HITACHI
Inspire the Next

Job Management Partner 1 Version 10

Job Management Partner 1/Consolidated Management 2/Network Node Manager i Installation Guide

3021-3-342-20(E)

Notices

■ Relevant program products

For Windows Server 2008, Windows Server 2012

P-2942-82AL Job Management Partner 1/Consolidated Management 2/Network Node Manager i 10-50

P-2942-83AL Job Management Partner 1/Consolidated Management 2/Network Node Manager i Advanced 10-50

For Linux 6

P-8242-82AL Job Management Partner 1/Consolidated Management 2/Network Node Manager i 10-50

P-8242-83AL Job Management Partner 1/Consolidated Management 2/Network Node Manager i Advanced 10-50

For HP-UX (IPF)

P-1J42-82AL Job Management Partner 1/Consolidated Management 2/Network Node Manager i 10-50

P-1J42-83AL Job Management Partner 1/Consolidated Management 2/Network Node Manager i Advanced 10-50

For Solaris

P-9D42-82AL Job Management Partner 1/Consolidated Management 2/Network Node Manager i 10-50

P-9D42-83AL Job Management Partner 1/Consolidated Management 2/Network Node Manager i Advanced 10-50

■ Trademarks

ActiveX is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Firefox is a registered trademark of the Mozilla Foundation.

HP-UX is a product name of Hewlett-Packard Development Company, L.P. in the U.S. and other countries.

Internet Explorer is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

Itanium is a trademark of Intel Corporation in the United States and other countries.

JBoss and Hibernate are trademarks or registered trademarks of Red Hat Inc. in the United States and other countries.

Linux(R) is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Mozilla is a trademark of the Mozilla Foundation in the U.S and other countries.

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

Oracle Technology - Notice of Restricted Rights

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

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

Red Hat is a trademark or a registered trademark of Red Hat Inc. in the United States and other countries.

■ Microsoft product name abbreviations

This manual uses the following abbreviations for Microsoft product names:

Abbreviation			Full name or meaning
ActiveX			ActiveX(R)
Internet Explorer			Microsoft(R) Internet Explorer(R)
			Windows(R) Internet Explorer(R)
Windows	Windows Server 2008	Windows Server 2008	Microsoft(R) Windows Server(R) 2008 Enterprise
			Microsoft(R) Windows Server(R) 2008 Standard
		Windows Server 2008 R2	Microsoft(R) Windows Server(R) 2008 R2 Datacenter
			Microsoft(R) Windows Server(R) 2008 R2 Enterprise
			Microsoft(R) Windows Server(R) 2008 R2 Standard
	Windows Server 2012	Windows Server 2012	Microsoft(R) Windows Server(R) 2012 Datacenter
			Microsoft(R) Windows Server(R) 2012 Standard
		Windows Server 2012 R2	Microsoft(R) Windows Server(R) 2012 R2 Datacenter
			Microsoft(R) Windows Server(R) 2012 R2 Standard

■ Acknowledgements

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

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

This product includes software developed by The Legion Of The Bouncy Castle.
(http://www.bouncycastle.org)
This product includes software developed by Trantor Standard Systems Inc.
(http://www.trantor.ca)

■ Restrictions

Information in this document is subject to change without notice and does not represent a commitment on the part of Hitachi. The software described in this manual is furnished according to a license agreement with Hitachi. The license agreement contains all of the terms and conditions governing your use of the software and documentation, including all warranty rights, limitations of liability, and disclaimers of warranty.

Material contained in this document may describe Hitachi products not available or features not available in your country.

No part of this material may be reproduced in any form or by any means without permission in writing from the publisher.

■ Issued

Dec. 2014: 3021-3-342-20(E)

■ Copyright

Summary of amendments

The following table lists changes in this manual (3021-3-342-20(E)) and product changes related to this manual.

Changes	Location
The following OSs are now supported: • Microsoft(R) Windows Server(R) 2012 R2 Datacenter • Microsoft(R) Windows Server(R) 2012 R2 Standard	--
Because it is not possible in Windows Server 2008 and later to log in to a console session from a remote desktop, the associated descriptions were removed.	*2.2*, Table 2-1, *3.1.1*
The description of the NNMi management server preinstallation checklist was changed.	Table 2-1
The following item was added under *Installing NNMi (Windows)*: • Confirmation of whether to perform the preinstallation checks and continue the installation	*3.1.1*
The following item was added under *Installing NNMi (UNIX)*: • Confirmation of whether to perform the preinstallation checks and continue the installation	*3.1.2*
The following items were added as tasks to be performed after installing NNMi: • Set the language environment (UNIX only) • Check the maximum Java heap size	*3.1.3(2)*, *3.1.3(3)*
The steps listed under *Specifying disk drive security settings (Windows)* were changed.	*A.1*
The following MIBs were added to the list of MIBs that are read during a new installation: • AX-BOOTMANAGEMENT-MIB • AX-DEVICE-MIB • AX-FLOW-MIB • AX-LOGIN-MIB • AX-NOTIFICATION • AX-OSPF-MIB • AX-OSPFV3-MIB • AX-QUEUE-MIB • AX-SMI-MIB • AX-STATS-MIB • AX-SYSTEM-MIB • AX-VRF-MIB	*Appendix C*

In addition to the above changes, minor editorial corrections were made.

Preface

This manual explains how to install *Job Management Partner 1/Consolidated Management 2/Network Node Manager i* and *Job Management Partner 1/Consolidated Management 2/Network Node Manager i Advanced* (hereafter referred to as *NNMi* if there is no difference in the products). Note that this manual is intended for all supported operating systems. When there are differences between the NNMi editions on different operating systems, this manual provides separate descriptions.

In this manual, *Job Management Partner 1* is abbreviated as *JP1*, and *Job Management Partner 1/Consolidated Management 2/Network Node Manager i* is abbreviated as *NNMi*, and Consolidated Management 2 is abbreviated as Cm2.

■ Intended readers

This manual is intended for IT personnel who design and implement network analysis management systems using NNMi.

■ Organization of this manual

This manual is organized into the following chapters and appendixes:

1. Introducing Network Node Manager i

Chapter 1 introduces NNMi and describes the items you set when installing NNMi.

2. Preinstallation Checklists

Chapter 2 explains what you need to do before installing NNMi.

3. Installing and Uninstalling NNMi

Chapter 3 guides you through the process of installing and uninstalling NNMi.

4. Getting Started with NNMi

Chapter 4 explains the settings needed for you to begin network management using NNMi.

A. Additional Information About Installation

Appendix A provides additional information about installing NNMi.

B. Troubleshooting Installation and Initial Startup

Appendix B describes how to troubleshoot installation and initial startup.

C. List of MIBs Read During a New Installation

Appendix C lists the MIBs that NNMi reads during new installation.

D. Version Changes

Appendix D describes the changes that have been made in each version.

E. Reference Material for This Manual

Appendix E provides reference information such as a list of related manuals and an explanation of the abbreviations used in this manual.

F. Glossary

Appendix F is a glossary that explains the terms used in this manual.

Contents

1 Introducing Network Node Manager i

Network Node Manager i software contains a toolset to help you maintain a healthy network across your organization. NNMi can discover network nodes (such as switches and routers) on an ongoing basis, providing an up-to-date representation of the network topology. As NNMi maintains an accurate picture of the network, it also helps you handle problems through management by exception; that is, 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.

1.1 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.

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

This guide is designed to help you get started. More detailed information about using NNMi can be found in NNMi Help. Detailed information about customizing the NNMi configuration can be found in the manual *Job Management Partner 1/Consolidated Management 2/Network Node Manager i Setup Guide*.

1.2 Environment variables used in this document

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

- Windows
  - `%NnmInstallDir%:`*drive*`:\Program Files(x86)\Hitachi\Cm2NNMi\`
  - `%NnmDataDir%:`*drive*`:\ProgramData\Hitachi\Cm2NNMi\`
- UNIX
  - `$NnmInstallDir:/opt/OV`
  - `$NnmDataDir:/var/opt/OV`

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

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

For details about other NNMi environment variables that you can source, see the manual *Job Management Partner 1/Consolidated Management 2/Network Node Manager i Setup Guide*.

2 Preinstallation Checklists

This chapter describes how to perform the preparations and checks required before you install NNMi.

2.1 Checking the hardware and software

Before installing NNMi, read the information about supported NNMi hardware and software in the NNMi *Release Notes* and in the manual *Job Management Partner 1/Consolidated Management 2/Network Node Manager i Setup Guide*.

2.2 Preparing the preinstallation NNMi management server environment

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 *2.1 Checking the hardware and software*.

Before you install NNMi on the NNMi management server, complete the checklist in Table 2-1.

Important note

Configure the remote desktop as described below before installing and configuring NNMi. This configuration increases the resources that Windows uses, so we recommend that you return to the original configuration after you complete these tasks, if necessary.

- Configuration path

  Windows Server 2008

  Administrative Tools > **Terminal Services** > **Terminal Services Configuration**

  Windows Server 2008 R2

  Administrative Tools > **Remote Desktop Services** > **Remote Desktop Session Host Configuration**

  Windows Server 2012 and later

  Local Group Policy Editor# > **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Temporary folders**

  #: To open **Local Group Policy Editor**, enter `gpedit.msc` in the **Start** window.

- Configuration settings

  Windows Server 2008 and Windows Server 2008 R2

  Clear the **Use temporary folders per session** and **Delete temporary folders on exit** check boxes. Log off, and then log back on to apply the new settings to the system.

  Windows Server 2012 and later

  Enable **Do not use temporary folders per session** and **Do not delete temp folder upon exit**. To apply these settings to the system, log off and then log on again.

Table 2–1: NNMi management server preinstallation checklist

Completed? (y/n)	NNMi management server preparation
	Make sure that the host name of the server where you plan to install NNMi is RFC-compliant. Host names are allowed to use alphanumerics (`A` to `Z`, `a` to `z`, `0` to `9`), hyphens (`-`), and periods (`.`) (to demarcate domain names). Setup of host names that are not RFC-compliant (host names that use underscores (_), for example) might result in failure of the NNMi console connection or command execution.
	Make sure that the name of the local host can be resolved on the server on which NNMi is installed and that `localhost` is set up with the name resolved to `127.0.0.1`.
	Windows Make sure that the `C` drive is used as the OS's system drive. NNMi cannot be installed in an environment where the system drive is not drive `C`.
	Windows If you have restrictive security settings in place, you might need to adjust the permission on the drive or drives on which you want to place the NNMi install and data directories. For details, see *A.1 Specifying disk drive security settings (Windows)*.

Completed? (y/n)	NNMi management server preparation
	Windows Short file names in the 8.3 format must be enabled. If they are disabled, execute the following command: `fsutil behavior set disable8dot3 0` Short file names in the 8.3 format must also be set if the directory specified as the installation directory and the names of its parent directories are not in the 8.3 format. If short file name are not set, execute the following command: `fsutil file setshortname` *directory-being-configured short-file-name*
	Windows Check for the SNMP service; if installed, the SNMP trap service needs to be disabled on this server.
	Install and enable a supported Web browser. For details, see *2.1 Checking the hardware and software* and *A.3 Enabling the Web browser for the NNMi console*.
	Dynamic Host Configuration Protocol (DHCP) users: Makes sure that the NNMi management server is consistently assigned the same IP address.
	Windows To improve installation performance, disable anti-virus software until NNMi installation is complete. When NNMi installation is complete, restart the anti-virus software.

	Linux
	Before you can install NNMi on a Linux server, the library files listed below that are needed by NNMi must be installed. Also, install the library files that have dependence relationships with these files:
	`/lib64/libaio.so.1`
	`/usr/lib/libstdc++.so.6`
	`/usr/lib64/libXtst.so.6`
	`/usr/lib64/libXi.so.6`
	For details, see *A.4 Installing required libraries in Linux*.

	Do not install NNMi until you have verified that all ports used by NNMi are available. For a list of the ports used by NNMi and the direction in which data passes through the firewall, see *C. List of Ports Used by NNMi* in the manual *Job Management Partner 1/Consolidated Management 2/Network Node Manager i Setup Guide*.
	Do not block communication with the IP address of the local host, such as by using a firewall.
	Configuration information from earlier versions of NNM remains, even if NNM is removed. See the *Release Notes* for the earlier version of NNM to identify the older information, and then delete that information prior to installing NNMi.
	Windows Before installing NNMi, make sure that the Windows Services window (the window started from **Control Panel** > **Administrative Tools** > **Services**) is not running. If it is, close it.

	Windows
	If the sum of the character string set in the system environment variable `Path` and the lengths of the directory paths below is 950 bytes or more, NNMi installation might fail even on OS versions that allow character strings of 1,024 bytes or more to be set in environment variables.
	`%NnmInstallDir%bin\;`
	`%NnmDataDir%shared\nnm\actions\;`
	Temporarily shorten the character string set in `Path`, and then install NNMi. After installation is complete, you can again add to the character string in system environment variable `Path`, within the bounds that the OS can handle.

