HP Network Node Manager iSPI Performance for Metrics

for the Windows® operating system

Software Version: 9.11

Installation Guide

hp

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

© Copyright 2009 – 2011 Hewlett-Packard Development Company, L.P.

Trademark Notices

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

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

UNIX® is a registered trademark of The Open Group.

Acknowledgements

This product includes libjpeg library. This software is copyright (C) 1991-1998, Thomas G. Lane.

The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated.

This product includes libxml2 library. Copyright (C) 1998-2003 Daniel Veillard. All Rights Reserved.

This product includes libxp library. Copyright © 2001,2003 Keith Packard.

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 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 Introduction

The Network Performance Server (**NPS**) provides the infrastructure that you can use in conjunction with Network Node Manager i Software (**NNMi**) to analyze performance characteristics of your network. With the performance data collected by different HP Network Node Manager i Software Smart Plug-ins (**iSPIs**), the NPS builds data tables, runs queries in response to user selections, and displays query results in web-based reports that help you diagnose and troubleshoot problems in your network environment.

The NPS media offers you the option to install the HP Network Node Manager i Software Smart Plug-in Performance for Metrics (**NNM iSPI Performance for Metrics**), which provides the core performance management capability to NNMi by gathering and monitoring the metric data polled by NNMi from different network elements. With the combination of NNMi and the NNM iSPI Performance for Metrics, you can monitor the operational performance of the network infrastructure.

The NPS provides the infrastructure and resources for other iSPI Performance (for example, the iSPI Performance for Traffic and iSPI Performance for Quality Assurance) products to generate reports. If you do not want to use the NNM iSPI Performance for Metrics, you can choose to install the NPS without enabling the NNM iSPI Performance for Metrics. You can generate reports with any other iSPI Performance product if the NPS is installed in your environment.

If you choose to install the NNM iSPI Performance for Metrics during installation, the installer activates an Instant-On license for the NNM iSPI Performance for Metrics at the end of the installation. The Instant-On license remains active for 30 days. After the Instant-On license expires, you cannot use the NNM iSPI Performance for Metrics until you purchase and activate a permanent license for the NNM iSPI Performance for Metrics. You can, however, continue to use the NPS infrastructure with the other iSPI Performance products (if the Instant-On or Permanent license of other iSPI Performance product is active).

Overview of Architecture

The NPS provides you with the infrastructure to store, process, and analyze the data obtained from different network elements by NNMi or custom collectors (available with iSPIs). After gathering the data from data sources, the NPS processes and aggregates the data, and then stores the data into the **column-based** database management system (DBMS). The business intelligence framework—**BI server**—provides a foundation for data analysis and reporting. With the help of data analysis tools available with the BI server, you can view ready-to-use reports that indicate the performance of network elements available in the environment.

Figure 1   High-Level Architecture of the NPS
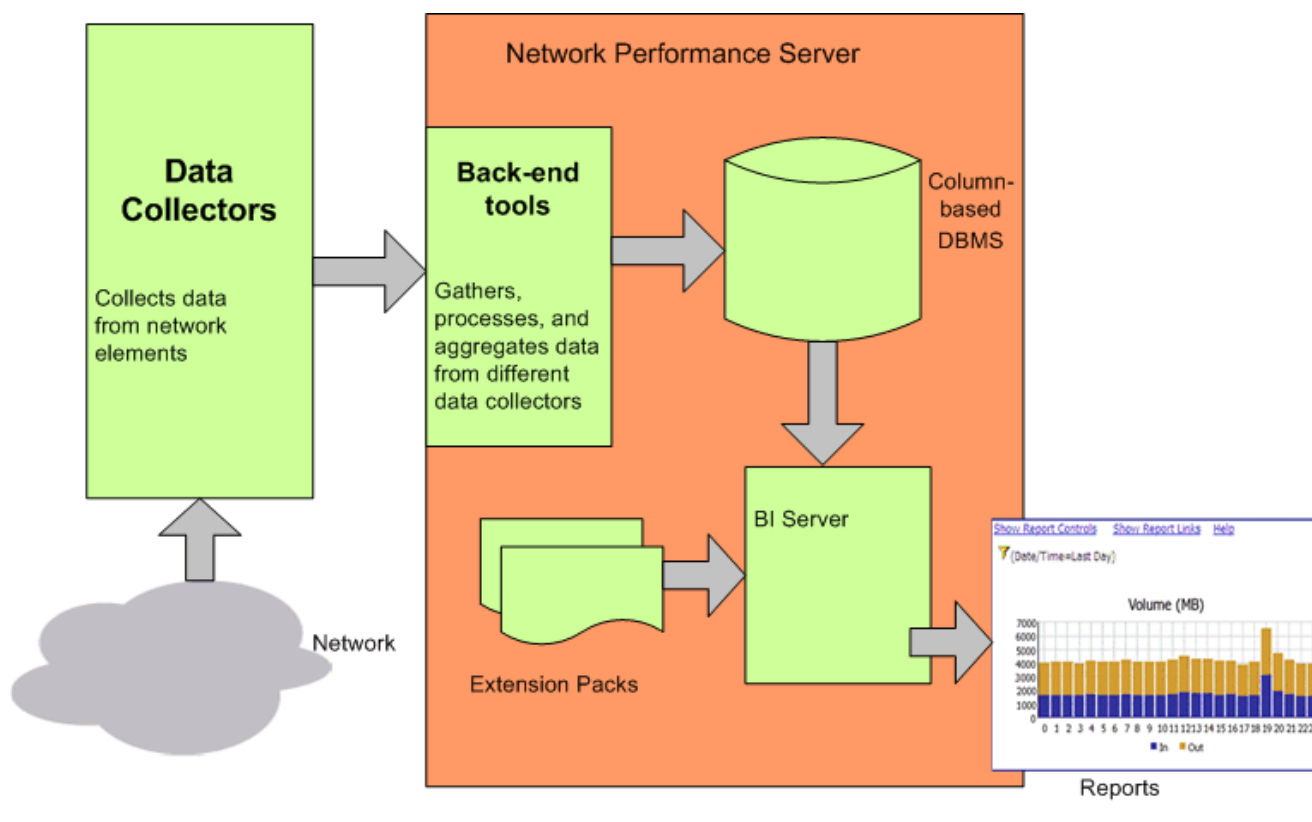
Components of the NPS

The components of the NPS can be grouped into the following categories:

- **Column-based DBMS**

  The column-based DBMS adds the data warehousing capability to the NPS solution. The DBMS can store a large amount of data, gathered from different sources, and enables the NPS to compute aggregates from a large number of data points. You can store the data, once collected, for up to 400 days into the DBMS, 70 days being the default retention period. The backup and restore feature enables you to save your data in a compressed, backed-up format. You can use the saved data if you need to restore the database after a system or disk crash.

- **BI Server**

  The BI server enables you to generate insightful, web-based reports from the data available in the DBMS with the help of pre-defined report templates. The BI Server enables you to design and save non-default, ad-hoc queries and background report scheduling. You can publish scheduled reports on the BI Server Portal. You can also configure the BI Server to e-mail the scheduled reports.

- **Extension pack**

  Extension packs provide rules and definitions to generate reports from the data gathered from different sources. The default, ready-to-use extension pack available with the NPS—the Self Diagnostics extension pack—helps you view reports indicating the health and performance of different components and processes of the NPS.

Installation Overview

You can install the NPS on the NNMi management server or on a dedicated, standalone server. Based on sizing guidelines provided in the *Network Performance Server Support Matrix* document, you can select the option that suits your requirement.

▶ Do not install the NPS on a system where the **iSPI for Performance** (8.00/8.01/8.11) is installed and running. To install the NPS on such a system, completely remove the iSPI for Performance, restart the system, and then begin the installation procedure.

With the NPS, do not use an NNMi management server that is already configured with an instance of the iSPI for Performance (8.00/8.01/8.11). However, you can follow this upgrade path:

1 Upgrade NNM iSPI Performance for Metrics 8.13 to the NPS/NNM iSPI Performance for Metrics 9.00

2 Upgrade NNM iSPI Performance for Metrics 9.00 to the NPS/NNM iSPI Performance for Metrics 9.10

Installing on the NNMi Management Server

Installing the NPS on the NNMi management server involves running the installer program. The installation process in this scenario is relatively simpler.

The installer offers you an option to install the NNM iSPI Performance for Metrics. You can choose not to install the NNM iSPI Performance for Metrics while installing the NPS. If you like, you can install the NNM iSPI Performance for Metrics on the NPS system at a later time.

Installing on a Dedicated Server

In addition to running the installer program, this installation option requires you to perform additional configuration steps with the following utilities:

- **Enablement script**

  The enablement script, available on the NNMi management server (placed on the system by the NNMi installer), facilitates communication between NNMi and the NPS.

- **Configuration utility**

The NPS installation process introduces the configuration utility to the system. The configuration utility enables you to specify the information that helps NPS processes communicate with the NNMi management server.

Sources for Additional Information

Consult the following HP sources for additional information:

- *Network Performance Server online help*
    - Troubleshooting tips
    - NPS utilities
    - Report descriptions and use-case scenarios
- *Network Node Manager i Software Deployment Reference*
- *Network Node Manager i Software Release Notes*
- *Network Node Manager i Software Support Matrix*

Documentation Conventions

The NPS documentation uses the following conventions:

Table 1   NPS Documentation Conventions

Symbol	Meaning
%NPSInstallDir%	*Windows only.* The environment variable for the NPS application directory. This variable is automatically created by the NPS installer.
%NPSDataDir%	*Windows only.* The NPS data directory. When you install the NPS on the NNMi management server, the NPS installer uses *%NPSDataDir%* as the data directory.
%nnminstalldir%	*Windows only.* The environment variable for the NNMi application directory. This variable is automatically created by the NNMi installer. If you install the NPS on an NNMi (Windows) management server, *%NPSInstallDir%* is created here for NPS application files.
%nnmdatadir%	*Windows only.* The environment variable for the NNMi data directory. This variable is automatically created by the NNMi installer. If you install the NPS on an NNMi (Windows) management server, the *%NPSDataDir%* is placed here to store for NPS configuration and data files.

