HP Automated Network Management

Solution Version: 9.10

Configuration Guide

Document Release Date: June 2011

Software Release Date: June 2011

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Adobe is a trademark of Adobe Systems Incorporated.

AMD is a trademark of Advanced Micro Devices, Inc.

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

Intel, Itanium, and Intel Xeon are trademarks of Intel Corporation in the U.S. and other countries.

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

Oracle is a registered trademark of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group.

Documentation Updates

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

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

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

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

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

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

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

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

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport user ID, go to:

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

To find more information about access levels, go to:

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

Contents

1 ANM Requirements

This chapter describes the hardware and software prerequisites for ANM.

Supported Product Versions

Table 1 lists the software products and versions that comprise ANM 9.10. Table 2 lists the additional software products and versions enabled by the purchase of ANM Advanced 9.10.

Table 1 ANM Products

Product Name	Product Abbreviation	Version
HP Network Node Manager i Software	NNMi	9.10 with hot fix QCCR1B88988 or the latest consolidated patch
HP Network Automation	NA	9.10 with hot fix NAS9.10_89861 or the latest consolidated patch
HP Network Node Manager iSPI Performance for Quality Assurance Software	NNM iSPI Performance for QA	9.10
NNM iSPI Network Engineering Toolset Software	NNM iSPI NET	9.10
HP Network Node Manager iSPI Performance for Metrics Software	NNM iSPI Performance for Metrics	9.10
HP Network Node Manager iSPI Performance for Traffic Software	NNM iSPI Performance for Traffic	9.10

Table 2 ANM Advanced Optional Additional Integrated Products

Product Name	Product Abbreviation	Version
HP Network Node Manager iSPI for MPLS Software	NNM iSPI for MPLS	9.10
HP Network Node Manager iSPI for IP Multicast Software	NNM iSPI for IP Multicast	9.10
HP Network Node Manager iSPI for IP Telephony Software	NNM iSPI for IP Telephony	9.10

Example Deployment Architecture

Figure 1 shows the example deployment architecture for ANM. The instructions in this document support this architecture. This architecture is based on the following assumptions:

- Each product that requires a database uses the embedded database available with that product.
- All servers are on the same network segment without firewalls between servers. Having a firewall between the solution servers affects product performance.
- The network includes supported network devices.
- The network includes devices running a supported flow technology and devices with embedded IP SLA capabilities.

Figure 1 Example ANM Deployment Architecture

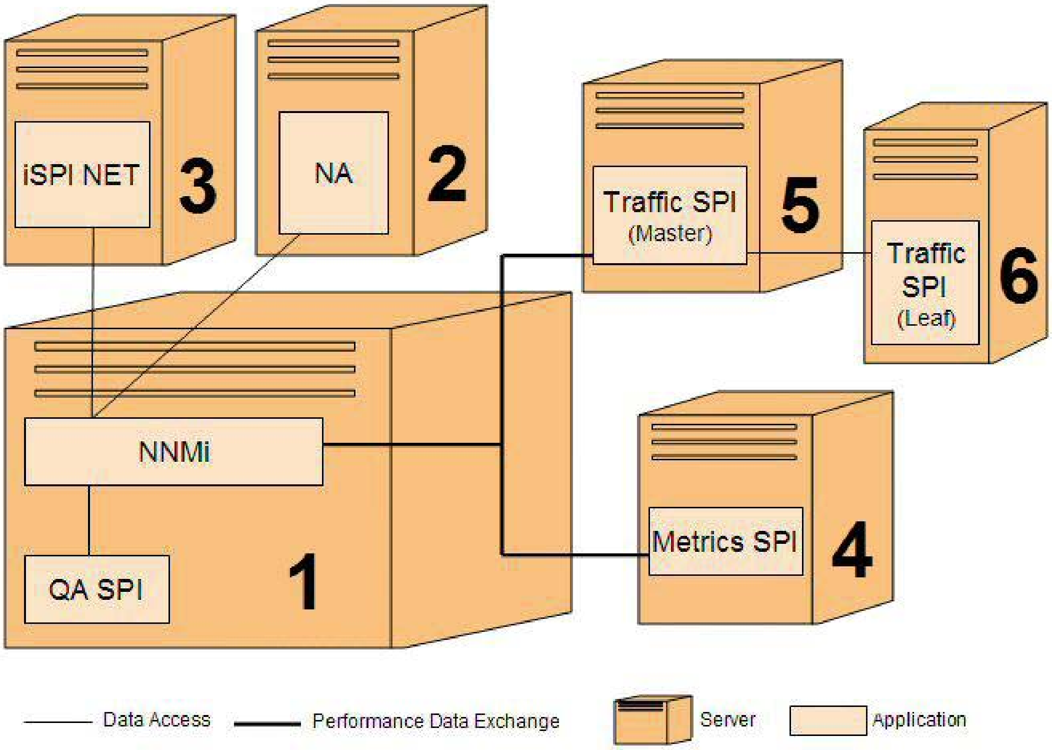

Table 3 lists the servers included in the example deployment architecture.

Table 3 Example Deployment Servers

Server Number	Installed Software
1	• NNMi • NNM iSPI Performance for QA • NNM iSPI Performance for Traffic extensions • ANM Advanced optional integrated products: — NNM iSPI for MPLS — NNM iSPI for IP Multicast — NNM iSPI for IP Telephony
2	• NA
3	• NNM iSPI NET
4	• Network Performance Server (NPS) used by all of the NNM Performance iSPIs • NNM iSPI Performance for Metrics
5	• NNM iSPI Performance for Traffic master collector
6	• NNM iSPI Performance for Traffic leaf collector

Hardware and Software Requirements

This section consolidates the information from the product support matrices for a medium-sized network with the following parameters:

- 3,000 to 8,000 managed devices
- Up to 60,000 performance polled interfaces polled at five minute intervals
- 30,000 configured QA probes
- 2,000 to 4,000 flow records per second sent to the NNM iSPI Performance for Traffic master collector
- 2,000 to 3,000 flow records per second sent to the NNM iSPI Performance for Traffic leaf collector

The stated requirements are for physical systems. For additional information, including requirements for virtual systems, non-embedded databases, and different environment sizes, see the product support matrices, which are available from the HP manuals web site as described in Product Documentation on page 17.

