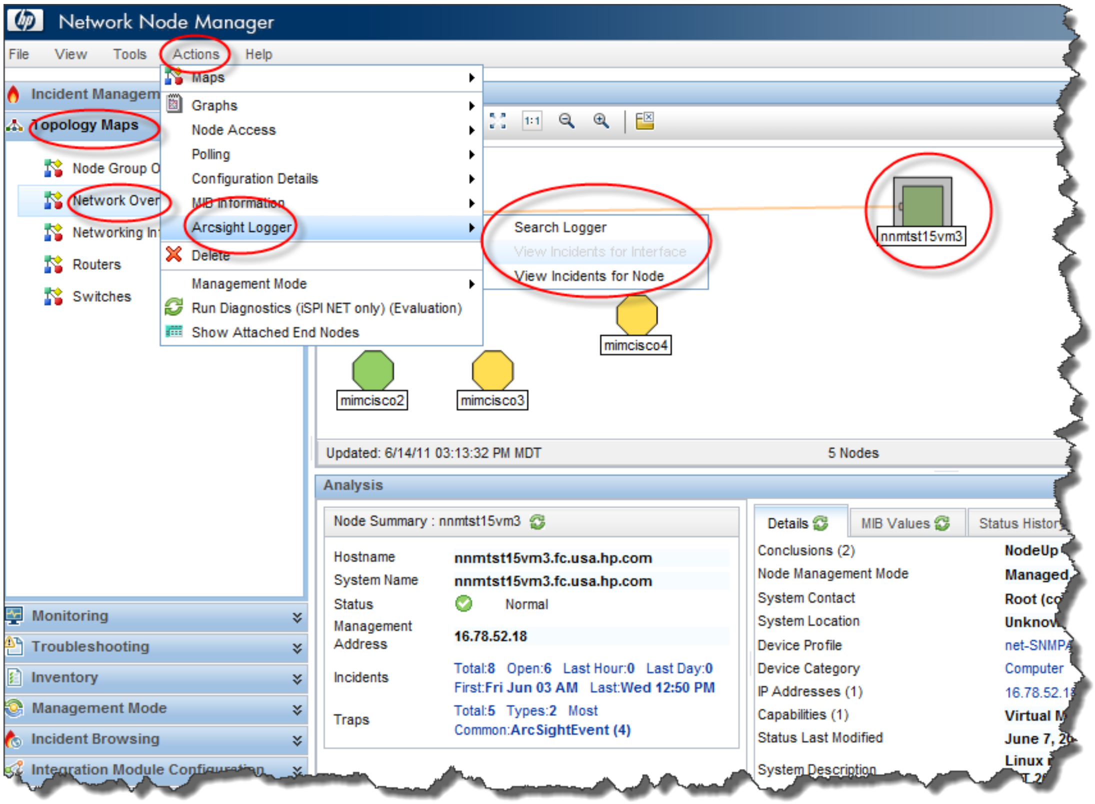
Message	NNMi health status is now at Critical
Severity	Critical
Lifecycle State	Registered
RCA Active	false
Source Object	nnmtst15vm3.fc.usa.hp.com (Configuration Item)
Created/Opened	6/8/11 12:50 PM (Open for 6.1 days)

Topology Maps Workspace

In the **Topology Maps** workspace, click **Network Overview**.

Use the NNMi console to open the Logger application from a node. To do this, select a node while using the **Topology Maps** workspace; then use the NNMi console **Actions** menu to open the Logger application as shown in as shown in Figure 32.

Figure 32 Opening Logger from a Node in the Topology Maps Workspace



Updated: 6/14/11 03:13:32 PM MDT   5 Nodes

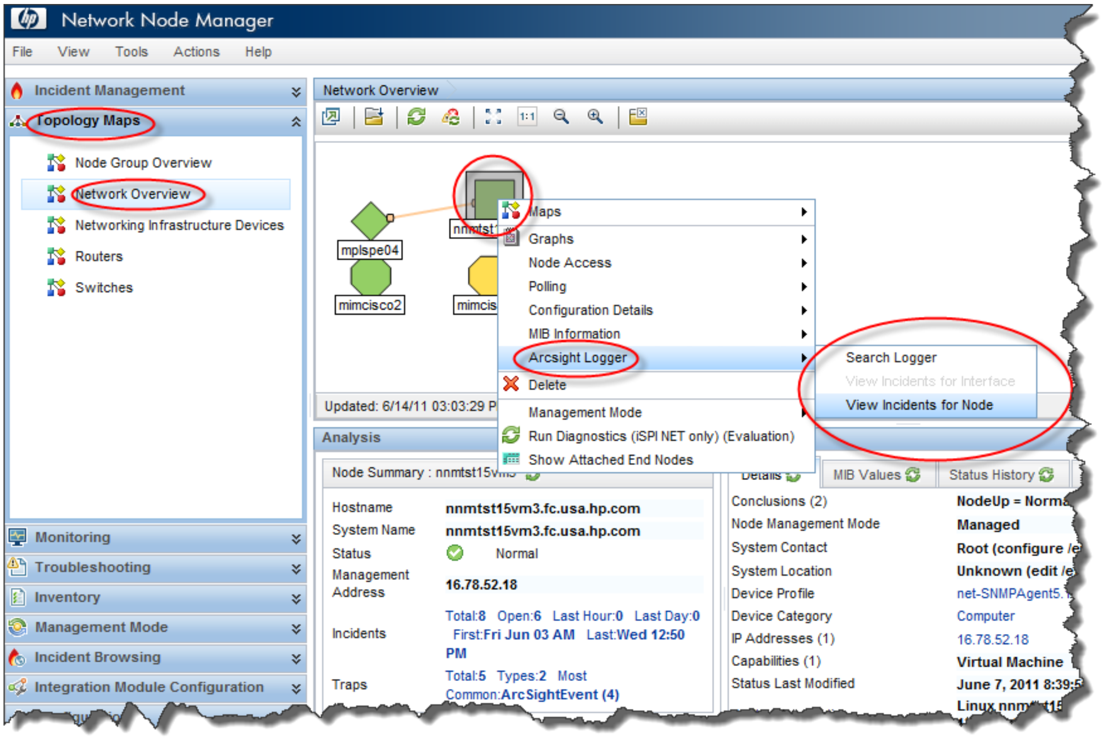
Node Summary : nnmtst15vm3

Hostname	nnmtst15vm3.fc.usa.hp.com
System Name	nnmtst15vm3.fc.usa.hp.com
Status	✓ Normal
Management Address	16.78.52.18
Incidents	Total:8 Open:6 Last Hour:0 Last Day:0 First:Fri Jun 03 AM Last:Wed 12:50 PM
Traps	Total:5 Types:2 Most Common:ArcSightEvent (4)

Conclusions (2)	NodeUp
Node Management Mode	Managed
System Contact	Root (co
System Location	Unknow
Device Profile	net-SNMPA
Device Category	Computer
IP Addresses (1)	16.78.52.1
Capabilities (1)	Virtual M
Status Last Modified	June 7, 20
System Description	Linux

You can also right-click a node; then use the menu to open the Logger application as shown in Figure 33.

Figure 33 Opening Logger by Right-Clicking on a Node in the Topology Maps Workspace



Updated: 6/14/11 03:03:29 P

Node Summary : nnmtst15vm3

Hostname	nnmtst15vm3.fc.usa.hp.com
System Name	nnmtst15vm3.fc.usa.hp.com
Status	Normal
Management Address	16.78.52.18
Incidents	Total:8 Open:6 Last Hour:0 Last Day:0 First:Fri Jun 03 AM Last:Wed 12:50 PM
Traps	Total:5 Types:2 Most Common:ArcSightEvent (4)

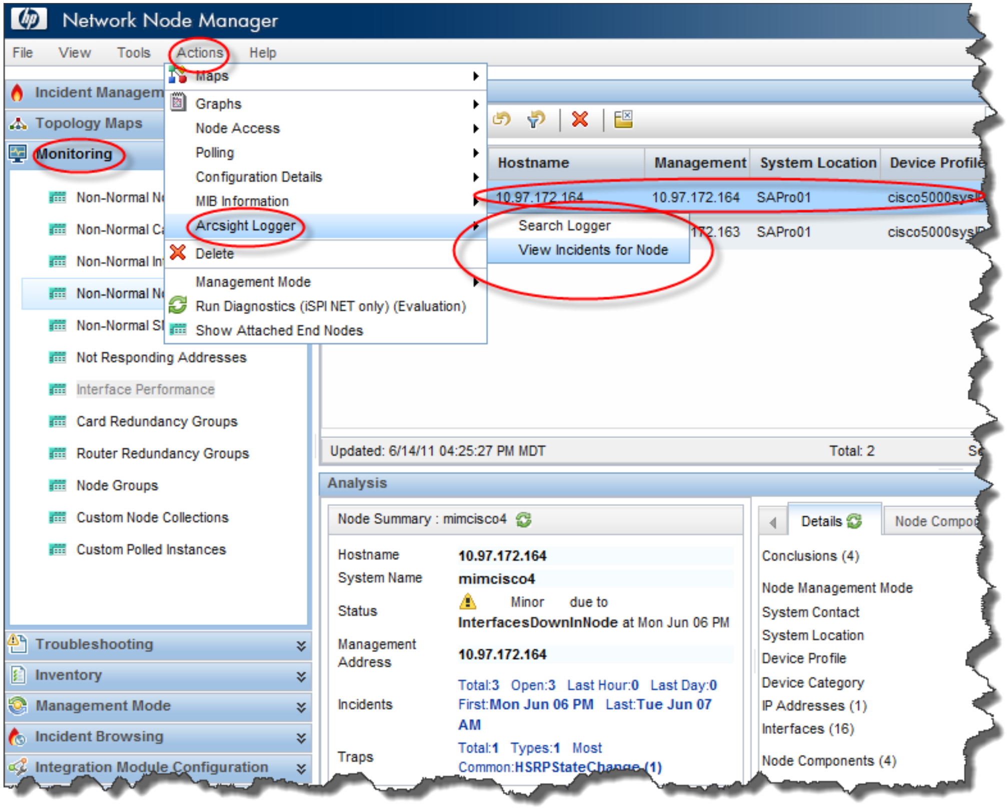
Conclusions (2)	NodeUp = Norma
Node Management Mode	Managed
System Contact	Root (configure /e
System Location	Unknown (edit /e
Device Profile	net-SNMPAgent5.
Device Category	Computer
IP Addresses (1)	16.78.52.18
Capabilities (1)	Virtual Machine
Status Last Modified	June 7, 2011 8:39:5
	Linux nnm t15

Monitoring Workspace

In the **Monitoring** workspace, click **Non-Normal Nodes**.

Use the NNMi console to open the Logger application from a node or interface. To do this, select a node or interface while using the **Monitoring** workspace; then use the NNMi console **Actions** menu to open the Logger application as shown in as shown in Figure 34.

Figure 34 Opening Logger from a Node in the Monitoring Workspace



Hostname	Management	System Location	Device Profile
10.97.172.164	10.97.172.164	SAPro01	cisco5000sysID
	172.163	SAPro01	cisco5000sysID

Updated: 6/14/11 04:25:27 PM MDT Total: 2

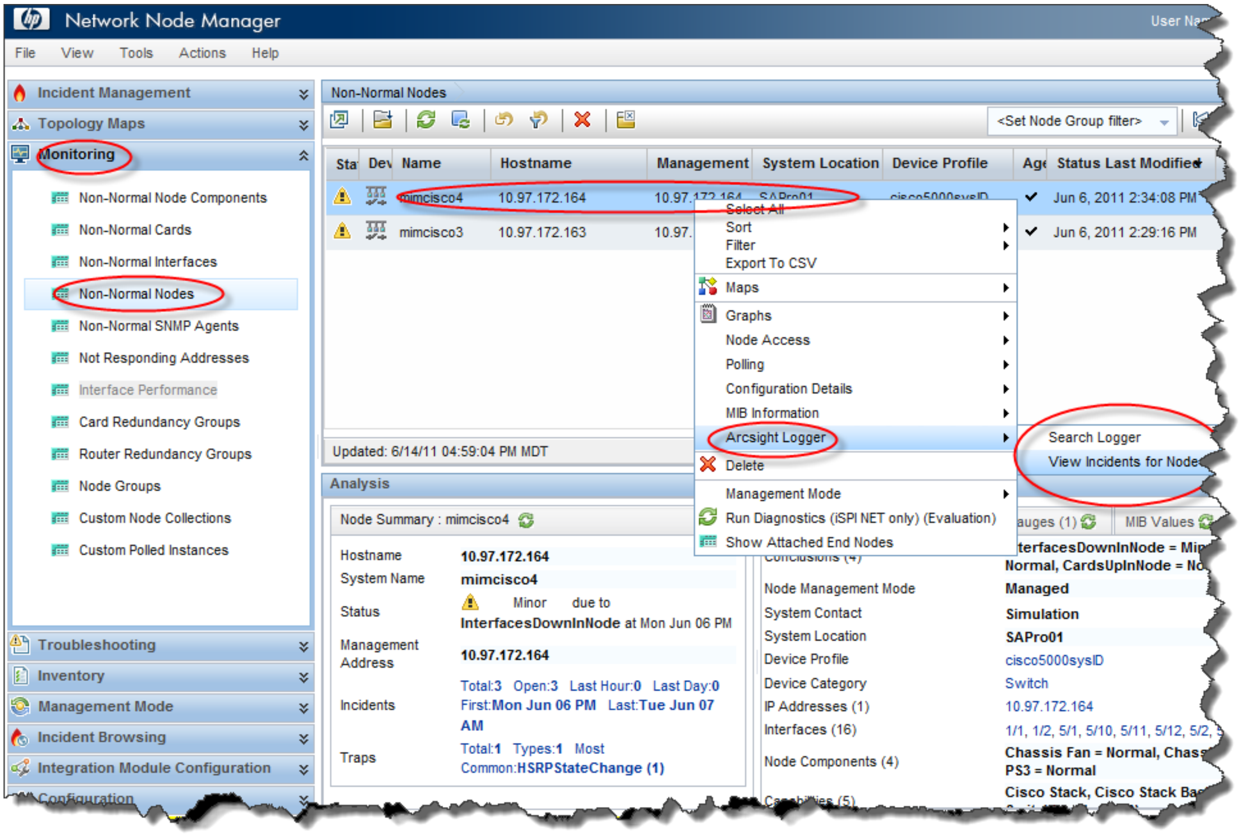
Node Summary : mimcisco4

Hostname	10.97.172.164
System Name	mimcisco4
Status	Minor due to InterfacesDownInNode at Mon Jun 06 PM
Management Address	10.97.172.164
Incidents	Total:3 Open:3 Last Hour:0 Last Day:0 First:Mon Jun 06 PM Last:Tue Jun 07 AM
Traps	Total:1 Types:1 Most Common:HSRPStateChange (1)

Conclusions (4)
Node Management Mode
System Contact
System Location
Device Profile
Device Category
IP Addresses (1)
Interfaces (16)
Node Components (4)

You can also right-click a node in the **Monitoring** workspace; then use the menu to open the Logger application as shown in Figure 35.

Figure 35 Opening Logger by Right-Clicking on a Node in the Monitoring Workspace



Sta	Dev	Name	Hostname	Management	System Location	Device Profile	Age	Status Last Modified
⚠		mimcisco4	10.97.172.164	10.97.172.164	SAPro01	cisco5000sysID	✓	Jun 6, 2011 2:34:08 PM
⚠		mimcisco3	10.97.172.163	10.97.			✓	Jun 6, 2011 2:29:16 PM

Updated: 6/14/11 04:59:04 PM MDT

Hostname	10.97.172.164
System Name	mimcisco4
Status	⚠ Minor due to InterfacesDownInNode at Mon Jun 06 PM
Management Address	10.97.172.164
Incidents	Total:3 Open:3 Last Hour:0 Last Day:0 First:Mon Jun 06 PM Last:Tue Jun 07 AM
Traps	Total:1 Types:1 Most Common:HSRPStateChange (1)

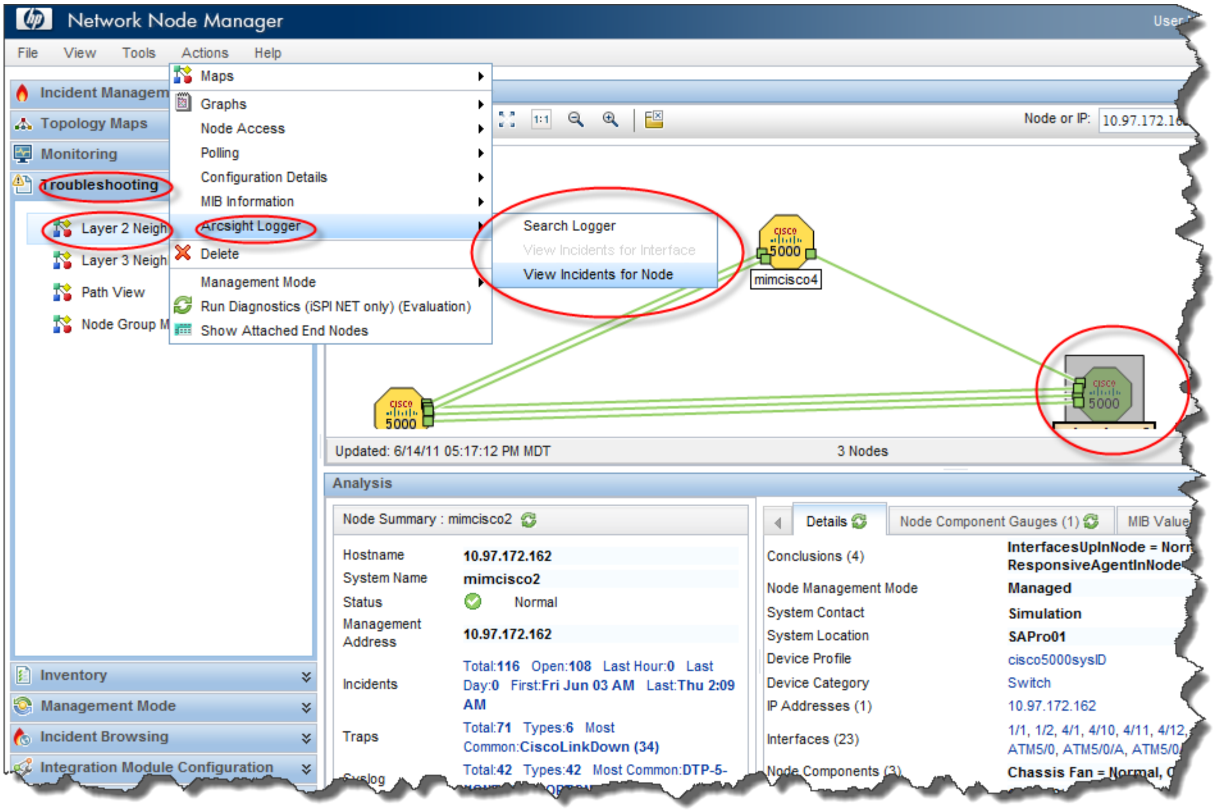
Conclusions (4)	terfacesDownInNode = Mi Normal, CardsUpInNode = No
Node Management Mode	Managed
System Contact	Simulation
System Location	SAPro01
Device Profile	cisco5000sysID
Device Category	Switch
IP Addresses (1)	10.97.172.164
Interfaces (16)	1/1, 1/2, 5/1, 5/10, 5/11, 5/12, 5/2,
Node Components (4)	Chassis Fan = Normal, Chass PS3 = Normal
Capabilities (5)	Cisco Stack, Cisco Stack Ba

Troubleshooting Workspace

In the **Troubleshooting** workspace, open a **Layer 2 Neighbor View.**

Use the NNMi console to open the Logger application from a node. To do this, select a node while using the **Troubleshooting** workspace; then use the NNMi console **Actions** menu to open the Logger application as shown inFigure 36.

Figure 36 Opening Logger from a Node in the Troubleshooting Workspace



Updated: 6/14/11 05:17:12 PM MDT 3 Nodes

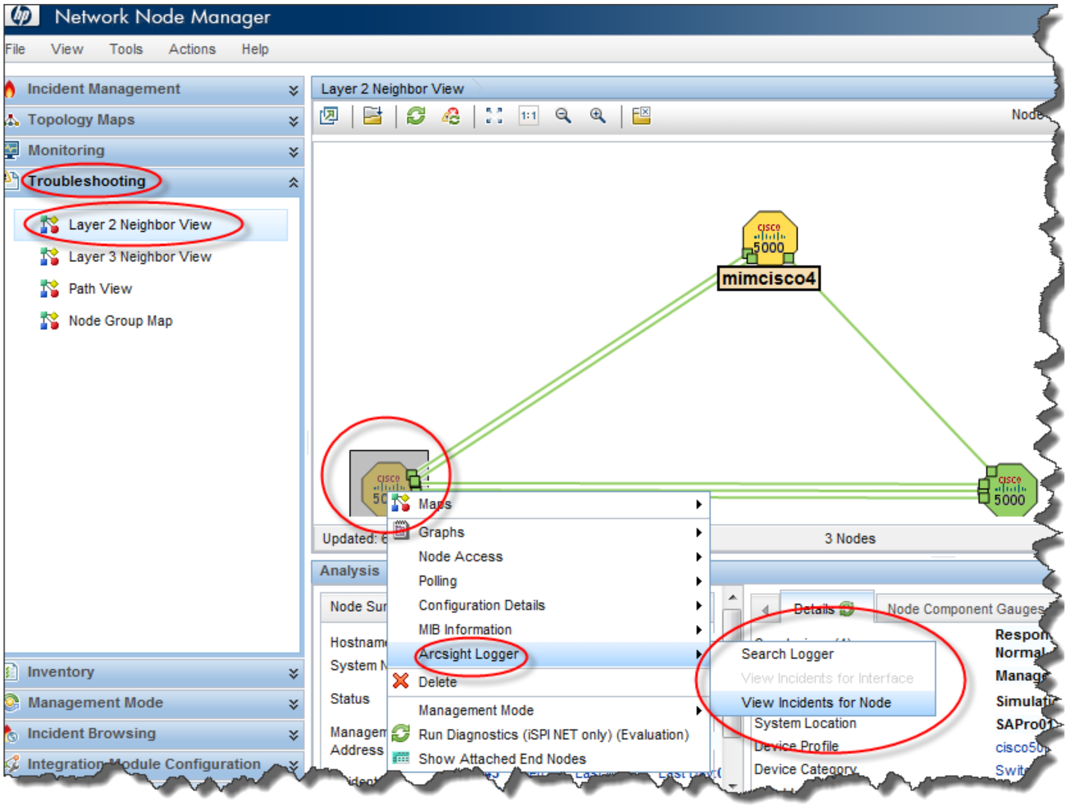
Node Summary : mimcisco2

Hostname 10.97.172.162
System Name mimcisco2
Status Normal
Management Address 10.97.172.162
Incidents Total:116 Open:108 Last Hour:0 Last Day:0 First:Fri Jun 03 AM Last:Thu 2:09 AM
Traps Total:71 Types:6 Most Common:CiscoLinkDown (34)
Syslog Total:42 Types:42 Most Common:DTP-5-

Conclusions (4) InterfacesUpInNode = Norr ResponsiveAgentInNode
Node Management Mode Managed
System Contact Simulation
System Location SAPro01
Device Profile cisco5000sysID
Device Category Switch
IP Addresses (1) 10.97.172.162
Interfaces (23) 1/1, 1/2, 4/1, 4/10, 4/11, 4/12, ATM5/0, ATM5/0/A, ATM5/0
Node Components (3) Chassis Fan = Normal, C

You can also right-click a node in the **Troubleshooting** workspace; then use the menu to open the Logger application from a node as shown in Figure 37.

Figure 37 Opening Logger by Right-Clicking on a Node in the Troubleshooting Workspace

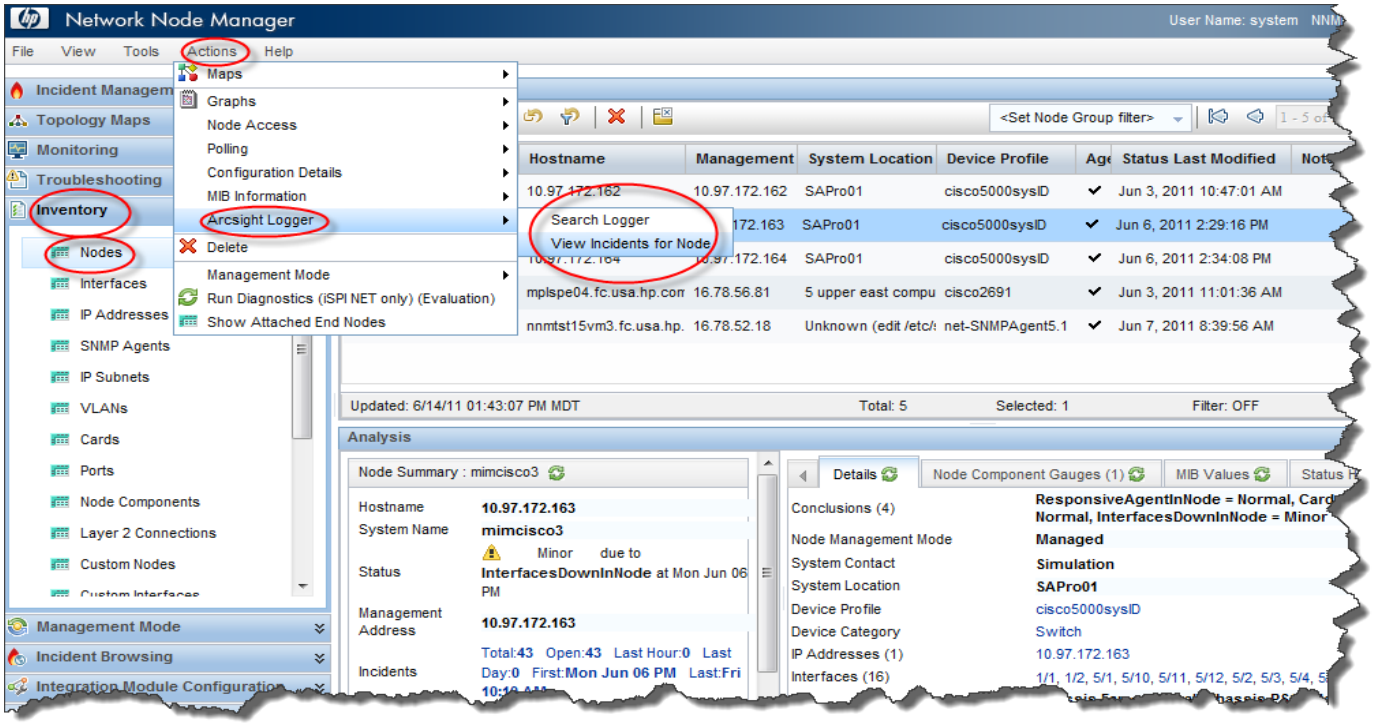


Inventory Workspace

In the **Inventory** workspace, click **Nodes**.

Use the NNMi console to open the Logger application from a node or interface. To do this, select a node or interface while using the **Inventory** workspace; then use the NNMi console menus to open the Logger application as shown in Figure 38.

Figure 38 Opening Logger from a Node or Interface in the Inventory Workspace



Hostname	Management	System Location	Device Profile	Ag	Status Last Modified	Not
10.97.172.162	10.97.172.162	SAPro01	cisco5000sysID	✓	Jun 3, 2011 10:47:01 AM	
	172.163	SAPro01	cisco5000sysID	✓	Jun 6, 2011 2:29:16 PM	
10.97.172.164	10.97.172.164	SAPro01	cisco5000sysID	✓	Jun 6, 2011 2:34:08 PM	
mplspe04.fc.usa.hp.com	16.78.56.81	5 upper east compu	cisco2691	✓	Jun 3, 2011 11:01:36 AM	
nnmtst15vm3.fc.usa.hp.	16.78.52.18	Unknown (edit /etc/s	net-SNMPAgent5.1	✓	Jun 7, 2011 8:39:56 AM	

Updated: 6/14/11 01:43:07 PM MDT Total: 5 Selected: 1 Filter: OFF

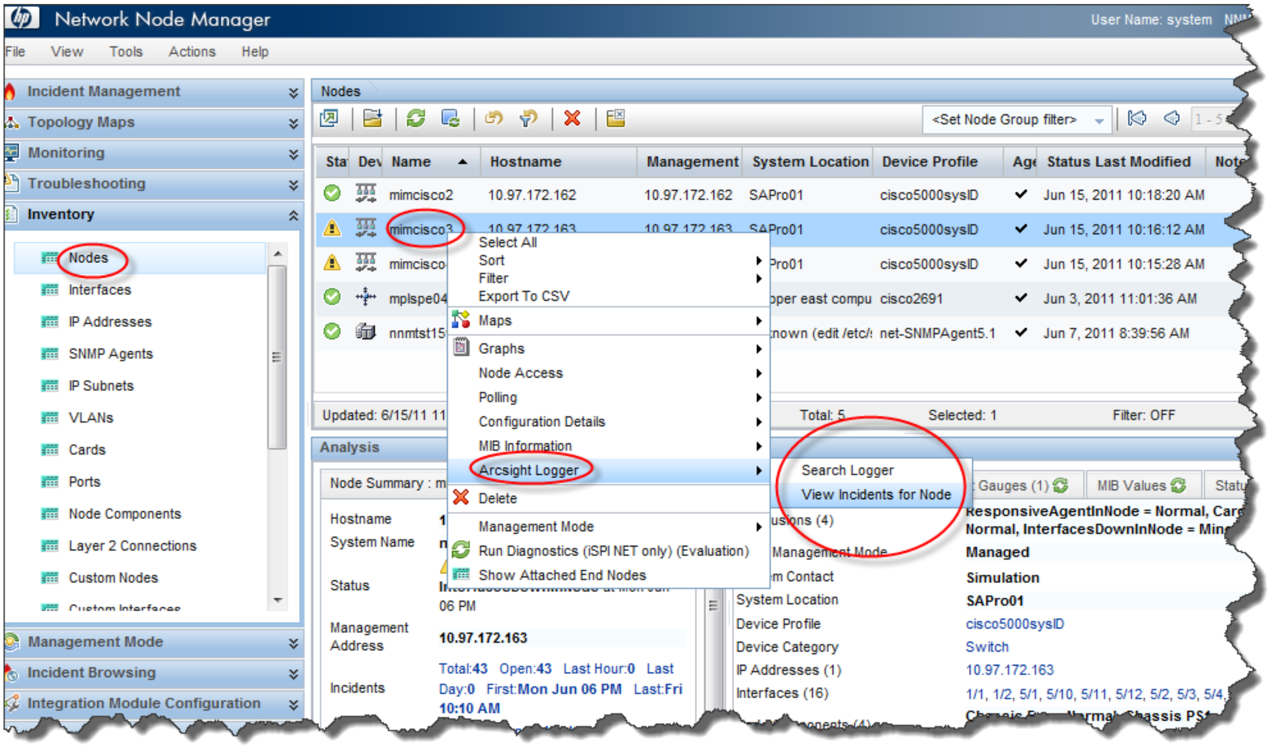
Node Summary : mimcisco3

Hostname	10.97.172.163
System Name	mimcisco3
Status	⚠ Minor due to InterfacesDownInNode at Mon Jun 06 PM
Management Address	10.97.172.163
Incidents	Total:43 Open:43 Last Hour:0 Last Day:0 First:Mon Jun 06 PM Last:Fri 10:10 AM

Conclusions (4)	ResponsiveAgentInNode = Normal, Card Normal, InterfacesDownInNode = Minor
Node Management Mode	Managed
System Contact	Simulation
System Location	SAPro01
Device Profile	cisco5000sysID
Device Category	Switch
IP Addresses (1)	10.97.172.163
Interfaces (16)	1/1, 1/2, 5/1, 5/10, 5/11, 5/12, 5/2, 5/3, 5/4, 5

You can also right-click a node in the **Inventory** workspace; then use the menu to open the Logger application from a node as shown in Figure 39.

Figure 39 Opening Logger by Right-Clicking on a Node or Interface in the Inventory Workspace



Sta	Dev	Name	Hostname	Management	System Location	Device Profile	Age	Status Last Modified	Note
		mimcisco2	10.97.172.162	10.97.172.162	SAPro01	cisco5000sysID	✓	Jun 15, 2011 10:18:20 AM	
		mimcisco3	10.97.172.163	10.97.172.163	SAPro01	cisco5000sysID	✓	Jun 15, 2011 10:16:12 AM	
		mimcisco			Pro01	cisco5000sysID	✓	Jun 15, 2011 10:15:28 AM	
		mplspe04			pper east compu	cisco2691	✓	Jun 3, 2011 11:01:36 AM	
		nnmtst15			nown (edit /etc/s	net-SNMPAgent5.1	✓	Jun 7, 2011 8:39:56 AM	

Hostname 1
System Name n
Status In... 06 PM
Management Address 10.97.172.163
Incidents Total:43 Open:43 Last Hour:0 Last Day:0 First:Mon Jun 06 PM Last:Fri 10:10 AM

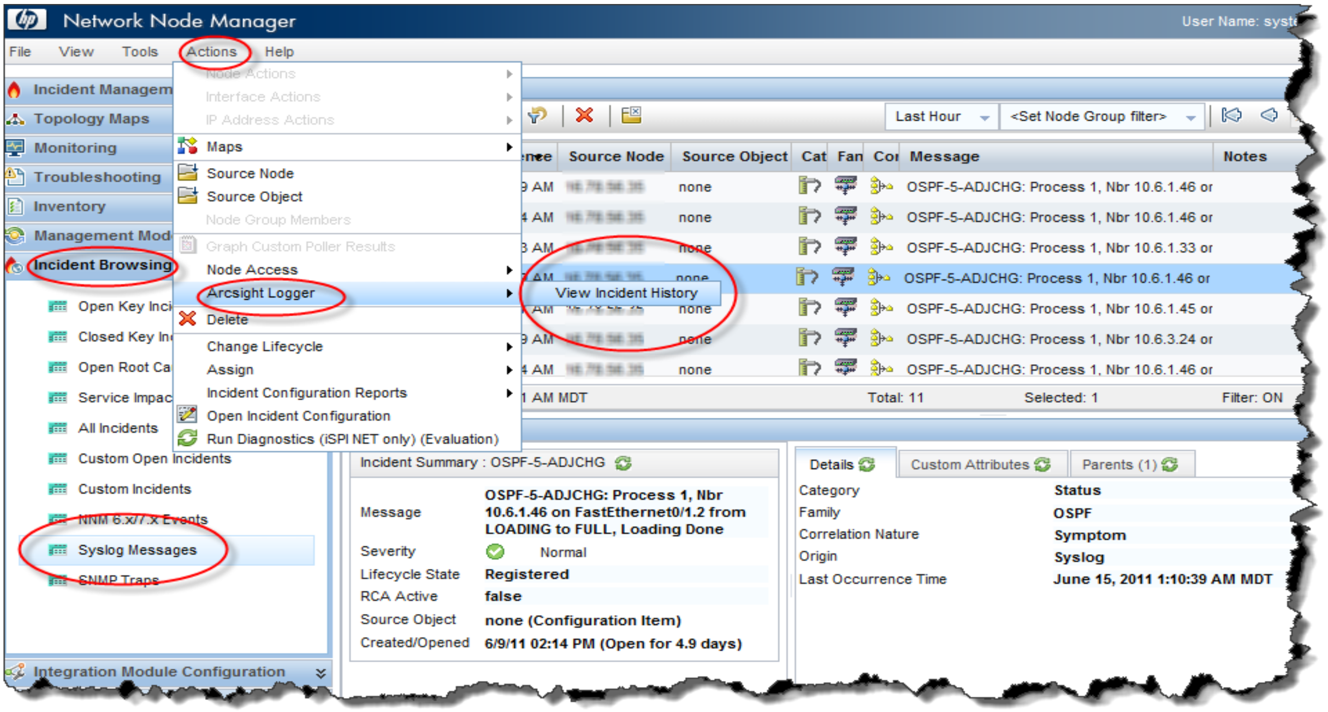
usions (4) ResponsiveAgentInNode = Normal, Card Normal, InterfacesDownInNode = Minor
Management Mode Managed
m Contact Simulation
System Location SAPro01
Device Profile cisco5000sysID
Device Category Switch
IP Addresses (1) 10.97.172.163
Interfaces (16) 1/1, 1/2, 5/1, 5/10, 5/11, 5/12, 5/2, 5/3, 5/4,

Incident Browsing Workspace

In the **Incident Browsing** workspace, click **Syslog Messages** to view the `ArcSightEvents` Logger forwarded to NNMi .

You can use the NNMi console to open the Logger application from an NNMi incident. To do this, select an incident while using the **Incident Browsing** workspace and use the NNMi console menus to view the incident history as shown in Figure 40.

Figure 40 View Incident History Using Actions Menu



ence	Source Node	Source Object	Cat	Fan	Cor	Message	Notes
9 AM	[redacted]	none				OSPF-5-ADJCHG: Process 1, Nbr 10.6.1.46 or	
4 AM	[redacted]	none				OSPF-5-ADJCHG: Process 1, Nbr 10.6.1.46 or	
3 AM	[redacted]	none				OSPF-5-ADJCHG: Process 1, Nbr 10.6.1.33 or	
AM	[redacted]	none				OSPF-5-ADJCHG: Process 1, Nbr 10.6.1.46 or	
AM	[redacted]	none				OSPF-5-ADJCHG: Process 1, Nbr 10.6.1.45 or	
9 AM	[redacted]	none				OSPF-5-ADJCHG: Process 1, Nbr 10.6.3.24 or	
4 AM	[redacted]	none				OSPF-5-ADJCHG: Process 1, Nbr 10.6.1.46 or	

1 AM MDT Total: 11 Selected: 1 Filter: ON

Incident Summary : OSPF-5-ADJCHG

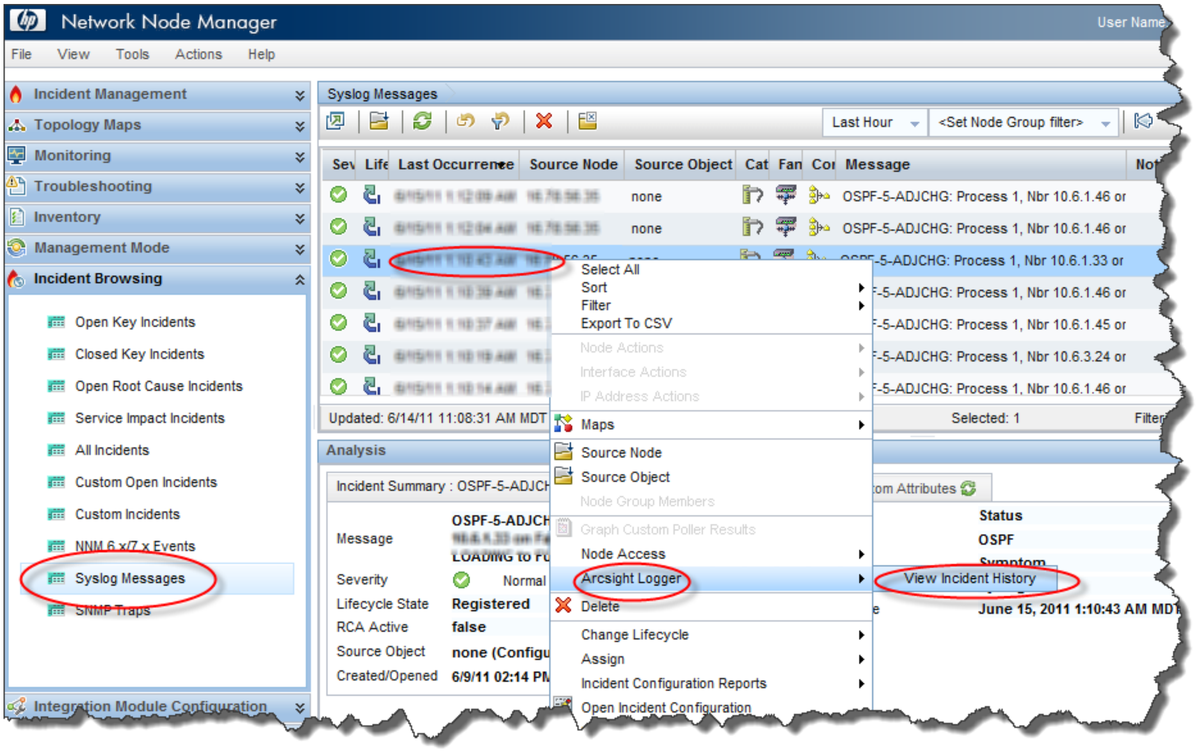
Message	OSPF-5-ADJCHG: Process 1, Nbr 10.6.1.46 on FastEthernet0/1.2 from LOADING to FULL, Loading Done
Severity	✓ Normal
Lifecycle State	Registered
RCA Active	false
Source Object	none (Configuration Item)
Created/Opened	6/9/11 02:14 PM (Open for 4.9 days)

Details | Custom Attributes | Parents (1)

Category	Status
Family	OSPF
Correlation Nature	Symptom
Origin	Syslog
Last Occurrence Time	June 15, 2011 1:10:39 AM MDT

You can also right-click an incident and use the **ArcSight Logger** > **View Incident History** to open the Logger application from an NNMi incident.

Figure 41 Fight-Click a Syslog Message, then View Incident History



Sev	Life	Last Occurrence	Source Node	Source Object	Cat	Fan	Co	Message	No
✓		[redacted]	[redacted]	none				OSPF-5-ADJCHG: Process 1, Nbr 10.6.1.46 or	
✓		[redacted]	[redacted]	none				OSPF-5-ADJCHG: Process 1, Nbr 10.6.1.46 or	
✓		[redacted]	[redacted]					OSPF-5-ADJCHG: Process 1, Nbr 10.6.1.33 or	
✓		[redacted]	[redacted]					F-5-ADJCHG: Process 1, Nbr 10.6.1.46 or	
✓		[redacted]	[redacted]					F-5-ADJCHG: Process 1, Nbr 10.6.1.45 or	
✓		[redacted]	[redacted]					F-5-ADJCHG: Process 1, Nbr 10.6.3.24 or	
✓		[redacted]	[redacted]					F-5-ADJCHG: Process 1, Nbr 10.6.1.46 or	

Updated: 6/14/11 11:08:31 AM MDT

Selected: 1

Filter

Message OSPF-5-ADJCH [redacted] LOADING to FU

Severity ✓ Normal

Lifecycle State Registered

RCA Active false

Source Object none (Configu

Created/Opened 6/9/11 02:14 PM

Status

OSPF

Symptom

June 15, 2011 1:10:43 AM MDT

Disabling the HP NNMi–Logger Integration

To disable the integration, do the following:

1. From the NNMi console, click **Integration Module Configuration** > **HP ArcSight**.
2. Remove the **Enable ArcSight Integration** selection.
3. Click **Submit**.

HP Asset Manager

HP Asset Manager is an asset management platform for tracking and maintaining corporate inventory, including IT assets. Asset Manager provides the following functionality:

- Manage software license compliance, entitlements, and costs
- Discover, provision, manage, and improve the use of physical and virtual IT assets
- Use distributed sources of inventory, asset, and service data efficiently
- Automate management of equipment, space, cooling, and power

For information about purchasing Asset Manager, contact your HP sales representative.

This chapter contains the following topics:

- HP NNMi–HP Asset Manager Integration
- Using the HP NNMi–HP Asset Manager Integration

HP NNMi–HP Asset Manager Integration

When HP Network Node Manager i Software is integrated with HP Asset Manager, the Asset Manager portfolio can be automatically populated with device information from the NNMi database.

Value

The HP NNMi–HP Asset Manager integration provides the following benefits:

- Reduces network traffic to the managed devices. NNMi discovers the devices, and Asset Manager synchronizes with the NNMi topology.
- Provides the complete network inventory to Asset Manager. This inventory is kept current through NNMi spiral discover.
- Simplifies network management configuration. Network discovery configuration is stored in NNMi only.

Integrated Products

The information in this chapter applies to the following products:

- Asset Manager with HP Connect-It

  For the list of supported versions, see the *NNMi System and Device Support Matrix*.

- NNMi 9.10

NNMi and Asset Manager must be installed on separate computers. The NNMi management server and the Asset Manager computer can be of the same or different operating systems.

Documentation

The HP NNMi–HP Asset Manager integration is fully described in the *HP Connect-It Connectors* guide, which is available for the Connect-It and Integration Connectors product category at **http://h20230.www2.hp.com/selfsolve/manuals**.

Using the HP NNMi–HP Asset Manager Integration

The steps to enable the HP NNMi–HP Asset Manager integration take place on the Asset Manager server.

Enabling the HP NNMi–HP Asset Manager integration populates the Asset Manager portfolio with NNMi node, interface, and IP address information.

For information about enabling, using, disabling, and troubleshooting the HP NNMi–HP Asset Manager integration, see the *HP Connect-It Connectors* guide.

HP Business Service Management Topology

HP Business Service Management (BSM) software provides tools for managing the availability of applications in production, monitoring system performance, monitoring infrastructure performance, and proactively resolving problems when they arise.

For information about purchasing BSM, contact your HP sales representative.

This chapter contains the following topics:

HP NNMi–HP BSM Topology Integration

The HP NNMi–HP BSM Topology integration populates the BSM Run-time Service Model (RTSM) with the NNMi topology. BSM stores each device in the NNMi topology as a configuration item (CI). BSM RTSM Users and integrated applications can see the relationships among network devices.

Additionally, the integration stores the identifier of populated CIs in the NNMi database. Uses for the CIs of the NNMi-managed devices include the following:

- NNMi components in the MyBSM portal.
- Path health views available from the BSM Real User Monitor (RUM).
- The HP NNMi—HP BSM Operations Management integration can associate incidents regarding NNMi-managed devices with BSM CIs. For more information, see Configuration Item Identifiers on page 564.
- The agent implementation of the HP NNMi–HPOM integration can associate incidents regarding NNMi-managed devices with BSM CIs. For more information, see Configuration Item Identifiers on page 584.

Value

The HP NNMi–HP BSM Topology integration sets up NNMi as the authoritative source for network device status and relationship information. The integration is an enabler for other integrations with BSM. It does not provide access to the BSM user interface from the NNMi console.

Integrated Products

The information in this chapter applies to the following products:

- BSM

  For the list of supported versions, see the *NNMi System and Device Support Matrix*.

- NNMi 9.10

NNMi and BSM must be installed on separate computers. The NNMi management server and the BSM gateway server computer can be of the same or different operating systems.

For the most recent information about supported hardware platforms and operating systems, see the support matrices for both products.

Documentation

This chapter describes how to configure NNMi to communicate with BSM.

The BSM documentation suite describes the BSM features and capabilities in detail. The documentation suite is included on the BSM product media.

Enabling the HP NNMi–HP BSM Topology Integration

⚠ NNMi cannot simultaneously integrate with HP BSM topology and HP Universal CMDB (UCMDB). If the HP NNMi–HP UCMDB integration is configured on this NNMi management server, disable that configuration before enabling the HP NNMi–HP BSM Topology integration. If you want NNMi information in both databases, do *both* of the following in any order:

- Configure the HP NNMi–HP BSM Topology integration, as described in this chapter.
- Configure the BSM integration with UCMDB, as described in the *UCMDB Data Flow Management Guide*, which is included on the UCMDB product media. This manual is also available for the UCMDB product at:
  http://h20230.www2.hp.com/selfsolve/manuals

On the NNMi management server, configure the connection between NNMi and BSM by following these steps:

1 *Optional*. Update the RTSM for interfaces to set the interface display label to prefer interface name over MAC address:

   a In the BSM user interface, open the **CI Type Manager** page (**Admin > RTSM Administration > Modeling > CI Type Manager**).

   b In the **CI Types** pane, select Interface (**Configuration Item > Infrastructure Element > Node Element > Interface**).

   c On the **Default Label** tab in the editing pane, under **CI Type Attributes**, select **InterfaceName**.

   d Under **CI Type Label Definition Format**, set the format to:

```
interface_name | mac_address
```

2 In the NNMi console, open the **HP NNMi–HP BSM Topology Integration Configuration** form (**Integration Module Configuration > HP BSM Topology**).