On Linux, the NPS installer directly installs the necessary files into the following directories:

- **Application files:** /opt/OV

- **Data and configuration files:** `/var/opt/OV`

2 Prerequisites and Planning

Before you begin the installation, make sure that all the prerequisites are met. After evaluating your requirements, identify the most suitable installation option for the environment, and then you can create a step-by-step plan for the installation.

Prerequisites

➤ The NPS installer performs checks to verify if the following prerequisites are met.

- **Primary Domain Name System (DNS) suffix**

  The system where you plan to install the NPS must have a primary DNS suffix configured. Also, the system must be reachable on the network using the fully-qualified domain name (FQDN).

- **Port availability**

  The NPS uses the following ports for different processes: 9300, 9301, 9302, 9303, and 9304. Before installation, make sure that these ports are free. To see the list of used ports on the system, run the **netstat** command.

In addition, make sure to remove the following application and variable from the system:

- **Cygwin**

  Make sure that the Cygwin software is not present on the system.

- **JAVA_HOME**

  If you have a third-party Java Runtime Environment (JRE), and your third-party JRE is incompatible with the embedded JRE that ships with the NPS, installation errors and runtime errors may occur. To avoid these errors, make sure the JAVA_HOME environment variable is *not* set on the system.

Planning the Installation

An installation plan prepares you for the installation process and helps you gather all the information required to complete the installation. After reviewing your requirements and finalizing the installation option (installation on the management server or a dedicated server), create a plan for the installation.

NNMi Version

You can use the NPS 9.10 only with NNMi 9.10. Make sure to upgrade NNMi to the version 9.10 before installing the NPS.

To verify the version of NNMi, follow these steps:

1   Log on to the NNMi console.

2   Click **Help** → **About HP Network Node Manager i Software**.

3   Verify that the version is 9.10.

Platform Combination

If you choose to install the product on a dedicated server, make sure that the platform combination of the NPS and management server is supported.

Use an NNMi management server that runs on one of the following operating systems:

• Windows

• Linux

• SUSE Linux: Only NNMi is supported on this platform, and not NPS.

• HP-UX: Only NNMi is supported on this platform, and not NPS.

• Solaris: Only NNMi is supported on this platform, and not NPS.

Table 2   Platform Combinations

NPS Media	Supported NNMi Platform
Linux	• Linux • SUSE Linux • HP-UX • Solaris
Windows	• Windows • Linux • SUSE Linux • HP-UX • Solaris

Please refer to the *HP Network Node Manager iSPI Performance for Metrics System and Device Support Matrix* for more information on supported operating systems.

File Sharing Mechanism

When you install the NPS on a dedicated server, you must enable the file sharing mechanism between the NPS and NNMi management server.

At the end of the installation, one of the following file sharing techniques is enabled depending on the platform combination.

Table 3   File Sharing Technique Used by NNMi and the NPS

NNMi Management Server	NPS	File Sharing Technique
Windows	Windows	Windows network share
Linux, HP-UX, or Solaris	Windows	Server Message Block (SMB)

The Windows network share and SMB share require a user account with sufficient privileges. You can create the user account with the help of the enablement script.

File Sharing with the Samba Software

To use an SMB share, the Samba software (provided with the operating system) must be installed on the NNMi management server.

The SMB share may not work in the following scenarios:

- The NNMi management server runs on security-enhanced Linux (SELinux)
- Firewalls running on either server or the network

To use the SMB share, you must configure the security policies or firewall settings to make exceptions for the SMB traffic.

Domain Names

When you install the NPS on a dedicated server, the NNMi management server and dedicated server must have the same domain name.

Verify that the dedicated server and NNMi management server are in the same DNS domain; for example, hp.com. Membership in different sub-domains is allowed, but the parent domain must be the same. For example, the following systems can be used as the NNMi management server and the NPS system:

- nnm.hp.com
- iSPI.hp.com

Pre-Installation Checklist

The pre-installation checklist, provided with Table 4 on page 16 helps you ensure that all the pre-installation tasks are complete.

Table 4   Preinstallation Checklist

Task	Reference Document/Topic	Complete (y/n)
Identify the installation option: on the management server or a dedicated server	*Network Performance Server Support Matrix*	
Verify that the iSPI for Performance (8.00/8.01/8.11) is not present on the system where you want to install the NPS.		
Verify that the NNMi version is 9.10.		
Verify that NNMi is not configured with an instance of the iSPI for Performance (8.00/8.01/8.11).		
Verify that the system (where you want to install the product) meets the system requirements.	*Network Performance Server Support Matrix*	
Verify that the system (where you want to install the product) meets the prerequisites.	Prerequisites on page 13	
Only for the dedicated server installation: Verify that you have selected a supported platform combination	Platform Combination on page 14	
Only for the dedicated server installation: If you want to use an NNMi management server running on Linux, HP-UX, or Solaris, make sure that the Samba software installed on the management server.	File Sharing Mechanism on page 14	

Table 4   Preinstallation Checklist

Task	Reference Document/Topic	Complete (y/n)
Only for the dedicated server installation: Verify that the management server and dedicated server belong to the same DNS domain. Note down the FQDN of the dedicated server.	Domain Names on page 15	
Only for the dedicated server installation: If you want to use a security-enabled Linux as an NNMi management server, make sure to configure the security policies to make exceptions for the SMB traffic on the SELinux management server.	Platform Combination on page 14	
Only for the dedicated server installation: If you want to use a Linux management server, and if firewalls are configured on either server or the network, make sure to modify the firewall settings to make exceptions for the SMB traffic.		

After you complete all the tasks specified in Table 4, start the installation procedure.

Single Sign-On

Installing the NPS enables a security mechanism known as Single Sign-on (SSO). SSO allows the NPS to recognize the same user names and passwords that the NNMi Console recognizes. When SSO is enabled, a user who is already logged on to NNMi, can move from NNMi to an iSPI report without having to log on a second time.

For SSO to work, the NPS and NNMi must share the same domain name and the URL that launches NNMi must include NNMi's fully-qualified domain name (FQDN). If you point a browser at a URL using an unqualified host name, the SSO servlet will display an error page requesting you to use a fully-qualified hostname in the NNMi URL before launching reports.

If you want to use the NNMi management server's IP address instead of the FQDN, you must configure NNMi accordingly during installation, or use the **nnmsetofficialfqdn.ovpl** *<ipaddress>* command to set the NNMi FQDN to the IP address.

If NNMi and the NPS are installed on the same server, and NNMi is not yet configured with an FQDN, you can achieve the same results—no second logon window or error messages when you move from NNMi to a report—by using NNMi's IP address in the URL.

3 Installing on the NNMi Management Server

If you want to install the NPS on a dedicated server, skip this chapter and go to Installing on a Dedicated Server on page 27.

Before you begin the installation process, make sure that NNMi is running on the server and the version of NNMi is 9.10.

If you do not have the NPS on a DVD distributed by HP, you can download an ISO image from HP. After you download the file, mount the image to a drive or burn your own DVD. To burn the image directly to a CD, you will need to install a software application designed to burn ISO image files.

⚠ If you are installing NPS/NNM iSPI Performance for Metrics using terminal server session or remote desktop connection, make sure that you do **not** download the ISO image in any of the following drive types:

- Network drive
- Detachable media

Installing the NPS

To install the NPS, follow these steps:

1 Log on to the management server with the administrative privileges.

2 Insert the NPS installation media into the DVD drive.

   From the media root, run the setup.exe file

   The installation wizard opens.

   If the Application requirement check warnings dialog box opens, review the warning messages, take appropriate actions, and then click **Continue**.

3 On the Introduction page, click **Next**. The Product Agreement page opens.

4 On the Product Agreement page, select **I accept the terms....**, and then click **Next**. The Select Features page opens. This page offers you the option to install the NPS without enabling the NNM iSPI Performance for Metrics.

5 On the Select Features page, select the HP NNM NNM iSPI Performance for Metrics - ExtensionPacks check box if you want to use the NNM iSPI Performance for Metrics. If you clear the HP NNM NNM iSPI Performance for Metrics - ExtensionPacks check box, the installer does not install the NNM iSPI Performance for Metrics on the system.

6 Click **Next**. The installer program initiates the system checking process and verifies if system requirements are met.

7 If the installation check succeeds, click **Next**. The Pre-Install Summary page opens.

8 On the Pre-Install Summary page, click **Install**. The installation process begins.

9 When the installation process is complete, click **Done**.

Enabling Secured Mode of Transmission for NPS

After installing NPS, you can specify whether NPS should use secured mode of transmission; that is HTTPS instead of HTTP. By default the mode of transmission is unsecured, that is HTTP.

NPS and NNMi can use different mode of transmission. By default, NNMi enables secured mode of transmission during installation. You can either use HTTP or HTTPS while using NNMi. However, you must enable HTTPS for NPS.

If you enable secured mode of transmission, NPS uses HTTPS with Secure Sockets Layer (SSL) for additional security for the transmissions between NNM iSPI Performance for Metrics server and the client web browser.

Use the following commands to enable, disable or configure secured mode of transmission for NPS:

`configureWebAccess.ovpl`

By default, configureWebAccess.ovpl command uses the following port numbers:

- HTTP: 9300
- HTTPS: 9305

To enable, disable, or configure the HTTPS and HTTP ports, perform the following step:

1 Run the following command from the following location:

Windows: `%NPSInstallDir%\bin\configureWebAccess.ovpl`

2 Respond to the messages that the utility displays.

If the utility fails, check the following log files:

- Windows: `%NPSDataDir%\logs\prspi.log`

Check Whether the Secured Mode of Connection Is Enabled

Run the following command:

`configureWebAccess.ovpl -h`

The utility displays the mode of transmission.

