

HP Network Node Manager i-series Software

for the Linux Operating System

Software Version: 8.1x Patch 5 (8.13)

Installation Guide

Document Release Date: August 2009

Software Release Date: August 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.

Trademark Notices

0® 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, 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/>). Portions Copyright © 1999-2003 The Apache Software Foundation. All rights reserved.

This product includes ASM Bytecode Manipulation Framework software developed by Institute 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.

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 and log on. To register for an HP Passport ID, go to:

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

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

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

Support

Visit the HP Software Support 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 log on. Many also require a support contract. To register for an HP Passport ID, go to:

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

To find more information about access levels, go to:

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

Contents

1	Introducing HP Network Node Manager i-series Software	9
	The NNMi Console.....	9
	For Operators.....	9
	For Administrators.....	11
	About This Guide.....	12
	Environment Variables Used in This Document.....	13
2	Preinstallation Checklists	15
	Supported Hardware and Software.....	15
	NNMi Management Server Preparation.....	17
	Database Installation.....	19
	Check for a Well-Configured DNS.....	21
	NNMi Quick Start Configuration Wizard.....	23
3	Installing and Enabling NNMi	25
	Installing NNMi.....	25
	Silently Installing NNMi.....	30
	Silent Installation Using a Sample oinstallparams.ini File.....	31
	Using the Quick Start Configuration Wizard.....	35
	Licensing NNMi.....	40
	Preparing to Install a Permanent License Key.....	40
	Checking the License Type and the Number of Managed Nodes.....	40
	Obtaining and Installing a Permanent License Key.....	41
	From the Command Line.....	41
	Using Autopass and your HP Order Number (not possible behind a firewall) ...	41
	Obtaining Additional License Keys.....	42
	Removing NNMi.....	43
	Accessing NNMi Installation Log Files.....	45

4	Getting Started with NNMi	47
	Accessing NNMi	47
	NNMi Help	50
	Configuring Network Discovery	51
	Configuring Community Strings	52
	Configuring Auto-Discovery Rules	53
	Checking Discovery Progress	55
A	Additional Information	57
	Obtaining or Setting the Official Fully-Qualified Domain Name	57
	Configuring an XServer for Installation	58
	Enabling the Web Browser for the NNMi Console	58
	Installing Required Libraries on Linux	60
	Red Hat 4.6	60
	Red Hat 5.2	61
	Installing NNMi 8.10 on Red Hat 5.2	62
	Resetting the System Account Password	63
B	Troubleshooting Installation and Initial Startup	65
	Installation Problems	65
	Initial Startup Problems	67
	Glossary	73
	Index	77

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

The screenshot displays the HP Network Node Manager interface. The top window shows a list of nodes with columns for Status, DC, Name, Hostname, and Management Address. A callout bubble points to the 'Monitor device status' column. Below this, a 'Layer 3 Neighbor View' window shows a network topology diagram with nodes like mimisco8540, mimisco4k1, and mimp-gr2000. A callout bubble points to the 'View network device and topology details' button. To the right, a 'Quick View [Pinned]' window provides detailed information for the selected device, mimp-gr2000a.

Status	DC	Name	Hostname	Management Address
	---	mimisco2	mimisco2.superpoller8.i	10.97.77.162
	---	mimisco2k1-fr	mimisco2k1-fr.sim.mim	10.97.230.75
	---	mimisco3	mimisco3.superpoller8.i	10.97.77.163
	---	mimisco4	mimisco4.superpoller8.i	10.97.77.164
	---	mimisco4-noconn	mimisco4-noconn.super	10.97.77.166
	---	mimisco4k1	mimisco4k1.superpoller	10.97.77.130
	---	mimisco4k1-fr	mimisco4k1-fr.sim.mim	10.97.230.73
	---	mimisco4k1-noco	mimisco4k1-noconn.sup	10.97.77.131
	---	mimisco4k2-fr	mimisco4k2-fr.sim.mim	10.97.230.74
	---	mimisco5500	mimisco5500.superpolle	10.97.77.66
	---	mimisco8540	mimisco8540.superpolle	10.97.77.33
	---	mimiscrt1	mimiscrt1.sim.mim	10.97.240.18

Quick View [Pinned]	
mimisp-gr2000a	
Status:	Normal
Conclusions:	InterfacesUpInNode, ResponsiveAgentInNode, NodeU AllResponsiveAddressesInNode
Hostname:	mimisp-gr2000a.superpoller8.mim
Management Address:	10.97.77.226
Node Management Mode:	Managed
System Name:	mimisp-gr2000a
System Contact:	Mimic Simulations
System Location:	mimicsim2
Device Profile:	hitachiGR2000
Device Category:	Router
System Description:	Hitachi GR2000 HN-9533-12MX [GR2000-10] Routing s S-9181-61X 06-02 [ROUTE-OS6-X]
IP Addresses:	10.97.77.226, 10.97.77.233, 10.97.77.241
Interfaces:	0, 0, 0, 0, 0, 0, 0, 0, ...
Capabilities:	IP Forwarding (Layer 3)
Status Last Modified:	August 6, 2008 8:46:08 AM MDT

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 User Accounts and Roles 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>
Actions Menu	Use the URL Actions option in the Configuration workspace to configure the Actions menu. Edit the actions that are provided with NNMi and create new actions.	<i>Extending NNMi Capabilities</i>
Device Profiles	Use the Device Profiles option in the Configuration workspace to update device profile information.	<i>Configure Device Profiles</i>
Discovery	Use the Discovery Configuration workspace to configure NNMi to discover only those devices that are important to your team.	<i>Discovering Your Network</i>
Filters	Use the Node Groups and Interface Groups 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>
ICMP and SNMP Communication Protocols	Use the Communication Configuration 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>
Incidents	Use the Incident Configuration 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>
Interface Types	Use the IfTypes option in the Configuration workspace to add a new interface type to the NNMi list of Interface Type definitions.	<i>Add New IfTypes (Interface Types) to the List</i>

Table 1 NNMi configuration

What to Configure	How to Configure	NNMi Help Topics
Management Stations (6.x/7.x)	Use the Management Stations workspace to enable NNM 6.x or 7.x events to be forwarded to NNMi.	<i>Configuring Remote NNM 6.x and 7.x Management Stations</i>
Monitoring Network Health	Use the Monitoring Configuration workspace to define the method and frequency for monitoring important devices.	<i>Monitoring Network Health</i>
Node Group Map Settings	Use the Node Group option in the Configuration workspace to specify the Node Group map configuration.	<i>Define Node Group Map Settings</i>
Status	Use the Status Configuration option in the Configuration workspace to configure how NNMi calculates Node Group Status.	<i>Configure Node Group Status</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 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 50). Detailed information about customizing the NNMi configuration can be found in the *HP Network Node Manager Deployment Guide* (see [Supported Hardware and Software](#) on page 15).

Environment Variables Used in This Document

This document uses the following NNMi environment variables to reference file and directory locations. The default values are listed here. Actual values depend on the selections made during NNMi installation.

- *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 Deployment Guide*.

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 NNMi hardware and software shown in [Table 2](#) on page 16.



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

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

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

Table 2 Software and hardware preinstallation checklist

Complete (y/n)	Documentation to Read
	<i>HP Network Node Manager Deployment Guide</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 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-series 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-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://h20230.www2.hp.com/selfsolve/manuals>

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 15.

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 19.

Table 3 NNMi management server preinstallation checklist

Complete (y/n)	NNMi Management Server Preparation
	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: <ul style="list-style-type: none">• It must be DNS resolvable to the NNMi server.• It must be available for accessing the NNMi server from other computers on your network. For more information, see Obtaining or Setting the Official Fully-Qualified Domain Name on page 57.
	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 Configuring an XServer for Installation on page 58.
	Install and enable a supported web browser. See Supported Hardware and Software on page 15 and Enabling the Web Browser for the NNMi Console on page 58.
	Dynamic Host Configuration Protocol (DHCP) users: Make sure that the NNMi management server is consistently assigned the same IP address.

Table 3 NNMi management server preinstallation checklist

Complete (y/n)	NNMi Management Server Preparation
	<p>To install NNMi on a 64-bit Linux server, make sure your server contains the following files. These are the exact library versions that NNMi requires:</p> <ul style="list-style-type: none">• /usr/lib64/libstdc++.so.5• /usr/lib64/libstdc++.so.5.0.7 <p>For more information see Installing Required Libraries on Linux on page 60.</p>
	<p>Some Linux servers have an instance of Postgres running. You will need to disable this Postgres instance prior to installing NNMi. See Problem: Disabling a Postgres Instance on an NNMi Management Server Running the Linux Operating System on page 70.</p>
	<p>To prevent problems with the <code>nmsdbmgr</code> component, modify the <code>kernel.shmax</code> parameter. See Problem: The NNMi <code>nmsdbmgr</code> component does not operate correctly after installing NNMi on a Linux NNMi Management Server or after rebooting the NNMi Management Server on page 71.</p>

