

HP Network Node Manager i Software

For the HP-UX, Linux, and Solaris Operating Systems

Software Version: 9.10

Installation Guide

Manufacturing Part Number: TB774-90005

Document Release Date: March 2011

Software Release Date: March 2011



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2008–2011 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

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

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

UNIX® is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

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

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

Acknowledgements

This product includes software developed by the Apache Software Foundation.
(<http://www.apache.org>)

This product includes software developed by the Indiana University Extreme! Lab.
(<http://www.extreme.indiana.edu>)

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

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 User ID and sign in. To register for an HP Passport User 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
- 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

| | | |
|----------|--|-----------|
| 1 | Introducing HP Network Node Manager i Software | 7 |
| | About This Guide | 7 |
| | Environment Variables Used in This Document | 8 |
| 2 | Preinstallation Checklists | 9 |
| | Supported Hardware and Software | 9 |
| | NNMi Management Server Preparation | 11 |
| | Database Installation | 13 |
| | Check for a Well-Configured DNS | 15 |
| | NNMi Quick Start Configuration Wizard | 18 |
| 3 | Installing and Enabling NNMi | 19 |
| | Installing NNMi | 19 |
| | Silently Installing NNMi | 24 |
| | Silent Installation Using a Sample oinstallparams.ini File | 25 |
| | Silent Installation Using an oinstallparams.ini File from a Prior Installation . . . | 26 |
| | Using the Quick Start Configuration Wizard | 29 |
| | Licensing NNMi | 34 |
| | Preparing to Install a Permanent License Key | 34 |
| | Checking the License Type and the Number of Managed Nodes | 34 |
| | Obtaining and Installing a Permanent License Key | 35 |
| | Using Autopass and your HP Order Number (not possible behind a firewall) . . . | 35 |
| | From the Command Line | 35 |
| | Obtaining Additional License Keys | 36 |
| | Removing NNMi | 37 |
| | Accessing NNMi Installation Log Files | 39 |
| 4 | Getting Started with NNMi | 41 |

| | |
|---|-----------|
| Accessing NNMi | 41 |
| NNMi Help | 44 |
| Configuring Network Discovery | 45 |
| Configuring Community Strings | 46 |
| Configuring Auto-Discovery Rules | 47 |
| Checking Discovery Progress | 49 |
| A Additional Information | 51 |
| Obtaining or Setting the Official Fully-Qualified Domain Name | 51 |
| Configuring an X Server for Installation | 52 |
| Enabling the Web Browser for the NNMi Console | 52 |
| Resetting the System Account Password | 54 |
| B Troubleshooting Installation and Initial Startup | 55 |
| Installation Problems | 55 |
| Initial Startup Problems | 57 |
| Glossary | 63 |

1 Introducing HP Network Node Manager i Software

HP Network Node Manager i Software contains a toolset to help you maintain a healthy network across your organization. NNMi can discover network nodes (such as switches and routers) on an ongoing basis, providing an up-to-date representation of the network topology. As NNMi maintains an accurate picture of the network, it also helps you handle problems through **management by exception**—the ability to pinpoint network problems by using event correlation and root cause analysis (RCA). Unlike other network management software, NNMi applies sophisticated RCA algorithms to an accurate, ever-changing view of network topology to support dynamic fault management.

About This Guide

This guide helps you to install NNMi and to perform basic NNMi configuration. This guide includes the steps for single-server installation and for using the **Quick Start Configuration Wizard** immediately after installing NNMi. This guide also provides a simplified set of steps to help you start managing your network using the spiral discovery process.

HP developed the procedures in this guide to help you be successful in your initial deployment of NNMi. After you understand more about configuring basic NNMi processes (such as spiral discovery and polling), you can tune and expand your network management solution over time, thereby achieving a comprehensive management strategy.

HP designed this guide to help you get started. More detailed information about using NNMi can be found in the NNMi help (see [NNMi Help](#) on page 44). Detailed information about customizing the NNMi configuration can be found in the *HP Network Node Manager i Software Deployment Reference*.

Environment Variables Used in This Document

This document uses the following NNMi environment variables to reference file and directory locations.

UNIX

- \$NnmInstallDir: /opt/OV
- \$NnmDataDir: /var/opt/OV



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

For information about other NNMi environment variables that you can source, see the *HP Network Node Manager i Software Deployment Reference*.

2 Preinstallation Checklists

This chapter contains checklists for tasks to complete before installing NNMi, and includes where to find a list of supported hardware and software.

Supported Hardware and Software

Before installing NNMi, read the information about supported NNMi hardware and software shown in [Table 1](#) on page 9.



For the most up-to-date versions of all documents listed in [Table 1](#), go to:

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

You must have an HP passport ID to access this web site.

Table 1 Software and hardware preinstallation checklist

| Complete (y/n) | Documentation to Read |
|---------------------------|---|
| | <i>HP Network Node Manager i Software Deployment Reference</i> A web-only document providing advanced deployment and configuration information for NNMi enterprise installations available at http://h20230.www2.hp.com/selfsolve/manuals |
| | <i>HP Network Node Manager i Software Upgrade Reference</i> A web-only document providing advanced upgrade information for NNMi enterprise installations available at http://h20230.www2.hp.com/selfsolve/manuals |

Table 1 Software and hardware preinstallation checklist

| Complete (y/n) | Documentation to Read |
|-----------------------|---|
| | <i>HP Network Node Manager Software Release Notes</i> <ul style="list-style-type: none">• Filename = releasenotes_en.html• Product media = Top-level or root directory• NNMi console = Help > Documentation Library > Release Notes |
| | <i>HP Network Node Manager i Software System and Device Support Matrix</i> <ul style="list-style-type: none">• Filename = supportmatrix_en.html• Product media = Top-level or root directory• NNMi console = Linked from the release notes |



HP updates the *HP Network Node Manager i Software System and Device Support Matrix* when new information becomes available. Before you begin to deploy NNMi, check for the most recent *HP Network Node Manager i Software System and Device Support Matrix* for your version of the software at:

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

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

NNMi Management Server Preparation

An NNMi management server is a server on which the NNMi software is installed. Each NNMi management server must be a 64-bit machine. To learn more about hardware prerequisites, see [Supported Hardware and Software](#) on page 9.

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.

You can install NNMi from the console or by using an XServer with the `$DISPLAY` variable set appropriately.

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>

Before you install NNMi on the NNMi management server, complete the checklist in [Table 2](#). If you plan to use an Oracle database instance to store the NNMi data, see [Database Installation](#) on page 13.

Table 2 NNMi management server preinstallation checklist

| Complete (y/n) | NNMi Management Server Preparation |
|-----------------------|--|
| | <p>Determine the official fully-qualified domain name (FQDN) of the NNMi management server. You will need this information during installation. The official FQDN must meet the following requirements:</p> <ul style="list-style-type: none"> • It must be DNS resolvable to the NNMi management server. • It must be available for accessing the NNMi management server from other computers on your network. <p>For more information, see Obtaining or Setting the Official Fully-Qualified Domain Name on page 51.</p> |
| | <p>If you plan to install NNMi from an XServer, run the <code>xclock</code> command to verify that you have the <code>XDisplay</code> variable configured correctly. If the clock does not appear, see Configuring an X Server for Installation on page 52.</p> |
| | <p>If you plan to install patches during the NNMi installation, unzip any zipped patch files. Place the unzipped files in a folder on the target server.</p> |
| | <p>Install and enable a supported web browser. See Supported Hardware and Software on page 9 and Enabling the Web Browser for the NNMi Console on page 52.</p> |
| | <p>Dynamic Host Configuration Protocol (DHCP) users: Make sure that the NNMi management server is consistently assigned the same IP address.</p> |

Table 2 NNMi management server preinstallation checklist

| Complete (y/n) | NNMi Management Server Preparation |
|-----------------------|---|
| | <p>NNMi uses several well-known ports that must be available on the NNMi management server before installing NNMi. Verify that all of the following ports are available before installing NNMi:</p> <ul style="list-style-type: none">• TCP Ports 80, 443, 1098, 1099, 3873, 4444 through 4446, 4457 through 4460, 5432, 7800 through 7810, 8083, 8886, and 8887• UDP Port 162 <p>For more information about resolving port conflicts, see the <i>HP Network Node Manager i Software Deployment Reference</i>.</p> |
| | <p>If you require a non-US-English locale, configure the NNMi management server to support the locale you require (such as Japanese). For more information about the locales that NNMi supports, see the <i>HP Network Node Manager i Software System and Device Support Matrix</i>.</p> |
| | <p>If you need information about setting up the Global Network Management or Application Failover features, see the <i>HP Network Node Manager i Software Deployment Reference</i>.</p> |

Database Installation

NNMi supports the following database options:

Embedded database Provided with the NNMi product. This database has no installation prerequisites.

Oracle database instance for NNMi Created by an Oracle database administrator. To install an Oracle database instance for NNMi, complete the checklist in [Table 3](#).

Table 3 Oracle database preinstallation checklist

| Complete (y/n) | Oracle Database Preparation |
|---------------------------|---|
| | To improve performance and to avoid a port conflict with the NNMi software, Oracle must be installed on a separate server from the NNMi management server. For more information, see Problem: jboss port contention on page 58. |
| | Working with your Oracle database administrator, install an Oracle database according to the instructions provided by Oracle. |

Table 3 Oracle database preinstallation checklist (cont'd)

| Complete (y/n) | Oracle Database Preparation |
|-----------------------|--|
| | Create a database instance for NNMi. Make sure that you know the host name of the Oracle server and the database instance name; you will need this information during the NNMi installation. |
| | <p>Assign a tablespace size depending on the number of nodes in your installation. For example, for an 18,000 node network, set your beginning tablespace size for 12 gigabytes (GB). Set the option for unlimited tablespace extensions in increments of 12 GB.</p> <p>The database requirement grows as NNMi discovers additional nodes, so watch this growth carefully and expand your configured tablespace size when necessary.</p> |
| | <p>Create an Oracle user with the following permissions:</p> <ul style="list-style-type: none">• Create sequence• Create session• Create table• Create view• FLASHBACK ANY TABLE <p>HP recommends the FLASHBACK ANY TABLE permission, since this enables NNMi to create restore points during migration.</p> <p>Make note of the Oracle user name and password; you will need this information during the NNMi installation.</p> |

Check for a Well-Configured DNS

NNMi uses **Domain Name System (DNS)** to determine relationships between hostnames and IP addresses. This can result in a large number of name service queries when Auto-Discovery is enabled.

Make sure that your DNS servers are well configured to prevent long delays when resolving name service queries. This means that the DNS server responding to NNMi name service queries has these characteristics:

- The DNS server is an authoritative server and does not forward DNS requests.
- The DNS server has consistent hostname-to-IP address mappings and IP address-to-hostname mappings.

If the network uses multiple DNS servers, all of them must respond consistently to all name service queries.



Round-robin DNS (used to do load balancing of web application servers) is not appropriate because any given hostname can map to different IP addresses over time.



To improve the response time for `nslookup`, deploy a secondary DNS service on the NNMi management server or another system on the same subnet as the NNMi management server. Configure this secondary DNS service to mirror the information from the primary DNS service. Another option is to use the `/etc/hosts` file instead of DNS in small environments.

On the NNMi management server, make sure the following are configured appropriately for your environment:

- When an `nslookup` command is not successful, the `/etc/hosts` file takes precedence. Make sure that the host file contains a minimum of two entries:

```
127.0.0.1 (loopback loghost)
```

```
<NNMi management server IP Address> <NNMi management server Name>
```

The NNMi management server name referred to in the previous paragraph is the official fully-qualified domain name (FQDN) of the NNMi management server set during installation. The NNMi management server IP Address referred to in the previous paragraph is the IP address of the FQDN for the NNMi management server.

- `nsswitch.conf` file configuration: Make sure that the `nslookup` search conforms to the `nslookup` command search order configured in the `nsswitch.conf` file. See the `nsswitch.conf(4)` manpage provided with your operating system.

- `resolv.conf` file: Make sure that all identified DNS servers provide consistent hostname-to-IP address mappings and IP address-to-hostname mappings. See the `resolv.conf(4)` manpage provided with your operating system.

If you know that there are problems with the DNS configuration in your network domain (hostnames or addresses that do not resolve properly), instruct NNMi to avoid `nslookup` requests for unimportant devices. The benefits of doing this are as follows:

- Speed up Spiral Discovery.
- Keep network traffic generated by NNMi to a minimum.

To identify problem devices to NNMi, create the following two files before configuring NNMi discovery. NNMi never issues a DNS request for hostnames or IP addresses identified in these files:

- `hostnlookup.conf` (enter fully-qualified domain names or wildcards that identify groups of hostnames)
- `ipnlookup.conf` (enter IP addresses or wildcards that identify groups of IP addresses)

Use an ASCII editor to populate the files. Place the files in the following location on the NNMi management server: `$NnmDataDir/shared/nnm/conf/`

NNMi Quick Start Configuration Wizard

You can run the **Quick Start Configuration Wizard** immediately after installation to configure NNMi in a limited (or test) environment. If you plan to use this wizard, complete the checklist in [Table 4](#).

Table 4 NNMi Quick Start Configuration Wizard preinstallation checklist

| Complete (y/n) | Preparation for Initial Configuration |
|-----------------------|--|
| | Determine a limited IP range for Auto-Discovery. For information about determining how many devices you can install based on license limitations, see Licensing NNMi on page 34. |
| | Determine IP addresses for discovery seeds. For information about seeds, see About Discovery Seeds and Auto-Discovery Rules on page 29. |
| | Obtain the read-only SNMP community strings for the nodes within the discovery range from your network administrator. |
| | Determine a user name and password for an NNMi administrator account. |

3 Installing and Enabling NNMi

This chapter guides you through the process of installing NNMi. The first time that you install NNMi, the installation program creates a file that stores your responses to the installation questions. For subsequent installations on other servers, you can use that file as input to a silent installation. For more information, see [Silently Installing NNMi](#) on page 24.

If you are installing NNMi for the first time, it is a good idea to accept all of the default configuration parameters during the installation process. In this way, you can work with the default configurations; then add customization as you expand your managed network over time.

- ▶ *Linux and Windows:* You can use the installation procedure shown in this chapter to install NNMi on virtual machines, such as servers running VMWare. See the *HP Network Node Manager i-series Software System and Device Support Matrix* for more information on virtual machines and their software and hardware requirements.

Installing NNMi

Make sure to complete the preinstallation requirements (see [Chapter 2, Preinstallation Checklists](#)).

- ▶ If you plan to store NNMi data in an Oracle database, you need to work with your Oracle database administrator. See [Database Installation](#) on page 13.

Unless you are upgrading from a supported version of NNMi, remove all previous NNMi installations. See [Removing NNMi](#) on page 37 for instructions about removing NNMi. See *Updating from NNMi 9.0x* in the *HP Network Node Manager i Software Deployment Reference* to view the supported upgrade paths.

Before installing NNMi on a Linux server, you can verify that the installation files are original HP-provided code and have not been manipulated by a third-party by using the HP Public Key and verification instructions provided on the following HP web site:

<https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning>.


To install NNMi, follow these steps:

- 1 Log on as a user with root privileges to the system where you plan to install NNMi.
- 2 Insert the NNMi installation media into the DVD drive.
- 3 Make sure that the DVD drive is mounted; then use the `cd` command to change to the `/cdrom` directory.
- 4 Enter the following command:


```
./setup.bin
```

The installation initialization process prompts you for the language you want to use, and allows you to pick from the languages you configured your system to support. Then the software checks to make sure you are ready to proceed with the installation.

If the **Application requirement check warnings** dialog box appears, click each warning to understand the nature of the warning and to determine what action you should take.

 NNMi is supported on a 64-bit Linux server, but not on a 32-bit Linux server. If the installation process displays a message instructing you to install some additional library files, follow the procedure shown in the *HP Network Node Manager i Software System and Device Support Matrix*.

- 5 After you respond to the warnings in the **Application requirement check warnings** dialog box, click **Continue**.
- 6 If the **Installer Configuration** dialog box appears, choose whether to use saved values from a previous installation or to change installation options. If you want to use the saved values, click **Yes**. If you want to select the installation options yourself, click **No**.
- 7 On the **Introduction** page, review the overview information for the installation; then click **Next**.

