

# HP Network Node Manager i-series Software

For the Solaris Operating System

Software Version: 8.10

---

## Installation Guide

Manufacturing Part Number: T4633-90011

Document Release Date: January 2009

Software Release Date: January 2009



## Legal Notices

### Warranty

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

The information contained herein is subject to change without notice.

### Restricted Rights Legend

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

### Copyright Notices

© Copyright 2008–2009 Hewlett-Packard Development Company, L.P.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). Portions Copyright © 1999-2003 The Apache Software Foundation. All rights reserved.

This product includes ASM Bytecode Manipulation Framework software developed by Institut National de Recherche en Informatique et Automatique (INRIA). Copyright © 2000-2005 INRIA, France Telecom. All Rights Reserved.

This product includes Commons Discovery software developed by the Apache Software Foundation (<http://www.apache.org/>). Copyright © 2002-2008 The Apache Software Foundation. All Rights Reserved.

This product includes Netscape JavaScript Browser Detection Library software, Copyright © Netscape Communications 1999-2001

This product includes Xerces-J xml parser software developed by the Apache Software Foundation (<http://www.apache.org/>). Copyright © 1999-2002 The Apache Software Foundation. All rights reserved.

This product includes software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>). Xpp-3 Copyright © 2002 Extreme! Lab, Indiana University. All rights reserved.

## Trademark Notices

DOM4J® is a registered trademark of MetaStuff, Ltd.

Java™ is a US trademark of Sun Microsystems, Inc.

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

Oracle® is a registered trademark of Oracle Corporation 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 USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

For the full Oracle license text, refer to the `license-agreements` directory on the NNMi product DVD.

Printed in the U.S.

## Documentation Updates

This manual’s title page 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>**

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

You can visit the HP Software Support web site at:

**[www.hp.com/go/hpsoftwaresupport](http://www.hp.com/go/hpsoftwaresupport)**

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support 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 areas also require a support contract.

To register for an HP Passport ID, go to:

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

To find more information about access levels, go to:

**[http://h20230.www2.hp.com/new\\_access\\_levels.jsp](http://h20230.www2.hp.com/new_access_levels.jsp)**

# Contents

1	Introducing HP Network Node Manager i-series Software	7
	The NNMi Console	7
	For Operators	7
	For Administrators	9
	About This Guide	10
2	Pre-Installation Checklists	11
	Supported Hardware and Software	11
	NNMi Management Server Preparation	13
	Database Installation	14
	Check for a Well-Configured DNS	16
	NNMi Quick Start Configuration Wizard	18
3	Installing and Enabling NNMi	19
	Installing NNMi	19
	Silently Installing NNMi	23
	Silent Installation Using a Sample ovinstallparams.ini File	24
	Using the Quick Start Configuration Wizard	28
	Licensing NNMi	33
	Preparing to Install a Permanent License Key	33
	Checking the License Type and the Number of Managed Nodes	33
	Obtaining and Installing a Permanent License Key	34
	Obtaining Additional License Keys	34
	Removing NNMi	35
	Accessing NNMi Installation Log Files	37
4	Getting Started with NNMi	39
	Accessing NNMi	39

NNMi Help .....	42
Configuring Network Discovery .....	43
Configuring Community Strings .....	44
Configuring Auto-Discovery Rules.....	45
Checking Discovery Progress.....	47
<b>A Additional Information</b> .....	49
Obtaining or Setting the Official Fully-Qualified Domain Name.....	49
Configuring an XServer for Installation.....	50
Enabling the Web Browser for the NNMi Console.....	50
Resetting the System Account Password .....	52
<b>B Troubleshooting Installation and Initial Startup</b> .....	53
Installation Problems .....	53
Initial Startup Problems .....	55
<b>Glossary</b> .....	59
<b>Index</b> .....	65

# 1 Introducing HP Network Node Manager i-series Software

HP Network Node Manager i-series 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.