3 Select the **Enable Integration** check box to make the remaining fields on the form available.

4 Enter the information for connecting to the NNMi management server. For information about these fields, see NNMi Management Server Connection on page 463.

5 Enter the information for connecting to the BSM gateway server. For information about these fields, see BSM Gateway Server Connection on page 463.

6 *Optional*. Enter the information that describes which NNMi nodes should be maintained in BSM. For information about these fields, see BSM Topology Filter on page 464.

7 Click **Submit** at the bottom of the form.

   A new window opens a status message. If the message indicates a problem with connecting to the NNMi management server, click **Return**, and then adjust the values as suggested by the text of the error message.

Using the HP NNMi–HP BSM Topology Integration

The HP NNMi–HP BSM Topology integration populates the following CI types in the BSM RTSM:

- InfrastructureElement > Node

  The nodes in the NNMi topology. You can limit the set of nodes as described in BSM Topology Filter on page 464.

- InfrastructureElement > NodeElement> HardwareBoard

  The cards associated with the Node CIs that the integration populates in BSM.

- InfrastructureElement > NodeElement> Interface

  The interfaces associated with the Node CIs that the integration populates in BSM.

- InfrastructureElement > NodeElement> PhysicalPort

  The ports associated with the Node CIs that the integration populates in BSM.

- InfrastructureElement > NetworkEntity > IpAddress

  The IP addresses of the interfaces associated with the Node CIs that the integration populates in BSM.

- InfrastructureElement > NetworkEntity > IpSubnet

  All subnets in the NNMi topology.

- InfrastructureElement > NetworkEntity > Layer2Connection

  The NNMi Layer 2 connections with at least two connection ends that the integration populates as Node CIs in BSM.

For each CI created in the BSM RTSM, the integration stores the RTSM identifier in the NNMi database.

By default, NNMi does not discover end nodes. Update the NNMi discovery and monitoring configuration to include the end nodes that you want to see in BSM.

The HP NNMi–HP BSM Topology integration forwards NNMi information and updates to the BSM RTSM as a one-way communication. Because NNMi does not know or control how the BSM CI information is used, the integration relies on the BSM aging policies to delete CIs that have not been updated for a set period of time.

The HP NNMi–HP BSM Topology integration enables other products to use the NNMi topology information when they integrate with BSM. There is no direct user interaction with this integration.

Changing the HP NNMi–HP BSM Topology Integration Configuration

1 In the NNMi console, open the **HP NNMi–HP BSM Topology Integration Configuration** form (**Integration Module Configuration > HP BSM Topology**).

2 Modify the values as appropriate. For information about the fields on this form, see The HP NNMi–HP BSM Topology Integration Configuration form contains the parameters for configuring communications between NNMi and BSM. This form is available from the Integration Module Configuration workspace. on page 462.

3 Verify that the **Enable Integration** check box at the top of the form is selected, and then click **Submit** at the bottom of the form.

➤ The changes take effect immediately. You do not need to restart `ovjboss`.

Disabling the HP NNMi–HP BSM Topology Integration

1 In the NNMi console, open the **HP NNMi–HP BSM Topology Integration Configuration** form (**Integration Module Configuration > HP BSM Topology**).

2 Clear the **Enable Integration** check box at the top of the form, and then click **Submit** at the bottom of the form. The integration URL actions are no longer available.

➤ The changes take effect immediately. You do not need to restart `ovjboss`.

Troubleshooting the HP NNMi–HP BSM Topology Integration

This section contains the following topics:

- Interface Labels Appear as MAC Addresses in the BSM User Interface on page 461
- Duplicate CIs for Managed Nodes in the RTSM on page 461

For information about troubleshooting the connection to the RTSM, see the BSM documentation suite.

Interface Labels Appear as MAC Addresses in the BSM User Interface

By default, the RTSM prefers MAC addresses over interface names for an interface label. To display interface names in the BSM user interface, edit the interface model as described in step 1 on page 459.

Duplicate CIs for Managed Nodes in the RTSM

If HP Operations Manager also synchronizes with the RTSM, you might see duplicate CIs for managed nodes in the RTSM. Nodes discovered by HPOM are of CI type Computer, while nodes discovered by NNMi are of CI type Node. This duplication does not affect product performance.

Application Failover and the HP NNMi–HP BSM Topology Integration

If the NNMi management server participates in NNMi application failover, the HP NNMi–HP BSM Topology continues with the new NNMi management server hostname after failover occurs. Failover should be transparent to users of the integration.

The integration does not support automatic failover of the BSM server.

HP NNMi–HP BSM Topology Integration Configuration Form Reference

The **HP NNMi–HP BSM Topology Integration Configuration** form contains the parameters for configuring communications between NNMi and BSM. This form is available from the **Integration Module Configuration** workspace.

Only NNMi users with the Administrator role can access the **HP NNMi–HP BSM Topology Integration Configuration** form.

The **HP NNMi–HP BSM Topology Integration Configuration** form collects information for the following areas:

- NNMi Management Server Connection on page 463
- BSM Gateway Server Connection on page 463
- BSM Topology Filter on page 464

To apply changes to the integration configuration, update the values on the **HP NNMi–HP BSM Topology Integration Configuration** form, and then click **Submit**.

NNMi Management Server Connection

Table 40 lists the parameters for connecting to the NNMi management server. This is the same information that you use to open the NNMi console. You can determine many of these values by examining the URL that invokes an NNMi console session. Coordinate with the NNMi administrator to determine the appropriate values for this section of the configuration form.

Table 40 NNMi Management Server Information

Field	Description
NNMi SSL Enabled	The connection protocol specification. • If the NNMi console is configured to use HTTPS, select the **NNMi SSL Enabled** check box. This is the default configuration. • If the NNMi console is configured to use HTTP, clear the **NNMi SSL Enabled** check box. The integration selects the port for connecting to the NNMi console based on this specification.
NNMi Host	The official fully-qualified domain name of the NNMi management server. This field is read-only.
NNMi User	The user name for connecting to the NNMi web services. This user must have the NNMi Administrator or Web Service Client role.
NNMi Password	The password for the specified NNMi user.

BSM Gateway Server Connection

Table 41 lists the parameters for connecting to the BSM gateway server to communicate with the BSM RTSM. Coordinate with the BSM administrator to determine the appropriate values for this section of the configuration.

Table 41 BSM Gateway Server Information

BSM Gateway Server Parameter	Description
BSM SSL Enabled	The connection protocol specification for connecting to BSM. • If BSM is configured to use HTTPS, select the **BSM SSL Enabled** check box. This is the default configuration. • If BSM is configured to use HTTP, clear the **BSM SSL Enabled** check box.
BSM Host	The fully-qualified domain name of the BSM gateway server.
BSM Port	The port for connecting to BSM. If you are using the default BSM configuration, use port `80` (for non-SSL connections to BSM).
BSM RTSM User	The user name for the BSM RTSM administrator.
BSM RTSM password	The password for the BSM RTSM administrator. A BSM administrator can change the password for the BSM RTSM administrator by using the following URL: **http://<*BSM_hostname*>:21212/ucmdb-ui/applet/applet.jsp**

BSM Topology Filter

By default, the HP NNMi–HP BSM Topology integration conveys information about all nodes and interfaces in the NNMi topology to BSM. If you want the integration to maintain only a subset of the NNMi topology information in BSM, specify one or both of the optional node groups as described in this section.

The scenarios for the filtering NNMi topology information are as follows:

- Definitive—In NNMi, create one node group that explicitly defines every NNMi node to be included in the BSM topology. This approach requires an intimate knowledge of your network topology.

  For example, you might create a node group called BSM_Topology containing the following types of devices:

  - The application servers in the managed environment
  - The routers and switches that connect the application servers

  In this case, specify the node group (for example, BSM_Topology) as the topology filter node group. Do not specify an additional connections node group.

  The integration forwards information about every node in the specified topology filter node group (for example, BSM_Topology) and ignores all other nodes in the NNMi topology.

- Additive—In NNMi, identify (or create) a node group that defines the core infrastructure of the monitored network, and then create another node group that defines the end nodes of interest.

  For example, you might create the following NNMi node groups:

  - The BSM_Core group that contains the Networking Infrastructure Devices node group and other key connective devices
  - The BSM_End_Nodes group that contains the application servers in the managed network

  In this case, specify the first node group (for example, BSM_Core) as the topology filter node group. Also, specify the second node group (for example, BSM_End_Nodes) as the additional connections node group.

  The integration forwards information about every node in the topology filter node group (for example, BSM_Core). The integration then examines each node in the additional connections node group (for example, BSM_End_Nodes) as follows:

  - If the node is connected to one or more nodes in the topology filter node group, the integration forwards the information about that node to BSM.
  - If the node is not connected to any of the nodes in the topology filter node group, the integration ignores that node.

Table 42 lists the optional parameters for specifying a BSM topology filter and provides information about entering values for these parameters.

Table 42 BSM Topology Filter Information

BSM Topology Filter Parameter	Description
Topology Filter Node Group	The NNMi node group containing the primary set of nodes to populate in BSM. The integration populates the RTSM with information about every node in this node group. Enter the name of the node group exactly as it is written (with no quotation marks or extra characters) in the **Name** field of the **Node Group** form in NNMi. If you do not specify a topology filter node group, the HP NNMi–HP BSM Topology integration populates the RTSM with all nodes and interfaces in the NNMi topology. In this case, the integration ignores the value of the **Additional Connections Node Group** field.
Additional Connections Node Group	The NNMi node group containing hints of additional nodes to populate in BSM. The integration populates the RTSM with information about only those nodes in this node group that are connected (in the NNMi topology) to one or more nodes in the topology filter node group. Enter the name of the node group exactly as it is written (with no quotation marks or extra characters) in the **Name** field of the **Node Group** form in NNMi. If you specify a topology filter node group and specify an additional connections node group, the HP NNMi–HP BSM Topology integration forwards information about the nodes and interfaces in the topology filter node group and the connected nodes in the additional connections node group. If you specify a topology filter node group but do not specify an additional connections node group, the HP NNMi–HP BSM Topology integration forwards information about the nodes and interfaces in the topology filter node group only. If you do not specify a topology filter node group, the HP NNMi–HP BSM Topology integration populates the RTSM with all nodes and interfaces in the NNMi topology. In this case, the integration ignores the value of the **Additional Connections Node Group** field.

HP Universal CMDB

HP Universal CMDB (UCMDB) automatically maintains accurate, up-to-date information on infrastructure and application relationships through native integration to HP Discovery and Dependency mapping (DDM). UCMDB is beneficial for the following tasks:

- Using impact modeling to show the rippling effect of infrastructure and application changes before they occur.
- Tracking actual planned and unplanned changes through discovered change history.
- Gaining a shared, authoritative view of the environment through awareness of existing data repositories.

For information about purchasing UCMDB, contact your HP sales representative.

This chapter contains the following topics:

- HP NNMi–HP UCMDB Integration
- Using the HP NNMi–HP UCMDB Integration

HP NNMi–HP UCMDB Integration

The HP NNMi–HP UCMDB integration shares NNMi topology information with UCMDB. UCMDB stores each device in the NNMi topology as a configuration item (CI). UCMDB applies Discovery and Dependency Mapping (DDM) patterns to the CIs for the NNMi topology to predict the impact of a device failure. This impact analysis is available from the UCMDB user interface and also from the NNMi console.

➤ The HP NNMi–HP UCMDB integration information included in this chapter refers to the integration between NNMi and Universal CMDB version 9.0x.

Additionally, the integration stores the identifier of populated CIs in the NNMi database. Uses for the CIs of the NNMi-managed devices include the following:

- The HP NNMi—HP BSM Operations Management integration can associate incidents regarding NNMi-managed devices with UCMDB CIs. For more information, see Configuration Item Identifiers on page 564.

- The agent implementation of the HP NNMi–HPOM integration can associate incidents regarding NNMi-managed devices with UCMDB CIs. For more information, see Configuration Item Identifiers on page 584.

Value

The HP NNMi–HP UCMDB integration sets up NNMi as the authoritative source for network device relationships. The integration provides access to UCMDB impact analysis and CI details from the NNMi console.

Integrated Products

The information in this chapter applies to the following products:

- UCMDB 9.0x.

  For the list of supported versions, see the *NNMi System and Device Support Matrix*.

- NNMi 9.10

NNMi and UCMDB 9.0x cannot be installed on the same computer. The two products must be installed on different computers in either of the following configurations:

- Different operating systems. For example, the NNMi management server is a Linux system, and the UCMDB 9.0x server is a Windows system.
- The same operating system. For example, the NNMi management server is a Windows system, and the UCMDB 9.0x server is a second Windows system.

For the most recent information about supported hardware platforms and operating systems, see the support matrices for both products.

Documentation

The HP NNMi–HP UCMDB 9.0x integration is fully described in the *HP Universal CMDB–HP Network Node Manager (NNMi) Integration Guide*, which is included on the UCMDB 9.0x product media.

Using the HP NNMi–HP UCMDB Integration

⚠ NNMi cannot simultaneously integrate with HP Business Service Management (BSM) topology and HP UCMDB. If the HP NNMi–HP BSM Topology integration is configured on this NNMi management server, disable that configuration before enabling the HP NNMi–HP UCMDB integration. If you want NNMi information in both databases, do *both* of the following in any order:

- Configure the HP NNMi–HP BSM Topology integration, as described in HP Business Service Management Topology on page 457.
- Configure the BSM integration with UCMDB, as described in the *UCMDB Data Flow Management Guide*, which is included on the UCMDB product media. This manual is also available for the UCMDB product at: **http://h20230.www2.hp.com/selfsolve/manuals**

For information about enabling, using, disabling, and troubleshooting the HP NNMi–HP UCMDB integration, see the *HP Universal CMDB–HP Network Node Manager (NNMi) Integration Guide*.

HP Business Availability Center My BSM

HP Business Availability Center (BAC) software provides tools for managing the availability of applications in production, monitoring system performance, monitoring infrastructure performance, and proactively resolving problems when they arise. BAC includes the My BSM portal for viewing reports and real-time product performance information. (Prior to BAC version 8.00, the portal is called My BAC.)

Use the integration information in this chapter to integrate NNMi with BAC versions 7.x and 8.x. For information about integrating NNMi with BSM version 9.x, see the *HP Business Service Management Solutions and Integrations Guide* (version 9.x).

This chapter contains the following topics:

HP NNMi–HP BAC My BSM Integration

The HP NNMi–HP BAC My BSM integration is an enablement for viewing NNMi in the My BSM portal. The integration provides templates for adding NNMi and NNM iSPI for Performance portlets to a My BSM portal. For a quick portal demonstration, you can use the configuration tool in the NNMi console to customize these templates for your environment.

The My BSM administrator can further customize the configuration and the access rights of the default portlets by using the standard My BSM administration interface. The My BSM administrator can also use the My BSM administration interface to create custom portlets for other views of NNMi and the NNMi Smart Plug-ins (NNM iSPIs), and to combine views from multiple NNMi management servers on one portal page.

Value

The HP NNMi–HP BAC My BSM integration extends the information available through the My BSM portal.

Integrated Products

The information in this chapter applies to the following products:

- BAC

  For the list of supported versions, see the *NNMi System and Device Support Matrix*.

  To integrate with BSM version 9.x, use the BAC component gallery. For information about integrating NNMi with BSM version 9.x, see the *HP Business Service Management Solutions and Integrations Guide* (version 9.x).

- NNMi 9.10

For the most recent information about supported hardware platforms and operating systems, see the support matrices for both products.

Documentation

This chapter describes how to configure the default NNMi portlets for My BSM from the NNMi console.

The *Using My BAC Guide*, which is included on the BAC 7.x product media, describes how to configure and maintain My BAC.

The *Using My BSM Guide*, which is included on the BAC 8.x product media, describes how to configure and maintain My BSM.

Default NNMi Modules for My BSM

NNMi provides the following My BSM modules for configuration in the NNMi console:

- The NNMi demonstration module is defined in the `NOC_Demo_Portal.xml` template file. This module presents some key network status information as described in Table 43.
- The NNMi and NNM iSPI for Performance demonstration module is defined in the `NOC_Demo_Portal_iSPIPerf.xml` template file. This module adds some NNM iSPI for Performance reports to the network status information of the NNMi demonstration module. Table 44 on page 473 describes this module.

Table 43 NNMi Demonstration Module Contents

Page	Portlet	Portlet Description
Overview Map	Key Operations Map	The NNMi topology map for the specified node group.
Network Status/Device Health	Node Group Status	Equivalent to the results of the **Actions > Status Details** menu command for the specified node group in the NNMi console.
	Network Status	Equivalent to the **Node Groups** inventory view in the NNMi console.

Table 44 NNMi and NNM iSPI for Performance Demonstration Module Contents

Page	Portlet	Portlet Description
Overview Map	Key Operations Map	The NNMi topology map for the specified node group.
Network Status/Device Health	Node Group Status	Equivalent to the results of the **Actions > Status Details** menu command for the specified node group in the NNMi console.
	Network Status	Equivalent to the **Node Groups** inventory view in the NNMi console.
	Top-N Memory Utilization	The live NNM iSPI for Performance component health report showing the top 10 nodes by memory use.
	Top-N CPU Utilization	The live NNM iSPI for Performance component health report showing the top 10 nodes by CPU use.
NNM iSPI for Performance Exceptions	Top-N Devices by Component Exceptions	The live NNM iSPI for Performance component health dashboard showing the top 5 nodes by CPU use exceptions and the top 5 nodes by memory use exceptions.

Configuring the Demonstration Portlets

This section describes the initial configuration of the demonstration My BSM modules. The My BSM administrator can completely customize portlet content and user access to the portlets.

1. On the NNMi management server, create the module configuration XML file:

   a. In the NNMi console, open the **HP NNMi–HP BAC My BSM Configuration** form (**Integration Module Configuration > HP BAC My BSM**).

   b. Select one of the named XML files to customize:

      — If the NNM iSPI for Performance is not installed in your environment, select the `NOC_Demo_Portal.xml` file.

      — If the NNM iSPI for Performance is installed in your environment, select the `NOC_Demo_Portal_iSPIPerf.xml` file.

   c. Click **Load**.

   d. On each page of the **HP NNMi–HP BAC My BSM Configuration** form, edit the supplied text as appropriate, and then click **Next**. For information about these fields, see HP NNMi—HP BAC My BSM Configuration Form Reference on page 480.

   e. After navigating through all pages of the **HP NNMi–HP BAC My BSM Configuration** form, click **Finish**, and then save the XML file to a known place on your computer.

   f. Close the **HP NNMi–HP BAC My BSM Configuration** form.

2. Import the module configuration into BAC:

   a. On the BAC **Administration** tab, under **My BSM** (or **My BAC**), click **Import portlets and modules** (one of the options for managing portlet definitions).

   b. On the **Import My BSM Objects** page (or the **Import My BAC Objects** page), click **Browse**, and then select the XML file that you saved from the NNMi console.

   c. Select the **Replace same Portlet Definitions** check box.

   d. Select the **Replace same Modules** check box.

   e. Click **Import**.

      The **Import Status** window opens the results of the operation. If the import did not succeed, verify that both check boxes are selected, and then retry the import.

3. View the module in My BSM or My BAC:

   - Verify that each portlet opens the expected information.
   - Use the My BSM or My BAC administration tools to define which users can access the new portlets, to reorganize the pages, to edit the portlet definitions, and so forth.

Creating Custom NNMi Portlets

The easiest way to create a new portlet that opens NNMi or iSPI information is as follows:

1. In the My BSM administration interface, copy an existing NNMi portlet definition.
2. Change the URL in the new portlet definition to point to the information that you want to display in the portal.

   As you edit the portlet definitions, follow the HTML code structure used in the demonstration portlets. For a description of the HTML code structure, see Portlet Definition HTML Reference on page 476.

Determining the Portlet URL

URL for an NNMi console window

For information about how to create a URL for launching an NNMi console window directly, see **Help > NNMi Documentation Library > Integrate NNMi Elsewhere with URLs** in the NNMi console.

URL for an NNM iSPI for Performance report

The procedure for determining the URL for launching an NNM iSPI for Performance report depends on which web browser you are using to view the report.

The URL for accessing the report is the same in any web browser.

In Mozilla Firefox, to determine the URL for launching an NNM iSPI for Performance report, follow these steps:

1. Run the NNM iSPI for Performance report.
2. *Optional.* Click **Show Options** at the top of the report, and then customize the report view.
3. Click **Show URL** at the top of the report.

   The URL for the report is visible below the report banner and customization links. You can copy the URL for use in a portlet definition.
4. *Optional.* Click **Hide URL** to hide the report URL from view.

In Microsoft Internet Explorer, to determine the URL for launching an NNM iSPI for Performance report, follow these steps:

1. Run the NNM iSPI for Performance report.
2. *Optional*. Click **Show Options** at the top of the report, and then customize the report view.
3. Click **Add Bookmark** at the top of the report.
4. In the **Add a Favorite** window, click **Add**.
5. In the favorites list, right-click the favorite that you created in step 4, and then click **Properties**.

   The **URL** field opens the URL for the report. You can copy the URL from this field for use in a portlet definition.

Portlet Definition HTML Reference

The following rules apply to the HTMLPortlet type in BAC:

- Use a single quote character (') instead of the standard double quote character (").
- For every iframe start tag (<iframe>) use a corresponding iframe end tag (</iframe>) because some web browsers do not recognize empty-element <iframe/> tags correctly.
- In the iframe definition, specify one of the following values for id:

id Value	Description
nnmi-portlet	The ID of an iframe that opens an NNMi URL. This ID provides consistent configuration for human readers.
nnmi-auth	The ID of an iframe that manages single sign-on to the NNM iSPI for Performance. The JavaScript function for loading the NNM iSPI for Performance portlet interprets this ID value.
ispiperf-portlet	The ID of an iframe that opens an NNM iSPI for Performance report URL. The JavaScript function for loading the NNM iSPI for Performance portlet interprets this ID value.

NNMi portlet HTML structure

A BAC portlet that opens an NNMi URL contains a single iframe element that identifies the NNMi URL to display. The structure is as follows:

```
<html>
<head></head>
<body>
<iframe id='nnmi-portlet' src='<NNMi_URL>'></iframe>
</body>
</html>
```

Replace *<NNMi_URL>* with the URL for launching an NNMi console window.

For example, the following code defines a portlet that opens the status for the Routers node group. In this example, the height and width values are the suggested values for this portlet. You can change these values as needed.

```
<html>
<head></head>
<body>
<iframe id='nnmi-portlet'
  src='http://nnmi.example.com:8004/nnm/launch
    ?cmd=runTool
    &tool=nodegroupstatus
    &nodegroup=Routers
    &menus=false'
  width='100%'
  height='425px'>
</iframe>
</body>
</html>
```

NNM iSPI for Performance portlet HTML structure

A BAC portlet that opens an NNM iSPI for Performance report URL contains the following elements:

- Within the portlet header, the declaration of the `loadIspiPerf()` JavaScript function. This declaration defines the NNM iSPI for Performance report to display.
- One iframe element that handles single-sign on from NNMi to the NNM iSPI for Performance.
- A second iframe element that opens the NNM iSPI for Performance report named in the `loadIspiPerf()` function declaration of the portlet header.

The structure of a BAC portlet that opens an NNM iSPI for Performance report URL is as follows:

```
<html>
<head>
<script id='ispiperf-load'>function loadIspiPerf()
{
  var ispiperf_url='<Report_URL>';
  document.getElementById('ispiperf-portlet').src =
    ispiperf_url;
}
</script>
</head>
<body onload='loadIspiPerf();'>
<iframe id='nnmi-auth'
  src='http:<NNMi_host>:<NNMi_port>/nnm/launch?cmd=isRunning'>
</iframe>
<iframe id='ispiperf-portlet'></iframe>
</body>
</html>
```

Replace *<Report_URL>* with the URL for launching an NNM iSPI for Performance report. Replace *<NNMi_host>* and *<NNMi_port>* with the fully-qualified domain name of the NNMi management server and the port number for accessing NNMi, respectively.

For example, the following code defines a portlet that opens the node health report for the top N nodes. In this example, the height and width values are the suggested values for this portlet. You can change these values as needed.

```
<html>
<head>
<script id='ispiperf-load'>function loadIspiPerf()
{
  var ispiperf_url=
    'http://nnmi.example.com:8004/ssoservlet/protected
    /reports
      ?reportURL=http://ispiperf.example.com:9300/PerfSpi
      /PerfSpi
        ?package=NodeHealth
          &report=Top%20N%20Live
          &element=All%20Nodes/Components&timeperiod=
          &dow=
          &hod=
          &metric=CPU%20Utilization%20(Avg%25)
          &namespaceID=ErsAuthenticationProvider
          &ssoDomain=example.com';
  document.getElementById('ispiperf-portlet').src =
    ispiperf_url;
}
</script>
</head>
<body onload='loadIspiPerf();'>
<iframe id='nnmi-auth'
  src='http://nnmi.example.com:8004/nnm/launch
    ?cmd=isRunning'
  width='100%'
  height='1px'>
</iframe>
<iframe id='ispiperf-portlet'
  width='100%'
  height='750px'>
</iframe>
</body>
</html>
```

Configuring Single Sign-On for the HP NNMi–HP BAC My BSM Integration

Single sign-on is available for all HP enterprise applications that use identical initialization string values and also share a common network domain name. For information about configuring single sign-on for BAC My BSM, see Configuring Single Sign-On Between NNMi and HP BSM or HP BAC on page 145.

Troubleshooting the HP NNMi–HP BAC My BSM Integration

The NNMi Portlets Appear As a Sign-in Page

Verify the single sign-on configuration:

1 Sign in to the NNMi console with the user name for logging on to My BSM.

If sign in is not successful, ask the NNMi administrator to configure an account for the My BSM user.

2 Make sure that BAC and NNMi use the same initialization strings as described in Configuring Single Sign-On for the HP NNMi–HP BAC My BSM Integration on page 478.

Also see Single Sign-On Does Not Work Correctly on page 479.

An NNMi Portlet Does Not Load Correctly

In the My BSM administration interface, verify the NNMi management server host name and the port number in the portlet URL.

An NNM iSPI for Performance Portlet Does Not Load Correctly

In the My BSM administration interface, verify the NNM iSPI for Performance server host name, port number, and single-sign on domain in the portlet URL.

An NNM iSPI for Performance Portlet Opens an AsynchWait_Requests Error

As a BAC portal page loads an NNM iSPI for Performance portlet, it requests information from the NNM iSPI for Performance Cognos database. When a page contains multiple NNM iSPI for Performance portlets, simultaneous requests to the Cognos database from the single web browser session can result in an `AsynchWait_Requests` error. Reload the portal page.

Single Sign-On Does Not Work Correctly

All NNMi and NNM iSPI for Performance portlets do not load. The web browser might close with a message similar to the following:

```
The page you requested cannot be displayed because the LW-SSO host
has logged out.
```

Verify that all application servers that participate in a single sign-on integration are set to the same GMT time with a maximum difference of 15 minutes.

My BSM Reports HTML Validation Errors When I Save A Portlet Definition

Before you can save new portlets in My BSM, you must configure a setting in a BAC configuration file.

Edit the `<HP Business Availability Center root directory>\HPBAC\conf\dashboard.properties` file to add the following line:

```
Block-URL-Injections=false
```

HP NNMi—HP BAC My BSM Configuration Form Reference

Table 45 lists the fields included on the pages of the **HP NNMi–HP BAC My BSM Configuration** form. Coordinate with the NNM iSPI for Performance administrator to determine the correct value for the NNM iSPI for Performance fields. Text fields might contain any characters. NNMi does not validate configured values. Verify the new portlets in the My BSM portal.

Table 45 Module Configuration Information

Field	Description
Name	The name of the portal module. This text assists navigation within the My BSM portal.
Description	Text that describes the portal module. This text is visible in the My BSM administration interface.
Page Title	The name of a portal page. This text assists navigation within the portal.
Portlet Title	The name of the portlet as it appears in the portal.
Portlet Type	A field required for the My BSM configuration. This field is currently read-only.
NNMi Machine	The URL for accessing the NNMi management server. This field is pre-filled with the hostname and the port number for connecting to the NNMi management server for the current NNMi console session. • For the portlet to access the default NNMi management server, leave the default setting. • For the portlet to access a different NNMi management server, manually enter the correct URL.
NNMi Nodegroup	A list of node groups on the NNMi management server for the current NNMi console session. • If the portlet accesses the default NNMi management server, select a node group from the list. • If the portlet accesses a different NNMi management server, manually enter the correct node group name.
iSPI for Performance Machine	The URL for accessing the NNM iSPI for Performance server. This field is pre-filled with the hostname and the port number for connecting to the NNM iSPI for Performance server from the current NNMi console session. • For the portlet to access the default NNM iSPI for Performance server, leave the default setting. • For the portlet to access a different NNM iSPI for Performance server, manually enter the correct URL.

Table 45 Module Configuration Information (cont'd)

Field	Description
SSO Domain	The domain for single sign-on to the NNM iSPI for Performance.
Disable iSPI for Performance portlets check box	The **Disable iSPI for Performance portlets** check box is available on configuration form pages that define portlet access to NNM iSPI for Performance. If this check box is selected when the page first appears, the NNM iSPI for Performance is not configured on this NNMi management server. Therefore, the fields related to the NNM iSPI for Performance are unset. Clear this check box to enable the fields so that you can manually enter the information for accessing the NNM iSPI for Performance.

HP Network Automation

HP Network Automation software (NA) tracks, regulates, and automates configuration and software changes across globally distributed, multi-vendor networks through process-powered automation.

For information about purchasing NA, contact your HP sales representative.

This chapter contains the following topics:

HP NNMi–HP NA Integration

The HP NNMi–HP NA integration combines the NA configuration change detection capabilities with the NNMi network monitoring capabilities, placing more information at your fingertips when problems occur.

The NNMi integration with Cisco Network Compliance Manager (NCM) works in the same way as the HP NNMi–HP NA integration. The content of this chapter also applies to the HP NNMi–Cisco NCM integration.

The integration provides the following functionality:

- Synchronizes the NNMi and NA topologies for lower ownership cost and better management coverage of provisioned devices.
- Automatically runs NA device diagnostics when certain NNMi incidents occur.
- Prevents unnecessary alarming in NNMi while devices are out of service as NA applies device configuration updates.
- Updates the NNMi configuration with information for accessing managed devices.

Additionally, without exiting the NNMi console, you can connect to NA to view information about NA-managed devices and configuration change events. While in NA, you can perform any NA functions for which you have the necessary credentials.

The HP NNMi–HP NA integration adds menu items to the NNMi console for opening connections to NA and for viewing configuration information on devices managed by NA. These tools provide the following functionality:

- View detailed device information, including vendor, model, modules, operating system version, and recent diagnostic results.
- View device configuration changes and configuration history.
- Compare configurations (typically the most recent and last previous configurations) to see what changed, why, and who made the changes.
- View device compliance information.
- Run NA diagnostics and command scripts from NNMi nodes.
- Detect connections with mismatched speed or duplex configurations.

➤ These features are not available for network devices that are not configured in NA or for NA devices for which change detection is disabled.

Value

The HP NNMi–HP NA integration provides the following features and benefits in an environment already running both NNMi and NA:

- Alarm integration—NNMi integration communicates NA configuration change information to the NNMi console, enabling you to quickly identify whether configuration changes might have caused network problems. From within NNMi, you can quickly access NA functionality to view specific configuration changes and device information, identify who made the change, and roll back to the previous configuration to restore network operation. Because a majority of network outages are caused by device configuration errors, this feature can enhance both problem identification and response time in resolving network downtime.
- Access to NA configuration history from NNMi—In the NNMi console, a device-level menu provides access to NA features for reviewing configuration changes. For any device in the NA database, this feature opens configuration changes side-by-side so that you can easily view changes. You can also view configuration history.
- Operations efficiency—Network operations personnel can monitor and investigate information from two data sources within a single screen.

Integrated Products

The information in this chapter applies to the following products:

- NA

  For the list of supported versions, see the *NNMi System and Device Support Matrix*.

- NNMi 9.10

  The NNM iSPI NET license is no longer required for this integration.

Integration Configuration Details

The integration is limited to one NA server connected with one NNMi management server. NNMi and NA must be in the same network segment (also called an NA realm).

NNMi and NA can be installed on the same computer or on different computers.

For NNMi and NA to run correctly on the same computer, you must install NNMi before installing NA. If you install NA before installing NNMi, the NNMi installation reports a port conflict with NA and does not complete.

The two products can be installed on different computers in either of the following configurations:

- Different operating systems. For example, the NNMi management server is a Linux system, and the NA server is a Windows system.
- The same operating system. For example, the NNMi management server is a Windows system, and the NA server is a second Windows system.

For the most recent information about supported hardware platforms and operating systems, see the support matrices for both products.

Documentation

This chapter describes how to configure and use the integration.

Enabling the HP NNMi–HP NA Integration

Enabling the HP NNMi—HP NA integration sets the NNMi management server as the definitive topology master in the managed environment. In NNMi, create one node group containing the nodes to synchronize with the NA inventory. The integration synchronizes the contents of this node group with the appropriate NA Security partition as described in Topology Synchronization Between NNMi and NA on page 490.

This section describes the following procedures:

- Integration Configuration Upgraded from NNMi 9.0x on page 486
- New Integration Configuration on page 488

Integration Configuration Upgraded from NNMi 9.0x

Prior to NNMi version 9.10, NA provided the NNMi connector tool that established communication between NNMi and NA. NNMi now provides this functionality; the NA-provided NNMi connector is no longer used.

If the HP NNMi—HP NA integration was configured on an NNMi 9.0x management server, the process of upgrading to NNMi 9.10 disables the integration (but retains the configuration values). Objects in the NA database still contain the NNMi UUID and will be synchronized with the current NNMi topology when you enable the integration from the upgraded NNMi management server.

The integration now provides for single sign-on between the NNMi console and the NA user interface.

Beginning with NNMi 9.1x Patch 1, you can configure NNMi to map NNMi security groups to NA partitions. That means that, after you select the `Map NNMi security groups to NA partitions` check box and submit the change, a node synchronized to NA will always be added or updated to be in a security partition having the same name as that node's NNMi security group.

If a partition does not exist, NNMi creates one having the same name as the NNMi security group, associates it with the NA `Site` view with an *NNMi Security Group* description. NNMi's `Default Security Group` maps to NA's `Default Site` partition.

In this document, the term NA partition refers to the specific NA partition NNMi creates for each node. This NA partition has the same name as the NNMi security group.

The NA administrator should promptly configure security for NA users mapped to the newly created partitions. These security configurations should be based on the corresponding security constraints for the associated security groups in NNMi.

To enable the HP NNMi—HP NA integration for the NNMi 9.10 management server, follow these steps:

1. Verify that NA has been upgraded to a supported version, as listed in the "Integrations" section of the *NNMi System and Device Support Matrix*.
2. Uninstall the NNMi connector from the NNMi management server:
   - *Windows*: Open the Control Panel, click **Add or Remove Programs**, then remove **HP NA - HP Network Node Manager connector**.
   - *Linux or Solaris*: Run the following command:

     ```
     NA and NNMi installed on the same server:
     $NAINSTALLDIR/UninstallConnector/Uninstall\ NA

     NA and NNMi installed on separate servers:
     $NAINSTALLDIR/UninstallerData/Uninstall\ NA
     ```

   The default value of `$NAINSTALLDIR`:

   ```
   NA and NNMi installed on the same server: /opt/NA
   NA and NNMi installed on separate servers (Windows): C:\NA
   NA and NNMi installed on separate servers (Linux): /root/NA
   ```

3. Delete the remnant `integration.jar` file from the system:
   a. Stop the NA ManagementEngine service:

- *Windows*: Open the **Services** control panel (**Start > Settings > Control Panel > Administrative Tools > Services**). In the list of services, right-click **TrueControl ManagementEngine**, and then click **Stop**.
- *Linux or Solaris*: Run the following command:

  ```
  /etc/init.d/truecontrol stop
  ```

b Manually remove the `integration.jar` file from the following location:

- *Windows*: `%NAINSTALLDIR%\server\ext\jboss\server\default\lib\integration.jar`
- *Linux or Solaris*: `$NAINSTALLDIR/server/ext/jboss/server/default/lib/integration.jar`

c Restart the NA ManagementEngine service:

- *Windows*: Open the **Services** control panel (**Start > Control Panel > Administrative Tools > Services**). In the list of services, right-click **TrueControl ManagementEngine**, and then click **Start**.
- *Linux or Solaris*: Run the following command:

  ```
  /etc/init.d/truecontrol restart
  ```

4 *Optional*. Configure single sign-on between NNMi and NA as described in Configuring Single Sign-On Between NNMi and HP NA on page 147.

5. In the NNMi console, configure the connection from NNMi to NA:
   a. Open the **HP NNMi–HP NA Integration Configuration** form (**Integration Module Configuration > HP NA**).
   b. Select the **Enable Integration** check box to make the remaining fields on the form available.

      The **HP NNMi–HP NA Integration Configuration** form contain the values from the NNMi 9.0x configuration. The new fields on this form are set to their default values.
   c. Enter values for the new integration configuration fields (**Topology Filter Node Group**, **Topology Synchronization Interval**, and **Discover Device Drivers in NA**).

      For information about these fields, see Integration Behavior on page 503.
   d. Click **Submit** at the bottom of the form.

      A new window opens a status message. If the message indicates a problem with connecting to the NA server, click **Return**, and then adjust the values for connecting to the NA server as suggested by the text of the error message.
6. If the NA menu items are not available on the NNMi console **Actions** menu, log out of the NNMi console, and then log back in.

New Integration Configuration

To enable the HP NNMi—HP NA integration, follow these steps:

1. *Optional*. Configure single sign-on between NNMi and NA as described in Configuring Single Sign-On Between NNMi and HP NA on page 147.
2. *Optional*. If you want the integration to discover the drivers on devices in the synchronized topology, specify the SNMP configuration for the nodes in the NNMi topology. In the NA user interface, follow these steps:
   a. Open the **Device Password Rule** page (**Devices > Device Tools > Device Password Rules**).
   b. Create one or more password rules that specify how to communicate with the nodes in the NNMi topology.
3. In the NNMi console, configure the connection from NNMi to NA:
   a. Open the **HP NNMi–HP NA Integration Configuration** form (**Integration Module Configuration > HP NA**).
   b. Select the **Enable Integration** check box to make the remaining fields on the form available.
   c. Enter the information for connecting to the NNMi management server. For information about these fields, see NNMi Management Server Connection on page 502.
   d. Enter the information for connecting to the NA server. For information about these fields, see NA Server Connection on page 503.

e. Enter values for the remaining fields:

   For information about these fields, see Integration Behavior on page 503.

f. Click **Submit** at the bottom of the form.

   A new window opens a status message. If the message indicates a problem with connecting to the NA server, click **Return**, and then adjust the values for connecting to the NA server as suggested by the text of the error message.

4. *Optional*. In the NA user interface, alter the default settings of the NA functionality provided by the integration:

   a. Open the **Administrative Settings - 3rd Party Integrations** page (**Admin > Administrative Settings > 3rd Party Integrations**).

   b. Verify that **Enabled** is selected for **3rd Party Integrations**.

   c. Change the selections for any of the following fields:

      — **Rediscover Hosts After Tasks**

      — **Out of Service Events**

      — **If the device task fails**

      — **If device compliance check fails after the task completed**

      — **Propagate SNMP Community Strings**

      For information about these fields, see NNMi Integration Configuration in NA Reference on page 504.

   d. Click **Save** at the bottom of the page.

5. *Optional*. If you want the integration to detect connections with mismatched speed or duplex configurations, populate the MAC addresses for the interfaces of the NNMi devices in the NA topology. In the NA user interface, follow these steps:

   a. For each node in the NNMi topology, verify that the NNMUuid property is set on the corresponding device in the NA inventory.

      The integration topology synchronization process sets the NNMUuid property. This property is listed in the **Device Details** section of the device page in NA.

   b. On the **Device Password Rule** page (**Devices > Device Tools > Device Password Rules**), create one or more password rules that specify how to communicate with the nodes in the NNMi topology.

      If you created password rules in step 2 on page 488, you do not need to do so again.

   c. On the **New Task - Discover Driver** page (**Devices > Device Tasks > Discover Driver**), discover the drivers for the devices imported from the NNMi topology.

      If you configured the integration to discover drivers, the integration has already completed this step.

   d. Create a snapshot of the devices imported from the NNMi topology (**Devices > Device Tasks > Take Snapshot**).

      If you configured the integration to discover drivers, the integration has already completed this step.

   e. Run the **NA Topology Data Gathering** diagnostic (**Devices > Device Tasks > Run Diagnostics**) for the devices imported from the NNMi topology.

f Verify that each device synchronized with the NNMi topology has a MAC address for each of its interfaces.

  On a device page, click **View > Device Detail > MAC Addresses** to display the MAC addresses for that device.

6 If the NA menu items are not available on the NNMi console **Actions** menu, log out of the NNMi console, and then log back in.

Using the HP NNMi–HP NA Integration

The HP NNMi–HP NA integration adds functionality to both NNMi and NA. This section contains the following topics:

- Topology Synchronization Between NNMi and NA on page 490
- NNMi Functionality Provided by the Integration on page 492
- NA Functionality Provided by the Integration on page 495

Topology Synchronization Between NNMi and NA

The HP NNMi—HP NA integration dynamically synchronizes the topology for the nodes in the specified NNMi synchronization node group with the devices in the appropriate NA security partition. The integration matches NNMi nodes with NA devices by comparing hostnames and IP addresses (if necessary). The integration adds the NA ID to each synchronized NNMi node and the NNMi UUID to each synchronized NA device.

The **Topology Filter Node Group** parameter on the **HP NNMi–HP NA Integration Configuration** form specifies the NNMi synchronization node group.

This synchronization occurs as follows:

- When the integration is first enabled on the **HP NNMi–HP NA Integration Configuration** form, the integration performs a complete topology synchronization between the NNMi synchronization node group and the appropriate NA security partition.
  - If any NNMi nodes in the synchronization node group do not exist in NA, the integration adds these nodes to the appropriate NA security partition.
  - If any NNMi nodes in the synchronization node group already exist in NA, the integration moves these devices to the NA Default Site partition or into the appropriate NA security partition if NNMi Security Group to NA Partition mapping is enabled.
  - If any devices in the NA inventory are not in the NNMi synchronization node group, the integration sends discovery hints to NNMi for these devices. The NNMi auto-discovery rule configuration determines whether these nodes are discovered. The NNMi node group configuration determines which node groups include the devices hinted by NA.

  It is possible for the NA inventory to contain nodes that are not in the NNMi synchronization node group. All nodes in the NNMi synchronization node group are in the appropriate NA security partition after synchronization completes.

- After initial synchronization, the integration maintains the topology synchronization as follows:
  - When a new node is added to the NNMi synchronization node group, the integration creates this device in the appropriate NA security partition.
  - When a new device is added to the NA inventory, the integration sends a discovery hint to NNMi.
    - The NA devices are part of the appropriate NA Security partition established when you enabled the HP NNMi—HP NA integration.
    - The NA devices can be identified by an IP address.
    - The NA devices do not have an associated NNMi UUID.
    - The NA devices are not members of the NNMi node group that contains the nodes to synchronize with the NA inventory.
  - When a synchronized node is deleted from NNMi, the integration unmanages the corresponding device in NA. The device history is still available for unmanaged devices in NA.
  - When a synchronized device is deleted from NA, the integration deletes the corresponding node from the NNMi topology.

If you have an auto-discovery rule defined in NNMi that prevents NNMi from acting on the hints from NA, do the following:

1. Modify the auto-discovery rule to include those devices that are in the appropriate NA Security partition, but not in the NNMi node group containing the nodes to synchronize with the NA inventory.
2. Repeat the steps to enable the NNMi-NA integration so NNMi can act on the NA hints sent to NNMi.

When a synchronized node is moved out of the NNMi synchronization node group to a different node group, the NA inventory is not immediately affected. However, if this node is later deleted from NNMi, the integration unmanages the corresponding device in NA. Likewise, if this node is later deleted from NA, the integration deletes the corresponding node from the NNMi topology.

Periodic Synchronization Considerations

Periodically, the HP NNMi–HP NA integration performs a complete topology synchronization from NNMi to NA. The HP NNMi–HP NA integration does not perform a complete topology synchronzation from NA to NNMi. If the HP NNMi–HP NA integration remains enabled, this periodic synchronization follows the same process as the synchronization that occurs when the integration is first enabled.

The **Topology Synchronization Interval** parameter on the **HP NNMi–HP NA Integration Configuration** form specifies the frequency of periodic topology synchronization.

Consider the following guidelines when choosing the topology synchronization interval:

- Topology synchronization is a fail-safe mechanism. If the connection between the NNMi management server and the NA server is highly reliable, the topology synchronization interval can be large.
- The recommended minimum topology synchronization interval for 500 or fewer synchronized nodes is 24 hours. For each additional 500 synchronized nodes, consider adding another 24 (or more) hours.

Periodic topology synchronization is load balanced with NNMi Spiral Discovery and paced to avoid overloading the NNMi management server. During periods of high discovery activity, topology synchronization remains quiet.

Support for HP Blade System Virtual Connect Devices

HP Blade System Virtual Connect devices can federate to form a Virtual Connect domain consisting of a primary device and one or more standby and slave devices. The integration should pass to the NA inventory information about only those Virtual Connect devices that are acting as a domain primary or as standalone devices.

To limit which Virtual Connect devices are synchronized with the NA inventory, follow these steps:

1. Create one or more NNMi node groups based on an additional filter that uses any of the following capabilities:
   - com.hp.nnm.capability.node.hpvcStandalone
   - com.hp.nnm.capability.node.hpvcPrimary
   - com.hp.nnm.capability.node.hpvcStandby
   - com.hp.nnm.capability.node.hpvcSlave
2. Create one parent node group for all node groups created in step 1.

   In this parent node group, also include any other devices that should be synchronized with the NA inventory.
3. Update the **Topology Filter Node Group** parameter on the **HP NNMi–HP NA Integration Configuration** form with the name of the parent node group. For more information, see Integration Behavior on page 503.

NNMi Functionality Provided by the Integration

The HP NNMi–HP NA integration provides communication from NNMi to NA for the following functionality:

- Launching NA Views from the NNMi Console on page 492
- Configuring NA Diagnostics and Command Scripts as Incident Actions on page 493
- Viewing the Results of Incident Actions that Access NA on page 494
- Identifying Layer 2 Connections with Mismatched States on page 494

Launching NA Views from the NNMi Console

The HP NNMi–HP NA integration provides links to NA from the NNMi console.

Enabling the HP NNMi–HP NA integration adds the following items to the **Actions** menu in the NNMi console:

- **Show HP NA Diagnostic Results**—Opens a list of the NA tasks that have been scheduled for the device in an NNMi incident. Select a task to view the task results. For more information, see Viewing the Results of Incident Actions that Access NA on page 494.

- **Rerun HP NA Diagnostics**—Runs any NA actions that are configured for the device in an NNMi incident. For more information, see Viewing the Results of Incident Actions that Access NA on page 494.
- **Show mismatched connections**—Opens a table of all layer 2 connections with possible speed or duplex configuration differences. For more information, see Identifying Layer 2 Connections with Mismatched States on page 494.
- **View HP NA Device Information**—Opens the current NA **Device Details** page for the device selected in NNMi.
- **View HP NA Device Configuration**—Opens the NA **Current Configuration** page for the device selected in NNMi.