If there are discrepancies between the requirements listed in this chapter and those listed in the individual product support matrices, follow the information in the product support matrices.

The ANM servers need not be homogenous. With a few exceptions noted in this chapter, each server may be any of the supported types for that software.

This section describes the requirements for the following systems:

- Web Browser and Software for Clients and all Solution Servers on page 10
- Server 1 (NNMi, NNM iSPI Performance for QA, and NNM iSPI Performance for Traffic extensions) on page 11
- Server 2 (NA) on page 12
- Server 3 (NNM iSPI NET) on page 13
- Server 4 (NPS and NNM iSPI Performance for Metrics) on page 13
- Server 5 (NNM iSPI Performance for Traffic Master Collector) on page 15
- Server 6 (NNM iSPI Performance for Traffic Leaf Collector) on page 15

Web Browser and Software for Clients and all Solution Servers

Table 4 lists the web browser requirements and additional software required to use certain ANM features.

Table 4 Web Browser and Software Requirements for Using ANM

Purpose	Requirements
Run the NNMi console, the NA console, and the NPS console	One of: • Microsoft® Internet Explorer version 8 (not running in Compatibility View mode) • Mozilla Firefox version 3.6.13 or later minor version through 3.x
View NNMi graphs and the NNMi MIB browser	• Adobe® Flash Player Plug-in version 10.1053.64 or later
View NA summary reports	• Microsoft Excel 2000 or later
View exported map files	One of: • Microsoft Visio 2007 • Microsoft Visio 2010

Each web browser that will be used to run any of the ANM consoles must be configured as follows:

- Disable all pop-up window blockers.
- Enable cookies.
- Enable JavaScript.
- Set Internet Explorer to enable VML.
- Set Firefox to open new windows as separate windows, not tabs.
- Set the display resolution to at least 1024 x 768.

Server 1 (NNMi, NNM iSPI Performance for QA, and NNM iSPI Performance for Traffic extensions)

Table 5 lists the combined requirements for the following software to be installed on server 1:

- NNMi
- NNM iSPI Performance for QA
- NNM iSPI Performance for Traffic extensions

Table 5 ANM Server 1 Requirements

Area	Minimum Requirements
Hardware	• System: — Microsoft Windows® or Linux: Intel® 64-bit (x86-64) or AMD 64-bit (AMD64) x 4 CPU Cores — HP-UX: Intel Itanium® Processor Family — Solaris: UltraSPARC IIIi, or IV, or IV+; or SPARC64 V, or V+ or VI, or VII (M-class) • RAM: 20GB for NNMi and NNM iSPI Performance for QA combined • Virtual Memory: Double the amount of RAM • Disk space for installation and operation: 200GB for NNMi and NNM iSPI Performance for QA combined Recommended that free space be on a different drive than the operating system. **NOTE**: The NNM iSPI for IP Multicast, NNM iSPI for IP Telephony, and NNM iSPI for MPLS must be co-resident with NNMi. If you plan to install any of these NNM iSPIs, increase the server 1 requirements as follows: 1 From the support matrix of each additional NNM iSPI, determine the following values: — Number of CPU cores — RAM — Disk space for installation and runtime 2 Add these values to the values listed in Table 5. The available virtual memory should be double the total RAM requirement for all installed products. For information about downloading the product support matrices, see Product Documentation on page 17.

Table 5 ANM Server 1 Requirements

Area	Minimum Requirements
Operating System	**NOTE**: If the NNMi management server (server 1) runs on a Windows operating system, the NPS server (server 4) also *must* run on a Windows operating system. • Windows: — Windows Server 2008 x64 Datacenter Edition with Service Pack 2 — Windows Server 2008 R2 x64 Datacenter Edition — Windows Server 2008 x64 Enterprise Edition with Service Pack 2 — Windows Server 2008 R2 x64 Enterprise Edition — Windows Server 2008 x64 Standard Edition with Service Pack 2 — Windows Server 2008 R2 x64 Standard Edition • HP-UX: HP-UX 11i v3 • Linux: — Red Hat Enterprise Server AS 5.2 (or later minor version through 5.x) — Red Hat Enterprise Server ES 5.2 (or later minor version through 5.x) • Solaris: Oracle Solaris 10 SPARC

Server 2 (NA)

Table 6 lists the requirements for NA to be installed on server 2.

Table 6 ANM Server 2 Requirements

Area	Minimum Requirements
Hardware	• System: — Windows or Linux: Intel Xeon® or equivalent, 3.0+GHz x 4 CPU Cores — Solaris: Dual UltraSPARC IIIi+, 1.3GHz • RAM: 8GB • Virtual Memory: Double the amount of RAM • Disk space for installation and operation: 140GB Recommended that free space be on a different drive than the operating system.
Operating System	• Windows: Windows Server 2008 R2 x64 with Service Pack 1 **NOTE**: Windows Server 2003 is not supported for new installations. • Linux: — Red Hat RHEL Server 5 — SUSE Linux Enterprise Server 10 • Solaris: Oracle Solaris 10 SPARC
Perl	• To use the Perl SDK: — Windows: ActivePerl 5.8.x — Linux or Solaris: Perl 5.8.x • To use the NA connect module with SSH: Perl Net::SSH::Expect module

Server 3 (NNM iSPI NET)

Table 7 lists the requirements for NNM iSPI NET to be installed on server 3.