- 8 On the **License Agreement** page, review the NNMi license terms. If you agree with the terms of the license agreement, select **I accept...**; then click **Next**.
- 9 On the **Setup Type** page, select **Typical**; then click **Next**.
- 10 If you are completing an upgrade from an earlier version of NNMi and you plan to use an existing Oracle database instance, continue to [step 15](#).
- 11 If you are completing a new installation (not an upgrade from an earlier version of NNMi), you will see the **Choose the database type** page. On this page, select one of the following options; then click **Next**.
 - To use the database solution provided with NNMi, select **HP Software Embedded Database**, click **Next** and continue to [step 15](#).
 - If you plan to use an existing Oracle database instance in one of the following configurations, select **Oracle**; then continue to [step 12](#):
 - Standalone
 - As a global manager in a global network management configuration using application failover
 - In a an application failover or HA configuration
-  See the *HP Network Node Manager i Software Deployment Reference* for more information about the global manager and the global network management feature.
- 12 On the **Choose Database Initialization Preferences** page, do one of the following:
 - If you want to initialize an Oracle database using previously defined database accounts, select **Primary Server Installation**; then click **Next**.
 - If you want to connect to an existing database that is already initialized by another primary installation and use this installation in an application failover or HA configuration, select **Secondary Server Installation**; then click **Next**.
- 13 On the **Enter your database server information** page, enter the Host name of the Oracle database system. Enter the name of the NNMi database Instance; then click **Next**.
- 14 On the **Enter the database user account information** page, enter the Username and Password for the Oracle database user.

If the installation process reports an error, see [Problem: The NNMi installation process does not accept the Oracle user name and password](#) on page 55.

- 15 The **Install Checks** page displays progress as the installation software checks for additional NNMi installation requirements. After the check completes, click **Next**.
- 16 On the **Pre-Install Summary** page, review your installation choices; then do one of the following actions:

- To change any of the settings, click **Previous**.
- To start the installation process, click **Install**.

The installation process installs NNMi and performs some initial configuration; this process normally takes between ten and thirty minutes to complete..

▶ If you are upgrading to NNMi 9.10 using the embedded database on an HP-UX NNMi management server, the installation includes an automatic reload of the embedded database. This step will take some additional time. For example, this step will add between ten and twenty minutes to the installation time, depending on the database size.

- 17 If you are completing a new installation, and not an upgrade from an earlier version of NNMi, you will see the **System Account Password** dialog box. Follow the instructions on the screen to create a password for the system account; then click **OK**.

▶ The **system account** is a special administrator account that NNMi creates during installation. After installation, the system account is still valid; however, it should only be used for command-line security and for recovery purposes. For instructions on how to review or change the system password, see [Resetting the System Account Password](#) on page 54.

- 18 In the **NNM Web Server Port** dialog box, notice the port number; you will use this port to access NNMi. Click **OK** to accept the default port, or change the port number, then click **OK**.
- 19 In the **NNMi Https Web Server Port** dialog box, you can accept or change the port number that NNMi uses for the NNMi web server. Click **OK** to accept the default port or to accept the port change you made. If this is an NNMi upgrade, go to [step 21](#) on page 23.

- 20 The installation process searches for an official fully-qualified domain name (FQDN) for the NNMi management server. If the dialog box contains an incomplete or unresolvable FQDN, modify the name; then click **OK**.
- ▶ This entry is used as the official FQDN to provide users with access to the NNMi management server. It is also used to enable single sign-on (SSO) for NNM iSPIs. For SSO to work, URL access to NNMi and NNM iSPIs must share a common domain. If you do not have a FQDN for the NNMi management server, you can substitute the NNMi management server's IP address; however, this will make the single sign-on for NNM iSPIs unusable.
- Following installation, if you have problems accessing NNMi due to an incorrect or unresolvable FQDN, see [Obtaining or Setting the Official Fully-Qualified Domain Name](#) on page 51.
- 21 The installation process prompts you for the location of any NNMi patches you want to install before starting NNMi. Select **Install Patches** or **Skip Patching** to continue.
- ▶ Before installing patches, unzip any zipped patch files and place the unzipped files in a folder on the target server before completing [step 21](#). NNMi installation supports patch files that come in the following formats: *patchfilename.msi* for Windows, *patchfilename.tar* for Solaris, *patchfilename* (shar file) or *patchfilename.depot* for HP-UX, and *patchfilename.rpm* for Linux. Do not change the original format of these files.
 - ▶ For support information, including information on how to obtain patches, see [Support](#) on page 4.
- 22 The installation process completes installation and configuration and starts the NNMi services. This process takes several minutes.
- ▶ jboss is an application server that contains the NNMi services. At this point in the installation routine, a jboss port conflict can occur. In this case, see [Problem: jboss port contention](#) on page 58.
- 23 If you are upgrading from an earlier version of NNMi, database migration occurs now, extending the configuration time. At the end, a successful migration dialog box appears. If errors occurred during the database migration, contact HP Support.
- 24 Click **Finish**.

- 25 After the installation software completes the NNMi configuration, a dialog box appears that explains how to start the **Quick Start Configuration Wizard**.

Carefully read the information included in this dialog box.

For information about this wizard, see [Using the Quick Start Configuration Wizard](#) on page 29.



If you installed NNMi and plan to use an existing Oracle database instance in an application failover or HA configuration, see the *HP Network Node Manager i Software Deployment Reference* for instructions.

- 26 Click **Done** to complete the installation.

Silently Installing NNMi

This section provides two approaches you can use to install NNMi silently on an unattended system:

- [Silent Installation Using a Sample ovinstallparams.ini File](#) on page 25 provides steps to silently install NNMi using a sample `ovinstallparams.ini` file.
- [Silent Installation Using an ovinstallparams.ini File from a Prior Installation](#) on page 26 provides steps to silently install NNMi using the `ovinstallparams<time_stamp>.ini` file from a prior installation.

To avoid confusion, the following terms are used in this section:

- **Source**—The server where you do an initial installation by using the NNMi installation wizard. The installation options that you choose for this server are captured for subsequent silent installations.
- **Target**—The server where you plan to do the silent installation.

Silent Installation Using a Sample ovinstallparams.ini File

The NNMi installation media contains an example of an `ovinstallparams.ini` file. Look in the support directory of the NNMi installation media to view the file contents or to obtain a copy of this sample `ovinstallparams.ini` file.

- ▶ Unless you are upgrading from a supported version of NNMi, make sure that all previous NNMi installations are removed. See *Updating from NNMi 9.0x* in the *HP Network Node Manager i Software Deployment Reference* and [Removing NNMi](#) on page 37 for more information.

- 1 On the target server (where you plan to install NNMi), log on with root privileges.
- 2 Copy the `ovinstallparams.ini` file from the support directory of the NNMi installation media to the following directory:
Linux: /tmp
HP-UX or Solaris: /var/tmp
- 3 Modify the `ovinstallparams.ini` file as shown below:

- a The following entries set the silent installation script to use the embedded database. Configure these settings as shown below:

```
[obs.install]
db.embedded=Solid
```

- ▶ If you are using an Oracle database and are not using HA or application failover, you must use a unique value for the `db.instance` parameter.
- ▶ If you are using an Oracle database, and are using HA or application failover, run the **ovstop -c** command on the source system before beginning a silent installation.

- b The following entry sets the HTTP port number for accessing NNMi. A common approach is to use port 8004 (the existing port number) if you are installing NNMi on a Windows operating system, but to modify the port to 80 if you are installing NNMi on a UNIX operating system.

```
[nonOV.jboss]
httpport=8004
```

- 4 On the target server, insert the NNMi installation media into the DVD drive.
- 5 Make sure that the DVD drive is mounted; then use the `cd` command to change to the `/cdrom` directory.

- 6 Enter the following command:

```
./setup.bin -i silent
```

The silent installation runs as a background process and takes some time. No progress indicator is visible.

After the silent installation completes, NNMi is installed and available for use on the target server.

- 7 To make sure that the NNMi services are running, enter the following at the command line:

```
ovstatus -c
```

- 8 Stop the NNMi processes using the `ovstop -c` command.
- 9 As root or administrator, run the `nnmchangesyspw.ovpl` script to set the system password. You will need this new system password to complete [step 11](#).
- 10 Start the NNMi processes using the `ovstart -c` command.
- 11 To configure NNMi, see [Using the Quick Start Configuration Wizard](#) on page 29.

Silent Installation Using an `ovinstallparams.ini` File from a Prior Installation

When you first install NNMi using the interactive installation wizard, your responses to installation questions are stored in the `ovinstallparams<time_stamp>.ini` file. This file can be used as input to perform subsequent silent installations of NNMi on an unattended system.

The installation questions file is stored in the following location:

```
HP-UX and Solaris: /var/tmp/HPOvInstaller/  
NNM_<version_number>/
```

```
Linux: /tmp/HPOvInstaller/NNM_<version_number>/
```

To silently install NNMi follow these steps:

- 1 On the target server (where you plan to install NNMi), log on with `root` privileges.

▶ Unless you are upgrading from a supported version of NNMi, make sure that all previous NNMi installations are removed. See *Updating from NNMi 9.0x* in the *HP Network Node Manager i Software Deployment Reference* and [Removing NNMi](#) on page 37 for more information.

- 2 Remove the following directory if it exists:

HP-UX and Solaris: `/var/tmp/HPOvInstaller/`

Linux: `/tmp/HPOvInstaller/`

- 3 On the source server, complete an installation of NNMi, using the NNMi installation wizard. See [Installing NNMi](#) on page 19.

▶ To complete a silent installation, the source server must run the same operating system as the target server. For example, to install NNMi silently on a Windows target server, the source server must also be a Windows server.

- 4 On the source server, make a backup copy of the following file; then place the backup in a safe location:

HP-UX and Solaris: `/var/tmp/HPOvInstaller/`

`NNM_<version_number>/ovinstallparams<time_stamp>.ini`

Linux: `/tmp/HPOvInstaller/NNM_<version_number>/`

`ovinstallparams<time_stamp>.ini`

- 5 Copy the `ovinstallparams<time_stamp>.ini` file from the source server to the target server as follows:

- a On the target server, place the `ovinstallparams<time_stamp>.ini` file in the following directory:

HP-UX or Solaris: `/var/tmp/`

Linux: `/tmp/`

- b Rename the file you copied as follows:

`ovinstallparams.ini`

- 6 Add these two lines to the `ovinstallparams.ini` file:

```
[nonOV.jboss]
httpport=<port_number>
```

In this instance, `<port_number>` is the port that was identified in [step 18](#) on page 22 of the interactive installation.

For example:

```
[nonOV.jboss]
httpport=80
```

- ▶ If the previous installation used an Oracle database and did not use HA or application failover, you must use a unique value for the `db.instance` parameter.

- 7 On the target server, insert the NNMi installation media into the DVD drive.
- 8 Make sure that the DVD drive is mounted; then use the `cd` command to change to the `/cdrom` directory.
- 9 Enter the following command:

```
./setup.bin -i silent
```

The silent installation runs as a background process and takes some time. No progress indicator is visible.

After the silent installation completes, NNMi is installed and available for use on the target server.

- 10 To make sure that the NNMi services are running, enter the following at the command line:

```
ovstatus -c
```

- 11 Stop the NNMi processes using the `ovstop -c` command.
- 12 As root, run the `nnmchangesyspw.ovpl` script to set the system password. You will need this new system password to complete [step 14](#).
- 13 Start the NNMi processes using the `ovstart -c` command.
- 14 To configure NNMi, see [Using the Quick Start Configuration Wizard](#) on page 29.

Using the Quick Start Configuration Wizard

This section guides you through some basic configuration tasks for NNMi. These tasks must be completed *after* you install NNMi.

HP recommends that you use the **Quick Start Configuration Wizard** for initial setup (such as in a test environment), including:

- Configuring SNMP community strings
- Completing discovery of a limited range of network nodes
- Setting up an initial administrator account



You cannot use the **Quick Start Configuration Wizard** to complete SNMP Version 3 (SNMPv3) configuration. If you have devices that you prefer to monitor using SNMPv3, do the following:

- 1 Open the NNMi console.
- 2 Select **Communication Configuration** from the **Configuration** workspace.
- 3 Complete the SNMPv3 configuration.

After initial configuration, you can use the NNMi console for additional configuration tasks, such as adding nodes to the network topology and configuring monitoring. For more information, see the NNMi help.

About Discovery Seeds and Auto-Discovery Rules

A discovery **seed** is a node that can help NNMi discover the network topology. For example, a seed might be a core router in your management environment. Each seed is identified by an IP address or host name; see *Specify Discovery Seeds* in the NNMi help.

- To configure discovery so that only the devices that you specify as seeds are discovered, disable auto-discovery; see *Do Not Use Auto-Discovery Rules* in the NNMi help.
- To configure discovery so that the devices that you specify as seeds become the starting point for additional discovery, create and configure auto-discovery rules; see *Configure Auto-Discovery Rules* in the NNMi help.

For overview information about the discovery process see *How Spiral Discovery Works* in the NNMi help.

- 1 After the installation process completes, launch the **Quick Start Configuration Wizard**, as shown below.

 You should run the **Quick Start Configuration Wizard** immediately after installation. To manually launch the **Quick Start Configuration Wizard**, go to the following URL:

`http://<fully_qualified_domain_name>:<port_number>/quickstart/`

Where *<fully_qualified_domain_name>* represents the fully-qualified domain name of the NNMi management server and *<port_number>* is the port number described in [step 18](#) on page 22.

If your NNMi management server has more than one domain name, NNMi chooses one during the installation process. To determine which fully-qualified domain name NNMi is using, run the `nnmofficialfqdn.ovpl` script. See the *nnmofficialfqdn.ovpl* reference page, or the UNIX manpage, for more information.


The **NNM Quick Start Configuration Wizard** opens in a web browser window.

- 2 Log on as follows:

User Name: **system**

Password: The password that you created at the end of the installation process (in [step 17](#) on page 22) or during silent installation (in [step 12](#) on page 28).

- 3 On the **Configure Community Strings** page, enter a community string for one of the nodes in the discovery range; then click **Add**.

 NNMi automatically tries to match community strings to known devices. You do not need to manually associate each community string with a specific device.

- 4 Repeat [step 3](#) until the **SNMP Community Strings** list includes the community strings for all nodes in the discovery range; then click **Next**.

➤ The SNMP community strings that you add here are saved in the NNMi database. In the NNMi console, the SNMP community strings are visible on the **Default Community Strings** tab of the **Communication Configuration** form.

- 5 On the **Configure Auto-Discovery Rule** page, associate the existing rule name with the **Included IP Address Range**. Enter the range of IP addresses for the discovery rule; then click **Next**.

Examples of valid IP address ranges include:

- 10.1.1.*
- 10.1.1.1-99
- 10.10.50-55.*
- 10.1-7.1-9.1-9

- 6 On the **Configure Seeds** page, add discovery seed information for your network; then click **Next**.

Enter discovery seeds in the form of IP addresses or fully-qualified domain names. The network devices represented by these seeds help the NNMI spiral discovery process discover your network accurately.

➤ You can use the `nnmloadseeds.ovpl` command to load seeds using a command line. See the *nnmloadseeds.ovpl* reference page, or the UNIX manpage, for more information.

- 7 On the **Test Seeds** page, review the results of the communication tests. If any of the seed nodes cannot be reached with the community strings that you identified in [step 3](#), click **Previous** to navigate to the **Configure Community Strings** page. Correct the community strings; then click **Next**.
- 8 Repeat [step 7](#) until all nodes can be reached; then click **Next**.
- 9 On the **Configure Administrator Account** page, enter a **User Name**, set the **Password** for a new account for administering the NNMI software; then click **Next**.
- 10 On the **Summary** page, review the information that you specified; then do one of the following actions:
 - To change any of the settings, click **Previous**.
 - To use the current settings, click **Commit**.

Add Community Strings

Configure Auto Discovery

Add Discovery Seeds

Test Seeds

Create Administrator Account

Summary

Summary

Review the displayed information and use the navigation buttons to make any corrections. Choose commit to apply and save these configuration changes.

Default Community Strings: [public]
Auto Discovery Rule: quickstart rule
Included IP Range: 10.97.*,*
Seeds: [10.97.246.162, 10.97.246.196]
Administrative User Name: administrator

- 11 The **Wizard is complete** page indicates that you have successfully configured NNMi to discover a portion of your network. Click **Previous** to make changes or click **Launch UI**.

The NNMi console user interface opens. To begin using NNMi, see [Chapter 4, Getting Started with NNMi](#).

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 the NNMi management server
- If the license is for NNMi running under HA, the virtual IP address of the cluster
 - ▶ For NNMi running under HA, the NNMi production license is tied to the virtual IP address of the cluster. Additionally, one of the nodes in the HA cluster requires an NNMi non-production license.
- 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.

Removing NNMi

To remove NNMi from a local system, follow these steps:

- 1 Log on with `root` privileges to the system where you plan to remove NNMi.
- 2 If you have NNMi configured to use application failover, global network management, or HA, unconfigure NNMi from these features by following instructions in the *NNMi Deployment Reference*.
- 3 Run the `nnmversion.ovpl` script to obtain a list of the NNMi patches installed on the NNMi management server.
- 4 Remove all NNMi patches installed on the NNMi management server. See the patch installation text for each patch for instructions on how to remove the patch.
- 5 To begin uninstalling NNMi, do the following:

- At a command prompt, enter the following command:
`/opt/OV/Uninstall/NNM/setup.bin`

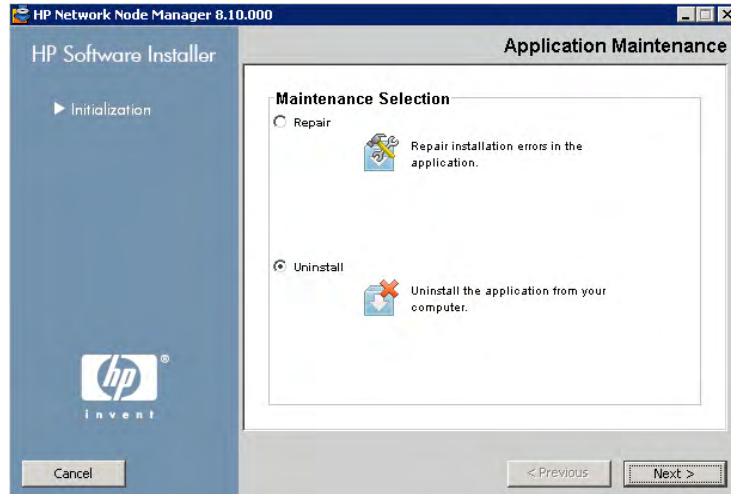
 You can use the `setup.` command with the `-i silent` option to silently remove NNMi.

The installation initialization process prompts you for the language you want to use, allowing you to pick from the languages your system supports. It then checks your system to ensure that it is ready to proceed with the software removal.

If the **Application requirement check warnings** dialog box appears, click each warning to understand the nature of the warning and to determine what action to take.

- 6 After you respond to the warnings in the **Application requirement check warnings** dialog box, click **Continue**.

- 7 The installation process completes an inventory of your system and prompts you to select a maintenance task. Select **Uninstall**; then click **Next**.



- 8 On the **Pre-Uninstall Summary** page, review the list of files that will be removed from the system; then do one of the following:
- To cancel the uninstall, click **Cancel**.
 - To go back, click **Previous**.
 - To remove the files from the system, click **Uninstall**.
- 9 On the **Uninstall Complete** page, click **Done**.

Accessing NNMi Installation Log Files

NNMi logs information about the installation and removal processes. You can view this information at the following location:

```
/var/opt/OV/log/nnm/
```

The most important log files are as follows:

- `nnm-install-config.log`: Contains a record of the most recent installation, including the processes that have been initialized (see the end of the `nnm-install-config.log` file).
- `/tmp/nnm-install-config_sh.log`: Contains a record of some preinstallation and postinstallation activity.
- `/tmp/HPOvInstallerLog.txt`: If you have installed NNMi and suspect problems, consult this log file.

In addition, the following log files might be useful:

- `/tmp/nnm-preinstallcheck.log`: If the preinstallation check contains unresolved warnings or errors, consult this log file to diagnose problems.
- `/tmp/NNMUninstall.log`: If you have uninstalled NNMi and suspect problems, consult this log file.

4 Getting Started with NNMi

This chapter provides information to help you begin network management with NNMi, including more information about the discovery process. You can find more detailed information for operators and administrators in the NNMi help (see [NNMi Help](#) on page 44).

Accessing NNMi

Now that you have installed NNMi, completed post-installation configuration tasks, and set up discovery using the **Quick Start Configuration Wizard**, you can begin managing your network. All network monitoring and event-handling tasks can be accessed through the NNMi console, which opens in a web browser.



To view the NNMi console in Japanese or Simplified Chinese, set the language preference in your browser.

To access the NNMi console, follow these steps:

- 1 Make sure that you are using a supported web browser (see [Supported Hardware and Software](#) on page 9).
- 2 Enable the web browser for JavaScript, pop-up windows from the NNMi management server, and to accept cookies from the NNMi management server (see [Enabling the Web Browser for the NNMi Console](#) on page 52).

- 3 Enter the following URL into a web browser window:

`http://<fully_qualified_domain_name>:<port>/nnmi/`

Where `<fully_qualified_domain_name>` represents the fully-qualified domain name of the NNMi management server, and `<port>` is the port that the jboss application server uses for communicating with the NNMi console.

- ▶ If the NNMi management server has more than one domain name, NNMi chooses one during the installation process. To determine which fully-qualified domain name NNMi is using, run the **`nnmofficialfqdn.ovpl`** script. See the *nnmofficialfqdn.ovpl* reference page, or the UNIX manpage, for more information.

If you do not know which port to use, see [Problem: The NNMi console page cannot be found](#) on page 57.

- ▶ If you cannot start an NNMi console when pointing your browser to an NNMi management server that is installed on a Linux operating system, you might have a Linux firewall on the NNMi management server that is blocking the http port. See [Problem: You cannot start the NNMi Console when accessing a Linux NNMi management server](#) on page 60.

In the NNMi console product window, select a link to either run the NNMi console in a new web browser window or to use the current web browser window.

In the NNMi sign-in window, enter your user account name and password; then click **Sign In**. For more information, see [About User Accounts and Roles](#) on page 43.

About User Accounts and Roles

During installation, NNMi provides a special **system account** to access NNMi for the first time. After installation, **do not use the system account**.

For everyday use, the NNMi administrator sets up an account for each user (or group of users) and assigns a pre-configured user role to each account. User roles determine who has access to the NNMi console, as well as which workspaces and actions are available to each user. NNMi provides the following user roles for NNMi console access. These roles are predefined by the program and cannot be modified:

- Administrator
- Operator Level 2
- Operator Level 1
- Guest

Before configuring NNMi sign-in access for your team, determine which pre-defined NNMi role is appropriate for each team member. The roles are hierarchical, meaning the higher level roles include all privileges of the lower roles in the hierarchy (Administrator is highest, Guest is lowest).

User accounts and roles, along with command-line access, are configured in the NNMi console. For more information, see *Controlling Access to NNMi* in the NNMi help.



NNMi provides an out-of-the-box https configuration using a self-signed certificate created during installation. See the *HP Network Node Manager i Software Deployment Reference* for more information about using a signed certificate from a Certificate Authority instead of the self-signed certificate.

NNMi Help

The NNMi help describes how to use the NNMi console. The detailed information in the NNMi help is organized into the following sections:

- *Using the NNMi Console*
- *Help for Operators*
- *Help for Administrators*

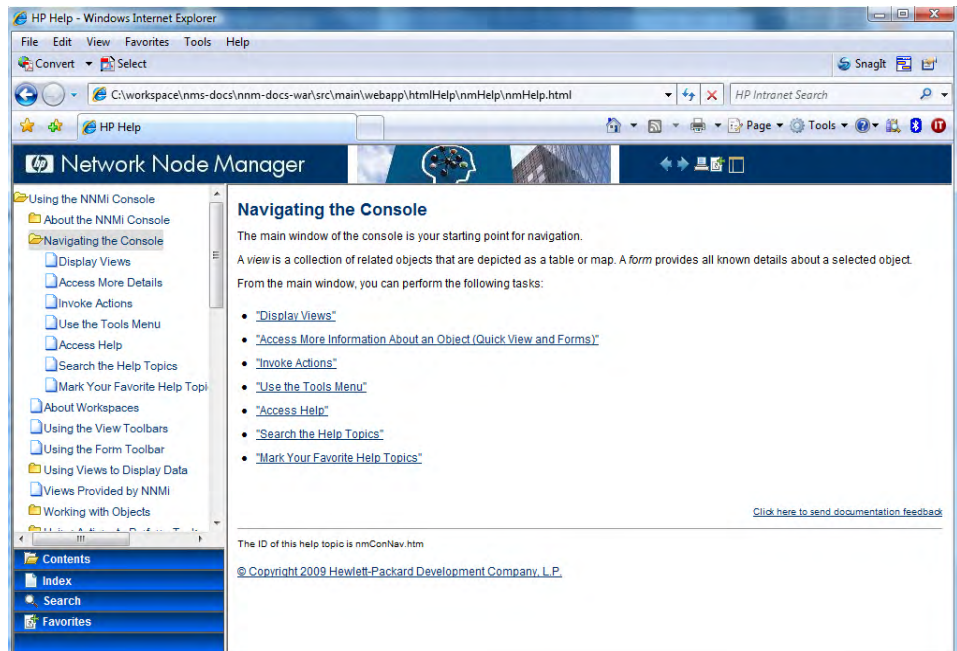
To access the NNMi help, click **Help** on the NNMi console menu bar; then click one of the options above the first separator line on the menu.



The NNMi console includes forms for entering information. The form name is in the upper right corner of the window. From any NNMi form, you can access the help information about that form. On the **Help** menu, click **Using the <xyz> form** where <xyz> has the title of the current form.

Figure 1 shows the NNMi help window.

Figure 1 NNMi help



Configuring Network Discovery

As you begin to use NNMi to discover and manage your network, it is a good practice to start with a test network and to configure NNMi to discover and manage a few nodes with only a few interfaces. The **Quick Start Configuration Wizard** (see [page 29](#)) provides an easy way to set up this type of small configuration. HP recommends that you use the **Quick Start Configuration Wizard** immediately after installing NNMi.

As you become more familiar with NNMi, you will understand how its rich set of features applies to managing your network. You can expand the network topology that NNMi manages over time, systematically adding new discovery rules and putting new areas under management.

The topics in this section provide a brief overview of the configuration tasks that are required before initiating the discovery process. The checklist in [Table 5](#) summarizes these tasks.

Table 5 Discovery configuration checklist

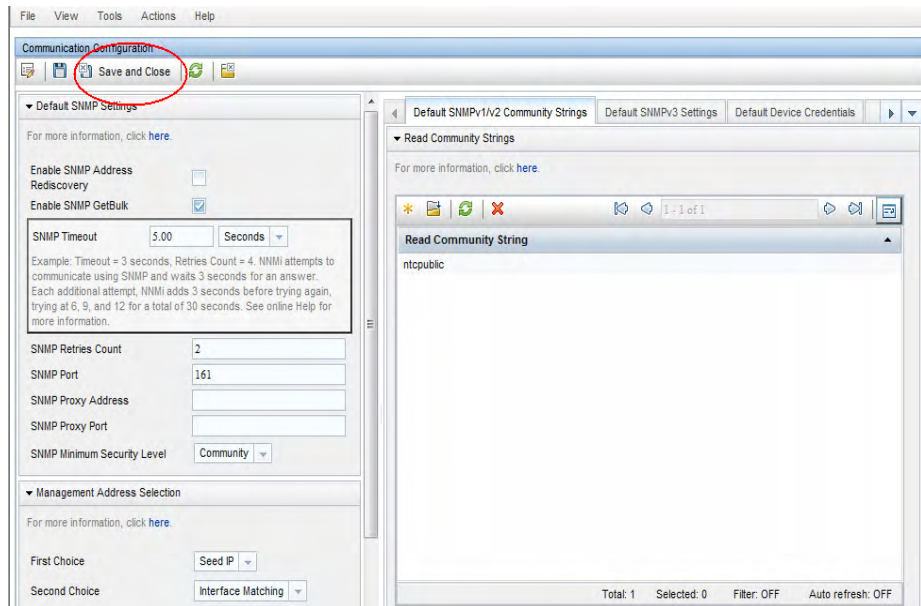
| Complete (y/n) | Task |
|----------------|---|
| | Verify that all nodes to be discovered are connected to the network and configured with a supported version of SNMP (SNMPv1, SNMPv2c, or SNMPv3). |
| | Obtain read-only community strings from your network administrator for the nodes that you plan to manage. |
| | Using the NNMi console, configure community strings as described in Configuring Community Strings on page 46. |
| | Using the NNMi console, configure the spiral discovery process as described in Configuring Auto-Discovery Rules on page 47. |
| | Using the NNMi console, check the spiral discovery progress as described in Checking Discovery Progress on page 49. |

For more information about the discovery process, see *Discovering Your Network* in the NNMi help.

Configuring Community Strings

To configure NNMi with community strings, follow these steps:

- 1 From the workspace navigation panel, select the **Configuration** workspace.
- 2 Open the **Communication Configuration** form, as shown here:



- 3 On the **Default SNMPv1/v2 Community Strings** tab, click the **New** icon.
- 4 On the **Default Read Community String** form, in the **Read Community String** box, enter a community string for one of the nodes in the discovery range; then click the **Save and New** icon.
- 5 Repeat [step 4](#) to enter all community strings for the nodes in the discovery range; then click the **Save and Close** icon.
- 6 On the **Communication Configuration** form, click the **Save and Close** icon.

For more information about setting up device community strings and loading community strings from a file, see *Configuring Communication Protocol* in the NNMi help.

Configuring Auto-Discovery Rules

One of the most important network management tasks is keeping your view of the network topology up-to-date. NNMi maintains the topology through ongoing **discovery** of network nodes. The NNMi discovery process ensures that root cause analysis and the troubleshooting tools provide accurate information to resolve incidents (see [Network Discovery](#) on page 48).

To configure auto-discovery rules, follow these steps:

- 1 From the workspace navigation panel, select the **Configuration** workspace.
- 2 Open the **Discovery Configuration** form.
- 3 Click the **Auto-Discovery Rules** tab; then click the **New** icon.
- 4 On the **Auto-Discovery Rule** form, under **Basics**, enter the rule **Name** and **Ordering** information.

The order is a numerical value that specifies the priority of this rule in comparison to other auto-discovery rules. For more information, click **Help > Using the Auto-Discovery Rule form**.

- 5 Under **Auto-Discovery Starting Point for this Rule**, select the appropriate auto-discovery actions for this rule.
- 6 On the **IP Ranges** tab, click the **New** icon.
- 7 On the **Auto Discovery IP Range** form, enter the **IP Range**, leave the **Range Type** set to **Include in rule**; then click the **Save and Close** icon.
- 8 On the **Auto-Discovery Rule** form, click the **Save and Close** icon.
- 9 Repeat [step 3](#) through [step 8](#) until you have added all of the rules that you want to use.
- 10 On the **Discovery Configuration** form, click the **Save and Close** icon to save all new auto-discovery rules to the NNMi database.
- 11 From the **Configuration** workspace, open **Discovery**; then click **Seeds**.
- 12 Click the **New** icon.
- 13 On the **Discovery Seed** form, enter a hostname or IP address; then click the **Save and Close** icon.
- 14 Repeat [step 12](#) and [step 13](#) until you have added all host names or IP addresses for discovery seeds.
- 15 On the **Discovery Configuration** form, click the **Save and Close** icon.

To monitor the progress of discovery, see [Checking Discovery Progress](#) on page 49.



For additional information about setting up discovery, see *Configure Discovery* in the NNMi help.

Network Discovery

NNMi collects information about the devices in your network (such as switches and routers), and proactively manages any devices that are important to you and your team. There are two discovery modes to choose from:

- **Discovery Seeds:** You provide a list of devices and maintain total control over which devices NNMi discovers and monitors.
- **Auto-Discovery Rules:** You provide a list of addresses and host names as discovery seeds, and NNMi uses this information as starting points for extensive automatic discovery. You set limits on the NNMi discovery process by providing IPv4 address ranges and MIB II sysObjectIDs.

After you choose a discovery mode, **NNMi Spiral Discovery** takes over. Using a wide range of protocols and techniques, NNMi gathers a wealth of information about your network inventory, ascertains the relationships between devices (such as subnets and VLANs), and accurately maps out the connectivity between those devices. The NNMi Causal Engine determines current status of each device (plus each interface and address associated with that device) and proactively notifies you when any trouble or potential trouble is detected.

This dynamic discovery process continues over time. When things change in your network management domain, NNMi Spiral Discovery automatically updates information.

To learn more about network discovery, see *Discovering Your Network* in the NNMi help.

Checking Discovery Progress

After initiating the spiral discovery process, verify that the process is running correctly.



Because spiral discovery is dynamic, NNMi discovers network nodes on a continuous basis. Whenever a new node is added to a discovery rule, NNMi discovers the node, collects topology information about the node, and begins to monitor the node.

There are several ways to gauge discovery progress. Do any of the following actions to check the discovery progress:

- During discovery, check the status of seeds by using **Configuration > Discovery>Seeds**. Review the status information in the **Discovery Seed Results** column. When discovery is nearing completion, the majority of the nodes have the **Node created** status.
- During discovery, check the discovery progress by using **Help > System Information**; then clicking the **Database** tab. Check the **Database Object Counts** several times during a one hour period. The numbers in the **Nodes**, **SNMP Agents**, **Interfaces**, **IP Addresses**, and **L2 Connections** fields will stabilize. If these numbers are no longer increasing in value over the sampling period, then discovery is complete.
- During discovery, from the NNMi console click **Nodes** in the **Inventory** workspace. Check the value in the **Total** field several times during a one hour period. If this value is no longer increasing in value over the sampling period, then discovery is complete.
- During discovery, from the NNMi console, check the discovery progress by using the **Tools > NNMi Self-Monitoring Graphs > Discovery Progress** tool.
- During discovery, from the NNMi console, check the discovery progress by using the **Tools > Status Distribution Graphs >Node Status** tool.
- During discovery, from the NNMi console click **Initial Discovery Progress** in the **Topology Maps** workspace. Watch the map grow in complexity during a one hour period. If the map growth slows, then stops growing over the sampling period, then discovery is complete.



If you suspect a problem with discovery, see [Problem: NNMi is not discovering nodes](#) on page 59.

A Additional Information

The following sections contain information about installing NNMi and troubleshooting NNMi startup problems. Other sections in this guide reference these sections as appropriate.

Obtaining or Setting the Official Fully-Qualified Domain Name

NNMi users access NNMi using the official fully-qualified domain name (FQDN). FQDN is also used to enable single sign-on (SSO) to NNM iSPIs.

- 1 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 FQDN set during installation. See the *nnmofficialfqdn.ovpl* reference page, or the UNIX manpage, for more information.
 - In the NNMi console, click **Help > About Network Node Manager i Software**. Scroll down to find the value for the fully-qualified domain name beneath the **Management Server** heading.
- 2 If you need to change the FQDN that was set during installation, use the `nnmsetofficialfqdn.ovpl` command. See the *nnmsetofficialfqdn.ovpl* reference page, or the UNIX manpage, for more information.
- 3 Single sign-on to NNM iSPIs requires that users access the NNMi console through a URL that contains the FQDN. To make it easier for users to satisfy this requirement, you can configure NNMi to redirect NNMi URLs to the FQDN. If you do this, you must have an official FQDN configured. See the NNMi help for more information.

Configuring an X Server for Installation

If you plan to install NNMi from an X Server, set up and test the X Server by following these steps:

- 1 Set the `DISPLAY` environment variable to the appropriate value: set this to the value of the system displaying the progress of the installation process.
- 2 Export the `DISPLAY` environment variable.
- 3 Run the `xhost` command to enable a connection from the system running the installation process to the system displaying the installation process.
- 4 Run the `xclock` command to verify the configuration.
The clock should appear on the X Server.

Enabling the Web Browser for the NNMi Console

Before signing on to NNMi, make sure to configure the web browser to interact with the NNMi console. The following items must be enabled in the web browser on each client machine that will access the NNMi management server:

- JavaScript
- Pop-up windows from the NNMi management server
- Cookies from the NNMi management server



To complete the following procedures, you need to know the fully-qualified domain name of the NNMi management server.

If the NNMi management server has more than one domain name, NNMi chooses one during the installation process. To determine which fully-qualified domain name NNMi is using, run the **`nmmofficialfqdn.ovpl`** script. See the *nmmofficialfqdn.ovpl* reference page, or the UNIX manpage, for more information.

The method for preparing your web browser should be similar to the following procedures:

Mozilla Firefox

- 1 In Mozilla Firefox, click **Tools > Options** or **Edit > Preferences**.
- 2 On the **Content** tab, enable the **Enable JavaScript** check box.
- 3 Next to the **Enable JavaScript** check box, click **Advanced**.
- 4 Enable the **Raise or lower windows** check box; then click **OK**.
- 5 Click the **Content** tab; then enable the **Block pop-up windows** check box.
- 6 Click **Exceptions**; then add the fully-qualified domain name of the NNMi management server to the list of allowed sites.
- 7 Click the **Privacy** tab, then pull-down **Use custom settings for history**.
- 8 Enable the **Accept cookies from sites** check box; then click **Exceptions**.
- 9 Add the fully-qualified domain name of the NNMi management server to the list of allowed sites.
- 10 Click **OK**.
- 11 Restart the web browser.

Microsoft Internet Explorer

- 1 In Internet Explorer, click **Tools > Internet Options**.
- 2 On the **Security** tab, select the zone that includes the NNMi management server; then click **Custom level**.
- 3 Under **Scripting**, select the **Enable** option for **Active scripting**.
- 4 On the **Privacy tab Settings** area; select one of the options between **Accept All Cookies** and **Medium High**.
 - ▶ This setting affects the Internet zone only. If you are connecting to the NNMi management server over an Intranet, this setting has no effect.
- 5 On the **Privacy** tab, select the **Turn on Pop-up Blocker** check box; then click **Settings**.
- 6 Add the fully-qualified domain name of the NNMi management server to the list of allowed sites.
- 7 Restart the web browser.

Resetting the System Account Password

During NNMi installation, you set the system account password. If you forget the system account password, you can change it by using the `nnmchangesyspw.ovpl` script; follow these steps:

- 1 Stop the NNMi processes using the `ovstop -c` command.
- 2 As root, run the `nnmchangesyspw.ovpl` script to set the system password.
- 3 Start the NNMi processes using the `ovstart -c` command.

See the `nnmchangesyspw.ovpl` reference page, or the UNIX manpage, for more information.

B Troubleshooting Installation and Initial Startup

Installation Problems

Problem: The NNMi installation process does not accept the Oracle user name and password

Solution:

- 1 Verify the Oracle user name and password with your Oracle database administrator; then continue the installation.
- 2 If [step 1](#) does not solve the problem, obtain the correct port number from your Oracle database administrator; then continue the installation.

Problem: The NNMi installation requires more disk space than is available on the host system

Solution: When you install NNMi on UNIX or Linux, you are not able to choose where to install the binaries (\$NnmInstallDir), and where to store the data files (\$NnmDataDir). These locations are as follows:

- \$NnmInstallDir=/opt/OV
- \$NnmDataDir=/var/opt/OV

See the *HP Network Node Manager i Software System and Device Support Matrix* for the disk space requirements for your server. If you do not have enough disk space in either /opt/OV or /var/opt/OV, use the following workaround to remedy the situation:

- 1 Uninstall NNMi, if necessary.
- 2 Create symbolic links from the install targets to larger partitions that have enough available disk space to install the binaries and store the data files. The syntax to create the symbolic links is as follows:

```
ln -s <large disk> /opt/OV
```

```
ln -s <large disk> /var/opt/OV
```

Refer to the `ln` manpage for detailed information about creating symbolic links.



For Solaris, set the `PKG_NONABI_SYMLINKS` environment variable to **true**.

3 Install NNMi.

Initial Startup Problems

Problem: Cannot run the NNMi command line tools on UNIX NNMi Management Servers

Solution: Verify that the PATH variable contains the `/opt/OV/bin` location. If it does not, add the `/opt/OV/bin` location to the PATH variable.

Problem: The NNMi console page cannot be found

Solution: The URL for accessing the NNMi console includes the port that the jboss application server uses for communicating with the NNMi console. To access the NNMi console, enter the following URL into a web browser window:

`http://<fully_qualified_domain_name>:<port>/nnm/`

Where `<fully_qualified_domain_name>` is the fully-qualified domain name of the NNMi management server, and `<port>` is the port that the jboss application server uses for communicating with the NNMi console.



If your NNMi management server has more than one domain name, NNMi chooses one during the installation process. To determine which fully-qualified domain name NNMi is using, run the **`nnmofficialfqdn.ovpl`** script. See the *nnmofficialfqdn.ovpl* reference page, or the UNIX manpage, for more information.

The NNMi installer configures the jboss application server to use an available port. Because the installer does this configuration automatically, no user action is required. The selected port number is listed in the **jboss Application Server Port** dialog box that appears during the NNMi installation process.

To determine the port that is being used for your installation of NNMi, view the following file:

```
$NnmDataDir/conf/nnm/props/nms-local.properties
```

Look for the entry within the file that resembles the following text:

```
jboss.http.port=80
```

The port assigned to **jboss.http.port** is the port to specify in the URL. See the *nnm.ports* reference page, or the UNIX manpage, for more information.

Problem: jboss port contention

Solution: By default, the jboss application server uses several ports for communication with NNMi. These ports are commonly used by Oracle and other applications. If the NNMi installer determines that the jboss application server ports are already being used by other applications, such as the Oracle database server, the installer displays an error message regarding the port contention. To determine if port contention is a problem for NNMi, check the following log file:

```
$NnmDataDir/log/nnm/jbossServer.log
```

To resolve any port contentions, follow these steps:

- 1 As a user with root privileges, open the following file in any text editor:

```
$NnmDataDir/conf/nnm/props/nms-local.properties
```
- 2 Modify the existing entries, replacing any conflicting port numbers with available port numbers.
- 3 Save the file; then restart the NNMi services:

```
ovstop -c  
ovstart -c
```

See the *nnm.ports* reference page, or the UNIX manpage, for more information.

Problem: Some NNMi program components do not work correctly

Solution: Verify that all NNMi services have been installed and started:

- 1 At a command prompt, enter the following command:

```
ovstatus -c
```

The command output should look similar to the output shown in [Table 6](#).

- 2 Stop or start NNMi services as needed. At the command prompt, type the appropriate command:

```
ovstop -c <service name>  
ovstart -c <service name>
```

Table 6 Output from ovstatus - c command

| Name | PID | State | Last Message(s) |
|----------|------|---------|--------------------------|
| OVsPMD | 3262 | RUNNING | - |
| pmd | 3327 | RUNNING | Initialization complete. |
| ovjboss | 3292 | RUNNING | Initialization complete. |
| nmsdbmgr | 3263 | RUNNING | Database available. |

Problem: NNMi is not discovering nodes

Solution:

- 1 From the workspace navigation panel, select the **Configuration** workspace.
- 2 Open the **Discovery Configuration** form.
- 3 On the **Discovery Seeds** tab, look at the values in the **Discovery Status** column.

If the status of many of the discovered nodes is something other than **Node created**, then the NNMi discovery process was not successful.

If the status is **No SNMP response**, verify that you can ping the node, and that you can run `nnmsnmpwalk.ovpl -c communitystring nodename` to obtain information from the node. If you cannot run these tools, check the following items:

- a Ping the node to make sure it is responding.
- b Make sure that the node has SNMP enabled.
- c Make sure that the node has your local management server on its access list of SNMP agents.
- d Make sure to configure the correct community strings for the nodes so that NNMi discovers them correctly. This information is listed on the **Communication Configuration** form on the **Default Community Strings** tab.
- e Make sure that there are no access control lists configured on your routers, switches, or firewalls that might be limiting discovery.

For more information, see *Configure Discovery* in the NNMi help.

Problem: You cannot start the NNMi Console when accessing a Linux NNMi management server

If you cannot start an NNMi console when pointing your browser to an NNMi management server that is installed on a Linux operating system, you might have a Linux firewall on the NNMi management server that is blocking the HTTP port. To remedy this problem, do the following:

- 1 Open the Security Level form using one of the following menus or commands:
 - Applications->System Settings->Security Level
 - System->Administration->Security Level and Firewall
 - Run the `/usr/bin/system-config-securitylevel` command and wait for the dialog box to appear.
- 2 After the dialog box appears, complete only one of the following remedies:
 - Disable the firewall.
 - Leave the firewall enabled and add the following specific ports:

| <i>Ports</i> | <i>Protocol</i> |
|------------------------|-----------------|
| 161 | udp |
| 162 | udp |
| <i>jboss.http.port</i> | tcp |

In the table above, *jboss.http.port* represents the port you selected for the NNMi management server during installation. Add the *jboss.http.port* value shown in the `$NnmDataDir/conf/nnm/props/nms-local.properties` file to the list of allowed ports. See the *nnm.ports* reference page or the UNIX manpage for more information.

- ▶ If you plan to use SSO, add the *jboss.https.port* value shown in the `$NnmDataDir/conf/nnm/props/nms-local.properties` file to the list of allowed ports.

Problem: Disabling a Postgres instance on an NNMi management server running the Linux operating system

Some Linux servers have an instance of Postgres running. You will need to disable the Postgres instance before installing NNMi. Complete the following steps to check for an instance of Postgres and to disable it:

- 1 To check for the presence of a Postgres instance, enter the following:

```
ps -ef | grep postgres
```

- 2 View the information on your screen. If there is an instance of Postgres running, disable it before continuing with the NNMi installation process using the following command:

```
chkconfig postgresql off
```

- 3 Install NNMi.

Glossary

A

account

See [user account](#).

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.

Auto-Discovery

A *spiral discovery* process during which all SNMP nodes that match one or more *discovery rules* are automatically discovered and placed under management. Contrast with [seeded discovery](#). See also [spiral discovery](#) and [discovery rule](#).

C

community string

A plain-text password used to authenticate SNMP queries to SNMP agents.

console

See [NNMi console](#).

D

discovery process

The process by which NNMi returns information about network nodes so that the nodes 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 continuous, or can be initiated on demand. See also [spiral discovery](#), [Auto-Discovery](#), and [seeded discovery](#).

discovery rule

A range of user-defined IP addresses used to limit the auto-discovery process. Configure a discovery rule in the NNMi console as part of setting up *auto-discovery*. See also [Auto-Discovery](#).

E

embedded database

The database provided with the NNMi software. You can also configure NNMi to use an Oracle database.

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

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 designed to aid network administration and to consolidate network management activities. Activities include the ongoing discovery of network nodes, monitoring events, and providing network fault management. See also [NNMi console](#).

I

incident

A notification of an important event regarding your network. The event is reflected by a change of background color of a node in a network map and is reported through incident views. Not all incidents result in a change in a node's color.

J

jboss application server

An application server program for use with Java 2 Platform, Enterprise Edition (J2EE), and Enterprise Java Beans (EJB).

L

Layer 2 (L2)

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. The switch is a device that redirects data messages at the Layer 2 level by using the destination

Media Access Control (MAC) address to determine where to direct the message.

Layer 3 (L3)

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. It also recognizes and forwards incoming messages for local host domains. Everything in a subnet is connected at the Layer 3 (IP) level.

N

NNMi

See [HP Network Node Manager i Software](#).

NNMi management server

The computer system on which the NNMi software is installed and on which the NNMi process and services run.

NNMi console

The user interface of the NNMi software. Operators and administrators use the NNMi console for most network management tasks in NNMi.

node

In the network context, a computer system or device (for example,

printer, router, or bridge) in a network. Nodes must be SNMP-configured to be fully managed by NNMi.

O

ovstatus command

A command that reports the current status of the NNMi managed processes. For more information, see [Help > Documentation Library > Reference Pages](#) (in the NNMi help).

ovstart command

A command that starts the NNMi managed processes. For more information, see [Help > Documentation Library > Reference Pages](#) (in the NNMi help).

ovstop command

A command that stops the NNMi managed processes. For more information, see [Help > Documentation Library > Reference Pages](#) (in the NNMi help).

P

port

In the hardware context, a location for passing information into and out of a network device.

Q

Quick Start Configuration Wizard

The Quick Start Configuration Wizard automatically runs

immediately after NNMi installation completes. Use the Quick Start Configuration Wizard to provide the read community strings for your SNMPv1 or SNMPv3 environment, set limits to the range of discovered nodes, or set up an administrator account.

R

rule

See [discovery rule](#).

Root Cause Analysis (RCA)

A class of problem solving methods aimed at identifying the root causes of network incidents. NNMi considers an incident to be active when the NNMi root cause analysis (RCA) engine is actively evaluating the problem reported by this incident.

S

seed

An SNMP 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. If auto-discovery is disabled, the discovery process is limited to *seeded discovery*. In this case, only the seeds that you specify are discovered and added to the NNMi database. See also

[Auto-Discovery](#) and [seeded discovery](#).

seeded discovery

A process, based on *seeds* or seed files, that discovers and returns Layer 2 connectivity information *only about the nodes that you specify as seeds*. Seeded discovery maintains a limited network inventory for specific queries and tasks. Contrast with [Auto-Discovery](#). See also [spiral discovery](#).

SID

System identifier.

Simple Network Management Protocol (SNMP)

The ARPA network management protocol running above TCP/IP that is used to communicate network management information between a manager process and an agent process.

SNMP

See [Simple Network Management Protocol \(SNMP\)](#).

SNMP trap

An unconfirmed event, generated by an SNMP agent in response to an internal state change or fault condition, which conforms to the protocol specified in RFC-1155.

spiral discovery

The ongoing refinement of network topology information, which includes

information about inventory, containment, relationships, and connectivity in networks managed by NNMi. See [discovery process](#). See also [Auto-Discovery](#) and [seeded discovery](#).

system account

A special account provided for use during NNMi installation. After installation, the system account should only be used for command-line security and for recovery purposes. See also [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

user account

A way to provide access to NNMi for users or groups of users. 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 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](#).