Make sure that you do *not* use the following ports for HTTPS protocol:

- 9300
- 9301
- 9302
- 9303
- 9004

Make sure that you do *not* use the following ports for HTTP protocol:

- 9301
- 9302
- 9303

- 9304

By default, BI Server uses a built-in Certificate Authority (CA) for secured mode of transmission. You can disable it and use a third party CA. See Configuring Third party Certifying Authority for BI Server on information about how to configure a third party CA for BI Server.

Installing the NPS in a High Availability Cluster

When NNMi is installed in a high availability (HA) cluster, you can install and configure the NPS as an add-on product on the NNMi management servers. To install the NPS in HA clusters, follow these steps:

1. On the active node, run the following command to verify that all NNMi services are running:

   ovstatus -c

2. On the active node, install the NPS with the instructions in Installing the NPS on page 19.

3. Stop the NPS by running the **stopALL.ovpl** command.

4. If you are a member of the Windows Administrators user Group but not using the built-in Administrator account, follow these steps on the active node:

   a. Go to **Start > Administrative Tools > Services**.

   b. In the Services window, right-click **NNM iSPI Performance ETL Server**, and then click **Properties**.

   c. Change the default Log On setting (Local System) to This Account, and then specify the credentials of the user account that you are using.

5. Run the following command on the active node:

   On Windows:

   %nnminstalldir%**misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon PerfSPIHA**

   ☛ The nnmhaconfigure.ovpl command is an interactive command and requires you to specify details related to the HA environment. See the *Network Node Manager i Software 9.10 Deployment Reference* for more information on the nnmhaconfigure.ovpl command.

6. Verify the configuration.

   Run the following command:

   On Windows:

   %nnminstalldir%\misc\nnm\ha\nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS

   You should see PerfSPIHA.

7. On each passive node, install the NPS with the instructions in Installing the NPS on page 19.

8. Stop the NPS by running the **stopALL.ovpl** command.

9 If you are a member of the Windows Administrators user Group but not using the built-in Administrator account, follow these steps on each passive node:

   a Go to **Start > Administrative Tools > Services**. Make sure that you are logged in with the Windows Server 2008 administrative privileges.

   b In the Services window, right-click **NNM iSPI Performance ETL Server**, and then click **Properties**.

   c Change the default Log On setting (Local System) to This Account, and then specify the credentials of the user account that you are using.

10 Run the following command on each passive node:

   On Windows:

   %nnminstalldir%**misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon PerfSPIHA**

   > ⚑ The `nnmhaconfigure.ovpl` command requires you to specify the HA resource group name when you run the command on a passive node. See the *Network Node Manager i Software 9.10 Deployment Reference* for more information on the `nnmhaconfigure.ovpl` command.

11 Verify the configuration.

   Run the following command on each passive node:

   %nnminstalldir%\misc\nnm\ha\nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS

If you created a custom collection extension pack, perform the following additional tasks:

1 On the active node, go to the following directory:

   ```
   %nnminstalldir%\nonOV\cognos\c8\webapps\PerfSpi\WEB-INF\classes\com\
   hp\ov\perfspi
   ```

2 Copy all the properties files (files with the extension `.properties`) that are available in the directory, and then transfer those files to the same directory on each passive node.

To ensure smooth application failover, make sure that all hosts in the same HA group have the same configurations for secured mode of transmission (HTTPS). The hosts in the same HA group must have same configurations for the transmission protocol, port number, and digital certificates.

Installing the NNM iSPI Performance for Metrics

Skip this section if you chose to install the NNM iSPI Performance for Metrics while installing the NPS.

If you choose not to install the NNM iSPI Performance for Metrics at the time of installation, you can do so at a later time. To install the NNM iSPI Performance for Metrics, follow these steps:

1 Log on to the NNMi management server with the administrative privileges.

2 From the NPS media, run the `setup.exe` file.

3 Select Modify on the Maintenance Selection page.

4 Follow the on-screen instructions. Select the HP NNM NNM iSPI Performance for Metrics
- ExtensionPacks check box on the Select Features page.

The installer installs the NNM iSPI Performance for Metrics on the system.

Alternatively, you can run the following command from the /opt/OV/NNMPerformanceSPI/bin
or *%nnminstalldir%*\bin directory:

metricsExtensionPacks.ovpl install

▶ If NNMi and the NPS are installed in an HA cluster, perform the above procedure only on the
active node. On each passive node, perform the following tasks:

1 Log on to the NNMi management server with the administrative privileges.

2 Run the enablement script nnmenableperfspi.ovpl from the%nnminstalldir%\bin
directory. While running the enablement script, answer **Y** for the following question:

```
Would you like to also enable the iSPI Metrics evaluation license ?
```

3 From the active node, copy all the properties files (files with the extension `.properties`)
from the
%nnminstalldir%\nonOV\cognos\c8\webapps\PerfSpi\WEB-INF\classes\com\hp
\ov\perfspi directory and transfer those files to the same directory on the passive
node.

Disabling the NNM iSPI Performance for Metrics

If you want use the NPS with other iSPI Performance products, but do not want to use the
NNM iSPI Performance for Metrics, you can disable the NNM iSPI Performance for Metrics
without removing the NPS.

To disable the NNM iSPI Performance for Metrics, follow these steps:

1 Log on to the NNMi management server with the administrative privileges.

2 From the NPS media, run the `setup.exe` file.

3 Select Modify on the Maintenance Selection page.

4 Follow the on-screen instructions. Clear the HP NNM NNM iSPI Performance for Metrics
- ExtensionPacks check box on the Select Features page.

The installer disables the NNM iSPI Performance for Metrics on the system.

Alternatively, you can run the following command from the %nnminstalldir%\bin directory:

metricsExtensionPacks.ovpl uninstall

▶ If NNMi and the NPS are installed in an HA cluster, perform the above procedure only on the
active node. On each passive node, perform the following tasks:

1 Log on to the NNMi management server with the administrative privileges.

2 Run the enablement script from the `%nnminstalldir%\bin` directory. While running
the enablement script, answer **N** for the following question:

```
Would you like to also enable the iSPI Metrics evaluation license ?
```

Removing the NPS

To remove the NPS from the management server, follow these steps:

⚠ If you want to continue to use the reports created by different iSPI Performance products, do not remove the NPS. You cannot use reports if the NPS is not available in the environment.

1 Log on to the management server with the administrative privileges.

2 Make sure NNMi is running.

3 From the Start menu, click **All Programs→ HP → NNM iSPI Performance → Uninstall.** The wizard opens.

   If the Application requirement check warnings dialog box opens, review the warning messages, take appropriate actions, and then click **Continue**.

4 A welcome page opens. Click **OK**.

5 On the Application Maintenance page, select **Uninstall**, and then click **Next**. The Pre-Uninstallation Summary page opens.

6 On the Pre-Uninstallation Summary page, click **Uninstall**. The program starts removing the NPS from the system.

7 When the program completely removes the NPS, click **Done**. The removal process removes all the components of the NPS from the system.

To avoids problems with subsequent re-installations on a Windows server, perform the following tasks after uninstalling the NPS :

1 Restart the Windows server

2 Verify that the %NPSDataDir%\NNMPerformanceSPI folder is removed.

Removing the NPS from an HA Cluster

To remove the NPS from an HA cluster, perform the following tasks:

Task 1: Remove the NPS from Passive Nodes

On each passive node, follow these steps:

1 Log on to the passive node with the administrative privileges.

2 Run the following command to disable the HA configuration for the NPS on the passive NNMi management server:

   %nnminstalldir%**misc\nnm\ha\nnmhaunconfigure.ovpl NNM -addon PerfSPIHA**

3 Run the following command to stop all NPS processes:

   %NPSInstallDir%\bin**stopALL.ovpl**

4 Follow the instructions in to remove the NPS from the node.

Task 2: Remove the NPS from the Active Node

1 Log on to the active node with the administrative privileges.

2   Run the following command to disable the HA configuration for the NPS on the active NNMi management server:

%nnminstalldir%**misc\nnm\ha\nnmhaunconfigure.ovpl NNM -addon PerfSPIHA**

3   Run the following command to stop all NPS processes:

%NPSInstallDir%\bin**stopALL.ovpl**

4   Follow the instructions in Removing the NPS on page 24 to remove the NPS from the active node.

4 Installing on a Dedicated Server

If you want to install the NPS on a dedicated server, you must run the enablement script first on the NNMi management server, and then run the installer program on the dedicated server.

If you do not have the NPS on a DVD distributed by HP, you can download an ISO image from HP. After you download the file, mount the image to a drive or burn your own DVD. To burn the image directly to a CD, you will need to install a software application designed to burn ISO image files.

⚠ If you are installing NPS/NNM iSPI Performance for Metrics using terminal server session or remote desktop connection, make sure that you do **not** download the ISO image in any of the following drive types:

- Network drive
- Detachable media

Running the Enablement Script

Before you begin the installation on the dedicated server, you must run the enablement script on the NNMi management server. The NNMi version must be 9.10. The enablement script is placed on the management server by the NNMi installer.

Run on a Windows Management Server

If you want to use a Windows NNMi management server, follow these steps:

1 Log on to the NNMi management server with administrative privileges.

2 Go to the following location:

    %nnminstalldir%\bin

3 Run the script `nnmenableperfspi.ovpl`. The enablement script starts operating in the interactive mode. The script shows the following message:

    Would you like to also enable the iSPI Metrics evaluation license ?

4 Type **Y**, and then press **ENTER**.

If you select **N**, the extension packs for the NNM iSPI Performance for Metrics will remain disabled.

The script shows the following message:

    Would you like to begin?