## The NNMi Console

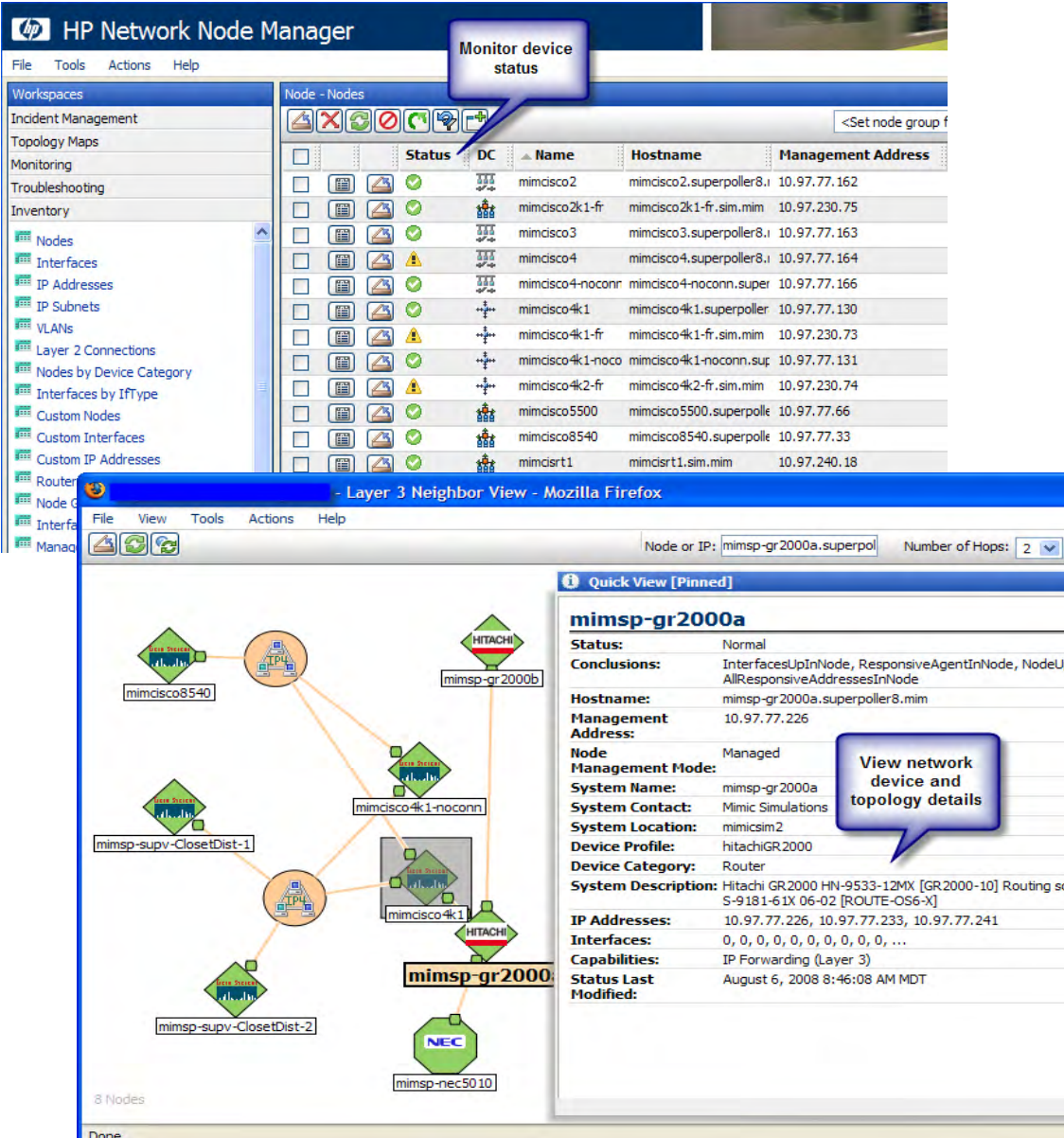
To provide a window into the state of your network, NNMi consolidates topology and status information into a single web-based user interface called the NNMi console. The NNMi console features a streamlined incident browser, a rich set of topology views, troubleshooting tools, and other features designed for efficiency and ease-of-use. In addition, the NNMi console provides secure access through pre-configured user roles for operators and administrators.

## For Operators

Operators can choose from several approaches to using NNMi for fault management. Whether you are starting from a trouble ticket or from information initially provided by NNMi, you can quickly detect, isolate, and troubleshoot network problems. You can also log each step taken to identify and fix network faults.

Figure 1 shows how the NNMi console helps you manage the network by monitoring device status, and by creating a dynamic representation of network topology for further diagnosis and troubleshooting.

Figure 1 Network management tasks



## For Administrators

Administrators use the NNMi console to configure the items that are described in [Table 1](#).

**Table 1 NNMi configuration**

What to Configure	How to Configure	NNMi Help Topics
Sign-In Access to NNMi	Use the <b>User Accounts and Roles</b> workspace to provide and control access to NNMi. Configure a name and password for each user. Assign a role to each user.	<i>Controlling Access to NNMi</i>
ICMP and SNMP Communication Protocols	Use the <b>Communication Configuration</b> workspace to specify the SNMP community strings for your environment. Configure NNMi settings for timeout, retry, and port usage for ICMP and SNMP traffic.	<i>Configuring Communication Protocol</i>
Discovery	Use the <b>Discovery Configuration</b> workspace to configure NNMi to discover only those devices that are important to your team.	<i>Discovering Your Network</i>
Filters	Use the <b>Node Groups</b> and <b>Interface Groups</b> workspaces to define filters that identify groups of devices. The groups you define can be used to fine-tune the monitoring configuration settings or used to filter table views.	<i>Define Node Groups</i> <i>Define Interface Groups</i>
Monitoring Network Health	Use the <b>Monitoring Configuration</b> workspace to define the method and frequency for monitoring important devices.	<i>Monitoring Network Health</i>
Incidents (optional)	Use the <b>Incident Configuration</b> workspace to review the pre-defined incident configurations that are provided with NNMi. Edit any of these pre-defined incident configurations and create new incident configurations.	<i>Configuring Incidents</i>
Actions Menu (optional)	Use the <b>URL Actions</b> workspace to configure the Actions menu. Edit the actions that are provided with NNMi and create new actions.	<i>Extending NNMi Capabilities</i>
Remote NNM 6.x/7.x Management Stations (optional)	Use the <b>Management Stations</b> workspace to enable NNM 6.x or 7.x events to be forwarded to NNMi.	<i>NNM 6.x/7.x Management Station Form</i>

## 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 that introduce the spiral discovery process to help you start using NNMi to manage your network.

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 42). Detailed information about customizing the NNMi configuration can be found in the *HP Network Node Manager i-series Software Deployment and Migration Guide* (see [Supported Hardware and Software](#) on page 11).

## 2 Pre-Installation 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 NNMi hardware and software that is shown in [Table 2](#).