Table 7 ANM Server 3 Requirements

Area	Minimum Requirements
Hardware	• System: — Windows: Intel 64-bit (x86-64) or AMD 64-bit (AMD64) x 4 CPU Cores • RAM: 4GB • Disk space for installation and operation: 2GB Recommended that free space be on a different drive than the operating system.
Operating System	• Windows: — Windows Server 2008 x64 Datacenter Edition with Service Pack 2 — Windows Server 2008 R2 x64 Datacenter Edition — Windows Server 2008 x64 Enterprise Edition with Service Pack 2 — Windows Server 2008 R2 x64 Enterprise Edition — Windows Server 2008 x64 Standard Edition with Service Pack 2 — Windows Server 2008 R2 x64 Standard Edition

Server 4 (NPS and NNM iSPI Performance for Metrics)

Table 8 lists the combined requirements for the following software to be installed on server 4:

- NPS
- NNM iSPI Performance for Metrics extension pack
- NNM iSPI Performance for QA extension pack
- NNM iSPI Performance for Traffic extension pack

Table 8 ANM Server 4 Requirements

Area	Minimum Requirements
Hardware	• System: — Windows or Linux: Intel 64-bit (x86-64) or AMD 64-bit (AMD64) x 12 CPU Cores • RAM: 72GB for NPS, NNM iSPI Performance for Metrics, NNM iSPI Performance for QA, and NNM iSPI Performance for Traffic combinedVirtual Memory: Double the amount of RAM • Disk space for installation and operation: 6TB for NPS, NNM iSPI Performance for Metrics, NNM iSPI Performance for QA, and NNM iSPI Performance for Traffic combined Recommended that free space be on a different drive than the operating system. **NOTE**: This requirement is for the minimum retention period. For longer retention periods, increase the operational disk space. **NOTE**: The NNM iSPI for IP Multicast, NNM iSPI for IP Telephony, and NNM iSPI for MPLS must be co-resident with NNMi. If you plan to install any of these NNM iSPIs, increase the server 4 requirements as follows: 1 From the support matrix of each additional NNM iSPI, determine the disk space requirement for report data. 2 Add this values to the disk space value listed in Table 8. The available virtual memory should be double the total RAM requirement for all installed products. For information about downloading the product support matrices, see Product Documentation on page 17.
Operating System	**NOTE**: If the NNMi management server (server 1) runs on a Windows operating system, the NPS server (server 4) also *must* run on a Windows operating system. • Windows: — Windows Server 2008 x64 Datacenter Edition with Service Pack 2 — Windows Server 2008 R2 x64 Datacenter Edition — Windows Server 2008 x64 Enterprise Edition with Service Pack 2 — Windows Server 2008 R2 x64 Enterprise Edition — Windows Server 2008 x64 Standard Edition with Service Pack 2 — Windows Server 2008 R2 x64 Standard Edition • Linux: — Red Hat Enterprise Server AS 5.3 (or later minor version through 5.x) — Red Hat Enterprise Server ES 5.3 (or later minor version through 5.x)

Server 5 (NNM iSPI Performance for Traffic Master Collector)

Table 9 lists the requirements for the NNM iSPI Performance for Traffic master collector to be installed on server 5.

Table 9 ANM Server 5 Requirements

Area	Minimum Requirements
Hardware	• System: — Windows or Linux: Intel 64-bit (x86-64) or AMD 64-bit (AMD64) x 4 CPU Cores • RAM: 8GB • Virtual Memory: Double the amount of RAM • Disk space for installation and operation: 800MB Recommended that free space be on a different drive than the operating system.
Operating System	**NOTE**: Recommended that the NNM iSPI Performance for Traffic master collector and the NNM iSPI Performance for Traffic leaf collector run on the same operating system. • Windows: — Windows Server 2008 x64 Datacenter Edition with Service Pack 2 — Windows Server 2008 R2 x64 Datacenter Edition — Windows Server 2008 x64 Enterprise Edition with Service Pack 2 — Windows Server 2008 R2 x64 Enterprise Edition — Windows Server 2008 x64 Standard Edition with Service Pack 2 — Windows Server 2008 R2 x64 Standard Edition • Linux: — Red Hat Enterprise Server AS 5.2 (or later minor version through 5.x) — Red Hat Enterprise Server ES 5.2 (or later minor version through 5.x)

Server 6 (NNM iSPI Performance for Traffic Leaf Collector)

Table 10 lists the requirements for the NNM iSPI Performance for Traffic leaf collector to be installed on server 6.

Table 10 ANM Server 6 Requirements

Area	Minimum Requirements
Hardware	• System: — Windows or Linux: Intel 64-bit (x86-64) or AMD 64-bit (AMD64) x 4 CPU Cores • RAM: 8GB • Virtual Memory: Double the amount of RAM • Disk space for installation and operation: 800MB Recommended that free space be on a different drive than the operating system.

Table 10 ANM Server 6 Requirements

Area	Minimum Requirements
Operating System	**NOTE**: Recommended that the NNM iSPI Performance for Traffic master collector and the NNM iSPI Performance for Traffic leaf collector run on the same operating system. • Windows: — Windows Server 2008 x64 Datacenter Edition with Service Pack 2 — Windows Server 2008 R2 x64 Datacenter Edition — Windows Server 2008 x64 Enterprise Edition with Service Pack 2 — Windows Server 2008 R2 x64 Enterprise Edition — Windows Server 2008 x64 Standard Edition with Service Pack 2 — Windows Server 2008 R2 x64 Standard Edition • Linux: — Red Hat Enterprise Server AS 5.2 (or later minor version through 5.x) — Red Hat Enterprise Server ES 5.2 (or later minor version through 5.x)

Product Documentation

The complete documentation set for each ANM product is available on the HP Product Manuals web site at **h20230.www2.hp.com/selfsolve/manuals**. Use your HP Passport account to access this site, or register a new HP Passport identifier.