5 Type **Y**, and then press **ENTER**. The script asks if you want to install the NPS on the local system with NNMi.

6   Type **N**, and then press **ENTER**. The script asks for the FQDN of the system where you plan to install the NPS.

7   Type the FQDN, and then press **ENTER**.

Use only FQDN; do not use the IP address. If you want to install and configure the NPS in an HA cluster, specify the virtual hostname of the cluster and make sure that you run this script after the NPS HA resource group is configured and started.

The script shows the following message:

```
Is SSL enabled (or will it be enabled) on the iSPI Performance machine? (Y/
N):
```

8   Type **Y**. The script then shows the following message:

```
The default port for the iSPI is 9300.
```

```
Press [return] to use this port.
```

9   Press **ENTER**. The script asks if you would like to add the NPS share to your system.

10   Type **Y**. The script creates a share in the following location:

```
%NnmDataDir%\shared\perfSpi
```

The NPS will access this location from the dedicated server to gather data collected by NNMi.

11   The script asks you to provide the user name of a new user, which will be created by the script on the NNMi management server and will be used by the NPS to access the shared location. Provide the user name and password of your choice for the user at the prompt. The selected user name and password must meet the password strength policies in effect—on the NNMi management server and the NPS system

Note down the user name and password that you provide at the prompt. You must specify the same user details at the NPS on the dedicated server.

12   If a share already existed on the system, the script shows the following message:

```
A PerfSpi share has been created already.
```

```
Would you like to removed then re-created?
```

Type **Y**. The script removes the share, and then re-creates the share for the newly created user.

13   The enablement script stops. The script summary shows the shared path (to be accessed by the NPS) in the following format:

```
\\<FQDN>\PerfSpi
```

Note down this location and use it later with the NPS on the dedicated server in exactly the same format.

The script performs the following tasks while running on the management server:

- Depending on your selection, enables the Instant-On license for the NNM iSPI Performance for Metrics.

- Adds a new item—the **Reporting- Report Menu** item—to the Actions menu in the NNMi console.

- Shares a location on the management server.

- Creates a new user on the management server.

- Enables the Single Sign-On security for the NPS.

14 Type **Y**. The script then shows the following message:

Samba Share

Choose this option since you are using a Windows NPS media. The script asks you to provide the user name of a new user (system user; not an NNMi user), which will be created by the script on the NNMi management server and will be used by the NPS to access the shared location. Provide the user name and password of your choice for the user at the prompt. The selected user name and password must meet the password strength policies in effect—on the NNMi management server and the NPS systemNote down the user name and password that you provide at the prompt. You must specify the same user details at the NPS on the dedicated server.Installing the NPS

You must perform this procedure on the dedicated server. To run the installer program for the NPS, follow these steps:

1 Log on to the dedicated server with the administrative privileges.

2 Insert the NPS installation media into the DVD drive.

From the media root, run the `setup.exe` file.
The installation wizard opens.

If the Application requirement check warnings dialog box opens, review the warning messages, take appropriate actions, and then click **Continue**. The Product Agreement page opens.

3 On the Product Agreement page, select **I accept the terms....**, and then click **Next**. The Select Features page opens. This page offers you the option to install the NPS without enabling the NNM iSPI Performance for Metrics.

4 On the Select Features page, select the HP NNM NNM iSPI Performance for Metrics - ExtensionPacks check box if you want to use the NNM iSPI Performance for Metrics. If you clear the HP NNM NNM iSPI Performance for Metrics - ExtensionPacks check box, the installer does not enable the NNM iSPI Performance for Metrics on the system.

Click **Next**.

The Choose the application and data folder page opens.

5 On the Choose the application and data folder page, if you want, you can specify non-default locations for these folders.

By default, the installer program sets these fields to the following locations:

- **Application folder:** `C:\Program Files (x86)\HP\HP BTO Software`

- **Data folder:**

  — For Windows 2008:

    `C:\ProgramData\HP\HP BTO Software`

6 Click **Next**.

7 The installer program initiates the system checking process and verifies if system requirements are met.

8 If the installation check succeeds, click **Next**. The Pre-Install Summary page opens.

9 On the Pre-Install Summary page, click **Install**. The installation process begins.

10 Toward the end of the installation process, the Configuration Utility opens. In the Configuration Utility, follow these steps:

a Select the Named User account option.

     b   Specify the user name and password of the user created by the enablement script.

          Specify the path to the shared location created by the enablement script on the NNMi management server.Use exactly the same format displayed by the enablement script summary.Specify the detailed data archive retention period. Depending on the system resource, choose a value for this parameter.For information on required storage for each data retention type, see

     c   Click **Apply**.

     d   Click **Start** to start the necessary processes for the NPS on the dedicated server.

11   When the installation process is complete, click **Done**.

Enabling Secured Mode of Transmission for NPS

After installing NPS, you can specify whether NPS should use secured mode of transmission; that is HTTPS instead of HTTP. By default the mode of transmission is unsecured, that is HTTP.

NPS and NNMi can use different mode of transmission. By default, NNMi enables secured mode of transmission during installation. You can either use HTTP or HTTPS while using NNMi. However, you must enable HTTPS for NPS.

If you enable secured mode of transmission, NPS uses HTTPS with Secure Sockets Layer (SSL) for additional security for the transmissions between NNM iSPI Performance for Metrics server and the client web browser.

Use the following commands to enable, disable or configure secured mode of transmission for NPS:

`configureWebAccess.ovpl`

By default, configureWebAccess.ovpl command uses the following port numbers:

- HTTP: 9300
- HTTPS: 9305

To enable, disable, or configure the HTTPS and HTTP ports, perform the following step:

1   Run the following command from the following location:

    Windows:`%NPSInstallDir%\bin\configureWebAccess.ovpl`

2   Respond to the messages that the utility displays.

If the utility fails, check the following log files:

- Windows: `%NPSDataDir%\logs\prspi.log`

Check Whether the Secured Mode of Connection Is Enabled

Run the following command:

`configureWebAccess.ovpl -h`

The utility displays the mode of transmission.

Make sure that you do *not* use the following ports for HTTPS protocol:

- 9300
- 9301

- 9302

- 9303

- 9004

Make sure that you do *not* use the following ports for HTTP protocol:

- 9301

- 9302

- 9303

- 9304

By default, BI Server uses a built-in Certificate Authority (CA) for secured mode of transmission. You can disable it and use a third party CA. See Configuring Third party Certifying Authority for BI Server on information about how to configure a third party CA for BI Server.

Installing the NNM iSPI Performance for Metrics

Skip this section if you chose to install the NNM iSPI Performance for Metrics while installing the NPS.

If you choose not to install the NNM iSPI Performance for Metrics at the time of installation, you can do so at a later time. To install the NNM iSPI Performance for Metrics, follow these steps:

1   Log on to the NNMi management server with the root or administrative privileges.

2   Run the enablement script—nnmenableperfspi.ovpl—from the *%nnminstalldir%*\bin directory. While running the enablement script, answer **Y** for the following question:

    Would you like to also enable the iSPI Metrics evaluation license ?

3   Log on to the NPS system with the administrative privileges.

4   From the NPS media, run the setup.exe file.

5   Select Modify on the Maintenance Selection page.

6   Follow the on-screen instructions. Select the HP NNM NNM iSPI Performance for Metrics - ExtensionPacks check box on the Select Features page.

    The installer installs the NNM iSPI Performance for Metrics on the system.

    Alternatively, run the following command from%nnminstalldir%\bin directory on the NPS system, and then run the following command:

metricsExtensionPacks.ovpl install

➤ If NNMi and the NPS are installed in an HA cluster, perform the above procedure only on the active node. On each passive node, perform the following tasks:

1   Log on to the NNMi management server with the root or administrative privileges.

2   Run the enablement script from the %nnminstalldir%\bin directory. While running the enablement script, answer **Y** for the following question:

    `Would you like to also enable the iSPI Metrics evaluation license ?`

3   From the active node, copy all the properties files (files with the extension `.properties`) from the
    %nnminstalldir%\nonOV\cognos\c8\webapps\PerfSpi\WEB-INF\classes\com\hp\ov\perfspi directory and transfer those files to the same directory on the passive node.

Disabling the NNM iSPI Performance for Metrics

If you want use the NPS with other iSPI Performance products, but do not want to use the NNM iSPI Performance for Metrics, you can disable the NNM iSPI Performance for Metrics without removing the NPS.

To disable the NNM iSPI Performance for Metrics, follow these steps:

1   Log on to the NNMi management server with the root or administrative privileges.

2   Run the enablement script—`nnmenableperfspi.ovpl`—from the %nnminstalldir%\bin directory. While running the enablement script, answer **N** for the following question:

    `Would you like to also enable the iSPI Metrics evaluation license ?`

3   Log on to the NPS media with the administrative privileges.

4   From the NPS media, run the `setup.exe` file.

5   Select Modify on the Maintenance Selection page.

6   Follow the on-screen instructions. Clear the HP NNM NNM iSPI Performance for Metrics - ExtensionPacks check box on the Select Features page.

    The installer disables the NNM iSPI Performance for Metrics on the system.

    Alternatively, run the following command from the %nnminstalldir%\bin directory, and then run the following command:

`metricsExtensionPacks.ovpl uninstall`

➤ If NNMi and the NPS are installed in an HA cluster, perform the above procedure only on the active node. On each passive node, perform the following tasks:

1   Log on to the NNMi management server with the root or administrative privileges.

2   Run the enablement script from the `%nnminstalldir%\bin` directory. While running the enablement script, answer **N** for the following question:

    `Would you like to also enable the iSPI Metrics evaluation license ?`

Installing the NPS System in HA Clusters

When you install the NPS on a dedicated server that runs in an HA cluster, you can choose one of the following deployment options.

- Option 1: The NPS system is in an HA cluster

- Option 2: Only the NNMi management server is in an HA cluster

If you are using Windows Server 2008, use a domain account with the administrative privileges to install the NPS and configure HA group.

Option 1: Install the NPS in an HA Cluster

To install only the NPS in an HA cluster, follow these steps:

1   Configure the HA cluster on the systems where you want to install the NPS.

2   Obtain the following details of the cluster:

- Virtual hostname of the cluster. The virtual hostname must map to the virtual IP address of the cluster.

- HA resource group of the cluster

- File system type, disk group, volume group for the shared file system

- Mount point of the NPS shared disk

3   Without running the enablement script on the management server, install the NPS on the primary node in the cluster by following the instructions in page 29, but do not start the services. Ignore errors in the Configuration Utility.

4   If you are a member of the Windows Administrators user Group but not using the built-in Administrator account, follow these steps on the active node:

a   Go to **Start > Administrative Tools > Services**.

b   In the Services window, right-click **NNM iSPI Performance ETL Server**, and then click **Properties**.

c   Change the default Log On setting (Local System) to This Account, and then specify the credentials of the user account that you are using.

d   Manually edit the *%NPSDataDir%*\rconfig\NNMPerformanceSPI.cfg file to include the following property:

```
PRSPI_NNMDIR              //<nnmhostname>/PerfSpi
```

In this instance, <nnmhostname> is the FQDN of the NNMi management server.

5   On the primary node, follow these steps:

a   Run the following command to make sure that the NPS processes are not running:

%NPSInstallDir%\bin\stopALL.ovpl

b   Define the disk device group (and logical volume) consisting of at least one shared disk for the performance HA resource group.

c   Create the directory mount point for the shared disk.

d   To configure the HA resource group of the NPS, run the following command:

%nnminstalldir%\misc\nnm\ha\nnmhaconfigure.ovpl PerfSPIHA

The command prompts you to specify the details obtained in step 2.

e   Verify the configuration.

Run the following command:

%nnminstalldir%\misc\nnm\ha\nnmhaclusterinfo.ovpl -group <resource_group> -nodes

The local node should be listed.

%nnminstalldir%\misc\nnm\ha**nnmhaclusterinfo.ovpl -config PerfSPIHA -get PerfSPI_HA_CONFIGURED**

The command should display YES.

6   Install the NPS on the each passive node in the cluster by following the instructions in page 29, but do not start the services.

7   Bring NPS HA resource group online either by using the Failover Cluster Manager or by running the following command:

%nnminstalldir%\misc\nnm\ha\nnmhastartrg.ovpl PerfSPIHA <resource_group>

8   Run the enablement script on the NNMi management server (see Running the Enablement Script on page 27). While running the enablement script, provide the virtual hostname of the NPS cluster.

9   If you are a member of the Windows Administrators user Group but not using the built-in Administrator account, follow these steps on each passive node:

a   Go to **Start > Administrative Tools > Services**.

b   In the Services window, right-click **NNM iSPI Performance ETL Server**, and then click **Properties**.

c   Change the default Log On setting (Local System) to This Account, and then specify the credentials of the user account that you are using.

d   Manually edit the *%NPSDataDir%*\rconfig\NNMPerformanceSPI.cfg file to include the following property:

PRSPI_NNMDIR   //<nnmhostname>/PerfSpi

In this instance, <nnmhostname> is the FQDN of the NNMi management server.

10 On each passive node, run the following command:

%nnminstalldir%\misc\nnm\ha\nnmhaconfigure.ovpl PerfSPIHA

If you created a custom collection extension pack, perform the following additional tasks:

1   Go to the following directory on the active NPS system:

%nnminstalldir%\nonOV\cognos\c8\webapps\PerfSpi\WEB-INF\classes\com\hp\ov\perfspi

2   From the active node, copy all properties files available in the directory, and then transfer those files to the same directory on each passive NPS system.

Option 2: Only the NNMi Management Server is in an HA Cluster

In this scenario, run the enablement script (step 8 on page 34) once on the active NNMi management server, and once on every passive NNMi management server, and then install the NPS by following the instructions in page 29.

Troubleshooting Tips

The Configuration Utility shows the following failure message:

FATAL: Service configuration test failed

- *Cause 1:*

  Incorrect user name or password.

  Solution:

  Make sure to specify the user name and password specified with the enablement script.

- *Cause 2:*

  Incorrect format of the shared path.

  Solution:

  Make sure to specify the correct share path in the correct format. To specify the correct path, follow these steps:

  a Go to the NNMi management server.

  b Collect the log file `nnmenableperfspi_log.txt` for the enablement script from the following location: `%nnmdatadir%\log` or `/var/opt/OV/log`

  c At the end of the file, look for the shared location details in the Summary or Next Steps section.

  d Copy the location from the log file and paste in the Path field in the Configuration Utility.

- *Cause 3:*

  On the NNMi management server running on security-enhanced Linux (SELinux), security policies are enabled. As a result, the SMB share is not working.

  Solution:

  Disable the security policies on the SELinux management server.

The Configuration Utility shows that the shared drive is not accessible

Cause:

The firewall setting on the network prevents the NPS to access shared files by using the SMB protocol.

Solution:

To resolve this, use the appropriate tools to make exceptions for the SMB traffic.

Removing the NPS

To remove the NPS from the dedicated server, follow these steps:

⚠ If you remove the NPS, you will not be able to generate reports using the data polled by any iSPIs.

1 Make sure NNMi is running.

2 Log on to the NNMi management server with the administrative or root privileges.

3 Go to the following location:

On Windows: %nnminstalldir%\bin

4 Run the disablement script (`nnmdisableperfspi.ovpl`).

5 Log on to the dedicated server with the administrative privileges.

6 From the Start menu, click **All Programs→ HP → NNM iSPI Performance → Uninstall.** The wizard opens.

If the Application requirement check warnings dialog box opens, review the warning messages, take appropriate actions, and then click **Continue**.

7 A welcome page opens. Click **OK**.

8 On the Application Maintenance page, select **Uninstall**, and then click **Next**. The Pre-Uninstallation Summary page opens.

9 On the Pre-Uninstallation Summary page, click **Uninstall**. The program starts removing the NPS from the system.

10 When the program completely removes the NPS, click **Done**. The removal process removes all the components of the NPS from the system.

Removing the NPS from HA Clusters

If you want to remove the NPS from an HA cluster, perform the following tasks:

Task 1:   Unconfigure the HA Nodes

To unconfigure the NPS HA nodes, follow these steps:

1 On each passive node, follow these steps:

a Log on to the node with the administrative privileges (use the same user that was used while configuring HA).

b Run the following command:

%nnminstalldir%\misc\nnm\ha\nnmhaunconfigure.ovpl PerfSPIHA <resource_group>

c Stop all NPS processes by running the **stopALL.ovpl** command.

2 On the active node, follow these steps:

a Log on to the node with the administrative privileges (use the same user that was used while configuring HA).

b Run the following command:

%nnminstalldir%`\misc\nnm\ha\nnmhastoprg.ovpl PerfSPIHA` *<resource_group>*

c Run the following command:

%nnminstalldir%`\misc\nnm\ha\nnmhaunconfigure.ovpl PerfSPIHA` *<resource_group>*

d Stop all NPS processes by running the `stopALL.ovpl` command.

Task 2: Remove the NPS

Remove the NPS from the active node and each passive node by following the instructions in Removing the NPS on page 36.

5 Getting Started

➤ • If you acquired a license for only the iSPI Performance for Traffic, you will not be able to use the features of the NNM iSPI Performance for Metrics. To use the combined capabilities of the iSPI Performance for Traffic and NNM iSPI Performance for Metrics, you must separately acquire the licenses for both the iSPI Performance for Traffic and NNM iSPI Performance for Metrics.

• If NNMi is deployed in Global Network Management (GNM) environment, deploy one instance of NPS for each NNMi management server. That is, each regional manager and the global manager must have separate instances of NPS installed and deployed.

Launching the NPS Reports

You can launch the NPS reports from:

- The NNMi console
- Report Menu
- From the Start Menu

Launching from the NNMi Console

1   Enter the following URL into a web browser window:

   http://<fully-qualified-domain-name>:<port>/nnm/

   In this instance, *<fully-qualified-domain-name>* is the fully-qualified domain name of the NNMi management server, and *port* is the port used by the jboss application server to communicate with the NNMi console.

2   When the NNMi console logon window opens, type your user account name and password, and then click **Sign In**.

3   When the NNMi console opens, select **Actions > Reporting - Report Menu**. The NPS report window opens.

Directly Launching the Report Menu

1   Point your browser to the following URL:

   http://*<fully-qualified-domain-name>*:9300

   In this instance, *<fully-qualified-domain-name>* is the fully-qualified domain name of the NPS system.

2   When the NNMi console logon window opens, type your user account name and password, and then click **Sign In**.

3   The Report Menu opens. From this page, you can open any report.

Launching from the Start Menu

You can launch the Report Menu of the NPS from the Windows Start Menu. To launch the Report Menu, click **Start** → **All Programs** → **HP NNM iSPI Performance** → **Report Menu**.

Verify Error-Free Installation

To verify that the NPS is installed without errors, perform these tasks:

- Task 1: Locating Application Files and Runtime Files on page 40
- Task 2: Validating the Configuration File on page 41

Task 1:   Locating Application Files and Runtime Files

NPS software consists of static application software files (binaries) and dynamic runtime files. The NNMPerformanceSPI directory in the default path for static application files contains the following folders:

- `bin`
- `config`
- `Docs`
- `extentionpacks`
- `Installation`
- `java`
- `lib`
- `L10N`
- `build.info (text file containing date of NPS software build)`

The default path to the dynamic runtime files is:

The **NNMPerformanceSPI** directory in the default path to the dynamic runtime files contains the following folders:

- `contentstore`
- `database`
- `logs`
- `nnmappfailover`
- `rconfig`
- `PerfSPI_Diagnostics`

The default path to the dynamic runtime files contains an additional folder for each installed ExtensionPack. When NNM iSPI Performance for Metrics is installed, this path contains Interface_Health and Component_Health folders.

The configuration checker verifies that the main configuration file contains valid entries. To launch the configuration checker:

Start > All Programs > HP > NNM iSPI for Performance > Configuration Checker

If everything is okay, the checker displays the following message:

```
INFO: configuration file validated OK
```

If you installed the NPS on a dedicated system, you must specify the user credentials that were created during the installation ().

Using the Configuration Utility

Use the Configuration Utility to change the following parameters:

- Path to the NNM datafiles folder
- Credentials required to access the shared drive on the NNM server
- Data retention

To make any of these changes, follow these steps:

1   Launch the Configuration Utility.

　　Start > All Programs > HP > NNM iSPI for Performance > Configuration Utility

2   Click **Stop**. (Clicking **Stop** stops data processing and table creation)

3   Make any of these changes:

　　Change the account name

　　Change the password

- Change the account name

　　　▶　For a same-system install, use the "local system" account option.

- Change the password

　　　▶　Not applicable to same-system installs.

- Change the path to the shared NNM datafiles directory
- Modify the default retention period for archive table data:

　▶　The raw data is retained on the system for the duration specified in this field. The summary data can be retained for 400 days, the default data retention period being 70 days.

　　— Default = 14 days

　　— Maximum retention period = 400 days

4   Click **Apply**.

5   Click **Start**.

6   Click **Exit**.

The system will not read your changes until you restart. Under certain circumstances (for example, a shared file system is not ready), you may be required to delay restarting.

Troubleshooting the NPS

If you want to ensure trouble-free operation of the NPS, you can use the following diagnostic tools:

- Log File Monitor on page 42
- Log File Analyzer on page 42
- Diagnostic Reports on page 43

Log File Monitor

The log file monitor is Chainsaw. Using Chainsaw, you can monitor DEBUG, INFO, WARN, ERROR, and FATAL messages as they reach the prspi.log file. The perfspi.log file contains every message generated since previous night at midnight. The path to prspi.log is:

%NPSDataDir%\logs\prspi.log

Follow these steps to verify that the NPS is running without errors.

1   Open the Log File Monitor.

   Start > All Programs > HP > NNM iSPI for Performance > Log File Monitor

2   The welcome page includes several tabs. Select the message interface tab (the path to perfspi.log). This view includes three panes:

   - Event pane — top center
   - Detail event pane — below the Event pane
   - Tree logger pane — to the left of the Event pane

      You can use the tree logger pane to filter the messages in the event pane.

   The event pane is constantly changing, showing the most recent message as it arrives in `prspi.log`, and additional information about that message in the detail event pane.

▶   If the log file is truncated and archived, Chainsaw may stop scrolling messages. If this happens, restart Chainsaw.

Log File Analyzer

Use the Log File Analyzer to display:

- A daily summary of warnings produced by processes within each extension package
- A daily summary of errors produced by processes within each extension package
- Timing data for selected processes within each extension package

Follow these steps:

1   Open the Log File Analyzer:

   Start > All Programs > HP > NNM iSPI for Performance > Log File Analyzer

2   Review warnings and errors.

The summary data for warnings and errors covers the previous two weeks. The last summary, covering today, will be incomplete. The summary data indicates:

- Date

- Number of errors per process, if any

- Number of warnings per process, if any

A warning normally indicates a transient condition, usually a temporary mismatch, that will self-correct. If you see a warning message or an error message, you may want to examine it in more detail by viewing the associated logfile in a text editor.

3   Scroll down past the summary of warnings and errors to see timing data. Timing data shows:

- Total number of times a process executed over the previous two weeks

- Average execution time per process over the previous two weeks

- Standard deviation

- Maximum execution time per process over the previous two weeks

- Average number of records processed per execution

- Average number of records processed per second

Diagnostic Reports

The Self Diagnostics extension pack contains the following reports:

- Calendar
- Chart Detail
- Heat Chart
- Managed Inventory
- Most Changed
- Peak Period
- Top N
- Top 10 Task Duration
- Top N Chart

These reports monitor trends related to the duration of NPS processes. For details about report contents, see online help.

Diagnostic Collector

You can use the diagnostic collector to gather diagnostic information from different log files. To gather the diagnostic information, follow these steps:

1   Log on to the NPS system with the administrative privileges.

2   Start the diagnostic collector:

Start > All Programs > HP > NNM iSPI for Performance > Diagnostic Collector

The diagnostic collector collects different log files and combines them into the `DiagnosticFilesYYYYMMDD_HHMMSS.tar.gz` file, which is placed into the following directory:

`%NPSDataDir%\collectDiag`

You can send the `tar.gz` file to HP Support while investigating a problem.

Changing the Defaults for Performance Polling

When you install the NPS, some performance polling is enabled for you, automatically. If your polling requirements are different from the defaults, the defaults must be changed. Changing the defaults is an NNMi console task.

To change the performance polling defaults for a node group, use the Node Settings form. To access this form from the NNMi console, select:

Workspaces > Configuration > Monitoring Configuration > Node Settings

If you need help changing performance polling defaults, refer to the following help topic in the Administration section of online help for the NPS:

Setting Performance Polling in NNMi

Setting Thresholds for Exceptions

Although several NPS reports monitor exceptions, data about exceptions will be missing from these reports until thresholds for performance metrics are set in NNMi. There are no default thresholds, so no thresholds are set for you automatically. Setting thresholds is a manual step.

To avoid generating too many exceptions, or too many incidents related to threshold conditions, set thresholds that will flag *abnormal* behavior. You can develop a better understanding of abnormal behavior by studying variance in NPS reports.

When you are ready to set thresholds, use the **Threshold Settings** tab on the **Node Settings** form. If you need help with this task, refer to the following topic in the Administration section of online help for the NPS:

Setting Thresholds in NNMi

NPS provides you the baseline metrics to define the normal (expected) range of values for any given metric. The baselines metrics enable you to forecast the future value for a given metric based on the historical data.

NNMi supplies the upper normal value based on values that you enter in the Threshold Configuration form. You can disable the upper normal value if you do not require to set the upper threshold for the metric.

See *Online Help for Administrators* for information about Threshold Configuration form.

Changing the Admin Password for the BI Server

You can launch the Report Menu from the NNMi console if you log on (to the NNMi console) as an administrator. If the Single Sign-On authentication feature of NNMi does not work, you can launch the NPS Report Menu with the following steps:

1 Launch the following URL:

   http://<FQDN_of_NPS_system>:9300/p2pd/NPS.html

2 Click the BI Server tab on the navigation panel, and then select Log On as BI Server Administrator.

3 Set the namespace to `ErsAuthenticationProvider` (the default setting). Do not set the namespace to the other option (`ErsTrustedSignonProvider`).

4 Click **OK**.

5 Log on with the user name `ErsAdmin`.

We recommend changing the default password for BI Server (`ErsAdmin`) promptly, soon after installation. Follow these steps:

1 Navigate to this directory: %NPSInstallDir%\bin

2 Type the following command, followed by your new password:

   changeBIpwd.ovpl *<newpassword>*

3 The system displays the following message:

   ErsAdmin password set successfully.

Configuring Third party Certifying Authority for BI Server

NPS uses HTTPS with Secure Sockets Layer (SSL) for additional security for the transmissions between NNM iSPI Performance for Metrics server and the client web browser. To use SSL communication, the BI Server requires authorized public keys (certificates). By default, BI Server components use a built-in Certificate Authority (CA) service to establish the root of trust in its security infrastructure. However, in an environment, where the client web browser does not use the built-in Certificate Authority, configure BI Server to use 3rd party CA following these steps:

1 Under $cfg{cognos_home}\configuration create the following folders:

   — Folder to store the signed keypairs: `$cfg{cognos_home}\configuration\`*<Folder Name>*

      For example, `$cfg{cognos_home}\configuration\MySigning`

   — Folder to store the encrypted keypairs:
      `$cfg{cognos_home}\configuration\`*<Folder Name>*

      For example, `$cfg{cognos_home}\configuration\MyEncryption`

   ▶ The variable $cfg{cognos_home} is defined in the runtime configuration file – `NNMPerformanceSPI.cfg`.

2 Backup the `$cfg{cognos_home}\configuration\cogstartup.xml` file.

3 Start IBM Cognos Configuration utility.

4　From the **File** menu, select **Export As** to export the configuration in clear text.

5　The configuration utility prompts you to specify a filename to save the configuration. Name the file as `cogstartup.xml`, overwriting the existing file.

6　Stop BI Server using the following command from the following location:

`stopBI.ovpl`

7　Navigate to `$cfg{cognos_home}\bin` folder.

8　Use the following command to create the keystore and export the Certificate Signing Requests (CSR) to sign the certificates. Make sure that you specify values for every parameter.

ThirdPartyCertificateTool.bat -java:local -c -s -d "CN=*<FQDN of the BI server host>*, OU=*<OrganizationUnit>*, O=*<Organization>*, L=*<System Location>*, ST=*<State>*, c=*<Country>*" -r sign.csr -D ..\configuration*<Name of the folder created in step 1 to store the signed keypairs>* -p *<Password to access the keystore>*

Example

```
ThirdPartyCertificateTool.bat  -java:local -c -s -d
"CN=BISystem.usa.abc.com, OU=NPSsigning, O=cognos, L=Bethesda,
ST=Maryland, c=US" -r sign.csr -D ..\configuration\MySigning -p
admin1234
```

9　Use the following command to create the keystrore and export the CSR to encrypt certificate. Make sure that you specify values for every parameter.