For the most up-to-date versions of all documents listed in [Table 2](#), go to:

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

**Table 2    Software and hardware pre-installation checklist**

<b>Complete (y/n)</b>	<b>Documentation to Read</b>
	<i>HP Network Node Manager i-series Software Deployment and Migration Guide</i>  A web-only document providing advanced deployment and configuration information for NNMi enterprise installations available at <b><a href="http://h20230.www2.hp.com/selfsolve/manuals">http://h20230.www2.hp.com/selfsolve/manuals</a></b>
	<i>HP Network Node Manager Software Release Notes</i> <ul style="list-style-type: none"><li>• <b>Filename</b> = releasenotes_en.html</li><li>• <b>Product media</b> = Top-level or root directory</li><li>• <b>NNMi console</b> = <b>Help &gt; Documentation Library &gt; Release Notes</b></li></ul>
	<i>HP Network Node Manager i-series Software System and Device Support Matrix</i> <ul style="list-style-type: none"><li>• <b>Filename</b> = supportmatrix_en.html</li><li>• <b>Product media</b> = Top-level or root directory</li><li>• <b>NNMi console</b> = Linked from the release notes</li></ul>



HP updates the *HP Network Node Manager i-series 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-series Software System and Device Support Matrix* for your version of the software at:

**[http://www.hp.com/go/hpsoftwaresupport/support\\_matrices](http://www.hp.com/go/hpsoftwaresupport/support_matrices)**

You must have an HP Passport 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 dedicated 64-bit machine. To learn more about hardware prerequisites, see [Supported Hardware and Software](#) on page 11.

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

Before you install NNMi on the NNMi management server, complete the checklist in [Table 3](#). If you plan to use an Oracle database instance to store the NNMi data, see [Database Installation](#) on page 14.

**Table 3    NNMi management server pre-installation 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"><li>• It must be DNS resolvable to the NNMi server.</li><li>• It must be available for accessing the NNMi server from other computers on your network.</li></ul> <p>For more information, see <a href="#">Obtaining or Setting the Official Fully-Qualified Domain Name</a> on page 49.</p>
	<p>If you plan to install NNMi from an XServer, run the <code>xclock</code> command to verify that the XDisplay is configured correctly. If the clock does not appear, see <a href="#">Configuring an XServer for Installation</a> on page 50.</p>
	<p>Install and enable a supported web browser. See <a href="#">Supported Hardware and Software</a> on page 11 and <a href="#">Enabling the Web Browser for the NNMi Console</a> on page 50.</p>
	<p>Dynamic Host Configuration Protocol (DHCP) users: Make sure that the NNMi management server is consistently assigned the same IP address.</p>

**Table 3    NNMi management server pre-installation checklist**

Complete (y/n)	NNMi Management Server Preparation
	<p>NNMi uses several well-known ports that must be available on the NNMi management server prior to installing NNMi. Do not install NNMi until you verify that all of the following ports are available:</p> <ul style="list-style-type: none"><li>• TCP Ports 443, 1098, 1099, 3873, 4444, 4445, 4446, 4447, 8083, 8086, and 8087</li><li>• UDP Ports 162 and 696</li></ul>
	<p>Configure your NNMi management server to support your desired locale. Refer to the <i>HP Network Node Manager i-series Software System and Device Support Matrix</i> for more information about the locales that NNMi supports.</p>

## Database Installation

NNMi supports the following database options:

<i>Embedded database</i>	Provided with the NNMi product. The embedded database performs well for most deployments. This database has no installation prerequisites.
<i>Oracle database instance for NNMi</i>	Created by an Oracle database administrator. Use an Oracle database for enterprise installations and for larger production environments. To install an Oracle database instance for NNMi, complete the checklist in <a href="#">Table 4</a> .

**Table 4 Oracle database pre-installation checklist**

<b>Complete (y/n)</b>	<b>Oracle Database Preparation</b>
	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 <a href="#">Problem: jboss port contention</a> on page 56.
	Working with your Oracle database administrator, install an Oracle database according to the instructions provided by Oracle.
	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.
	(Recommended.) Assign a tablespace size depending on the number of nodes in your installation. Refer to the <i>HP Network Node Manager i-series Software System and Device Support Matrix</i> to learn about recommended Oracle configurations. See <a href="#">Supported Hardware and Software</a> on page 11 for more information.
	<p>Create an Oracle user with the following permissions:</p> <ul style="list-style-type: none"><li>• Create sequence</li><li>• Create session</li><li>• Create table</li><li>• Create view</li></ul> <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 IPv4 addresses. This can result in a large number of `nslookup` requests when Auto-Discovery is enabled.

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

- The DNS server is an authoritative server and does not forward DNS requests.
- The DNS server has consistent hostname-to-IPv4 address mappings and IPv4 address-to-hostname mappings.

If the network uses multiple DNS servers, all of them must respond consistently to any particular `nslookup` request.



Round-robin DNS (used to do load balancing of web application servers) is not appropriate because any given hostname can map to different IPv4 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:

- *All operating systems:* 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 localhost)  
  
<NNMi management server> (IPv4 address of the NNMi management server)
- Ensure that the `nslookup` search path resolves to the `nsswitch.conf` file. Refer to the `nsswitch.conf(4)` manpage that was provided with your operating system. Make sure that all identified DNS servers provide consistent hostname-to-IPv4 address mappings and IPv4 address-to-hostname mappings.

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 prior to configuring NNMi discovery. NNMi never issues a DNS request for hostnames or IPv4 addresses identified in these files:

- `hostNoLookup.conf` (enter fully-qualified domain names or wildcards that identify groups of hostnames)
- `ipNoLookup.conf` (enter IPv4 addresses or wildcards that identify groups of IPv4 addresses)

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

# NNMi Quick Start Configuration Wizard

You can run the **Quick Start Configuration Wizard** immediately after installation to help you configure NNMi in a limited (or test) environment. If you plan to use this wizard, complete the checklist in [Table 5](#).

**Table 5    NNMi Quick Start Configuration Wizard pre-installation 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 <a href="#">Licensing NNMi</a> on page 33.
	Determine IP addresses for discovery seeds. For information about seeds, see <a href="#">About Discovery Seeds and Auto-Discovery Rules</a> on page 28.
	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 23.

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.

- You can use the installation procedure shown in this chapter to install NNMi on servers running VMWare. Refer to the HP Network Node Manager i-series Software System and Device Support Matrix for more information on the VMWare software and hardware requirements.