Table 11 lists the search category for each ANM product. To locate documentation for a given product, choose the product name from Table 11, choose product version `9.10`, and then choose the operating system. Select the version of the document that matches the software version (for example, 9.10 Patch 1) you are using.

➤ To view files in PDF format (.pdf), Adobe Reader must be installed on your system. To download Adobe Reader, visit the Adobe web site at www.adobe.com.

Table 11 Documentation Search Categories on the HP Manuals Web Site

Product	Search Category	Referenced Documents
NNMi	network node manager	• *HP Network Node Manager i Software System and Device Support Matrix* • *HP Network Node Manager i Software Installation Guide* • *HP Network Node Manager i Software Deployment Reference*
NA	network automation	• *HP Network Automation Support Matrix* • *HP Network Automation Upgrade and Installation Guide* • *HP Network Automation User's Guide*
NNM iSPI Performance for QA	network node manager iSPI Performance for QA	• *HP Network Node Manager iSPI Performance for Quality Assurance System and Device Support Matrix* • *HP Network Node Manager iSPI Performance for Quality Assurance Software Installation Guide* • *HP Network Node Manager iSPI Performance for Quality Assurance Software Release Notes* • *HP Network Node Manager iSPI Performance for Quality Assurance Software Deployment Reference*
NNM iSPI NET	network node manager iSPI for NET	• *HP Network Node Manager iSPI Network Engineering Toolset Diagnostics Server System and Device Support Matrix* • *HP NNM iSPI Network Engineering Toolset Software Planning and Installation Guide*
NNM iSPI Performance for Metrics	network node manager iSPI Performance for Metrics	• *HP Network Node Manager i Software Smart Plug-in Performance for Metrics/ Network Performance Server System and Device Support Matrix* • *HP Network Node Manager iSPI Performance for Metrics Software Installation Guide*

Table 11 Documentation Search Categories on the HP Manuals Web Site

Product	Search Category	Referenced Documents
NNM iSPI Performance for Traffic	network node manager iSPI Performance for Traffic	• *HP Network Node Manager iSPI Performance for Traffic Software System and Device Support Matrix* • *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide* • *HP Network Node Manager iSPI Performance for Traffic Software Deployment Reference*
NNM iSPI for MPLS	network node manager SPI for MPLS VPN	• *HP Network Node Manager iSPI for MPLS Software System and Device Support Matrix* • *HP Network Node Manager iSPI for MPLS Software*
NNM iSPI for IP Multicast	network node manager SPI for IP multicast	• *HP Network Node Manager iSPI for IP Multicast Software System and Device Support Matrix* • *HP Network Node Manager iSPI for IP Multicast Software Installation Guide*
NNM iSPI for IP Telephony	network node manager SPI for IP telephony	• *HP Network Node Manager iSPI for IP Telephony Software System and Device Support Matrix* • *HP Network Node Manager iSPI for IP Telephony Software Installation Guide*

2 Configuring ANM

This chapter outlines the process for installing and configuring ANM.

For a new installation, complete all procedures in the following sections:

- Install and Configure ANM on page 19
- Verify the HP NNMi–HP NA Integration on page 23
- License ANM on page 24

For an upgrade from ANM 9.00, complete all procedures in the following sections:

- Upgrade from ANM 9.00 on page 25
- Verify the HP NNMi–HP NA Integration on page 23

Install and Configure ANM

This section outlines the procedure for installing and configuring ANM for the example deployment architecture. For additional information, see the product documentation, which is available from the HP manuals web site as described in Product Documentation on page 17.

Note the following:

- It is recommended to run ANM in a test lab before deploying the solution to production.
- For assistance configuring ANM for your specific environment, contact the HP Professional Services Organization.
- Perform all configuration steps using administrator access to the ANM products.
- Single sign-on among the ANM products provides for moving from one console to another without repeatedly logging on. During the ANM configuration process, the administrator must log on to NNMi and NA separately.
- Anti-virus and backup software can interfere with the products' operation if the software locks files while the products are running. Any application that locks files should be configured to exclude the installation and data directories (selected during the installation process).
- Windows 2008 includes the concept of User Access Control (UAC). Users who are part of the Administrator group may not have full Administrator privileges. All scripts and commands associated with the products detect and warn if the user is not enabled. Scripts and commands must be run with full Administrator access. To achieve full Administrator access, right-click the **Command Tool** icon, and then click **Run as Administrator**.

Prepare a Web Browser for Client Systems and All Solution Servers

On each ANM server and client, configure a supported web browser as described in "Enabling the Web Browser for the NNMi Console" in the *HP Network Node Manager i Software Installation Guide*.

To take advantage of single sign-on among the ANM products, always start the NNMi console with a URL that includes the fully-qualified domain name of the NNMi management server.

Install and Configure NNMi (Server 1)

Install NNMi before installing any of the other ANM products.

To install and configure NNMi, follow these steps:

1. Verify that server 1 meets the requirements listed in Table 5 on page 11.
2. Prepare the server 1 as described in "Installation Prerequisites" for the server operating system type in the *HP Network Node Manager i Software System and Device Support Matrix*.
3. On server 1, install NNMi as described in the *HP Network Node Manager i Software Installation Guide*.
4. Install the required hot fix (identified in Table 1 on page 7) or the latest consolidated patch.
5. Configure NNMi with the access credentials and appropriate timeout and retry values for different devices and areas of your network. For information, see *Configuring Communication Protocol* in the NNMi help.
6. Configure NNMi discovery. For information, see *Configure Discovery* in the NNMi help.
7. Enable single sign-on for NNMi as described in "Enabling SSO for a Single Domain" in the *HP Network Node Manager i Software Deployment Reference*.
8. Create two NNMi users with the Web Service Client role:
   - One NNMi user for NNM iSPI Performance for QA.
   - One NNMi user for NNM iSPI Performance for Traffic.