ThirdPartyCertificateTool.bat -java:local -c -e -d "CN=*<FQDN of the BI server host>*, OU=*<Organization Unit>*, O=*<Organization>*, L=*<System Location>*, ST=*<State>*, c=*<Country>*" -r encrypt.csr -D ..\configuration*<Name of the folder created in step 1 to store the encrypted keypairs>* -p *<Password to access the keystore>*

Example

```
ThirdPartyCertificateTool.bat -java:local -c -e -d
"CN=BISystem.usa.abc.com, OU=NPSencrypt, O=cognos, L=Bethesda,
ST=Maryland, c=US" -r encrypt.csr -D ..\configuration\MyEncryption -p
admin1234
```

10　The following files are generated:

—　sign.csr

—　encrypt.csr

11　Send the `encrypt.csr` and `sign.csr` files generated in the `$cfg{cognos_home}\bin` folder to to your CA to get the following signed certificates:

—　sign.cer

—　encrypt.cer

⚐　ThirdPartyCertificateTool command requires the certificate files to be in PEM (Base64 encoded ASCII) format. If you received these files in a different format (although almost every CA supports exporting to PEM format), convert them to the PEM format. Follow the instructions specific your CA, to convert the certificate files. This task may require additional steps.

12 Save the `sign.cer` and `encrypt.cer` files in the `$cfg{cognos_home}\bin` folder.

13 Save the root certificate for your CA in the `$cfg{cognos_home}\bin` folder as `CAroot.cer`.

14 Save the intermediate certificate for your CA in the `$cfg{cognos_home}\bin` folder as `CAintermediate.cer`.

15 Create a CA chain certificate by combining the root certificate and the intermidiate certificate. For example, **cat CAintermediate.cer CAroot.cer > CAchain.cer**

16 Import the signed certificate file `sign.cer` into the built-in CA's keystores using the following command:

ThirdPartyCertificateTool.bat -java:local -i -s -r sign.cer -D ..\configuration*<Name of the folder created in step 1 to store the signed keypairs>* -p *<Password to access the keystore>* -t *<Chain certificate file name>*

17 Import the signed certificate `encrypt.cer` into the built-in CA's keystores using the following command:

ThirdPartyCertificateTool.bat -java:local -i -e -r encrypt.cer -D ..\configuration*<Name of the folder created in step 1 to store the encrypted keypairs>* -p *<Password to access the keystore>* -t *<Chain certificate file name>*

18 Create a truststore and import the root certificate for the CA in the truststore using the following command:

ThirdPartyCertificateTool.bat -java:local -i -T -r *<Root certificate file name>* -D ..\configuration*<Name of the folder created in step 1 to store the signed keypairs>* -p root

The command imports the root certificate for the CA in the `jCAKeystore` file in the folder where you store the signed keypairs.

The command uses the password "root" to import the root certificate.

19 Import the intermediate certificate for the CA into the truststore using the following command:

ThirdPartyCertificateTool.bat -java:local -i -T -r *<Intermidiate certificate file name>* -D ..\configuration*<Name of the folder created in step 1 to store the signed keypairs>* -p root

The command imports the root certificate for the CA in the `jCAKeystore` file in the folder where you store the signed keypairs.

The command uses the password "root" to import the root certificate.

20 Start IBM Cognos Configuration utility.

21 Configure the following properties to match the values you typed in the command line utility:

   a **Signing key store location:** Specify the name of the folder created in step 1 to store the signed keypairs. For example, $cfg{cognos_home}/MySigning

   b Signing key store password: Specify the password created to access the keystore. For example, admin1234

   c Encryption key store location: Specify the name of the folder created in step 1 to store the encrypted keypairs. For example, $cfg{cognos_home}/MyEncryption

      d   Encryption key store password: Specify the password created to access the keystore. For example, admin1234

      e   Use Third Party CA: Set this property to **true**

      f   Certificate Authority key store password: Specify the password created to access the root certificate. For example, root

22 From the File menu, click **Save** to save the configuration.

23 Start BI Server.

6 Licensing

To obtain a permanent license, acquire a password for a permanent license, and then install the license password using Autopass License Management. Install the license password on the NNMi server, not on the NPS system, even if the NPS is installed on a dedicated server.

➤ If you acquired a license for an iSPI other than the NNM iSPI Performance for Metrics, you will not be able to use the features of the NNM iSPI Performance for Metrics after the 30-day evaluation period is over. To use the capabilities of the NNM iSPI Performance for Metrics with NPS, you must separately acquire the licenses for the NNM iSPI Performance for Metrics.

Do not modify any of the report templates provided with the iSPI products (modified report templates will not be supported).

Acquiring a Permanent License for the NNM iSPI Performance for Metrics

Follow these steps to acquire a permanent license for the NNM iSPI Performance for Metrics:

1   Gather the following information:

 a   HP product number and order number (these numbers are on the Entitlement Certificate)

 b   IP address of the NNMi management server

 c   Your company or organization information

2   At a command prompt, run the following command:

 `%NnmInstallDir%\bin\nnmlicense.ovpl PerfSPI -g`

3   The Autopass License Management window opens. In the **License Password** dialog box, click **Request License**.

4   Install the license password by following the instructions in the window.

Alternatively, to apply the permanent license with a text file, follow these steps:

1   Obtain the HP product number and order number (these numbers are on the Entitlement Certificate).

2   Open a text file with a text editor, and then type the license password in the text file.

3   Save the text file.

4   On the NNMi management server, run the following command:

 %NnmInstallDir%\bin\nnmlicense.ovpl PerfSPI -f *<license_text_file>*

Acquiring Additional License Passwords for the NNM iSPI Performance for Metrics

Contact your HP Sales Representative or your Authorized Hewlett-Packard Reseller for information about the NNM licensing structure and to learn how to add license tiers for enterprise installations.

To obtain additional license passwords, go to the HP password delivery service:

https://webware.hp.com/welcome.asp

Restrictions Regarding 3rd-Party Software

- The following restrictions apply to the BI Server Software:
  - You cannot have more than one Administrator at one time.
  - You cannot have more than 5 simultaneous users of Query Studio.
  - You cannot extend the iSPI data model, or add additional data sources to the iSPI system.
  - You cannot use the Report Studio, Analysis Studio, Metric Studio, and Event Studio features with the NNM iSPI Performance for Metrics license.
- The Sybase IQ Software is provided as the embedded database for the NPS. Other uses of the Sybase IQ Software are not permitted.

7 Upgrading the NNM iSPI Performance for Metrics

You can upgrade the NNM iSPI Performance for Metrics from the version 8.13 to 9.00 and from 9.00 to 9.10. The version 9.10 of the NNM iSPI Performance for Metrics is supported with the NNMi 9.10. Before upgrading, you must make sure NNMi is upgraded to 9.10.

Before starting the upgrade, make sure that you back up all NPS data using the following command:

On Windows:

```
%NPSInstallDir%\NNMPerformanceSPI\bin\backup.ovpl -b <dir> -f
```

Upgrading on the NNMi Management Server

If the version 9.00 of the NNM iSPI Performance for Metrics is installed on the NNMi management server, follow these steps:

1   Make sure NNMi has been upgraded to 9.10.

2   Log on to the management server with the administrative privileges.

3   Make sure all the prerequisites are met (Prerequisites on page 13).

4   Follow the instructions in Installing the NPS on page 19.

If you are using NNM iSPI Performance for Metrics 8.13:

Before upgrading to NNM iSPI Performance for Metrics 9.10, upgrade to NNM iSPI Performance for Metrics 9.00.

Upgrading on a Dedicated Server

If the version 9.00 of the NNM iSPI Performance for Metrics is installed on a dedicated server, follow these steps:

1   Make sure NNMi has been upgraded to 9.10.

2   Log on to the NNMi management server with the administrative privileges.

3   Run the enablement script by following the instructions in Running the Enablement Script on page 27.

4   Log on to the NNM iSPI Performance for Metrics server with the administrative privileges.

5   Make sure all the prerequisites are met (Prerequisites and Planning on page 13).

6   Follow the instructions in page 29.

If you are using NNM iSPI Performance for Metrics 8.13:

Before upgrading to NNM iSPI Performance for Metrics 9.10, upgrade to NNM iSPI Performance for Metrics 9.00.

Upgrading on a Dedicated Server in a High Availability Cluster (HA "standalone")

1   Make sure NNMi has been upgraded to 9.10.

2   Log on to the NNMi management server with administrative privileges.

3   Run the enablement script by following the instructions in Running the Enablement Script on page 27. Make sure that you use the hostname of the HA cluster when prompted for hostname.

4   Log on to a node in your NPS cluster with administrative privileges

5   Identify the currently active node in your HA cluster using the following command:

%installdir%\misc\nnm\ha\nnmhaclusterinfo.ovpl PerfSPIHA -group <resource_group> -activeNode

6   To prevent failover during the upgrade process create the following maintenance file on the active server:

%NnmDataDir%\hacluster\<resource_group>\maintenance

7   On each inactive node in the cluster:

a   Log on to NPS with administrative privileges.

b   Make sure all the prerequisites are met (Prerequisites and Planning on page 13).

c   Temporarily remove the node from the HA cluster by running the following command:

%installdir%\misc\nnm\ha\nnmhaunconfigure.ovpl PerfSPIHA <resource_group>

Follow the instructions in page 29 for upgrading on a dedicated non HA server. Make sure that the upgrade completes without errors. .

Do not reconfigure HA until after the primary node has been upgraded.

8   Run the following command before upgrading NPS:

%installdir%\NNMPerformanceSPI\bin\stopALL.ovpl

9   When you have completed upgrading all inactive nodes, return to the active node and follow the instructions in page 29 for upgrading on a dedicated non HA server. Make sure that the upgrade completes without errors.

10 When this is complete, remove the following file:

%NnmDataDir%\hacluster\<resource_group>\maintenance

11 On each inactive node in the cluster:

a   Log on to NPS with administrative privileges

b   Run the following command before configuring HA:

%installdir%\NNMPerformanceSPI\bin\stopALL.ovpl

c   Reinstate the node into the HA cluster by running the following command:

%installdir%\misc\nnm\ha\nnmhaconfigure.ovpl PerfSPIHA

Upgrading on the NNMi Management Server in a High Availability cluster (HA "add on")

1   Ensure that the NNMi 9.0x configuration is consistent across all HA nodes by forcing a failover, in turn, to each of the passive nodes.