Completed? (y/n)	NNMi management server preparation
	Windows If you are installing NNMi using a path other than the default, you can use alphanumerics (A to Z, a to z, 0 to 9), hyphens (-), periods (.), underscores (_), and single-byte spaces for the names of the install and data directories. The maximum length of the absolute paths for these directories is 60 characters.
	Windows Do not specify paths that include junction points, such as *drive*:\Documents and Settings. Doing so might cause problems, such as temporary files not being deleted.
	Windows If you install NNMi in an environment in which environment variables %TEMP% and %TMP% have different values, installation might fail. Make sure that the values of %TEMP% and %TMP% are the same before installation. If they differ, set %TEMP% and %TMP% to the same values.
	Windows Do not set the following variables as environment variables: ● LANG ● Anything that begins with LC If another product sets these environment variables, it might not be compatible with NNMi. Installation might fail if NNMi is installed with these variables set.
	Windows In Windows Server 2008 R2 or Windows Server 2012 or later, if a Remote Desktop session host has been installed in Remote Desktop Services, the following setting is required before you install NNMi: ● Execute change user /install to change to install mode. For details about this setting, see Help for the Remote Desktop session host. In the case of Windows Server 2008, substitute *terminal server* for *Remote Desktop session host* in the text above.
	Windows If changes you have made to the system on which you plan to install NNMi require restarting the OS, do so prior to installing NNMi. For example, the OS must be restarted if the registry value below exists. If this value exists, NNMi might suspend the installation: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations This registry value normally disappears when the OS is restarted.
	Windows NNMi uses a %TEMP% directory of up to 500 MB when it is installed or removed. The install or removal might fail without sufficient disk space. **UNIX** NNMi uses a /tmp directory of up to 1 GB when it is installed or removed. The install or removal might fail without sufficient disk space.
	Windows During installation, under **Administrative Tools** > **Terminal Services** > **Terminal Services Configuration** (for Windows Server 2008 R2, **Administrative Tools** > **Remote Desktop Services** > **Remote Desktop Session Host Configuration**), clear the **Use temporary folders per session** and **Delete temporary folders on exit** check boxes. Log off, and then log back on to apply the new settings to the system. In Windows Server 2012 and later, under **Local Group Policy Editor** > **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Temporary folders**, enable **Do not use temporary folders per session** and **Do not delete temp folder upon exit**. To apply these settings to the system, log off and then log on again.

Completed? (y/n)	NNMi management server preparation
	UNIX If you are re-installing NNMi, also re-install all applications that require NNMi and configure them accordingly.
	UNIX Install applications that require NNMi after the configuration of the environment that follows NNMi installation has been completed. Remember to execute the `ovstop` command before you install applications.
	UNIX During NNMi installation, do not change the size of the terminal window in which Hitachi PP Installer is running. Doing so might prevent NNMi from installing properly.
	HP-UX The kernel must be configured (check using `/usr/sbin/smh`). Configure kernel parameters in the `Kernel Configuration/Tunables` section. ● Add `50` to `nproc`. The minimum value is 300. ● If `max_thread_proc` is less than 2,048, set it to `2048`. ● If `nkthread` is less than 10,000, set it to `10000`. ● Adjust `filecache_max` as needed so that an `ovjboss` heap can be allocated. For details about the minimum size for the `ovjboss` heap, see *Java heap size* in *4. Memory and Disk Space Requirements* in *Release Notes*.

	Linux
	NNMi requires a UDP reception buffer of 8 MB and a UDP transmission buffer of 2 MB.
	To change the settings for memory spaces allocated to buffers, edit the `/etc/sysctl.conf` file to add the following entries:
	`# NNM settings for UDP receive and send buffer sizes`
	`net.core.rmem_max = 8388608`
	`net.core.wmem_max = 2097152`
	After editing the `/etc/sysctl.conf` file, apply the changes by restarting the OS or executing the `/sbin/sysctl -p` command.

	Linux
	The value of `kernel.shmmax` might be too small. If it is, edit the `/etc/sysctl.conf` file to add the following entries. Hitachi recommends a value of 64 GB.
	`# NNM settings for embedded database`
	`kernel.shmmax = 68719476736`
	If you set the value of `kernel.shmmax`, after editing the `/etc/sysctl.conf` file, apply the changes by restarting the OS or executing the `/sbin/sysctl -p` command.

	Solaris
	NNMi requires a UDP reception buffer of 8 MB and a UDP transmission buffer of 2 MB.
	To change the UDP memory allocations, execute the following command:
	`ndd -set /dev/udp udp_max_buf 8388608`
	To apply the change made to the UDP memory allocation after a system restart, create a system start script.
	Example:
	Create the `/etc/init.d/ndd` file.
	Example of `ndd` file:
	`#!/bin/sh`
	`ndd -set /dev/udp udp_max_buf 8388608`
	Set the file permissions.

Completed? (y/n)	NNMi management server preparation

	`chmod 0744 /etc/init.d/ndd`
	`chown root:sys /etc/init.d/ndd`
	To start the NNMi service at run level 3, create the `/etc/rc3.d/S70ndd` file.
	`cd /etc/init.d`
	`ln ndd /etc/rc3.d/S70ndd`

	Solaris
	NNMi uses shared memory. Set the amount of shared memory according to the amount of physical memory, as follows:
	• If physical memory is less than 8 GB, allocate 1 GB of shared memory.
	• If physical memory is at least 8 GB but less than 16 GB, allocate 2 GB of shared memory.
	• If physical memory is at least 16 GB but less than 24 GB, allocate 3 GB of shared memory.
	• If physical memory is 24 GB or greater, allocate 5 GB of shared memory.
	To set `project.max-shm-memory`, set its value in both the `user.root` project and the `system` project.
	The following example sets `project.max-shm-memory` to 5 GB:
	`prctl -n project.max-shm-memory -v 5368709120 -r -i project user.root`
	`projmod -a -K "project.max-shm-memory=(priv,5368709120,deny)" user.root`
	`prctl -n project.max-shm-memory -v 5368709120 -r -i project system`
	`projmod -a -K "project.max-shm-memory=(priv,5368709120,deny)" system`
	If the NNMi service is configured to start automatically at system startup, `/etc/init.d/netmgt` is executed at system startup. Make sure the system project settings have been updated before `/etc/init.d/netmgt` is executed.

	Solaris
	You must increase the number of semaphores to 256. To set `project.max-sem-ids`, set its value in both the `user.root` project and the `system` project.
	The following example sets `project.max-sem-ids`:
	`prctl -n project.max-sem-ids -v 256 -r -i project user.root`
	`projmod -a -K "project.max-sem-ids=(priv,256,deny)" user.root`
	`prctl -n project.max-sem-ids -v 256 -r -i project system`
	`projmod -a -K "project.max-sem-ids=(priv,256,deny)" system`
	If the NNMi service is configured to start automatically at system startup, `/etc/init.d/netmgt` is executed at system startup. Make sure the system project settings have been updated before `/etc/init.d/netmgt` is executed.

	Solaris When the `useradd` command is used to create users, by default the home directory will be `/home/`*user-name*. However, under the default settings in Solaris, directories cannot be created in `/home`. If your environment does not allow directories to be created in `/home`, change the `useradd` command's default home directory to a location that allows directories to be created. The following example changes the default home directory to `/export/home/`*user-name*: `# /usr/sbin/useradd -D -b /export/home`
	Solaris If you will be upgrading NNMi, check the home directory of the user `nmsdbmgr` before upgrading. The following shows an example of the command used to check the home directory: `# /usr/bin/finger nmsdbmgr` If the home directory of the user `nmsdbmgr` (for example, `/home/nmsdbmgr`) cannot be created, change the home directory to a directory that can be created. The following example changes the home directory of the user `nmsdbmgr` to `/export/home/nmsdbmgr`:

Completed? (y/n)	NNMi management server preparation
	# /usr/sbin/usermod -d /export/home/nmsdbmgr nmsdbmgr

2.3 Checking for a well-configured DNS

NNMi uses Domain Name System (DNS) to determine relationships between host names and IP addresses. This can result in a large number of name service queries when auto-discovery is enabled.

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

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

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

Important note

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

Reference note

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

- Windows
  `%SystemRoot%\system32\drivers\etc\hosts`
- UNIX
  `/etc/hosts`

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

- The `hosts` file might take precedence with some OS configurations. Make sure that the `hosts` file contains a minimum of two entries:
  `127.0.0.1 localhost`
  NNMi-management-server-IP-address NNMi-management-server-name
  NNMi-management-server-IP-address is the IP address of the fully qualified domain name (FQDN) of the NNMi management server. *NNMi-management-server-name* is the FQDN name for the NNMi management server set during installation.
- Windows
  Make sure that all DNS servers used by the NNMi management server provide consistent host name-to-IP address mappings and IP address-to-host name mappings.
- UNIX
  Make sure that `nslookup` discovery conforms to the `nslookup` command discovery sequence set in the `nsswitch.conf` file.
  Make sure that all DNS servers that you are aware of provide consistent host name-to-IP address mappings and IP address-to-host name mappings.

If you know that there are problems with the DNS configuration in your network domain (host names 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 two files listed below before configuring NNMi discovery. NNMi never issues a DNS request for host names or IP addresses identified in these files.

- `hostnolookup.conf` (enter fully qualified domain names or wildcards that identify groups of host names)
- `ipnolookup.conf` (enter IP addresses or wildcards that identify groups of IP addresses)

Use a text editor to populate the files. Place the files in the following locations on the NNMi management server:

Windows

```
%NnmDataDir%shared\nnm\conf\
```

`%NnmDataDir%` is the data directory specified during installation.

UNIX

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

2.4 Preparing to use the 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 2-2.

Table 2–2: NNMi Quick Start Configuration Wizard preinstallation checklist

Completed? (y/n)	Preparation for initial environment configuration
	Determine a limited IP address range for auto-discovery#. For details about the number of licenses (number of management nodes), see *3.3 Licensing NNMi*.
	Determine IP addresses for discovery seeds. For details about seeds, see *About discovery seeds and auto-discovery rules* in *3.2 Using the Quick Start Configuration Wizard*.
	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.

#

If use of network address translation (NAT) means that you will be managing areas in the network that contain duplicated IP addresses, select one address domain (an unduplicated address) that is to be detected by the Quick Start Wizard. Then see *Overlapping Addresses in NAT Environments* in NNMi Help or *Managing Overlapping IP Addresses in NAT Environments* in the *Job Management Partner 1/Consolidated Management 2/Network Node Manager i Setup Guide*.

3

Installing and Uninstalling NNMi

This chapter guides you through the process of installing and uninstalling NNMi. It also explains how to specify settings and how to obtain licenses after installation. Because the *Release Notes* also contain information about installation, please refer to the *Release Notes* as you read this chapter.

3.1 Installing NNMi

Windows

Before installing NNMi, complete the requirements listed in the preinstallation checklist, including disabling anti-virus software. (See *2. Preinstallation Checklists*.)

UNIX

Before installing NNMi, complete the requirements listed in the preinstallation checklists. (See *2. Preinstallation Checklists*.)

See the *Release Notes* for procedures for upgrading NNMi (including how to apply patches).

3.1.1 Installing NNMi (Windows)

To perform a new installation of NNMi in a Windows system, follow these steps:

Important note

Configure the remote desktop as follows before you install and configure NNMi. This configuration increases the resources that Windows uses, so you can return to the original configuration after completing these tasks, if necessary.

- Configuration path

  Windows Server 2008

  Administrative Tools > **Terminal Services** > **Terminal Services Configuration**

  Windows Server 2008 R2

  Administrative Tools > **Remote Desktop Services** > **Remote Desktop Session Host Configuration**

  Windows Server 2012 and later

  Local Group Policy Editor# > **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Temporary folders**

  #: To open **Local Group Policy Editor**, enter `gpedit.msc` in the Start window.

- Configuration settings

  Windows Server 2008 and Windows Server 2008 R2

  Clear the **Use temporary folders per session** and **Delete temporary folders on exit** check boxes. Log off, and then log back on to apply the new settings to the system.

  Windows Server 2012 and later

  Enable **Do not use temporary folders per session** and **Do not delete temp folder upon exit**. To apply these settings to the system, log off and then log on again.

1. Log on as a user with administrator privileges to the system where you plan to install NNMi.
   If UAC is enabled, a user who is not the built-in `Administrator` must be promoted to administrator.
2. Insert the NNMi installation media into the drive.
   The Hitachi Program Product Installer window opens.
3. Start installation as indicated by the installer.
4. Enter information as indicated by the installer.

To use a default value, press the **Enter** key without entering any value. The default is the value shown in brackets.

- Specify the HTTP port number for the NNMi Web server.

  Enter the HTTP port number for the NNMi Web server used to access NNMi. Enter a port number that is not being used by another program. The default value is `80`.

  An input example follows:

```
** Network Node Manager i Installer **
* Starting NNMi installation.
* Enter default port for HTTP server =>
* [80]
8004 ↵
```

- Specify the installation directory.

  Enter the directory where you want to install the NNMi program. The default value is as follows:

```
drive:\Program Files (x86)\Hitachi\Cm2NNMi\
```

Input example:

```
* Enter program install directory =>
* [C:\Program Files (x86)\Hitachi\Cm2NNMi\]
C:\Hitachi\Cm2NNMi\ ↵
```

Important note

NNMi includes 32 bit-compatible programs, so it cannot be installed in the *drive*`:\Program Files\` folder of a 64-bit system.

Hitachi recommends that you install NNMi in *drive*`:\Program Files (x86)\`.

- Specify the data directory.

  Enter the directory where you want to store NNMi configuration files and data such as databases and log files. The default value is as follows:

```
drive:\ProgramData\Hitachi\Cm2NNMi\
```

Input example:

```
* Enter program data directory =>
* [C:\ProgramData\Hitachi\Cm2NNMi\]
D:\NNMiData\ ↵
```

- Check the display of entered data and make sure that installation has started.

  The three data entries shown above are displayed. If there are no problems with the data displayed, enter `yes` to start installation. To change the entered data, enter `no`.