   For information, see *Configuring Security* in the NNMi help.

Install and Configure NPS and NNM iSPI Performance for Metrics (Server 4)

Prerequisite: NNMi must be installed on server 1.

To install and configure NPS and NNM iSPI Performance for Metrics, follow these steps:

1. Verify that server 4 meets the requirements listed in Table 8 on page 14.
2. On the NNMi management server (server 1), run the NNM iSPI Performance for Metrics enablement script as described in "Running the Enablement Script" in the *HP Network Node Manager iSPI Performance for Metrics Software Installation Guide*.
3. On server 4, install NPS as described in the *HP Network Node Manager iSPI Performance for Metrics Software Installation Guide*.

   During the installation, select to install NNM iSPI Performance for Metrics also.

4 In the NNMi console, configure fault and performance polling. For information, see *Configure Monitoring Behavior* in the NNMi help.

Install and Configure NNM iSPI Performance for QA (Server 1)

Prerequisites:

- NNMi must be installed on server 1.
- NPS must be installed on server 4.

To install and configure NNM iSPI Performance for QA, follow these steps:

1. On the NNMi management server (server 1), install NNM iSPI Performance for QA as described in the *HP Network Node Manager iSPI Performance for Quality Assurance Software Installation Guide*.
2. On the NNMi management server (server 1), configure single sign-on between NNMi and NNM iSPI Performance for QA as described in the known problems section of the *HP Network Node Manager iSPI Performance for Quality Assurance Software Release Notes*.

   This configuration enables NNMi users with the Administrator role to open the Quality Assurance Configuration console without entering logon credentials.
3. In the NNMi console, discover existing QA probes, configure QA probes, and set thresholds on QA probes. For information, see the *HP Network Node Manager iSPI Performance for Quality Assurance Software Help for Administrators*.

Install the NNM iSPI Performance for Traffic Master Collector (Server 5)

Prerequisites:

- NNMi must be installed on server 1.
- NPS must be installed on server 4.

To install and configure the NNM iSPI Performance for Traffic master collector, follow these steps:

1. Verify that server 5 meets the requirements listed in Table 9 on page 15.
2. On the NNMi management server (server 1), complete the preinstallation tasks as described in “Planning for Installation” of the *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*.
3. On the NNMi management server (server 1), install the NNM iSPI Performance for Traffic extension as described in “Installing the HP NNMi Extension for iSPI Performance for Traffic” of the *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*.
4. On server 5, install the NNM iSPI Performance for Traffic master collector as described in “Installing the Master Collector” of the *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*.

Install and Configure the NNM iSPI Performance for Traffic Leaf Collector (Server 6)

Prerequisites:

- NNMi must be installed on server 1.
- NPS must be installed on server 4.
- The NNM iSPI Performance for Traffic master collector must be installed on server 5.

To install and configure the NNM iSPI Performance for Traffic leaf collector, follow these steps:

1. Verify that server 6 meets the requirements listed in Table 10 on page 15.
2. On server 6, install the NNM iSPI Performance for Traffic leaf collector as described in "Installing the Leaf Collector" of the *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*.
3. Configure the NNM iSPI Performance for Traffic master collector and leaf collector. For information, see "Post-Installation Tasks" and "Getting Started with the NNM iSPI Performance for Traffic" in the *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*.
4. In the NNMi console, configure traffic thresholds. For information, see the NNM iSPI Performance for Traffic help.
5. For flow-enabled interfaces, enable the flow protocol to send flow records to the NNM iSPI Performance for Traffic leaf collector.

Install and Configure NNM iSPI NET (Server 3)

Prerequisite: NNMi must be installed on server 1.

To install and configure NNM iSPI NET, follow these steps:

1. Verify that server 3 meets the requirements listed in Table 7 on page 13.
2. On server 3, install NNM iSPI NET as described in the *HP NNM iSPI Network Engineering Toolset Software Planning and Installation Guide*.
3. In the NNMi console, configure NNM iSPI NET diagnostics on one or more NNMi incidents. For information, see "NNM iSPI NET Diagnostics" in the *HP NNM iSPI Network Engineering Toolset Software Planning and Installation Guide*.

Install and Configure NA and the HP NNMi—HP NA integration (Server 2)

Prerequisite: NNMi must be installed on server 1.

To install and configure NA and the HP NNMi—HP NA integration, follow these steps:

1. Verify that server 2 meets the requirements listed in Table 6 on page 12.
2. Prepare the server 2 as described in "Hardware and Software Requirements" in the *HP Network Automation Support Matrix*.
3. On server 2, install NA as described in the *HP Network Automation Upgrade and Installation Guide*.

4. Install the required hot fix (identified in Table 1 on page 7) or the latest consolidated patch.
5. On server 2, install the most recent driver pack.
6. Configure NA device password rules. For information, see “Creating Device Password Rules” in the *HP Network Automation User’s Guide*.
7. Configure the HP NNMi—HP NA integration. For information, see “New Integration Configuration” in the *HP Network Node Manager i Software Deployment Reference*.
   - Be sure to configure single-sign on between NNMi and NA.
   - On the HP NNMi–HP NA Integration Configuration form, make the following selections:
     - — Leave **Topology Filter Node Group** unset so the integration will synchronize the entire NNMi topology with the NA inventory.
     - — Set **Topology Synchronization Interval (hrs)** to an non-zero value.
     - — Select the **Discover Device Drivers in NA** check box.
     - — Set **NA Connection Check Interval (hrs)** to a non-zero value.
8. Configure NA device configurations. For information, see “Managing Device Configurations” in the *HP Network Automation User’s Guide*.
9. Configure NA device policies. For information, see “Managing Policy Assurance” in the *HP Network Automation User’s Guide*.