2   Determine which node in the NNMi 9.0x HA cluster is active:

%NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl -group <resource_group> -activeNode

The remainder of this procedure refers to the currently active node as server X and the currently passive node as server Y

3   On server Y, upgrade NNMi:

a   Disable HA resource group monitoring by creating the following maintenance file:

%NnmDataDir%\hacluster\<resource_group>\maintenance

The file can be empty.

b   Upgrade NNMi to the current version as described in *Upgrading from NNMi 9.0x* section in *HP Network Node Manager i Software Deployment Reference*.

c   Verify that the upgrade completed without error.

d   To upgrade NPS in add-on mode, make sure all the prerequisites are met (Prerequisites and Planning on page 13).

e   Temporarily remove the node from the HA cluster by running the following command:

%installdir%\misc\nnm\ha\nnmhaunconfigure.ovpl NNM –addon PerfSPIHA

f   Follow the instructions for upgrading on the NNMi Management Server in non HA server.

g   When the upgrade completes, stop all SPI processes by opening a new shell and running the following command:

%installdir%\NNMPerformanceSPI\bin\stopALL.ovpl

⚠   **Do not** reconfigure HA until after the primary node has been upgraded.

h   Delete the maintenance file:

%NnmDataDir%\hacluster\<resource_group>\maintenance

4   If the HA cluster includes multiple passive nodes, repeat step 3 for each passive node.

5   Return to the active server X before upgrading. Make sure that you have completed the pre-requisites before upgrading NPS on the NNMi Management Server in non HA server (Prerequisites on page 13).

6   Perform these tasks on each inactive node in the cluster:

    a   Log on to NPS with administrative privileges

    b   Reinstate the node into the HA cluster by running the following command:

        %installdir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon PerfSPIHA

    c   When this is complete remove the maintenance file from the active server:

        %NnmDataDir%\hacluster\<resource_group>\maintenance

7   Continue upgrading the active NNMi server.

8   On server X, upgrade NNMi:

    a   Force a failover to server Y.

        The NNMi database on the shared disk is upgraded to the format of the new NNMi product version at this time.

    b   Disable HA resource group monitoring by creating the following maintenance file:

        %NnmDataDir%\hacluster\<resource_group>\maintenance

        The file can be empty.

    c   Upgrade NNMi to the current version as described in *Upgrading from NNMi 9.0x* section in *HP Network Node Manager i Software Deployment Reference*.

    d   Verify that the upgrade completed without error.

    e   Upgrade all add-on NNM iSPIs to version 9.10.

        For information, see the documentation for each NNM iSPI.

    f   Delete the maintenance file:

        %NnmDataDir%\hacluster\<resource_group>\maintenance

9   Optional. Force a failover from server Y to server X so that the node that was active before the upgrade process is again the active node.

8 Installation Problems

Problem: Installer fails with the error *Problem occurred while initializing variables*

Details:

This problem is seen on Windows systems.

Solution:

Remove the contents of the *%TEMP%* directory, restart the system, and then start the installer.

Problem: Installer shows WARNING messages as a result of running system checks.

Details:

While you may continue with the installation despite warning messages, it is strongly recommended that the problems are corrected before proceeding. Warnings are displayed if system recommendations are not met. Clicking on the name of the individual installation check allows you to see more details. See the *Installation Guide*, Prerequisites and Planning on page 13, for more information.

Solutions:

Depends on warnings found

Problem: Installer shows ERROR messages as a result of running system checks.

Details:

You will not be allowed to continue with the installation if the minimum system requirements have not been met. You must correct these problems before proceeding to install.

Clicking on the name of the individual installation check allows you to see more details. See the *Installation Guide*, Prerequisites and Planning on page 13, for more information.

Solutions:

Depends on errors found

Problem: NNMi is not installed on machine, yet installer displays an ERROR message for NNMi Version check, indicating that NNMi version is incorrect.

Details:

Installer check details pane shows the following message:

```
Checking to see NNM Version supported...
```

```
Need to check to see NNM Version supported.

Running NNM Version check

/tmp/HPNNMPerformanceSPI/AppCheckNNMVersion.sh: line 24: /opt/OV/nonOV/perl/
a/bin/perl: No such file or directory

ERROR: NNM version not OK

NNM Version is not supported
```

Solutions:

Check to see if the following file exists: *%NPSDataDir%*/NNMVersionInfo. If it does and NNMi is definitely not installed on the system, it must be a remnant of a previously installed version and can be safely removed.

Problem: Installation takes a long time.

Details:

The installer can take up to 2 hours to complete on some systems, with most of the time being taken while installing the BI Server and ExtensionPacks. If the splash screens periodically change, and if the hourglass icon on the bottom-right corner rotates, the installer is not hung.

Solutions:

Allow the installer to proceed to completion.

Problem: NNMi console's Action menu has no link to Reporting - Report menu.

Details:

The enablement script was not run.

Solutions:

Run the nnmenableperfspi.ovpl script. See Running the Enablement Script on page 27

9 NNMi Application Failover

➤ The NPS does not support the application failover feature, but is compatible with the NNMi management server that is installed in the application failover setup.

If NNMi is installed and configured in the application failover setup, you must install the NPS on a dedicated server and not on the NNMi management server. If you want configure a redundant solution for the NPS, you must install the NPS in an HA cluster.

Application Failover for NNMi ensures redundancy by allowing a secondary NNMi server to take over immediately after a primary NNMi server fails. Application Failover relies on the clustering technology, a shared certificate that must be copied from NNMi to the NPS, and ongoing file system synchronization.

Except for a minor service interruption lasting about 15 minutes, Application Failover is transparent. Users will not notice that a failover took place and there are no special tasks for the NPS administrator to perform.

The ability of the NPS to support application failover depends on files the NPS retrieves from the primary server in the cluster. As soon as the NPS has these files, it begins monitoring the status of the primary server by checking for status changes every 5 minutes. If the NPS detects a status change, the NPS:

- Determines which server in the cluster is the new primary server

- Redirects data collection to a shared directory on the new primary server

- Begins collecting data (metrics and topology files) from the new primary

Immediately after these events take place, NPS users will be able to link from the NPS to NNMi views on the new primary server, just as they were able to do before the failover took place.

Application Failover

If you are running NNMi in an Application Failover cluster:

1 Run the enablement script once on the active NNMi server and once on each standby server in the cluster.

2 When you run the enablement script on the standby server, provide the same responses you provided when you ran the enablement script on the active server.

3 Later, if you choose to install permanent licenses for the NNM iSPI Performance for Metrics, be sure to install identical licenses on every server in the cluster.

Copying the Keystore File from NNM to the NPS

Follow these steps to copy the cluster.keystore certificate from NNMi to the NPS:

1 Go to following directory on the NNMi management server:

NNMi on Windows

`%NnmDataDir%\shared\nnm\conf\nnmcluster\cluster.keystore`

2 Copy the `cluster.keystore` file from the above location to the following directory on the NPS system:

`%NnmDataDir%\NNMPerformanceSPI\nnmappfailover\keystore`

A Performing a Silent Install

To perform a silent install on an unattended system, you need an initialization file that contains the correct parameters. An initialization file with the correct parameters is created when you do a normal install. You also have the option of creating your own initialization file using the following template:

```
[NONOV.OvTomcatA]
ShutdownPort=8005
Jk2Ajp13Port=8009

[installer.properties]
setup=HPNNMPerformanceSPI
licenseAgreement=true
group=Default
media=E:\packages\
appRevision=9.10.000
tempDir=C:\Documents and Settings\Administrator\Local Settings\Temp\
customFeatureSelected=NNMPerfSPI MetricsExtensionPacks
installDir=C:\Program Files (x86)\HP\HP BTO Software\
customLangSelected= en
dataDir=C:\Documents and Settings\All Users\Application Data\HP\HP BTO Soft-
ware\
systemDir=C:\WINDOWS\system32
appDescription=HP NNM iSPI for Performance
systemLocale=English
```

If you want to install only the NPS without enabling the NNM iSPI Performance for Metrics, set the `customFeatureSelected` parameter to only `NNMPerfSPI`.

Set the `media` parameter to the path to the packages directory (present on the media root) from the mount point on the system.

Alternatively, you can use the `ovinstallparams<time_stamp>.ini` file created during the installation of the NPS.

To run a silent install, follow these steps:

1   To create and use the ini file that you created with the template, follow these steps:

   a   Using the template, create your own ini file and give it this name:

      `ovinstallparams.ini`

   b   Copy the file to the `%TEMP%\` folder on the target system.

2   To use the ini file create by another NPS installation, follow these steps:

a   Collect the ini file (`ovinstallparams<`*`time_stamp`*`>.ini`) from the source system (the system where the NPS is already installed).)

The path to the ini file is:

`%TEMP%\HPOvInstaller\HPNNMPerformanceSPI_9.10.000`

b   Make necessary modifications to the file. If you want to install only the NPS without enabling the NNM iSPI Performance for Metrics, set the `customFeatureSelected` parameter to only `NNMPerfSPI`. Set the `media` parameter to the path to the packages directory (present on the media root) from the mount point on the system.

c   Remove the time stamp from the file name; change the file name to:

`ovinstallparams.ini`

d   Copy the file to the `%TEMP%\` folder on the target system.

3   Log on to the target system as administrator.

4   Insert the NPS DVD in the DVD-ROM drive on the target system and enter the following command at the command prompt:

<*DVD_drive*>`\setup.exe -i silent`

5   The silent install begins. There is no progress indicator.

6   To confirm a successful install, check the latest installation log file.

a   Navigate to:

`%TEMP%\HPOvInstaller\HPNNMPerformanceSPI_9.10.000`

b   Open this file:

`HPNNMPerformanceSPI_9.10.000_<timestamp>_HPOvInstallerLog.html`

c   If the install was successful, the last line is *Successfully completed.*