  An input example follows:

```
* port : 80
* install directory : C:\Hitachi\Cm2NNMi\
* data directory : D:\NNMiData\
* Do you start installation with above settings you entered ? (yes/no)
* If you need to change the settings, please enter no.
yes ↵
```

- Confirm whether to perform the preinstallation checks and continue the installation.
  The preinstallation checks will be performed first when installation starts.

  Reference note

  In order to verify the items listed in Table 2-1 NNMi management server preinstallation checklist, the preinstallation check will verify that the ports used by NNMi are available.

  Do not install NNMi until you have verified that all the ports used by NNMi are available. For a list of the ports used by NNMi and the direction in which data passes through the firewall, see *C. List of Ports Used by NNMi* in the *Job Management Partner 1/Consolidated Management 2/Network Node Manager i Setup Guide*.

  If no problems are found in this preinstallation check, continue with the installation.

  If there is a problem with the preinstallation check, the installer will output the problem and ask whether you want to continue the installation. Enter `yes` to continue the installation or `no` to terminate the installation.

  Example of input when there is a problem in the preinstallation check:

```
* Starting NNMi Precheck ...
* TCP Port: [443] is used.
* UDP Port: [162] is used.
* NNMi Precheck result: NG
* There are some problem(s) with the settings.
* Do you want to continue NNMi installation ? (yes/no)
* If you enter no, the installation will stop.
no ↵
```

  Important note

  Do not use **Ctrl+Z** when entering this data. Entering **Ctrl+Z** suspends the installation. If the installation is suspended, resume the installation procedure from step 3.

  Note that the installation takes ten to twenty minutes or more. Do not suspend the installation once it is underway. Interrupting the installation creates undesirable conditions that might render re-installation by normal means impossible.

  Even if the precheck result is `OK`, this is not a guarantee that the installation will be successful. You must also make sure all the checklists in *2. Preinstallation Checklists* are completed.

Execute NNMi commands in a command prompt window that is opened after the installation has finished. Commands will not run correctly if they are executed from a window opened before the installation has finished, because settings required by NNMi commands, such as the NNMi environment variables, will not have been configured yet.

3.1.2 Installing NNMi (UNIX)

To perform a new installation of NNMi in a UNIX system:

1. Log in as a user with root privileges to the system where you plan to install NNMi.

2. Set the locale.
   Set a supported locale in the environment variable `LC_ALL`. For details, see the NNMi *Release Notes*.

3. Place the NNMi media in the drive, and then mount the drive.
   For details about how to mount drives, see the NNMi *Release Notes* and OS documentation.

4. Start Hitachi PP Installer.
   Execute the following commands. *mount-dir* indicates the directory the drive is mounted as.
   - HP-UX
     `# /`*mount-dir*`/IPFHPUX/setup /`*mount-dir*
   - Solaris
     `# /`*mount-dir*`/SOLARIS/setup /`*mount-dir*
   - Linux
     `# /`*mount-dir*`/X64LIN/setup /`*mount-dir*

   For details about how to start Hitachi PP Installer, see the NNMi *Release Notes*.

5. In the Hitachi PP Installer startup window, enter `I` to display a list of software that can be installed.

6. Move the cursor to `JP1/Cm2/Network Node Manager i`, select it using the space bar, and then enter `I`.
   A message will appear asking you whether you want to continue the installation.

7. Enter `y` or `Y`.

8. Enter information as indicated by the installer.
   To use default values, press the **Enter** key without entering any values. Defaults are the values shown in brackets.
   - Specify the HTTP port number for the NNMi Web server.
     Enter the HTTP port number for the NNMi Web server used to access NNMi. Enter a port number that is not being used by another program. The default value is `80`.
     Example of input:

```
** Network Node Manager i Installer **
* Starting NNMi installation.
* Enter default port for HTTP server =>
* [80]
8004 ↵
```

   - Check the display of entered data and make sure that installation has started.
     The data entered as shown above is displayed. If there are no problems with the data displayed, enter `yes` to start installation. To change the entered data, enter `no`.
     An input example follows:

```
* port : 80
* Do you start installation with above settings you entered ? (yes/no)
* If you need to change the settings, please enter no.
yes ↵
```

   - Confirm whether to perform the preinstallation checks and continue the installation.
     The preinstallation checks will be performed first when installation starts.

> **Reference note**
>
> In order to verify the items listed in Table 2-1 NNMi management server preinstallation checklist, the preinstallation check will verify that the ports used by NNMi are available.

Do not install NNMi until you have verified that all the ports used by NNMi are available. For a list of the ports used by NNMi and the direction in which data passes through the firewall, see *C. List of Ports Used by NNMi* in the *Job Management Partner 1/Consolidated Management 2/Network Node Manager i Setup Guide*.

If no problems are found in this preinstallation check, continue with the installation.

If there is a problem with the preinstallation check, the installer will output the problem and ask whether you want to continue the installation. Enter `yes` to continue the installation or `no` to terminate the installation.

Example of input when there is a problem in the preinstallation check:

```
* Starting NNMi Precheck ...
* TCP Port: [443] is used.
* UDP Port: [162] is used.
* NNMi Precheck result: NG
* There are some problem(s) with the settings.
* Do you want to continue NNMi installation ? (yes/no)
* If you enter no, the installation will stop.
no ↵
```

Important note

Note that the installation takes ten to twenty minutes or more. Do not interrupt the installation once it is underway. Interrupting the installation creates undesirable conditions that could render re-installation by normal means impossible.

Even if the precheck result is `OK`, this is not a guarantee that the installation will be successful. You must also make sure all the checklists in *2. Preinstallation Checklists* are completed.

3.1.3 Operations after the installer finishes

This section describes tasks that must be performed after NNMi is installed. Perform these tasks no matter which OS you are using.

(1) Set the NNMi system account password

An account password is set for the initial sign-in to the NNMi console. Use the `nnmchangesyspw.ovpl` script to set the password. Run the `nnmchangesyspw.ovpl` script without arguments, and register a password as indicated by the displayed messages.

Reference note

The system account is a special administrator account created by the installation process. It is used when you sign in to the NNMi console for the first time. It is not normally used after the creation of a user with the administrator role on the NNMi console. The system account remains enabled after the installation finishes, but it is used only to execute on the command line or for restoration purposes. For details about how to set or change the system password, see *A.5 Setting the system account password*.

(2) Set the language environment (UNIX only)

Depending on the OS settings, rebooting the machine might automatically invoke the `ovstart` command with the setting `LANG=C`. In such a case, background processes will output messages in English. To prevent output of messages in English, configure the following settings to invoke the `ovstart` command in the supported locale at system startup.

- HP-UX

  In the file `/sbin/init.d/HPSwNnm500`, add either of the following before `$OVHOME/bin/ovstart && echo "ovstart \c"`:

  ```
  LANG=ja_JP.SJIS
  export LANG
  ```

  or

  ```
  LANG=ja_JP.eucJP
  export LANG
  ```

  or

  ```
  LANG=zh_CN.hp15CN
  export LANG
  ```

- Solaris

  In the file `/etc/init.d/netmgt`, add either of the following before `$SU_CMD /opt/OV/bin/ovstart`:

  ```
  LANG=ja_JP.eucJP
  export LANG
  ```

  or

  ```
  LANG=ja_JP.PCK
  export LANG
  ```

  or

  ```
  LANG=zh
  export LANG
  ```

- Linux

  In the file `/etc/init.d/netmgt`, add the following two lines before `/opt/OV/bin/ovstart`:

  ```
  LANG=ja_JP.UTF-8
  export LANG
  ```

  or

  ```
  LANG=zh_CN.utf8
  export LANG
  ```

(3) Check the maximum Java heap size

During installation, the maximum Java heap size (`-Xmx`) is set automatically according to the physical memory. Review the `-Xmx` value after consulting *4. Memory and Disk Space Requirements* and *9.1 Systems* in the *Release Notes*. In addition, review the `-Xmx` value in the event of changes to the scale of the monitoring to be done with NNMi.

(4) Starting NNMi services

Execute the `ovstart` command to start NNMi services.

(5) Create an account to serve the administrator role

Sign in to the NNMi console and create an account to serve the administrator role.

1. A window for NNMi sign-in appears.
   Enter the following URL in the window for entering the Web browser address.

   ```
   http://fully-qualified-domain-name:port/nnm/
   ```

   where *fully-qualified-domain-name* is the fully qualified domain name of the NNMi administrator server, and *port* is the HTTP port number of the NNMi Web server that was set during installation.

2. Enter the user name and password for the system account, and click the sign-in button.
   - User name: `system`
   - Password: The system account password created in *(1) Set the NNMi system account password*

3. Create the user accounts.
   On the NNMi console, under **Configuration** workspace > **Security** > **User Accounts**, click the **New** icon. Enter a name and password and click the **Save and Close** icon to save the user account. For details, see *Configure User Accounts (User Account Form)* in NNMi Help.

   Important note

   Between 1 and 40 characters can be entered for both the name and the password. Alphanumerics (`A` to `Z`, `a` to `z`, `0` to `9`), underscores (_), and single-byte spaces can be used.

4. Map the administrator role to the user account.
   On the NNMi console, under **Configuration** workspace > **Security** > **User Account Mappings**, click the **New** icon, and then specify the following parameters.
   - User account: The user account created in step 3
   - User group: NNMi administrator

   Click the **Save and Close** icon to save the mapping. For details, see *User Account Mapping Tasks* in NNMi Help.

   Important note

   Do not create a new user group. Instead, select from among the default user groups.

3.2 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. Very few parameters can be set from the Quick Start Configuration Wizard, which means that it is not possible to configure all settings necessary to start monitoring with NNMi. Hitachi normally recommends that you perform configuration from the NNMi console. For details, see the manual *Job Management Partner 1/Consolidated Management 2/Network Node Manager i Setup Guide*. You can 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

  If use of network address translation (NAT) means that you will be managing areas in the network that contain duplicated IP addresses, select one address domain (an unduplicated address) that is to be detected by the Quick Start Wizard. Then see *Overlapping Addresses in NAT Environments* in the NNMi Help or *Managing Overlapping IP Addresses in NAT Environments* in the *Job Management Partner 1/Consolidated Management 2/Network Node Manager i Setup Guide*.
- Setting up an initial administrator account

Important note

You cannot use the Quick Start Configuration Wizard to complete the 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. In the **Configuration** workspace, select **Communication Configuration**.
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 details, see NNMi Help.

Reference note

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 monitoring environment. Each seed is identified by an IP address or host name; see *Configure Auto-Discovery Rules* in 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 *Specify Discovery Seeds* in NNMi Help.
- To configure discovery so that only the devices that you specify as seeds are discovered, do not create auto-discovery rules.

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

1. After the installation process finishes, launch the Quick Start Configuration Wizard as follows:

   Run the Quick Start Configuration Wizard immediately after installation. To manually launch the Quick Start Configuration Wizard, go to the following URL:

   ```
   http:// fully-qualified-domain-name:port/quickstart/
   ```

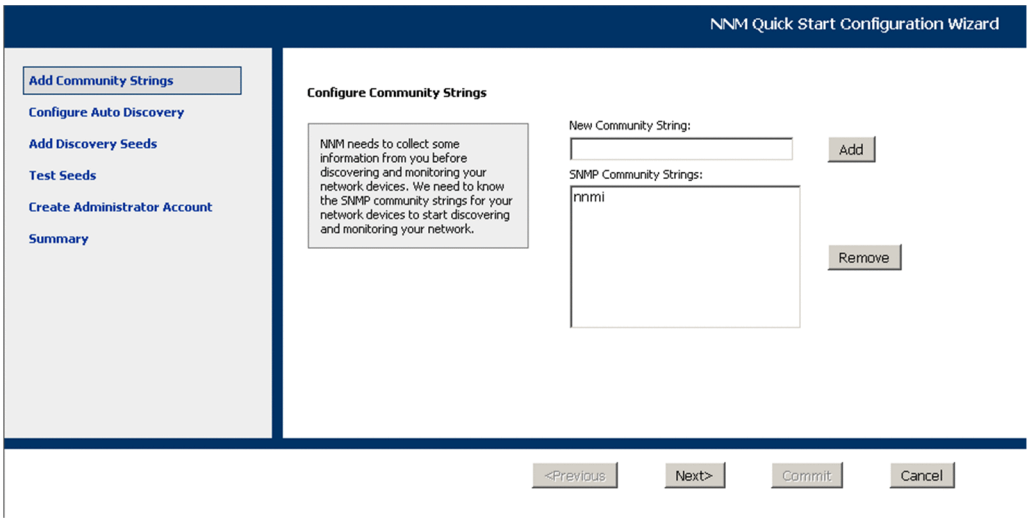
where *fully-qualified-domain-name* is the fully qualified domain name of the NNMi administrator server, and *port* is the port number that was set during installation.

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. For details, see the *nnmofficialfqdn.ovpl Reference Page*.

The NNMi Quick Start Configuration Wizard opens in a Web browser window.

2. Log on as follows:
   - User name: `system`
   - Password: Use the password for the system account that you created in *(1) Set the NNMi system account password* in *3.1.3 Operations after the installer finishes*.