Verify the HP NNMi–HP NA Integration

To verify that the HP NNMi—HP NA integration is correctly enabled, follow these steps:

1. Log on to the NNMi console as a user with the Administrator role.
2. In the NNMi console, verify that the NA SNMP trap incident configurations are in place:
   a. Open the SNMP Trap Configurations view (**Configuration > Incidents > SNMP Trap Configurations**).
   b. Locate the trap definitions for named **NASnmpTrapv1** and **NASnmpTrapv2**.
3. Log on to NA as a user with administrator privileges.
4. In the NA console, verify that the NA inventory matches the NNMi topology:
   a. In the menu at the top of the Home page, select **Devices > Inventory.**
   b. Confirm that all the devices listed in NNMi were imported to NA.
5. In the NA console, click **Admin > 3rd Party Integrations > NNM Integration Connection Test.**

   A success message appears.

   ➤ If an error message appears, confirm that you configured the integration correctly or contact your support representative.

License ANM

The permanent license keys for NNMi and the NNM iSPIs are tied to the IP address of the NNMi management server.

The permanent license key for NA is tied to the IP address of the NA server.

On the NNMi management server (server 1), install the following license keys on the NNMi management server:

- One or more NNMi license keys as needed to enable management of all nodes in your network. For instructions, see “Licensing NNMi” in the *HP Network Node Manager i Software Installation Guide*.
- One NNM iSPI NET license key. For instructions, see “License NNM iSPI NET” in the *HP NNM iSPI Network Engineering Toolset Software Planning and Installation Guide*.
- One or more NNM iSPI Performance for Metrics license keys as needed to enable performance reporting of all nodes in your network. For instructions, see “Licensing” in the *HP Network Node Manager iSPI Performance for Metrics Software Installation Guide*.
- One or more iSPI Points license key; this license key applies to all of the NNM iSPIs except for NNM iSPI NET and NNM iSPI Performance for Metrics. Ensure that you have enough iSPI points for your use of these NNM iSPIs. For information about how iSPI points accumulate and instructions on installing the license keys, see the following documentation:
  - “License Related Information” in the *HP Network Node Manager iSPI Performance for Quality Assurance Software Installation Guide*.
  - “Licensing” in the *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*.
- One Collector Connection Software LTU license key for each NNM iSPI Performance for Traffic leaf collector. For instructions, see “Licensing” in the *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*.

On the NA server (server 2), install one NA license key. For instructions, see “Obtaining a NA 9.1 License” and “Deploying NA License Information” in the *HP Network Automation Upgrade and Installation Guide*.

Upgrade from ANM 9.00

To upgrade from ANM 9.00 to ANM 9.10, follow these steps:

1. Upgrade NNMi to version 9.10 as described in “Upgrading from NNMi 9.0x” in the *HP Network Node Manager i Software Deployment Reference*.
2. Upgrade NNM iSPI Performance for Metrics to version 9.10 as described in “Upgrading the NNM iSPI Performance for Metrics” in the *HP Network Node Manager iSPI Performance for Metrics Software Installation Guide*.
3. Upgrade NNM iSPI Performance for QA as described in “Upgrading on a Windows or UNIX® Management Server” in the *HP Network Node Manager iSPI Performance for Quality Assurance Software Installation Guide*.
4. Upgrade NNM iSPI Performance for Traffic as described in “Upgrade the NNM iSPI Performance for Traffic 9.01 to 9.10” in the *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*.
5. If necessary, upgrade NNM iSPI NET as described in “Upgrade NNM iSPI NET” in the *HP NNM iSPI Network Engineering Toolset Software Planning and Installation Guide*.
6. Upgrade NA as described in “Upgrading to or Initially Installing NA 9.1” in the *HP Network Automation Upgrade and Installation Guide*.
7. Upgrade the HP NNMi—HP NA integration as described in “Integration Configuration Upgraded from NNMi 9.0x” in the *HP Network Node Manager i Software Deployment Reference*.

3 Configuring the ANM Example Scenarios

This chapter outlines the process for configuring the ANM example scenarios. It assumes that ANM is configured as described in Chapter 2, Configuring ANM.

It contains the following topics:

Scenario 1: Identify and correct an out-of-compliance device change

Incorrect device configuration is a common cause of network problems. ANM can monitor the network for devices with non-compliant configurations and can generate notifications when a device configuration is outside of this expected configuration. ANM provides tools for comparing the current device configuration to the previous device configuration and for resetting the device to use a previous configuration.

Scenario Prerequisites

- The device must be in the NNMi topology and the NA inventory.
- Configure the Device to Send syslog Messages to NA on page 28.
- An NA device configuration policy must be applied to the device.
- The ANM operator must have permission in NA to view and modify the device configuration.
- Customize the NA SNMP Trap Incidents on page 28.
- Set NA to Run the Check Policy Compliance Task When a Device Configuration Changes on page 28.
- Configure NA to Send SNMP Traps to NNMi When a Policy Compliance Check Fails on page 29.

Configure the Device to Send syslog Messages to NA

1. In the NA console, click **Tasks > New Task > Configure Syslog**.
2. On the New Task/Template –Configure Syslog page, do the following:
   a. Set *Applies to* to the device.
   b. Under Scheduling Options, set Recurring Options to Periodically, and then specify an appropriate interval.
   c. Click **Save**.

Customize the NA SNMP Trap Incidents

In the NNMi console, the NASnmpTrapv1 and NASnmpTrapv2 incident configurations convert the SNMP traps sent by NA into incidents that NNMi can display and process.