Table 3 NNMi management server preinstallation checklist

Complete (y/n)	NNMi Management Server Preparation
	NNMi 8.12 supports Linux Red Hat 5.2 after you complete some configuration steps. See Installing NNMi 8.10 on Red Hat 5.2 on page 62.
	NNMi uses several well-known ports that must be available on the NNMi management server prior to installing NNMi. Verify that all of the following ports are available before installing NNMi: <ul style="list-style-type: none">• TCP Ports 80, 443, 1098, 1099, 3873, 4444, 4445, 4446, 4447, 4457, 4458, 8083, 8086, and 8087• UDP Ports 162, 696, and 45588
	If you require a non-US-English locale, configure the NNMi management sever to support the locale you require (such as Japanese or Korean). See the <i>HP Network Node Manager i-series Software System and Device Support Matrix</i> for more information about the locales that NNMi supports.

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. Use an Oracle database for enterprise installations and for larger production environments. To install an Oracle database instance for NNMi, complete the checklist in [Table 4](#).

Table 4 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 67.
	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.
	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. The database requirement grows as NNMi discovers additional nodes, so watch this growth carefully and expand your configured tablespace size when necessary.
	Create an Oracle user with the following permissions: <ul style="list-style-type: none">• Create sequence• Create session• Create table• Create view Make note of the Oracle user name and password; you will need this information during the NNMi installation.

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 `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-IP address mappings and IP 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 IP addresses over time.



To improve the response time for `nslookup`, deploy a secondary DNS service on the NNMi management server or another system with 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> (IP address of the NNMi management server)
```
- Make sure that the `nslookup` search path resolves to the `nsswitch.conf` file. See the `nsswitch.conf(4)` manpage provided with your operating system. Make sure that all identified DNS servers provide consistent hostname-to-IP address mappings and IP 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 IP addresses identified in these files:

- `hostNoLookup.conf` (enter fully-qualified domain names or wildcards that identify groups of hostnames)
- `ipNoLookup.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 5](#).

Table 5 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 40.
	Determine IP addresses for discovery seeds. For information about seeds, see About Discovery Seeds and Auto-Discovery Rules on page 35.
	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 30.

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. See 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 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 19.

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 43 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 patches, see the patch installation instructions.

To install NNMi, follow these steps:

- 1 Log on 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 your system configuration supports. 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 [Installing Required Libraries on Linux](#) on page 60.

- 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](#).
 - ▶ 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 66.
 - 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 65.
- 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.

- ▶ If you choose to use an Oracle database for your NNMi installation, the installation script still installs the embedded (Postgres) database. NNMi stores internal application data in the embedded database. If you notice this embedded database installation detail during your NNMi installation, this is a normal part of installing NNMi when using an Oracle database with NNMi.

16 In the **NNM Web Server Port** dialog box, note 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 67.

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 57.

- 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 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 63.

- 19 Click **Finish** to complete 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 35.

▶ During installation, the NNMi installation routine creates an `nmsdbmgr` account. NNMi uses the `nmsdbmgr` account to run the embedded DB service, `nmsdbmgr`. This account is required because `root` cannot run the embedded database.

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 31 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 33 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 on 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 26 and [Removing NNMi](#) on page 43 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. Configure these settings as shown below:

```
[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 35.

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:

```
/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 [Table 6](#) on page 26 and [Removing NNMi](#) on page 43 for more information.
- 2 Remove the `/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 25.
 - ▶ 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 Linux target server, the source server must also be a Linux server.
- 4 On the source server, make a backup copy of the following file; then place the backup in a safe location:

```
/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 `/tmp/` directory.
 - 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 16](#) on page 29 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 35.

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 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 29.


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 18](#) on page 30).

- 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:
 - 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 30 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
- Your company or organization information

From the Command Line

- 1 At the command prompt for the NNMi management server, enter the following:

```
/opt/OV/bin/nmlicense.ovpl NNM -f license_file
```

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

- 2 NNMi automatically completes the installation.

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:

```
/opt/OV/bin/nmlicense.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.

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. 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.

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

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 To begin uninstalling NNMi, do the following:
 - At a command prompt, enter the following command: `/opt/OV/Uninstall/NNM/setup.bin`

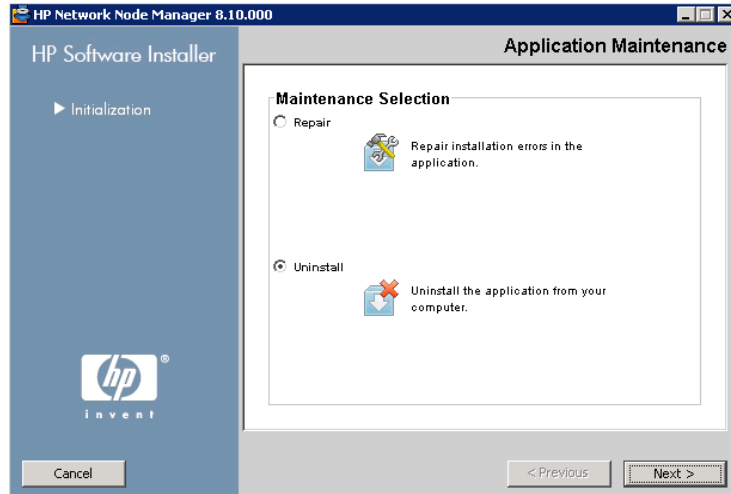
 You can use the `setup.bin` command with the `-i silent` option to silently remove NNMi.

The installation initialization process prompts you for the language you want 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**.

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



- 5 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**.
- 6 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/nm/
```

The most important log files are as follows:

- `nm-install-config.log`: Contains a record of the most recent installation, including the processes that have been initialized (see the end of the `nm-install-config.log` file).
- `nm-install-config_sh.log`: Contains a record of some preinstallation and postinstallation activity.

In addition, the following log files might be useful:

- `/tmp/nm-preinstallcheck.log`: If the preinstallation 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 50).

Accessing NNMi

Now that you have installed NNMi, completed postinstallation 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 15).
- 2 Enable the web browser for JavaScript, enable pop-up windows from the NNMi management server, and enable the browser to accept cookies from the NNMi management server (see [Enabling the Web Browser for the NNMi Console](#) on page 58).

- 3 Enter the following URL into the 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 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: NNMi console page cannot be found](#) on page 67.

- ▶ 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 may 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 69.

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 49.

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.



To enable the NNMi web server to use the https protocol for transferring data to the NNMi console, see the *HP Network Node Manager Deployment 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*

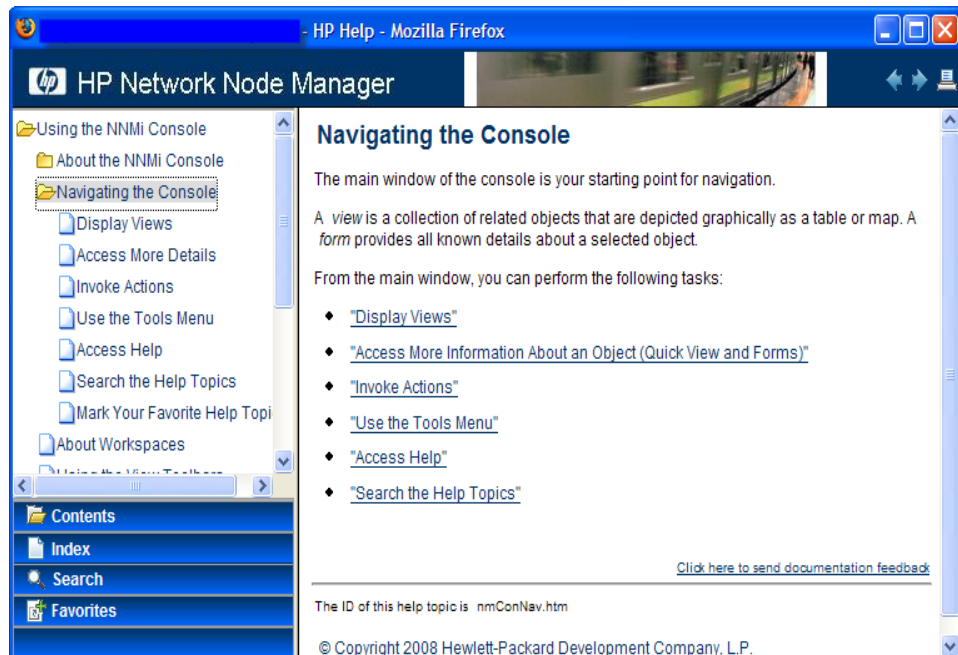
To access the NNMi help, click **Help** on the NNMi console menu bar; then click one of the options above the first separator line on the menu.



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 35](#)) 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 Configuring Community Strings on page 52.
	Using the NNMi console, configure the spiral discovery process as described in Configuring Auto-Discovery Rules on page 53.
	Using the NNMi console, check the spiral discovery progress as described in Checking Discovery Progress on page 55.

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 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, 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 54).

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 55.



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 the progress of any discovery. Using the NNMi console, check the discovery progress using any of the following methods:

- 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, discovery is complete.
- During discovery, 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, discovery is complete.
- During discovery, click **Network Overview** in the Topology Maps workspace. Watch the map grow in complexity during a one hour period. If the map growth slows and then stops growing over the sampling period, discovery is complete.



If you suspect a problem with discovery, see [Problem: NNMi is not discovering nodes on page 69](#).

A Additional Information

The following sections contain important additional 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 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-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 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 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 enable a 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 sign on 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 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. See 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 **Enable**.
- 4 On the **Privacy** tab select **Settings**; 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 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.

Installing Required Libraries on Linux

If you have identified the server to install NNMi, but have not yet installed Linux on that server, do the following during your Linux operating system installation:

Red Hat 4.6

- 1 Select the option to install a custom set of packages.
- 2 Select the package labeled Compatibility Arch Developer Support.
- 3 Complete the operating system installation.

To install NNMi on a 64-bit Linux server, you must have the following library files installed. These are the exact library versions that NNMi requires:

- /usr/lib64/libstdc++.so.5
- /usr/lib64/libstdc++.so.5.0.7

If you find that these files are not installed, do not install NNMi since it will not install or function correctly. To resolve this issue, complete the following procedure:

- 1 Find the Red Hat Linux Advanced Server (AS) Version 4-Update 6x86-64 or Enterprise Server (ES) Version 4-Update 6x86-64 installation disks and insert Red Hat installation disk 2, if available. (See below if you cannot locate the proper installation disk.)
- 2 Change to the following directory: /media/cdrom/RedHat/RPMS.
- 3 Run the following command:

```
rpm -i compat-libstdc++-33-3.2.3-47.3.x86_64.rpm
```
- 4 After this command completes, you are ready to install NNMi on your Linux server.

If you cannot locate the Red Hat Linux installation disks, you need to do the following to install the 32-bit and 64-bit RPMs that contain these libraries:

- /usr/lib/libstdc++.so.5.0.7 (32-bit)
 - /usr/lib64/libstdc++.so.5.0.7 (64-bit)
- 1 Run the **up2date** command. You will need a Red Hat support key.

- 2 Obtain the following RPMs:

```
compat-libstdc++-33-3.2.3-47.3.i386.rpm
```

```
compat-libstdc++-33-3.2.3-47.3.x86_64.rpm
```

- 3 Run the following commands:

```
a rpm -i compat-libstdc++-33-3.2.3-47.3.i386.rpm
```

```
b rpm -i compat-libstdc++-33-3.2.3-47.3.x86_64.rpm
```

After this command completes, you are ready to install NNMi on the Linux server.

Red Hat 5.2

- 1 Select the option to install a custom set of packages.
- 2 Select the package labeled **Compatibility Arch Developer Support**.
- 3 Complete the operating system installation.

To install NNMi on a 64-bit Linux server, you must have the following library files installed. These are the exact library versions that NNMi requires:

- /usr/lib64/libstdc++.so.5
- /usr/lib64/libstdc++.so.5.0.7
- /usr/lib/libstdc++.so.5
- /usr/lib/libstdc++.so.5.0.7

To see if these libraries are installed, run the following command:

```
yum list compat-libstdc++-33
```

The results should resemble the following text:

```
Installed Package
```

```
compat-libstdc++-33.i386 3.2.3-61 installed
```

```
compat-libstdc++-33.x86_64 3.2.3-61 installed
```

If the results show available instead of installed, you need to install the libraries before installing NNMi.

If you find that these files are not installed, do not install NNMi since it will not install or function correctly. To resolve this issue, complete the following procedure:

- 1 Find the Red Hat Linux installation disks and insert Red Hat installation disk 3, if available. (See below if you cannot locate the proper installation disk.)
- 2 Change to the following directory: `/media/cdrom/RedHat/RPMS`
- 3 Run the following commands:

```
rpm -i compat-libstdc++-33-3.2.3-*.i386.rpm
```

```
rpm -i compat-libstdc++-33-3.2.3-*.x86_64.rpm
```

After these commands complete, you are ready to install NNMi on the Linux server.

If you cannot locate the Red Hat Linux installation disks, you need to do the following to install the 32-bit and 64-bit RPMs that contain these libraries:

- `/usr/lib/libstdc++.so.5.0.7` (32-bit)
- `/usr/lib64/libstdc++.so.5.0.7` (64-bit)

Run the following command to download and install the latest library version. You will need a Red Hat support key.

```
yum install compat-libstdc++-33
```

After this command completes, you are ready to install NNMi on the Linux server.

Installing NNMi 8.10 on Red Hat 5.2

After you complete the following configuration steps, you will be able to run NNMi on Red Hat 5.2. These steps include the tasks you need to complete after installing NNMi 8.10.

- 1 Before installing NNMi 8.10, do one the following to set SELinux to either disabled or permissive:
 - Edit the `/etc/sysconfig/selinux` file and make the SELinux changes.

- Use the **System->Administration->SELinux Management** tool and make the SELinux changes.

Write down the original value of SELinux, so you can change this parameter to its original value after you complete this procedure.

- 2 Install NNMi 8.10.
- 3 After you successfully complete the NNMi 8.10 installation, run the following command: **chcon -t textrel_shlib_t /opt/OV/lib/***



Running the above command results in the following errors. You can safely ignore these errors:

```
chcon: /opt/OV/lib/libxalan-c.so.18: No such file or directory
```

```
chcon: /opt/OV/lib/libxalanMsg.so.18: No such file or directory
```

```
chcon: /opt/OV/lib/libxerces-c.so.25: No such file or directory
```

- 4 Set SELinux to its original value.
- 5 Install the NNMi 8.1x Patch 3.



After you install NNMi 8.1x Patch 3 you no longer need to complete the steps above to install future patches.

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

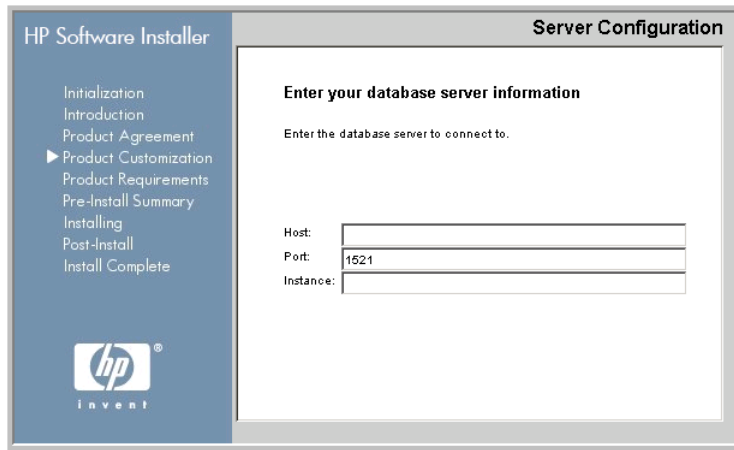
B Troubleshooting Installation and Initial Startup

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` man page 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. 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/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. See the *nnm.ports.properties* 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/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
```

See the *nnm.ports.properties* 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 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**, 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 -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 may 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 may 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/shared/nm/conf/nm.ports.properties` file to the list of allowed ports. See the *nm.ports.properties* reference page, or the UNIX man page, for more information.

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 prior to 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.

Problem: The NNMi nmsdbmgr component does not operate correctly after installing NNMi on a Linux NNMi Management Server or after rebooting the NNMi Management Server

If you run the `ovstatus -c nmsdbmgr` command on the NNMi management server, and the results show problems with the `nmsdbmgr` component, you need to adjust the `kernel.shmmax` parameter.

- 1 Run the `/sbin/sysctl -a | /bin/grep kernel.shmmax` command on the NNMi management server.
- 2 Check the results. If the display shows less than 300 megabytes (300,000,000 bytes), continue with [step 3](#) to change the value.
- 3 Run the `/sbin/sysctl -w kernel.shmmax=300000000` command.
- 4 Restart the NNMi processes using the `ovstart -c` command.
- 5 Run the `ovstatus -c nmsdbmgr` command and check the results. If the `nmsdbmgr` component is now functioning correctly, complete [step](#) .

To make this a permanent change to the `kernel.shmmax` parameter, edit the `/etc/sysctl.conf` file and add the following entry: `kernel.shmmax = 300000000`. Be sure to save your changes.

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. You can also configure NNMi 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 fully managed by NNMi.

O

ovstatus command

A command that reports the current status of the NNMi managed processes. For more information, see the `ovstatus` manpage (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, see the `ovstatus` manpage (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, see the `ovstatus` manpage (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 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](#).

Index

A

- accessing
 - console, 47
 - installation log files, 45
- accounts
 - system
 - accessing NNMi, 49
 - installing NNMi, 30
 - user, 49
- Actions menu, configuring, 11
- administrator
 - help, 50
 - NNMi console functions, 11
 - role, 49
- algorithms, RCA, 9
- application server, jboss, 67
- approach, 12
- assigning, user roles, 11
- authoritative DNS, 21
- auto-discovery
 - configuring, 53
 - disabling, 35
 - mode, 54
 - rules, 35
- avoiding nslookup requests, 22

B

- browser, see web browser

browsers

- accessing NNMi console, 47
- incident, 9

C

- certificate, entitlement, 41
- checking
 - discovery progress, 55
 - license types, 40
- checklists
 - configuration, 23
 - discovery, 51
 - preinstallation, 15
- command-line security, 30
- commands
 - nnmlicense.ovpl, 41
 - nnmsnmpwalk, 69
 - ovstart, 68
 - ovstatus
 - silent installation, 32, 34
 - troubleshooting, 68
 - ovstop, 68
 - setup.bin
 - removing NNMi, 43
 - silent install, 32, 34
- community strings
 - configuring, 52
 - required, 51

- configuration
 - discovery checklist, 51
 - DNS service, 21
 - preinstallation checklist, 23
- configuring
 - Actions menu, 11
 - auto-discovery, procedure, 53
 - community strings, 52
 - device discovery, 11
 - network discovery, 51
 - NNMi, 12
 - NNMi console, 11
 - passwords, 11
 - traffic settings, 11
 - user names, 11
 - XServer, 58
- console, see NNMi console
- creating
 - actions, 11
 - incident configurations, 11

D

- database
 - embedded, 19
 - Oracle, 19
 - Oracle instance, 20
 - Oracle tablespace size, 20
 - Oracle user, 20
- defining filters, 11
- deinstalling NNMi, 43 to 44
- developer toolkit, 42
- devices
 - configuring discovery, 11
 - defining filters, 11
 - monitoring, 10 to 12
- DHCP, 17
- disabling
 - auto-discovery, 35

- discovery
 - auto-discovery rules, 54
 - checking progress, 55
 - configuration checklist, 51
 - configuring
 - auto-discovery, 53
 - network, 51
 - modes, 54
 - network, 54
 - nslookup requests, 21
 - seeds
 - mode, 54
 - rules, 35
 - spiral, 54
 - troubleshooting, 69
- disk space, insufficient, 66
- DISPLAY environment variable, 58
- DNS
 - authoritative server, 21
 - mappings must be consistent, 21
 - multiple servers, 21
 - round-robin, 21
 - secondary service on the NNMi management server, 21
 - used by NNMi, 21
 - well-configured, 21
- domain name system, see DNS
- dynamic fault management, 9
- dynamic host configuration protocol, 17

E

- embedded database, 19
- enabling
 - JavaScript, 47
 - NNM 6.x/7.x event forwarding, 12
- enabling web browser for NNMi console, 58
- entitlement certificate, 41

environment variables
DISPLAY, 58

event correlation, 9

F

fault management, dynamic, 9

files

- hostNoLookup.conf, 22
- hosts, 21
- installation log, 45
- ipNoLookup.conf, 22
- nms-sdk-dev.zip, 42
- nnm-install-config.log, 45
- nnm-preinstallcheck.log, 45
- nsswitch.conf, 21
- ovinstallparams.ini, 30

filters, defining, 11

fully-qualified node names, 38

G

getting license passwords, 41

Guest role, 49

H

hardware, supported, 15

help, online, 50

hostname-to-IP address mappings must be consistent, 21

hostNoLookup.conf file, 22

hosts file, 21

HP password delivery service, 42

https protocol, 49

I

ICMP traffic, 11

improving response time for nslookup requests, 21

incident

- browser, 9
- configurations, 11

initial startup problems, 67 to 69

installation

- accessing log files, 45
- options file, 30
- preinstallation checklists, 15
- preparing permanent license password, 40
- questions file, 33
- silent install, 30
- troubleshooting, 65 to 66

installing NNMi, 12

installation

- options file, 30
- wizard, 25
- insufficient disk space, 66
- licenses, 40 to 42
- Oracle database problem, 65
- permanent license passwords, 41
- silently, 30

Instant-On license, 40

insufficient disk space, 66

interface, user, 9

IP addresses

- discovery seeds, entering, 38
- management server, 41

IP address-to-hostname mappings must be consistent, 21

ipNoLookup.conf file, 22

IP ranges, valid, 37

J

- jboss
 - application server
 - accessing NNMi console, 48
 - troubleshooting, 67
 - port
 - contention problem, 67
 - NNMi console access, 67
 - specifying for http, 34

L

- licensing NNMi
 - checking types, 40
 - developer license, 42
 - procedures, 40 to 42
 - temporary license, 40
 - terms, 27
- Linux libraries
 - installing, 60
 - required, 60
- log files, accessing installation, 45

M

- management by exception, 9
- management server
 - DHCP, 17
 - IP address, 41
- management stations, NNM 6.x/7.x, 12
- monitoring devices, 10 to 12
- multiple DNS servers, 21

N

- network
 - discovery
 - configuring, 51
 - modes, 54
 - management tasks, 10
 - topology, 53
- nmsdbmgr account, 30
- nmsdbmgr service, 30
- nms-sdk-dev.zip file, 42
- NNM 6.x/7.x management stations, 12
- NNMi
 - database choices, 19
 - help, 50
 - release notes, 15
 - secondary DNS service, 21
 - system device support matrix, 15
- NNMi console
 - accessing, 47
 - administrator functions, 11
 - description, 9
 - enabling web browser for, 58
 - help, 50
 - jboss port problem, 67
 - modifying Linux firewall, 48, 69
 - operator functions, 9
 - signing in, 48
- nnm-install-config.log file, 45
- NNMi Quick Start Configuration wizard
 - prerequisites, 23
 - URL, 36
 - using, 35
- nnmlicense.ovpl command, 41
- nnm-preinstallcheck.log file, 45
- nnmsnmpwalk command, 69
- NNMUninstall.log file, 45
- nodes, pinging, 69

- nslookup requests
 - avoiding, 22
 - for NNMi discovery, 21
 - improving response time, 21
 - preventing delays, 21
- nsswitch.conf file, 21

O

- obtaining license passwords, 41
- ongoing discovery, 53
- online help, 50
- Operator Level 1 role, 49
- Operator Level 2 role, 49
- operators
 - help, 50
 - NNMi console functions, 9
- Oracle database
 - installation problem, 65
 - instance for NNMi, 20
 - prerequisites, 19
 - tablespace size, 20
 - user for NNMi, 20
- out-of-box roles, 49
- ovinstallparams.ini file, 30
- ovstart command, 68
- ovstatus command
 - silent installation, 32, 34
 - troubleshooting, 68
- ovstop command, 68

P

- passwords
 - delivery service URL, 42
 - license, 41
 - permanent license, 40
 - user
 - configuring, 11
 - signing in, 48
- permanent license password, 40
- pinging node, 69
- ports
 - configuring usage, 11
 - jboss contention, 67
- Postgres
 - Disabling on Linux NNMi management server, 18, 70
- pre-configured user roles, 49
- pre-defined incident configurations, 11
- preparing permanent license password, 40
- prerequisites
 - database, 19
 - hardware, 15
 - NNMi Quick Start Configuration wizard, 23
 - software, 15
- preventing delays for nslookup requests, 21
- problems
 - initial startup, 67 to 69
 - installation, 65 to 66

Q

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

R

- RCA, 9

- release notes, 15
- removing NNMi, 43 to 44
- requesting license passwords, 41
- restarting services, 68
- retry, configuring, 11
- roles, user
 - configuring, 11
 - pre-defined, 49
- root
 - cause analysis, 9
 - privileges, 43
- round-robin DNS, 21
- rules, auto-discovery, 35

S

- security, command-line, 30
- seeds, discovery, 35
- services
 - list, 68
 - restarting for NNMi, 68
- setup.bin command, 32, 34
- signing in to NNMi console, 48
- silent installation, 30
- SNMP
 - supported versions, 51
 - traffic, 11
- software
 - supported, 15
- source system, installation, 31
- spiral discovery, 54
- startup, troubleshooting, 67 to 69
- status, monitoring device, 10

- supported
 - hardware, 15
 - SNMP versions, 51
 - software, 15
 - web browsers, 15
- symbolic links, 66
- system account
 - changing password, 30, 63
 - user roles, 49
- system device support matrix, 15

T

- target system, installation, 31
- tasks
 - discovery configuration, 51
 - network management, 10
- temporary license, 40
- ticket, trouble, 9
- timeout, configuring, 11
- toolkit, developer, 42
- topology, network, 53
- traffic, configuring settings, 11
- troubleshooting
 - discovery, 69
 - initial startup, 67 to 69
 - installation, 65 to 66
- trouble ticket, 9
- types, checking license, 40

U

- uninstalling NNMi, 43 to 44
- URLs
 - HP password delivery service, 42
 - NNMi console, 48
 - NNMi Quick Start Configuration wizard, 36

- user
 - help, 50
 - interface, 9
 - name
 - configuring, 11
 - signing in, 48
 - password
 - configuring, 11
 - signing in, 48
 - roles, 11
- using, NNMi Quick Start Configuration wizard, 35

V

- valid IP address ranges, 37
- versions, supported SNMP, 51

W

- web browser
 - accessing NNMi console, 47
 - enabling for NNMi console, 58
 - set language preference, 47
 - supported, 15
- wizard
 - installing NNMi, 25
 - NNMi Quick Start Configuration
 - URL, 36
 - using, 35

X

- XServer, configuring, 58