### Installing NNMi

Make sure that you have completed the pre-installation requirements (see [Pre-Installation 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 14.

Unless you are upgrading from a supported version of NNMi, make sure that all previous NNMi installations are removed. See [Table 6](#) to view the supported upgrade paths. See [Removing NNMi](#) on page 35 for instructions on removing NNMi.

**Table 6 Supported Upgrades**

Current Version	Upgrade to NNMi 8.01	Upgrade to NNMi 8.02	Upgrade to NNMi 8.03 or higher *	Upgrade to NNMi 8.10
NNMi 8.01	NA	Supported	Supported	Install NNMi version 8.10.
NNMi 8.02	NA	NA	Supported	Install NNMi version 8.10.
NNMi 8.03 or higher *	NA	NA	NA	Install NNMi version 8.10.

\* Excluding NNMi 8.1x

To install NNMi, follow these steps:

- 1 Log in 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 wish to use, allowing you to pick from the languages your system is configured to support. It then checks your system to ensure that it is 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.

- 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, and 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 a new installation (not an upgrade to a newer 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 14](#).
    - The embedded database performs well for most deployments. For more information about embedded database limitations, refer to the *HP Network Node Manager i-series Software System and Device Support Matrix*. See [Supported Hardware and Software](#) on page 11.
    - When installing NNMi on UNIX or Linux systems, if you suspect that you do not have enough available disk space to complete a successful installation, see [Problem: The NNMi installation requires more disk space than is available on the host system](#) on page 54.
  - If you are completing a new installation (not an upgrade to a newer version of NNMi) and you plan to use an existing Oracle database instance, select **Oracle**; then continue to [step 11](#).
  - If you are completing an upgrade to a newer version of NNMi and you plan to use an existing Oracle database instance, continue to [step 14](#).
- 11 On the **Choose Database Initialization Preferences** page, select **Primary Server Installation**; then click **Next**.
- 12 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**.

- 13 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: NNMi installation process does not accept the Oracle user name and password](#) on page 53.
- 14 The **Install Checks** page displays progress as the installation software checks for additional NNMi installation requirements. After the check completes, click **Next**.
- 15 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 takes some time.
- 16 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 and to start the system configuration process.
- 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 56.
- 17 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 server, you can substitute the NNMi 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 49.

- 18 If you are completing a new installation, and not an upgrade to a newer version of NNMi, you will see the **System Account Password** dialog box. Follow the displayed instructions 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 52.

- 19 Click **Finish** to complete the rest of the installation.

After the installation software completes the NNMi configuration, the **Launch Quick Start Configuration Wizard** dialog box appears. For information about this wizard, see [Using the Quick Start Configuration Wizard](#) on page 28.

## 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 24 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 the silent installation.
- **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.

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

▶ Unless you are upgrading from a supported version of NNMi, make sure that all previous NNMi installations are removed. See [Table 6](#) on page 20 and [Removing NNMi](#) on page 35 for more information.

- 2 Copy the `ovinstallparams.ini` file from the support directory of the NNMi installation media to the `/tmp` directory.
- 3 Modify the `ovinstallparams.ini` file as shown below:

- a The following entries set the silent installation script to use the embedded database. Do not modify these settings.

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

- 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 28.

## 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:

```
/var/tmp/HPOvInstaller/NNM_<version_number>/
```

To silently install NNMi follow these steps:

- 1 On the target server (where you plan to install NNMi), log in with `root` privileges.
  - Unless you are upgrading from a supported version of NNMi, make sure that all previous NNMi installations are removed. See [Table 6](#) on page 20 and [Removing NNMi](#) on page 35 for more information.
- 2 Remove the `/var/tmp/HPOvInstaller/` directory, if it exists.
- 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 Solaris target server, the source server must also be a Solaris server.
- 4 On the source server, make a backup copy of the following file; then place the backup in a safe location:

```
/var/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 `/var/tmp/` directory.
  - b Rename the copied file to the following file name:

```
ovinstallparams.ini
```

- 6 Add the following 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 16](#) on page 22 of the interactive installation.

For example:

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

- 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 or administrator, 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 28.

# 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: from the NNMi console, select **Communication Configuration** from the **Configuration Workspace** and 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, refer to 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; refer to *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; refer to *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**; refer to *Configure Auto-Discovery Rules* in the NNMi help.

For overview information about the discovery process refer to *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 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 16](#) 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. Refer to 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 Sign in as follows:

- User Name: **system**
- Password: The password that you created at the end of the installation process (in [step 18](#) on page 23).

- 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

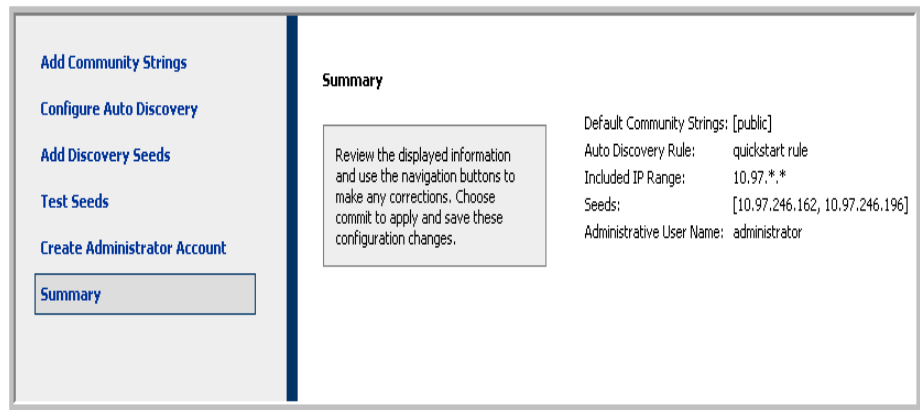
- 6 On the **Configure Seeds** page, add discovery seed information for your network; then click **Next**.

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. Refer to 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**.



- 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 [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 30 days after you install NNMi. This temporary Instant-On license key allows 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, refer to 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 will automatically unmanage 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, refer to *Delete a Node* in the NNMi help.

## Obtaining and Installing a Permanent License Key

In order 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
- Your company or organization information

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

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

```
$NNM_BIN/nnmlicense.ovpl NNM -g
```

- 2 When the **Autopass: License Management** dialog box appears, follow the instructions on the screen to obtain, install, and backup your permanent license key.

## 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>**



**Note to Developers:** With the NNMi Developer Toolkit, you can enhance the capabilities of NNMi by integrating custom web service clients. Upon installation of an NNMi Developer license, unpack the `nms-sdk-dev.jar` file located in the `doc` folder to access documentation and samples demonstrating the use of the NNMi Developer Toolkit.

# Removing NNMi

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

- 1 Log in with `root` privileges to the system where you plan to remove NNMi.
  - 2 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.bin` command with the `-i silent` option to silently remove NNMi.

The installation initialization process prompts you for the language you wish to use, allowing you to pick from the languages your system is configured to support. 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.

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

- 

- ## Installing and Enabling NNMi

# 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 (refer to the end of the `nnm-install-config.log` file).
- `nnm-install-config_sh.log`—Contains a record of some pre-installation and post-installation activity.

In addition, the following log files might be useful:

- `nnm-preinstallcheck.log`—If the pre-installation check contains unresolved warnings or errors, consult this log file to diagnose problems.
- `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 42).

### 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, Simplified Chinese, or Korean, 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 11).
- 2 Enable the web browser for JavaScript, allow pop-up windows from the NNMi management server, and allow the browser to accept cookies from the NNMi management server (see [Enabling the Web Browser for the NNMi Console](#) on page 50).

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

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

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 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. Refer to the *nnmofficialfqdn.ovpl* reference page, or the UNIX manpage, for more information.

If you do not know which port to use, see [Problem: NNMi console page cannot be found](#) on page 55.

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 41.

### 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, refer to *Controlling Access to NNMi* in the NNMi help.



To enable the NNMi web server to use the https protocol for transferring data to the NNMi console, refer to the *HP Network Node Manager i-series Software Deployment and Migration Guide*.

# 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*

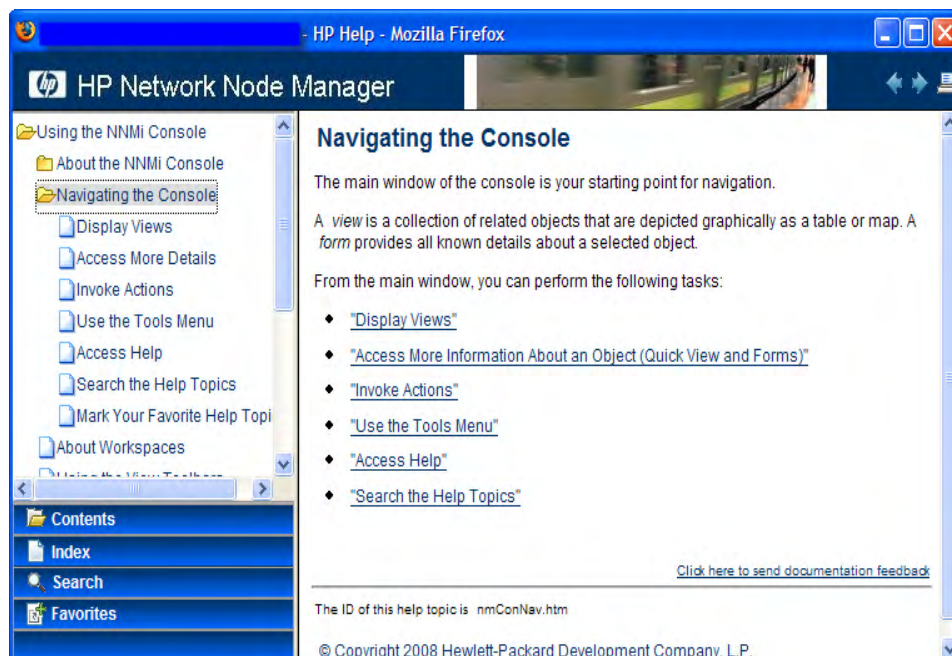
To access the NNMi help, click **Help** on the NNMi console menu bar; then click one of the options above the first separator line on the menu.



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 2 shows the NNMi help window.

**Figure 2** 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 28](#)) 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 7](#) summarizes these tasks.

**Table 7    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 <a href="#">Configuring Community Strings</a> on page 44.
	Using the NNMi console, configure the spiral discovery process as described in <a href="#">Configuring Auto-Discovery Rules</a> on page 45.
	Using the NNMi console, check the spiral discovery progress as described in <a href="#">Checking Discovery Progress</a> on page 47.

For more information about the discovery process, refer to *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:

The screenshot shows the 'Communication Configuration' form. On the left, there are three sections: 'Default SNMP Settings', 'Default ICMP Settings', and 'Registration'. 'Default SNMP Settings' includes fields for 'SNMP Timeout' (5 Seconds, 0 Milliseconds), 'SNMP Retries Count' (1), 'SNMP Port' (161), 'SNMP Proxy Address', 'SNMP Proxy Port', and 'SNMP Minimum Security Level' (Community Only). 'Default ICMP Settings' includes 'ICMP Timeout' (2 Seconds, 0 Milliseconds) and 'ICMP Retries Count' (1). 'Registration' shows 'Last Modified' as 'July 24, 2008 9:52:00 AM MDT'. On the right, the 'Default Community Strings' tab is active, showing a table with one entry: 'public'. The table has columns for 'Read Community String' and 'public'. The status bar at the bottom indicates 'Last update: 12:46:49 MDT', 'Total: 1', 'Selected: 1', 'Filter: OFF', and 'Auto refresh: OFF'.


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

For more information about setting up device community strings and loading community strings from a file, refer to *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 46).

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 On the **Auto-Discovery Rules** tab, click  **New**.
- 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 for this Rule**, select the appropriate auto-discovery actions for this rule.
- 6 On the **IP Ranges** tab, click  **New**.
- 7 On the **Auto Discovery IP Range** form, enter the **IP Range**, leave the **Range Type** set to **Include in rule**; then click  **Save and Close**.
- 8 On the **Auto-Discovery Rule** form, click  **Save and Close**.
- 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  **Save and Close** to save all new auto-discovery rules to the NNMi database.
- 11 Open the **Discovery Configuration** form again.
- 12 On the **Discovery Configuration** form, click the **Discovery Seeds** tab; then click  **New**.

13 On the **Discovery Seed** form, enter a hostname or IP address; then click  **Save and Close**.

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  **Save and Close**.

To monitor the progress of discovery, see [Checking Discovery Progress](#) on page 47.



For additional information about setting up discovery, refer to *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, refer to *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.

To gauge the progress of any discovery, do the following actions:

- During discovery, check the status of seeds by using **Configuration > Discovery Configuration**. On the **Discovery Seeds** tab, 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 progress of discovery by using **Help > About Network Node Manager i-series**. Check this message 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.



If you suspect a problem with discovery, see [Problem: NNMi is not discovering nodes](#) on page 58.



# A Additional Information

The following sections contain information that might be important for 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). It is also used to enable Single Sign-On (SSO) to NNM iSPIs.

- 1 To determine the official FQDN of the NNMi server, use one of the following methods:
  - Use the **`nnmofficialfqdn.ovpl`** command to display the value of the FQDN set during installation. Refer to the *nnmofficialfqdn.ovpl* reference page, or the UNIX manpage, for more information.
  - In the NNMi console, click **Help > About Network Node Manager i-Series**. Scroll down to find the value for the fully-qualified domain name beneath the **Management Server** heading.
- 2 If you need to change the official FQDN that was set during installation, use the **`nnmsetofficialfqdn.ovpl`** command. Refer to 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 official FQDN. To make it easier for users to satisfy this requirement, you can configure NNMi to redirect NNMi URLs to the official FQDN. If you do this, it is important that you have an appropriate official FQDN configured. Refer to the NNMi help for more information.

# Configuring an XServer for Installation

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

- 1 Set the `DISPLAY` environment variable to the appropriate value.
- 2 Run the `xhost` command to allow connection from the system running the installation process to the system displaying the installation process.
- 3 Run the `xclock` command to verify the configuration.

The clock should appear on the XServer.

## Enabling the Web Browser for the NNMi Console

Before signing in to NNMi, ensure that the web browser is configured to interact with the NNMi console. The following items must be enabled in the web browser:

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



To complete the following procedures, you will 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 **`nnmofficialfqdn.ovpl`** script. Refer to the *nnmofficialfqdn.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**.
- 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 On the **Content** tab, enable the **Block pop-up windows** check box; then click **Exceptions**.
- 6 Add the fully-qualified domain name of the NNMi management server to the list of allowed sites.
- 7 On the **Privacy** tab, enable the **Accept cookies from sites** check box; then click **Exceptions**.
- 8 Add the fully-qualified domain name of the NNMi management server to the list of allowed sites.
- 9 Click **OK**.
- 10 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, under **Settings**, select one of the options in the range **Accept All Cookies** to **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 impact.
- 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 or administrator, run the **`nnmchangesyspw.ovpl`** script to set the system password.
- 3 Start the NNMi processes using the **`ovstart -c`** command.

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

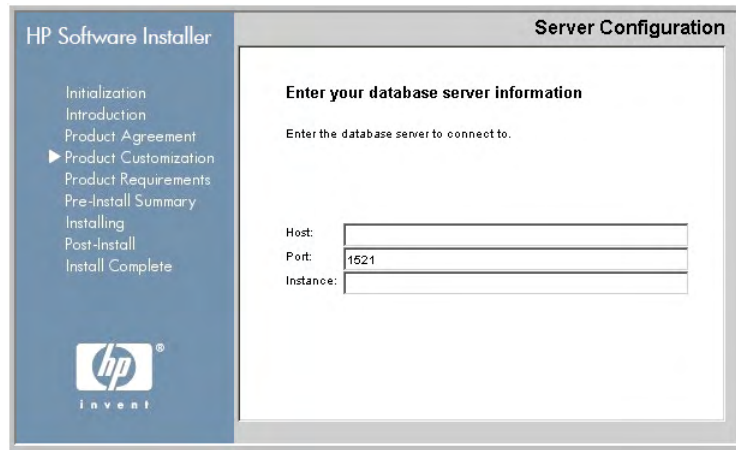
## B Troubleshooting Installation and Initial Startup

### Installation Problems

Problem: 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 try to continue the installation.
- 3 If [step 2](#) does not solve the problem, click **Previous** repeatedly to return to the **Setup Type** page of the installation wizard.
- 4 On the **Setup Type** page, select **Custom Installation**; then click **Next**.
- 5 Continue with the custom installation. When you get to the **Enter your database server information** page, as shown here, enter the host, port, and instance provided by your Oracle administrator.



- 6 Click **Next** to continue with 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 (\$OV\_INST\_DIR), and where to store the data files (\$OV\_DATA\_DIR). These locations default to the following settings:

- OV\_INST\_DIR=/opt/OV
- OV\_DATA\_DIR=/var/opt/OV

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.

- 3 Install NNMi.

# Initial Startup Problems

## Problem: 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, you must 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. Refer to 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:

```
/var/opt/OV/shared/nnm/conf/nnm.ports.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.

## 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:

```
/var/opt/OV/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:

```
/var/opt/OV/shared/nnm/conf/nnm.ports.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
```

## 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 8](#).

- 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 8 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**, the NNMi discovery process probably did not go well.

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

- a Make sure that the node is responding by pinging the node.
- b Make sure that the node has SNMP enabled.
- c Make sure that the node has your local management server on its SNMP agent's access list.
- d Make sure that you have configured the correct community strings for the nodes that NNMi is discovering. This information is listed on the **Communication Configuration** form on the **Default Community Strings** tab.

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

# Glossary

## A

### **account**

See [user account](#).

### **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. The embedded database performs well for most deployments. NNMi can be configured to use an Oracle database.

## H

### **HP Network Node Manager i-series 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.

## 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.

## M

### **management server**

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

## N

### **NNMi**

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

### **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 managed by NNMi.

## O

### ovstatus command

A command that reports the current status of the NNMi managed processes. For more information, refer to the `ovstatus` man page (at a command prompt) or **Help > Documentation Library > Reference Pages** (in the NNMi help).

### ovstart command

A command that starts the NNMi managed processes. For more information, refer to the `ovstatus` man page (at a command prompt) or **Help > Documentation Library > Reference Pages** (in the NNMi help).

### ovstop command

A command that stops the NNMi managed processes. For more information, refer to the `ovstatus` man page (at a command prompt) or **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.

## 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 have access to 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](#).



# Index

## A

- accessing
  - console, 39
  - installation log files, 37
- accounts
  - system
    - accessing NNMi, 41
    - installing NNMi, 23
  - user, 41
- Actions menu, configuring, 9
- administrator
  - help, 42
  - NNMi console functions, 9
  - role, 41
- algorithms, RCA, 7
- application server, jboss, 55
- approach, 10
- assigning, user roles, 9
- authoritative DNS, 16
- auto-discovery
  - configuring, 45
  - disabling, 28
  - mode, 46
  - rules, 28
- avoiding nslookup requests, 17

## B

- browser, see web browser

- browsers

- accessing NNMi console, 39
  - incident, 7

## C

- certificate, entitlement, 34
- checking
  - discovery progress, 47
  - license types, 33
- checklists
  - configuration, 18
  - discovery, 43
  - pre-installation, 11
- command-line security, 23
- commands
  - nnmlicense.ovpl, 34
  - nnmsnmpwalk, 58
  - ovstart, 56
  - ovstatus
    - silent installation, 25, 27
    - troubleshooting, 57
  - ovstop, 56
  - setup.bin
    - removing NNMi, 35
    - silent install, 25, 27
- community strings
  - configuring, 44
  - required, 43

- configuration
  - discovery checklist, 43
  - DNS service, 16
  - pre-installation checklist, 18
- configuring
  - Actions menu, 9
  - auto-discovery, procedure, 45
  - community strings, 44
  - device discovery, 9
  - network discovery, 43
  - NNMi, 10
  - NNMi console, 9
  - passwords, 9
  - traffic settings, 9
  - user names, 9
  - XServer, 50
- console, see NNMi console
- creating
  - actions, 9
  - incident configurations, 9

## D

- database
  - embedded, 14
  - Oracle, 14
  - Oracle instance, 15
  - Oracle tablespace size, 15
  - Oracle user, 15
- defining filters, 9
- de-installing NNMi, 35 to 36
- developer toolkit, 34
- devices
  - configuring discovery, 9
  - defining filters, 9
  - monitoring, 8 to 9
- DHCP, 13
- disabling
  - auto-discovery, 28

- discovery
  - auto-discovery rules, 46
  - checking progress, 47
  - configuration checklist, 43
  - configuring
    - auto-discovery, 45
    - network, 43
  - modes, 46
  - network, 46
  - nslookup requests, 16
  - seeds
    - mode, 46
    - rules, 28
  - spiral, 46
  - troubleshooting, 58
- disk space, insufficient, 54
- DISPLAY environment variable, 50
- DNS
  - authoritative server, 16
  - mappings must be consistent, 16
  - multiple servers, 16
  - round-robin, 16
  - secondary service on the NNMi management server, 16
  - used by NNMi, 16
  - well-configured, 16
- documentation, updated, 3
- domain name system, see DNS
- dynamic fault management, 7
- dynamic host configuration protocol, 13

## E

- embedded database, 14
- enabling
  - JavaScript, 39
  - NNM 6.x/7.x event forwarding, 9

- enabling web browser for NNMi
  - console, 50
- entitlement certificate, 34
- environment variables
  - DISPLAY, 50
- event correlation, 7

## F

- fault management, dynamic, 7
- files
  - hostNoLookup.conf, 17
  - hosts, 16
  - installation log, 37
  - ipNoLookup.conf, 17
  - nms-sdk-dev.zip, 34
  - nnm-install-config.log, 37
  - nnm-preinstallcheck.log, 37
  - nsswitch.conf, 16
  - ovinstallparams.ini, 23
- filters, defining, 9
- fully-qualified node names, 31

## G

- getting license passwords, 34
- Guest role, 41

## H

- hardware, supported, 11
- help, online, 42
- hostname-to-IP address mappings
  - must be consistent, 16
- hostNoLookup.conf file, 17
- hosts file, 16
- HP password delivery service, 34
- https protocol, 41

## I

- ICMP traffic, 9
- improving response time for
  - nslookup requests, 16
- incident
  - browser, 7
  - configurations, 9
- initial startup problems, 55 to 58
- installation
  - accessing log files, 37
  - options file, 23
  - pre-installation checklists, 11
  - preparing permanent license
    - password, 33
  - questions file, 26
  - silent install, 23
  - troubleshooting, 53 to 54
- installing NNMi, 10
  - installation
    - options file, 23
    - wizard, 19
  - insufficient disk space, 54
  - licenses, 33 to 34
  - Oracle database problem, 53
  - permanent license passwords, 34
  - silently, 23
- Instant-On license, 33
- insufficient disk space, 54
- interface, user, 7
- IP addresses
  - discovery seeds, entering, 31
  - management server, 34
- IP address-to-hostname mappings
  - must be consistent, 16
- IP ranges, valid, 30
- ipNoLookup.conf file, 17

## J

- jboss
  - application server
    - accessing NNMi console, 40
    - troubleshooting, 55
  - port
    - contention problem, 56
    - NNMi console access, 55
    - specifying for http, 27

## L

- licensing NNMi
  - checking types, 33
  - developer license, 34
  - procedures, 33 to 34
  - temporary license, 33
  - terms, 21
- location, documentation, 3
- log files, accessing installation, 37

## M

- management by exception, 7
- management server
  - DHCP, 13
  - IP address, 34
- management stations, NNM 6.x/7.x, 9
- manuals, updated, 3
- monitoring devices, 8 to 9
- multiple DNS servers, 16

## N

- network
  - discovery
    - configuring, 43
    - modes, 46
  - management tasks, 8
  - topology, 45
- nms-sdk-dev.zip file, 34
- NNM 6.x/7.x management stations, 9
- NNMi
  - database choices, 14
  - help, 42
  - release notes, 11
  - secondary DNS service, 16
  - system device support matrix, 11
- NNMi console
  - accessing, 39
  - administrator functions, 9
  - description, 7
  - enabling web browser for, 50
  - help, 42
  - jboss port problem, 55
  - operator functions, 7
  - signing in, 40
- NNMi Quick Start Configuration wizard
  - prerequisites, 18
  - URL, 29
  - using, 28
- nnm-install-config.log file, 37
- nnmlicense.ovpl command, 34
- nnm-preinstallcheck.log file, 37
- nnmsnmpwalk command, 58
- NNMUninstall.log file, 37
- nodes, pinging, 58

- nslookup requests
  - avoiding, 17
  - for NNMi discovery, 16
  - improving response time, 16
  - preventing delays, 16
- nsswitch.conf file, 16

## O

- obtaining license passwords, 34
- ongoing discovery, 45
- online help, 42
- Operator Level 1 role, 41
- Operator Level 2 role, 41
- operators
  - help, 42
  - NNMi console functions, 7
- Oracle database
  - installation problem, 53
  - instance for NNMi, 15
  - prerequisites, 14
  - tablespace size, 15
  - user for NNMi, 15
- out-of-box roles, 41
- ovinstallparams.ini file, 23
- ovstart command, 56
- ovstatus command
  - silent installation, 25, 27
  - troubleshooting, 57
- ovstop command, 56

## P

- passwords
  - delivery service URL, 34
  - license, 34
  - permanent license, 33
  - user
    - configuring, 9
    - signing in, 40
- permanent license password, 33
- pinging node, 58
- ports
  - configuring usage, 9
  - jboss contention, 56
- pre-configured user roles, 41
- pre-defined incident configurations, 9
- preparing permanent license password, 33
- prerequisites
  - database, 14
  - hardware, 11
  - NNMi Quick Start Configuration wizard, 18
  - software, 11
- preventing delays for nslookup requests, 16
- problems
  - initial startup, 55 to 58
  - installation, 53 to 54

## Q

- Quick Start Configuration wizard,
  - see NNMi Quick Start Configuration Wizard

## R

- RCA, 7

- release notes, 11
- removing NNMi, 35 to 36
- requesting license passwords, 34
- restarting services, 57
- retry, configuring, 9
- roles, user
  - configuring, 9
  - pre-defined, 41
- root
  - cause analysis, 7
  - privileges, 35
- round-robin DNS, 16
- rules, auto-discovery, 28

## S

- security, command-line, 23
- seeds, discovery, 28
- services
  - list, 57
  - restarting for NNMi, 57
- setup.bin command, 25, 27
- signing in to NNMi console, 40
- silent installation, 23
- SNMP
  - supported versions, 43
  - traffic, 9
- software
  - supported, 11
- source system, installation, 23
- spiral discovery, 46
- startup, troubleshooting, 55 to 58
- status, monitoring device, 8
- support, HP Software Support, 4

- supported
  - hardware, 11
  - SNMP versions, 43
  - software, 11
  - web browsers, 11
- symbolic links, 54
- system account
  - changing password, 23, 52
  - user roles, 41
- system device support matrix, 11

## T

- target system, installation, 23
- tasks
  - discovery configuration, 43
  - network management, 8
- technical support, 4
- temporary license, 33
- ticket, trouble, 7
- timeout, configuring, 9
- toolkit, developer, 34
- topology, network, 45
- traffic, configuring settings, 9
- trouble ticket, 7
- troubleshooting
  - discovery, 58
  - initial startup, 55 to 58
  - installation, 53 to 54
- types, checking license, 33

## U

- uninstalling NNMi, 35 to 36
- updated documentation, 3

## URLs

- HP password delivery service, 34
- NNMi console, 40
- NNMi Quick Start Configuration wizard, 29

## user

- guides, 3
- help, 42
- interface, 7
- name
  - configuring, 9
  - signing in, 40
- password
  - configuring, 9
  - signing in, 40
- roles, 9

- using, NNMi Quick Start Configuration wizard, 28

## V

- valid IP address ranges, 30
- versions, supported SNMP, 43

## W

### web browser

- accessing NNMi console, 39
- enabling for NNMi console, 50
- set language preference, 39
- supported, 11

### wizard

- installing NNMi, 19
- NNMi Quick Start Configuration URL, 29
- using, 28

## X

- XServer, configuring, 50