If you want all traps sent by NA to NNMi to appear in the key incident views in the NNMi console, set the NASnmpTrapv1 and NASnmpTrapv2 incident configurations to be root cause.

➤ This action sets all NA traps to be root cause regardless of content.

In the NNMi console, edit the NASnmpTrapv1 and NASnmpTrapv2 incident configurations to be root cause. This change sets all traps sent by the NA to NNMi to appear in the key incident views in the NNMi console.

1. In the NNMi console, in the Configuration workspace, click **Incidents > SNMP Trap Configurations**.
2. Edit each of the NASnmpTrapv1 and NASnmpTrapv2 incident configurations to select the **Root Cause** check box.

Set NA to Run the Check Policy Compliance Task When a Device Configuration Changes

In the NA console, on the Event Notification & Response Rules page, create a new rule that checks for policy compliance whenever a device's configuration changes.

1. In the NA console, click **Admin > Event Notification & Response Rules**.
2. On the Event Notification & Response Rules page, click the **New Event Notification & Response Rules** link at the top of the page.
3. On the New Event Notification & Response Rule page, do the following:
   a. Enter a rule name.
   b. Set *To take this action* to **Run Task**.
   c. Set *When the following events occur* to **Device Configuration Change**.
   d. Set *And then run this task* to **Check Policy Compliance**.
4. On the New Task/Template – Check Policy Compliance page, click **Done**.
5. On the Edit Event Notification & Response Rule page, click **Save**.

Configure NA to Send SNMP Traps to NNMi When a Policy Compliance Check Fails

In the NA console, on the Event Notification & Response Rules page, update the NA/NNM Integration via SNMP Traps rule to send SNMP traps when policy non-compliance events occur.

1. In the NA console, click **Admin > Event Notification & Response Rules**.
2. On the Event Notification & Response Rules page, locate the NA/NNM Integration via SNMP Traps rule, and then click the **Edit** link in this row.
3. On the Edit Event Notification & Response Rule page, do the following:
   a. In the *When the following events occur* list, verify that **Policy Non-Compliance** is selected.
   b. If necessary, **Ctrl-click** this row to add it to the selection list.
   c. Note the value set for SNMP Version, and change this value if appropriate.
   d. Click **Save**.

Scenario Overview

After the scenario prerequisites are in place, ANM can be used as follows:

1. NA receives a syslog event (or another change trigger), captures the new configuration, and automatically runs a compliance check on the new configuration.
2. NA sends an SNMP trap that describes the non-compliance to NNMi. NNMi displays this trap in the Open Key Incidents view.
3. From the NNMi incident, open the NA Device Configuration Diffs page to see a comparison of the current device configuration with the previous device configuration.
4. In NA, run the Deploy to Running Config task to roll back the device configuration.
5. NA restores the good configuration to the device and captures the new configuration. Then, NA automatically checks for compliance against the new configuration.

Scenario 2: Troubleshoot network fault issues

When a device fault occurs, it is helpful to gather information about the device at the time of the fault. ANM can query a device automatically and provides tools for responding to device fault incidents.

Scenario Prerequisites

- The device must be in the NNMi topology and the NA inventory.
- The device must be configured to send traps to the NNMi management server.
- OSPF traps must be enabled on the device.
- The ANM operator must have permission in NA to view and modify the device configuration.

Enable the OSPFNbrStateChange Incident

In the NNMi console, enable the OSPFNbrStateChange incident configuration.

1. In the NNMi console, in the Configuration workspace, click **Incidents > SNMP Trap Configurations**.
2. Open the OSPFNbrStateChange incident configuration.
3. Select the **Enabled** check box.
4. Save the configuration.

Scenario Overview

After the scenario prerequisites are in place, ANM can be used as follows:

1. NNMi determines that an OSPF neighbor state has changed and generates an OSPFNbrStateChange incident for that router. This incident triggers NA to gather information about the router.
2. NA runs a show neighbor device diagnostic to determine the OSPF neighbors of the router and then stores the task ID of the diagnostic as an attribute of the NNMi OSPFNbrStateChange incident.
3. From the NNMi incident, open the diagnostic report and determine that the OSPF adjacency is stuck in the INIT state.
4. In NA, view the diagnostic report of the OSPF neighbor router and observe the ACL configuration error.
5. In NA, modify the ACL of the OSPF neighbor router to permit hello packets.
6. To prevent this problem from recurring, create an NA device policy that the problem ACL is not permitted on this device or any other relevant device. Violations of this policy are handled by Scenario 1: Identify and correct an out-of-compliance device change.

Scenario 3: Re-address IPv4 addresses to the appropriate IPv6 addresses

When completed manually, the process of re-addressing an IPv4 network to use IPv6 addresses is time-consuming and error prone. ANM can automate both the collection of current IPv4 addresses in use and the setting of IPv6 addresses on managed devices.

Scenario Prerequisites

- The area of the network to be re-addressed must be in the NNMi topology and the NA inventory.
- Prepare a list of available IPv6 addresses.

Scenario Overview

After the scenario prerequisites are in place, ANM can be used as follows:

1. In the NNMi console, filter the IP Addresses inventory view to show only the area of the network to be re-addressed, and then export that list to comma-separated values (CSV) format.
2. With the CSV file open in a spreadsheet application, map each IPv4 address to an IPv6 address, and then save the spreadsheet file in CSV format.
3. Create a script that configures the new IPv6 addresses.
4. In the NA console, assign a scheduled task to run the script against the appropriate devices at the appropriate time.

Scenario 4: Troubleshoot application performance problems from a network context

Unexpected network traffic across important network interfaces is a common cause of application performance problems. ANM can monitor the utilization of important interfaces and can generate notifications when that utilization is beyond the acceptable level. ANM provides tools for updating the device configuration to block unauthorized traffic on important interfaces.