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



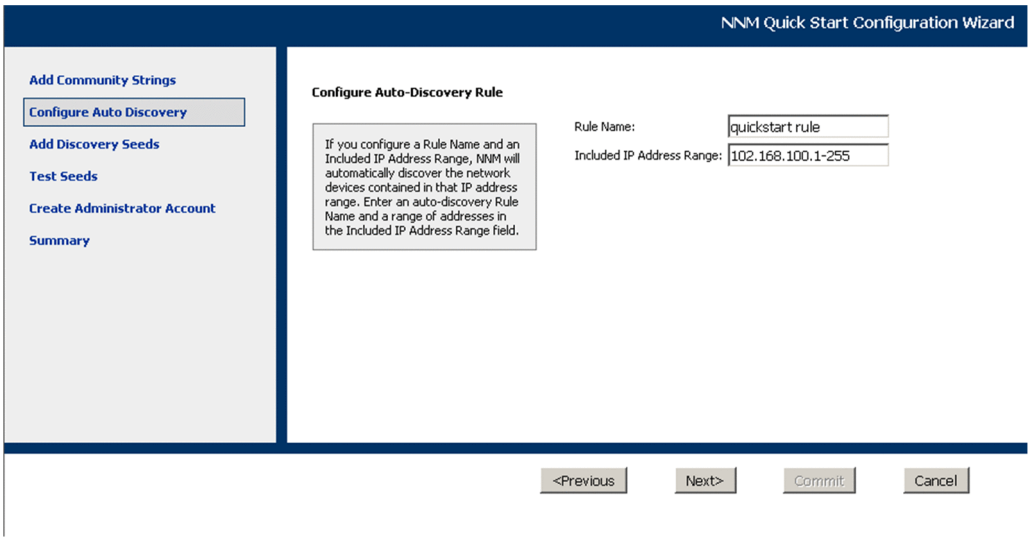
> **Reference note**
>
> NNMi automatically tries to match community strings to known devices. You do not need to manually associate each community string with a specific device.

4. Repeat step 3 until the **SNMP Community Strings** list includes the community strings for all nodes in the discovery range, and 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 SNMPv1/v2 Community Strings** tab of the **Communication Configuration** form.

5. On the **Configure Auto-Discovery Rules** page, associate the existing rule name with the **Included IP Address Range**. Enter the range of IP addresses for the discovery rule, and 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, enter discovery seed information for your network, and then click **Add**. After that, 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.

   > **Reference note**
   >
   > You can use the `nnmloadseeds.ovpl` command to load seeds using a command line. For details, see the *nnmloadseeds.ovpl Reference Page*.

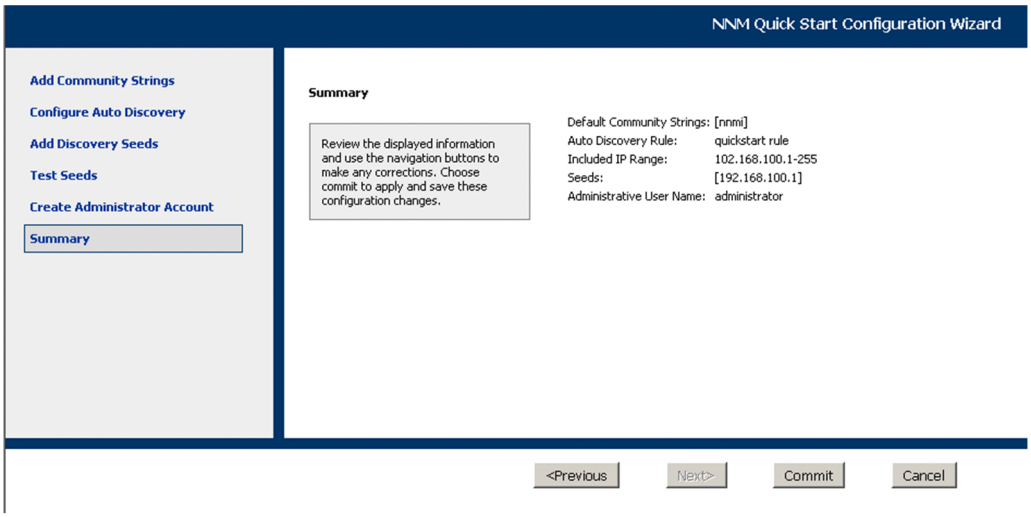
7. On the **Test Seeds** page, review the results of the communication tests. If any of the seed nodes cannot be reached with the community strings that you identified in step 3, click **Previous** to navigate to the **Configure Community Strings** page. Correct the community strings, and then click **Next**.

8. Repeat step 7 until all nodes can be reached, and then click **Next**.

9. On the **Configure Administrator Account** page, enter a **User Name**, and set the **Password** for a new account for administering the NNMi software. Then, click **Next**.

10. On the **Summary** page, review the information that you specified. Then, do one of the following actions:

    - To change any of the settings, click **Previous**.
    - To use the current settings, click **Commit**.



11. The **Wizard is complete** page indicates that you have successfully configured NNMi to discover a portion of your network. From here, do one of the following:
    - Click **Previous** to go back and make changes.
    - Click **Launch UI** to start the NNMi console user interface. To begin using NNMi, see *4. Getting Started with NNMi*.

> **Reference note**
>
> For Windows, after installation, restart any anti-virus software.

3.3 Licensing NNMi

If you do not have a permanent license key installed, the NNMi product includes a temporary license key that is valid for 60 days after you install NNMi. Therefore, obtain and install a permanent license key as soon as possible.

3.3.1 Preparing to install a permanent license key

The temporary license has a 250 node limit. If you have been running NNMi with a temporary 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.

(1) 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 i**.
2. In the About Network Node Manager i window, click **Licensing Information**.
3. Look for the value shown in the **Consumption** field.
   This value 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 details, see *Delete Nodes* in NNMi Help.

3.3.2 Obtaining and installing a permanent license key

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

- The Software License Agreement
- The IP address of the NNMi management server
- Your company or organization information

For details about how to obtain and install a permanent license key, see the *Release Notes*.

3.4 Removing NNMi

3.4.1 Removing NNMi (Windows)

1. Log on with administrator privileges to the system from which you plan to remove NNMi.
   If UAC is enabled, a user who is not the built-in Administrator must be promoted to administrator.

2. Stop all NNMi services.

3. Under **Control Panel** > **Programs and Features**, select **Network Node Manager** and then click **Uninstall or Change**.

4. A dialog box is displayed asking whether you want to start the uninstallation. Enter `yes` to start uninstalling NNMi.

   Example of input:

   ```
   ** Network Node Manager i Installer **
   * Starting uninstallation ? (yes/no) =>
   yes
   ```

5. After you have finished uninstalling NNMi, delete the NNMi installation directory and data directory.
   Performing an uninstallation might not always delete the NNMi installation and data directories. In this case, delete them manually.
   If default values were selected during installation, delete the following directories.

   - *drive*`:\Program Files (x86)\Hitachi\Cm2NNMi\`
   - *drive*`:\Program Files\Hitachi\Cm2NNMi\`
   - *drive*`:\ProgramData\Hewlett-Packard\HPOvLIC\`
   - *drive*`:\ProgramData\Hitachi\Cm2NNMi\`

6. Delete temporary directories and files.
   Delete the following temporary directories and files that are created by NNMi.
   The examples below show everything that might exist. There is no problem if some of the following do not exist. If you need the log output file for the uninstallation (`NNMUninstall.log`), make a copy of it before you delete the temporary file.

   ```
   %TEMP%\HPOvInstaller\
   %TEMP%\HPOvLic.log
   %TEMP%\HPOvPerlA-install.log
   %TEMP%\Install_Autopass.log
   %TEMP%\InstallerData
   %TEMP%\JP1NNMiMIBLoad.log
   %TEMP%\NNMUninstall.log
   %TEMP%\NNM_8.10.000_HPOvInstaller.txt
   %TEMP%\NNM_9.00.000_HPOvInstaller.txt
   %TEMP%\NNM_9.10.000_HPOvInstaller.txt
   %TEMP%\NNM_9.20.000_HPOvInstaller.txt
   %TEMP%\nmscreatedb.log
   %TEMP%\nnm_hotfixes.log
   %TEMP%\nnm_installconfig_vbs.log
   %TEMP%\nnm_premigration.log
   %TEMP%\nnm_preinstallcheck_phaseI.log
   ```

```
%TEMP%\nnm_preinstallcheck_phaseII.log
%TEMP%\ovRemoveDir.exe
%TEMP%\ovDetach.exe
%TEMP%\ovCleanUp.bat
%TEMP%\persistent_state
%TEMP%\preinstallcheck
%TEMP%\JP1NNMiInstaller.log
%TEMP%\JP1NNMiPostinstaller.log
%TEMP%\InstallScript.iap_xml
%TEMP%\nnm_preupgrade.log
%TEMP%\nnm_pre_dialogcheck.log
%TEMP%\OvLauncher.log
%TEMP%\nnm_pre-uninstall.log
```

7. Delete the environment variables.

   Uninstalling NNMi does not delete the environment variables `NnmDataDir`, `NnmInstallDir`, `OVCSL_LOG`, `OVCSL_LOG_APPLICATION`, and `OVCSL_LOG_FILE`, or *NnmInstallDir*`\bin\`, which is added to the environment variable `PATH` when NNMi is installed. Delete them manually. Note that *NnmInstallDir* is the value set in environment variable `NnmInstallDir`.

3.4.2 Removing NNMi (UNIX)

1. Log in as a user with root privileges to the system from which you plan to remove NNMi.
2. Stop all NNMi services.
3. Start the NNMi Uninstaller.

   Execute the following commands to start Hitachi PP Installer.

   - HP-UX or Solaris

   ```
   # /etc/hitachi_setup
   ```

   - Linux

   ```
   # /etc/hitachi_x64setup
   ```

4. Following the instructions, select the NNMi Uninstaller, and perform the uninstallation.
5. After you have finished uninstalling NNMi, delete the NNMi installation directory and data directory.

   Performing uninstallation might not always delete the NNMi installation and data directories. In this case, delete them manually.

   Delete the following directories.

   - Installation directory

   ```
   /opt/OV
   ```

   - Data directories

   ```
   /etc/opt/OV
   /var/opt/OV
   ```

6. Delete temporary directories and files.

   Delete the following temporary directories and files that are created by NNMi.

   The examples below show everything that might exist. There is no problem if some of the following do not exist. If you need the log output file for the uninstallation (`NNMUninstall.log`), make a copy of it before you delete the temporary file.

   - HP-UX

```
/var/tmp/HPOvInstaller
/var/tmp/HPOvPerlA-install.log
/var/tmp/NNMUninstall.log
/var/tmp/NNM_8.10.000_HPOvInstaller.txt
/var/tmp/NNM_9.00.000_HPOvInstaller.txt
/var/tmp/NNM_9.10.000_HPOvInstaller.txt
/var/tmp/NNM_9.20.000_HPOvInstaller.txt
/var/tmp/JP1NNMiInstaller.log
/var/tmp/JP1NNMiPostinstaller.log
/tmp/debug
/tmp/ia_remove.shxxx.tmp (where xxx is one or more numeric characters)
/tmp/install.dir.xxx (where xxx is one or more numeric characters)
/tmp/JP1NNMiMIBLoad.log
/tmp/nnm-premigration.log
/tmp/nnm_preinstallcheck_phaseI.log
/tmp/nnm_preinstallcheck_phaseII.log
/tmp/ovinstallparams.ini
/tmp/persistent_state
/tmp/preinstallcheck
/tmp/nnm-preupgrade.log
/tmp/nnm_pre_dialogcheck.log
```

   - Solaris

```
/var/tmp/HPOvInstaller
/var/tmp/HPOvPerlA-install.log
/var/tmp/NNMUninstall.log
/var/tmp/NNM_8.10.000_HPOvInstaller.txt
/var/tmp/NNM_9.00.000_HPOvInstaller.txt
/var/tmp/NNM_9.10.000_HPOvInstaller.txt
/var/tmp/NNM_9.20.000_HPOvInstaller.txt
/var/tmp/JP1NNMiInstaller.log
/var/tmp/JP1NNMiPostinstaller.log
/tmp/debug
/tmp/install.dir.xxx (where xxx is one or more numeric characters)
/tmp/JP1NNMiMIBLoad.log
/tmp/nnm-premigration.log
/tmp/nnm_preinstallcheck_phaseI.log
/tmp/nnm_preinstallcheck_phaseII.log
/tmp/ovinstallparams.ini
/tmp/persistent_state
/tmp/preinstallcheck
/tmp/nnm-preupgrade.log
/tmp/nnm_pre_dialogcheck.log
```

   - Linux

```
/var/tmp/HPOvPerlA-install.log
/var/tmp/JP1NNMiInstaller.log
```

```
/var/tmp/JP1NNMiPostinstaller.log
/var/tmp/rpm-tmp.xxx (where xxx is one or more alphanumeric characters)
/tmp/install.dir.xxx (where xxx is one or more numeric characters)
/tmp/ia_remove.shxxx.tmp (where xxx is one or more numeric characters)
/tmp/HPOvInstaller
/tmp/NNMUninstall.log
/tmp/NNM_8.10.000_HPOvInstaller.txt
/tmp/NNM_9.00.000_HPOvInstaller.txt
/tmp/NNM_9.10.000_HPOvInstaller.txt
/tmp/NNM_9.20.000_HPOvInstaller.txt
/tmp/debug
/tmp/JP1NNMiMIBLoad.log
/tmp/nnm-premigration.log
/tmp/nnm_preinstallcheck_phaseI.log
/tmp/nnm_preinstallcheck_phaseII.log
/tmp/ovinstallparams.ini
/tmp/persistent_state
/tmp/preinstallcheck
/tmp/nnm-preupgrade.log
/tmp/nnm_pre_dialogcheck.log
```

4 Getting Started with NNMi

This chapter provides information that you need to know before you begin using NNMi to manage your network. It includes a general overview of both how to access NNMi and how to specify network discovery settings. You can find more detailed information for operators and administrators in NNMi Help.

4.1 Accessing NNMi

Now that you have installed NNMi and completed post-installation configuration tasks, 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 access the NNMi console, follow these steps:

1. Make sure that you are using a supported Web browser.
   See *2.1 Checking the hardware and software*.

2. Enable the Web browser for JavaScript, pop-up windows from the NNMi management server, and to accept cookies from the NNMi management server.
   See *A.3 Enabling the Web browser for the NNMi console*.

3. Enter the following URL into a Web browser window:
   `http://`*fully-qualified-domain-name*`:`*port*`/nnm/`
   where *fully-qualified-domain-name* represents the fully qualified domain name of the NNMi management server, and *port* is the port that 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. For details, see the *nnmofficialfqdn.ovpl Reference Page*.
   If you do not know which port to use, see *B.2(2) Problem: The NNMi console page cannot be found*.
   If you cannot start an NNMi console when pointing your browser to an NNMi management server that is installed on a Windows operating system, you might have a Windows firewall on the NNMi management server that is blocking the http port. See *B.2(5) Problem: You cannot start the NNMi console when accessing a Windows NNMi management server*.

4. In the NNMi sign-in window, enter your user account name and password, and then click **Sign In**.
   For details, see *About user accounts and roles* below.

About user accounts and roles

After installation, NNMi provides a special system account to be used to access NNMi for the first time. Do not use this system account for everyday use.

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 user roles listed below 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-level 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 details, see *Configuring Security* in NNMi Help.

NNMi provides an out-of-the-box https configuration using a self-signed certificate created during installation. For details about using a signed certificate from a Certificate Authority instead of the self-signed certificate, see the manual *Job Management Partner 1/Consolidated Management 2/Network Node Manager i Setup Guide*.

4.2 Accessing NNMi Help

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

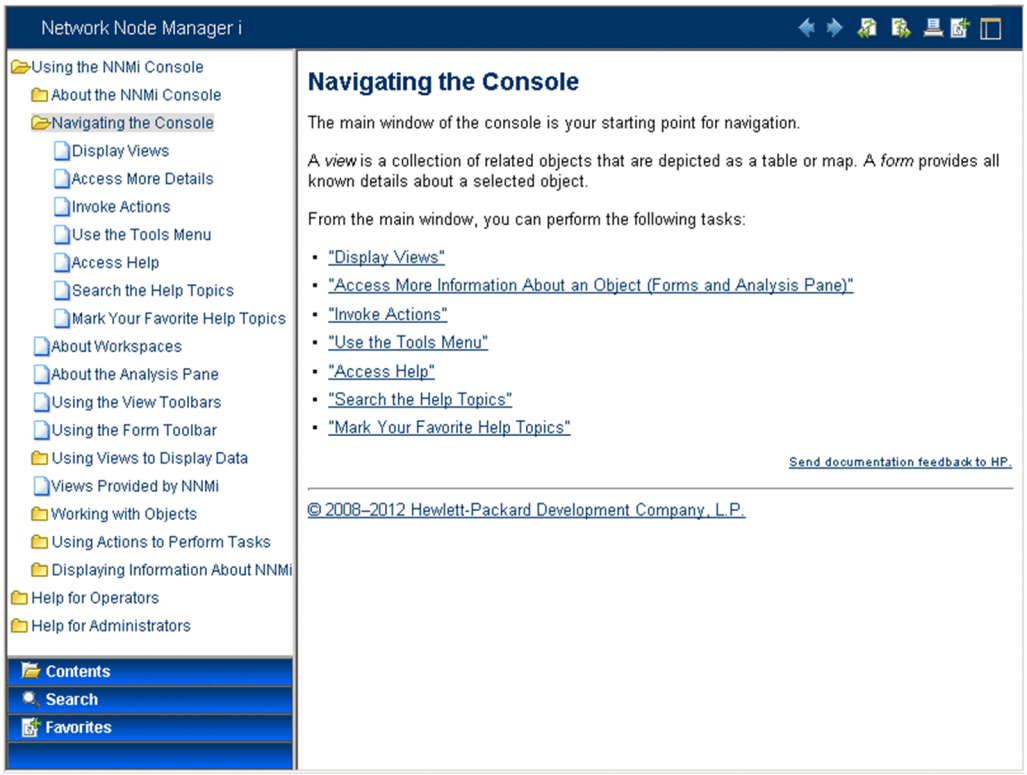
- *Using the NNMi Console*
- *Help for Operators*
- *Help for Administrators*

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

> **Reference note**
>
> The NNMi console includes forms for entering information. The form name is in the upper left 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*** is the title of the current form.

The following figure shows the NNMi Help window.

Figure 4–1: NNMi help



4.3 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 configure NNMi to discover and manage a few nodes with only a few interfaces. The Quick Start Configuration Wizard (see *3.2 Using the Quick Start Configuration Wizard*) provides an easy way to set up this type of small configuration. Hitachi 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 the following table summarizes these tasks.

Table 4–1: Discovery configuration checklist

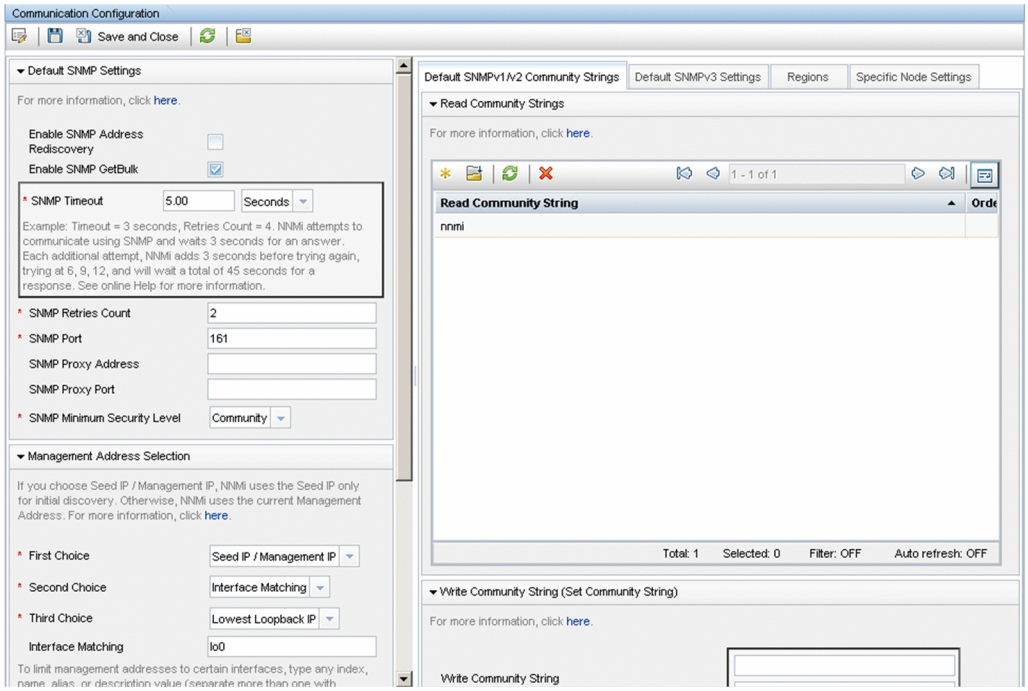
Completed? (y/n)	Task
	Verify that all nodes to be discovered are connected to the network and configured with a supported version of SNMP (SNMPv1, SNMPv2c, or SNMPv3).
	Obtain read-only community strings from your network administrator for the nodes that you plan to manage.
	Using the NNMi console, configure community strings as described in *4.3.1 Configuring community strings*.
	Using the NNMi console, configure the spiral discovery process as described in *4.3.2 Configuring auto-discovery rules*.
	Using the NNMi console, check the spiral discovery progress as described in *4.3.3 Checking discovery progress*.

For details about the discovery process, see *Discovering Your Network* in NNMi Help.

4.3.1 Configuring community strings

To configure NNMi with community strings, follow these steps:

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



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

For details about setting up device community strings and loading community strings from a file, see *Configuring Communication Protocol* in NNMi Help.

4.3.2 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* in the *Reference note* below)

To configure auto-discovery rules, follow these steps:

1. From the workspace navigation panel, from the **Configuration** workspace, open **Discovery**.
2. Open the **Discovery Configuration** form.
3. Click the **Auto-Discovery Rules** tab, and then click the **New** icon.
4. On the **Auto-Discovery Rule** form, under **Basics**, enter the rule **Name** and **Ordering** information.
   The order is a numerical value that specifies the priority of this rule in comparison to other auto-discovery rules. For details, click **Help** > **Using the Auto-Discovery Rule Form**.

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

To monitor the progress of discovery, see *4.3.3 Checking discovery progress*.

For details about configuring discovery, see *Configure Discovery* in NNMi Help.

Reference note

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 the 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 NNMi Help.

4.3.3 Checking discovery progress

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

Reference note

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

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

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

  ### Reference note

  If you suspect a problem with discovery, see *B.2(4) Problem: NNMi is not discovering nodes*.

Appendixes

A. Additional Information About Installation

This section provides additional information about installing NNMi.

A.1 Specifying disk drive security settings (Windows)

To set disk drive security before installing NNMi, complete the following steps:

1. Open **Computer** to view your disk drives.
2. For the drive you plan to use for the NNMi installation, choose **Properties** in the right-click menu, and then click the **Security** tab.
3. Log on as a user with administrator privileges, making sure that **Full control** is allowed (either directly or derived through group membership).
4. On the **Security** tab, click **Advanced** to open **Advanced Security Settings**, and make sure the **Applies To** field for Administrators is set to **This folder, subfolders, and files**. If this is not the case, change the setting.
5. Make sure that **Full control** is allowed for the built-in **Local Service** user (either directly or derived through the local users group). If this is not the case, change the setting.
6. On the **Security** tab, click **Advanced** to open **Advanced Security Settings**, and make sure the **Applies To** field for the built-in **Local Service** user is set to **This folder, subfolders, and files**. If this is not the case, change the setting.
7. Apply your changes.
8. Proceed with the NNMi installation.

A.2 Obtaining or setting the official fully qualified domain name

NNMi users access NNMi by using the official fully qualified domain name (FQDN).

1. To determine the official FQDN of the NNMi management server, use one of the following methods:
   - Use the `nnmofficialfqdn.ovpl` command to display the value of the FQDN setting. For details, see the *nnmofficialfqdn.ovpl Reference Page*.
   - In the NNMi console, click **Help** > **System Information**. From the **Server** tab, find the value for the fully qualified domain name.
2. If you need to change the FQDN that was set during installation, use the `nnmsetofficialfqdn.ovpl` command.
   For details, see the *nnmofficialfqdn.ovpl Reference Page*.

A.3 Enabling the Web browser for the NNMi console

Before you sign on to NNMi, make sure that the Web browser is configured to interact with the NNMi console. The following items must be enabled in the Web browser on each client machine that will access the NNMi management server:

- JavaScript
- Pop-up windows from the NNMi management server
- Cookies from the NNMi management server
- ActiveX
- VML, if you use Internet Explorer 8
- If the IE ESC configuration is enabled in an environment that uses Internet Explorer, add `about:blank` to **Trusted Sites**.

Below are Web browser configuration examples.

Important note

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

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* for more information.

(1) Mozilla Firefox

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

(2) Microsoft Internet Explorer

1. In Internet Explorer, click **Tools**, and then choose **Internet Options**.
2. On the **Security** tab, select the zone that includes the NNMi management server, and then click **Custom Level**.
3. In **ActiveX controls and plug-ins**, under **Run ActiveX controls and plug-ins**, select the **Enable** option.

4. Under **Scripting**, select the **Enable** option for Active scripting.

5. On the **Privacy** tab **Settings** area, select one of the options between **Accept All Cookies** and **Medium High**.

   Reference note

   This setting affects the Internet zone only. If you are connecting to the NNMi management server over an intranet, this setting has no effect.

6. On the **Privacy** tab, select the **Turn on Pop-up Blocker** check box, and then click **Settings**.

7. Add the fully qualified domain name of the NNMi management server to the list of allowed sites.

8. Restart the Web browser.

For Internet Explorer 8, perform one of the following two procedures:

If the Internet Explorer Enhanced Security (IE ESC) configuration is enabled, perform the following steps in addition to the above:

1. In Internet Explorer, choose **Tools**, **Internet Options**, and then click the **Security** tab.

2. Add `about:blank` to the **Trusted sites** zone.

(3) Microsoft Internet Explorer 8

In the case of Internet Explorer 8, in addition to the steps in *(2) Microsoft Internet Explorer*, configure the browser using either of the following methods:

(a) Method 1

1. In Internet Explorer, select **Tools** > **Internet Options**, and then click the **Security** tab.

2. Add the site of the connected NNMi server to the **Local intranet** or **Trusted sites** zone.

3. In the security zone added in step 2, click **Customize Level**, and then enable **Binary and script behaviors**. Hitachi recommends that you add the NNMi server to the **Trusted sites** zone, and that you enable privileges within a more restricted zone.

(b) Method 2

For this method, you must log in as a user with administrator privileges.

1. If the most recent patch is out of date, VML might be disabled.
   Use Windows Update or another method to install the latest update of Internet Explorer on the client machine.

2. If performing step 1 does not solve the problem, perform step 3.

3. Check whether VML's `vgx.dll` is registered. If it is not, run the following command:

   ```
   regsvr32 "%ProgramFiles%\Common Files\Microsoft Shared\VGX\vgx.dll"
   ```

   Check the Access Control List settings on `vgx.dll`.

   ```
   cacls "%ProgramFiles%\Common Files\Microsoft Shared\VGX\vgx.dll"
   ```

A.4 Installing required libraries in Linux

Before you can install NNMi on a Linux server, the library files listed below that are needed by NNMi must be installed. Also, install the library files that have dependence relationships with these files:

- `/lib64/libaio.so.1`
- `/usr/lib/libstdc++.so.6`
- `/usr/lib64/libXtst.so.6`
- `/usr/lib64/libXi.so.6`

For details, see the NNMi *Release Notes* and the operating system documentation.

A.5 Setting the system account password

You can set or change the system account password by using the `nnmchangesyspw.ovpl` script. Follow these steps:

1. Use the `ovstop -c` command to stop the NNMi processes.
2. As an administrator, run the `nnmchangesyspw.ovpl` script to set the system password.
3. Use the `ovstart -c` command to start the NNMi processes.

For details, see the *nnmchangesyspw.ovpl Reference Page*.

B. Troubleshooting Installation and Initial Startup

B.1 Installation problems

(1) Problem: NNMi installation requires more disk space than is currently available in the host system (UNIX)

(a) Solution

When installing NNMi in UNIX, you are not allowed to select the location where binary data is installed (`$OV_INST_DIR`) or the location where data files are installed (`$OV_DATA_DIR`). These locations are set as follows in the initial configuration:

- `OV_INST_DIR=/opt/OV`
- `OV_DATA_DIR=/var/opt/OV`

If there is insufficient disk space in either `/opt/OV` or `/var/opt/OV`, improve availability with either of the following methods:

1. If necessary, uninstall NNMi.
2. Create a symbolic link from the installation target to a partition that has sufficient disk space to install the binary data, and save the data files. The syntax for creating symbolic links is as follows:

`ln -s` *large-disk* `/opt/OV`

`ln -s` *large-disk* `/var/opt/OV`

Important note

- Set the access permission for the parent directory at the installation site to `555` or higher.
- For Solaris, set environment variable `PKG_NONABI_SYMLINKS` to `true`.

1. Install NNMi.

(2) Problem: A message is displayed during installation indicating that the preinstallation procedure (phase II) has failed and the /tmp/nnm_preinstall_phasell.log file needs to be checked for the details (UNIX)

(a) Solution

The NNMi installation script automatically creates two groups (`nmsgrp` and `nmsdb`), two users (`nmsproc` and `nmsdbmgr`), and the corresponding `$HOME` directories. This operation might fail for either of the following reasons:

- Users and groups cannot be created because `useradd` or `groupadd` was disabled by the IT department.
- The root user cannot create a `$HOME` directory because the `$HOME` directory exists on NFS.

Installation stops whenever the NNMi installer is unable to create these groups, users, or directories. In such a case, you can create the users manually and restart the installation.

1. Create the `nmsproc` user in the `nmsgrp` group.
   Set the `$HOME` directory to any directory that exists.

2. Create the `nmsdbmgr` user in the `nmsdb` group.
   Set the `$HOME` directory to any directory that exists.

If you know that these operations will fail but you need to control user IDs, group IDs, or the locations of `$HOME`, you can first create the groups, users, and `$HOME` directories, and then start the installer.

When the `useradd` command is used to create a user, the default home directory will be `/home/`*user-name*. In Solaris, however, note that, with the default setting, directories cannot be created in `/home`. If your environment does not allow directories to be created in `/home`, change the `useradd` command's default home directory to a location that allows directories to be created.

B.2 Initial startup problems

(1) Problem: The user cannot run the NNMi command line tools on UNIX NNMi management servers

(a) Solution

Check whether system environment variable `PATH` includes `/opt/OV/bin`. If it does not, add `/opt/OV/bin` to system environment variable `PATH`.

(2) Problem: The NNMi console page cannot be found

(a) Solution

The URL for accessing the NNMi console includes the port that JBoss Application Server uses for communicating with the NNMi console. To access the NNMi console, enter the following URL into a Web browser window:

```
http://fully-qualified-domain-name:port/nnm/
```

where *fully-qualified-domain-name* is the fully qualified domain name of the NNMi management server, and *port* is the port that 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. For details, see the *nnmofficialfqdn.ovpl Reference Page*.

To determine which port JBoss Application Server is using, use the following files:

Windows

`%NnmDataDir%Conf\nnm\props\nms-local.properties`

`%NnmDataDir%` is the data directory specified during installation.

UNIX

`/var/opt/OV/conf/nnm/props/nms-local.properties`

In this file, look for the following line:

```
nmsas.server.port.web.http=80
```

The port assigned to `nmsas.server.port.web.http` is the port to specify in the URL. For details, see the *nnm.ports Reference Page*.

(3) Problem: JBoss port contention

(a) Solution

By default, JBoss Application Server uses several ports for communication with NNMi. These ports are commonly used by other applications as well.

To resolve any port contention, follow these steps:

1. As a user with administrator privileges (Windows) or root privileges (UNIX), open the following file in any text editor:
   - Windows
     `%NnmDataDir%Conf\nnm\props\nms-local.properties`
     `%NnmDataDir%` is the data directory specified during installation.
   - UNIX
     `/var/opt/OV/conf/nnm/props/nms-local.properties`
2. Modify the existing entries, replacing any conflicting port numbers with available port numbers.
3. Save the file, and then restart the NNMi services:

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

> **Reference note**
>
> For Windows, the `ovstop` and `ovstart` commands can be executed from the **Start** menu. For details about the ports used by NNMi, see the *nnm.ports Reference Page*.

(4) Problem: NNMi is not discovering nodes

(a) Solution

1. From the **Workspace** navigation panel, select the **Configuration** workspace.
2. From **Configuration**, open the **Seeds** view.
3. Check the values in the **Discovery Seed Results** 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 the `nnmsnmpwalk.ovpl` command to obtain information from the node. For details, see the *nnmsnmpwalk.ovpl Reference Page*. 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. Be 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 SNMPv1/v2 Community Strings** tab.

e. Make sure that there are no Access Control Lists configured on your routers, switches, or firewalls that might be limiting discovery.

For details, see *Configure Discovery* in NNMi Help.

(5) Problem: You cannot start the NNMi console when accessing a Windows NNMi management server

If you cannot start an NNMi console when pointing your browser to a Windows NNMi management server, a firewall might be blocking the HTTP port. To troubleshoot this problem, run the browser on the NNMi management server. If you can access the NNMi console from this browser, but remote browsers fail, you need to check your ports.

To remedy this problem, add the `nmsas.server.port.web.http` value shown in the `%NnmDataDir%\conf\nnm\props\nms-local.properties` file to the list of allowed ports. For details, see the *nnm.ports Reference Page*.

`%NnmDataDir%` is the data directory specified during installation.

C. List of MIBs Read During a New Installation

The table below lists the MIBs that are read during a new installation of NNMi.

These MIBs are not read during upgrading.

The MIB files shown in the table are relative paths from the following path:

- Windows

  ```
  %NnmInstallDir%misc\nnm\snmp-mibs\
  ```

  In Windows, the path demarcator is the backward slash (\), not the forward slash (/).

- UNIX

  ```
  $NnmInstallDir/misc/nnm/snmp-mibs/
  ```

Table C–1: MIBs read during a new installation

MIB name	MIB file
ATM-FORUM-MIB	Vendor/Cisco/ATM-FORUM-MIB.my
ATM-FORUM-TC-MIB	Vendor/Cisco/ATM-FORUM-TC-MIB.my
ATM-MIB	Standard/rfc2515-ATM-MIB.mib
ATM-TC-MIB	Standard/rfc2514-ATM-TC-MIB.mib
ATM2-MIB	Standard/rfc3606-ATM2-MIB.mib
AX-BOOTMANAGEMENT-MIB	Vendor/OTHER-VENDORS/AX-BOOTMANAGEMENT-MIB.my
AX-DEVICE-MIB	Vendor/OTHER-VENDORS/AX-DEVICE-MIB.my
AX-FLOW-MIB	Vendor/OTHER-VENDORS/AX-FLOW-MIB.my
AX-LOGIN-MIB	Vendor/OTHER-VENDORS/AX-LOGIN-MIB.my
AX-NOTIFICATION	Vendor/OTHER-VENDORS/AX-NOTIFICATION.my
AX-OSPF-MIB	Vendor/OTHER-VENDORS/AX-OSPF-MIB.my
AX-OSPFV3-MIB	Vendor/OTHER-VENDORS/AX-OSPFV3-MIB.my
AX-QUEUE-MIB	Vendor/OTHER-VENDORS/AX-QUEUE-MIB.my
AX-SMI-MIB	Vendor/OTHER-VENDORS/AX-SMI-MIB.my
AX-STATS-MIB	Vendor/OTHER-VENDORS/AX-STATS-MIB.my
AX-SYSTEM-MIB	Vendor/OTHER-VENDORS/AX-SYSTEM-MIB.my
AX-VRF-MIB	Vendor/OTHER-VENDORS/AX-VRF-MIB.my
AX1230S	Vendor/OTHER-VENDORS/AX1230S-MIB.my
AX1240S	Vendor/OTHER-VENDORS/AX12S.my
AX2000R	Vendor/OTHER-VENDORS/AX2K-MIB.MY
AX2430S	Vendor/OTHER-VENDORS/AX24S.my
AX2530S	Vendor/OTHER-VENDORS/AX2530S-MIB.my
AX3630S	Vendor/OTHER-VENDORS/AX36S.my

MIB name	MIB file
AX5400S-TRAP	Vendor/OTHER-VENDORS/AXS.MY
AX6300S	Vendor/OTHER-VENDORS/AX63S.my
AX7700R-TRAP	Vendor/OTHER-VENDORS/AXR.MY
AX7800R	Vendor/OTHER-VENDORS/AXR.MY
AX7800R-TRAP	Vendor/OTHER-VENDORS/AXR.MY
AX7800S	Vendor/OTHER-VENDORS/AXS.MY
AX7800S-TRAP	Vendor/OTHER-VENDORS/AXS.MY
AXS-6700S-TRAP	Vendor/OTHER-VENDORS/AX63S.my
AXS-AX1240S-TRAP	Vendor/OTHER-VENDORS/AX12S.my
AXS-AX1250S-TRAP	Vendor/OTHER-VENDORS/AX12S.my
AXS-AX2230S-TRAP	Vendor/OTHER-VENDORS/AX12S.my
AXS-AX3630S-TRAP	Vendor/OTHER-VENDORS/AX36S.my
AXS-AX3640S-TRAP	Vendor/OTHER-VENDORS/AX36S.my
AXS-AX3650S-TRAP	Vendor/OTHER-VENDORS/AX36S.my
AXS-AX3830S-TRAP	Vendor/OTHER-VENDORS/AX36S.my
AXS-AX6300S-TRAP	Vendor/OTHER-VENDORS/AX63S.my
AXS-AX6600S-TRAP	Vendor/OTHER-VENDORS/AX63S.my
Apresia-Series	Vendor/OTHER-VENDORS/Apresia-mibs.mib
Apresia-SeriesLightFMGM	Vendor/OTHER-VENDORS/ApresiaLightFMGM-mibs.mib
ArcsightModule	Vendor/Hewlett-Packard/hp-arcsight.mib
BGP4-MIB	Standard/rfc4273-BGP4-MIB.mib
BRIDGE-MIB	Standard/rfc4188-BRIDGE-MIB.mib
CISCO-AAL5-MIB	Vendor/Cisco/CISCO-AAL5-MIB.my
CISCO-ATM-IF-MIB	Vendor/Cisco/CISCO-ATM-IF-MIB.my
CISCO-ATM-SWITCH-ADDR-MIB	Vendor/Cisco/CISCO-ATM-SWITCH-ADDR-MIB.my
CISCO-C2900-MIB	Vendor/Cisco/CISCO-C2900-MIB.my
CISCO-CDP-MIB	Vendor/Cisco/CISCO-CDP-MIB.my
CISCO-DOT11-ASSOCIATION-MIB	Vendor/Cisco/CISCO-DOT11-ASSOCIATION-MIB.my
CISCO-DOT11-IF-MIB	Vendor/Cisco/CISCO-DOT11-IF-MIB.my
CISCO-ENTITY-FRU-CONTROL-MIB	Vendor/Cisco/CISCO-ENTITY-FRU-CONTROL-MIB.my
CISCO-ENTITY-VENDORTYPE-OID-MIB	Vendor/Cisco/CISCO-ENTITY-VENDORTYPE-OID-MIB.my
CISCO-ENVMON-MIB	Vendor/Cisco/CISCO-ENVMON-MIB.my
CISCO-FLASH-MIB	Vendor/Cisco/CISCO-FLASH-MIB.my
CISCO-FRAME-RELAY-MIB	Vendor/Cisco/CISCO-FRAME-RELAY-MIB.my
CISCO-HSRP-MIB	Vendor/Cisco/CISCO-HSRP-MIB.my

MIB name	MIB file
CISCO-IETF-IP-MIB	Vendor/Cisco/CISCO-IETF-IP-MIB.my
CISCO-IETF-IPMROUTE-MIB	Vendor/Cisco/CISCO-IETF-IPMROUTE-MIB.my
CISCO-IETF-PIM-EXT-MIB	Vendor/Cisco/CISCO-IETF-PIM-EXT-MIB.my
CISCO-IETF-PIM-MIB	Vendor/Cisco/CISCO-IETF-PIM-MIB.my
CISCO-IETF-PW-ENET-MIB	Vendor/Cisco/CISCO-IETF-PW-ENET-MIB.my
CISCO-IETF-PW-MIB	Vendor/Cisco/CISCO-IETF-PW-MIB.my
CISCO-IETF-PW-MPLS-MIB	Vendor/Cisco/CISCO-IETF-PW-MPLS-MIB.my
CISCO-IETF-PW-TC-MIB	Vendor/Cisco/CISCO-IETF-PW-TC-MIB.my
CISCO-MEMORY-POOL-MIB	Vendor/Cisco/CISCO-MEMORY-POOL-MIB.my
CISCO-MVPN-MIB	Vendor/Cisco/CISCO-MVPN-MIB.my
CISCO-NBAR-PROTOCOL-DISCOVERY-MIB	Vendor/Cisco/CISCO-NBAR-PROTOCOL-DISCOVERY-MIB.my
CISCO-PIM-MIB	Vendor/Cisco/CISCO-PIM-MIB.my
CISCO-PRODUCTS-MIB	Vendor/Cisco/CISCO-PRODUCTS-MIB.my
CISCO-QOS-PIB-MIB	Vendor/Cisco/CISCO-QOS-PIB-MIB.my
CISCO-RF-MIB	Vendor/Cisco/CISCO-RF-MIB.my
CISCO-RHINO-MIB	Vendor/Cisco/CISCO-RHINO-MIB.my
CISCO-RTTMON-MIB	Vendor/Cisco/CISCO-RTTMON-MIB.my
CISCO-RTTMON-TC-MIB	Vendor/Cisco/CISCO-RTTMON-TC-MIB.my
CISCO-SMI	Vendor/Cisco/CISCO-SMI.my
CISCO-STACK-MIB	Vendor/Cisco/CISCO-STACK-MIB.my
CISCO-TC	Vendor/Cisco/CISCO-TC.my
CISCO-VTP-MIB	Vendor/Cisco/CISCO-VTP-MIB.my
CISCOWAN-SMI	Vendor/Cisco/CISCOWAN-SMI.my
COMETAGT-AIX	Vendor/OTHER-VENDORS/hitachi-cometAgt-aix
COMETAGT-LINUX	Vendor/OTHER-VENDORS/hitachi-cometAgt-linux
COMETAGT-SOLARIS	Vendor/OTHER-VENDORS/hitachi-cometAgt-solaris
COMETAGT-TRU64	Vendor/OTHER-VENDORS/hitachi-cometAgt-tru64
DHCP-MIB	Vendor/Microsoft/dhcp.mib
DIFFSERV-DSCP-TC	Standard/rfc3289-DIFFSERV-DSCP-TC.mib
DIFFSERV-MIB	Standard/rfc3289-DIFFSERV-MIB.mib
DISMAN-NSLOOKUP-MIB	Standard/rfc4560-DISMAN-NSLOOKUP-MIB.mib
DISMAN-PING-MIB	Standard/rfc4560-DISMAN-PING-MIB.mib
DISMAN-TRACEROUTE-MIB	Standard/rfc4560-DISMAN-TRACEROUTE-MIB.mib
DRAFT-MSDP-MIB	Vendor/Cisco/MSDP-MIB.my
DS1-MIB	Standard/rfc4805-DS1-MIB.mib

MIB name	MIB file
DS3-MIB	Standard/rfc3896-DS3-MIB.mib
DVMRP-MIB	Vendor/Nortel/DVMRP-MIB.mib
ENTITY-MIB	Standard/rfc4133-ENTITY-MIB.mib
ENTITY-STATE-MIB	Standard/rfc4268-ENTITY-STATE-MIB.mib
ENTITY-STATE-TC-MIB	Standard/rfc4268-ENTITY-STATE-TC-MIB.mib
EXTREME-BASE-MIB	Vendor/Extreme/v730b49.mib
EXTREME-CABLE-MIB	Vendor/Extreme/v730b49.mib
EXTREME-DLCS-MIB	Vendor/Extreme/v730b49.mib
EXTREME-DOS-MIB	Vendor/Extreme/v730b49.mib
EXTREME-EAPS-MIB	Vendor/Extreme/v730b49.mib
EXTREME-EDP-MIB	Vendor/Extreme/v730b49.mib
EXTREME-ENH-DOS-MIB	Vendor/Extreme/v730b49.mib
EXTREME-ESRP-MIB	Vendor/Extreme/v730b49.mib
EXTREME-FDB-MIB	Vendor/Extreme/v730b49.mib
EXTREME-FILETRANSFER-MIB	Vendor/Extreme/v730b49.mib
EXTREME-NETFLOW-MIB	Vendor/Extreme/v730b49.mib
EXTREME-NP-MIB	Vendor/Extreme/v730b49.mib
EXTREME-OSPF-MIB	Vendor/Extreme/v730b49.mib
EXTREME-PBQOS-MIB	Vendor/Extreme/v730b49.mib
EXTREME-POE-MIB	Vendor/Extreme/v730b49.mib
EXTREME-PORT-MIB	Vendor/Extreme/v730b49.mib
EXTREME-POS-MIB	Vendor/Extreme/v730b49.mib
EXTREME-QOS-MIB	Vendor/Extreme/v730b49.mib
EXTREME-RTSTATS-MIB	Vendor/Extreme/v730b49.mib
EXTREME-SERVICES-MIB	Vendor/Extreme/v730b49.mib
EXTREME-SLB-MIB	Vendor/Extreme/v730b49.mib
EXTREME-SNMPV3-MIB	Vendor/Extreme/v730b49.mib
EXTREME-STP-EXTENSIONS-MIB	Vendor/Extreme/v730b49.mib
EXTREME-SYSTEM-MIB	Vendor/Extreme/v730b49.mib
EXTREME-TRAP-MIB	Vendor/Extreme/v730b49.mib
EXTREME-TRAPPOLL-MIB	Vendor/Extreme/v730b49.mib
EXTREME-V2TRAP-MIB	Vendor/Extreme/v730b49.mib
EXTREME-VC-MIB	Vendor/Extreme/v730b49.mib
EXTREME-VLAN-MIB	Vendor/Extreme/v730b49.mib
EXTREME-WIRELESS-MIB	Vendor/Extreme/v730b49.mib

MIB name	MIB file
EXTREMEdot11AP-MIB	Vendor/Extreme/v730b49.mib
EXTREMEdot11f-MIB	Vendor/Extreme/v730b49.mib
EtherLike-MIB	Standard/rfc3635-EtherLike-MIB.mib
FDDI-SMT73-MIB	Standard/Historic/rfc1512-FDDI-SMT73-MIB.mib
FOUNDRY-SN-ROOT-MIB	Vendor/Foundry/FOUNDRY-SN-ROOT-MIB.mib
FRAME-RELAY-DTE-MIB	Standard/rfc2115-FRAME-RELAY-DTE-MIB.mib
FtpServer-MIB	Vendor/Microsoft/ftp.mib
HC-RMON-MIB	Standard/rfc3273-HC-RMON-MIB.mib
HCNUM-TC#	NNM/server/lib/nms-mib-model.jar/com/hp/ov/nms/mib/model/hibernate/rfc2856-HCNUM-TC.mib
HOST-RESOURCES-MIB	Standard/rfc2790-HOST-RESOURCES-MIB.mib
HOST-RESOURCES-TYPES	Standard/rfc2790-HOST-RESOURCES-TYPES.mib
HP-ICF-OID	Vendor/Hewlett-Packard/ProCurve/hpicfOid.mib
HP-SITESCOPE-MIB	Vendor/Hewlett-Packard/HP-SITESCOPE-MIB.mib
HP-SN-AGENT-MIB	Vendor/Hewlett-Packard/hpEtherSwitch/hp-sn-agent.mib
HP-SN-ROOT-MIB	Vendor/Hewlett-Packard/hpEtherSwitch/hp-sn-root.mib
HP-SN-SWITCH-GROUP-MIB	Vendor/Hewlett-Packard/hpEtherSwitch/hp-sn-switch.mib
HP-UNIX	Vendor/Hewlett-Packard/hp-unix
HttpServer-MIB	Vendor/Microsoft/http.mib
IANA-ADDRESS-FAMILY-NUMBERS-MIB	Standard/IANA-ADDRESS-FAMILY-NUMBERS-MIB.mib
IANA-MAU-MIB	Standard/rfc4836-IANA-MAU-MIB.mib
IANA-RTPROTO-MIB	Vendor/Cisco/IANA-RTPROTO-MIB.my
IANATn3270eTC-MIB	Standard/IANATn3270eTC-MIB.mib
IANAifType-MIB	Standard/IANAifType-MIB.mib
IEEE8021-TC-MIB	IEEE/IEEE8021-TC-MIB.mib
IEEE8023-LAG-MIB	IEEE/IEEE8023-LAG-MIB.mib
IEEE802dot11-MIB	IEEE/IEEE802dot11-MIB.mib
IF-MIB	Standard/rfc2863-IF-MIB.mib
IGMP-MIB	Vendor/Cisco/IGMP-MIB.my
IGMP-STD-MIB	Vendor/Cisco/IGMP-STD-MIB.my
INET-ADDRESS-MIB	Standard/rfc4001-INET-ADDRESS-MIB.mib
INTEGRATED-SERVICES-MIB	Standard/rfc2213-INTEGRATED-SERVICES-MIB.mib
IP-FORWARD-MIB	Standard/rfc4292-IP-FORWARD-MIB.mib
IP-MIB	Standard/rfc4293-IP-MIB.mib
IPMCAST-MIB	Standard/rfc5132-IPMCAST-MIB.mib

MIB name	MIB file
IPMROUTE-MIB	Vendor/Cisco/IPMROUTE-MIB.my
IPMROUTE-STD-MIB	Vendor/Cisco/IPMROUTE-STD-MIB.my
IPV6-FLOW-LABEL-MIB	Standard/rfc3595-IPV6-FLOW-LABEL-MIB.mib
IPV6-MIB	Standard/rfc2465-IPV6-MIB.mib
IPV6-TC	Standard/rfc2465-IPV6-TC.mib
ISDN-MIB	Standard/rfc2127-ISDN-MIB.mib
InternetServer-MIB	Vendor/Microsoft/inetsrv.mib
JUNIPER-CHASSIS-DEFINES-MIB	Vendor/Juniper/mib-jnx-chas-defines
JUNIPER-JS-IF-EXT-MIB	Vendor/Juniper/mib-jnx-js-if-ext
JUNIPER-JS-SMI	Vendor/Juniper/mib-jnx-js-smi
JUNIPER-MIB	Vendor/Juniper/mib-jnx-chassis
JUNIPER-SMI	Vendor/Juniper/mib-jnx-smi
JUNIPER-V1-TRAPS	Vendor/Juniper/v1_traps
JUNIPER-VPN-MIB	Vendor/Juniper/mib-jnx-vpn
Juniper-MIBs	Vendor/Juniper/Juniper-MIBs.mib
Juniper-UNI-SMI	Vendor/Juniper/Juniper-UNI-SMI.mib
LANGTAG-TC-MIB	Standard/rfc5131-LANGTAG-TC-MIB.mib
LLDP-MIB	IEEE/lldp.mib
LanMgr-Mib-II-MIB	Vendor/Microsoft/lmmib2.mib
MAU-MIB	Standard/rfc4836-MAU-MIB.mib
MGMD-STD-MIB	Standard/rfc5519-MGMD-STD-MIB.mib
MPLS-L3VPN-STD-MIB	Standard/rfc4382-MPLS-L3VPN-STD-MIB.mib
MPLS-LSR-MIB	Vendor/Cisco/MPLS-LSR-MIB.my
MPLS-LSR-STD-MIB	Standard/rfc3813-MPLS-LSR-STD-MIB.mib
MPLS-MIB	Vendor/Juniper/mib-jnx-mpls
MPLS-TC-STD-MIB	Standard/rfc3811-MPLS-TC-STD-MIB.mib
MPLS-TE-MIB	Vendor/Cisco/MPLS-TE-MIB.my
MPLS-TE-STD-MIB	Standard/rfc3812-MPLS-TE-STD-MIB.mib
MPLS-VPN-MIB	Vendor/Cisco/MPLS-VPN-MIB.my
MSDP-MIB	Vendor/Nortel/MSDP-MIB.mib
Nortel-Magellan-Passport-StandardTextualConventionsMIB	Vendor/Nortel/Nortel-Magellan-Passport-StandardTextualConventionsMIB.mib
Nortel-Magellan-Passport-TextualConventionsMIB	Vendor/Nortel/Nortel-Magellan-Passport-TextualConventionsMIB.mib
Nortel-Magellan-Passport-UsefulDefinitionsMIB	Vendor/Nortel/Nortel-Magellan-Passport-UsefulDefinitionsMIB.mib

MIB name	MIB file
Nortel-MsCarrier-MscPassport-StandardTextualConventionsMIB	Vendor/Nortel/Nortel-MsCarrier-MscPassport-StandardTextualConventionsMIB.mib
Nortel-MsCarrier-MscPassport-TextualConventionsMIB	Vendor/Nortel/Nortel-MsCarrier-MscPassport-TextualConventionsMIB.mib
Nortel-MsCarrier-MscPassport-UsefulDefinitionsMIB	Vendor/Nortel/Nortel-MsCarrier-MscPassport-UsefulDefinitionsMIB.mib
OLD-CISCO-CHASSIS-MIB	Vendor/Cisco/OLD-CISCO-CHASSIS-MIB.my
OLD-CISCO-INTERFACES-MIB	Vendor/Cisco/OLD-CISCO-INTERFACES-MIB.my
OLD-CISCO-SYS-MIB	Vendor/Cisco/OLD-CISCO-SYS-MIB.my
OSPF-MIB	Standard/rfc4750-OSPF-MIB.mib
P-BRIDGE-MIB	Standard/rfc4363-P-BRIDGE-MIB.mib
PIM-MIB	Vendor/Cisco/PIM-MIB.my
PIM-STD-MIB	Standard/rfc5060-PIM-STD-MIB.mib
POWER-ETHERNET-MIB	Standard/rfc3621-POWER-ETHERNET-MIB.mib
PerfHist-TC-MIB	Standard/rfc3593-PerfHist-TC-MIB.mib
Q-BRIDGE-MIB	Standard/rfc4363-Q-BRIDGE-MIB.mib
RAPID-CITY	Vendor/Nortel/RAPID-CITY.mib
RFC-1212#	NNM/server/lib/nms-mib-model.jar/com/hp/ov/nms/mib/model/hibernate/rfc1212-RFC1212.mib
RFC-1215	Standard/rfc1215-RFC1215.mib
RFC1155-SMI#	NNM/server/lib/nms-mib-model.jar/com/hp/ov/nms/mib/model/hibernate/rfc1155-RFC1155-SMI.mib
RFC1213-MIB#	NNM/server/lib/nms-mib-model.jar/com/hp/ov/nms/mib/model/hibernate/rfc1213-RFC1213-MIB.mib
RFC1253-MIB	Vendor/OTHER-VENDORS/RFC1253-MIB.my
RFC1271-MIB#	NNM/server/lib/nms-mib-model.jar/com/hp/ov/nms/mib/model/hibernate/rfc1271-RFC1271-MIB.mib
RFC1315-MIB	Standard/rfc1315-RFC1315-MIB.mib
RIPv2-MIB	Standard/rfc1724-RIPv2-MIB.mib
RMON-MIB	Standard/rfc2819-RMON-MIB.mib
RMON2-MIB	Standard/rfc4502-RMON2-MIB.mib
RS-232-MIB	Standard/rfc1659-RS-232-MIB.mib
SMON-MIB	Standard/rfc2613-SMON-MIB.mib
SNMP-FRAMEWORK-MIB	Standard/rfc3411-SNMP-FRAMEWORK-MIB.mib
SNMP-REPEATER-MIB	Standard/rfc2108-SNMP-REPEATER-MIB.mib
SNMP-TARGET-MIB	Standard/rfc3413-SNMP-TARGET-MIB.mib
SNMP-VIEW-BASED-ACM-MIB	Standard/rfc3415-SNMP-VIEW-BASED-ACM-MIB.mib

MIB name	MIB file
SNMPv2-CONF#	NNM/server/lib/nms-mib-model.jar/com/hp/ov/nms/mib/model/hibernate/rfc1904-SNMPv2-CONF.mib
SNMPv2-MIB#	NNM/server/lib/nms-mib-model.jar/com/hp/ov/nms/mib/model/hibernate/rfc3418-SNMPv2-MIB.mib
SNMPv2-SMI#	NNM/server/lib/nms-mib-model.jar/com/hp/ov/nms/mib/model/hibernate/rfc2578-SNMPv2-SMI.mib
SNMPv2-TC#	NNM/server/lib/nms-mib-model.jar/com/hp/ov/nms/mib/model/hibernate/rfc2579-SNMPv2-TC.mib
SONET-MIB	Standard/rfc3592-SONET-MIB.mib
TOKEN-RING-RMON-MIB	Standard/Historic/rfc1513-TOKEN-RING-RMON-MIB.mib
TRANSPORT-ADDRESS-MIB	Standard/rfc3419-TRANSPORT-ADDRESS-MIB.mib
TUNNEL-MIB	Standard/rfc4087-TUNNEL-MIB.mib
VMWARE-AGENTCAP-MIB	Vendor/VMware/VMWARE-AGENTCAP-MIB.mib
VMWARE-ENV-MIB	Vendor/VMware/VMWARE-ENV-MIB.mib
VMWARE-OBSOLETE-MIB	Vendor/VMware/VMWARE-OBSOLETE-MIB.mib
VMWARE-PRODUCTS-MIB	Vendor/VMware/VMWARE-PRODUCTS-MIB.mib
VMWARE-RESOURCES-MIB	Vendor/VMware/VMWARE-RESOURCES-MIB.mib
VMWARE-ROOT-MIB	Vendor/VMware/VMWARE-ROOT-MIB.mib
VMWARE-SYSTEM-MIB	Vendor/VMware/VMWARE-SYSTEM-MIB.mib
VMWARE-TC-MIB	Vendor/VMware/VMWARE-TC-MIB.mib
VMWARE-VC-EVENT-MIB	Vendor/VMware/VMWARE-VC-EVENT-MIB.mib
VMWARE-VMINFO-MIB	Vendor/VMware/VMWARE-VMINFO-MIB.mib
VPN-TC-STD-MIB	Standard/rfc4265-VPN-TC-STD-MIB.mib
VRRP-MIB	Standard/rfc2787-VRRP-MIB.mib
WINDOWS-NT-PERFORMANCE	Vendor/Microsoft/WINDOWS-NT-PERFORMANCE.mib
WINS-MIB	Vendor/Microsoft/wins.mib
X-DDI-MIB	Vendor/Nortel/x-ddi-adapter-mib
XYLAN-BASE-MIB	Vendor/OTHER-VENDORS/XYLAN-BASE-MIB.mib
XYLAN-HEALTH-MIB	Vendor/OTHER-VENDORS/XYLAN-HEALTH-MIB.mib
cmSmsAgt	Vendor/OTHER-VENDORS/hitachi-cometAgtEx-winNT
cometAgt	Vendor/OTHER-VENDORS/hitachi-cometAgt
cometAgtEx	Vendor/OTHER-VENDORS/hitachi-cometAgtEx-winNT
windowsNTAgt	Vendor/OTHER-VENDORS/hitachi-cometAgt-winNT

#: Some MIB files are contained in JAR files. The MIB files in the table are relative paths within the JAR files shown below.

Windows

```
%NnmInstallDir%NNM\server\lib\nms-mib-model.jar
```

UNIX

```
$NnmInstallDir/NNM/server/lib/nms-mib-model.jar
```

D. Version Changes

D.1 Changes from version 10-10 to version 10-50

- The following OSs are now supported:
  - Microsoft(R) Windows Server(R) 2012 R2 Datacenter
  - Microsoft(R) Windows Server(R) 2012 R2 Standard
- Because it is not possible in Windows Server 2008 and later to log in to a console session from a remote desktop, the associated descriptions were removed.
- The description of the NNMi management server preinstallation checklist was changed.
- The following item was added under *Installing NNMi (Windows)*:
  - Confirmation of whether to perform the preinstallation checks and continue the installation
- The following item was added under *Installing NNMi (UNIX)*:
  - Confirmation of whether to perform the preinstallation checks and continue the installation
- The following items were added as tasks to be performed after installing NNMi:
  - Set the language environment (UNIX only)
  - Check the maximum Java heap size
- The steps listed under *Specifying disk drive security settings (Windows)* were changed.
- The following MIBs were added to the list of MIBs that are read during a new installation:
  - AX-BOOTMANAGEMENT-MIB
  - AX-DEVICE-MIB
  - AX-FLOW-MIB
  - AX-LOGIN-MIB
  - AX-NOTIFICATION
  - AX-OSPF-MIB
  - AX-OSPFV3-MIB
  - AX-QUEUE-MIB
  - AX-SMI-MIB
  - AX-STATS-MIB
  - AX-SYSTEM-MIB
  - AX-VRF-MIB

D.2 Changes from version 10-00 to version 10-10

- Descriptions for Windows Server 2012 were added.
- Notes about using network address translation (NAT) for discovering nodes were added.
- Changes were made to the Quick Start Configuration Wizard window and its description.

- The description of uninstalling NNMi was changed.
- Changes were made to the NNMi Help window and the **Communication Configuration** form.
- Changes and additions were made to the description of disk drive security settings for Windows.
- The descriptions of the settings and procedures for enabling Web browsers were changed.
- Additions and changes were made to the description of installing required libraries in Linux.
- Information about the following installation problem was added:
  - A message is displayed during installation indicating that the preinstallation procedure (phase II) has failed and the `/tmp/nnm_preinstall_phaseII.log` file needs to be checked for the details.
- Additions and changes were made to the list of MIBs read during a new installation.

E. Reference Material for This Manual

This appendix provides reference information, including various conventions, for this manual.

E.1 Related publications

This manual is part of a related set of manuals. The manuals in the set are listed below (with the manual numbers):

- *Job Management Partner 1 Version 10 Job Management Partner 1/Consolidated Management 2/Network Node Manager i Setup Guide* (3021-3-343-10(E))

E.2 Conventions: Abbreviations for product names

This manual uses the abbreviations listed below for Hitachi product names and for the names of products from other companies. The following table lists the naming convention used in this manual along with the full name of each product:

Abbreviation		Full name or meaning
Firefox		Firefox(R)
HP-UX	HP-UX (IPF)	HP-UX 11i V3 (IPF)
Linux	Linux 6	Red Hat Enterprise Linux(R) Server 6 (64-bit x86_64)
NNMi	NNMi	Job Management Partner 1/Consolidated Management 2/Network Node Manager i
	NNMi Advanced	Job Management Partner 1/Consolidated Management 2/Network Node Manager i Advanced
Solaris		Solaris 10 (SPARC)

HP-UX, Linux, and Solaris are often referred to collectively as *UNIX*.

E.3 Conventions: Acronyms

This manual also uses the following acronyms:

Acronym	Full name or meaning
ARP	Address Resolution Protocol
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IPF	Itanium(R) Processor Family
MIB	Management Information Base
NFS	Network File System

Acronym	Full name or meaning
SNMP	Simple Network Management Protocol
VLAN	Virtual LAN

E.4 Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

- 1 KB (kilobyte) is 1,024 bytes.
- 1 MB (megabyte) is $1{,}024^2$ bytes.
- 1 GB (gigabyte) is $1{,}024^3$ bytes.
- 1 TB (terabyte) is $1{,}024^4$ bytes.

F. Glossary

account

See *user account*.

application failover

In NNMi, an optional capability that transfers control of NNMi processes to a standby server when the currently active server fails. This optional capability, which must be configured by the user, utilizes JBoss clustering support.

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*.

community string

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

console

See *NNMi console*.

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*.

global manager

The NNMi management server in a Global Network Management deployment that consolidates data from distributed NNMi regional manager servers. The global manager provides a unified view of topology and incidents across the whole environment. A global manager must have an NNMi Advanced license.

Global Network Management

A distributed deployment of NNMi with one or more global managers consolidating data from one or more geographically distributed regional managers.

high availability

Used in this guide to refer to a hardware and software configuration that provides for uninterrupted service if part of the configuration fails. High availability (HA) means that the configuration has redundant components to keep applications running at all times even if a component fails. NNMi can be configured to support one of several commercially available HA solutions. Contrast with *application failover*.

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 also reported through incident views.

JBoss Application Server

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

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 quality of service, knowing the address of the neighboring nodes in the network, and selecting routes. It also recognizes and forwards incoming messages for local host domains. Everything in a subnet is connected at the Layer 3 (IP) level.

NNMi

An abbreviation for Job Management Partner 1/Consolidated Management 2/Network Node Manager i and Job Management Partner 1/Consolidated Management 2/Network Node Manager i Advanced.

NNMi is a software product designed to aid network administration and consolidate network management activities. Activities include the ongoing discovery of network nodes, monitoring of events, and providing network fault management. See also *NNMi console*.

NNMi console

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

NNMi management server

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

node

In the network context, a computer system or device (for example, a printer, router, or bridge) in a network.

ovstart command

A command that starts the NNMi managed processes. For details, see **Help** > **NNMi Documentation Library** > **Reference Pages** (in NNMi Help).

ovstatus command

A command that reports the current status of the NNMi managed processes. For details, see **Help** > **NNMi Documentation Library** > **Reference Pages** (in NNMi Help).

ovstop command

A command that stops the NNMi managed processes. For details, see **Help** > **NNMi Documentation Library** > **Reference Pages** (in NNMi Help).

port

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

Quick Start Configuration Wizard

The Quick Start Configuration Wizard automatically runs immediately after NNMi installation finishes. Use the Quick Start Configuration Wizard to provide the read community strings for your SNMPv1 or SNMPv2c environment, set limits to the range of discovered nodes, or set up an administrator account.

Root Cause Analysis (RCA)

A problem solving function for identifying the root causes of network incidents. NNMi considers an incident to have occurred when the NNMi root cause analysis (RCA) engine evaluates a reported problem.

rule

See *discovery rule*.

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 the environment to be monitored. 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*.

Simple Network Management Protocol (SNMP)

The 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 system account is a special account provided for use during NNMi installation. After installation finishes, the system account is used only for command line security or restoration purposes. See also *user account*.

topology (network)

In communication networks, a schematic description of the arrangement of a network, including its nodes and connections.

trap

See *SNMP trap*.

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, Operator Level 2, Operator Level 1, Guest.

See also *user account*.

Index

S

T

U

W