➤ If real-time change detection is disabled for a device, the information shown is the configuration NA captured at the last device polling interval. If configuration changes were made following that capture, the information on the **Current Configuration** page might not be the actual current configuration.

- **View HP NA Device Configuration Diffs**—Opens the NA **Compare Device Configuration** page for the device selected in NNMi.
- **View HP NA Device Configuration History**—Opens the **NA Device Configurations History** page for the device selected in NNMi.
- **View HP NA Policy Compliance Report**—Opens the NA **Policy, Rule and Compliance Search Results** page for the device selected in NNMi.
- **Telnet to HP NA Device**—Opens a **Telnet** window for connecting to the device selected in NNMi.
- **SSH to HP NA Device**—Opens an **SSH** window for connecting to the device selected in NNMi.
- **Launch HP NA**—Opens the NA user interface.
- **Launch HP NA Command Scripts**—Opens the **New Task—Run Command Script** page in NA. The page is pre-filled for the node or incident selected in the NNMi console.
- **Launch HP NA Diagnostics**—Opens the **New Task—Run Diagnostics** page in NA. The page is pre-filled for the node or incident selected in the NNMi console.

For information about using the NA functionality, see the *HP Network Automation User's Guide*.

Configuring NA Diagnostics and Command Scripts as Incident Actions

Enabling the HP NNMi–HP NA integration modifies some out-of-the-box NNMi incidents to include incident actions that access NA diagnostics each time the associated incident type occurs. Table 46 lists the modified incidents.

Table 46 NNMi Incidents Configured with NA Diagnostics

NNMi Incident	NA Diagnostic
OSPFNbrStateChange	Show Neighbor
OSPFVirtIfStateChange	Show Neighbor

Table 46 NNMi Incidents Configured with NA Diagnostics (cont'd)

NNMi Incident	NA Diagnostic
OSPFIfStateChange	Show Neighbor Show Interfaces
InterfaceDown	Show Interfaces
CiscoChassisChangeNotification	Show Module

You can add an action that accesses NA to any other NNMi incident, and you can modify the default incident actions. On the **Actions** tab for an incident, add a new lifecycle transition action with **Command Type** of `ScriptOrExecutable`. In the **Command** text box, enter either `naruncmdscript.ovpl` or `narundiagnostic.ovpl` with the appropriate arguments. For examples, see the action configurations of the incidents listed in Table 46.

Viewing the Results of Incident Actions that Access NA

When an incident of a type that has been configured with an NA action arrives, NNMi initiates the configured action and stores the task ID of the diagnostic or command script as an attribute of that incident. The presence of the task ID enables the **Show HP NA Diagnostic Results** and **Rerun HP NA Diagnostics** items on the **Actions** menu.

To view the outcome of the action at the time the incident occurred, in an NNMi incident view, select the incident, and then select **Actions > Show HP NA Diagnostic Results**.

To view current results of the configured action, in an NNMi incident view, select the incident, and then select **Actions > Rerun HP NA Diagnostics**.

If you run the task multiple times, NNMi lists the most recent task ID on the **Custom Attributes** tab of the **Incident** form. The **Show HP NA Diagnostic Results** action opens all of the tasks that have been run for the incident so that you can compare the results from different runs.

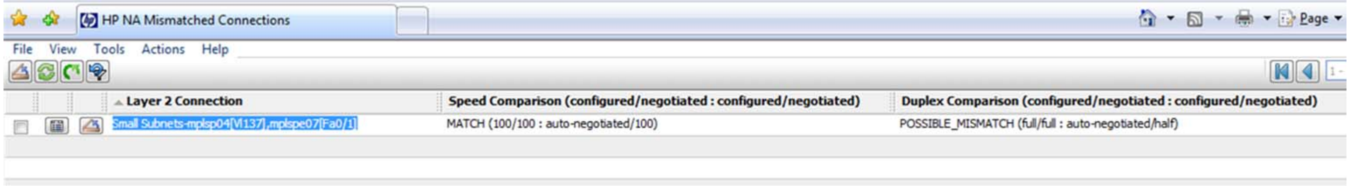
Identifying Layer 2 Connections with Mismatched States

When the HP NNMi—HP NA integration is enabled, NNMi periodically queries NA for the speed and duplex settings of the two interfaces on either end of each layer 2 connection in the NNMi topology. Additionally, NNMi queries NA for the speed and duplex settings of the interfaces for any new connection added to the NNMi topology and, when the NNM iSPI Performance for Metrics is running, for any connection with performance threshold exceptions that might indicate a mismatched connection. NNMi uses a mismatch detection algorithm to determine whether the values might result in a mismatched connection.

NNMi can perform the mismatch analysis only when the NA inventory includes the MAC addresses for both interfaces that form a layer 2 connection. If the NA interface records do not include valid MAC addresses, run the NA **Topology Data Gathering** diagnostic to update the MAC address fields. For more information, see step 5 on page 489.

The **Actions > Show mismatched connections** command opens a table, shown in Figure 42, of layer 2 connections that NNMi suspects might contain speed mismatches, duplex mismatches, or both speed and duplex mismatches.

Figure 42 Example Mismatched Connections Table



Layer 2 Connection	Speed Comparison (configured/negotiated : configured/negotiated)	Duplex Comparison (configured/negotiated : configured/negotiated)
Small Subnets-mplsp04[Vl137],mplspe07[Fa0/1]	MATCH (100/100 : auto-negotiated/100)	POSSIBLE_MISMATCH (full/full : auto-negotiated/half)

For each suspect connection, the table lists the speed and duplex values for the interfaces on either side of the connection and an interpretation of the data. The possible interpretations are as follows:

- `MATCH` indicates that the speed values and duplex values most likely result in a properly functioning layer 2 connection.
- `POSSIBLE_MISMATCH` indicates that the speed values, the duplex values, or both speed and duplex values might conflict, resulting in a poor or non-performing connection.
- `MISMATCH` indicates that the speed values, the duplex values, or both speed and duplex values most likely conflict, resulting in a poor or non-performing connection.

The **HP NA Connection Check Interval** parameter on the **HP NNMi–HP NA Integration Configuration** form specifies the frequency of the connection queries.

NA Functionality Provided by the Integration

The HP NNMi–HP NA integration provides communication from NA to NNMi for the following functionality:

- Sending Device Configuration Change Notifications on page 495
- Maintaining Accurate Device Information on page 495
- Disabling Network Management During Device Configuration on page 496
- Propagating Device Community String Changes on page 497
- NA Event Rules on page 497

Sending Device Configuration Change Notifications

NA sends SNMP traps to NNMi when a device is added to the NA inventory and when the configuration changes on a device in the NA inventory. The NNMi operator can see these traps in the incident views and investigate the changes if necessary.

The integration adds the NASnmpTrapv1 and NASnmpTrapv2 SNMP trap incident configurations to NNMi.

Maintaining Accurate Device Information

For certain device configuration tasks, after the task completes, NA triggers NNMi to rediscover the device.

The **Rediscover Host After Tasks** field on the NA **Administrative Settings - 3rd Party Integrations** page specifies the device configuration tasks that trigger NNMi to rediscover a device. The default selections are:

- Update Device Software
- Deploy Passwords
- Reboot Device
- Discover Driver

You can select any or all of the following additional tasks:

- Run Command Script
- Run Diagnostics
- Delete ACLs
- Configure Syslog
- Run ICMP Test
- Take Snapshot
- Synchronize Startup and Running
- OS Analysis

To disable this feature, clear all selections from the task list.

Disabling Network Management During Device Configuration

For certain device configuration tasks, NA triggers NNMi to set the device to the DISABLED status during the configuration process. This administrative status suppresses NNMi monitoring of the device to prevent unnecessary incidents. Before configuring a device, NA sends an out-of-service event to NNMi. After device configuration succeeds, NA sends an in-service event to NNMi, which removes the DISABLED status from the device and resumes regular state polling.

The **Out of Service Events** field on the NA **Administrative Settings - 3rd Party Integrations** page specifies the device configuration tasks that trigger NNMi to set a device to the DISABLED status during the task. The default selections are:

- Update Device Software
- Deploy Passwords
- Reboot Device

You can select any or all of the following additional tasks:

- Run Command Script
- Run Diagnostics
- Delete ACLs
- Configure Syslog
- Discover Driver
- Run ICMP Test
- Take Snapshot

- Synchronize Startup and Running
- OS Analysis

To disable this feature, clear all selections from the task list.

If device configuration does not complete satisfactorily, the behavior depends on the integration configuration.

- The **If the device task fails** setting on the NA **Administrative Settings - 3rd Party Integrations** page specifies whether the integration should remove or retain the DISABLED status in NNMi if device configuration is not successful.
- The **If device compliance check fails after the task completed** setting on the NA **Administrative Settings - 3rd Party Integrations** page specifies whether the integration should remove or retain the DISABLED status in NNMi if the device configuration is not compliant.

These settings apply to all device tasks selected in the **Out of Service Events** field. You cannot set the recovery behavior per task.

Propagating Device Community String Changes

When SNMP community string propagation is enabled, the integration behaves as follows:

- If the SNMPv1 or SNMPv2c community string that NA uses for accessing a synchronized device changes, NA informs NNMi of the change. NNMi then updates its settings for communicating with that device.

  NNMi immediately starts using the new community string for the device.

  NA sends updates to NNMi only when the community string for managing a device changes. NNMi does not receive updates when NA deploys a new community string to a device.

- If a new device is added to the NA inventory, NA informs NNMi of the SNMPv1 and SNMP v2c community strings that NA uses for managing the device.

The integration does not propagate SNMPv3 users from NA to NNMi.

The **Propagate SNMP Community Strings** setting on the NA **Administrative Settings - 3rd Party Integrations** page specifies whether the integration should forward SNMP community strings from NA to NNMi. By default, community string propagation does not occur.

NA Event Rules

NA event rules define how NA communicates with the NNMi management server.

Do not modify or delete these event rules in NA.

The integration defines the following event rules in NA:

- NA/NNMi Integration via SNMP Traps

  When a new device is added to the NA inventory or a device configuration is changed, this NA event sends an SNMP trap to NNMi. For more information, see Sending Device Configuration Change Notifications on page 495.

- NA/NNMi Topology Synchronization for Device Addition

  When a new device is added to the NA inventory, this NA event sends a device hint to NNMi. For more information, see Topology Synchronization Between NNMi and NA on page 490.

- NA/NNMi Topology Synchronization for Device Deletion

  When a device is deleted from the NA inventory, this NA event sends a request to delete the device from the NNMi topology. For more information, see Topology Synchronization Between NNMi and NA on page 490.

- NA/NNMi Integration Rediscover Host

  When the configuration for a device in the NA inventory changes, this NA event requests the latest NNMi status for the device. For more information, see Maintaining Accurate Device Information on page 495.

- NA/NNMi Integration Out Of Service

  When a task is started, this NA event sets the device to the OUT OF SERVICE state in NNMi. After the task completes, this event sets the device back to the IN SERVICE state in NNMi. For more information, see Disabling Network Management During Device Configuration on page 496.

- NA/NNMi Integration Snmp Community String Propagate

  When the Last Used Device Password Changed is changed for a device in the NA inventory, this NA event sends the community string that NA is using to manage the device to NNMi. For more information, see Propagating Device Community String Changes on page 497.

Changing the HP NNMi–HP NA Integration

1. In the NA user interface, open the **Administrative Settings - 3rd Party Integrations** page (**Admin > Administrative Settings > 3rd Party Integrations**).

   a. Modify the values as appropriate. For information about the fields on this form, see the following references:

      — Maintaining Accurate Device Information on page 495

      — Disabling Network Management During Device Configuration on page 496

      — Propagating Device Community String Changes on page 497

   b. Click **Save** at the bottom of the page.

2. In the NNMi console, open the **HP NNMi–HP NA Integration Configuration** form (**Integration Module Configuration > HP NA**).

   a. Modify the values as appropriate. For information about the fields on this form, see HP NNMi–HP NA Integration Configuration Form Reference on page 501.

   b. Verify that the **Enable Integration** check box at the top of the form is selected, and then click **Submit** at the bottom of the form.

➤ The changes take effect immediately. You do not need to restart `ovjboss`.

Disabling the HP NNMi–HP NA Integration

1. In the NNMi console, open the **HP NNMi–HP NA Integration Configuration** form (**Integration Module Configuration > HP NA**).
2. Clear the **Enable Integration** check box at the top of the form, and then click **Submit** at the bottom of the form. The integration actions are no longer available.

The changes take effect immediately. You do not need to restart `ovjboss`.

Troubleshooting the HP NNMi–HP NA Integration

This section contains the following topics:

- Test the Integration on page 499
- NA Devices are Missing from the NNMi Topology on page 501

Test the Integration

If the integration has worked successfully in the past, it is possible that some aspect of the configuration, for example, the NNMi or NA user password, has changed recently. Try updating the integration configuration as described in HP NNMi–HP NA Integration Configuration Form Reference on page 501, before walking through this entire procedure.

1. In the NNMi console, open the **HP NNMi–HP NA Integration Configuration** form (**Integration Module Configuration > HP NA**).

   For information about the fields on this form, see HP NNMi–HP NA Integration Configuration Form Reference on page 501.

2. To check the status of the integration, in the **HP NNMi–HP NA Integration Configuration** form, click **Submit** at the bottom of the form (without making any configuration changes).

   When successful, this step initiates a complete topology synchronization between NNMi and NA.

   A new window opens a status message.

   If the message indicates a problem with connecting to the NA server, NNMi and NA are not able to communicate. Continue with step 3 of this procedure.

3. To verify the accuracy and access level of the NA credentials, log on to the NA user interface with the credentials for the **NA User** from the **HP NNMi–HP NA Integration Configuration** form.

   If you cannot log on to the NA user interface, contact the NA administrator to verify your logon credentials.

4. To verify that the connection to the NA server is configured correctly, in a web browser on the NNMi management server, enter the following URL:

   http://<*naserver*>:<*naport*>/soap

Where the variables are related to values on the **HP NNMi–HP NA Integration Configuration** form as follows:

- *<naserver>* is the value of **NA Host**.
- *<naport>* is the value of **NA Port**.

If the NA web service is running on the specified server and port, the NA server responds with a message similar to:

```
NAS SOAP API: Only handles HTTP POST requests
```

- If the expected message appears, continue with step 5.
- If you see an error message, the connection to the NA server is not configured correctly. Contact the NA administrator to verify the information you are using to connect to the NA web services. Continue to troubleshoot the connection to NA until you see the expected message.

5 Verify that the connection to NNMi is configured correctly:

If you used the information described in this step to connect to the NNMi console in step 1 of this procedure, you do not need to reconnect to the NNMi console. Continue with step 6.

a In a web browser on the NA server, enter the following URL:

http://<*NNMiserver*>:<*port*>/nnm/

Where the variables are related to values on the **HP NNMi–HP NA Integration Configuration** form as follows:

— <NNMiserver> is the value of **NNMi Host**.

— <port> is the value of **NNMi Port**.

b When prompted, enter the credentials for an NNMi user with the Administrator role.

You should see the NNMi console. If the NNMi console does not appear, contact the NNMi administrator to verify the information you are using to connect to NNMi. Continue to troubleshoot the connection to NNMi until the NNMi console appears.

You cannot log on to the NNMi console as a user with the Web Service Client role.

6 Contact the NNMi administrator to verify the values of the **NNMi User** with the Web Service Client role and the corresponding **NNMi Password**.

7 Update the **HP NNMi–HP NA Integration Configuration** form with the values that you used for successful connections in step 4 and step 5 of this procedure. Also, re-enter the NNMi user and password from step 6 on this form.

For more information, see HP NNMi–HP NA Integration Configuration Form Reference on page 501.

8 Click **Submit** at the bottom of the form.

9 If the status message still indicates a problem with connecting to the NA server, do the following:

a Clear the web browser cache.

b Clear all saved form or password data from the web browser.

c Close the web browser window completely, and then re-open it.

d Repeat step 7 and step 8 of this procedure.

10 Test the configuration by launching one of the actions listed in Using the HP NNMi–HP NA Integration on page 490.

NA Devices are Missing from the NNMi Topology

If a device in the NA inventory does not appear in the NNMi synchronization node group, follow these steps:

1 Examine the NNMi node inventory to determine whether the device is in the topology but in a different node group.

If this is the case, update the definition of the NNMi synchronization node group to include the device.

2 Examine the NNMi IP address inventory to determine whether the IP address used in NA is listed in NNMi.

If the IP address is included in NNMi, determine which node hosts the IP address. This node should be synchronized with the NA device. NNMi might be using a different management address for this node than the IP address that NA sent as a discovery hint.

3 Optionally re-enable the integration.

NA only sends discovery hints when the integration is enabled and when a new device is added to the NA inventory. If the device was added to NA during a network outage or before the NNMi synchronization node group and auto-discovery rules were correctly included, re-enable the integration to cause NA to re-send the discovery hint.

Application Failover and the HP NNMi–HP NA Integration

If the NNMi management server participates in NNMi application failover, the HP NNMi–HP NA integration reconfigures the NA server with the new NNMi management server hostname after failover occurs. Failover should be transparent to users of the integration.

The integration does not support failover of the NA server.

HP NNMi–HP NA Integration Configuration Form Reference

In the NNMi console, the **HP NNMi–HP NA Integration Configuration** form contains the parameters for configuring communications from NNMi to NA. This form is available from the **Integration Module Configuration** workspace.

Only NNMi users with the Administrator role can access the **HP NNMi–HP NA Integration Configuration** form.

The **HP NNMi–HP NA Integration Configuration** form collects information for the following general areas:

- NNMi Management Server Connection
- NA Server Connection
- Integration Behavior

To apply changes to the integration configuration, update the values on the **HP NNMi–HP NA Integration Configuration** form, and then click **Submit**.

NNMi Management Server Connection

Table 47 lists the parameters for connecting to the NNMi management server from NA. You can determine many of these values by examining the URL that invokes an NNMi console session. Coordinate with the NNMi administrator to determine the appropriate values for this section of the configuration form.

Table 47 NNMi Management Server Information in the NNMi Console

Field	**Description**
NNMi Host	The official fully-qualified domain name of the NNMi management server. This field is read-only. **NOTE**: The integration selects the port for connecting to the NNMi console by determining the value of `jboss.http.port` in the following file: • *Windows*: `%NnmDataDir%\conf\nnm\props\nms-local.properties` • *UNIX*: `$NnmDataDir/conf/nnm/props/nms-local.properties`
NNMi User	The user name for connecting to the NNMi console. This user must have the NNMi Web Service Client role. **NOTE**: The password for this user name is passed in cleartext. Best practice: Create and use an `NNMiIntegration` user account with the Web Service Client role.
NNMi Password	The password for the specified NNMi user.

NA Server Connection

Table 48 lists the parameters for connecting to the web services on the NA server. Coordinate with the NA administrator to determine the appropriate values for this section of the configuration form.

Table 48 NA Server Information in the NNMi Console

HP NA Server Parameter	Description
NA Host	The fully-qualified domain name or the IP address of the NA server.
NA Port	The port for connecting to the NA web services. The default NA ports are as follows: • 80—for connections to NA on a separate computer from NNMi • 8080—for connections to NA on the same computer as NNMi **TIP:** The NA URL opens the SSL port, which does not work for integration communications. Enter the correct non-SSL port.
NA User	A valid NA user account name with the NA Administrator role. **NOTE:** The password for this user name is passed in cleartext. Best practice: Create and use an `NAIntegration` user account.
NA Password	The password for the specified NA user.

Integration Behavior

Table 49 lists the NNMi console parameters for configuring the behavior of the HP NNMi–HP NA integration.

Table 49 Integration Behavior Information in the NNMi Console

Parameter	Description
Topology Filter Node Group	The NNMi node group containing the set of nodes to synchronize with the NA topology. The integration populates the NA inventory with information about every node in this node group. Select the node group from the list of node groups on this NNMi management server. If no node group is specified, the integration synchronizes the entire NNMi topology into the NA inventory.
Topology Synchronization Interval (hrs)	The frequency with which NNMi performs a complete topology synchronization with NA as described in Topology Synchronization Between NNMi and NA on page 490. The default interval for the connection check is 24 hours. To disable periodic topology synchronization, set this value to `0`.

Table 49 Integration Behavior Information in the NNMi Console (cont'd)

Parameter	Description
Discover Device Drivers in NA	The NA configuration specification. If the **Discover Device Drivers in NA** check box is selected, NA automatically discovers the device drivers for the devices added to NA as a result of topology synchronization with NNMi. The default setting is cleared. In this case, you can initiate device driver discovery manually.
NA Connection Check Interval (hrs)	The frequency with which NNMi verifies with NA the interface data for all layer 2 connections in the NNMi topology as described in Identifying Layer 2 Connections with Mismatched States on page 494. The default interval for the connection check is 24 hours. To disable the periodic connection check, set this value to `0`.

NNMi Integration Configuration in NA Reference

In the NA user interface, the **NNMi Integration** section of the **Administrative Settings - 3rd Party Integrations** page contains the parameters for configuring communications from NA to NNMi. Enabling the integration on the **HP NNMi–HP NA Integration Configuration** form sets the fields on the **Administrative Settings - 3rd Party Integrations** page. Access the **Administrative Settings - 3rd Party Integrations** page to change the integration behavior for NNMi device rediscovery triggers, out-of-service triggers, and SNMP community string propagation.

The **Administrative Settings - 3rd Party Integrations** page is available from **Admin > Administrative Settings > 3rd Party Integrations**. To apply changes to the integration configuration, update the values on this page, and then click **Save**.

➤ Only NA users with the Administrator role can access the **Administrative Settings - 3rd Party Integrations** page.

Integration Communication

Table 50 lists the parameters for connecting to the NNMi web services from the NA server. The integration configures these parameters with the information on the **HP NNMi–HP NA Integration Configuration** form in the NNMi console.

Table 50 Integration Connection Information in the NA User Interface

Field	Description
NA User	The NA user account name specified on the **HP NNMi–HP NA Integration Configuration** form.
NA Partition	The NA partition specified on the **HP NNMi–HP NA Integration Configuration** form.
NNMi Host	The NNMi management server name specified on the **HP NNMi–HP NA Integration Configuration** form.

Table 50 Integration Connection Information in the NA User Interface (cont’d)

Field	Description
NNMi HTTP Port	The NNMi console port determined by the integration.
NNMi User	The NNMi user name specified on the **HP NNMi–HP NA Integration Configuration** form.
NNMi Password	The NNMi user password specified on the **HP NNMi–HP NA Integration Configuration** form.

Additional Integration Behavior

Table 51 lists the NA user interface parameters for configuring the behavior of the HP NNMi–HP NA integration.

Table 51 Integration Behavior Information in the NA User Interface

Field	Description
Rediscover Hosts After Tasks	The NA tasks for which the integration triggers an NNMi device discovery upon task completion. The default selections are: • Update Device Software • Deploy Passwords • Reboot Device • Discover Driver For more information, see Maintaining Accurate Device Information on page 495.
Out of Service Events	The NA tasks for which the integration sets a device to the DISABLED state while the task occurs. The default selections are: • Update Device Software • Deploy Passwords • Reboot Device For more information, see Disabling Network Management During Device Configuration on page 496.
If the device task fails	The device task failure recovery specification for out-of-service events. The default setting is to return the device to service in NNMi. For more information, see Disabling Network Management During Device Configuration on page 496.
If device compliance check fails after the task completed	The device compliance check failure recovery specification for out-of-service events. The default setting is to return the device to service in NNMi. For more information, see Disabling Network Management During Device Configuration on page 496.
Propagate SNMP Community Strings	The community string propagation specification. The default setting is disabled. For more information, see Propagating Device Community String Changes on page 497.

PCM+

PCM+ is a network management platform for mapping, configuring, and monitoring HP Networking devices. PCM+ provides the following functionality:

- Unified management of wired and wireless Ethernet across the entire network
- Configuration, updating, monitoring, and troubleshooting of HP ProCurve devices
- Policy-based and multi-device management
- Proactive alerts with automatic alert responses
- Advanced traffic-monitoring capabilities

For information about purchasing PCM Plus, contact your HP sales representative.

This chapter contains the following topics:

HP NNMi–PCM+ Integration

By including HP Network Node Manager i Software (NNMi) in the PCM+ environment, network administrators who use PCM+ to monitor and manage their HP Networking devices gain additional insight into those devices.

The HP NNMi–PCM+ integration provides the following functionality:

- Synchronization of IPv4 HP Networking device information from the NNMi database with PCM+. (At this time, PCM+ does not support IPv6 ProCurve devices.)
- Synchronization of SNMPv2 community strings and SNMPv3 user-based security model (USM) settings for communicating with the managed HP Networking devices between the two applications.

Value

The HP NNMi–PCM+ integration provides the following benefits:

- Reduces network traffic to the HP Networking devices as NNMi discovers the HP Networking devices for both NNMi and PCM+.
  - NNMi forwards richer ProCurve device information to PCM+.
  - Simplified PCM+ network maps contain only known HP Networking devices.
- Consolidates HP Networking device event processing in NNMi.
- Reduces the cost of delivering maximum HP Networking device availability.

Integrated Products

The information in this chapter applies to the following products:

- PCM+

  For the list of supported versions, see the *NNMi System and Device Support Matrix*.

- NNMi 9.10

NNMi and PCM+ must be installed on separate computers. The NNMi management server and the PCM+ computer can be of the same or different operating systems.

The PCM+ remote agent cannot be installed on the NNMi management server.

One installation of PCM+ version 4.00 can integrate with NNMi version 8.1x (or higher) or with NNM version 7.x, but not with both products at the same time.

Documentation

The HP NNMi–PCM+ integration is fully described in Appendix A of the *PCM+ Network Administrator's Guide*, which is available at http://h20000.www2.hp.com/bizsupport/TechSupport DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=101&prodTypeId=12883&prodSeriesId=3961207.

Using the HP NNMi–PCM+ Integration

The steps to enable the HP NNMi–PCM+ integration take place on the PCM+ server (configuration) and the NNMi management server (installation of PCM+ trap definitions).

Enabling the HP NNMi–PCM+ integration adds the ICMEVT_PCMPLUS_EVENTS_ALL incident configuration to NNMi for all application events that PCM+ forwards to NNMi. This incident has SNMP object ID .1.3.6.1.4.1.11.2.3.7.11.0.63000000.

For information about enabling, using, disabling, and troubleshooting the HP NNMi–PCM+ integration, see Appendix A of the *PCM+ Network Administrator's Guide*.

HP RAMS MPLS WAN

The HP RAMS MPLS WAN integration enables HP Route Analytics Management System (RAMS) to support enterprises that have multiple sites connected by a WAN through ISPs that use multi-protocol label switching (MPLS) within their own networks.

For information about purchasing HP RAMS, contact your HP sales representative.

This chapter contains the following topics:

- HP NNMi–HP RAMS MPLS WAN Integration
- Using the HP NNMi–HP RAMS MPLS WAN Integration

HP NNMi–HP RAMS MPLS WAN Integration

The HP NNMi–HP RAMS MPLS WAN integration provides features for accessing MPLS WAN information from the NNMi console.

Value

The HP NNMi–HP RAMS MPLS WAN integration adds the feature to view the connectivity through different network clouds, so that NNMi users can detect and view the multiple sites connected by a WAN.

Integrated Products

The information in this chapter applies to the following products:

- RAMS

  For the list of supported versions, see the *NNMi System and Device Support Matrix*.

- NNMi 9.10 with an NNMi Advanced license

For information about the NNMi supported hardware platforms and operating systems, see the *NNMi System and Device Support Matrix*.

Documentation

The HP NNMi–HP RAMS MPLS WAN integration is fully described in *Using Route Analytics Management Systems (RAMS) with NNMi Advanced* in the NNMi help.

Using the HP NNMi–HP RAMS MPLS WAN Integration

The steps to enable the HP NNMi–HP RAMS MPLS WAN integration take place on the NNMi management server.

For information about enabling, using, disabling, and troubleshooting the HP NNMi–HP RAMS MPLS WAN integration, see *Using Route Analytics Management Systems (RAMS) with NNMi Advanced* in the NNMi help.

HP SiteScope

HP SiteScope is an agentless monitoring solution for tracking the availability and performance of distributed IT infrastructures, for example: servers, operating systems, network devices, network services, applications, and application components. SiteScope provides real-time information for verifying infrastructure operations, staying apprised of problems, and solving bottlenecks before they become critical.

For information about purchasing SiteScope, contact your HP sales representative.

This chapter describes the following integrations:

- HP NNMi–HP SiteScope Events Integration on page 513
- HP NNMi–HP SiteScope System Metrics Integration on page 517

For information about the NNM iSPI for IP Telephony–HP SiteScope integration, see *Configuring Integration with SiteScope* the NNM iSPI for IP Telephony help.

HP NNMi–HP SiteScope Events Integration

This section contains the following topics:

- About the HP NNMi–HP SiteScope Events Integration on page 514
- Enabling the HP NNMi–HP SiteScope Events Integration on page 515
- Using the HP NNMi–HP SiteScope Events Integration on page 515
- Changing the HP NNMi–HP SiteScope Events Integration on page 516
- Disabling the HP NNMi–HP SiteScope Events Integration on page 516
- Troubleshooting the HP NNMi–HP SiteScope Events Integration on page 516

About the HP NNMi–HP SiteScope Events Integration

With the HP NNMi–HP SiteScope Events integration, SiteScope servers send SNMP traps to the NNMi management server when the configured SiteScope monitor alert conditions are met. NNMi converts the monitor alert traps into NNMi incidents. From these incidents, an NNMi console user can launch SiteScope in the context of that monitor.

Value

By providing SiteScope incident configuration in NNMi, the HP NNMi–HP SiteScope Events integration simplifies the process of interpreting SNMP traps regarding status of devices and applications that SiteScope monitors.

These traps are generated only for alerts configured in SiteScope. The integration makes these traps visible in the NNMi console as incidents. NNMi automatically closes these alert incidents if SiteScope indicates that the alert condition no longer exists (becomes normal).

Integrated Products

The information in this section applies to the following products:

- SiteScope

  For the list of supported versions, see the *NNMi System and Device Support Matrix*.

- NNMi 9.10

NNMi and SiteScope can be installed on the same computer or on different computers.

For the most recent information about supported hardware platforms and operating systems, see the support matrices for both products.

Supported SiteScope Monitors

The HP NNMi–HP SiteScope Event integration receives SNMP traps sent from the SiteScope server for any SiteScope monitor type, as configured in SiteScope. The SiteScope alert configuration must include the NNMi management server as the trap target.

The SiteScope trap configuration determines whether the SiteScope server or the managed host is set as the source object. If the source object is not managed in NNMi, the **Discard Unresolved SNMP Traps** check box setting on the **Incident Configuration** form determines how NNMi handles that trap. For more information, see *Handle Unresolved Incoming Traps* in the NNMi help.

Documentation

This section describes how to configure and use the integration.

The *HP SiteScope Using SiteScope* guide, which is included on the SiteScope product media, describes how to configure SiteScope monitors and how to configure SiteScope to send event data to NNMi.

Enabling the HP NNMi–HP SiteScope Events Integration

To enable the HP NNMi–HP SiteScope Events integration, configure one or more SiteScope monitors to send SNMP traps to NNMi. The high-levels steps are as follows:

The NNMi incident types are enabled by default.

1 In the SiteScope user interface, create an SNMP preference to send the HP SiteScope event trap to the NNMi management server.

2 In the SiteScope user interface, create an alert that sets the SNMP trap preference as the alert action target. (In this alert, create an alert action for each possible monitor status.)

For detailed information, see “How to Configure SiteScope to Send Event Data to NNMi” in the *Working with Network Node Manager i (NNMi)* chapter of *HP SiteScope Using SiteScope* guide.

Using the HP NNMi–HP SiteScope Events Integration

NNMi defines two incident types for the SiteScope monitor alert traps:

- SiteScopeAlertEvent1 converts SNMPv1-format traps to NNMi incidents.
- SiteScopeAlertEvent2 converts SNMPv2c-format traps to NNMi incidents.

The configuration of these incident types is identical. The SiteScope SNMP trap preference determines whether SiteScope sends SNMPv1- or SNMPv2c-format traps to NNMi.

Within the incident configuration, incident severity is set as follows:

- The default incident status is CRITICAL, which maps to SiteScope event severity of ERROR, NOTAVAILABLE, or NODATA.
- Incident enrichment sets the incident status to WARNING when the SiteScope event severity is WARNING.
- Incident enrichment sets the incident status to NORMAL when the SiteScope event severity is GOOD.

Each SiteScopeAlertEvent trap contains a URL for launching SiteScope in the context of that monitor. This URL is available in the .1.3.6.1.4.1.11.15.1.2.1.4 custom incident attribute (CIA) on the **Custom Attributes** tab of the **Incident** form. The URL passes encrypted credentials for logging on to SiteScope as the Integration Viewer user.

For each SiteScopeAlertEvent incident, NNMi performs pairwise handling on the SiteScopeAlertEvent traps by comparing data included in the traps’ payloads. Each trap contains an event key varbind (OID .1.3.6.1.4.1.11.15.1.3.1.7). If a trap also contains an event close key pattern varbind (OID .1.3.6.1.4.1.11.15.1.3.1.8), NNMi compares the value of the event close key pattern varbind with that of the event key varbind in existing incidents. NNMi closes the matching existing incidents and correlates them under the incoming trap. NNMi adds the cia.reasonClosed CIA and a correlation note to each of the closed incidents. Additionally, NNMi automatically closes each SiteScopeAlertEvent incident of NORMAL status.

The SiteScope SNMP traps appear in the System and Applications family.

For more information about the contents of the SiteScopeAlertEvent trap, see the HP-SITESCOPE-MIB, which is delivered with NNMi.

Changing the HP NNMi–HP SiteScope Events Integration

To change the HP NNMi–HP SiteScope Events integration, do any of the following:

- In the NNMi console, edit the incident configurations for the SiteScopeAlertEvent1 and SiteScopeAlertEvent2 SNMP traps.
- In the SiteScope user interface, change the monitor alert configurations.

Disabling the HP NNMi–HP SiteScope Events Integration

To disable the HP NNMi–HP SiteScope Events integration, do one or both of the following:

- In the NNMi console, clear the **Enabled** check box on the SiteScopeAlertEvent1 and SiteScopeAlertEvent2 **SNMP Trap Configuration** forms.
- In the SiteScope user interface, do one of the following:
  - Remove monitors and groups from the alert action target.
  - Disable or delete the SNMP trap alert associated with the SiteScope monitors.

Troubleshooting the HP NNMi–HP SiteScope Events Integration

This section contains the following topics:

- NNMi Incident Views Do Not Display SiteScopeAlertEvent Incidents on page 516
- SiteScope Does Not Open Correctly from the URL in a SiteScope Incident on page 517

NNMi Incident Views Do Not Display SiteScopeAlertEvent Incidents

If the NNMi incident views do not contain all of the expected SiteScopeAlertEvent incidents, follow these steps:

1. In the NNMi console, check the SiteScopeAlertEvent1 and SiteScopeAlertEvent2 incident configurations:
   - Verify that the SiteScopeAlertEvent1 and SiteScopeAlertEvent2 incident types are enabled.
   - If interface or node settings are configured, verify that they are not blocking expected SiteScope traps.
2. In the NNMi console, check the filter for the incident view.

   Compare the current filter with the SiteScopeAlertEvent1 and SiteScopeAlertEvent2 incident configurations. Verify that the filter does not block these incident types.
3. If the **Discard Unresolved SNMP Traps** check box on the **Incident Configuration** form is selected, verify that the nodes associated with SiteScope monitors are in the NNMi topology.

   The SiteScope trap configuration determines whether the SiteScope server or the managed host is set as the source object.
4. In the SiteScope user interface, verify the configuration of the SNMP trap preference for the HP SiteScope event trap.

5 In the SiteScope user interface, verify that each expected monitor alert sets the SNMP trap preference as the alert action target.

6 In the SiteScope user interface, send a test trap to NNMi.

SiteScope Does Not Open Correctly from the URL in a SiteScope Incident

If SiteScope does not correctly launch from the URL in the .1.3.6.1.4.1.11.15.1.2.1.4 CIA on the **Custom Attributes** tab of the **Incident** form, follow these steps:

1 Verify access to the SiteScope user interface:

   a In a new browser window, open the SiteScope user interface directly.

   If the SiteScope user interface does not work correctly, verify that the browser configuration matches the requirements described in the *HP SiteScope Release Notes*.

   b Copy the URL from the .1.3.6.1.4.1.11.15.1.2.1.4 CIA to the browser address field. Delete the logon credentials. In the SiteScope logon window, enter your SiteScope logon information.

2 Verify the SiteScope Integration Viewer user credentials in the URL. Copy the URL from the .1.3.6.1.4.1.11.15.1.2.1.4 CIA to the browser address field. (Keep the logon credentials.)

If this test fails, ask the SiteScope administrator about the status of the Integration Viewer user. If the password for the Integration Viewer user has changed recently, the URLs to SiteScope that existed before the password change do not work.

HP NNMi–HP SiteScope System Metrics Integration

This section contains the following topics:

About the HP NNMi–HP SiteScope System Metrics Integration

The HP NNMi–HP SiteScope System Metrics integration populates the NNM iSPI Performance for Metrics Network Performance Server (NPS) with system metrics data collected by SiteScope monitors. The integration handles data as follows:

1 SiteScope collects monitor data into XML files and passes the collected data to NNMi at the reporting interval of the SiteScope data integration preference.

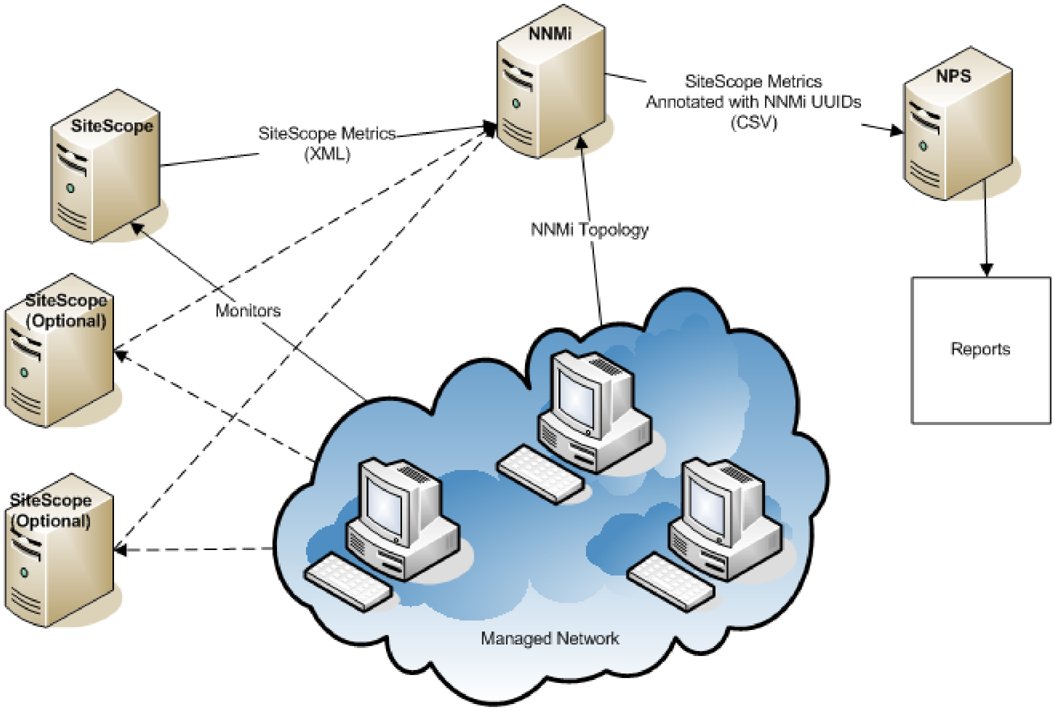
2 NNMi augments the SiteScope data with NNMi node UUIDs.

3 NNMi places the augmented data in the configured location for NPS retrieval.

4 The NPS consumes the augmented data at the NPS accumulation interval.

Figure 43 shows the data flow for the HP NNMi–HP SiteScope System Metrics integration.

Figure 43 HP NNMi–HP SiteScope System Metrics Integration Data Flow



Value

The HP NNMi–HP SiteScope System Metrics integration enables reporting of SiteScope-collected metrics in the NPS.

Integrated Products

The information in this section applies to the following products:

- SiteScope

  For the list of supported versions, see the *NNMi System and Device Support Matrix*.

- NNMi 9.10
- NNM iSPI Performance for Metrics version 9.10

  This integration requires an NNM iSPI Performance for Metrics license.

NNMi, the NNM iSPI Performance for Metrics, and SiteScope can be installed on the same computer or on different computers.

For the most recent information about supported hardware platforms and operating systems, see the support matrices for all products.

Supported SiteScope Monitors

The HP NNMi–HP SiteScope System Metrics integration understands data from the following types of SiteScope monitors:

- CPU Utilization Monitor
- Disk Space Monitor
- Memory Monitor
- The Process monitored object of the Microsoft Windows Resources Monitor
- The Process monitored object of the UNIX Resources Monitor

The nodes being monitored must be managed in NNMi. The integration discards data for nodes that are not in the NNMi topology and for unmanaged nodes.

Documentation

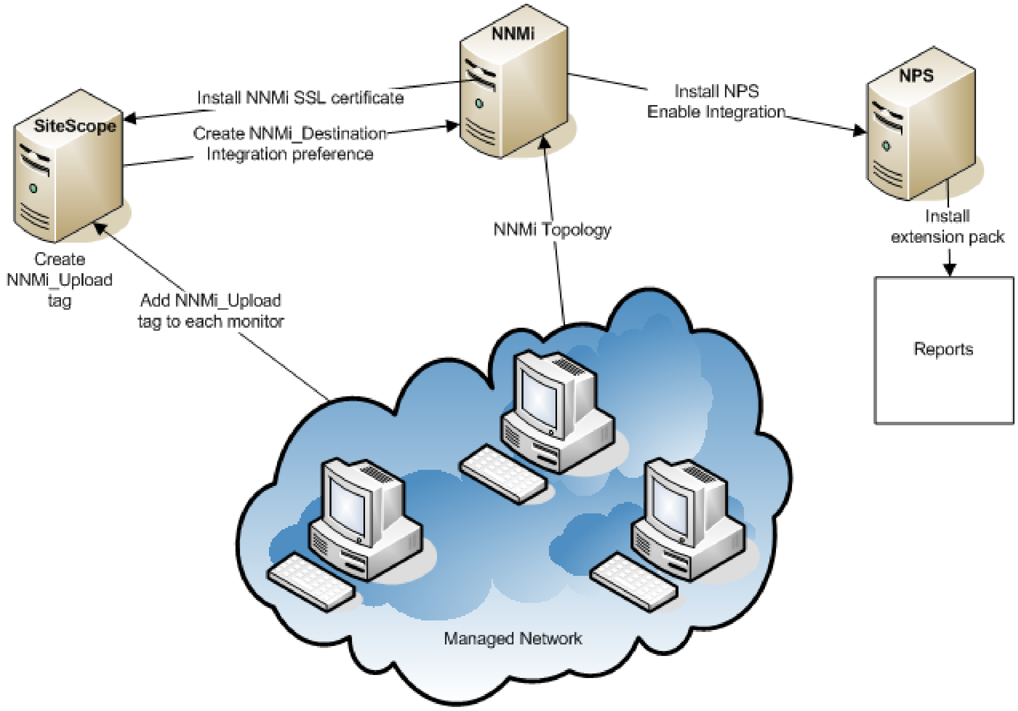
This section describes how to configure NNMi to communicate with SiteScope and the NPS reports available for the SiteScope-collected data.

The *HP SiteScope Using SiteScope* guide, which is included on the SiteScope product media, describes how to configure SiteScope monitors.

Enabling the HP NNMi–HP SiteScope System Metrics Integration

Figure 44 shows the configuration points for the HP NNMi–HP SiteScope System Metrics integration.

Figure 44 HP NNMi–HP SiteScope System Metrics Integration Configuration Points


NNMi
Install NNMi SSL certificate
Create NNMi_Destination Integration preference
SiteScope
Install NPS Enable Integration
NPS
Create NNMi_Upload tag
NNMi Topology
Install extension pack
Add NNMi_Upload tag to each monitor
Reports
Managed Network

To enable the HP NNMi–HP SiteScope System Metrics integration, follow these steps:

1 In the NNMi console, enable integration and configure the NPS with the SiteScope system metrics integration pack:

   a *Optional*. Create an NNMi user with the Web Service Client role that the integration uses to connect to the NNMi console.

   Alternatively, you can use an existing user with the Web Service Client role for the integration.

   b Open the **HP NNMi–HP SiteScope System Metrics Integration Configuration** form (**Integration Module Configuration > HP SiteScope System Metrics**).

   c Select the **Enable Integration** check box.

   d Enter the information for connecting to the NNMi management server. For information about these fields, see HP NNMi–HP SiteScope System Metrics Integration Configuration Form Reference on page 530.

   e Click **Submit** at the bottom of the form.

   The window opens a status message. If the message indicates a problem with the NNMi credentials, click **Return**, and then adjust the values as suggested by the text of the error message.

   f From the results window, copy the data integration URL to a temporary location. You will use this value while configuring SiteScope.

2 In the SiteScope user interface, configure the SiteScope server for SSL communications with NNMi:

   a From the **Preferences** workspace, open the **Certificate Management** page, and then click **Import Certificates** ✱.

   b Under **Source Selection**, provide information to identify the NNMi management server to SiteScope:

   — Verify that **Host** is selected, and then enter the fully-qualified domain name of the NNMi management server.

   — If necessary, change the port number to match the HTTPS port on the NNMi management server.

   For more information, see NNMi Port on page 530.

   c Click **Load**.

   The NNMi certificate information appears under **Loaded Certificates**. Note the certificate alias.

   d Select the NNMi certificate, and then click **Import**.

   The NNMi certificate is listed on the **Certificate Management** page.

3 In the SiteScope user interface, create a search/filter tag that you will use to identify the NNMi target.

   a From the **Preferences** workspace, open the **Search/Filter Tag** page, and then click **New Tag** ✱.

   b Enter a tag name (for example, NNMi_upload) and at least one value.

4. In the SiteScope user interface, configure the connection between SiteScope and NNMi:

    a. From the **Preferences** workspace, open the **Integration Preferences** page, and then click **New Integration** ✱, and then click **Data Integration**.

    b. Under **General Settings**, enter a name (for example, NNMi_receiver) and optional description.

    c. Under **Data Integration Preferences Settings**, include the following settings:

        — In the **Receiver URL** field, paste the URL you saved at the end of step 1 of this procedure (for example: `https://nnmi_server.example.com:443/sitescope-adapter/sitescopereceiver`).

        — Select the **GZIP compression** check box.

        — Clear the **Include additional data** and **Error on redirect** check boxes. (These are the default settings.)

        — Select the **Authentication when requested** check box. (This is the default setting.)

        — Clear the **Disable integration** check box. (This is the default setting.)

        For all other settings, the default configuration is acceptable.

    d. Under **Web Server Security Settings**, enter the user name and password for the NNMi user that you specified on the integration configuration form in step 1.

    e. Under **Reporting Tags**, select the search/filter tag that you created in step 3 (for example, NNMi_upload).

5. In the SiteScope user interface, configure the monitors that contribute to the SiteScope reports in the NPS:

    a. As needed, create new monitors or identify existing monitors of the supported types:

        — CPU Utilization Monitor

        — Disk Space Monitor

        — Memory Monitor

        — The Process monitored object of the Microsoft Windows Resources Monitor

        — The Process monitored object of the UNIX Resources Monitor

    b. Add the search/filter tag that you created in step 3 (for example, NNMi_upload) to the monitors that should pass data to NNMi.

        The integration can only process data for managed nodes in the NNMi topology. So, only apply the tag to monitors on nodes in the NNMi topology.

    c. Recommended. Collect the monitors that pass data to NNMi in one monitor group.

Using the HP NNMi–HP SiteScope System Metrics Integration

The HP NNMi–HP SiteScope System Metrics integration provides the following SiteScope monitor reports in the NPS:

- Calendar
- Chart Detail
- Heat Chart
- Managed Inventory
- Most Changed
- Peak Period
- Threshold Sleeve
- Top N
- Top N Chart

To access the SiteScope system metric reports, follow these steps:

1. In the NNMi console, click **Actions > Reporting – Report Menu**.
2. In the **Reports** workspace of the NPS, open the **SiteScope System Metrics > SiteScope > System_Metrics** folder.

Best practice

The following tips apply to the SiteScope system metric reports:

- For some reports, such as Top N, a report that focuses on one type of SiteScope monitor is easier to interpret than a report on multiple monitor types. In the topology filter, select a single value for the ComponentType attribute.
- If the Node Name attribute is not set, the report includes data for all monitors of the selected type. To limit the report data to one or more specific nodes, set the Node Name attribute accordingly. If the ComponentType attribute is set, the Node Name selection list shows only those nodes that have the selected monitor type.
- For reports on Windows Resource Monitors, it might be helpful to filter out the `_Total on` and `Idle on` data. To do so, in the topology filter, set the ComponentName attribute to not equal `_Total on` and `Idle on`.

Table 52 lists the grouping options added by the integration.

Table 52 Available Report Grouping Options

Option Name	Description
Windows Process – Creating Process	An integer value that identifies the process ID (PID) of the parent process that created the measured process.
Windows Process – ID Process	An integer value that identifies the process ID (PID) of the measured process.

Table 52 Available Report Grouping Options (cont'd)

Option Name	Description
Unix Process – PID	An integer value that identifies the process ID (PID) of the measured process.
Unix Process – User	An integer value that identifies the UNIX user ID (uid) of the measured process.
Qualified Component Name	A string value that identifies the metric name and the node on which the metric is collected. The qualified component name is in the form `<metric_name> on <node_long_name>` (for example: `disk percent full on device.example.com`). Qualified Component Name is the recommended grouping selection.

Table 53 lists the metrics added by integration. For each metric, you can select to report the actual values. For many metrics, you can also report threshold information. For information about interpreting the reported values, see the documentation for each operating system.

Table 53 Available SiteScope System Metrics

Monitor Type	Available Metrics
CPU Utilization[1]	• CPU Utilization
Disk Space	• Disk MB Free • Disk Percent Full
Memory[2]	• Memory Pages/Sec • Virtual Memory Used Percent • Virtual Memory MB Free • Swap Memory Used Percent • Swap Memory MB Free • Physical Memory Used Percent • Physical Memory MB Free

Table 53 Available SiteScope System Metrics (cont'd)

Monitor Type	Available Metrics
Microsoft Windows Resources	• Windows Process – Percent Privileged Time • Windows Process – Percent Processor Time • Windows Process – Percent User Time • Windows Process – Creating Process ID • Windows Process – Elapsed Time • Windows Process – Handle Count • Windows Process – ID Process • Windows Process – IO Data Bytes/sec • Windows Process – IO Data Operations/sec • Windows Process – IO Data Other Bytes/sec • Windows Process – IO Other Operations/sec • Windows Process – IO Read Bytes/sec • Windows Process – IO Read Operations/sec • Windows Process – IO Write Bytes/sec • Windows Process – IO Write Operations/sec • Windows Process – Page Faults • Windows Process – Page File Bytes • Windows Process – Page File Bytes Peak • Windows Process – Pool Nonpaged Bytes • Windows Process – Pool Paged Bytes • Windows Process – Priority Base • Windows Process – Private Bytes • Windows Process – Thread Count • Windows Process – Virtual Bytes • Windows Process – Virtual Bytes Peak • Windows Process – Working Set • Windows Process – Private Working Set • Windows Process – Working Set Peak
UNIX Resources[3]	• Unix Process – CPU Percent • Unix Process – Memsize • Unix Process – Number_Running • Unix Process – PID • Unix Process – User

[1] SiteScope summarizes CPU use data collected on the HP-UX and AIX operating systems as a single average value for the system, not per specific CPU. Because the integration does not send average values to NPS, CPU use data is not available for the HP-UX and AIX operating systems.

[2] SiteScope does not collect all of these metrics for all operating systems.

[3] For the UNIX Resources monitor on the HP-UX operating system, SiteScope collects CPU percent, number running, and process ID only. Memory size and user data are not available for HP-UX nodes.

Changing the HP NNMi–HP SiteScope System Metrics Integration

You can change the HP NNMi–HP SiteScope System Metrics integration in the following ways:

- Change the Connection from NNMi to the NPS
- Change the Connection from SiteScope to NNMi

Change the Connection from NNMi to the NPS

To change the information for connecting to the NPS, follow these steps:

1. In the NNMi console, open the **HP NNMi–HP SiteScope System Metrics Integration Configuration** form (**Integration Module Configuration > HP SiteScope System Metrics**).
2. Modify the values as appropriate. For information about the fields on this form, see HP NNMi–HP SiteScope System Metrics Integration Configuration Form Reference on page 530.
3. Verify that the **Enable Integration** check box at the top of the form is selected, and then click **Submit** at the bottom of the form.

   The changes take effect immediately. The effect is to update the data integration URL displayed on the **HP NNMi–HP SiteScope System Metrics Integration Configuration** form If this URL changes, update the SiteScope data integration preference as described in step 4 on page 521.

Change the Connection from SiteScope to NNMi

To change the information for the SiteScope data receiver, follow these steps:

1. In the SiteScope interface, open the data integration that defines the connection between SiteScope and NNMi (from **Preferences > Integration Preferences**).
2. Modify the values as appropriate. For information about the fields on this form, see the SiteScope help.
3. Verify that the **Disable Integration** check box is cleared, and then click **OK** at the bottom of the form.

   The changes take effect immediately.

Disabling the HP NNMi–HP SiteScope System Metrics Integration

To completely disable the HP NNMi–HP SiteScope System Metrics integration, complete both of the following procedures:

- Disable the Connection from NNMi to the NPS
- Disable the Connection from SiteScope to NNMi

Disable the Connection from NNMi to the NPS

To stop NNMi from processing the SiteScope monitor data, follow these steps:

1. In the NNMi console, open the **HP NNMi–HP SiteScope System Metrics Integration Configuration** form (**Integration Module Configuration > HP SiteScope System Metrics**).
2. Clear the **Enable Integration** check box at the top of the form, and then click **Submit** at the bottom of the form.

   The changes take effect immediately.

Disable the Connection from SiteScope to NNMi

To stop SiteScope from sending monitor data to the NNMi management server, follow these steps:

1. In the SiteScope interface, open the data integration that defines the connection between SiteScope and NNMi (from **Preferences > Integration Preferences**).
2. Select the **Disable Integration** check box, and then click **OK** at the bottom of the form.

   The changes take effect immediately.

Troubleshooting the HP NNMi–HP SiteScope System Metrics Integration

Messages related to the processing of SiteScope data, including XML parsing errors and monitor data for nodes not in the NNMi topology, are logged to the `nnm.0.0.log` (and older) files on the NNMi management server. If you encounter problems on the NNMi management server, check these log files for SEVERE and WARNING messages for the classes beginning with the string `com.hp.ov.nnm.sitescope.im` or `com.hp.ov.nms.im.sitescope`. For more information, see NNMi Logging on page 383.

The SiteScope log file collects messages about problems with the data integration. Look in the SiteScope log file for data transmission errors, which most likely result from one or more of the following configuration problems:

- Certificate errors; the NNMi certificate is not properly loaded into SiteScope.
- User name and password authentication errors; the values for **NNMi User**, **NNMi Password**, or both are incorrect on the **HP NNMi–HP SiteScope System Metrics Integration Configuration** form in the NNMi console.
- Integration module enablement errors; the **Enable Integration** check box is cleared on the **HP NNMi–HP SiteScope System Metrics Integration Configuration** form in the NNMi console.

For more information on the SiteScope log file, see the SiteScope documentation.

This section contains the following topics:

- Verify the Integration Data Flow on page 527
- Verify the NNMi Side of the Integration Configuration on page 528
- No Report Data for Nodes in a NAT’d Environment Behind a Firewall on page 529

Verify the Integration Data Flow

XML files from SiteScope

The system metrics integration places the SiteScope data samples as `*.gz` files in the following directory on the NNMi management server:

- *Windows*: `%NnmDataDir%\shared\perfspi\datafiles\metric\working\sitescope`
- *UNIX*: `$NnmDataDir/shared/perfspi/datafiles/metric/working/sitescope`

By default, the system metrics integration places a new file in this directory every minute, and NNMi consumes these files every five minutes.

The reporting interval of the SiteScope data integration preference determines the frequency at which SiteScope sends data samples to the system metrics integration. The NNMi consumption rate is not customer configurable.

If the `sitescope` directory remains empty for more than two minutes, SiteScope is not delivering the files. In this case, do the following:

1. In the SiteScope user interface, verify that the data integration preference is enabled and configured is as described in step 4 on page 521.

   Also verify the value of the **Reporting Interval** field.

2. In the SiteScope user interface, verify that at least one monitor configuration includes the search/filter tag associated with the data integration preference.

If files accumulate in the `sitescope` directory, NNMi is not consuming the files. In this case, in the NNMi console, verify that the HP NNMi–HP SiteScope System Metrics integration is configured correctly. For detailed information, see Verify the NNMi Side of the Integration Configuration on page 528.

CSV files from NNMi

NNMi places `SiteScopeMetrics_*.csv.gz` files for NPS consumption in the following directory on the NNMi management server:

- *Windows*: `%NnmDataDir%\shared\perfspi\datafiles\metric\final`
- *UNIX*: `$NnmDataDir/shared/perfspi/datafiles/metric/final`

NNMi places a new file in this directory approximately every five minutes, and the NPS consumes these files approximately every five minutes.

The NNMi placement rate is not customer configurable. The NPS accumulation rate determines the frequency with which the NPS consumes the files in this directory. The NNM iSPI Performance for Metrics sets the NPS accumulation rate, which is not customer configurable.

If the `final` directory remains empty for more than ten minutes, NNMi is not delivering the files. In this case, in the NNMi console, verify that the HP NNMi–HP SiteScope System Metrics integration is configured correctly. For detailed information, see Verify the NNMi Side of the Integration Configuration on page 528.

If files accumulate in the `final` directory, the NPS is not consuming the files. In this case, see the NPS troubleshooting documentation.

Reports

If the SiteScope reports are not available in the NPS user interface within two hours after files pass through the `final` directory, the integration is not correctly configured. In this case, restart SiteScope, the NNMi ovjboss process, and the NPS:

1. Restart SiteScope:
   - *Windows*:
     - — Open the **Services** control panel (**Start > Control Panel > Administrative Tools > Services**).
     - — In the list of services, right-click **SiteScope**, and then click **Start**.
   - *Linux or Solaris*:
     - — Open a terminal window on the server where SiteScope is installed.
     - — Run the start command shell script using the following syntax:

       ```
       <installpath>/SiteScope/start
       ```
2. Restart NNMi by running the following commands:
   - a **`ovstop`**
   - b **`ovstart`**
3. Restart the NPS.

Verify the NNMi Side of the Integration Configuration

1. In the NNMi console, open the **HP NNMi–HP SiteScope System Metrics Integration Configuration** form (**Integration Module Configuration > HP SiteScope System Metrics**).

   For information about the fields on this form, see HP NNMi–HP SiteScope System Metrics Integration Configuration Form Reference on page 530.
2. To check the status of the integration, in the **HP NNMi–HP SiteScope System Metrics Integration Configuration** form, click **Submit** at the bottom of the form (without making any configuration changes).

   The window opens a status message.
3. Verify that the connection to NNMi is configured correctly:

   ➤ If you used the information described in this step to connect to the NNMi console in step 1 of this procedure, you do not need to reconnect to the NNMi console. Continue with step 4.

   - a In a web browser, enter the following URL:

     ***<protocol>*://*<NNMiserver>*:*<port>*/nnm/**

     Where the variables are related to values on the **HP NNMi–HP SiteScope System Metrics Integration Configuration** form as follows:
     - — If the **NNMi SSL Enabled** check box is selected, `<protocol>` is `https`.
     - — If the **NNMi SSL Enabled** check box is cleared, `<protocol>` is `http`.
     - — `<NNMiserver>` is the value of **NNMi Host**.
     - — `<port>` is the value of **NNMi Port**.

b When prompted, enter the credentials for an NNMi user with the Administrator role.

You should see the NNMi console. If the NNMi console does not appear, contact the NNMi administrator to verify the information that you are using to connect to NNMi. Continue to troubleshoot the connection to NNMi until the NNMi console appears.

➤ You cannot sign in to the NNMi console as a user with the Web Service Client role.

c Contact the NNMi administrator to verify the values of **NNMi User** and **NNMi Password** for the NNMi integration user with the Web Service Client role.

Passwords are hidden in the NNMi console. If you are not sure what password to specify for an NNMi user name, ask the NNMi administrator to reset the password.

4 Update the **HP NNMi–HP SiteScope System Metrics Integration Configuration** form with the values that you used for successful connections in step 3 of this procedure.

For more information, see HP NNMi–HP SiteScope System Metrics Integration Configuration Form Reference on page 530.

5 Click **Submit** at the bottom of the form.

6 If the status message still indicates a problem, do the following:

a Clear the web browser cache.

b Clear all saved form or password data from the web browser.

c Close the web browser window completely, and then re-open it.

d Repeat step 4 and step 5 of this procedure.

7 Test the configuration by watching the transfer of SiteScope monitor data as described in Verify the Integration Data Flow on page 527.

No Report Data for Nodes in a NAT'd Environment Behind a Firewall

In a network address translation (NAT) environment, if the SiteScope server is deployed behind a firewall and reports data for nodes with duplicate IP addresses outside the firewall, NNMi cannot determine which node is being monitored. In this case the integration does not provide the SiteScope data for these nodes to the NPS, so the NPS reports do not include this information.

HP NNMi–HP SiteScope System Metrics Integration Configuration Form Reference

The **HP NNMi–HP SiteScope System Metric Integration Configuration** form contains the parameters for configuring communications between NNMi and SiteScope. This form is available from the **Integration Module Configuration** workspace.

➤ Only NNMi users with the Administrator role can access the **HP NNMi–HP SiteScope System Metrics Integration Configuration** form.

The **HP NNMi–HP SiteScope System Metrics Integration Configuration** form collects information for the identifying the NNMi management server.

To apply changes to the integration configuration, update the values on the **HP NNMi–HP SiteScope System Metrics Integration Configuration** form, and then click **Submit**.

Table 54 lists the parameters for connecting to the NNMi management server. This is the same information that you use to open the NNMi console. You can determine many of these values by examining the URL that invokes an NNMi console session. Coordinate with the NNMi administrator to determine the appropriate values for this section of the configuration form.

Table 54 NNMi Management Server Information

Field	Description
NNMi SSL Enabled	The connection protocol specification. • If the NNMi console is configured to use HTTPS, select the **NNMi SSL Enabled** check box. • If the NNMi console is configured to use HTTP, clear the **NNMi SSL Enabled** check box.
NNMi Host	The fully-qualified domain name of the NNMi management server. This field is pre-filled with host name that was used to access the NNMi console. Verify that this value is the name that is returned by the **`nnmofficialfqdn.ovpl -t`** command run on the NNMi management server.
NNMi Port	The port for connecting to the NNMi console. This field is pre-filled with the port that the jboss application server uses for communicating with the NNMi console, as specified in the following file: • *Windows*: `%NnmDataDir%\conf\nnm\props\nms-local.properties` • *UNIX*: `$NnmDataDir/conf/nnm/props/nms-local.properties` For non-SSL connections, use the value of `jboss.http.port`, which is `80` or `8004` by default (depending on the presence of another web server when NNMi was installed). For SSL connections, use the value of `jboss.https.port`, which is `443` by default.
NNMi User	The user name for connecting to the NNMi console. This user must have the Web Service Client role.
NNMi Password	The password for the specified NNMi user.

HP Systems Insight Manager

HP Systems Insight Manager (SIM) provides systems management of HP server and storage devices. SIM features include system discovery and identification, a single-event view, inventory data collection, and reporting.

SIM is beneficial for the following tasks:

- Troubleshooting complex problems that span server and storage infrastructure.
- Maintaining server and storage asset information.
- Modeling the impact of infrastructure and application changes before they occur.
- Tracking actual planned and unplanned changes through discovered change history.
- Gaining a shared, authoritative view of the environment through awareness of existing data repositories.
- Training network management personnel across domains of expertise.
- Shifting network management focus from daily maintenance toward future business needs.

For information about purchasing SIM, contact your HP sales representative.

This chapter contains the following topics:

HP NNMi–HP SIM Integration

The HP NNMi–HP SIM integration provides actions for accessing several SIM tools from the NNMi console.

Value

The HP NNMi–HP SIM integration adds network device information to NNMi, so that NNMi users can detect and investigate potential network problems for HP ProLiant servers and storage devices.

Integrated Products

The information in this chapter applies to the following products:

- SIM

  For the list of supported versions, see the *NNMi System and Device Support Matrix*.

- NNMi 9.10

NNMi and SIM must be installed on separate computers. The NNMi management server and the SIM server computer can be of the same or different operating systems.

For the most recent information about supported hardware platforms and operating systems for NNMi, see the *NNMi System and Device Support Matrix*.

For the most recent information about supported hardware platforms and operating systems for SIM, see the quickspecs, which are available at:

www.hp.com/go/sim

Documentation

This chapter describes how to configure NNMi to communicate with SIM and how to use the integration from the NNMi console.

The SIM documentation suite describes the SIM features and capabilities in detail. The documentation suite is available for download from the SIM information library, which is available at:

www.hp.com/go/sim

Enabling the HP NNMi–HP SIM Integration

On the NNMi management server, configure the connection between NNMi and SIM by following these steps:

1. In the NNMi console, open the **HP NNMi–HP SIM Integration Configuration** form (**Integration Module Configuration > HP SIM**).
2. Select the **Enable Integration** check box to make the remaining fields on the form available.
3. Enter the information for connecting to the NNMi management server. For information about these fields, see NNMi Management Server Connection on page 536.
4. Enter the information for connecting to the SIM server. For information about these fields, see SIM Server Connection on page 537.
5. Click **Submit** at the bottom of the form.

   A new window opens a status message. If the message indicates a problem with connecting to the NNMi management server, click **Return**, and then adjust the values as suggested by the text of the error message.
6. Load the incident definitions for SIM-managed devices:
   1. Change to the following directory:
      - *Windows*: `%NnmInstallDir%\newconfig\HPOvNmsEvent`
      - *UNIX*: `$NnmInstallDir/newconfig/HPOvNmsEvent`
   2. Import the SIM incident definitions by entering the following command:

      ```
      nnmconfigimport.ovpl -f nnm-sim-incidentConfig.xml \
      -u <username> -p <password>
      ```
7. Optional and recommended. Load the MIB definition files for the traps that SIM-managed devices generate:
   1. Change to the following directory:
      - *Windows*:
        `%NNM_SNMP_MIBS%\Vendor\Hewlett-Packard\SystemsInsightManager`
      - *UNIX*:
        `$NNM_SNMP_MIBS/Vendor/Hewlett-Packard/SystemsInsightManager`
   2. Use the nnmloadmib.ovpl command to load the appropriate MIB files for the managed environment. For example:

      ```
      nnmloadmib.ovpl -load cpqhost.mib -u <username> -p <password>
      ```

      - For the HP ProLiant device traps, load the `cpqhost.mib` file, and then load the remaining `cpq*.mib` files in the `SystemsInsightManager` directory.
      - For the HP Virtual Connect device traps, load the `vc*.mib` files and the `fa-mib40.mib` file into NNMi.
   3. Verify that the MIBs loaded correctly, by entering the following command:

      ```
      nnmloadmib.ovpl -list -u <username> -p <password>
      ```

Using the HP NNMi–HP SIM Integration

The HP NNMi–HP SIM integration provides links from the NNMi console to the SIM agent on a device or directly to SIM. The integration does not provide single sign-on between the products. You must enter your SIM user credentials to view the SIM pages.

Enabling the HP NNMi–HP SIM integration adds the following actions to the NNMi console:

- **HP System Management Homepage**—Opens the HP System Management device home page for the node selected in the NNMi console.
- **HP Systems Insight Manager Home**—Opens the SIM home page.
- **HP Systems Insight Manager**—Opens the SIM System page for the node selected in the NNMi console.

Changing the HP NNMi–HP SIM Integration Configuration

1. In the NNMi console, open the **HP NNMi–HP SIM Integration Configuration** form (**Integration Module Configuration > HP SIM**).
2. Modify the values as appropriate. For information about the fields on this form, see HP NNMi–HP SIM Integration Configuration Form Reference on page 536.
3. Verify that the **Enable Integration** check box at the top of the form is selected, and then click **Submit** at the bottom of the form.

➤ The changes take effect immediately. You do not need to restart `ovjboss`.

Disabling the HP NNMi–HP SIM Integration

1. In the NNMi console, open the **HP NNMi–HP SIM Integration Configuration** form (**Integration Module Configuration > HP SIM**).
2. Clear the **Enable Integration** check box at the top of the form, and then click **Submit** at the bottom of the form. The integration actions are no longer available.

➤ The changes take effect immediately. You do not need to restart `ovjboss`.

Troubleshooting the HP NNMi–HP SIM Integration

SIM Actions Do Not Work

If you have verified the values in the **HP NNMi–HP SIM Integration Configuration** form and you are still not able to open a SIM page from the NNMi console, do the following:

1. Clear the web browser cache.
2. Clear all saved form or password data from the web browser.
3. Close the web browser window completely, and then re-open it.
4. Re-enter the values in the **HP NNMi–HP SIM Integration Configuration** form.

   Because NNMi cannot silently verify the connection to the SIM server, the **HP NNMi–HP SIM Integration Configuration** form status message applies to the NNMi management server connection information only.

5. Verify that SIM is running by opening the SIM homepage in a web browser.

OID Not Found in the MIB Cache Message in Traps

If the MIB definition files for the traps that SIM-managed devices generate are not loaded in NNMi, you might see an error similar to the following text:

<Cia .1.3.6.1.4.1.11.5.7.5.2.1.1.1.7.0 with value 1 was not found within the mib cache>

To resolve these errors, load the MIBs as described in step 7 on page 533.

HP NNMi–HP SIM Integration Configuration Form Reference

The **HP NNMi–HP SIM Integration Configuration** form contains the parameters for configuring communications between NNMi and SIM. This form is available from the **Integration Module Configuration** workspace.

Only NNMi users with the Administrator role can access the **HP NNMi–HP SIM Integration Configuration** form.

The **HP NNMi–HP SIM Integration Configuration** form collects information for the following general areas:

- NNMi Management Server Connection
- SIM Server Connection

To apply changes to the integration configuration, update the values on the **HP NNMi–HP SIM Integration Configuration** form, and then click **Submit**.

NNMi Management Server Connection

Table 55 lists the parameters for connecting to the NNMi management server. This is the same information that you use to open the NNMi console. You can determine many of these values by examining the URL that invokes an NNMi console session. Coordinate with the NNMi administrator to determine the appropriate values for this section of the configuration form.

Table 55 NNMi Management Server Information

Field	Description
NNMi SSL Enabled	The connection protocol specification. • If the NNMi console is configured to use HTTPS, select the **NNMi SSL Enabled** check box. This is the default configuration. • If the NNMi console is configured to use HTTP, clear the **NNMi SSL Enabled** check box.
NNMi Host	The fully-qualified domain name of the NNMi management server. This field is pre-filled with the hostname that was used to access the NNMi console. Verify that this value is the name returned by the **`nnmofficialfqdn.ovpl -t`** command run on the NNMi management server.
NNMi Port	The port for connecting to the NNMi console. This field is pre-filled with the port that the jboss application server uses for communicating with the NNMi console, as specified in the following file: • *Windows*: `%NnmDataDir%\conf\nnm\props\nms-local.properties` • *UNIX*: `$NnmDataDir/conf/nnm/props/nms-local.properties` For non-SSL connections, use the value of `jboss.http.port`, which is `80` or `8004` by default (depending on the presence of another web server when NNMi was installed). For SSL connections, use the value of `jboss.https.port`, which is `443` by default.

Table 55 NNMi Management Server Information (cont'd)

Field	Description
NNMi User	The user name for connecting to the NNMi console. This user must have the NNMi Administrator or Web Service Client role.
NNMi Password	The password for the specified NNMi user.

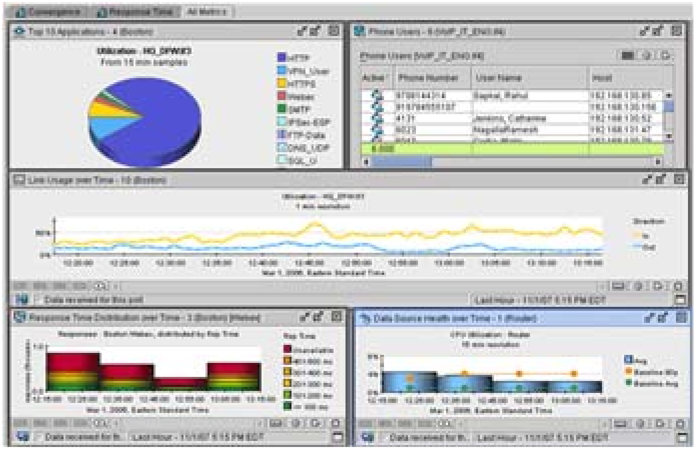
SIM Server Connection

Table 56 lists the parameters for connecting to the SIM server to open SIM pages. Coordinate with the SIM administrator to determine the appropriate values for this section of the configuration.

Table 56 SIM Server Information

SIM Server Parameter	Description
SIM SSL Enabled	The connection protocol specification for connecting to SIM. • If SIM is configured to use HTTPS, select the **HP SIM SSL Enabled** check box. This is the default configuration. • If SIM is configured to use HTTP, clear the **HP SIM SSL Enabled** check box.
SIM Host	The fully-qualified domain name of the SIM server.
SIM Port	The port for connecting to SIM. If you are using the default SIM configuration, use port `50000` (for SSL connections to SIM).

nGenius Performance Manager



NetScout Systems nGenius Performance Manager provides visibility into complex networks for the following purposes:

- Application recognition and monitoring
- Analysis and troubleshooting of packets and flows
- Response time analysis
- Reporting and capacity planning
- Convergence management
- Alarming and event identification

nGenius Performance Manager leverages deep packet inspection and flow-based technologies to deliver visibility into real-time, operational intelligence that spans several types of data:

- High-level key performance indicators (KPIs), such as response time, errors, or jitter
- Application flow data, such as use, conversations, or top talkers
- Packet-level analysis, such as decodes and bounce diagrams

nGenius Performance Manager collects performance data from a wide variety of network data sources, allowing it to monitor the usage patterns of all network infrastructures, topologies, and applications. nGenius Performance Manager then presents the results in a collection of real-time and historical views and reports that can show the following information:

- Application performance
- Users and abusers of network resources
- Resource consumption of network capacity

For information about purchasing nGenius Performance Manager, contact your HP sales representative.

This chapter contains the following topics:

HP NNMi–nGenius Performance Manager Integration

By including nGenius Performance Manager in the HP Network Node Manager i Software (NNMi) environment, network administrators who use NNMi to monitor and manage their network devices gain application-level visibility through nGenius devices.

The HP NNMi–nGenius Performance Manager integration provides the following functionality:

- Receive nGenius Performance Manager server and probe alarms in the NNMi incident views.
- Investigate the cause of an incident by launching contextual views into nGenius Performance Manager.
- Display nGenius Probes with a NetScout icon in NNMi map views.
- Launch nGenius Performance Manager QuickViews from the NNMi console.
- Launch the nGenius Performance Manager application from the NNMi console.
- Launch NNMi Layer 2 and Layer 3 Neighbor views for the nGenius Performance Manager incidents that are available in the NNMi incident views.
- Launch the NNMi Path View map for nGenius Performance Manager incidents that are available in the NNMi incident views.
- Forward Clear Trap alarms to NNMi for each alarm generated by nGenius Performance Manager.

Value

The HP NNMi–nGenius Performance Manager integration provides the following benefits:

- Reduces the cost of delivering maximum network availability.
- Consolidates the network management infrastructure in a single console.
- Increases staff productivity and efficiency with integrated fault and application-aware performance data.
- Shrinks MTTR with contextual drill down to flow and packet-level details to identify the performance problems.

Integrated Products

The information in this chapter applies to the following products:

- nGenius Performance Manager

  For the list of supported versions, see the *NNMi System and Device Support Matrix*.

- nGenius K2 version shipped with nGenius Performance Manager
- CDM Agent Firmware
- nGenius InfiniStream appliance
- NNMi 9.10

NNMi and nGenius Performance Manager Server must be installed on separate computers. The NNMi management server and the nGenius Performance Manager Server computer can be of the same or different operating systems.

Documentation

The HP NNMi–nGenius Performance Manager integration is fully described in the following document:

> *Integrating nGenius Performance Manager with HP Network Node Manager i Software* (NetScout part number 733-0194 Rev. A, available from **http://www.netscout.com**)

Enabling the HP NNMi–nGenius Performance Manager Integration

The nGenius Performance Manager Integration utility for HP Network Node Manager installation file is available in the following location on the nGenius Performance Manager server:

- *Windows*: `%nGenius Install%\rtm\bin\nGeniusNNM8.zip`
- *UNIX*: `$nGenius Install/rtm/bin/nGeniusNNM8.zip`

As a user with administrative or root privileges, install the integration utility on the NNMi management server. The utility imports all NNMi integration-related configuration data for the nGenius Server into NNMi.

The high-level steps for installing the nGenius Performance Manager Integration utility are as follows. For detailed information, see *Integrating nGenius Performance Manager with HP Network Node Manager i Software*.

1. Extract the installation files and configure NNMi support within nGenius Performance Manager.
2. Configure NetScout incidents (alarms) in NNMi.
3. Configure the nGenius Probe to send SNMP traps to port 395.
4. *Optional*. Configure Probe Router Mapping.

Using the HP NNMi–nGenius Performance Manager Integration

For information about using the HP NNMi–nGenius Performance Manager integration, see *Integrating nGenius Performance Manager with HP Network Node Manager i Software*.

Disabling the HP NNMi–nGenius Performance Manager Integration

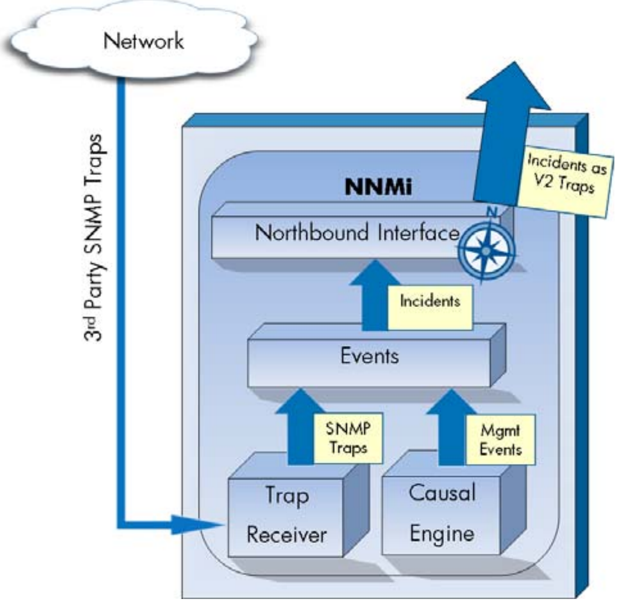
For information about disabling the HP NNMi–nGenius Performance Manager integration, see *Integrating nGenius Performance Manager with HP Network Node Manager i Software*.

Troubleshooting the HP NNMi–nGenius Performance Manager Integration

For information about troubleshooting the HP NNMi–nGenius Performance Manager integration, contact NetScout Systems Customer Support. Contact information is available at:

http://www.netscout.com/support

NNMi Northbound Interface



HP Network Node Manager i Software (NNMi) provides the NNMi northbound interface for forwarding NNMi incidents to any application that can receive SNMPv2c traps. For each NNMi management server, you can implement the NNMi northbound interface to multiple northbound applications, each configured separately.

NNMi includes support for using the NNMi northbound interface to integrate with the following products:

- The Operations Management functionality of the HP Business Service Management (BSM) platform; for information, see HP BSM Operations Management on page 559.
- The HP Operations Manager (HPOM) active messages browser; for information, see HP NNMi—HPOM Integration (Agent Implementation) on page 577.
- IBM Tivoli Netcool/OMNIbus; for information, see HP NNMi Integration Module for Netcool Software on page 615.

To integrate with a different northbound application, follow the instructions in this chapter.

This chapter contains the following topics:

NNMi Northbound Interface

The NNMi northbound interface forwards NNMi management events as SNMPv2c traps to a northbound application. The northbound application might filter, act on, and display the NNMi traps. The northbound application might also provide tools for accessing the NNMi console in the context of an NNMi trap.

The NNMi northbound interface can send incident lifecycle state change notifications, incident correlation notifications, and incident deletion notifications to the northbound application. In this way, the northbound application can replicate the results of NNMi causal analysis.

The NNMi northbound interface can also forward the SNMP traps that NNMi receives to the northbound application. The NNMi northbound interface does not forward events generated by NNM 6.x or 7.x management stations to the northbound application.

Value

The NNMi northbound interface enables event consolidation in a third-party or custom event consolidator. The NNMi northbound interface enriches events with information that can be used to integrate other applications with NNMi.

Supported Versions

The information in this chapter applies to NNMi version 9.00 or higher.

For the most recent information about supported hardware platforms and operating systems, see the *NNMi System and Device Support Matrix*.

Terminology

This chapter uses the following terms:

- Northbound application—Any application that can receive and process SNMPv2c traps.
- Trap-receiving component—The portion of a northbound application that receives SNMP traps.
  - Some applications include a separately installable component that receives SNMP traps and forwards them to another component for processing.
  - For any northbound application that does not include such a component, “trap-receiving component” is synonymous with “northbound application.”
- NNMi northbound interface—The NNMi functionality that forwards NNMi incidents as SNMPv2c traps to a northbound application.
- Northbound destination—One configuration of the NNMi northbound interface that defines the connection to the trap-receiving component of a northbound application and specifies the types of traps that NNMi will send to that northbound application.

Documentation

This chapter describes how to configure NNMi to forward NNMi incidents to any northbound application. For information about a particular northbound application, see that application's documentation.

Enabling the NNMi Northbound Interface

⚠ NNMi does not limit the amount of information sent in an SNMP trap using UDP. If any network hardware in the transmission path cannot handle the size of the trap data, or if network traffic is heavy, the trap might be lost. Therefore, it is recommended that the trap-receiving component of the northbound application be installed on the NNMi management server. The northbound application is responsible for ensuring reliable information transfer.

To enable the NNMi northbound interface, follow these steps:

1. If necessary, configure the northbound application to understand the NNMi trap definitions.
2. On the NNMi management server, configure NNMi incident forwarding:
   a. In the NNMi console, open the **HP NNMi–Northbound Interface Destinations** form (**Integration Module Configuration > Northbound Interface**), and then click **New**.

      (If you have selected an available destination, click **Reset** to make the **New** button available.)

   b. Select the **Enabled** check box to make the remaining fields on the form available.
   c. Enter the information for connecting to the northbound application.

      For information about these fields, see Northbound Application Connection Parameters on page 553.

   d. Specify the sending options and incident filter for which content to send to the northbound application.

      For information about these fields, see NNMi Northbound Interface Integration Content on page 554.

   e. Click **Submit** at the bottom of the form.

      A new window opens a status message. If the message indicates a problem with the settings, click **Return**, and then adjust the values as suggested by the text of the error message.

3. *Optional.* Create contextual interaction with NNMi by creating URLs that provide access to NNMi views from the northbound application.

   For information, in the NNMi console, click **Help > NNMi Documentation Library > Integrate NNMi Elsewhere with URLs**.

Using the NNMi Northbound Interface

When the NNMi northbound interface is enabled, the northbound destination determines the information that NNMi sends to a northbound application. Configure the northbound application to display and interpret the forwarded traps, as appropriate in your network environment. For complete information about the contents and format of the traps that NNMi sends to a northbound application, see the `hp-nnmi-nbi.mib` and `hp-nnmi-registrations.mib` files.

NNMi sends only one copy of each management event, SNMP trap, or notification trap to a northbound destination. NNMi does not queue traps. If the trap-receiving component of a northbound application is unavailable when NNMi forwards a trap, that trap is lost.

This section describes the types of traps the integration can send. For information about setting the content configuration, see NNMi Northbound Interface Integration Content on page 554.

Incident Forwarding

Management events

When the northbound destination includes management events, NNMi forwards each management event incident to the northbound application when that incident changes to the REGISTERED lifecyle state.

The OID of the forwarded management event is the SNMP Object ID on the **Management Event Configuration** form in the NNMi console. NNMi forwards all custom management events with the OID 1.3.6.1.4.1.11.2.17.19.2.0.9999.

Third-party SNMP traps

When the northbound destination includes third-party SNMP traps, NNMi forwards each incoming SNMPv1, v2c, or v3 format trap to the northbound application when the associated incident changes to the REGISTERED lifecyle state. NNMi preserves the original trap varbinds in order (as defined in the MIB) and appends the NNMi-specific varbinds to the message payload. If the original trap does not contain all of the defined varbinds, NNMi pads NULL values for the missing varbinds. If the MIB is not loaded in NNMi, NNMi cannot correctly reconstruct the trap and append the NNMi incident data; therefore, NNMi does not forward this trap.

For third-party SNMP traps, note the following:

- Because NNMi reconstructs a trap from its SNMP trap incident, the forwarded trap is in SNMPv2c format regardless of the format in which NNMi received the original trap.
- The forwarded SNMP trap shows the NNMi management server as the source object. To determine the original source object, examine the values of the (n+21)th varbind, IncidentNodeHostname (1.3.6.1.4.1.11.2.17.19.2.2.21) and the (n+24)th varbind, IncidentNodeMgmtAddr (1.3.6.1.4.1.11.2.17.19.2.2.24), where n is the number of varbinds defined for the trap in the MIB.

If any of the devices that NNMi manages also send traps to the northbound application, the northbound application must manage the duplicate device traps.

For a comparison of trap forwarding mechanisms, see Trap and Incident Forwarding on page 93.

Incident Lifecycle State Change Notifications

Enhanced closed traps

When the northbound destination includes enhanced closed notifications, NNMi sends an EventLifecycleStateClosed (1.3.6.1.4.1.11.2.17.19.2.0.1000) trap to the northbound application when the lifecycle state of an incident changes to CLOSED in NNMi. The EventLifecycleStateClosed trap includes much of the data from the original incident. The previous lifecycle state value is not included. The EventLifecycleStateClosed trap identifies the original incident in the sixth varbind, IncidentUuid (1.3.6.1.4.1.11.2.17.19.2.2.6).

State change traps

When the northbound destination includes lifecycle state changed notifications, NNMi sends a LifecycleStateChangeEvent (1.3.6.1.4.1.11.2.17.19.2.0.1001) trap to the northbound application when the lifecycle state of an incident changes to the IN PROGESS, COMPLETED, or CLOSED lifecycle state in NNMi. The northbound application can associate the LifecycleStateChangeEvent with the original incident.

The LifecycleStateChangeEvent trap identifies the original incident and the lifecycle state change in the following varbinds:

- IncidentUuid, the sixth varbind (1.3.6.1.4.1.11.2.17.19.2.2.6)

  This value matches the value of the sixth varbind in a management event or the (n+6)th varbind in a third-party SNMP trap varbind.

- IncidentLifecycleStatePreviousValue, the seventh varbind (1.3.6.1.4.1.11.2.17.19.2.2.200)

- IncidentLifecycleStateCurrentValue, the eighth varbind (1.3.6.1.4.1.11.2.17.19.2.2.201)

  The following table lists the possible integer values for lifecycle state.

Name	Integer Value
registered	1
inprogress	2
completed	3
closed	4
dampened	5

Incident Correlation Notifications

When the northbound destination includes incident correlation notifications, NNMi sends incident correlation traps to the northbound application as NNMi causal analysis correlates incidents. The northbound application can use the information in the traps to replicate the correlation changes.

Single correlation traps

For the single correlation trap option, the integration sends the following correlation traps:

- EventDedupCorrelation (1.3.6.1.4.1.11.2.17.19.2.0.1100)
- EventImpactCorrelation (1.3.6.1.4.1.11.2.17.19.2.0.1101)
- EventPairwiseCorrelation (1.3.6.1.4.1.11.2.17.19.2.0.1102)

- EventRateCorrelation (1.3.6.1.4.1.11.2.17.19.2.0.1103)
- EventApaCorrelation (1.3.6.1.4.1.11.2.17.19.2.0.1104)
- EventCustomCorrelation (1.3.6.1.4.1.11.2.17.19.2.0.1105)

Each trap identifies one parent-child incident correlation relationship in the following varbinds:

- IncidentCorrelationIndicatorParentUuid, the sixth varbind (1.3.6.1.4.1.11.2.17.19.2.2.6)
- IncidentCorrelationIndicatorChildUuid, the seventh varbind (1.3.6.1.4.1.11.2.17.19.2.2.300)

Group correlation traps

For the group correlation option, the integration sends the following correlation traps:

- EventDedupCorrelationGroup (1.3.6.1.4.1.11.2.17.19.2.0.2100)
- EventImpactCorrelationGroup (1.3.6.1.4.1.11.2.17.19.2.0.2101)
- EventPairwiseCorrelationGroup (1.3.6.1.4.1.11.2.17.19.2.0.2102)
- EventRateCorrelationGroup (1.3.6.1.4.1.11.2.17.19.2.0.2103)
- EventApaCorrelationGroup (1.3.6.1.4.1.11.2.17.19.2.0.2104)
- EventCustomCorrelationGroup (1.3.6.1.4.1.11.2.17.19.2.0.2105)

Each trap identifies the parent-child incident correlation relationships in the following varbinds:

- IncidentCorrelationIndicatorParentUuid, the sixth varbind (1.3.6.1.4.1.11.2.17.19.2.2.6)
- IncidentCorrelationIndicatorChildCount, the seventh varbind (1.3.6.1.4.1.11.2.17.19.2.2.301)
- IncidentCorrelationIndicatorChildUuidCsv, the eighth varbind (1.3.6.1.4.1.11.2.17.19.2.2.302)

  This value is a comma-separated-value list of child incident UUIDs.

Incident Deletion Notifications

When the northbound destination includes incident deletion notifications, NNMi sends an EventDeleted (1.3.6.1.4.1.11.2.17.19.2.0.3000) trap to the northbound application when an incident is deleted in NNMi. The EventDeleted trap identifies the original incident in the sixth varbind, IncidentUuid (1.3.6.1.4.1.11.2.17.19.2.2.6).

Event Forwarding Filter

When the northbound destination includes an incident filter, the object identifiers (OIDs) in the filter include or exclude (depending on the selected configuration option) the following event types:

- NNMi management event incidents
- Third-party SNMP traps
- EventLifecycleStateClosed traps
- LifecycleStateChangeEvent traps
- EventDeleted traps

- Correlation notification traps

  The following notes apply to correlation notification traps:

  - If the incident filter prevents the forwarding of the parent incident for a correlation, NNMi does not send a correlation notification trap to the northbound application.
  - If the incident filter prevents the forwarding of a child incident for a correlation, the forwarded correlation notification trap does not include that child incident's UUID. (If the correlation notification trap would not contain any child incident UUIDs, NNMi does not send that trap to the northbound application.)
  - The DuplicateCorrelation management event is forwarded independently of the EventDedupCorrelation or EventDedupCorrelationGroup correlation notification traps. Likewise, the RateCorrelation management event is forwarded independently of the EventRateCorrelation or EventRateCorrelationGroup correlation notification traps. If the incident filter prevents the forwarding of one of these correlation notification traps, NNMi might still forward the associated management events.

Changing the NNMi Northbound Interface

To change the NNMi northbound interface configuration parameters, follow these steps:

1. In the NNMi console, open the **HP NNMi–Northbound Interface Destinations** form (**Integration Module Configuration > Northbound**).
2. Select a destination, and then click **Edit**.
3. Modify the values as appropriate.

   For information about the fields on this form, see NNMi Northbound Interface Destination Form Reference on page 553.
4. Verify that the **Enabled** check box at the top of the form is selected, and then click **Submit** at the bottom of the form.

   The changes take effect immediately.

Disabling the NNMi Northbound Interface

No SNMP trap queuing occurs while a northbound destination is disabled.

To discontinue the forwarding of NNMi incidents to a northbound application, follow these steps:

1. In the NNMi console, open the **HP NNMi–Northbound Interface Destinations** form (**Integration Module Configuration > Northbound**).
2. Select a destination, and then click **Edit**.

   Alternatively, click **Delete** to entirely remove the configuration for the selected destination.

3 Clear the **Enabled** check box at the top of the form, and then click **Submit** at the bottom of the form.

  The changes take effect immediately.

Troubleshooting the NNMi Northbound Interface

If the NNMi northbound interface is not working as expected, follow these steps until you have resolved the problem:

1 Verify that the trap destination port is not blocked by a firewall.

  Ensure that the NNMi management server can directly address the northbound application by host and port.

2 Verify that the integration is running correctly:

  a In the NNMi console, open the **HP NNMi–Northbound Interface Destinations** form (**Integration Module Configuration > Northbound**).

  b Select a destination, and then click **Edit**.

  c Verify that the **Enabled** check box is selected.

3 If the northbound destination includes management events, verify this functionality:

  a In the **Closed Key Incidents** view of the NNMi console, open any incident.

  b Set the incident lifecycle state to **Registered**, and then click **Save**.

  c Set the incident lifecycle state to **Closed**, and then click **Save and Close**.

  d After 30 seconds, determine whether the northbound application received an EventLifecycleStateClosed trap (or a LifecyleStateChangeEvent trap) for this incident should.

    — If the northbound application received the trap, continue with step 4.

    — If the northbound application did not receive the trap, configure a new northbound destination to connect with a different northbound application, and then repeat this test from step a.

      If the repeated test succeeds, the problem is with the first northbound application. Consult that application's documentation for troubleshooting information.

      If the repeated test fails, contact HP Support for assistance.

4 If the northbound destination includes SNMP traps, verify this functionality:

  a Generate an SNMP trap against a node in the NNMi topology by entering the following command on the NNMi management server:

```
nnmsnmpnotify.ovpl -u username -p password -a \
discovered_node NNMi_node linkDown
```

  Where *discovered_node* is the hostname or IP address of a node in the NNMi topology and *NNMi_node* is the hostname or IP address of the NNMi management server.

b After 30 seconds, determine whether the northbound application received the forwarded trap.

— If the northbound application received the trap, the NNMi northbound interface is working correctly.

— If the northbound application did not receive the trap, configure a new northbound destination to connect with a different northbound application, and then repeat this test from step a.

If the repeated test succeeds, the problem is with the first northbound application. Consult that application's documentation for troubleshooting information.

If the repeated test fails, contact HP Support for assistance.

Application Failover and the NNMi Northbound Interface

If the NNMi management server will participate in NNMi application failover, the information in this topic applies to any integration that implements the NNMi northbound interface for sending traps to a northbound application.

The traps that NNMi sends to a northbound application include the NNMi URL in the NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2). Traps received before application failover reference what is now the standby NNMi management server. When the URL points to the standby NNMi management server, any actions that use the URL value (for example, launching the NNMi console) will fail.

Local Northbound Application

If the trap-receiving component of the northbound application is located on the NNMi management server, the following considerations apply to the configuration of the NNMi northbound interface:

- The trap-receiving component of the northbound application must be installed and configured identically on the active and standby NNMi management servers. Configure SNMP trap reception on the same port on both NNMi management servers.
- Configure the NNMi northbound interface on the primary NNMi management server only.

  On the **HP NNMi–Northbound Interface Destination** form, select either the **NNMi FQDN** or the **Use Loopback** option for **Host** identification.

At startup, the NNMi northbound interface determines the correct name or IP address of the current NNMi management server. In this way, the northbound interface sends traps to the trap-receiving component of the northbound application on the active NNMi management server.

Remote Northbound Application

If the trap-receiving component of the northbound application is not located on the NNMi management server, configure the NNMi northbound interface on the primary NNMi management server only. On the **HP NNMi–Northbound Interface Destination** form, select the **Other** option for **Host** identification.

NNMi Northbound Interface Destination Form Reference

The **HP NNMi–Northbound Interface Destination** form contains the parameters for configuring communications between NNMi and a northbound application. This form is available from the **Integration Module Configuration** workspace. (On the **HP NNMi–Northbound Interface Destinations** form, click **New**; or select a destination, and then click **Edit**.)

➤ Only NNMi users with the Administrator role can access the **HP NNMi–Northbound Interface Destination** form.

The **HP NNMi–Northbound Interface Destination** form contains information for the following areas:

- Northbound Application Connection Parameters on page 553
- NNMi Northbound Interface Integration Content on page 554
- NNMi Northbound Interface Destination Status Information on page 556

To apply changes to the integration configuration, update the values on the **HP NNMi–Northbound Interface Destination** form, and then click **Submit**.

Northbound Application Connection Parameters

Table 57 lists the parameters for configuring the connection to the northbound application.

Table 57 Northbound Application Connection Information

Field	Description
Host	The fully-qualified domain name (preferred) or the IP address of the server on which the trap-receiving component of the northbound application runs. The integration supports the following methods for identifying the server: • **NNMi FQDN** NNMi manages the connection to the northbound application on the NNMi management server and the **Host** field becomes read-only. This is the recommended configuration for northbound applications on the NNMi management server. • **Use Loopback** NNMi manages the connection to the northbound application on the NNMi management server and the **Host** field becomes read-only. • **Other** Enter a hostname or IP address for identifying the northbound application server in the **Host** field. NNMi validates that the hostname or IP address in the **Host** field is not configured as a loopback adapter. This is the default configuration. **NOTE:** If the NNMi management server participates in NNMi application failover, see Application Failover and the NNMi Northbound Interface on page 551 for information about the impact of application failover on the integration.

Table 57 Northbound Application Connection Information (cont'd)

Field	Description
Port	The UDP port where the northbound application receives SNMP traps. Enter the port number specific to the northbound application. **NOTE:** If the trap-receiving component of the northbound application is on the NNMi management server, this port number must be different from the port on which NNMi receives SNMP traps, as set in the **SNMP Port** field on the **Communication Configuration** form in the NNMi console.
Community String	A read-only community string for the northbound application to receive traps. If the northbound application configuration requires a community string in the received SNMP traps, enter that value. If the northbound application configuration does not require a specific community string, use the default value, which is `public`.

NNMi Northbound Interface Integration Content

Table 58 lists the parameters for configuring which content the NNMi northbound interface sends to the northbound application.

Table 58 NNMi Northbound Interface Content Configuration Information

Field	Description
Incidents	The incident forwarding specification. • **Management** NNMi forwards only NNMi-generated management events to the northbound application. • **3rd Party SNMP Trap** NNMi forwards only SNMP traps that NNMi receives from managed devices to the northbound application. • **Both** NNMi forwards to the northbound application both NNMi-generated management events and SNMP traps that NNMi receives from managed devices. This is the default configuration. NNMi begins forwarding incidents as soon as you enable the northbound destination. For more information, see Incident Forwarding on page 546.

Table 58 NNMi Northbound Interface Content Configuration Information (cont'd)

Field	Description
Lifecycle State Changes	The incident change notification specification. • **Enhanced Closed** NNMi sends an incident closed trap to the northbound application for each incident that changes to the CLOSED lifecycle state. This is the default configuration. • **State Changed** NNMi sends an incident lifecycle state changed trap to the northbound application for each incident that changes to the IN PROGESS, COMPLETED, or CLOSED lifecycle state. • **Both** NNMi sends an incident closed trap to the northbound application for each incident that changes to the CLOSED lifecycle state. Additionally, the integration sends an incident lifecycle state changed trap to the northbound application for each incident that changes to the IN PROGESS, COMPLETED, or CLOSED lifecycle state. **NOTE:** In this case, each time an incident changes to the CLOSED lifecycle state, the integration sends two notification traps: an incident closed trap and an incident lifecycle state changed trap. For more information, see Incident Lifecycle State Change Notifications on page 547.
Correlations	The incident correlation notification specification. • **None** NNMi does not notify the northbound application of incident correlations resulting from NNMi causal analysis. This is the default configuration. • **Single** NNMi sends a trap for each parent-child incident correlation relationship resulting from NNMi causal analysis. • **Group** NNMi sends one trap per correlation that lists all child incidents correlated to a parent incident. For more information, see Incident Correlation Notifications on page 547.
Deletions	The incident deletion specification. • **Don't Send** NNMi does not notify the northbound application when incidents are deleted in NNMi. This is the default configuration. • **Send** NNMi sends a deletion trap to the northbound application for each incident that is deleted in NNMi. For more information, see Incident Deletion Notifications on page 548.

Table 58 NNMi Northbound Interface Content Configuration Information (cont'd)

Field	Description
NNMi Console Access	The connection protocol specification in the URL for browsing to the NNMi console from the northbound application. The traps that NNMi sends to the northbound application include the NNMi URL in the NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2). The configuration page defaults to the setting that matches the NNMi configuration. If the NNMi console is configured to accept both HTTP and HTTPS connections, you can change the HTTP connection protocol specification in the NNMi URL. For example, if all users of the northbound application are on the intranet, you can set NNMi console access from the northbound application to be over HTTP. To change the protocol for connecting to the NNMi console from the northbound application, select the **HTTP** option or the **HTTPS** option as appropriate.
Incident Filters	A list of object identifiers (OIDs) on which the integration filters the events sent to the northbound application. Each filter entry can be a valid numeric OID (for example, .1.3.6.1.6.3.1.1.5.4.1.3.6.1.4.1.9) or OID prefix (for example, .1.3.6.1.6.3.1.1.5.*). Select one of the following options: • **None** NNMi sends all events to the northbound application. This is the default configuration. • **Include** NNMi sends only the specific events that match the OIDs identified in the filter. • **Exclude** NNMi sends all events except for the specific events that match the OIDs identified in the filter. Specify the incident filter: • To add a filter entry, enter the text in the lower text box, and then click **Add**. • To delete a filter entry, select that entry from the list in the upper box, and then click **Remove**. For more information, see Event Forwarding Filter on page 548.

NNMi Northbound Interface Destination Status Information

Table 59 lists the read-only status information for the northbound destination. This information is useful for verifying that the integration is working correctly.

Table 59 NNMi Northbound Interface Destination Status Information

Field	Description
Trap Destination IP Address	The IP address to which the destination host name resolves. This value is unique to this northbound destination.

Table 59 NNMi Northbound Interface Destination Status Information (cont'd)

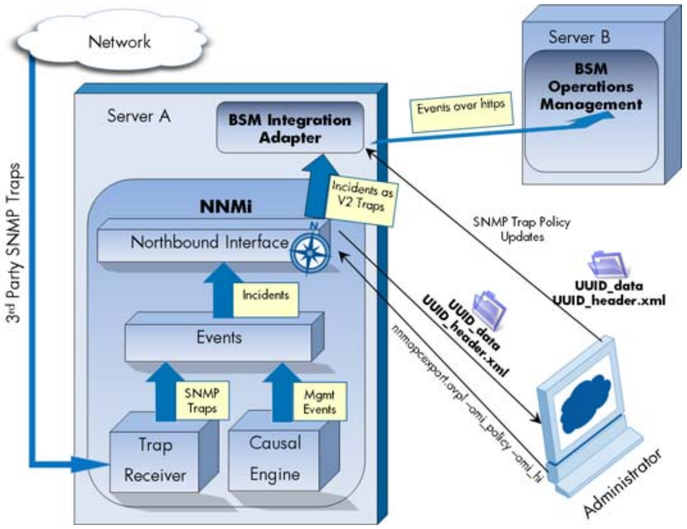
Field	Description
Uptime (seconds)	The time (in seconds) since the northbound component was last started. The traps that NNMi sends to a northbound application include this value in the sysUptime field (1.3.6.1.2.1.1.3.0). This value is the same for all integrations that use the NNMi northbound interface. To see the latest value, either refresh or close and re-open the form.
NNMi URL	The URL for connecting to the NNMi console. The traps that NNMi sends to a northbound application include this value in the NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2). This value is unique to this northbound destination.

MIB Information used by the NNMi Northbound Interface

Complete the following steps to load specific MIBs into NNMi, then view the management information used for incident notifications sent by the NNMi northbound integration.

1. From a command prompt, run the **`nnmloadmib.ovpl -load hp-nnmi.mib`** command to load the `hp-nnmi.mib` file.
2. From a command prompt, run the **`nnmloadmib.ovpl -load hp-nnmi-registrations.mib`** command to load the `hp-nnmi-registrations.mib` file.
3. From a command prompt, run the **`nnmloadmib.ovpl -load hp-nnmi-nbi.mib`** command to load the `hp-nnmi-nbi.mib` file.
4. Optional Step: From a command prompt, run the **`nnmloadmib.ovpl -load hp-nnmi-ispi-perf-nbi.mib`** command to load the `hp-nnmi-ispi-perf-nbi.mib` file.
5. From the NNMi console, open the **Configuration** workspace.
6. Click **MIBs->Loaded MIBs**.
7. Double-click each of the MIBs you just loaded; then click **MIB Variables** to view the MIB information.

HP BSM Operations Management



The Operations Management functionality of the HP Business Service Management (BSM) platform provides comprehensive event management; proactive performance monitoring; and automated alerting, reporting, and graphing for management operating systems, middleware, and application infrastructure. BSM Operations Management consolidates events from a wide range of sources into a single view.

For information about purchasing BSM, contact your HP sales representative.

This chapter contains the following topics:

HP NNMi—HP BSM Operations Management Integration

The HP NNMi—HP BSM Operations Management integration forwards NNMi management event incidents as SNMPv2c traps to the HP BSM Integration Adapter on the NNMi management server. The BSM Integration Adapter filters the NNMi traps and forwards them to the BSM Operations Management event browser.

The HP NNMi—HP BSM Operations Management integration can also forward the SNMP traps that NNMi receives to the adapter. The integration does not forward events generated by NNM 6.x or 7.x management stations to the adapter.

The HP NNMi—HP BSM Operations Management integration also provides for accessing the NNMi console from within the BSM Operations Management event browser.

This chapter describes the direct integration between NNMi and the BSM Operations Management event browser. Alternatively, you could integrate NNMi with HP Operations Manager (HPOM), which could then forward events to the BSM Operations Management event browser.

The HP NNMi—HP BSM Operations Management integration is a specific implementation of the NNMi northbound interface, which is described in NNMi Northbound Interface on page 543.

The HP NNMi—HP BSM Operations Management integration consists of the following components:

- nnmi-hpom agent integration module
- nnmopcexport.ovpl tool

Value

The HP NNMi—HP BSM Operations Management integration provides event consolidation in the BSM Operations Management event browser for the network management, system management, and application management domains, so that users of the BSM Operations Management event browser can detect and investigate potential network problems.

The primary features of the integration are as follows:

- Automatic incident forwarding from NNMi to the BSM Integration Adapter. Forwarded incidents appear in the BSM Operations Management event browser.
- Access to the NNMi console from the BSM Operations Management event browser.
  - Open the NNMi **Incident** form in the context of a selected event.
  - Open an NNMi view (for example, the Layer 2 Neighbor view) in the context of a selected event and node.
  - Launch an NNMi tool (for example, status poll) in the context of a selected event and node.

Integrated Products

The information in this chapter applies to the following products:

- BSM with the HP Operations Manager i license

  For the list of supported versions, see the *NNMi System and Device Support Matrix*.

- NNMi 9.10 on the Windows or Linux operating system only

NNMi and BSM must be installed on separate computers. The NNMi management server and the BSM server computer can be of the same or different operating systems.

The BSM Integration Adapter requires a license and must be installed on the NNMi management server computer *after* NNMi installation.

For the most recent information about supported hardware platforms and operating systems, see the support matrices for all products.

Documentation

This chapter describes how to configure NNMi to communicate with the BSM Operations Management event browser.

The BSM documentation describes how to install and use the BSM Integration Adapter and the applications that access the NNMi console from the BSM Operations Management event browser.

- *HP BSM Integration Adapter Installation and Configuration Guide*
- *HP BSM Integration Adapter User Guide*
- HP BSM Integration Adapter help
- *HP BSM Operations Management Extensibility Guide*

Enabling the HP NNMi—HP BSM Operations Management Integration

It is recommended that an experienced BSM Integration Adapter user complete the procedure for enabling the HP NNMi—HP BSM Operations Management integration.

➤ When NNMi integrates with the HP Business Service Management (BSM) topology database, the HP NNMi—HP BSM Operations Management integration can associate incidents regarding NNMi-managed devices with BSM configuration items (CIs). This information is not available with the standard NNMi northbound interface. For more information, see Configuration Item Identifiers on page 564.

To enable the HP NNMi—HP BSM Operations Management integration, follow these steps:

1 On the NNMi management server, generate an SNMP trap policy file for the traps that NNMi forwards:

   a Verify that the NNMi services are running:

   ```
   ovstatus -c
   ```

   All NNMi services should show the state RUNNING.

   b Generate the SNMP trap policy file by entering the following command:

   ```
   nnmopcexport.ovpl -u <username> -p <password> \
   -template "NNMi Management Events" -application "NNMi" \
   -omi_policy -omi_hi
   ```

   The values for ***<username>*** and ***<password>*** correspond to an NNMi console user with the Administrator role.

This command creates two files in the current directory:

- The *<UUID>*`_data` file is the SNMP trap policy file, where *<UUID>* is a universally unique identifier.
- The *<UUID>*`_header.xml` file identifies the *<UUID>*`_data` file to the BSM Integration Adapter.

Do not edit or rename these output files, as doing so renders them unusable by the BSM Integration Adapter.

The SNMP trap policy file includes a policy condition for each management event and SNMP trap configuration in the current NNMi incident configuration. For information about customizing the output of this command, see the *nnmopcexport.ovpl* reference page, or the UNIX manpage.

For information about the default policy conditions and customizing conditions, see Using the HP NNMi—HP BSM Operations Management Integration on page 564.

2 On the NNMi management server, configure the BSM Integration Adapter:

a Install and configure the BSM Integration Adapter as described in the *HP BSM Integration Adapter Installation and Configuration Guide*.

The HP Operations agent from HPOM and the BSM Integration Adapter cannot run simultaneously on one system. If necessary, uninstall the HP Operations agent before installing the BSM Integration Adapter.

b Use the BSM Integration Adapter user interface to import the header and policy files created in step 1 of this procedure.

For more information, see *Managing policies* > *Import policies* in the HP BSM Integration Adapter help.

c Use the BSM Integration Adapter user interface to start the new policies.

For more information, see *Managing policies* > *Activate and deactivate policies* in the HP BSM Integration Adapter help.

3 Identify an available port for SNMP communications between NNMi and the BSM Integration Adapter.

The BSM Integration Adapter will listen on this port for the SNMP traps that NNMi forwards to this port. While enabling the integration, this port number is used in both step 4 (for the BSM Integration Adapter) and step 5 (for NNMi) of this procedure.

The SNMP communications port is different from the HTTP port for the Apache Tomcat server that you specified while configuring the BSM Integration Adapter with the `ia-config.bat` (Windows) or `ia-config.sh` (Linux) command.

Because the BSM Integration Adapter is installed on the NNMi management server, this port number must be different from the port on which NNMi receives SNMP traps.

a In the NNMi console, open the **Communication Configuration** form from the **Configuration** workspace.

b In the **Default SNMP Settings** area, notice the value of **SNMP Port**.

c Select a port that is different from the value of **SNMP Port** on the **Communication Configuration** form. A good practice is to use a port number similar to 162, which is the standard UDP port for receiving SNMP traps. For example, if port 162 is not available, try port 5162.

d On the NNMi management server, run the command **`netstat -a`**, and then search the output for the port you selected in step c. If that port number does not appear in the output, it is probably available for the BSM Integration Adapter to use.

4 On the NNMi management server, configure the agent inside the BSM Integration Adapter with a custom port for receiving SNMP traps from NNMi by entering the following commands:

- *Windows* NNMi management server:

  a Configure the agent:

  ```
  ovconfchg -ns eaagt -set SNMP_TRAP_PORT <custom_port> \
  -set SNMP_SESSION_MODE NNM_LIBS
  ```

  b Restart the agent:

  ```
  ovc -restart opctrapi
  ```

- *Linux* NNMi management server:

  a Configure the agent:

  ```
  ovconfchg -ns eaagt -set SNMP_TRAP_PORT <custom_port> \
  -set SNMP_SESSION_MODE NO_TRAPD
  ```

  b Restart the agent:

  ```
  ovc -restart opctrapi
  ```

For *<custom_port>*, use the port that you identified in step 3 of this procedure.

5 On the NNMi management server, configure NNMi incident forwarding to the BSM Integration Adapter:

a In the NNMi console, open the **HP NNMi–HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).

b Click **HPOM agent implementation**, and then click **New**.

(If you have selected an available destination, click **Reset** to make the **New** button available.)

c On the **HP NNMi–HPOM Agent Destination** form, select the **Enabled** check box to make the remaining fields on the form available.

d Enter the information for connecting to the BSM Integration Adapter on the NNMi management server. The trap destination port is the port that you identified in step 3 of this procedure.

For information about these fields, see BSM Integration Adapter Connection on page 572.

e Specify the sending options. Select the **HTTP** option for the **NNMi Console Access** field.

For information about these fields, see BSM Operations Management Integration Content on page 573.

f Click **Submit** at the bottom of the form.

A new window opens a status message. If the message indicates a problem with the settings, click **Return**, and then adjust the values as suggested by the text of the error message.

6 *Optional*. On the BSM server, install and configure the HPOprInf infrastructure content pack.

For information, see the *HP BSM Operations Management Extensibility Guide*.

Using the HP NNMi—HP BSM Operations Management Integration

The HP NNMi—HP BSM Operations Management integration provides a one-way flow of NNMi management events and SNMP traps to the BSM Operations Management event browser. The NNMi SNMP trap policy determines how the BSM Operations Management event browser treats and opens the incoming traps. For example, you can change a policy condition to include the value of a trap custom attribute in the event title.

NNMi sends only one copy of each management event or SNMP trap to the BSM Integration Adapter. This behavior is different from that of the NNM 6.x/7.x integration with HPOM.

View the forwarded NNMi incidents in the BSM Operations Management event browser. Menu commands in the BSM Operations Management event browser provide access to NNMi views in the context of the selected event. Information embedded in each event supports this cross-navigation:

- The `nnmi.server.name` and `nnmi.server.port` custom attributes in the event identify the NNMi management server.
- The `nnmi.incident.uuid` custom attribute identifies the incident in the NNMi database.

In the BSM Operations Management event browser, the original source object appears in the **Object** field on the **Additional Info** tab and in the `nnm.source.name` custom attribute.

Configuration Item Identifiers

In HP Business Service Management (BSM) and HP Universal CMDB Software (UCMDB), a configuration item (CI) is a database representation of a component in the IT environment. A CI can be a line of business, business process, application, server hardware, or a service.

When NNMi integrates with the BSM topology database or UCMDB, NNMi shares CI information with BSM or UCMDB for the devices that NNMi manages. In this case, the HP NNMi—HP BSM Operations Management integration can associate incidents regarding NNMi-managed devices with BSM or UCMDB CIs. The SNMP trap policy conditions enable this association.

For information about the integrations with BSM and UCMDB, see:

- HP Business Service Management Topology on page 457
- HP Universal CMDB on page 467

Health Indicators

Because the NNMi SNMP trap policy file was created with the `-omi_hi` option to `nnmopcexport.ovpl`, the policy file associates a health indicator with each standard NNMi management event in the SNMP trap policy file, as appropriate. (Not all management event types have health indicators.) The health indicator is available in the `EtiHint` custom attribute.

For the specific health indicators, see the SNMP trap policy file.

Default Policy Conditions

The default integration behavior varies with the integration content, as described here:

- NNMi management event incidents
  - The NNMi SNMP trap policy file includes conditions for all NNMi management event configurations defined in the NNMi incident configuration when the file was generated.
  - The events created from NNMi management events appear in the BSM Operations Management event browser.
  - These traps include the CI information described in Configuration Item Identifiers on page 564.
  - The events created from these traps include health indicators described in Health Indicators on page 565.
- Third-party SNMP traps
  - The NNMi SNMP trap policy file includes conditions for all SNMP trap configurations defined in the NNMi incident configuration when the file was generated.
  - The events created from third-party traps appear in the BSM Operations Management event browser.
  - These traps include the CI information described in Configuration Item Identifiers on page 564.
  - The events created from these traps do not include health indicators.
  - If you configure the integration to forward all received SNMP traps and the BSM Operations Management event browser receives SNMP traps directly from devices that NNMi manages, the BSM Operations Management event browser receives duplicate device traps. You can set the policies to correlate SNMP traps from NNMi with those that the BSM Operations Management event browser receives directly from managed devices.
- EventLifecycleStateClosed traps
  - The BSM Integration Adapter logs the events created from these traps. Generally, they do not appear in the BSM Operations Management event browser.
  - The NNMi SNMP trap policy file causes the BSM Integration Adapter to acknowledge the event that corresponds to the closed NNMi incident in the BSM Operations Management event browser.

- LifecycleStateChangeEvent traps
  - — The NNMi SNMP trap policy file does not include conditions for processing these traps. The BSM Integration Adapter does not forward these traps to the BSM Operations Management event browser.
- EventDeleted traps
  - — The NNMi SNMP trap policy file does not include conditions for processing these traps. The BSM Integration Adapter does not forward these traps to the BSM Operations Management event browser.
- Correlation notification traps
  - — The BSM Integration Adapter logs the events created from these traps. They do not appear in the BSM Operations Management event browser.
  - — The BSM Integration Adapter processes the NNMi correlation traps to replicate NNMi incident correlation in the BSM Operations Management event browser.

Customizing Policy Conditions

Use the BSM Integration Adapter user interface to customize the default policy conditions. For more information, see *Developing SNMP interceptor policies > Configure SNMP rules* in the HP BSM Integration Adapter help.

More Information

For more information about the HP NNMi—HP BSM Operations Management integration, see the following references:

- For descriptions of the trap types that the integration sends to the BSM Integration Adapter, see Using the NNMi Northbound Interface on page 546.
- For information about the format of the traps that NNMi sends to the BSM Integration Adapter, see the `hp-nnmi-nbi.mib` file.
- For detailed information about using the HP NNMi—HP BSM Operations Management integration, see the *HP BSM Operations Management Extensibility Guide*.

Changing the HP NNMi—HP BSM Operations Management Integration

This section contains the following topics:

- Update the SNMP Trap Policy Conditions for New NNMi Traps on page 567
- Change the Configuration Parameters on page 567

Update the SNMP Trap Policy Conditions for New NNMi Traps

If new SNMP trap incident configurations have been added to NNMi since the integration was configured, follow these steps:

1. On the NNMi management server, use the `nnmopcexport.ovpl` command to create an SNMP trap policy file for the new traps.

   For the `-template` option, specify a name that is different from the names of the existing SNMP trap policy files.

   Use the `-omi_policy` and `-omi_hi` options.

   You can limit the file contents to a specific author or OID prefix value. For more information, see the *nnmopcexport.ovpl* reference page, or the UNIX manpage.

2. Use the BSM Integration Adapter user interface to import and start the new header and policy files.

Alternatively, you can re-create the SNMP trap policy file for all NNMi management events and SNMP traps. If you take this approach, delete the old policies from the BSM Integration Adapter user interface.

➤ If the BSM Integration Adapter configuration includes multiple policy conditions for one NNMi incident, duplicate messages appear in the BSM Operations Management event browser.

Change the Configuration Parameters

To change the integration configuration parameters, follow these steps:

1. In the NNMi console, open the **HP NNMi–HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).

2. Click **HPOM agent implementation**.

3. Select a destination, and then click **Edit**.

4. Modify the values as appropriate.

   For information about the fields on this form, see HP NNMi–HPOM Agent Destination Form Reference (BSM Operations Management Integration) on page 572.

5. Verify that the **Enable Integration** check box at the top of the form is selected, and then click **Submit** at the bottom of the form.

   The changes take effect immediately.

Disabling the HP NNMi—HP BSM Operations Management Integration

No SNMP trap queuing occurs while a destination is disabled.

To discontinue the forwarding of NNMi incidents to the BSM Integration Adapter, follow these steps:

1. In the NNMi console, open the **HP NNMi–HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).
2. Click **HPOM agent implementation**.
3. Select a destination, and then click **Edit**.

   Alternatively, click **Delete** to entirely remove the configuration for the selected destination.
4. Clear the **Enable Integration** check box at the top of the form, and then click **Submit** at the bottom of the form.

   The changes take effect immediately.

Optionally deactivate or delete the SNMP trap policy as described in the HP BSM Integration Adapter help.

Troubleshooting the HP NNMi—HP BSM Operations Management Integration

This section contains the following topics:

- BSM Operations Management Event Browser Contains No Forwarded Incidents on page 568
- BSM Operations Management Event Browser Contains Only Some Forwarded Incidents on page 571

BSM Operations Management Event Browser Contains No Forwarded Incidents

In the following procedure, the `OVBIN` environment variable refers to the `bin` directory containing the commands for configuring the agent inside the BSM Integration Adapter. The `OVBIN` environment variable defaults to the following value:

- *Windows*: `<drive>\Program Files\HP\HP BTO Software\bin`
- *Linux*: `/opt/OV/bin`

If the BSM Operations Management event browser does not contain any incidents from NNMi, follow these steps:

1 On the NNMi management server, verify the agent configuration:

- *Windows* NNMi management server:

  ```
  %OVBIN%\ovconfget eaagt
  ```

- *Linux* NNMi management server:

  ```
  $OVBIN/ovconfget eaagt
  ```

The command output should include the following information:

- *Windows*:

  ```
  SNMP_SESSION_MODE=NNM_LIBS
  SNMP_TRAP_PORT=<custom_port>
  ```

- *Linux*:

  ```
  SNMP_SESSION_MODE=NO_TRAPD
  SNMP_TRAP_PORT=<custom_port>
  ```

The value of *<custom_port>* should *not* be 162 and should match the value of the **Port** field on the **HP NNMi–HPOM Agent Destination** form.

2 Evaluate the agent configuration by considering the results from step 1:

- If the agent configuration is as expected, continue with step 3 of this procedure.
- If the SNMP_SESSION_MODE parameter is not set correctly, repeat step 4 on page 563 until the ovconfget command returns the expected results.
- If the value of *<custom_port>* is 162 or does not match the value of the **Port** field on the **HP NNMi–HPOM Agent Destination** form, repeat step 3 on page 562 through step 5 on page 563, as appropriate, until the ovconfget command returns the expected results.

3 On the NNMi management server, verify that the agent is running:

- *Windows* NNMi management server:

  ```
  %OVBIN%\opcagt -status
  ```

- *Linux* NNMi management server:

  ```
  $OVBIN/opcagt -status
  ```

The command output should include an opctrapi entry similar to the following example:

```
opctrapi  OVO SNMP Trap Interceptor  AGENT,EA  (4971)  Running
```

If the output is not as expected, restart the agent:

```
ovc -restart opctrapi
```

4. On the NNMi management server, verify that the agent is listening on the expected SNMP trap port:

   a. Run the following command:

      — *Windows*: **`netstat -an | findstr <custom_port>`**

      — *Linux*: **`netstat -an | grep <custom_port>`**

      Where *`<custom_port>`* is the value of `SNMP_TRAP_PORT` from step 1 of this procedure.

   b. Verify that the output includes the state LISTENING or LISTEN.

      If the output is not as expected, restart the agent:

      ```
      ovc -restart opctrapi
      ```

5. On the NNMi management server, verify that the SNMP trap policy file for NNMi has been deployed to the BSM Integration Adapter on the NNMi management server:

   - *Windows* NNMi management server:

     ```
     %OVBIN%\ovpolicy -list
     ```

   - *Linux* NNMi management server:

     ```
     $OVBIN/ovpolicy -list
     ```

   The command output should include an entry similar to the following example:

   ```
   Type     Name                          Status     Version
   --------------------------------------------------------------
   trapi    "NNMi Management Events"      enabled    0001.0000
   ```

   The value of the `Name` field is the name of the SNMP trap policy file from the `-template` option to `nnmopcexport.ovpl` in step 1 on page 561.

6. Verify that the BSM Integration Adapter is receiving traps:

   a. Verify that the BSM Integration Adapter can send events to the BSM Operations Management event browser.

   b. Enable tracing of the BSM Integration Adapter to determine whether the traps arrive at the BSM Integration Adapter.

7. Verify that NNMi is forwarding management events to the BSM Integration Adapter.

   For information, see Troubleshooting the NNMi Northbound Interface on page 550.

BSM Operations Management Event Browser Contains Only Some Forwarded Incidents

If one or more NNMi incidents do not appear in the BSM Operations Management event browser, follow these steps:

1. On the NNMi management server, verify that the SNMP trap policy does not suppress the trap.
2. On the BSM server, verify that BSM Operations Management is running.

   If the BSM server shuts down, the BSM Integration Adapter queues received traps. The BSM Integration Adapter forwards the queued traps when the BSM Operations Management event browser becomes available.

   If the BSM Integration Adapter shuts down, the forwarded traps are lost. NNMi does not resend traps.
3. On the NNMi management server, verify that the NNMi processes are running:

   ```
   ovstatus -c
   ```

   Any traps sent to NNMi while it is shut down are lost.

HP NNMi–HPOM Agent Destination Form Reference (BSM Operations Management Integration)

The **HP NNMi–HPOM Agent Destination** form contains the parameters for configuring communications between NNMi and the BSM Integration Adapter. This form is available from the **Integration Module Configuration** workspace. (On the **HP NNMi–HPOM Integration Selection** form, click **HPOM agent implementation**. Click **New**, or select a destination, and then click **Edit**.)

➤ Only NNMi users with the Administrator role can access the **HP NNMi–HPOM Agent Destination** form.

The **HP NNMi–HPOM Agent Destination** form collects information for the following areas:

- BSM Integration Adapter Connection on page 572
- BSM Operations Management Integration Content on page 573
- BSM Integration Adapter Destination Status Information on page 575

To apply changes to the integration configuration, update the values on the **HP NNMi–HPOM Agent Destination** form, and then click **Submit**.

BSM Integration Adapter Connection

Table 60 lists the parameters for configuring the connection to the BSM Integration Adapter.

Table 60 BSM Integration Adapter Connection Information

Field	Description
Host	The fully-qualified domain name (preferred) or the IP address of the NNMi management server, which is the system on which the BSM Integration Adapter receives SNMP traps from NNMi. The integration supports the following methods for identifying the BSM Integration Adapter host: • **NNMi FQDN** NNMi manages the connection to the BSM Integration Adapter on the NNMi management server and the **Host** field becomes read-only. This is the default and recommended configuration. • **Use Loopback** Do not use this option. • **Other** Do not use this option. **NOTE:** If the NNMi management server participates in NNMi application failover, see Application Failover and the NNMi Northbound Interface on page 551 for information about the impact of application failover on the integration module.

Table 60 BSM Integration Adapter Connection Information (cont'd)

Field	Description
Port	The UDP port where the BSM Integration Adapter receives SNMP traps. Enter the port number specific to the BSM Integration Adapter. This value is the port that you identified in step 3 on page 562. To determine the port, run the **`ovconfget eaagt`** command on the NNMi management server. The trap port is the value of the `SNMP_TRAP_PORT` variable. **NOTE:** This port number must be different from the port on which NNMi receives SNMP traps, as set in the **SNMP Port** field on the **Communication Configuration** form in the NNMi console.
Community String	A read-only community string for the BSM Integration Adapter to receive traps. For the HP NNMi—HP BSM Operations Management integration, use the default value, which is `public`.

BSM Operations Management Integration Content

Table 61 lists the parameters for configuring which content NNMi sends to the BSM Integration Adapter.

Table 61 BSM Operations Management Integration Content Configuration Information

Field	Description
Incidents	The incident forwarding specification. • **Management** NNMi forwards only NNMi-generated management events to the BSM Integration Adapter. • **SNMP 3rd Party Trap** NNMi forwards only SNMP traps that NNMi receives from managed devices to the BSM Integration Adapter. • **Both** NNMi forwards to the BSM Integration Adapter both NNMi-generated management events and SNMP traps that NNMi receives from managed devices. This is the default configuration. NNMi begins forwarding incidents as soon as you enable the destination. For more information, see Incident Forwarding on page 546.

Table 61 BSM Operations Management Integration Content Configuration Information (cont'd)

Field	Description
Lifecycle State Changes	The incident change notification specification. • **Enhanced Closed** NNMi sends an incident closed trap to the BSM Integration Adapter for each incident that changes to the Closed lifecycle state. This is the default configuration. • **State Changed** NNMi sends an incident lifecycle state changed trap to the BSM Integration Adapter for each incident that changes to the In Progress, Completed, or Closed lifecycle state. • **Both** NNMi sends an incident closed trap to the BSM Integration Adapter for each incident that changes to the Closed lifecycle state. Additionally, the integration sends an incident lifecycle state changed trap to the BSM Integration Adapter for each incident that changes to the In Progess, Completed, or Closed lifecycle state. **NOTE:** In this case, each time an incident changes to the Closed lifecycle state, the integration sends two notification traps: an incident closed trap and an incident lifecycle state changed trap. For more information, see Incident Lifecycle State Change Notifications on page 547.
Correlations	The incident correlation notification specification. • **None** NNMi does not notify the BSM Integration Adapter of incident correlations resulting from NNMi causal analysis. This is the default configuration. • **Single** NNMi sends a trap for each parent-child incident correlation relationship resulting from NNMi causal analysis. • **Group** NNMi sends one trap per correlation that lists all child incidents correlated to a parent incident. For more information, see Incident Correlation Notifications on page 547.
Deletions	The incident deletion specification. • **Don't Send** NNMi does not notify the BSM Integration Adapter when incidents are deleted in NNMi. This is the default configuration. • **Send** NNMi sends a deletion trap to the BSM Integration Adapter for each incident that is deleted in NNMi. For more information, see Incident Deletion Notifications on page 548.
NNMi Console Access	The connection protocol specification in the URL for browsing to the NNMi console from the BSM Operations Management event browser. The traps that NNMi sends to the BSM Integration Adapter include the NNMi URL in the NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2). The integration requires an HTTP connection to the NNMi console. Select the **HTTP** option.

Table 61 BSM Operations Management Integration Content Configuration Information (cont'd)

Field	Description
Incident Filters	A list of object identifiers (OIDs) on which the integration filters the events sent to the BSM Integration Adapter. Each filter entry can be a valid numeric OID (for example, .1.3.6.1.6.3.1.1.5.4.1.3.6.1.4.1.9) or OID prefix (for example, .1.3.6.1.6.3.1.1.5.*). Select one of the following options: • **None** NNMi sends all events to the BSM Integration Adapter. This is the default configuration. • **Include** NNMi sends only the specific events that match the OIDs identified in the filter. • **Exclude** NNMi sends all events except for the specific events that match the OIDs identified in the filter. Specify the incident filter: • To add a filter entry, enter the text in the lower text box, and then click **Add**. • To delete a filter entry, select that entry from the list in the upper box, and then click **Remove**. For more information, see Event Forwarding Filter on page 548.

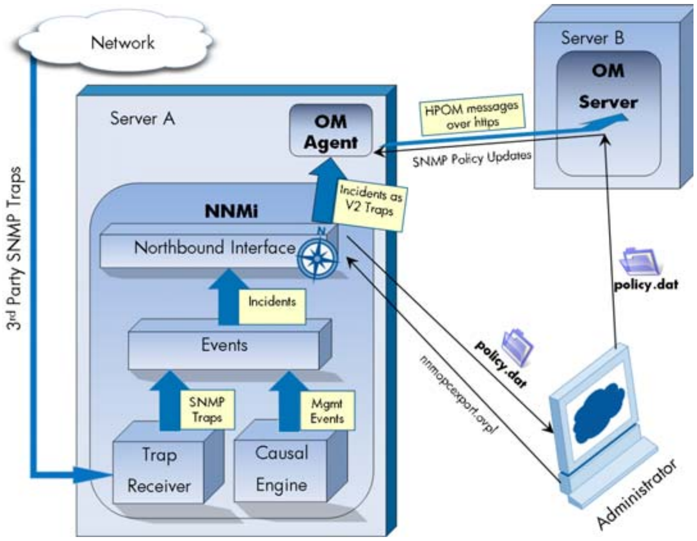
BSM Integration Adapter Destination Status Information

Table 62 lists the read-only status information for the BSM Integration Adapter. This information is useful for verifying that the integration is working correctly.

Table 62 BSM Integration Adapter Destination Status Information

Field	Description
Trap Destination IP Address	The IP address to which the BSM Integration Adapter destination host name resolves. This value is unique to this destination.
Uptime (seconds)	The time (in seconds) since the northbound component was last started. The traps that NNMi sends to the BSM Integration Adapter include this value in the sysUptime field (1.3.6.1.2.1.1.3.0). This value is the same for all integrations that use the NNMi northbound interface. To see the latest value, either refresh or close and re-open the form.
NNMi URL	The URL for connecting to the NNMi console. The traps that NNMi sends to the BSM Integration Adapter include this value in the NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2). This value is unique to this northbound destination.

HP Operations Manager



HP Operations Manager (HPOM) provides comprehensive event management; proactive performance monitoring; and automated alerting, reporting, and graphing for management operating systems, middleware, and application infrastructure. HPOM consolidates events from a wide range of sources into a single view.

For information about purchasing HPOM, contact your HP sales representative.

This chapter describes the available integrations:

- HP NNMi—HPOM Integration (Agent Implementation)
- HP NNMi—HPOM Integration (Web Services Implementation)

HP NNMi—HPOM Integration (Agent Implementation)

The agent implementation of the HP NNMi—HPOM integration is the preferred solution for integrating HPOM with NNMi.

If the agent and the web services implementations of the HP NNMi—HPOM integration both forward messages to the same HPOM management server, you might not see all messages from both implementations in the HPOM active messages browser. For this reason, HP does not support running both implementations of the HP NNMi—HPOM integration from one NNMi management server to the same HPOM management server concurrently.

This section contains the following topics:

- About the HP NNMi–HPOM Integration (Agent Implementation) on page 578
- Enabling the HP NNMi–HPOM Integration (Agent Implementation) on page 579
- Using the HP NNMi–HPOM Integration (Agent Implementation) on page 584
- Changing the HP NNMi–HPOM Integration Configuration (Agent Implementation) on page 586
- Disabling the HP NNMi–HPOM Integration (Agent Implementation) on page 587

- Troubleshooting the HP NNMi–HPOM Integration (Agent Implementation) on page 588
- HP NNMi–HPOM Agent Destination Form Reference (Agent Implementation) on page 591

About the HP NNMi–HPOM Integration (Agent Implementation)

The agent implementation of the HP NNMi–HPOM integration forwards NNMi management events as SNMPv2c traps to an HP Operations agent on the NNMi management server. The agent filters the NNMi traps and forwards them to the HPOM active messages browser. The agent configuration determines which HPOM management server receives the forwarded incident.

The HP NNMi–HPOM integration can also forward the SNMP traps that NNMi receives to the agent. The integration does not forward events generated by NNM 6.x or 7.x management stations to the agent.

The HP NNMi–HPOM integration also provides for accessing the NNMi console from within HPOM.

The agent implementation of the HP NNMi—HPOM integration is a specific implementation of the NNMi northbound interface, which is described in NNMi Northbound Interface on page 543.

The agent implementation of the HP NNMi–HPOM integration consists of the following components:

- nnmi-hpom agent integration module
- nnmopcexport.ovpl tool

Value

The HP NNMi–HPOM integration provides event consolidation in the HPOM active messages browser for the network management, system management, and application management domains, so that HPOM users can detect and investigate potential network problems.

The primary features of the integration are as follows:

- Automatic incident forwarding from NNMi to the HP Operations agent. Forwarded incidents appear in the HPOM active messages browser.
- Access to the NNMi console from HPOM.
  - HPOM users can open the NNMi **Incident** form in the context of a selected message.
  - HPOM users can launch an NNMi view (for example, the Layer 2 Neighbor view) in the context of a selected message and node.
  - HPOM users can launch an NNMi tool (for example, status poll) in the context of a selected message and node.

Integrated Products

The information in this section applies to the following products:

- HPOM for Windows (also called OMW)
- HPOM for UNIX (also called OMU)
- HPOM for Linux (also called OML)

For the list of supported versions, see the *NNMi System and Device Support Matrix*.

- NNMi 9.10

NNMi and HPOM must be installed on separate computers. The NNMi management server and the HPOM management server computer can be of the same or different operating systems.

The HP Operations agent requires a license and must be installed on the NNMi management server computer *after* NNMi installation.

For the most recent information about supported hardware platforms and operating systems, see the support matrices for all products.

Documentation

This chapter describes how to configure NNMi to communicate with HPOM.

The HPOM documentation describes how to install and use the HPOM applications that access the NNMi console from the HPOM active messages browser.

- For HPOM for Windows, see the information for the HP NNMi Adapter in the HPOM help.
- For HPOM for UNIX version 9.xx, see the *Integrating NNMi into HPOM* section in the *HP Operations Manager for UNIX Administrator's Reference*.
- For HPOM for UNIX version 8.3x, see the *HP NNMi–HPOM Integration for HP Operations Manager User's Guide*.
- For HPOM for Linux, see the *Integrating NNMi into HPOM* section in the *HP Operations Manager for Linux Administrator's Reference*.

Enabling the HP NNMi–HPOM Integration (Agent Implementation)

It is recommended that an experienced HPOM administrator complete the procedure for enabling the agent implementation of the HP NNMi–HPOM integration.

When NNMi integrates with the HP Business Service Management (BSM) topology database, the agent implementation of the HP NNMi–HPOM integration can associate incidents regarding NNMi-managed devices with BSM configuration items (CIs). This information is not available with the standard NNMi northbound interface. For more information, see Configuration Item Identifiers on page 584.

To enable agent implementation of the HP NNMi–HPOM integration, follow these steps:

1 On the NNMi management server, generate an SNMP trap policy file:

  a Verify that the NNMi services are running:

```
ovstatus -c
```

  All NNMi services should show the state RUNNING.

  b Generate the SNMP trap policy file by entering the following command:

```
nnmopcexport.ovpl -u <username> -p <password> \
-template "NNMi Management Events" -application "NNMi" \
-file NNMi_policy.dat
```

  The values for ***<username>*** and ***<password>*** correspond to an NNMi console user with the Administrator role.

  If HPOM will forward the NNMi incidents to the HP OMi event browser or to the BSM Operations Management event browser, also use the `-omi_hi` option to add health indicators to the management event policy conditions. For more information, see Health Indicators on page 584.

  The SNMP trap policy file includes a policy condition for each management event and SNMP trap configuration in the current NNMi incident configuration. For information about customizing the output of this command, see the *nnmopcexport.ovpl* reference page, or the UNIX manpage.

  For information about the default policy conditions and customizing conditions, see Using the HP NNMi–HPOM Integration (Agent Implementation) on page 584.

2 On the HPOM management server, configure HPOM to receive messages from NNMi:

  a In the HPOM console, add a node for the NNMi management server.

  b Install the HP Operations agent on the NNMi management server.

  c Transfer the `NNMi_policy.dat` file created in step 1 of this procedure from the NNMi management server to the HPOM management server.

  d Import the `NNMi_policy.dat` file into HPOM.

  — *HPOM for Windows*: Use the `ImportPolicies` command.

  — *HPOM for UNIX* version 9.x: Use the `opcpolicy` command.

  — *HPOM for UNIX* version 8.x: Use the `opctempl` command.

  — *HPOM for Linux*: Use the `opcpolicy` command.

  e Deploy the `NNMi Management Events` policy to the NNMi managed node.

  f In the HPOM console, add an external node to catch all forwarded NNMi incidents.

  For initial testing, set the node filter to `<*>.<*>.<*>.<*>` (for an IP filter) or `<*>` (for a name filter). After you validate the integration, restrict the external node filter to match your network.

  If you do not set up an HPOM managed node for an NNMi incident source node, the HPOM management server discards all incidents regarding that node.

For more information, see the following references:

- *HPOM for Windows*:
  - *Import OVO for UNIX templates* in the HPOM help
  - *Configuring external nodes* in the HPOM help
- *HPOM for UNIX*:
  - *HP Operations Manager for UNIX HTTPS Agent Concepts and Configuration Guide*
  - *HP Operations Manager for UNIX Concepts Guide*
  - *HP Operations Manager for UNIX Administrator's Reference*
  - *HP Operations Manager for UNIX Developer's Toolkit Developer's Reference*
  - *opcnode(1M)*, *opcbbcdist(1M)*, *opcragt(1M)*, *opccfgupl(1M)*, *opcpolicy(1M)* (version 9.xx), and *opctempl(1M)* (version 8.3x) manpages
- *HPOM for Linux*:
  - *HP Operations Manager for Linux HTTPS Agent Concepts and Configuration Guide*
  - *HP Operations Manager for Linux Concepts Guide*
  - *HP Operations Manager for Linux Administrator's Reference*
  - *HP Operations Manager for Linux Developer's Toolkit Developer's Reference*
  - *opcnode(1M)*, *opcbbcdist(1M)*, *opcragt(1M)*, *opccfgupl(1M)*, and *opcpolicy(1M)* manpages

3 Identify an available port for SNMP communications between NNMi and the HP Operations agent.

The HP Operations agent will listen on this port for the SNMP traps that NNMi forwards to this port. While enabling the integration, this port number is used in both step 4 (for the HP Operations agent) and step 5 (for NNMi) of this procedure.

Because the HP Operations agent is installed on the NNMi management server, this port number must be different from the port on which NNMi receives SNMP traps.

a In the NNMi console, open the **Communication Configuration** form from the **Configuration** workspace.

b In the **Default SNMP Settings** area, notice the value of the **SNMP Port**.

c Select a port that is different from the value on the **Communication Configuration** form. A good practice is to use a port number similar to 162, which is the standard UDP port for receiving SNMP traps. For example, if port 162 is not available, try port 5162.

d On the NNMi management server, run the command **`netstat -a`**, and then search the output for the port you selected in step c. If that port number does not appear in the output, it is probably available for the HP Operations agent to use.

4 On the NNMi management server, configure the HP Operations agent with a custom port for receiving SNMP traps from NNMi by entering the following commands:

- *Windows* NNMi management server:
  - Configure the agent:

    ```
    ovconfchg -ns eaagt -set SNMP_TRAP_PORT <custom_port> \
    -set SNMP_SESSION_MODE NNM_LIBS
    ```

  - Restart the agent:

    ```
    ovc -restart opctrapi
    ```

- *UNIX* NNMi management server:
  - Configure the agent:

    ```
    ovconfchg -ns eaagt -set SNMP_TRAP_PORT <custom_port> \
    -set SNMP_SESSION_MODE NO_TRAPD
    ```

  - Restart the agent:

    ```
    ovc -restart opctrapi
    ```

For *<custom_port>*, use the port that you identified in step 3 of this procedure.

5 On the NNMi management server, configure NNMi incident forwarding to the HP Operations agent:

a In the NNMi console, open the **HP NNMi–HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).

b Click **HPOM agent implementation**, and then click **New**.

(If you have selected an available destination, click **Reset** to make the **New** button available.)

c On the **HP NNMi–HPOM Agent Destination** form, select the **Enabled** check box to make the remaining fields on the form available.

d Enter the information for connecting to the HP Operations agent on the NNMi management server. The trap destination port is the port that you identified in step 3 of this procedure.

For information about these fields, see HP Operations Agent Connection on page 591.

e Specify the sending options. Select the **HTTP** option for the **NNMi Console Access** field.

For information about these fields, see HPOM Integration Content on page 592.

f Click **Submit** at the bottom of the form.

A new window opens a status message. If the message indicates a problem with the settings, click **Return**, and then adjust the values as suggested by the text of the error message.

6 *Optional*. In HPOM, add the custom message attributes for NNMi incidents to the active messages browser. Follow the appropriate steps:

- *HPOM for Windows*:
  - In the browser, right-click any column heading, and then click **Options**.
  - In the **Enter Custom Message Attributes** list, select an attribute, and then click **Add**.
- *HPOM for UNIX* or *HPOM for Linux*:
  - In the Java GUI Message Browser, right-click any column heading, and then click **Customize Message Browser Columns**.
  - On the **Custom** tab, select from the **Available Custom Message Attributes**, and then click **OK**.

Note the following information:

- Most of the custom message attributes for NNMi incidents begin with the text `nnm`.
- For the agent implementation of the HP NNMi–HPOM integration, some interesting attributes for NNMi incidents are as follows:

  ```
  nnm.name
  nnm.server.name
  ```

  For information about other interesting CMAs, see Using the HP NNMi–HPOM Integration (Agent Implementation) on page 584.
- To change the order in which the custom message attributes appear in the messages browser, drag a column heading to the new location.

7 *Optional*. On the HPOM management server, enable contextual launching of the NNMi views.

- *HPOM for Windows*: Associate the NNMi source nodes with the HP NNMi Web Tools group.

  For information, see *Enable tools in the By Node tool group* in the HPOM help.
- *HPOM for UNIX*: Install the basic set of NNMi applications, and optionally install additional NNMi applications.

  HPOM version 9.00 or higher automatically installs the basic NNMi applications.

  For information, see the section on installing and configuring the HP NNMi–HPOM integration in the *HP Operations Manager for UNIX Administrator's Reference* (version 9.xx) or the *HP NNMi–HPOM Integration for HP Operations Manager User's Guide* (version 8.3x).
- *HPOM for Linux*: HPOM automatically installs the basic NNMi applications. Optionally install additional NNMi applications.

  For information, see the section on installing and configuring the HP NNMi–HPOM integration in the *HP Operations Manager for Linux Administrator's Reference*.

Using the HP NNMi–HPOM Integration (Agent Implementation)

The agent implementation of the HP NNMi–HPOM integration provides a one-way flow of NNMi management events and SNMP traps to the HP Operations agent. The SNMP trap policy conditions determine how HPOM treats and opens the incoming traps. For example, you can change a policy condition to include the value of a trap custom message attribute (CMA) in the message text.

➤ NNMi sends only one copy of each management event or SNMP trap to the HP Operations agent. This behavior is different from that of the NNM 6.x/7.x integration with HPOM.

View the forwarded NNMi incidents in the HPOM active messages browser. HPOM menu commands provide access to NNMi views in the context of the selected message. Information embedded in each message supports this cross-navigation:

- The `nnmi.server.name` and `nnmi.server.port` CMAs in the message identify the NNMi management server.
- The `nnmi.incident.uuid` CMA identifies the incident in the NNMi database.

The original source object appears in the **Object** column of the HPOM active messages browser and in the `nnm.source.name` CMA. (In the web services implementation of the HP NNMi–HPOM integration, the original source object is only available in `nnm.source.name` CMA.)

Configuration Item Identifiers

In HP Business Service Management (BSM) and HP Universal CMDB Software (UCMDB), a configuration item (CI) is a database representation of a component in the IT environment. A CI can be a line of business, business process, application, server hardware, or a service.

When NNMi integrates with the BSM topology database or UCMDB, NNMi shares CI information with BSM or UCMDB for the devices that NNMi manages. In this case, the agent implementation of the HP NNMi–HPOM integration can associate incidents regarding NNMi-managed devices with BSM or UCMDB CIs. The SNMP trap policy conditions enable this association.

For information about the integrations with BSM and UCMDB, see:

- HP Business Service Management Topology on page 457
- HP Universal CMDB on page 467

Health Indicators

If the NNMi SNMP trap policy file was created with the `-omi_hi` option to `nnmopcexport.ovpl`, the policy file associates a health indicator with each standard NNMi management event in the SNMP trap policy file, as appropriate. (Not all management event types have health indicators.) The health indicator is available in the `EtiHint` CMA.

For the specific health indicators, see the SNMP trap policy file.

Default Policy Conditions

The default integration behavior varies with the integration content, as described here:

- NNMi management event incidents
  - The NNMi SNMP trap policy file includes conditions for all NNMi management event configurations defined in the NNMi incident configuration when the file was generated.
  - The messages created from NNMi management events appear in the HPOM active messages browser.
  - These traps include the CI information described in Configuration Item Identifiers on page 584.
  - The messages created from these traps might include health indicators described in Health Indicators on page 584.
- Third-party SNMP traps
  - The NNMi SNMP trap policy file includes conditions for all SNMP trap configurations defined in the NNMi incident configuration when the file was generated.
  - The messages created from third-party traps appear in the HPOM active messages browser.
  - These traps include the CI information described in Configuration Item Identifiers on page 584.
  - The messages created from these traps do not include health indicators.
  - If you configure the integration to forward all received SNMP traps and the HPOM management server receives SNMP traps directly from devices that NNMi manages, HPOM receives duplicate device traps. You can set the policies to correlate SNMP traps from NNMi with those that HPOM receives directly from managed devices.
- EventLifecycleStateClosed traps
  - The HP Operations agent logs the messages created from these traps. Generally, they do not appear in the HPOM active messages browser.
  - The NNMi SNMP trap policy file causes the HP Operations agent to acknowledge the message that corresponds to the closed NNMi incident in the HPOM active messages browser.
- LifecycleStateChangeEvent traps
  - The NNMi SNMP trap policy file does not include conditions for processing these traps. The HP Operations agent does not forward these traps to the HPOM active messages browser.
- EventDeleted traps
  - The NNMi SNMP trap policy file does not include conditions for processing these traps. The HP Operations agent does not forward these traps to the HPOM active messages browser.

- Correlation notification traps
  - The HP Operations agent logs the messages created from these traps. They do not appear in the HPOM active messages browser.
  - These traps have no impact on the HPOM active messages browser.

Customizing Policy Conditions

To customize the default policy conditions, edit the conditions on the HPOM management server, and then re-deploy the policy to the HP Operations agent on the NNMi management server. For more information, see the following reference:

- *HPOM for Windows*: *SNMP Interceptor Policies* (version 9.0x) or *Policy development* (version 8.1x) in the HPOM help
- *HPOM for UNIX*: *HP Operations Manager for UNIX Concepts Guide*
- *HPOM for Linux*: *HP Operations Manager for Linux Concepts Guide*

More Information

For more information about the agent implementation of the HP NNMi–HPOM integration, see the following references:

- For descriptions of the trap types that the integration sends to the HP Operations agent, see Using the NNMi Northbound Interface on page 546.
- For information about the format of the traps that NNMi sends to the HP Operations agent, see the `hp-nnmi-nbi.mib` file.
- For detailed information about using the HP NNMi–HPOM integration, see the HPOM documentation.
  - *HPOM for Windows*: See *Agent implementation of the NNMi Adapter* in the HPOM help.
  - *HPOM for UNIX*: See the section on installing and configuring the HP NNMi–HPOM integration in the *HP Operations Manager for UNIX Administrator's Reference* (version 9.xx) or the *HP NNMi–HPOM Integration for HP Operations Manager User's Guide* (version 8.3x).
  - *HPOM for Linux*: See the section on installing and configuring the HP NNMi–HPOM integration in the *HP Operations Manager for Linux Administrator's Reference*.

Changing the HP NNMi–HPOM Integration Configuration (Agent Implementation)

Update the SNMP Trap Policy Conditions for New NNMi Traps

If new SNMP trap incident configurations have been added to NNMi since the integration was configured, follow these steps:

1. On the NNMi management server, use the `nnmopcexport.ovpl` command to create an SNMP trap policy file for the new traps.

   For the `-template` option, specify a name that is different from the names of the existing SNMP trap policy files.

You can limit the file contents to a specific author or OID prefix value. For more information, see the *nnmopcexport.ovpl* reference page, or the UNIX manpage.

2. Transfer the new SNMP trap policy file from the NNMi management server to the HPOM management server, and then import it into HPOM.
3. On the HPOM management server, deploy the new policy to the NNMi managed node.

Alternatively, you can re-create the SNMP trap policy file for all NNMi management events and SNMP traps. If you take this approach, importing the new policy file into HPOM overwrites any existing policy customizations.

Change the Configuration Parameters

To change the integration configuration parameters, follow these steps:

1. In the NNMi console, open the **HP NNMi–HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).
2. Click **HPOM agent implementation**.
3. Select a destination, and then click **Edit**.
4. Modify the values as appropriate.

   For information about the fields on this form, see HP NNMi–HPOM Agent Destination Form Reference (Agent Implementation) on page 591.
5. Verify that the **Enable Integration** check box at the top of the form is selected, and then click **Submit** at the bottom of the form.

   The changes take effect immediately.

Disabling the HP NNMi–HPOM Integration (Agent Implementation)

No SNMP trap queuing occurs while a destination is disabled.

To discontinue the forwarding of NNMi incidents to the HP Operations agent, follow these steps:

1. In the NNMi console, open the **HP NNMi–HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).
2. Click **HPOM agent implementation**.
3. Select a destination, and then click **Edit**.

   Alternatively, click **Delete** to entirely remove the configuration for the selected destination.
4. Clear the **Enable Integration** check box at the top of the form, and then click **Submit** at the bottom of the form.

   The changes take effect immediately.

Optionally, deactivate or delete the SNMP trap policy as described in the HPOM documentation.

Troubleshooting the HP NNMi–HPOM Integration (Agent Implementation)

HPOM Active Messages Browser Does Not Receive Any Forwarded Incidents

In the following procedure, the `OVBIN` environment variable refers to the `bin` directory for the HP Operations agent commands, which defaults to the following value:

- *Windows*: `<drive>\Program Files\HP\HP BTO Software\bin`
- *UNIX*: `/opt/OV/bin`

If the HPOM active messages browser does not contain any incidents from NNMi, follow these steps:

1. On the NNMi management server, verify the HP Operations agent configuration:
   - *Windows* NNMi management server:

     `%OVBIN%\ovconfget eaagt`
   - *UNIX* NNMi management server:

     `$OVBIN/ovconfget eaagt`

   The command output should include the following information:
   - *Windows*: `SNMP_SESSION_MODE=NNM_LIBS`
   - *UNIX*: `SNMP_SESSION_MODE=NO_TRAPD`
   - `SNMP_TRAP_PORT=<custom_port>`

     The value of `<custom_port>` should *not* be 162 and should match the value of the **Port** field on the **HP NNMi–HPOM Agent Destination** form.
2. Evaluate the HP Operations agent configuration by considering the results from step 1:
   - If the HP Operations agent configuration is as expected, continue with step 3 of this procedure.
   - If the `SNMP_SESSION_MODE` parameter is not set correctly, repeat step 4 on page 582 until the `ovconfget` command returns the expected results.
   - If the value of `<custom_port>` is 162 or does not match the value of the **Port** field on the **HP NNMi–HPOM Agent Destination** form, repeat step 3 on page 581 through step 5 on page 582, as appropriate, until the `ovconfget` command returns the expected results.
3. On the NNMi management server, verify that the HP Operations agent is running:
   - *Windows* NNMi management server:

     `%OVBIN%\opcagt -status`
   - *UNIX* NNMi management server:

     `$OVBIN/opcagt -status`

   The command output should include an opctrapi entry similar to the following example:

   ```
   opctrapi  OVO SNMP Trap Interceptor  AGENT,EA  (4971)  Running
   ```

If the output is not as expected, restart the HP Operations agent:

```
ovc -restart opctrapi
```

4. On the NNMi management server, verify that the HP Operations agent is listening on the expected SNMP trap port:

   a. Run the following command:

      — *Windows*: **`netstat -an | findstr <custom_port>`**

      — *UNIX*: **`netstat -an | grep <custom_port>`**

      Where *`<custom_port>`* is the value of `SNMP_TRAP_PORT` from step 1 of this procedure.

   b. Verify that the output includes the state LISTENING or LISTEN.

      If the output is not as expected, restart the HP Operations agent:

      ```
      ovc -restart opctrapi
      ```

5. On the HPOM management server, verify the external node filter for the NNMi management server node.

   The HPOM management server must be configured to accept incidents from the devices that NNMi manages. HPOM ignores any forwarded incident from an NNMi source node that is not configured as a managed node or included in an external node filter, as described in step 2 on page 580.

6. On the NNMi management server, verify that the SNMP trap policy file for NNMi has been deployed to the HP Operations agent on the NNMi management server:

   - *Windows* NNMi management server:

     ```
     %OVBIN%\ovpolicy -list
     ```

   - *UNIX* NNMi management server:

     ```
     $OVBIN/ovpolicy -list
     ```

   The command output should include an entry similar to the following example:

   ```
   Type     Name                          Status     Version
   ----------------------------------------------------------------
   trapi    "NNMi Management Events"      enabled    0001.0000
   ```

   The value of the `Name` field is the name of the SNMP trap policy file from the `-template` option to `nnmopcexport.ovpl` in step 1 on page 580.

7. Verify that the HP Operations agent is receiving traps:

   a. Verify that the HP Operations agent can send messages to the HPOM management server.

   b. Enable tracing of the HP Operations agent to determine whether the traps arrive at the HP Operations agent.

   For information about troubleshooting the HP Operations agent, see the following reference:

   - *HPOM for Windows*: HPOM help
   - *HPOM for UNIX*: *HP Operations Manager for UNIX HTTPS Agent Concepts and Configuration Guide*
   - *HPOM for Linux*: *HP Operations Manager for Linux HTTPS Agent Concepts and Configuration Guide*

8 Verify that NNMi is forwarding management events to the HP Operations agent.

For information, see Troubleshooting the NNMi Northbound Interface on page 550.

HPOM Active Messages Browser Does Not Receive Some Forwarded Incidents

If one or more NNMi incidents do not appear in the HPOM active messages browser, follow these steps:

1 On the NNMi management server, verify that the SNMP trap policy does not suppress the trap.

2 On the HPOM management server, verify the external node filter for the NNMi management server node.

The HPOM management server must be configured to accept incidents from the devices that NNMi manages. HPOM ignores any forwarded incident from an NNMi source node that is not configured as a managed node or included in an external node filter, as described in step 2 on page 580.

3 On the HPOM management server, verify that HPOM is running.

If the HPOM management server shuts down, the HP Operations agent queues received traps. The HP Operations agent forwards the queued traps when the HPOM management server becomes available.

If the HP Operations agent shuts down, the forwarded traps are lost. NNMi does not resend traps.

4 On the NNMi management server, verify that the NNMi processes are running:

```
ovstatus -c
```

Any traps sent to NNMi while it is shut down are lost.

HP NNMi–HPOM Agent Destination Form Reference (Agent Implementation)

The **HP NNMi–HPOM Agent Destination** form contains the parameters for configuring communications between NNMi and the HP Operations agent. This form is available from the **Integration Module Configuration** workspace. (On the **HP NNMi–HPOM Integration Selection** form, click **HPOM agent implementation**. Click **New**, or select a destination, and then click **Edit**.)

Only NNMi users with the Administrator role can access the **HP NNMi–HPOM Agent Destination** form.

The **HP NNMi–HPOM Agent Destination** form collects information for the following areas:

- HP Operations Agent Connection on page 591
- HPOM Integration Content on page 592
- HP Operations Agent Destination Status Information on page 594

To apply changes to the integration configuration, update the values on the **HP NNMi–HPOM Agent Destination** form, and then click **Submit**.

HP Operations Agent Connection

Table 63 lists the parameters for configuring the connection to the HP Operations agent.

Table 63 HP Operations Agent Connection Information

Field	Description
Host	The fully-qualified domain name (preferred) or the IP address of the NNMi management server, which is the system on which the HP Operations agent receives SNMP traps from NNMi. The integration supports the following methods for identifying the HP Operations agent host: • **NNMi FQDN** NNMi manages the connection to the HP Operations agent on the NNMi management server and the **Host** field becomes read-only. This is the default and recommended configuration. • **Use Loopback** Do not use this option. • **Other** Do not use this option. **NOTE:** If the NNMi management server participates in NNMi application failover, see Application Failover and the NNMi Northbound Interface on page 551 for information about the impact of application failover on the integration module.

Table 63 HP Operations Agent Connection Information (cont'd)

Field	Description
Port	The UDP port where the HP Operations agent receives SNMP traps. Enter the port number specific to the HP Operations agent. This value is the port that you identified in step 3 on page 581. To determine the port, run the **`ovconfget eaagt`** command on the NNMi management server. The trap port is the value of the `SNMP_TRAP_PORT` variable. **NOTE:** This port number must be different from the port on which NNMi receives SNMP traps, as set in the **SNMP Port** field on the **Communication Configuration** form in the NNMi console.
Community String	A read-only community string for the HP Operations agent to receive traps. For the HP NNMi—HPOM integration, use the default value, which is `public`.

HPOM Integration Content

Table 64 lists the parameters for configuring which content NNMi sends to the HP Operations agent.

Table 64 HPOM Integration Content Configuration Information

Field	Description
Incidents	The incident forwarding specification. • **Management** NNMi forwards only NNMi-generated management events to the HP Operations agent. • **SNMP 3rd Party Trap** NNMi forwards only SNMP traps that NNMi receives from managed devices to the HP Operations agent. • **Both** NNMi forwards to the HP Operations agent both NNMi-generated management events and SNMP traps that NNMi receives from managed devices. This is the default configuration. NNMi begins forwarding incidents as soon as you enable the destination. For more information, see Incident Forwarding on page 546.

Table 64 HPOM Integration Content Configuration Information (cont'd)

Field	Description
Lifecycle State Changes	The incident change notification specification. • **Enhanced Closed** NNMi sends an incident closed trap to the HP Operations agent for each incident that changes to the CLOSED lifecycle state. This is the default configuration. • **State Changed** NNMi sends an incident lifecycle state changed trap to the HP Operations agent for each incident that changes to the IN PROGRESS, COMPLETED, or CLOSED lifecycle state. • **Both** NNMi sends an incident closed trap to the HP Operations agent for each incident that changes to the CLOSED lifecycle state. Additionally, the integration sends an incident lifecycle state changed trap to the HP Operations agent for each incident that changes to the IN PROGESS, COMPLETED, or CLOSED lifecycle state. **NOTE:** In this case, each time an incident changes to the CLOSED lifecycle state, the integration sends two notification traps: an incident closed trap and an incident lifecycle state changed trap. For more information, see Incident Lifecycle State Change Notifications on page 547.
Correlations	The incident correlation notification specification. • **None** NNMi does not notify the HP Operations agent of incident correlations resulting from NNMi causal analysis. This is the default configuration. • **Single** NNMi sends a trap for each parent-child incident correlation relationship resulting from NNMi causal analysis. • **Group** NNMi sends one trap per correlation that lists all child incidents correlated to a parent incident. For more information, see Incident Correlation Notifications on page 547.
Deletions	The incident deletion specification. • **Don't Send** NNMi does not notify the HP Operations agent when incidents are deleted in NNMi. This is the default configuration. • **Send** NNMi sends a deletion trap to the HP Operations agent for each incident that is deleted in NNMi. For more information, see Incident Deletion Notifications on page 548.
NNMi Console Access	The connection protocol specification in the URL for browsing to the NNMi console from the HPOM message browser. The traps that NNMi sends to the HP Operations agent include the NNMi URL in the NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2). The integration requires an HTTP connection to the NNMi console. Select the **HTTP** option.

Table 64 HPOM Integration Content Configuration Information (cont'd)

Field	Description
Incident Filters	A list of object identifiers (OIDs) on which the integration filters the events sent to the HP Operations agent. Each filter entry can be a valid numeric OID (for example, .1.3.6.1.6.3.1.1.5.4.1.3.6.1.4.1.9) or OID prefix (for example, .1.3.6.1.6.3.1.1.5.*). Select one of the following options: • **None** NNMi sends all events to the HP Operations agent. This is the default configuration. • **Include** NNMi sends only the specific events that match the OIDs identified in the filter. • **Exclude** NNMi sends all events except for the specific events that match the OIDs identified in the filter. Specify the incident filter: • To add a filter entry, enter the text in the lower text box, and then click **Add**. • To delete a filter entry, select that entry from the list in the upper box, and then click **Remove**. For more information, see Event Forwarding Filter on page 548.

HP Operations Agent Destination Status Information

Table 65 lists the read-only status information for the HP Operations agent. This information is useful for verifying that the integration is working correctly.

Table 65 HP Operations Agent Destination Status Information

Field	Description
Trap Destination IP Address	The IP address to which the HP Operations agent destination host name resolves. This value is unique to this HP Operations agent destination.
Uptime (seconds)	The time (in seconds) since the northbound component was last started. The traps that NNMi sends to the HP Operations agent include this value in the sysUptime field (1.3.6.1.2.1.1.3.0). This value is the same for all integrations that use the NNMi northbound interface. To see the latest value, either refresh or close and re-open the form.
NNMi URL	The URL for connecting to the NNMi console. The traps that NNMi sends to the HP Operations agent include this value in the NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2). This value is unique to this northbound destination.

HP NNMi—HPOM Integration (Web Services Implementation)

The agent implementation of the HP NNMi—HPOM integration is the preferred solution for integrating HPOM with NNMi.

If the agent and the web services implementations of the HP NNMi—HPOM integration both forward messages to the same HPOM management server, you might not see all messages from both implementations in the HPOM active messages browser. For this reason, HP does not support running both implementations of the HP NNMi—HPOM integration from one NNMi management server to the same HPOM management server concurrently.

This section contains the following topics:

About the HP NNMi–HPOM Integration (Web Services Implementation)

The web services implementation of the HP NNMi–HPOM integration forwards NNMi incidents to the HPOM active messages browser. The integration synchronizes incidents between NNMi and HPOM. It also provides for accessing the NNMi console from within HPOM.

The HP NNMi–HPOM integration supports a “many-to-many” arrangement. Each NNMi management server can forward incidents to multiple HPOM management servers. Likewise, each HPOM management server can receive incidents from multiple NNMi management servers. The integration interprets the unique identifier of an incident to determine the source NNMi management server.

The HP NNMi–HPOM integration consists of the following components:

- **HP NNMi–HPOM Integration Module**

  The HP NNMi–HPOM integration module forwards incidents from NNMi to HPOM. It is installed and configured on the NNMi management server.

- **HP Operations Manager Incident Web Service**

  HPOM uses the HP Operations Manager Incident Web Service (IWS) to receive the incidents that are forwarded from NNMi.

- **HPOM applications for contextual access of the NNMi console**

  HPOM provides applications for accessing forms, views, and tools in the NNMi console. For example, you can open an NNMi incident directly from the HPOM active messages browser. The specific application determines the context in which the NNMi console opens. Configure the applications before you can use them.

Value

The HP NNMi–HPOM integration provides event consolidation in the HPOM active messages browser for the network management, system management, and application management domains, so that HPOM users can detect and investigate potential network problems.

The primary features of the integration are as follows:

- Automatic incident forwarding from NNMi to HPOM.
  - Forwarded incidents appear in the HPOM active messages browser.
  - You can create filters that limit which incidents NNMi forwards.
- Synchronization of Incident updates between NNMi and HPOM as described in the following table.

Trigger	Result
In HPOM, the message is acknowledged.	In NNMi, the corresponding incident's lifecycle state is set to Closed.
In HPOM, the message is unacknowledged.	In NNMi, the corresponding incident's lifecycle state is set to Registered.
In NNMi, the incident's lifecycle state is set to Closed.	In HPOM, the corresponding message is acknowledged.
In NNMi, the incident's lifecycle state is changed from Closed to any other state.	In HPOM, the corresponding message is unacknowledged.

- Access to the NNMi console from HPOM.
  - HPOM users can open the NNMi **Incident** form in the context of a selected message.
  - HPOM users can launch an NNMi view (for example, the Layer 2 Neighbor view) in the context of a selected message and node.
  - HPOM users can launch an NNMi tool (for example, status poll) in the context of a selected message and node.
  - When HPOM is consolidating NNMi incidents from multiple NNMi management servers, the integration interprets the unique identifier of each incident to access the correct NNMi management server.

Integrated Products

The information in this section applies to the following products:

- HPOM for Windows (also called OMW)
- HPOM for UNIX (also called OMU)
- HPOM for Linux (also called OML)

For the list of supported versions, see the *NNMi System and Device Support Matrix*.

- NNMi 9.10

NNMi and HPOM must be installed on separate computers. The NNMi management server and the HPOM management server computer can be of the same or different operating systems.

For the most recent information about supported hardware platforms and operating systems, see the support matrices for both products.

Documentation

This chapter describes how to configure NNMi to communicate with HPOM.

The HPOM documentation describes how to configure HPOM to communicate with NNMi. It also describes how to use the HP NNMi–HPOM integration.

- For HPOM for Windows, see the information for the HP NNMi Adapter in the HPOM help.
- For HPOM for UNIX version 9.xx, see the *Integrating NNMi into HPOM* section in the *HP Operations Manager for UNIX Administrator's Reference*.
- For HPOM for UNIX version 8.3x, see the *HP NNMi–HPOM Integration for HP Operations Manager User's Guide*.
- For HPOM for Linux, see the *Integrating NNMi into HPOM* section in the *HP Operations Manager for Linux Administrator's Reference*.

Enabling the HP NNMi–HPOM Integration (Web Services Implementation)

This section describes the procedure for enabling the HP NNMi–HPOM integration. For each NNMi management server and each HPOM management server that you want to include in the integration, complete the appropriate steps in the procedure for the version of HPOM that you are using.

HPOM for Windows

1 On the NNMi management server, configure NNMi incident forwarding to HPOM:

   a In the NNMi console, open the **HP NNMi–HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).

   b Click **web services implementation**.

   c On the **HP NNMi–HPOM Web Services Integration Configuration** form, select the **Enable Integration** check box to make the remaining fields on the form available.

d Enter the information for connecting to the NNMi management server.

The integration requires an HTTP connection to the NNMi console. Leave the **NNMi SSL Enabled** check box cleared.

For information about these fields, see NNMi Management Server Connection on page 608.

e Enter the information for connecting to the HPOM management server.

For information about these fields, see HPOM Management Server Connection on page 609.

f Enter values for the following fields:

— **Forward Only**

— **Holding period (minutes)**

— **Incident Filter**

For information about these fields, see Integration Behavior on page 610.

g If you want NNMi to forward incidents to multiple HPOM management servers, click **Add another HPOM server**, and then enter the information for the next HPOM management server in the HPOM fields.

The information for the first server appears in the **Additional HPOM Servers** list.

h Click **Submit** at the bottom of the form.

A new window opens a status message. If the message indicates a problem with connecting to the HPOM server, re-open the **HP NNMi–HPOM Web Services Integration Configuration** form (or press **ALT+LEFT ARROW** in the message window), and then adjust the values for connecting to the HPOM management server as suggested by the text of the error message.

2 In HPOM, configure the NNMi adapter for connecting to the NNMi management server as described in *Configure the NNMi Server Name and Port* of the HPOM help.

3 In HPOM, add a managed node for each NNMi node that will be named as a source node in the NNMi incidents that are forwarded to this HPOM management server. Also add a managed node for each NNMi management server that will forward incidents to this HPOM management server.

Alternatively, you can create one external node to catch all forwarded NNMi incidents. For initial testing, set the node filter to `<*>.<*>.<*>.<*>` (for an IP filter) or `<*>` (for a name filter). After you validate the integration, restrict the external node filter to match your network.

For more information, see *Configuring NNMi Server Nodes* in the HPOM help.

If you do not set up an HPOM managed node for an NNMi incident source node, the HPOM management server discards all incidents regarding that node.

4. *Optional*. In HPOM, add the custom message attributes for NNMi incidents to the active messages browser:
   a. In the browser, right-click any column heading, and then click **Options**.
   b. In the **Enter Custom Message Attributes** list, select an attribute, and then click **Add**.
      — The custom message attributes for NNMi incidents begin with the text `nnm`.
      — For the web services implementation of the HP NNMi–HPOM integration, the most interesting attributes for NNMi incidents are as follows:

```
nnm.assignedTo
nnm.category
nnm.emittingNode.name
nnm.source.name
```

      — To change the order in which the custom message attributes appear in the messages browser, drag a column heading to the new location.
5. *Optional*. In HPOM, enable contextual launching of the NNMi views by associating the NNMi source nodes with the HP NNMi Web Tools group.

   For more information, see *Enable tools in the By Node tool group* in the HPOM help.

HPOM for UNIX and HPOM for Linux

1. *HPOM for UNIX version 8.3x only.* Prepare the HPOM for UNIX management server:
   a. On the HPOM for UNIX management server, install the HP Operations Manager Incident Web Service (IWS) as described in the *HP Operations Manager Incident Web Service Integration Guide*.
   b. On the HPOM for UNIX management server, install the most recent HPOM consolidated patch, which is available at:

      http://h20230.www2.hp.com/selfsolve/patches
2. On the NNMi management server, configure NNMi incident forwarding to HPOM:
   a. In the NNMi console, open the **HP NNMi–HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).
   b. Click **web services implementation**.
   c. On the **HP NNMi–HPOM Web Services Integration Configuration** form, select the **Enable Integration** check box to make the remaining fields on the form available.
   d. Enter the information for connecting to the NNMi management server.

      ➤ The integration requires an HTTP connection to the NNMi console. Leave the **NNMi SSL Enabled** check box cleared.

      For information about these fields, see NNMi Management Server Connection on page 608.
   e. Enter the information for connecting to the HPOM management server.

      For information about these fields, see HPOM Management Server Connection on page 609.

f Enter values for the following fields:

   - **Forward Only**
   - **Holding period (minutes)**
   - **Incident Filter**

   For information about these fields, see Integration Behavior on page 610.

g If you want NNMi to forward incidents to multiple HPOM management servers, click **Add another HPOM server**, and then enter the information for the next HPOM management server in the HPOM fields.

   The information for the first server appears in the **Additional HPOM Servers** list.

h Click **Submit** at the bottom of the form.

   A new window opens a status message. If the message indicates a problem with connecting to the HPOM server, re-open the **HP NNMi–HPOM Web Services Integration Configuration** form (or press **ALT+LEFT ARROW** in the message window), and then adjust the values for connecting to the HPOM management server as suggested by the text of the error message.

i Click **Submit** at the bottom of the form.

3 In HPOM, add a managed node for each NNMi node that will be named as a source node in the NNMi incidents that are forwarded to this HPOM management server. Also add a managed node for each NNMi management server that will forward incidents to this HPOM management server.

Alternatively, you can create one external node to catch all forwarded NNMi incidents. For initial testing, set the node filter to `<*>.<*>.<*>.<*>` (for an IP filter) or `<*>` (for a name filter). After you validate the integration, restrict the external node filter to match your network.

For more information, see the *HP Operations Manager for UNIX Administrator's Reference* or the *HP Operations Manager for Linux Administrator's Reference*.

⚠ If you do not set up an HPOM managed node for an NNMi incident source node, the HPOM management server discards all incidents regarding that node.

4 *Optional*. In HPOM, add the custom message attributes for NNMi incidents to the active messages browser:

a In the Java GUI Message Browser, right-click any column heading, and then click **Customize Message Browser Columns**.

b On the **Custom** tab, select from the **Available Custom Message Attributes**, and then click **OK**.

   - The custom message attributes for NNMi incidents begin with the text `nnm`.
   - For the web services implementation of the HP NNMi–HPOM integration, the most interesting attributes for NNMi incidents are as follows:

```
nnm.assignedTo
nnm.category
nnm.emittingNode.name
nnm.source.name
```

   - To change the order in which the custom message attributes appear in the messages browser, drag a column heading to the new location.

5. *Optional*. On the HPOM management server, prepare the HPOM applications for accessing the NNMi console.

   a. *Required*. Install the basic set of NNMi applications.

      HPOM version 9.00 or higher automatically installs the basic NNMi applications.

   b. *Optional*. Install additional NNMi applications.

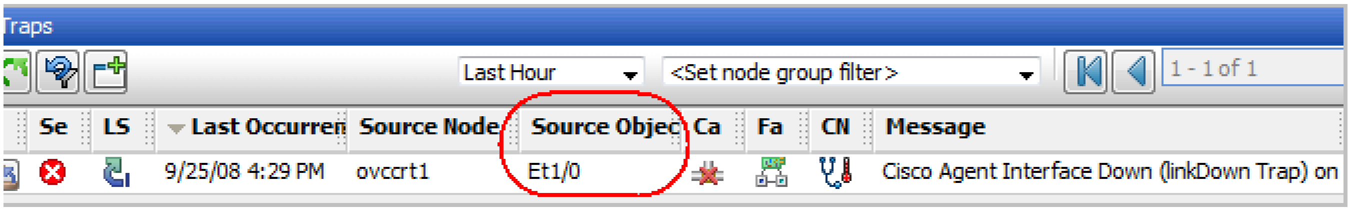
   For information, see the section on installing and configuring the HP NNMi–HPOM integration in the *HP Operations Manager for UNIX Administrator's Reference* (version 9.xx), the *HP NNMi–HPOM Integration for HP Operations Manager User's Guide* (version 8.3x), or the *HP Operations Manager for Linux Administrator's Reference*.

Using the HP NNMi–HPOM Integration (Web Services Implementation)

Usage Example

Figure 45 shows an interface down incident in the NNMi console. The information in the **Source Object** and **Message** columns together describe the situation.

Figure 45 Interface Down Incident in NNMi Console



raps

Last Hour

<Set node group filter>

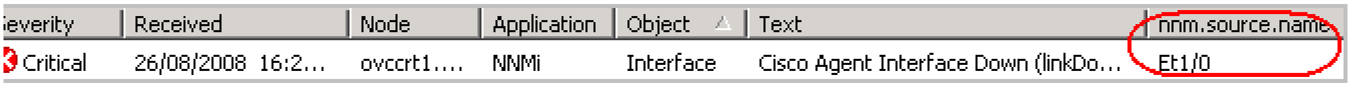
1 - 1 of 1

Se	LS	Last Occurren	Source Node	Source Objec	Ca	Fa	CN	Message
		9/25/08 4:29 PM	ovccrt1	Et1/0				Cisco Agent Interface Down (linkDown Trap) on

Figure 46 shows the NNMi incident as received by HPOM for Windows. Figure 47 shows the NNMi incident as received by HPOM for UNIX. The **nnm.source.name** and **Text** columns are equivalent to the **Source Object** and **Message** columns in the NNMi console.

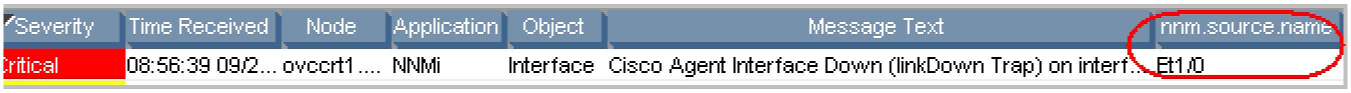
You must enable the display of the **nnm.source.name** custom message attribute column as described in step 4 on page 599 (for HPOM for Windows) and in step 4 on page 600 (for HPOM for UNIX and for HPOM for Linux).

Figure 46 Forwarded Incident in HPOM for Windows



ieverity	Received	Node	Application	Object	Text	nnm.source.name
Critical	26/08/2008 16:2...	ovccrt1....	NNMi	Interface	Cisco Agent Interface Down (linkDo...	Et1/0

Figure 47 Forwarded Incident in HPOM for UNIX



Severity	Time Received	Node	Application	Object	Message Text	nnm.source.name
ritical	08:56:39 09/2...	ovccrt1	NNMi	Interface	Cisco Agent Interface Down (linkDown Trap) on interf...	Et1/0

A Normal Situation: Unknown MSI Condition

The HPOM server receives forwarded NNMi incidents through MSI (not a regular trap policy). In the HPOM message browser, the format of the message source is **MSI** followed by the name of the MSI interface. The condition name corresponds to the `condition_id` field in the message, which is unset because there is no associated policy.

- *HPOM for Windows*: The policy type is empty.
- *HPOM for UNIX* or *HPOM for Linux*: The message source is of the format: **MSI: <*MSI_Interface*>: Unknown Condition**.

More Information

For detailed information about using the HP NNMi–HPOM integration, see the HPOM documentation.

- *HPOM for Windows*: See the topics about the HP NNMi adapter in the HPOM help.
- *HPOM for UNIX*: See the section on installing and configuring the HP NNMi–HPOM integration in the *HP Operations Manager for UNIX Administrator's Reference* (version 9.xx) or the *HP NNMi–HPOM Integration for HP Operations Manager User's Guide* (version 8.3x).
- *HPOM for Linux*: See the section on installing and configuring the HP NNMi–HPOM integration in the *HP Operations Manager for Linux Administrator's Reference*.

In the HPOM messages browser, the details for a forwarded NNMi incident are available as custom message attributes.

Changing the HP NNMi–HPOM Integration Configuration (Web Services Implementation)

1. In the NNMi console, open the **HP NNMi–HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).
2. Click **web services implementation**.
3. Modify the values as appropriate.
   - If you know the syntax of the entries in the Incident Filter and Additional HPOM Servers lists, you can modify the entries directly.
   - If you do not know the syntax for a list item, delete that entry and then re-enter it.

   For information about the fields on this form, see HP NNMi–HPOM Web Services Integration Configuration Form Reference on page 608.
4. Verify that the **Enable Integration** check box at the top of the form is selected, and then click **Submit** at the bottom of the form.

   The changes take effect immediately.

Disabling the HP NNMi–HPOM Integration (Web Services Implementation)

For All HPOM Management Servers

To discontinue the forwarding of NNMi incidents to all HPOM management servers, follow these steps:

1. In the NNMi console, open the **HP NNMi–HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).
2. Click **web services implementation**.
3. Clear the **Enable Integration** check box at the top of the form, and then click **Submit** at the bottom of the form.

   The changes take effect immediately.

If necessary, repeat this process for all NNMi management servers.

For One HPOM Management Server

To discontinue the forwarding of NNMi incidents to only one of the HPOM management servers, follow these steps:

1. In the NNMi console, open the **HP NNMi–HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).
2. Click **web services implementation**.
3. In the **Additional HPOM Servers** list, edit the text to delete the entry (or entries) for the HPOM management server to disconnect from the integration.

   Clicking **Clear** removes all HPOM servers from the list.

4. Click **Submit** at the bottom of the form.

   The changes take effect immediately.

Troubleshooting the HP NNMi–HPOM Integration (Web Services Implementation)

HPOM Does Not Receive Any Forwarded Incidents

If the integration has worked successfully in the past, it is possible that some aspect of the configuration, for example, the NNMi or HPOM user password, has changed recently. You might want to update the integration configuration as described in Changing the HP NNMi–HPOM Integration Configuration (Web Services Implementation) on page 602, before walking through this entire procedure.

1. In the NNMi console, open the **HP NNMi–HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).
2. Click **web services implementation**.

   For information about the fields on this form, see HP NNMi–HPOM Web Services Integration Configuration Form Reference on page 608.

3 Check the status of the integration, in the **HP NNMi–HPOM Web Services Integration Configuration** form, by clicking **Submit** at the bottom of the form (without making any configuration changes).

A new window opens a status message.

- If the message indicates success, the problem is most likely that HPOM is not configured to accept incidents from the devices that NNMi manages. HPOM ignores any forwarded incident from an NNMi source node that is not configured as a managed node in HPOM, as described in step 3 on page 598 (for HPOM for Windows) and in step 3 on page 600 (for HPOM for UNIX and for HPOM for Linux). Verify the HPOM configuration, and then test the integration as described in step 10 of this procedure.
- If the message indicates a problem with connecting to the HPOM server, NNMi and HPOM are not able to communicate. Continue with step 4 of this procedure.

4 Verify the accuracy and access level of the HPOM credentials by logging in to the HPOM console and displaying the HPOM active messages browser:

- *HPOM for Windows*: Log on to the computer as the **HPOM User** from the **HP NNMi–HPOM Web Services Integration Configuration** form, and then start the HPOM console.

  The user name is in the format `<Windows_domain>\<username>`.
- *HPOM for UNIX* or *HPOM for Linux*: Log on to the HPOM console with the credentials for the **HPOM User** from the **HP NNMi–HPOM Web Services Integration Configuration** form.

If you cannot log on to the HPOM console, contact the HPOM administrator to verify your logon credentials.

5 Verify that the connection to the HPOM management server is configured correctly:

a In a web browser, enter the following URL:

***<protocol>**://**<omserver>**:**<port>**/opr-webservice//Incident.svc?wsdl*

Where the variables are related to values on the **HP NNMi–HPOM Web Services Integration Configuration** form as follows:

— If the **HPOM SSL Enabled** check box is selected, *<protocol>* is `https`.

— If the **HPOM SSL Enabled** check box is cleared, *<protocol>* is `http`.

— *<omserver>* is the value of **HPOM Host**.

— *<port>* is the value of **HPOM Port**.

b When prompted, enter the credentials for the **HPOM User** from the **HP NNMi–HPOM Web Services Integration Configuration** form.

The resulting web page is an XML file that describes the IWS.

— If the XML file appears, the connection to the HPOM management server is configured correctly. Continue with step 6.

— If you see an error message, the connection to the HPOM management server is not configured correctly. Contact the HPOM administrator to verify the information you are using to connect to the HPOM web service. Continue to troubleshoot the connection to HPOM until you see the XML file.

6 Verify that the connection to NNMi is configured correctly:

If you used the information described in this step to connect to the NNMi console in step 1 of this procedure, you do not need to reconnect to the NNMi console. Continue with step 7.

a In a web browser, enter the following URL:

<protocol>://<NNMiserver>:<port>/nnm/

Where the variables are related to values on the **HP NNMi–HPOM Web Services Integration Configuration** form as follows:

- If the **NNMi SSL Enabled** check box is selected, *<protocol>* is `https`.

  If the **NNMi SSL Enabled** check box is selected, verify that the KeyManager process is running by entering the following command:

  ```
  ovstatus -v ovjboss
  ```

- If the **NNMi SSL Enabled** check box is cleared, *<protocol>* is `http`.
- *<NNMiserver>* is the value of **NNMi Host**.

  Use the fully-qualified domain name or the IP address of the NNMi management server. Do not use `localhost`.

- *<port>* is the value of **NNMi Port**.

  To verify the NNMi ports for HTTP or HTTPS, check the `nms-local.properties` file, as described in Table 66 on page 608.

b When prompted, enter the credentials for an NNMi user with the Administrator role.

You should see the NNMi console. If the NNMi console does not appear, contact the NNMi administrator to verify the information you are using to connect to NNMi. Continue to troubleshoot the connection to NNMi until the NNMi console appears.

You cannot log on to the NNMi console as a user with the Web Service Client role.

c Verify the values of the **NNMi User** and **NNMi Password**.

- If the **NNMi User** listed on the **HP NNMi–HPOM Web Services Integration Configuration** form has the Administrator role and you were able to connect to the NNMi console with this user name, then re-enter the corresponding password on the **HP NNMi–HPOM Web Services Integration Configuration** form.
- If the **NNMi User** listed on the **HP NNMi–HPOM Web Services Integration Configuration** form has the Web Service Client role, contact the NNMi administrator to verify the values of **NNMi User** and **NNMi Password**.

Passwords are hidden in the NNMi console. If you are not sure what password to specify for an NNMi user name, ask the NNMi administrator to reset the password.

7 Update the **HP NNMi–HPOM Web Services Integration Configuration** form with the values that you used for successful connections in step 5 and step 6 of this procedure.

For more information, see HP NNMi–HPOM Web Services Integration Configuration Form Reference on page 608.

8 Click **Submit** at the bottom of the form.

9 If the status message still indicates a problem with connecting to the HPOM server, do the following:

a Clear the web browser cache.

b Clear all saved form or password data from the web browser.

c Close the web browser window completely, and then re-open it.

d Repeat step 7 and step 8 of this procedure.

10 Test the configuration by generating an incident on the NNMi management server and determining whether it reaches the HPOM management server.

Alternatively, change the lifecycle state of an NNMi management event to OPEN. (If the lifecycle state is currently OPEN, change the lifecycle state to CLOSED and then back to OPEN.)

HPOM Does Not Receive Some Forwarded Incidents

Verify the HPOM nodes and the incident filter.

The HPOM management server must be configured to accept incidents from the devices that NNMi manages. HPOM ignores any forwarded incident from an NNMi source node that is not configured as a managed node in HPOM, as described in step 3 on page 598 (for HPOM for Windows) and in step 3 on page 600 (for HPOM for UNIX and for HPOM for Linux).

If the NNMi source node is configured as a managed node in HPOM, verify the incident filter configuration on the **HP NNMi–HPOM Web Services Integration Configuration** form. Then test the filter by generating an incident on the NNMi management server and determine whether it reaches the HPOM management server.

NNMi Incident Information Is Not Available in the HPOM Messages Browser

The important information from NNMi incidents is passed to HPOM as custom message attributes. Add one or more custom messages attributes for NNMi incidents as described in step 4 on page 599 (for HPOM for Windows) and in step 4 on page 600 (for HPOM for UNIX and for HPOM for Linux).

NNMi and HPOM Are Not Synchronized

If either of the management servers becomes unreachable, the incidents in the NNMi incident views and the HPOM active messages browser might become mismatched. The HP NNMi–HPOM integration can re-synchronize the incidents as described here.

- If an HPOM management server becomes unavailable to the HP NNMi–HPOM integration module, the integration module periodically checks for the availability of that HPOM management server and resumes incident forwarding when a connection can be re-established. When the connection to the HPOM management server is available, the integration module forwards any incidents that might have been missed while the HPOM management server was down.

- If the NNMi management server is unavailable when an HPOM user acknowledges or unacknowledges a forwarded incident, NNMi does not receive the change of state. NNMi and HPOM might show different states for this incident.

The Integration Does Not Work Through a Firewall

Ensure that the NNMi management server can directly address the HPOM IWS by host and port.

HP NNMi–HPOM Web Services Integration Configuration Form Reference

The **HP NNMi–HPOM Web Services Integration Configuration** form contains the parameters for configuring communications between NNMi and HPOM. This form is available from the **Integration Module Configuration** workspace. (On the **HP NNMi–HPOM Integration Selection** form, click **web services implementation**.)

➤ Only NNMi users with the Administrator role can access the **HP NNMi–HPOM Web Services Integration Configuration** form.

The **HP NNMi–HPOM Web Services Integration Configuration** form collects information for the following general areas:

- NNMi Management Server Connection on page 608
- HPOM Management Server Connection on page 609
- Integration Behavior on page 610
- Incident Filters on page 611

To apply changes to the integration configuration, update the values on the **HP NNMi–HPOM Web Services Integration Configuration** form, and then click **Submit**.

NNMi Management Server Connection

Table 66 lists the parameters for connecting to the NNMi management server. This is the same information that you use to open the NNMi console. You can determine many of these values by examining the URL that invokes an NNMi console session. Coordinate with the NNMi administrator to determine the appropriate values for this section of the configuration form.

Table 66 NNMi Management Server Connection Information

Field	Description
NNMi SSL Enabled	The connection protocol specification for connecting to the NNMi console. The integration requires an HTTP connection to the NNMi console. Leave the **NNMi SSL Enabled** check box cleared.
NNMi Host	The fully-qualified domain name of the NNMi management server. This field is pre-filled with the hostname that was used to access the NNMi console. Verify that this value is the name returned by the **`nnmofficialfqdn.ovpl -t`** command run on the NNMi management server.
NNMi Port	The port for connecting to the NNMi console. This field is pre-filled with the port that the jboss application server uses for communicating with the NNMi console, as specified in the following file: • *Windows*: `%NnmDataDir%\conf\nnm\props\nms-local.properties` • *UNIX*: `$NnmDataDir/conf/nnm/props/nms-local.properties` Use the value of `jboss.http.port`, which is `80` or `8004` by default (depending on the presence of another web server when NNMi was installed).

Table 66 NNMi Management Server Connection Information (cont'd)

Field	Description
NNMi User	The user name for connecting to the NNMi web services. This user must have the NNMi Administrator or Web Service Client role. **NOTE:** The password for this user name is passed in cleartext. Best practice: Create and use an `NNMiIntegration` user account with the Web Service Client role.
NNMi Password	The password for the specified NNMi user.

HPOM Management Server Connection

Table 67 lists the parameters for connecting to the web service on the HPOM management server. Coordinate with the HPOM administrator to determine the appropriate values for this section of the configuration.

Table 67 HPOM Management Server Connection Information

HPOM Server Parameter	Description
HPOM SSL Enabled	The connection protocol specification. • If HPOM is configured to use HTTPS, select the **HPOM SSL Enabled** check box. This is the default configuration. • If HPOM is configured to use HTTP, clear the **HPOM SSL Enabled** check box.
HPOM Host	The fully-qualified domain name of the HPOM management server. Verify that this name is resolvable from the NNMi management server by using the `nslookup` or `ping` command. If DNS is questionable, use the IP address of the HPOM management server. If possible, use the `traceroute` command to verify the network path from the NNMi management server to the HPOM management server.
HPOM Port	The port for connecting to the HPOM web service. To determine which port number to specify, do the following on the HPOM management server: • *HPOM for Windows*: Examine the port settings in the IIS Manager, which is available from the **Start** menu, for example, **Start > Administrative Tools > Internet Information Services (IIS) Manager**. • *HPOM for UNIX* or HPOM for *Linux*: Run the following command: **`ovtomcatbctl -getconf`** This field is pre-filled with the value `443`, which is the default port for SSL connections to HPOM for Windows. For SSL connections to HPOM for UNIX or HPOM for Linux, the default port is 8443 or 8444.

Table 67 HPOM Management Server Connection Information (cont'd)

HPOM Server Parameter	Description
HPOM User	A valid HPOM user account name with the HPOM Administrator role. This user must be permitted to view the HPOM active messages browser and the HPOM incident web service WSDL. *Windows only*: On the Windows operating system, HPOM works through Microsoft Internet Information Services (IIS) to authenticate user credentials. Specify a Windows user in the format `<Windows_domain>\<username>`. Best Practice: • *HPOM for Windows*: Specify a user who is a member of the `HP-OVE-ADMINS` user group. (Verify group membership in the Local Users and Groups area of the Microsoft Management Console, which is available from **Control Panel > Administrative Tools > Computer Management**.) • *HPOM for UNIX* or *HPOM for Linux*: Use the `opc_adm` user account.
HPOM Password	The password for the specified HPOM user.

Integration Behavior

Table 68 lists the parameters that describe the integration behavior. Coordinate with the NNMi administrator to determine the appropriate values for this section of the configuration.

Table 68 Integration Behavior Information

Field	Description
Forward Only	The behavior specification for the HP NNMi–HPOM integration module. By default, the integration module forwards incidents to and receives incident acknowledgements from the HPOM management servers identified on the **HP NNMi–HPOM Web Services Integration Configuration** form. You can disable the receipt of incident acknowledgements. • For one-way communication (forward incidents to HPOM but ignore incident acknowledgements from HPOM), select the **Forward Only** check box. • For two-way communication, leave the **Forward Only** check box cleared. This is the default behavior.
Holding period (minutes)	The number of minutes to wait before forwarding the configured incidents to HPOM. If an incident is closed during this time (for example, an SNMPLinkUp incident cancels an SNMPLinkDown incident), HPOM never receives that incident. If you want NNMi to forward incidents immediately, enter the value `0`. The default value is 5 minutes.
Incident Filter	A filter based on NNMi incident attributes that limits incident forwarding. The default filter (`nature=ROOTCAUSE origin=MANAGEMENTSOFTWARE`) specifies all root cause incidents that are generated by NNMi. You can modify the filter to change which incidents are forwarded to HPOM. **NOTE:** All text (attribute names and values) in the **Incident Filter** field is case-sensitive. For more information, see Incident Filters.

Incident Filters

The incident filter is the combination of all entries in the **Incident Filter** list. Filter entries with the same attribute value expand the filter (logical OR). Filter entries with different attribute values restrict the filter (logical AND). All filter entries work together; you *cannot* create a filter of the format `(a AND b) OR c`. For example filter entries, see Example Incident Filters on page 612.

To create the incident filter, follow these steps:

1. In the NNMi console, open the **HP NNMi–HPOM Integration Selection** form (**Integration Module Configuration > HPOM**).
2. Click **web services implementation**.
3. To delete a filter entry, in the **Incident Filter** list, edit the text to delete the entry (or entries).

   ⚠ Clicking **Clear** removes all filter entries from the list.

4. To add an incident filter entry:
   a. Select an attribute from the **name** list. For the supported attributes, see the table in step c.
   b. Select the comparison operation to perform. Supported operators are:
      - =
      - !=
      - <
      - <=
      - >
      - >=
   c. Enter a comparison value. The following table lists the supported attributes and the acceptable values for each attribute.

Attribute	Possible Values
name	Examine the incident configuration in the NNMi console to determine the available incident names.
nature	• ROOTCAUSE • SECONDARYROOTCAUSE • SYMPTOM • SERVICEIMPACT • STREAMCORRELATION • INFO • NONE

Attribute	Possible Values
origin	• MANAGEMENTSOFTWARE • MANUALLYCREATED • SYMPTOM • REMOTELYGENERATED • SNMPTRAP • SYSLOG • OTHER
family	• com.hp.nms.incident.family.Address • com.hp.nms.incident.family.Interface • com.hp.nms.incident.family.Node • com.hp.nms.incident.family.OSPF • com.hp.nms.incident.family.HSRP • com.hp.nms.incident.family.AggregatePort • com.hp.nms.incident.family.Board • com.hp.nms.incident.family.Connection • com.hp.nms.incident.family.Correlation
category	• com.hp.nms.incident.category.Fault • com.hp.nms.incident.category.Status • com.hp.nms.incident.category.Config • com.hp.nms.incident.category.Accounting • com.hp.nms.incident.category.Performance • com.hp.nms.incident.category.Security • com.hp.nms.incident.category.Alert
severity	• NORMAL • WARNING • MINOR • MAJOR • CRITICAL

5. Repeat step 4 until all filter entries are defined.
6. Click **Submit** at the bottom of the form.

Example Incident Filters

Forward NodeDown Incidents from NNMi to HPOM

```
name=NodeDown
```

Forward NodeDown and InterfaceDown Incidents from NNMi to HPOM

```
name=NodeDown
name=InterfaceDown
```

Forward CiscoLinkDown Incidents from NNMi to HPOM

```
name=CiscoLinkDown
```

Forward NNMi Management Events with Severity of MAJOR or MINOR

```
origin=MANAGEMENTSOFTWARE
severity=MAJOR
severity=MINOR
```

Forward NNMi Incidents with Severity of at least MINOR and nature of ROOTCAUSE or SERVICEIMPACT

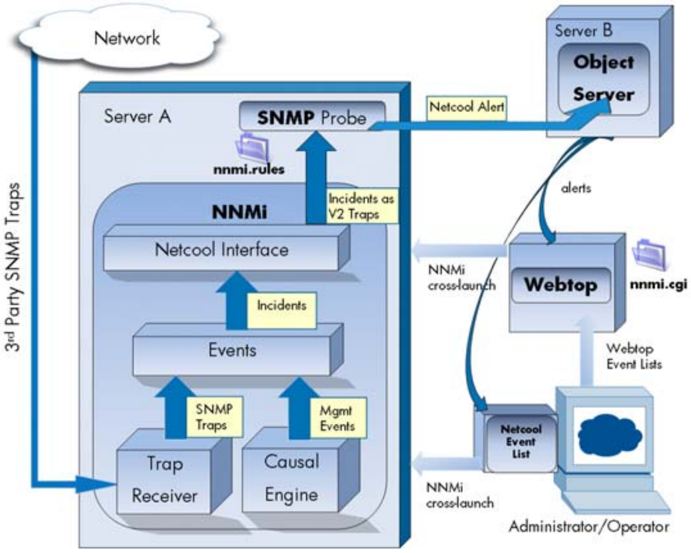
```
severity>=MINOR
nature=ROOTCAUSE
nature=SERVICEIMPACT
```

Incident Filter Limitations

Because all filter entries combine to create one incident filter for the NNMi management server, the following limitations apply:

- The stated severity applies to all incidents. For example, to forward NodeDown incidents with a severity of MINOR or higher and InterfaceDown incidents with a severity of MAJOR, set the filter severity to `>=MINOR` and use HPOM logic to filter out the unwanted InterfaceDown messages.
- The incident filter does not provide a mechanism for limiting incident forwarding to specific source nodes. The HPOM managed node (or external node) configuration limits the forwarded incidents that HPOM accepts.

HP NNMi Integration Module for Netcool Software



IBM Tivoli Netcool/OMNIbus consolidates events from a wide range of sources into a single view.

This chapter contains the following topics:

- HP NNMi Integration Module for Netcool Software
- Enabling the HP NNMi Integration Module for Netcool Software
- Using the HP NNMi Integration Module for Netcool Software
- Changing the HP NNMi Integration Module for Netcool Software
- Disabling the HP NNMi Integration Module for Netcool Software
- Troubleshooting the HP NNMi Integration Module for Netcool Software
- HP NNMi Integration Module for Netcool Software Destination Form Reference

HP NNMi Integration Module for Netcool Software

The HP NNMi Integration Module for Netcool Software forwards NNMi management events as SNMPv2c traps to a Netcool/OMNIbus SNMP Probe on the NNMi management server. The probe filters the NNMi traps and forwards them to the Netcool/OMNIbus server.

While the integration can also forward the SNMP traps that NNMi receives from managed devices to the probe, it is recommended that you instead use the NNMi SNMP trap forwarding mechanism. For more information, see the `hp-nnmi-nbi.mib` file.

The integration does not forward events generated by NNM 6.x or 7.x management stations to the probe.

The integration provides menu items that extend the Netcool event viewers for launching NNMi forms and views in the context of a selected event.

The NNMi Integration Module for Netcool Software is a specific implementation of the NNMi northbound interface, which is described in NNMi Northbound Interface on page 543.

The NNMi Integration Module for Netcool Software consists of the following components:

- nnmi-northbound integration module
- Configuration files for converting NNMi traps to Netcool/OMNIbus events and creating new menus in the Netcool/Webtop event lists and the Netcool/OMNIbus Event List

Value

The NNMi Integration Module for Netcool Software adds network-level fault and performance information to Netcool/OMNIbus, so that Netcool/OMNIbus users can detect and investigate potential network problems.

The primary features of the integration are as follows:

- Automatic management event forwarding from NNMi to Netcool/OMNIbus. Forwarded management events appear in the Netcool/Webtop event lists and the Netcool/OMNIbus Event List.
- Access to the NNMi console from Netcool/Webtop and Netcool/OMNIbus.
  - Netcool users can open an NNMi form (for example, the Node form) in the context of a selected event and topology object.
  - Netcool users can open an NNMi view (for example, the Layer 2 Neighbor view) in the context of a selected event and node.
  - Netcool users can open the NNMi Incident form in the context of a selected event.

Integrated Products

The information in this chapter applies to the following products:

- Netcool/OMNIbus

  For the list of supported versions, see the *NNMi System and Device Support Matrix*.

- Netcool/OMNIbus SNMP Probe
- NNMi 9.10 with an NNMi Integration Module for Netcool Software license

  As of NNMi 9.00, installing NNMi enables a temporary Instant-On license key for the NNMi Integration Module for Netcool Software. To use the integration after the Instant-On license key expires, obtain and install a permanent license key for the NNMi Integration Module for Netcool Software.

NNMi and Netcool/OMNIbus must be installed on separate computers. The NNMi management server and the Netcool/OMNIbus server computer can be of the same or different operating systems.

The Netcool/OMNIbus SNMP Probe must be installed on the NNMi management server computer.

For the most recent information about supported hardware platforms and operating systems, see the NNMi support matrix and the Netcool/OMNIbus product documentation.

Documentation

This chapter describes how to configure the NNMi Integration Module for Netcool Software to forward NNMi management events to a Netcool/OMNIbus SNMP Probe. It also describes how to use the integration functionality.

For information about Netcool/OMNIbus, see that application's documentation.

Enabling the HP NNMi Integration Module for Netcool Software

The NNMi Integration Module for Netcool Software includes files for configuring the Netcool/OMNIbus SNMP Probe and the Netcool event viewers. Because Netcool is highly configurable, the instructions for the Netcool side of the configuration might not exactly match your Netcool system. It is recommended that an experienced Netcool administrator complete the procedure for enabling the integration.

To enable the NNMi Integration Module for Netcool Software, follow these steps:

1 Gather the information for configuring Netcool:

  a On any computer, log on to the NNMi console as an NNMi user with the Administrator role.

  b In the NNMi console, open the **HP NNMi Integration Module for Netcool Software Configuration Actions** form (**Integration Module Configuration > Netcool**).

  c Download the rules include file for the Netcool/OMNIbus SNMP Probe by right-clicking the **nnmi.include.rules** link and then saving the file to a known place on the computer.

  The `nnmi.include.rules` file defines a rule for interpreting the SNMPv2c traps of the NNMi management events.

  — For information about the contents and format of the traps that NNMi sends to the probe, see the `hp-nnmi-nbi.mib` file.

  — For information about customizing the `nnmi.include.rules` file, see the Netcool/OMNIbus documentation.

  d *Optional*. Download the information for configuring the Netcool/Webtop event lists to launch NNMi views. Do both of the following:

  — Right-click the **nnmi_launch.cgi** link, and then save the file to a known place on the computer.

  — Right-click the **nnmi_launch_cfg.txt** link, and then save the file to a known place on the computer.

  e *Optional*. Download the information for configuring the Netcool/OMNIbus Event List to launch NNMi views. Do one of the following:

  — *Windows* Netcool/OMNIbus server:

  Right-click the **nnmi_confpack.zip** link, and then save the file to a known place on the computer.

  — *UNIX* Netcool/OMNIbus server:

  Right-click the **nnmi_confpack.gz** link, and then save the file to a known place on the computer.

2 Install the Netcool/OMNIbus SNMP Probe on the NNMi management server.

   a Configure the probe to receive SNMP traps on an available UDP port.

      — Note this port number for configuring the integration in NNMi.

      — Verify that the probe port is different from the port on which NNMi receives SNMP traps, which is configured on the **Communication Configuration** form in the NNMi console.

   b Copy the `nnmi.include.rules` file from step 1c to the NNMi management server.

   c Back up the master rules file, and then open the file in any text editor.

   d Within the Netcool enterprise trap switch block, add an `include` directive for the `nnmi.include.rules` file, and then save the master rules file.

   e Restart the probe, and then examine the probe log file to verify that there were no problems reloading the rules file.

   For more information about installing and configuring the probe, see the probe documentation.

3 Configure NNMi incident forwarding:

   a On any computer, log on to the NNMi console as an NNMi user with the Administrator role.

   b In the NNMi console, open the **HP NNMi Integration Module for Netcool Software Configuration Actions** form (**Integration Module Configuration > Netcool**).

   c Click **Enable/Disable** NNMi Integration Module for Netcool Software, and then click **New**.

   (If you have selected an available destination, click **Reset** to make the **New** button available.)

   d On the **HP NNMi Integration Module for Netcool Software Destination** form, select the **Enabled** check box to make the remaining fields on the form available.

   e Enter the information for connecting to the Netcool/OMNIbus SNMP Probe.

   For information about these fields, see Netcool/OMNIbus SNMP Probe Connection on page 623.

   f Specify the sending options.

   For information about these fields, see Integration Content on page 624.

   g Click **Submit** at the bottom of the form.

   A new window opens a status message. If the message indicates a problem with the settings, click **Return**, and then adjust the values as suggested by the text of the error message.

4 *Optional*. Configure the Netcool/Webtop event lists to launch NNMi views.

   a Copy the `nnmi_launch.cgi` file from step 1d to the `cgi-bin` directory on the Netcool/Webtop server.

   b Follow the instructions in the `nnmi_launch_cfg.txt` file from step 1d to prepare the CGI file and to configure the Netcool/Webtop menus.

5 *Optional*. Configure the Netcool/OMNIbus Event List to launch NNMi views.

   a Copy the `nnmi_confpack.*` archive file from step 1e to the computer where the instance of the Netcool/OMNIbus ObjectServer is running.

b Unpack the `nnmi_confpack.*` archive file to a temporary location.

c From the temporary location, run the following command:

— *Windows* Netcool/OMNIbus server:

```
%OMNIBUSHOME%\bin\nco_confpack -import \
-package nnmi.confpack \
-user <objectserver_administrator_username> \
-server <objectserver_name>
```

— *UNIX* Netcool/OMNIbus server:

```
$OMNIBUSHOME/bin/nco_confpack -import \
-package nnmi.confpack \
-user <objectserver_administrator_username> \
-server <objectserver_name>
```

d *UNIX only*: Verify that `$OMNIBROWSER` is set to the location of the Mozilla Firefox browser.

Using the HP NNMi Integration Module for Netcool Software

When the NNMi Integration Module for Netcool Software is enabled, NNMi sends SNMPv2c traps to the Netcool/OMNIbus SNMP Probe. View the content forwarded from NNMi in the Netcool/Webtop event lists and the Netcool/OMNIbus Event List.

For information about the types of traps the integration module can forward to the probe, see Using the NNMi Northbound Interface on page 546. For information about the contents and format of these traps, see the `hp-nnmi-nbi.mib` file. For a comparison of trap forwarding mechanisms, see Trap and Incident Forwarding on page 93.

NNMi sends only one copy of each management event trap (or received SNMP trap) to the Netcool/OMNIbus SNMP Probe. NNMi does not queue traps. If the probe is unavailable when NNMi forwards a trap, that trap is lost.

The integration module provides links to the NNMi console from the Netcool event viewers. Enter your NNMi user credentials to see the NNMi console views.

In Enabling the HP NNMi Integration Module for Netcool Software on page 617, step 4 and step 5 add the following menu items to the Netcool event viewers:

- **Source Object**—Opens the NNMi form for the object in the event selected in Netcool/OMNIbus.
- **Node**—Opens the NNMi Node form for the node in the event selected in Netcool/OMNIbus.
- **L2 Neighbors**—Opens the NNMi Layer 2 Neighbor View for the node in the event selected in Netcool/OMNIbus.
- **L3 Neighbors**—Opens the NNMi Layer 3 Neighbor View for the node in the event selected in Netcool/OMNIbus.

- **Incident Details**—Opens the NNMi Incident form for the event selected in Netcool/OMNIbus.

➤ On UNIX Netcool/OMNIbus servers:

- Mozilla Firefox must be the default web browser to support the launching of NNMi views from the Netcool/OMNIbus Event List.
- The `$OMNIBROWSER` environment variable must be set to the location of the Mozilla Firefox browser.

Changing the HP NNMi Integration Module for Netcool Software

To change the NNMi Integration Module for Netcool Software configuration parameters, follow these steps:

1. In the NNMi console, open the **HP NNMi Integration Module for Netcool Software Configuration Actions** form (**Integration Module Configuration > Netcool**).
2. Click **Enable/Disable** NNMi Integration Module for Netcool Software.
3. Select a destination, and then click **Edit**.
4. Modify the values as appropriate.

   For information about the fields on this form, see HP NNMi Integration Module for Netcool Software Destination Form Reference on page 623.
5. Verify that the **Enable** check box at the top of the form is selected, and then click **Submit** at the bottom of the form.

   The changes take effect immediately.

Disabling the HP NNMi Integration Module for Netcool Software

No SNMP trap queuing occurs while a destination is disabled.

To discontinue the forwarding of NNMi management events to the Netcool/OMNIbus SNMP Probe, follow these steps:

1. In the NNMi console, open the **HP NNMi Integration Module for Netcool Software Configuration Actions** form (**Integration Module Configuration > Netcool**).
2. Click **Enable/Disable** NNMi Integration Module for Netcool Software.
3. Select a destination, and then click **Edit**.

   Alternatively, click **Delete** to entirely remove the configuration for the selected destination.
4. On the **HP NNMi Integration Module for Netcool Software Destination** form, clear the **Enable** check box at the top of the form, and then click **Submit** at the bottom of the form.

   The changes take effect immediately.
5. To conserve system resources, shut down the Netcool/OMNIbus SNMP Probe while the destination is disabled.

To permanently disable the integration, also do the following:

- Uninstall the Netcool/OMNIbus SNMP Probe as described in the probe documentation.
- Remove the NNMi menu items from the Netcool/Webtop and Netcool/OMNIbus Event List configurations.

Troubleshooting the HP NNMi Integration Module for Netcool Software

Netcool/OMNIbus Does Not Receive Any Forwarded NNMi Management Events

If the Netcool event viewer does not contain any traps from NNMi, follow these steps:

1. Verify that the Netcool/OMNIbus SNMP Probe is receiving traps:

   a. Verify that the probe can send messages to the Netcool/OMNIbus server.

   b. Verify that the probe master rules file includes or contains the content of the `nnmi.include.rules` file.

   c. Verify the syntax of the master rules file.

   d. Examine the probe log file to verify that there were no problems loading the rules file.

   e. Examine the probe log file to determine whether the NNMi traps arrive at the probe.

   f. Examine the probe log file to determine whether the probe processes or drops the incoming traps.

   For information about troubleshooting the probe, see the Netcool/OMNIbus documentation.

2. Verify that NNMi is forwarding management events to the Netcool/OMNIbus SNMP Probe.

   For information, see Troubleshooting the NNMi Northbound Interface on page 550.

Netcool/OMNIbus Does Not Receive Some Forwarded NNMi Management Events

If one or more NNMi management event traps do not appear in the Netcool event viewer, follow these steps:

1. Verify that the Netcool/OMNIbus SNMP Probe master rules file includes or contains the content of the `nnmi.include.rules` file.

2. Verify that Netcool/OMNIbus is running.

   If the Netcool/OMNIbus server shuts down, the Netcool/OMNIbus SNMP Probe queues received traps. The probe forwards the queued traps when the Netcool/OMNIbus server becomes available.

   NNMi relies on the probe to queue and forward traps. If the probe shuts down, the forwarded traps are lost.

3. Verify that the NNMi processes are running.

Error When Launching an NNMi Form for a Layer 2 Connection

If the source object in an NNMi management event is a layer 2 connection, NNMi users with a role other than Administrator cannot open the NNMi form directly from the **Source Object** menu item in the Netcool event viewer. Instead, in the Netcool event viewer, use the **L2 Neighbors** menu item to connect to NNMi, and then double-click the connection in the Layer 2 Neighbor View.

HP NNMi Integration Module for Netcool Software Destination Form Reference

The **HP NNMi Integration Module for Netcool Software Destination** form contains the parameters for configuring communications between NNMi and a Netcool/OMNIbus SNMP Probe. When a valid NNMi Integration Module for Netcool Software license has been installed on the NNMi management server, this form is available from the **Integration Module Configuration** workspace. (On the **HP NNMi Integration Module for Netcool Software Configuration Actions** form, click **Enable/Disable** NNMi Integration Module for Netcool Software. Click **New**, or select a destination, and then click **Edit**.)

Only NNMi users with the Administrator role can access the **HP NNMi Integration Module for Netcool Software Destination** form.

The **HP NNMi Integration Module for Netcool Software Destination** form collects information for the following areas:

- Netcool/OMNIbus SNMP Probe Connection on page 623
- Integration Content on page 624
- Destination Status Information on page 627

To apply changes to the integration configuration, update the values on the **HP NNMi Integration Module for Netcool Software Destination** form, and then click **Submit**.

Netcool/OMNIbus SNMP Probe Connection

Table 69 lists the parameters for configuring the connection to the Netcool/OMNIbus SNMP Probe.

Table 69 Netcool/OMNIbus SNMP Probe Connection Information

Field	Description
Host	The fully-qualified domain name (preferred) or the IP address of the NNMi management server, which is the system on which the Netcool/OMNIbus SNMP Probe receives SNMP traps from NNMi. The integration supports the following methods for identifying the probe host: • **NNMi FQDN** NNMi manages the connection to the probe on the NNMi management server and the **Host** field becomes read-only. This is the default and recommended configuration. • **Use Loopback** NNMi manages the connection to the probe on the NNMi management server and the **Host** field becomes read-only. • **Other** Do not use this option. **NOTE:** If the NNMi management server participates in NNMi application failover, see Application Failover and the NNMi Northbound Interface on page 551 for information about the impact of application failover on the integration.

Table 69 Netcool/OMNIbus SNMP Probe Connection Information (cont'd)

Field	Description
Port	The UDP port where the Netcool/OMNIbus SNMP Probe receives SNMP traps. Enter the port number specific to the probe. To determine the port, examine the probe `mttrapd.properties` file on the NNMi management server. **NOTE:** This port number must be different from the port on which NNMi receives SNMP traps, as set in the **SNMP Port** field on the **Communication Configuration** form in the NNMi console.
Community String	A read-only community string for the Netcool/OMNIbus SNMP Probe to receive traps. If the probe configuration requires a specific community string in the received SNMP traps, enter that value. If the probe configuration does not require a specific community string, use the default value, which is `public`.

Integration Content

Table 70 lists the parameters for configuring which content the NNMi Integration Module for Netcool Software sends to the Netcool/OMNIbus SNMP Probe.

Table 70 NNMi Integration Module for Netcool Software Content Configuration

Field	Description
Incidents	The incident forwarding specification. • **Management** NNMi forwards only NNMi-generated management events to the Netcool/ OMNIbus SNMP Probe. This is the default configuration. • **SNMP 3rd Party Trap** NNMi forwards only SNMP traps that NNMi receives from managed devices to the probe. • **Both** NNMi forwards to the probe both NNMi-generated management events and SNMP traps that NNMi receives from managed devices. NNMi begins forwarding incidents as soon as you enable the destination. For more information, see Incident Forwarding on page 546.

Table 70 NNMi Integration Module for Netcool Software Content Configuration (cont'd)

Field	Description
Lifecycle State Changes	The incident change notification specification. • **Enhanced Closed** NNMi sends an incident closed trap to the Netcool/OMNIbus SNMP Probe for each incident that changes to the CLOSED lifecycle state. This is the default configuration. • **State Changed** NNMi sends an incident lifecycle state changed trap to the probe for each incident that changes to the IN PROGRESS, COMPLETED, or CLOSED lifecycle state. • **Both** NNMi sends an incident closed trap to the probe for each incident that changes to the CLOSED lifecycle state. Additionally, the integration sends an incident lifecycle state changed trap to the probe for each incident that changes to the IN PROGRESS, COMPLETED, or CLOSED lifecycle state. **NOTE:** In this case, each time an incident changes to the CLOSED lifecycle state, the integration sends two notification traps: an incident closed trap and an incident lifecycle state changed trap. For more information, see Incident Lifecycle State Change Notifications on page 547.
Correlations	The incident correlation notification specification. • **None** NNMi does not notify the Netcool/OMNIbus SNMP Probe of incident correlations resulting from NNMi causal analysis. This is the default configuration. • **Single** NNMi sends a trap for each parent-child incident correlation relationship resulting from NNMi causal analysis. • **Group** NNMi sends one trap per correlation that lists all child incidents correlated to a parent incident. For more information, see Incident Correlation Notifications on page 547.
Deletions	The incident deletion specification. • **Don't Send** NNMi does not notify the Netcool/OMNIbus SNMP Probe when incidents are deleted in NNMi. This is the default configuration. • **Send** NNMi sends a deletion trap to the probe for each incident that is deleted in NNMi. For more information, see Incident Deletion Notifications on page 548.

Table 70 NNMi Integration Module for Netcool Software Content Configuration (cont'd)

Field	Description
NNMi Console Access	The connection protocol specification in the URL for browsing to the NNMi console from the Netcool event viewer. The traps that NNMi sends to the Netcool/OMNIbus SNMP Probe include the NNMi URL in the NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2). The configuration page defaults to the setting that matches the NNMi configuration. If the NNMi console is configured to accept both HTTP and HTTPS connections, you can change the HTTP connection protocol specification in the NNMi URL. For example, if all Netcool users are on the intranet, you can set NNMi console access from the Netcool event viewer to be over HTTP. To change the protocol for connecting to the NNMi console from the Netcool event viewer, select the **HTTP** option or the **HTTPS** option as appropriate.
Incident Filters	A list of object identifiers (OIDs) on which the integration filters the events sent to the Netcool/OMNIbus SNMP Probe. Each filter entry can be a valid numeric OID (for example, .1.3.6.1.6.3.1.1.5.4.1.3.6.1.4.1.9) or OID prefix (for example, .1.3.6.1.6.3.1.1.5.*). Select one of the following options: • **None** NNMi sends all events to the probe. This is the default configuration. • **Include** NNMi sends only the specific events that match the OIDs identified in the filter. • **Exclude** NNMi sends all events except for the specific events that match the OIDs identified in the filter. Specify the incident filter: • To add a filter entry, enter the text in the lower text box, and then click **Add**. • To delete a filter entry, select that entry from the list in the upper box, and then click **Remove**. For more information, see Event Forwarding Filter on page 548.

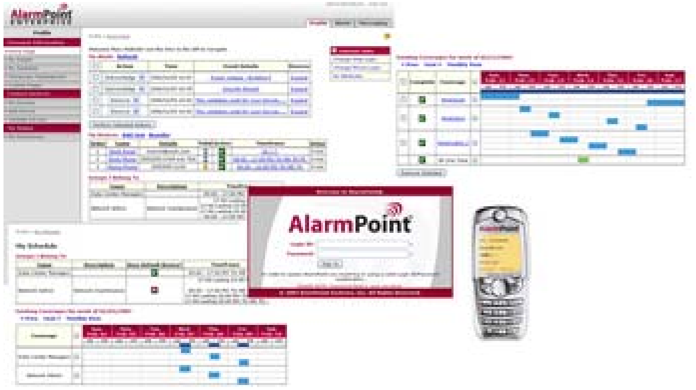
Destination Status Information

Table 71 lists the read-only status information for the NNMi Integration Module for Netcool Software destination. This information is useful for verifying that the integration is working correctly.

Table 71 NNMi Integration Module for Netcool Software Status Information

Field	Description
Trap Destination IP Address	The IP address to which the Netcool/OMNIbus SNMP Probe destination host name resolves. This value is unique to this probe destination.
Uptime (seconds)	The time (in seconds) since the northbound component was last started. The traps that NNMi sends to the Netcool/OMNIbus SNMP Probe include this value in the sysUptime field (1.3.6.1.2.1.1.3.0). This value is the same for all integrations that use the NNMi northbound interface. To see the latest value, either refresh or close and re-open the form.
NNMi URL	The URL for connecting to the NNMi console. The traps that NNMi sends to the Netcool/OMNIbus SNMP Probe include this value in the NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2). This value is unique to this northbound destination.

xMatters (formerly AlarmPoint)



xMatters, from xMatters, inc., is an interactive alerting platform, designed to capture and enrich important events, to route those events to the correct person on any communication device, and to give that person the ability to solve, escalate, or enlist others to resolve the situation.

Through integrations, xMatters can become the voice and interface of an automation engine or an intelligent application, such as HP Network Node Manager i Software (NNMi). When NNMi detects an event that requires attention, xMatters places phone calls or sends pages, instant messages, or email messages to the appropriate personnel, vendors, or customers.

xMatters is also persistent, escalating through multiple devices, communication mediums, and personnel until someone accepts responsibility or resolves the event. xMatters gives the notified person instant, two-way communication with NNMi. Responses are processed immediately on the NNMi management server, enabling remote resolution of the event.

xMatters mobile access, included with all xMatters enterprise licenses, extends the functionality of the xMatters platform to provide mobile web access to critical applications. xMatters mobile access provides access to enterprise applications from mobile devices for accessing and modifying ticket information, monitoring dashboards, and generating sophisticated reports.

For information about purchasing xMatters and xMatters mobile access, contact your HP sales representative or **sales@xmatters.com**.

This chapter describes the available integrations:

- HP NNMi–xMatters Integration
- HP NNMi–xMatters mobile access Integration

HP NNMi–xMatters Integration

About the HP NNMi–xMatters Integration

By including xMatters in the NNMi environment, network operations staff who use NNMi to monitor and manage their network devices gain intelligent alerting and two-way communication between personal communication tools and NNMi.

The HP NNMi–xMatters integration supports event notifications (from NNMi to xMatters) through the configuration of NNMi incident types. It also supports inbound actions (from xMatters to NNMi) to acknowledge the original incident, alter its priority, and add informational annotations.

Each NNMi management server can be integrated with xMatters, with xMatters mobile access, or with both xMatters and xMatters mobile access.

Value

With the HP NNMi–xMatters integration, the appropriate technician can be notified directly through voice, email, pager, or another device. The event resolver receives information about the failure and can make decisions in real time, such as acknowledging, ignoring, annotating, or changing the priority of the event.

After the recipient selects a response on their remote device, xMatters updates the NNMi incident in real time. The benefit is that this process is immediate—significantly faster than the time required for operations staff to notice the failures or malfunctions, determine who is on call, and then manually notify the correct person. Being able to take simple actions to update the incident from any device gives the event resolver a quick way to deal with many issues and communicate to other team members the current status of the incident.

During the process, xMatters logs every notification, response, and action. In addition, xMatters automatically annotates the original NNMi incident with status information.

The xMatters product features a self-service web-based user interface for assigning responsible personnel to each job. xMatters also includes an optional enhanced subscription panel that allows both managed- and self-subscription to NNMi incidents.

➤ xMatters lite, a limited edition of xMatters, is available for select versions of NNMi. xMatters lite for HP NNMi has a reduced feature set and comes pre-configured for an NNMi integration. xMatters lite is a great way to get started with the xMatters product family. xMatters lite is well-suited for a small production environment that does not require voice or distributed load capability.

Integrated Products

The information in this chapter applies to the following products:

- xMatters

  For the list of supported versions, see the *NNMi System and Device Support Matrix*.

- AlarmPoint Java Client
- NNMi 9.10

  The NNMi integration enablement license is *not* required for NNMi integrations with any of the xMatters products.

Documentation

The HP NNMi–xMatters integration is fully described in the *AlarmPoint for HP Network Node Manager i-series Integration Guide*, which is included with the integration.

The xMatters documentation suite describes the xMatters features and capabilities in detail. The documentation suite is available for download from the xMatters Customer Connect Site at:

https://connect.xmatters.com

The *AlarmPoint Express for HP NNMi Quick Start Guide* provides an introduction to the xMatters feature set. This guide describes how to install, configure, and maintain an HP NNMi–xMatters lite integration.

Enabling the HP NNMi–xMatters Integration

If you plan to implement both xMatters integrations with NNMi, it is recommended that you enable the HP NNMi–xMatters integration before you enable the HP NNMi–xMatters mobile access integration.

The high-level steps for installing and configuring the xMatters for NNMi integration are as follows. For detailed information, see the *AlarmPoint for HP Network Node Manager i-series Integration Guide*.

1. Install the AlarmPoint Java Client on the NNMi management server.
2. Install the NNMi-specific integration script for the AlarmPoint Java Client.
3. Install the Web Services Library on the xMatters web servers and the Application server.
4. *Optional*. Install the xMatters subscription panel for NNMi on the xMatters web servers.
5. Install the xMatters action scripts for NNMi by using the xMatters Developer IDE.
6. Install the integration voice files to the xMatters Application server.
7. Configure an Event Domain (and, optionally, a Subscription Domain) in xMatters.
8. Configure an NNMi user with the Web Services Client role.
9. Configure the NNMi incident types that should trigger the xMatters scripts.

10 Validate that the integration can inject NNMi incident parameters for xMatters notifications, and that xMatters responses properly update the NNMi incident.

Using the HP NNMi–xMatters Integration

NNMi and xMatters interact by delivering notifications to users and injecting the responses back into NNMi. When NNMi detects a problem in the network (for example, a NonSNMPNodeUnresponsive incident), the following process occurs:

1 NNMi calls the AlarmPoint Client (APClient) with the parameters describing the problem (for example, the computer affected and the situation).

2 The APClient submits the information to the AlarmPoint Agent (APAgent).

3 The APAgent ensures delivery of the problem details to xMatters, which in turn notifies the appropriate recipient.

4 The recipient responds to the notification by taking one of the actions listed in Table 72. The recipient's acknowledgement, annotation, or priority change updates NNMi through a web services call.

Table 72 Possible Responses to a Received Incident Notification

Action	Description
Acknowledge	User takes ownership of the incident, preventing further notifications to other users. The exception is subscription FYI notifications, which are reporting on the service outage. These notifications are not stopped until the problem has been solved.
Ignore	Stops notifying the current user.
Raise Priority	Increases the priority of the incident in NNMi by one level. (Voice only)
Lower Priority	Decreases the priority of the incident in NNMi by one level. (Voice only)
Set Priority Top	Sets the priority of the incident to Top. (Email, BES, and browser only)
Set Priority High	Sets the priority of the incident to High. (Email, BES, and browser only)
Set Priority Medium	Sets the priority of the incident to Medium. (Email, BES, and browser only)
Set Priority Low	Sets the priority of the incident to Low. (Email, BES, and browser only)
Annotate	Enables the user to append a message to the Notes field of the NNMi incident. (Non-HTML email only)

Disabling the HP NNMi–xMatters Integration

To disable the integration, remove the components installed by the integration's executable archive.

For information about removing an xMatters deployment, see the *AlarmPoint for HP Network Node Manager i-series Integration Guide*.

Troubleshooting the HP NNMi–xMatters Integration

For information about optimizing and extending the integration, and any currently known issues, see the *AlarmPoint for HP Network Node Manager i-series Integration Guide*.

HP NNMi–xMatters mobile access Integration

About the HP NNMi–xMatters mobile access Integration

By including xMatters mobile access in the NNMi environment, network operations staff can interact with NNMi incidents in a mobile device's web browser.

Each NNMi management server can be integrated with xMatters, with xMatters mobile access, or with both xMatters and xMatters mobile access.

Value

With the HP NNMi–xMatters mobile access integration, an NNMi operator can use the web browser on a mobile device to interact in real time with NNMi incidents:

- Query NNMi for current incidents
- View the details of an incident
- Modify the properties, such as status, lifecycle state, or assigned NNMi operator, of an incident

Integrated Products

The information in this chapter applies to the following products:

- xMatters mobile access

  For the list of supported versions, see the *NNMi System and Device Support Matrix*.

- xMatters integration agent
- NNMi 9.10

  The NNMi integration enablement license is *not* required for NNMi integrations with any of the xMatters products.

Documentation

The HP NNMi–xMatters mobile access integration is fully described in the *AlarmPoint Mobile Gateway for HP Network Node Manager i-series Software* integration guide, which is included with the integration.

The xMatters documentation suite describes the xMatters features and capabilities in detail. The documentation suite is available for download from the xMatters Customer Connect Site at:

https://connect.xmatters.com

Enabling the HP NNMi–xMatters mobile access Integration

If you plan to implement both xMatters integrations with NNMi, it is recommended that you enable the HP NNMi–xMatters integration before you enable the HP NNMi–xMatters mobile access integration. See Enabling the HP NNMi–xMatters Integration on page 631.

The high-level steps for installing and configuring the xMatters mobile access for NNMi integration are as follows. For detailed information, see the *AlarmPoint Mobile Gateway for HP Network Node Manager i-series Software* integration guide.

If the HP NNMi–AlarmPoint integration was configured for an earlier version of NNMi, you can upgrade from NNMi 9.0x to NNMi 9.10 without affecting the integration configuration. Verify that the xMatters version is 4.0 or higher.

1. Install the xMatters integration agent on the xMatters server.
2. Install the Web Services Library on the xMatters integration agent and web servers.
3. Install xMatters mobile access on the xMatters Webserver.
4. Install the NNMi Integration Service.
5. Create an NNMi user with the Web Service Client role.
6. Configure an Event Domain (if the HP NNMi–xMatters integration is not already configured) and Integration Service in xMatters.
7. Validate the interaction between xMatters mobile access and NNMi.

Using the HP NNMi–xMatters mobile access Integration

With the HP NNMi–xMatters mobile access integration, you can perform the following actions on an incident in a mobile web browser:

- Add notes
- Update priority
- Update lifecycle state
- Update the Assigned To operator
- View most of the incident details (those that the xMatters mobile access administrator has made available)
- Display the quick view of the Source Object and Node.

For more information about using the integration, see the *AlarmPoint Mobile Gateway for HP Network Node Manager i-series Software* integration guide and the *xMatters (alarmpoint) mobile access Guide*.

Disabling the HP NNMi–xMatters mobile access Integration

To disable the integration, remove the components installed by the integration's executable archive.

For information about removing an xMatters mobile access deployment, see the *AlarmPoint Mobile Gateway for HP Network Node Manager i-series Software* integration guide.

Troubleshooting the HP NNMi–xMatters mobile access Integration

For information about optimizing and extending the integration, and any currently known issues, see the *AlarmPoint Mobile Gateway for HP Network Node Manager i-series Software* integration guide.

Additional Information

This section contains the following appendices:

- NNMi Environment Variables
- NNMi 9.10 and Well-Known Ports
- NNMi 9.10 iSPI Well-Known Ports
- Suggested Configuration Changes

NNMi Environment Variables

HP Network Node Manager i Software (NNMi) provides many environment variables that are available for your use in navigating the file system and writing scripts.

This appendix contains the following topics:

- Environment Variables Used in This Document
- Other Available Environment Variables

Environment Variables Used in This Document

This document primarily uses the following two NNMi environment variables to reference file and directory locations. This list shows the default values. Actual values depend on the selections that you made during NNMi installation.

- *Windows Server 2008*:
  - `%NnmInstallDir%`: *<drive>*`\Program Files\HP\HP BTO Software`
  - `%NnmDataDir%`: *<drive>*`\ProgramData\HP\HP BTO Software`

> On Windows systems, the NNMi installation process creates these system environment variables, so they are always available to all users.

- UNIX:
  - `$NnmInstallDir`: `/opt/OV`
  - `$NnmDataDir`: `/var/opt/OV`

> On UNIX systems, you must manually create these environment variables if you want to use them.

Additionally, this document references some of the NNMi environment variables that you can source as part of your user log-on configuration on the NNMi management server. These variables are of the form `NNM_*`. For information about this extended list of NNMi environment variables, see Other Available Environment Variables on page 639.

Other Available Environment Variables

NNMi administrators access some NNMi file locations regularly. NNMi provides a script that sets up many environment variables for navigating to commonly accessed locations.

To set up the extended list of NNMi environment variables, use a command similar to the following examples:

- Windows: `"C:\Program Files\HP\HP BTO Software\bin\nnm.envvars.bat"`
- UNIX: `. /opt/OV/bin/nnm.envvars.sh`

After you run the command for your operating system, you can use the NNMi environment variables shown in Table 73 (Windows) or Table 74 (UNIX) to get to commonly used NNMi file locations.

Table 73 Environment Variable Default Locations for the Windows Operating System

Variable	Windows (example)
%NNM_BIN%	C:\Program Files (x86)\HP\HP BTO Software\bin
%NNM_CONF%	C:\ProgramData\HP\HP BTO Software\conf
%NNM_DATA%	C:\ProgramData\HP\HP BTO Software\
%NNM_DB%	C:\ProgramData\HP\HP BTO Software\shared\nnm\databases
%NNM_JAVA%	C:\Program Files (x86)\HP\HP BTO Software\nonOV\jdk\nnm\bin\java.exe
%NNM_JAVA_DIR%	C:\Program Files (x86)\HP\HP BTO Software\java
%NNM_JAVA_PATH_SEP%	;
%NNM_JBOSS%	C:\Program Files (x86)\HP\HP BTO Software\nonOV\jboss\nms
%NNM_JBOSS_DEPLOY%	C:\Program Files (x86)\HP\HP BTO Software\nonOV\jboss\nms\server\nms\deploy
%NNM_JBOSS_LOG%	C:\Program Files (x86)HP\HP BTO Software\nonOV\jboss\nms\server\nms\log
%NNM_JBOSS_ROOT%	C:\Program Files (x86)\HP\HP BTO Software\nonOV\jboss\nms
%NNM_JBOSS_SERVERCONF%	C:\Program Files (x86)\HP\HP BTO Software\nonOV\jboss\nms\server\nms
%NNM_JRE%	C:\Program Files (x86)\HP\HP BTO Software\nonOV\jdk\nnm
%NNM_LOG%	C:\ProgramData\HP\HP BTO Software\log
%NNM_LRF%	C:\ProgramData\HP\HP BTO Software\shared\nnm\lrf
%NNM_PRIV_LOG%	C:\ProgramData\HP\HP BTO Software\log
%NNM_PROPS%	C:\ProgramData\HP\HP BTO Software\shared\nnm\conf\props
%NNM_SHARED_CONF%	C:\ProgramData\HP\HP BTO Software\shared\nnm\conf
%NNM_SHARE_LOG%	C:\ProgramData\HP\HP BTO Software\log
%NNM_SNMP_MIBS%	C:\Program Files (x86)\HP\HP BTO Software\misc\nnm\snmp_mibs
%NNM_SUPPORT%	C:\Program Files (x86)\HP\HP BTO Software\support
%NNM_TMP%	C:\ProgramData\HP\HP BTO Software\tmp
%NNM_USER_SNMP_MIBS%	C:\ProgramData\HP\HP BTO Software\shared\nnm\user-snmp-mibs
%NNM_WWW%	C:\ProgramData\HP\HP BTO Software\shared\nnm\www

Table 74 Environment Variable Default Locations for UNIX Operating Systems

Variable	HP-UX
$NNM_BIN	/opt/OV/bin
$NNM_CONF	/var/opt/OV/conf
$NNM_DATA	/var/opt/OV
$NNM_DB	/var/opt/OV/shared/nnm/databases
$NNM_JAVA	/opt/OV/nonOV/jdk/nnm/bin/java
$NNM_JAVA_DIR	/opt/OV/java
$NNM_JAVA_PATH_SEP	:
$NNM_JBOSS	/opt/OV/nonOV/jboss/nms
$NNM_JBOSS_DEPLOY	/opt/OV/nonOV/jboss/nms/server/nms/deploy
$NNM_JBOSS_LOG	/opt/OV/nonOV/jboss/nms/server/nms/log
$NNM_JBOSS_ROOT	/opt/OV/nonOV/jboss/nms
$NNM_JBOSS_SERVERCONF	/opt/OV/nonOV/jboss/nms/server/nms
$NNM_JRE	/opt/OV/nonOV/jdk/nnm
$NNM_LOG	/var/opt/OV/log
$NNM_LRF	/var/opt/OV/shared/nnm/lrf
$NNM_PRIV_LOG	/var/opt/OV/log
$NNM_PROPS	/var/opt/OV/shared/nnm/conf/props
$NNM_SHARED_CONF	/var/opt/OV/shared/nnm/conf
$NNM_SHARE_LOG	/var/opt/OV/log
$NNM_SNMP_MIBS	/opt/OV/misc/nnm/snmp_mibs
$NNM_SUPPORT	/opt/OV/support
$NNM_TMP	/var/opt/OV/tmp
$NNM_USER_SNMP_MIBS	/var/opt/OV/shared/nnm/user-snmp-mibs
$NNM_WWW	/var/opt/OV/shared/nnm/www

NNMi 9.10 and Well-Known Ports

Table 75 shows the ports NNMi uses on the management server. NNMi listens on these ports. If port conflicts occur, you can change most of these port numbers as shown in the *Change Configuration* column. See the *nnm.port.4* reference page, or the UNIX manpage, for more information.

> For application failover to work successfully, open TCP ports 7800-7810. For the application failover feature to function correctly, the active and standby NNMi management servers must have unrestricted network access to each other.

.

Table 75 Ports Used on the NNMi Management Server

Port	Type	Name	Purpose	Change Configuration
80	TCP	`jboss.http.port`	Default HTTP port - used for Web UI & Web Services	Modify the `nms-local.properties` file You can also change this during installation
162	UDP	`trapPort`	SNMP trap port	Modify using the `nnmtrapconfig.ovpl` Perl script. See the *nnmtrapconfig.ovpl* reference page, or the UNIX manpage, for more information.
443	TCP	`jboss.https.port`	Default secure HTTPS port (SSL) - used for Web UI & Web Services	Modify the `nms-local.properties` file
1098	TCP	`jboss.rmi.port`	Default port for RMI naming service	Modify the `nms-local.properties` file
1099	TCP	`jboss.jnp.port`	Default bootstrap JNP service port (JNDI provider)	Modify the `nms-local.properties` file
3873	TCP	`jboss.ejb3.port`	Default EJB3 remoting connector port	Modify the `nms-local.properties` file
4444	TCP	`jboss.jrmp.port`	Default RMI object port (JRMP invoker)	Modify the `nms-local.properties` file
4445	TCP	`jboss.pooled.port`	Default RMI pooled invoker port	Modify the `nms-local.properties` file

Table 75 Ports Used on the NNMi Management Server (cont'd)

Port	Type	Name	Purpose	Change Configuration
4446	TCP	`jboss.socket.port`	Default RMI remoting server connector port	Modify the `nms-local.properties` file
4457	TCP	`jboss.bisocket.port`	Default messaging bi-socket connector	Modify the `nms-local.properties` file
4458	TCP	`jboss.jmsControl.port`	Default JMS control port; used for global network management communication	Modify the `nms-local.properties` file
4459	TCP	`jboss.sslbisocket.port`	Default messaging bi-socket connector; used for secure global network management communication	Modify the `nms-local.properties` file
4460	TCP	`jboss.ssljmsControl.port`	Default JMS control port; used for secure global network management communication	Modify the `nms-local.properties` file
5432	TCP		Postgres port	Not configurable
7800-7810	TCP		JGroups ports for application failover	Modify the `nms-cluster.properties` file
8083	TCP	`jboss.ws.port`	Default jboss Web Service port	Modify the `nms-local.properties` file
8886	TCP	`OVsPMD_MGMT`	NNMi `ovspmd` (process manager) management port	Modify the `/etc/services` file
8887	TCP	`OVsPMD_REQ`	NNMi `ovsmpd` (process manager) request port	Modify the `/etc/services` file
45588	UDP	`jgroups.udp.mcast_port`	JGroups Multicast port for LAN application failover	Modify the `nnmcluster.jvm.properties` file

Table 76 shows some of the ports NNMi uses to communicate with other systems. If a firewall separates NNMi from these systems, open many of these ports in the firewall. The actual set of ports depends on the set of integrations you configured to use with NNMi and how you configured those integrations. If column 4 indicates *Client*, NNMi connects or sends to this port; if column 4 indicates *Server*, NNMi listens on this port.

Table 76 Ports Used for Communication Between the NNMi Management Server and Other Systems

Port	Type	Purpose	Client, Server
80	TCP	Default HTTP port for NNMi; used for Web UI and Web Services	Server
80	TCP	Default HTTP port for NNMi connecting to other applications. The actual port depends on NNMi configuration.	Client
161	UDP	SNMP request port	Client

Table 76 Ports Used for Communication Between the NNMi Management Server and Other Systems (cont'd)

Port	Type	Purpose	Client, Server
162	UDP	SNMP trap port - traps received by NNMi	Server
162	UDP	SNMP trap port; Trap Forwarding, Northbound Interface, or NetCool integrations	Client
389	TCP	Default LDAP port	Client
395	UDP	nGenius Probe SNMP trap port	Client
443	TCP	Default secure HTTPS port; used for Web UI and Web Services	Server
443	TCP	Default secure HTTPS port for NNMi connecting to other applications; the actual port depends on NNMi configuration. Default HTTPS port for HP OM on Windows	Client
636	TCP	Default secure LDAP port (SSL)	Client
1741	TCP	Default CiscoWorks LMS web services port	Client
4457	TCP	Default messaging bi-socket connector used for global network management communication. The connection is from the global manager to the regional manager.	Client, Server
4458	TCP	Default JMS control port used for global network management communication. The connection is from the global manager to the regional manager.	Client, Server
4459	TCP	Default messaging bi-socket connector used for secure global network management communication. The connection is from the global manager to the regional manager.	Client, Server
4460	TCP	Default JMS control port used for secure global network management communication. The connection is from the global manager to the regional manager.	Client, Server
7800-7810	TCP	JGroups ports for application failover	Client and Server
8004	TCP	Default HTTP port for NNMi if another web server already has port 80. Used for Web UI and Web Services. Verify the actual HTTP port for your NNMi management server.	Server
8080	TCP	Default HTTP port for connecting to NA if installed on the same system as NNMi. Default HTTPS port for HP UCMDB web services	Client
8443 or 8444	TCP	Default HTTP port for connecting to HP OM for UNIX	Client
9300	TCP	Default HTTP port for connecting to NNM iSPI for Performance	Client
45588	UDP	JGroups Multicast port for LAN application failover	Client, Server
50000	TCP	Default HTTPS port for connecting to SIM	Client

➤ If you configure NNMi to use ICMP fault polling or ping sweep for discovery, configure the firewall to pass ICMP packets through the firewall.

➤ The Web Services approach for the NNMi-HP OM integration does not work through a firewall, however the NNMi-HP OM integration using the Northbound Interface does work through a firewall.

If you plan to use the global network management feature, Table 77 shows the well-know ports that need to be accessible from a global NNMi management server to a regional NNMi management server. The global network management feature requires these ports to be open for TCP access from the global NNMi management server to the regional NNMi management server. The regional NNMi management server will not open sockets back to the global NNMi management server.

Table 77 Required Accessible Sockets for Global Network Management

Security	Parameter	TCP Port
non-SSL	jboss.http.port	80
	jboss.bisocket.port	4457
	jboss.jmsControl.port	4458
SSL	jboss.https.port	443
	jboss.sslbisocket.port	4459
	jboss.ssljmsControl.port	4460

NNMi 9.10 iSPI Well-Known Ports

Table 78 shows the ports the HP Network Node Manager iSPI for MPLS Software uses on the management server. In case of port conflicts, almost all of these port numbers can be changed using the properties file located at: `%NnmDataDir%/shared/mpls/conf/nms-mpls.ports.properties`.

Table 78 Ports Used on the HP Network Node Manager iSPI for MPLS Software Management Server

Port	Type	Name	Purpose	Change Configuration
24040	TCP	`jboss.http.port`	Default HTTP port - used for Web UI & Web Services	Modify the nms-mpls. ports.properties file. You can also change this during installation.
24041	TCP	`jboss.ejb3.port`	Default EJB3 remoting connector port	Modify the `nms-mpls.ports.properties` file.
24042	TCP	`jboss.ws.port`	Default jboss Web Service port	Modify the `nms-mpls.ports.properties` file.
24043	TCP	`jboss.https.port`	Default HTTPS port	Modify the `nms-mpls.ports.properties` file.
24044	TCP	`jboss.jrmp.port`	Default RMI object port (JRMP invoker)	Modify the `nms-mpls.ports.properties` file.
24045	TCP	`jboss.socket.port`	Default RMI remoting server connector port	Modify the `nms-mpls.ports.properties` file.
24046	TCP	`jboss.jnp.port`	Default bootstrap JNP service port (JNDI provider)	Modify the `nms-mpls.ports.properties` file.
24047	TCP	`jboss.bisocket.port`	Default messaging bi-socket connector	Modify the `nms-mpls.ports.properties` file.
24048	TCP	`jboss.pooled.port`	Default RMI pooled invoker port	Modify the `nms-mpls.ports.properties` file.
24049	TCP	`jboss.rmi.port`	Default port for RMI naming service	Modify the `nms-mpls.ports.properties` file.

Table 78 Ports Used on the HP Network Node Manager iSPI for MPLS Software Management Server (cont'd)

Port	Type	Name	Purpose	Change Configuration
24091	TCP	jboss.ssljmsControl.port	Default SSL JMS control port	Modify the nms-mpls.ports.properties file.
24092	TCP	Jboss.sslbisocket.port	Default SSL bi-socket port	Modify the nms-mpls.ports.properties file.
24458	TCP	jboss.jmsControl.port	Default JMS Control port	Modify the nms-mpls.ports.properties file.

Table 79 shows the ports the NNM iSPI for IP Telephony uses on the management server. In case of port conflicts, almost all of these port numbers can be changed using the properties file located at: %NnmDataDir%/shared/ipt/conf/nms-ipt.ports.properties.

Table 79 Ports Used on the NNM iSPI for IP Telephony Management Server

Port	Type	Name	Purpose	Change Configuration
10043	TCP	jboss.https.port	Default HTTPS port	Modify the nms-ipt.ports.properties file.
10080	TCP	jboss.http.port	Default HTTP port - used for Web UI & Web Services	Modify the nms-ipt.ports.properties file. You can also change this during installation.
10083	TCP	jboss.rmi.port	Default port for RMI naming service	Modify the nms-ipt.ports.properties file.
10084	TCP	jboss.jrmp.port	Default RMI object port (JRMP invoker)	Modify the nms-ipt.ports.properties file.
10085	TCP	jboss.pooled.port	Default RMI pooled invoker port	Modify the nms-ipt.ports.properties file.
10086	TCP	jboss.socket.port	Default RMI remoting server connector port	Modify the nms-ipt.ports.properties file.
10087	TCP	jboss.bisocket.port	Default messaging bi-socket connector	Modify the nms-ipt.ports.properties file.

Table 79 Ports Used on the NNM iSPI for IP Telephony Management Server (cont'd)

Port	Type	Name	Purpose	Change Configuration
10088	TCP	`jboss.ws.port`	Default jboss Web Service port	Modify the `nms-ipt.ports.properties` file.
10089	TCP	`jboss.ejb3.port`	Default EJB3 remoting connector port	Modify the `nms-ipt.ports.properties` file.
10091	TCP	`jboss.ssljmsControl.port`	Default SSL JMS Control port	Modify the `nms-ipt.ports.properties` file.
10092	TCP	`jboss.sslbisocket.port`	Default SSL bi-socket port	Modify the `nms-ipt.ports.properties` file.
10099	TCP	`jboss.jnp.port`	Default bootstrap JNP service port (JNDI provider)	Modify the `nms-ipt.ports.properties` file.
10458	TCP	`jboss.jmsControl.port`	Default JMS Control port	Modify the `nms-ipt.ports.properties` file.

Table 80 shows the ports the NNM iSPI for IP Multicast uses on the management server. In case of port conflicts, almost all of these port numbers can be changed using the properties file located at: `%NnmDataDir%/shared/multicast/conf/nms-multicast.ports.properties`.

Table 80 Ports Used on the NNM iSPI for IP Multicast Management Server

Port	Type	Name	Purpose	Change Configuration
8084	TCP	`jboss.http.port`	Default HTTP port - used for Web UI & Web Services	Modify the `nms-multicast.ports.properties` file. You can also change this during installation.
14083	TCP	`jboss.rmi.port`	Default port for RMI naming service	Modify the `nms-multicast.ports.properties` file.
14084	TCP	`jboss.jrmp.port`	Default RMI object port (JRMP invoker)	Modify the `nms-multicast.ports.properties` file.
14085	TCP	`jboss.pooled.port`	Default RMI pooled invoker port	Modify the `nms-multicast.ports.properties` file.

Table 80 Ports Used on the NNM iSPI for IP Multicast Management Server (cont'd)

Port	Type	Name	Purpose	Change Configuration
14086	TCP	`jboss.socket.port`	Default RMI remoting server connector port	Modify the `nms-multicast.ports.properties` file.
14087	TCP	`jboss.bisocket.port`	Default messaging bi-socket connector	Modify the `nms-multicast.ports.properties` file.
14088	TCP	`jboss.ws.port`	Default jboss Web Service port	Modify the `nms-multicast.ports.properties` file.
14089	TCP	`jboss.ejb3.port`	Default EJB3 remoting connector port	Modify the `nms-multicast.ports.properties` file.
14091	TCP	`Jboss.ssljmsControl.port`	Default SSL JMS Control port	Modify the `nms-multicast.ports.properties` file.
14092	TCP	`jboss.sslbisocket.port`	Default SSL bi-socket port	Modify the `nms-multicast.ports.properties` file.
14099	TCP	`jboss.jnp.port`	Default bootstrap JNP service port (JNDI provider)	Modify the `nms-multicast.ports.properties` file.
14443	TCP	`jboss.https.port`	Default HTTPS port	Modify the `nms-multicast.ports.properties` file.
14458	TCP	`jboss.jmsControl.port`	Default JMS Control port	Modify the `nms-multicast.ports.properties` file.

Table 81 shows the ports the NNM iSPI Performance for Traffic (Traffic Master component) uses on the management server. In case of port conflicts, almost all of these port numbers can be changed using the properties file located at: `%NnmDataDir%/shared/traffic-master/conf/nms-traffic-master.ports.properties`.

Table 81 Ports Used on the NNM iSPI Performance for Traffic Management Server (Traffic Master)

Port	Type	Name	Purpose	Change Configuration
12043	TCP	`jboss.https.port`	Default HTTPS port	Modify the `nms-traffic-master.ports.properties` file.
12080	TCP	`jboss.http.port`	Default HTTP port	Modify the `nms-traffic-master.ports.properties` file.
12083	TCP	`jboss.rmi.port`	Default RMI port	Modify the `nms-traffic-master.ports.properties` file.
12084	TCP	`jboss.jrmp.port`	Default JRMP port	Modify the `nms-traffic-master.ports.properties` file.
12085	TCP	`jboss.pooled.port`	Default pooled port	Modify the `nms-traffic-master.ports.properties` file.
12086	TCP	`jboss.socket.port`	Default socket port	Modify the `nms-traffic-master.ports.properties` file.
12087	TCP	`jboss.bisocket.port`	Default bi-socket port	Modify the `nms-traffic-master.ports.properties` file.
12088	TCP	`jboss.ws.port`	Default WS port	Modify the `nms-traffic-master.ports.properties` file.

Table 81 Ports Used on the NNM iSPI Performance for Traffic Management Server (Traffic Master) (cont'd)

Port	Type	Name	Purpose	Change Configuration
12089	TCP	`jboss.ejb3.port`	Default EJB3 port	Modify the `nms-traffic-master.ports.properties` file.
12099	TCP	`jboss.jnp.port`	Default JNDI/JNP port	Modify the `nms-traffic-master.ports.properties` file.
12458	TCP	`jboss.jmsControl.port`	Default JMS control port	Modify the `nms-traffic-master.ports.properties` file.

Table 82 shows the ports the NNM iSPI Performance for Traffic (Traffic Leaf component) uses on the management server. In case of port conflicts, almost all of these port numbers can be changed using the properties file located at: `%NnmDataDir%/shared/traffic-leaf/conf/nms-traffic-leaf.ports.properties`.

Table 82 Ports Used on the NNM iSPI Performance for Traffic Management Server (Traffic Leaf)

Port	Type	Name	Purpose	Change Configuration
11080	TCP	`jboss.http.port`	Default HTTP port - used for Web UI & Web Services	Modify the `nms-traffic-leaf.ports.properties` file.
11081	TCP	`jboss.https.port`	Default HTTPS port	Modify the `nms-traffic-leaf.ports.properties` file.
11083	TCP	`jboss.rmi.port`	Default port for RMI naming service	Modify the `nms-traffic-leaf.ports.properties` file.
11084	TCP	`jboss.jrmp.port`	Default RMI object port (JRMP invoker)	Modify the `nms-traffic-leaf.ports.properties` file.
11085	TCP	`jboss.pooled.port`	Default RMI pooled invoker port	Modify the `nms-traffic-leaf.ports.properties` file.
11086	TCP	`jboss.socket.port`	Default RMI remoting server connector port	Modify the `nms-traffic-leaf.ports.properties` file.

Table 82 Ports Used on the NNM iSPI Performance for Traffic Management Server (Traffic Leaf) (cont'd)

Port	Type	Name	Purpose	Change Configuration
11087	TCP	jboss.bisocket.port	Default messaging bi-socket connector	Modify the nms-traffic-leaf.ports.properties file.
11088	TCP	jboss.ws.port	Default jboss Web Service port	Modify the nms-traffic-leaf.ports.properties file.
11089	TCP	jboss.ejb3.port	Default EJB3 remoting connector port	Modify the nms-traffic-leaf.ports.properties file.
11099	TCP	jboss.jnp.port	Default bootstrap JNP service port (JNDI provider)	Modify the nms-traffic-leaf.ports.properties file.
11458	TCP	jboss.jmsControl.port	Default JMS Control port	Modify the nms-traffic-leaf.ports.properties file.

Table 83 shows the ports theNNM iSPI Performance for QA uses on the management server. In case of port conflicts, almost all of these port numbers can be changed using the properties file located at: %NnmDataDir%/shared/qa/conf/nms-qa.ports.properties.

Table 83 Ports Used on the NNM iSPI Performance for QA Management Server

Port	Type	Name	Purpose	Change Configuration
54040	TCP	jboss.http.port	Default HTTP port - used for Web UI & Web Services	Modify the nms-qa.ports.properties file.
54041	TCP	jboss.ejb3.port	Default EJB3 remoting connector port	Modify the nms-qa.ports.properties file.
54042	TCP	jboss.ws.port	Default jboss Web Service port	Modify the nms-qa.ports.properties file.
54043	TCP	jboss.https.port	Default HTTPS port	Modify the nms-qa.ports.properties file.
54044	TCP	jboss.jrmp.port	Default RMI object port (JRMP invoker)	Modify the nms-qa.ports.properties file.

Table 83 Ports Used on the NNM iSPI Performance for QA Management Server (cont'd)

Port	Type	Name	Purpose	Change Configuration
54045	TCP	`jboss.socket.port`	Default RMI remoting server connector port	Modify the `nms-qa.ports.properties` file.
54046	TCP	`jboss.jnp.port`	Default bootstrap JNP service port (JNDI provider)	Modify the `nms-qa.ports.properties` file.
54047	TCP	`jboss.bisocket.port`	Default messaging bi-socket connector	Modify the `nms-qa.ports.properties` file.
54048	TCP	`jboss.pooled.port`	Default RMI pooled invoker port	Modify the `nms-qa.ports.properties` file.
54049	TCP	`jboss.rmi.port`	Default port for RMI naming service	Modify the `nms-qa.ports.properties` file.
54091	TCP	`jboss.ssljmsControl.port`	Default SSL JMS Control port	Modify the `nms-qa.ports.properties` file.
54092	TCP	`jboss.sslbisocket.port`	Default SSL bi-socket port	Modify the `nms-qa.ports.properties` file.
54458	TCP	`jboss.jmsControl.port`	Default JMS Control port	Modify the `nms-qa.ports.properties` file.

Suggested Configuration Changes

Some common actions for performance improvements and how to complete them.

Messages and Solutions

Message: `The database pool has` *`number`* `available connections.`

Solution: This is a warning that means that the database pool is being heavily used. If this only appears for a short time then it probably indicates NNMi is under high load. If it appears frequently then it might indicate a performance problem.

Message: `The database connection pool is exhausted. NNM should be restarted immediately.`

Solution: This is a serious error indicating that the database pool has failed for some reason and NNMi cannot access the database. Restart `ovjboss` or contact support to fix the issue.

Message: `Detected` *`number`* `missing database connections. NNM should be restarted in the near future to correct this issue.`

Solution: This is a warning that NNMi detected inconsistencies in the database pool. Restart `ovjboss` at a convenient time to address this issue.

Message: `The disk location` *`location name`* `only has` *`number`*`% free.`

Solution: NNMi opens this warning after a disk location used by NNMi gets low on space.

Message: `The average system load is` *`number`*`.`

Solution: NNMi opens this warning after the system load passes a threshold. If it shows occasionally during major activity, you can ignore the message. However, if it shows constantly then investigate if the system is underpowered for the size environment or if there is some other process on the system consuming significant resources.

Message: `The system is low on swap space with` *`number`* `MB remaining.`

Solution: NNMi opens this message after NNMi detects the system is running low on swap space. You should increase the free swap space or reduce the use of swap.

Message: `The NNMi process is currently using` *`number`*`% of allowed open files.`

Solution: This message indicates that NNMi is running out of file handles. It is expected that less than 1,000 files will be open at any one time but certain environments might cause more to be required. If the number of open file handles keeps growing however that might indicate a defect in the product.

Message: `The NNMi CPU utilization is at 100%.`

Solution: This indicates that the ovjboss process has been consuming 100% CPU on the system for a significant amount of time. This might be expected for brief periods of high load but if this warning appears constantly then the system might be underpowered for the load.

Message: `The global manager` *`hostname`* `has` *`number`* `outstanding messages waiting to be delivered.`

Solution: This indicates that a global manager connected to this system is either down or unable to receive messages fast enough. If the global manager is just down for maintenance then it should recover when it comes back online however if this number goes over several hundred thousand then it might need to be manually cleared out (contact support).

Message: `The connection to the regional manager` *`regional name`* `is down.`

Solution: Warning message if communication to a regional manager is interrupted. If this appears for a short time then it isn't a cause for concern but if this message appears for an extended period then some troubleshooting might be required. The global manager will not be receiving any state changes from the regional while this condition exists.

Message: `There are` *`number`* `out of` *`number`* `maximum connections currently open to the embedded database.`

Solution: This message warns that the embedded database NNMi uses is approaching its limit of open connections. This might indicate the system is under excessive load or that too many SPIs are installed. It is recommended action such as shutting down SPIs is taken before this number reaches the maximum.

Message: `The memory region` *`region name`* `is at` *`number`*`% usage.`

Message: `The system has spent` *`number`*`% of total uptime in the` *`collector name`* `collector.`

Solution: Both these messages indicate that `ovjboss` is low on memory. The memory settings for the specified region should be checked against what is recommended for the environment scale and increased if the system has available memory.

Message: `Incoming trap rate is` *`number`* `traps/sec since` *`date`*`. All traps are blocked since` *`date`* `and will remain so until rate goes below` *`number`* `traps/sec.`

Solution: Consider using `trapFilter.conf` to configure filters to block traps based on both IP address and trap OID. See Blocking Incidents using the trapFilter.conf File on page 367.

Problems and Solutions

Problem: NNMi does not always interpret and display SNMP data and MIB strings correctly.

Solution: This is caused by NNMi not always knowing which character set to use to interpret this data. The result is that NNMi opens garbled strings from some SNMP traps and other octetstring data, such as `sysDescription`, `sysContact` and other data. The solution is to use the correct character set to interpret this data.

For SNMP traps and other octetstring data that result in garbled text opens due to using improper character sets, do the following:

a Edit the following file:

— *Windows:* `%NNM_PROPS%\nms-jboss.properties`

— *UNIX:* `$NNM_PROPS/nms-jboss.properties`

b Remove the comment (`#!` characters) from the line that begins as follows: `#!com.hp.nnm.sourceEncoding=`

c Set the `com.hp.nnm.sourceEncoding` JVM property to a comma-separated list of source encodings that your environment currently supports using the examples shown in the `nms-jboss.properties` file. These examples show combinations of the Shift_JIS, EUC_JP, UTF-8, and ISO-8859-1 character sets.

d Save your changes.

e From a command prompt, run **`ovstop`**.

f From a command prompt, run **`ovstart`**.

g To test your changes, resend the suspect trap to NNMi and make sure the garbled display problem no longer occurs.

If the garbled text involves binary data or data that cannot be interpreted for any reason, do the following to configure NNMi to display the strings in hexadecimal format:

a Edit the following file:

— *Windows*: `%NNMDATADIR%\shared\nnm\conf\nnmvbnosrcenc.conf`

— *UNIX*: `$NNMDATADIR/shared/nnm/conf/nnmvbnosrcenc.conf`

b Add the trap OID, varbind OID value combinations that NNMi opens in a garbled format. Also add the combinations from any varbind values you do not want NNMi to decode, such as binary data. Use the examples shown in the `nnmvbnosrcenc.conf` file as templates to configure your combinations. This tells NNMi to display the Custom Incident Attribute values in the Incident form using a hexadecimal value.

c Save your changes.

d From a command prompt, run **`ovstop`**.

e From a command prompt, run **`ovstart`**.

f Test your changes to make sure these changes result in a hexidecimal display of the formerly garbled strings.

Problem: NNMi opens messages about license keys not matching the host (the NNMi Management Server)

Solution: This happens after someone installs an NNMi license key created with an IP address that does not match the IP address of the NNMi management server. The solution is to remove the invalid license keys:

1. At a command prompt, enter the following command to open the `Autopass` user interface:

   ```
   nnmlicense.ovpl NNM -gui
   ```

2. On the left side of the Autopass window, click **Remove License Key**.
3. Select the invalid license keys.
4. Click **Remove**.

Repeat step 1 through step 4 for any other affected NNMi product integrations by replacing **NNM** with the affected product. For example, to work with licenses related to the NNM iSPI Network Engineering Toolset Software, use the following command to open the `Autopass` user interface:

```
nnmlicense.ovpl iSPI-NET -gui
```

For additional information about licensing, see Licensing NNMi on page 117.

Problem: NNMi maps show an ESXi server and the virtual machines and servers running on the ESXi server. NNMi shows all of these systems connected by a cloud symbol. This is only a problem if you do not want to see the ESXi server, including the virtual machines and servers, on the NNMi map.

Solution: If you do not want NNMi showing ESXi servers, including the virtual machines and servers, do the following:

1. Open the NNMi console.
2. Go to the topology map showing the nodes you want to delete; delete the nodes representing the ESXi server and the virtual machines and servers.
3. Click **Discovery Configuration** in the **Configuration** workspace.
4. Click the **Auto-Discovery** Rules tab.
5. Create a new auto-discovery rule.
6. Enter a relatively low number in the `Ordering` field to give this rule a high precedence. Make sure the `Discover Included Nodes` check box is not checked.
7. Add a new IP address range for this rule.
8. For the nodes representing the ESXi server and the virtual machines and servers, add either the individual IP addresses or the IP address ranges for these nodes; then change the `Range Type` to be `Include by Rule` rather than `Ignore by Rule`.
9. Click **Save and Close** three times to save your work.

➤ These steps will not delete any existing nodes; however, it prevents future discovery of nodes within the excluded IP address range.

Problem: NNMi maps show a Linux server instead of ESXi servers and nodes.

Solution: You have deployed VMWARE on a Linux server with the Net-SNMP agent enabled. If you want NNMi to discover and show ESXi servers, you must complete a bare metal installation for the ESXi servers and nodes. For more information see http://www.vmware.com.

Problem: NNMi maps show ESXi devices as having `No SNMP` instead of showing them as ESXi devices.

Solution: The ESXi SNMP agent must be installed and enabled for NNMi to discover and map ESXi servers and nodes. Perhaps you uninstalled or disabled the ESXi SNMP agent. To remedy this, install or enable the ESXi SNMP agent. For more information see http://www.vmware.com.

Problem: I am using NNMi with an Oracle database. I configured a large node group that results in an error when generating a node group map.

Solution: This could occur if you configure NNMi as follow:

- You use NNMi with an Oracle database.
- You create a top level node group containing child node groups.
- Any of the child node groups contain 1000 or more members.
- You select either or both of the following selections in the **Node Group Map Settings**->**Connectivity**->**Node Group Connectivity** section for these node groups:
  - **Nodes to Node Groups**
  - **Node Groups to Node Groups**

To remedy this, limit the child node groups to less than 1000 members or do not select either or both **Nodes to Node Groups** or **Node Groups to Node Groups** in the **Node Group Map Settings**->**Connectivity**->**Node Group Connectivity** section for these node groups.

Problem: For some Cisco devices using PAgP (Port Aggregation Protocol), if a link goes down that is part of a port aggregation, NNMi might consider the port on that device to no longer be part of the port aggregation. This can result in NNMi not reporting the degraded state of the port aggregation.

Solution: Beginning with NNMi 9.0x Patch 4, there is a feature that helps NNMi better manage Cisco devices that use PAgP. You can configure this NNMi feature to attempt to determine if a down interface is still configured to be a part of a port aggregation. To enable this feature, do the following:

1 Edit the following file:

   - *Windows*: `%NNM_PROPS%\nms-disco.properties`
   - *UNIX*: `$NNM_PROPS/nms-disco.properties`

2 Look for the `enablePagpOperDownHeuristic` entry, which is similar to the following line:

```
#!com.hp.ov.nms.disco.enablePagpOperDownHeuristic=false
```

To enable the `enablePagpOperDownHeuristic`, change the line as follows:

```
com.hp.ov.nms.disco.enablePagpOperDownHeuristic=true
```

Make sure to remove the **#!** characters located at the beginning of the line.

3. Restart the NNMi management server.
   - a. Run the **ovstop** command on the NNMi management server.
   - b. Run the **ovstart** command on the NNMi management server.

Problem: You encounter pop-up dialog issues when using Internet Explorer 8 and the Internet Explorer ESC (Enhanced Security Configuration)

Solution: Windows 2003 and Windows 2008 server offer a feature called Internet ESC (Explorer Enhanced Security Configuration) in Internet Explorer 8. After this feature is enabled (this feature is currently enabled by default) all pop-up dialogs and windows are tested against a list of trusted sites. If the URL associated with the pop-up is not in the list of trusted sites, all of the controls in the dialog or window are disabled. For example, when this happens, clicking on the **OK**, **Apply**, and **Cancel** buttons has no effect.

Generally, with ESC enabled, whenever you open a dialog, the browser prompts you as to whether you want to enable the URL associated with the pop-up as a trusted site. To proceed, you must allow the URL. If you do not allow the URL, the dialog controls will not work and you will see the prompt whenever the dialog or window is opened. Eventually the nagging ceases because all important URLs will have been added to the list of Trusted Sites. One special URL that must be placed in the list is `about:blank`.

You can get into a situation where the NNMi console does not work. If, at some point, you click the **Don't show me this message again** check box in the `Trusted Sites` prompt, subsequent prompts will not be issued. If you had done this before installing NNMi, the NNMi console would hardly function: Dialogs would not pop up, but the controls in the dialog would not work. For example, if you opened the **Help**->**About** dialog, the **OK** button would not close the dialog. Also, all of the table view filter dialogs would not work. In the latter case, this is because the `about:blank` URL is not in the list of Trusted Sites.

The are several ways to resolve this problem:

— "Disable the Internet Explorer Enhanced Security Configuration feature using Server Manager.

— "Add the required URLs to the Trusted Security Sites using the **IE**->**Tools**->**Options**->**Security** tab; specifically, add `about:blank`.

— "Make sure the IE pop up window to permit additions to the Trusted Security Sites is enabled.

Glossary

A

account

See user account.

active cluster node

See active server.

active server

The server currently running the NNMi processes in an application failover or high availability configuration.

address hint

See discovery hint.

application failover

In NNMi, the optional capability (configured by the user and utilizing jboss clustering support) that transfers control of NNMi processes to a standby server if the currently active server fails.

ARP cache

The ARP (Address Resolution Protocol) cache is an operating system table that maps Data Link Layer (OSI Layer 2) addresses to Network Layer (OSI Layer 3) addresses. Data Link Layer addresses are typically MAC addresses, while Network Layer addresses are typically IP addresses. In rule-based discovery, NNMi uses ARP cache entries on discovered nodes (as well as other techniques) to find additional nodes that can be checked against the current discovery rules.

auto-discovery

See rule-based discovery.

C

Causal Engine

NNMi technology that applies root cause analysis (RCA) to network symptoms, using a causality-based approach. Causal Engine RCA is triggered by certain occurrences, including changes detected as a result of state polling, SNMP traps, and specific incidents. The Causal Engine uses RCA to determine the status of managed objects, to formulate conclusions about them, and to generate root cause incidents.

causality

Denotes the relationship between one event (the cause) and another event (the effect), which is the direct consequence (result) of the first. NNMi uses causality analysis algorithms to analyze event cycles and identify solutions for resolving network issues.

cluster

In an NNMi context, a grouping of hardware and software, linked by high availability technology or by using jboss clustering capabilities, that works together to ensure functional and data continuity if components overload or fail. The computers in a cluster are commonly connected to each other through high speed LANs. Clusters are usually deployed to improve availability, performance, or both.

cluster member or node

In an NNMi context, a system within a high availability or jboss cluster that has been or will be configured to support NNMi high availability or application failover.

community string

A password-like mechanism used in SNMPv1 and SNMPv2c implementations to authenticate SNMP queries to SNMP agents. The community string is passed in cleartext in SNMP packets, making it vulnerable to packet sniffing. SNMPv3 provides stronger security mechanisms for authentication.

conclusion

In NNMi, supporting detail generated and used by the Causal Engine that sheds further light on how the Causal Engine determined status and root cause incidents for a managed object.

console

See NNMi console.

controller

In NNMi application failover, a JGroups term for the cluster member that has the master cluster state. JGroups determines which member of the cluster is the controller based on the lowest IP address.

D

discovery hint

An IP address found by NNMi using an SNMP ARP cache query; a CDP, EDP, or other discovery protocol query; or a ping sweep. NNMi further queries IP addresses found as discovery hints, then checks the results against the current discovery rules in rule-based discovery.

discovery process

The process by which NNMi gathers information about network nodes so that they can be placed under management. Initial discovery runs as a two-phase process, returning device inventory information and then network connectivity information.

After initial discovery, the discovery process is ongoing. In list-based discovery, this means devices in the list of seeds will be updated if their configuration changes. In rule-based discovery, new devices will also be added if they match current discovery rules. Discovery can also be initiated on demand for a device or set of devices from the NNMi console or from the command line.

See also spiral discovery, rule-based discovery, and list-based discovery.

discovery rule

A range of user-defined IP addresses, system object IDs (OIDs), or both used to limit the rule-based discovery process. Configure discovery rules in the **Discovery Configuration** portion of the NNMi console under **Auto-Discovery Rules**. See also rule-based discovery.

discovery seed

See seed.

E

embedded database

The database included with NNMi. NNMi can also be configured to use an external Oracle database instead of the embedded database for most of its tables. See also PostgreSQL.

episode

A term used in NNMi root cause analysis to refer to a specific duration, triggered by a primary failure, during which secondary failures are suppressed or are correlated under the primary failure.

F

fault polling

A key NNMi monitoring activity, in which NNMi issues ICMP pings, SNMP read-only queries of status MIBs, or both for its managed interfaces, IP addresses, and SNMP agents to determine the state of each managed object. Users can customize the types of fault polling performed for different interface groups, node groups, and nodes under **Monitoring Configuration** in the **Configuration** workspace of the NNMi console. Fault polling is a subset of state polling.

G

global network management

A distributed deployment of NNMi with one or more global managers consolidating data from one or more geographically distributed regional managers.

global manager

The NNMi management server in a global network management deployment that consolidates data from distributed NNMi regional manager servers. The global manager provides a unified view of topology and incidents across the whole environment. A global manager must have an NNMi Advanced license.

H

HA

See high availability.

HA resource group

In modern high availability environments such as HP ServiceGuard, Veritas Cluster Server, or Microsoft Cluster Services, applications are represented as compounds of resources, such as the application itself, its shared file systems and a virtual IP address. The resources consist of an *HA resource group*, which represents an application running in a cluster environment.

high availability

Used in this guide to refer to a hardware and software configuration that provides for uninterrupted service if part of the configuration fails. High availability (HA) means that the configuration has redundant components to keep applications running at all times even if a component fails. NNMi can be configured to support one of several commercially available HA solutions. Contrast with application failover.

HP Network Node Manager i Software

An HP software product (abbreviated NNMi) designed to aid network administration and to consolidate network management activities, including the ongoing discovery of network nodes, monitoring events, and network fault management. Primarily accessed from the NNMi console.

I

ICMP

See Internet Control Message Protocol.

incident

In NNMi, a notification of an occurrence related to your network, displayed in NNMi console incident views and forms. NNMi includes a number of **Incident Management** and **Incident Browsing** views that enable users to filter incidents based on incident attributes. Most incident views display incidents generated directly by NNMi (sometimes called *management events*). NNMi also includes views for browsing incidents generated from SNMP traps and from NNM 6.x/7.x events.

interface

A physical port used to connect a node to the network.

interface group

One of NNMi's primary filtering techniques, where interfaces are grouped together to apply settings to a group or filter visualizations by group. Interface groups can be used for any or all of the following: configuring monitoring, filtering table views, and customizing map views. See also node group.

Internet Control Message Protocol

One of the core protocols of the Internet protocol suite (TCP/IP). ICMP ping is used by NNMi along with SNMP queries for state polling.

iSPI

See NNM iSPI.

L

L2

See Layer 2.

L3

See Layer 3.

Layer 2

Refers to the Data Link Layer of the multi-layered communication model, Open Systems Interconnection (OSI). The data link layer moves data across the physical links in the network. NNMi Layer 2 views provide information about the physical connectivity of devices.

Layer 3

Refers to the Network Layer of the multi-layered communication model, Open Systems Interconnection (OSI). The network layer is concerned with knowing the address of the neighboring nodes in the network, selecting routes, and quality of service. NNMi Layer 3 views provide information about connectivity from a routing perspective.

list-based discovery

A process, based on a list of seeds, that discovers and returns detailed network information *only about the nodes that you specify as seeds*. List-based discovery maintains a limited network inventory for specific queries and tasks. Contrast with rule-based discovery. See also discovery process and spiral discovery.

logical volume

A computer storage virtualization term referring to an arbitrarily sized space in a volume group that can be used as a separate file system or as a device swap space. Several of the high availability products supported by NNMi use logical volumes in their shared file systems.

M

management server

The NNMi management server is the computer system on which the NNMi software is installed. The NNMi processes and services run on the NNMi management server. (Prior NNM revisions used the term “NNM management station” for this system.)

MIB

See Management Information Base.

Management Information Base

In SNMP, the collection of data about the managed network, organized hierarchically. The data objects within the management information base refer to characteristics of managed devices. NNMi collects network management information by making SNMP queries to and receiving SNMP traps from managed nodes using MIB data objects (sometimes called “MIB objects,” “objects,” or “MIBs”).

N

NNM 6.x/7.x events

An NNMi term for events forwarded from older NNM management stations to NNMi. NNMi provides incident views for browsing the incidents that NNMi generates from these forwarded events.

NNM iSPI

A Smart Plug-in within the I family. An NNM iSPI adds functionality to NNMi for a specific technology such as MPLS or for a specific domain such as network engineering.

NNMi

See HP Network Node Manager i Software.

NNMi console

The NNMi user interface. Operators and administrators use the NNMi console for network management tasks in NNMi.

node

In the network context, a computer system or device (for example, printer, router, or bridge) in a network. While nodes that are able to respond to SNMP queries provide NNMi with the most comprehensive management information, NNMi can also perform restricted management of non-SNMP nodes.

node group

One of NNMi’s primary filtering techniques, where nodes are grouped together to apply settings to a group or filter visualizations by group. Node groups can be used for any or all of the following: configuring monitoring, filtering table views, and customizing map views. See also interface group.

O

OID

See Object Identifier.

Object Identifier

In SNMP, a numerical sequence that identifies a MIB data object. An OID consists of numbers separated by dots in which each number represents a particular data object at that level of the MIB hierarchy. The OID is the numerical equivalent of the MIB object name, for example, the MIB object name `iso.org.dod.internet.mgmt.mib-2.bgp.bgpTraps.bgpEstablished` is equivalent to its OID `1.3.6.1.2.1.15.0.1`.

ovstatus command

A command that reports the current status of the NNMi managed processes. Can be invoked from the NNMi console (**Tools** > **NNMi Status**) or at a command prompt. See the *ovstatus* reference page, or the UNIX manpage.

ovstart command

A command that starts the NNMi managed processes. Invoked at a command prompt. See the *ovstart* reference page, or the UNIX manpage.

ovstop command

A command that stops the NNMi managed processes. Invoked at a command prompt. See the *ovstop* reference page, or the UNIX manpage.

P

ping sweep

A network probe technique that sends ICMP ECHO requests to multiple IP addresses to determine which addresses are assigned to responsive nodes. When enabled in rule-based discovery, NNMi can use ping sweep on configured IP address ranges to find additional nodes. Some network administrators block ICMP ECHO requests because ping sweeps can be used in denial-of-service attacks.

port

In a network hardware context, a connector for passing information into and out of a network device.

PostgreSQL

An open source relational database that NNMi uses by default to store information such as topology, incidents, and configuration information. NNMi can also be configured to use Oracle instead of PostgreSQL for most of its tables.

public key certificate

Used in network security and encryption, a file that incorporates a digital signature to bind together a public key with identity information. A certificate is used to verify that a public key belongs to an individual or organization. NNMi uses SSL certificates, which contain a public key and a private key, for authentication and encryption of client-server communication.

R

RCA

See root cause analysis.

region

In NNMi, a grouping of devices for the purpose of configuring communication settings such as timeout values and access credentials.

regional manager

The NNMi management server in a global network management deployment that provides discovery, polling and trap reception for devices and forwards information to the global manager.

role

See user role.

rule

See discovery rule.

rule-based discovery

Often called *auto-discovery*, NNMi can use rule-based discovery to seek out nodes that NNMi should add to its database, following user-specified discovery rules. NNMi looks for discovery hints in data from discovered nodes, then checks these candidates against the specified discovery rules. Configure discovery rules in the **Discovery Configuration** portion of the NNMi console under **Auto-Discovery Rules**. Contrast with list-based discovery.

root cause analysis

In NNMi, root cause analysis (RCA) refers to a class of problem solving methods used by NNMi to determine root causes for network issues. In NNMi, the root cause is the actionable issue that will resolve associated problem symptoms if it is addressed. NNMi uses the identification of the root cause in two key ways: to notify the user of the actionable problem and to suppress reporting of secondary problem symptoms until the root cause issue has been resolved. Determination of root cause might result in status changes for managed objects, generation of root cause incidents, or both.

A example of how NNMi uses RCA is the scenario in which a managed router fails, and managed nodes on the other side of the router from the NNMi management server can no longer respond to state polling queries. NNMi uses RCA to determine that the state polling failures are secondary problem symptoms. It reports the router failure as the root cause incident and refrains from reporting the problem symptoms for the downstream nodes until the root cause router failure is resolved.

root cause incident

An NNMi incident in which the *Correlation Nature* attribute is set to *Root Cause*. NNMi uses root cause analysis (RCA) to establish the root cause incident as the actionable issue that will resolve associated problem symptoms if it is addressed. See root cause analysis.

S

seed

A network node that helps NNMi discover your network by acting as a starting point for the network discovery process. For example, a seed might be a core router in your management environment. Each seed is identified by an IP address or host name. Unless rule-based discovery has been configured, NNMi's discovery process is limited to list-based discovery of specified seeds.

seeded discovery

See list-based discovery.

Simple Network Management Protocol

A simple protocol operating at the application layer (Layer 7) of the OSI model, by which management information for a network element can be inspected or altered by remote users. SNMP is the predominant protocol used by NNMi to exchange network management information with agent processes on managed nodes. NNMi supports the three most common versions of SNMP: SNMPv1, SNMPv2c, and SNMPv3.

SNMP

See Simple Network Management Protocol.

SNMP trap

Network management using polling (solicited responses from SNMP agents) is an SNMP design principle that promotes simplicity. However, the protocol does provide for communication of unsolicited messages from SNMP agents to the SNMP manager process (in this case, NNMi). Unsolicited agent messages are known as “traps” and are generated by SNMP agents in response to internal state changes or fault conditions. NNMi generates incidents from received SNMP traps, displayed in the **SNMP Traps** incident browsing view.

SNMP trap storm

A high number of unsolicited SNMP agent messages that can overwhelm an SNMP manager process (in this case, NNMi). You can configure SNMP trap storm thresholds in NNMi, using the `nnmtrapconfig.ovpl` command. NNMi blocks traps when incoming trap rates exceed the specified threshold rate, until the trap rates fall below the re-arm rate.

spiral discovery

NNMi’s ongoing refinement of network topology information, which includes information about inventory, containment, relationships, and connectivity in networks managed by NNMi. See also discovery process, rule-based discovery, and list-based discovery.

state

NNMi generally uses the term **state** for self-reported managed object responses related to MIB II `ifAdminStatus`, MIB II `ifOperStatus`, performance, or availability. Contrast with status.

state polling

The directed monitoring performed by NNMi’s State Poller, which uses ICMP ping and SNMP queries to retrieve fault, performance, component health, and availability data from managed objects. See also fault polling.

status

In NNMi, an attribute of a managed object that indicates its overall health. The status is calculated by the Causal Engine from the managed object’s outstanding conclusions. Contrast with state.

sysObjectID

See system object ID.

system object ID

In NNMi, a specialized term for an SNMP Object Identifier that identifies a model or type of network element. The system object ID is part of a network element’s MIB object, which is queried by NNMi from individual nodes during discovery. Examples of network element types that can be classified by their system object IDs include any member of the HP ProCurve switch family, an HP J8715A ProCurve Switch, and an HP SNMP agent for HP IPF systems. Other vendors’ network elements can be likewise classified according to their system object IDs. A key use for the system object ID is in defining NNMi Device Profiles, which specify characteristics of network elements that can be deduced once a network element’s type is known.

system account

In NNMi, a special account provided for use during NNMi installation. After installation, the NNMi system account should only be used for command-line security and for recovery purposes. Contrast with user account.

T

topology (network)

In communication networks, a schematic description of the arrangement of a network, including its nodes and connections.

trap

See SNMP trap.

U

unconnected interface

From NNMi’s perspective, an unconnected interface is an interface that is not connected to another device discovered by NNMi. By default, the only unconnected interfaces that NNMi monitors are those that have IP addresses *and* are contained in nodes from the **Routers** node group.

user account

In NNMi, a way to provide access to NNMi for users or groups of users. NNMi user accounts are set up in the NNMi console and implement predetermined user roles. See system account and user role.

user role

As part of setting up user access, the NNMi administrator assigns a pre-configured user role to each NNMi user account. User roles determine which user accounts can access the NNMi console, as well as which workspaces and actions are available to each user account. NNMi provides the following hierarchical user roles, which are predefined by the program and cannot be modified: *Administrator*, *Web Service Client*, *Operator Level 2*, *Operator Level 1*, *Guest*. See also user account.

V

virtual host name

The host name associated with a virtual IP address.

virtual IP address

An IP address that is not tied to any particular network hardware, used in high availability configurations to send uninterrupted network traffic to the most appropriate server based on current failover or load-balancing needs.

volume group

A computer storage virtualization term referring to one or more disk drives that are configured to form a single large storage area. Several of the high availability products supported by NNMi use volume groups in their shared file systems.

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click *here*.

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 9.1x Patch 5

Document title: *NNMi Deployment Reference*

Feedback:

Java™
COMPATIBLE