Scenario Prerequisites

- The devices must be in the NNMi topology and the NA inventory.
- Performance monitoring and interface utilization thresholds must be enabled and configured in NNMi for the interfaces.
- An IP SLA test must be configured between routers in the network path.
- Thresholds must be configured for the IP SLA tests.
- Enable the InterfaceInputUtilizationHigh and InterfaceInputUtilizationLow Incidents on page 31.

Enable the InterfaceInputUtilizationHigh and InterfaceInputUtilizationLow Incidents

In the NNMi console, enable the InterfaceInputUtilizationHigh and InterfaceInputUtilizationLow incident configurations.

1. In the NNMi console, in the Configuration workspace, click **Incidents > Management Event Configurations**.
2. Open the InterfaceInputUtilizationHigh incident configuration.
3. Select the **Enabled** check box.
4. Save the configuration.
5. Repeat step 2 through step 4 for the InterfaceInputUtilizationLow incident configuration.

Scenario Overview

After the scenario prerequisites are in place, ANM can be used as follows:

1. NNMi generates a management event incident to indicate that interface utilization is beyond acceptable boundaries for an important network interface.
2. View the NNM iSPI Performance for Traffic Interface Traffic 1 Minute Top Applications report for the volume - In Bytes and Volume-Out Bytes metrics grouped by source host name, destination host name, and application name. This report reveals competing traffic from an unauthorized application.
3. In the NA console, run a Batch Insert ACL Line task to modify multiple ACLs to multiple devices to block unauthorized traffic.
4. Network traffic across the interface returns to acceptable levels, and the interface utilization incident automatically closes in the NNMi console.

Scenario 5: Ensure edge routers maintain expected service levels

From a network management point of view, it is important to keep servers available to all users. From a business management point of view, it is important to receive the level of service purchased from an Internet service provider (ISP). ANM can monitor the responsiveness of devices that are outside of the company's network and can generate notifications when responsiveness goes below acceptable levels.

Scenario Prerequisites

- The edge router must be in the NNMi topology.
- IP SLA tests must be configured on the edge router.
- The IP SLA tests must be in the NNM iSPI Performance for QA inventory.
- Thresholds must be configured for the metrics of the IP SLA tests.

Scenario Overview

After the scenario prerequisites are in place, ANM can be used as follows:

1. NNMi generates a management event incident to indicate that a particular metric of an IP SLA test from the edge router is beyond acceptable boundaries.
2. Notify the ISP of the problem.

Scenario 6: Use baseline data to identify abnormal system utilization

Irregular traffic patterns can signal inappropriate use of the network. ANM can determine normal traffic patterns and can generate notifications when traffic patterns are outside the normal range.

Scenario Prerequisites

- The device must be in the NNMi topology and the NA inventory.
- Performance monitoring and thresholds, including baseline settings, must be enabled and configured for the interface in NNMi.

Scenario Overview

After the scenario prerequisites are in place, ANM can be used as follows:

1. NNMi generates a management event incident to indicate a deviation from normal behavior with regards to utilization on the interfaces involved in the path to the web site.
2. View the NNM iSPI Performance for Traffic Conversations for Applications Top N report for the interface identified in the incident to determine which traffic is affected, including sources and destinations.
3. Determine that the web site URL is being loaded with many HTTP requests. The requests seem to be an attack on the web site.
4. In the NA console, modify the ACLs on the device hosting the web server to deny traffic from the sources of the attack.
5. Network traffic across the interface returns to acceptable levels, and the interface utilization incident automatically closes in the NNMi console.

Scenario 7: Identify and correct error rate and utilization problems

A high error rate on an interface usually causes the workstation, server, or any other device connected to that interface to work significantly slower. ANM can monitor interfaces and generate notifications when the error rate, or utilization, or both crosses pre-defined thresholds.

Scenario Prerequisites

- The device must be in the NNMi topology and the NA inventory.
- Performance monitoring and thresholds must be enabled and configured in NNMi for the interface.
- Enable the InterfaceInputErrorRateHigh and InterfaceInputUtilizationHigh Incidents on page 34.

Enable the InterfaceInputErrorRateHigh and InterfaceInputUtilizationHigh Incidents

In the NNMi console, enable the InterfaceInputErrorRateHigh and InterfaceInputUtilizationHigh incident configurations.

1. In the NNMi console, in the Configuration workspace, click **Incidents > Management Event Configurations**.
2. Open the InterfaceInputErrorRateHigh incident configuration.
3. Select the **Enabled** check box.
4. Save the configuration.
5. Repeat step 2 through step 4 for the InterfaceInputUtilizationHigh incident configuration.

Scenario Overview

After the scenario prerequisites are in place, ANM can be used as follows:

1. NNMi generates a management event incident to indicate a high error rate on an interface. The connection table on the incident details tab indicates a duplex mismatch.
2. From the NNMi console, open the device configuration difference page for the router on each end of the connection to see which duplex is configured on this interface and to check if the device configuration has been changed recently.
3. Open an NNM iSPI Performance for Metrics interface health report for the LAN collision rate and LAN collision count metrics grouped by qualified interface name. Also open an NNM iSPI Performance for Metrics interface health report for the LAN FCS error rate and LAN FCS error count metrics grouped by qualified interface name. This combination of reports shows one side of the connection with high errors while the other side has high collisions. This information is indicative of duplex mismatch.
4. From NA, update the switch configuration.
5. Check the interface performance history in the NNM iSPI Performance for Metrics reports to verify that the error problem no longer occurs.

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click *here*.

If no email client is available, copy the information below to a new message in a web mail client, and then send this message to **ovdoc-nsm@hp.com**.

Product name and version: ANM 9.10

Document title: *ANM Configuration Guide*

Feedback: