HP Network Node Manager iSPI Performance for Metrics

for the Linux operating system

Software Version: 9.20

Installation Guide

Document Release Date: November 2014
Software Release Date: May 2012

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

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:

- Apache software, version 1.1, copyright© 2000 The Apache Software Foundation. All rights reserved.
- Apache, version 2.0, January 2004. The Apache Software Foundation.
- GNU Lesser General Public License, version 2, copyright© 1989, 1991 Free Software Foundation, Inc.
- GNU Lesser General Public License, version 2.1, copyright© 1991, 1999 Free Software Foundation, Inc.
- GNU lesser General Public License, version 3, copyright© 2007 Free Software Foundation, Inc.
- IBM Cognos Business Intelligence 10.1.1. Copyright© International Business Machines Corporation 2010. All rights reserved.
- IPA Font v1.0, IPA
- libjpeg library, copyright© 1991-1998, Thomas G. Lane.
- libpng versions 1.2.5 through 1.2.10, copyright 2004, 2006© Glenn Randers-Pehrson.
- libxml2 library, copyright© 1998-2003 Daniel Veillard. All Rights Reserved.
- libxp library, copyright© 2001,2003 Keith Packard.
- The “New” BSD License, copyright© 2005-2008, The Dojo Foundation. All rights reserved.
- PacketProxy, copyright© 2002-2010, Daniel Stoedle, Yellow Lemon Software. All rights reserved.
- 7-Zip, copyright© 1999-2011 Igor Pavlov.

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 used with Network Node Manager i (NNMi) software to analyze the performance characteristics of your network. With the performance data collected by the HP Network Node Manager i Software Smart Plug-ins (iSPIs), NPS builds data tables, runs queries in response to user selections, and displays query results in web-based reports that enable you to diagnose and troubleshoot problems in your network environment.

The HP NNM iSPI Performance for Metrics (NNM iSPI Performance) software provides core performance management capability to NNMi by gathering and monitoring the metric data polled by NNMi from different network elements. The combination of NNMi and NNM iSPI Performance enables you monitor the operational performance of your network infrastructure.

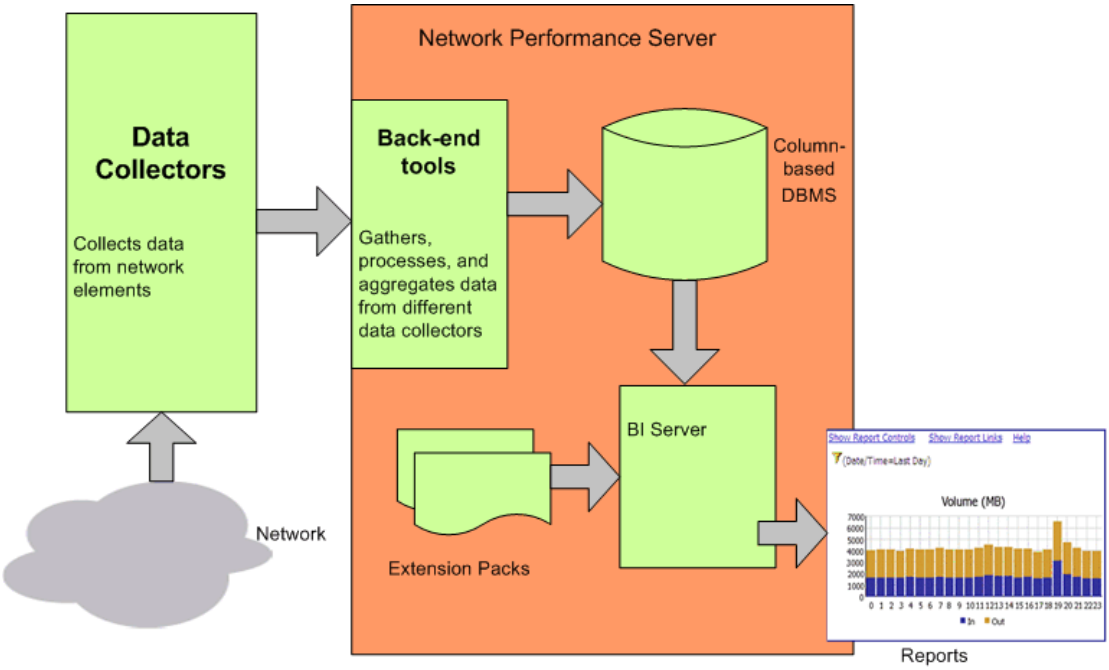
NPS provides the infrastructure and resources for other iSPI Performance products—for example, HP NNM iSPI Performance for Traffic and HP NNM iSPI Performance for Quality Assurance—to generate reports. If you do not want to use NNM iSPI Performance, you can install NPS without enabling it. When NPS is installed in your environment, you can generate reports with any other iSPI Performance product.

When you install NNM iSPI Performance, the installer activates an instant-on license. The instant-on license remains active for 30 days. After that, you cannot use NNM iSPI Performance until you purchase and activate a permanent license. You can, however, continue to use the NPS infrastructure with other iSPI Performance products if the licenses of those other products are active.

Overview of Architecture

NPS provides the infrastructure for storing, processing, and analyzing the data obtained from different network elements by NNMi or custom collectors (available with the iSPIs). After gathering the data, NPS processes and aggregates and stores it into the column-based database management system (DBMS). The business intelligence framework (BI Server) provides the foundation for analyzing data and reporting. The BI Server's analysis tools enable you to view ready-to-use reports that indicate the performance of network elements available in your environment.

High-Level View of NPS Architecture



NPS Components

NPS consists of the following.

- **Column-based DBMS**

  The column-based DBMS adds data warehousing capability to the NPS solution. The DBMS can store a large amount of data that is gathered from different sources, and enables NPS to compute aggregates from a large number of data points. You can store daily aggregated data for up to 800 days, hourly aggregated data for up to 400 days, and raw/detailed data for up to 400 days. The backup and restore feature enables you to save your data in a compressed, backed-up format. You can use the saved data to restore the database after a system or disk crash.

- **Content Store**

  The content store is a relational database (RDBMS) used to store report templates, schedules, schedule output, user created report content, and user and group information. It is a much smaller scale than the the column-based DBMS. Data is generally retained indefinitely, except for scheduled output where retention policies are set within the schedule itself. The content store can be backed up and restored.

- **Business Intelligence Server**

  The Business Intelligence (BI) Server enables you to generate insightful, web-based reports from the data in the DBMS with the help of pre-defined report templates. You can design and save non-default, ad hoc queries and background report schedules. You can publish scheduled reports on the BI Server portal and configure the BI Server to e-mail the scheduled reports.

- **Extension Packs**

Extension Packs provide rules and definitions for generating reports from the data. The default, ready-to-use Extension Packs available with NPS, the Self Diagnostics Extension Pack, helps you view reports that indicate the health and performance of various NPS components and processes.

Installation Overview

You can install NPS on the NNMi management server or on a dedicated, standalone server. To choose an option that suits your requirements, see the sizing guidelines published in the *HP Network Node Manager i Software Smart Plug-in Performance for Metrics/Network Performance Server System and Device Support Matrix*.

The upgrade guidelines are:

- Any version prior to 9.00: First upgrade to version 9.00 and then upgrade to 9.20.
- Version 9.00, 9.10, 9.11: Upgrade to version 9.20.

Installing on a Dedicated Server

This option requires you to perform additional configuration steps using the following utilities:

- **Enablement script** (made available on the NNMi management server by the NNMi installer) – Facilitates communication between NNMi and NPS, installs an instant-on license, and creates NNMi menu items.
- **Configuration utility** – Enables you to specify information that helps NPS processes communicate with the NNMi management server.

Installing on the NNMi Management Server

With this option, you only need to run the installer program.

The installer gives you the option to install NNM iSPI Performance at the same time that you install NPS. Or you can install it later.

Location of Installed Files

The NPS installer installs necessary files into the following directories:

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

Additional Product Information

For information on using the product, see the NNM iSPI Performance online help. A PDF version of the online help is provided on the product software DVD.

Information about NNMi can be found in the *Network Node Manager i Software Deployment Reference*, *Network Node Manager i Software Release Notes,* and *Network Node Manager i Software Support Matrix*.

2 Prerequisites and Planning

Before beginning the installation, make sure that all the prerequisites are met. Evaluate your requirements, identify the most suitable installation option for your environment, and create a step-by-step plan for the installation.

Prerequisites

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

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

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

- **Port availability**

  See Ports Information on page 62 for a list of ports used for different processes. Make sure that these ports are free. To see the list of used ports on the system, run the netstat command.

- **Required libraries**

  NPS uses several 32-bit software components. The following libraries are required:

  - `compat-libstdc++-296.i386`
  - `compat-libstdc++-33-3.2.3-61.i386`
  - `compat-libstdc++-33-3.2.3-61.x86_64`
  - `libjpeg.i386`
  - `libjpeg.x86_64`
  - `libpng.i386 libpng.x86_64`
  - `libXp.i386`
  - `libXp.x86_64`
  - `libXtst-1.0.1-3.1.i386`
  - `libXtst-1.0.1-3.1.x86_64`
  - `ncurses.i386`
  - `ncurses.x86_64`
  - `openmotif22.i386`
  - `openmotif22.x86_64`
  - `tcsh-6.14`
  - `unixODBC.i386`
  - `unixODBC.x86_64`
  - `unixODBC-devel.i386`

— `unixODBC-devel.x86_64`

To verify that the necessary libraries are available on the system:

a. Make sure the system is connected to the Internet and set up to work with Red Hat Network updates.

b. Log on to the system with root privileges.

c. To check that all the required libraries are installed, run the following command:

```
yum list
```

If any libraries are missing or old, run the following command:

```
yum install <libraries>
```

Replace <libraries> with the missing library name.

d. Type **Y** to install and update packages.

- **IPv4 address in the hosts file**

  The hosts file (in the `/etc` directory) must include at least one IPv4 address for localhost.

- **HP Public Key**

  If you are installing NNM iSPI Performance for Metrics 9.20 on a Linux NNMi management server, you must import the HP public key into the Linux RPM database before installing NNM iSPI Performance for Metrics 9.20. To do this, point your browser to the following location and follow the instructions: https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning

  If a dialog box appears during the NNM iSPI Performance for Metrics installation stating that the code signing key could not be found, do the following:

  a. Leave the dialog box displayed while completing step 2.

  b. Follow the instructions shown at https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning

  c. Click **No** on the dialog box to resume the NNM iSPI Performance for Metrics[1] installation.

Planning the Installation

An installation plan prepares you for the installation process and helps you gather all the information required to complete the installation. You should review the requirements, choose whether to install on the management server or on a dedicated server, and create a plan.

NNMi Version

Upgrade NNMi to version 9.20 before installing NPS.

To verify the version of NNMi:

1. Log on to the NNMi console.

1.

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

The version number should be 9.20.

Platform Combination

To install on a dedicated server, make sure that the platform combination of NPS and management server is supported. Use an NNMi management server that runs on one of the following operating systems:

- Windows
- Red Hat Enterprise Linux (RHEL)
- SUSE Linux: Only NNMi is supported, not NPS.
- HP-UX: Only NNMi is supported, not NPS.
- Solaris: Only NNMi is supported, not NPS.

For more information on supported operating systems, see the *HP Network Node Manager iSPI Performance for Metrics System and Device Support Matrix*.

File Sharing Mechanism

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

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

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

The NNMi management server shares the necessary files with NPS using network file system (NFS) protocol.

If you are using Security-Enhanced Linux (SELinux), make sure that the security settings are configured to allow NFS and automount.

Domain Names

When you install 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, mycompany.com. Membership in different subdomains 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.mycompany.com
- nps.reporting.mycompany.com

Pre-Installation Checklist

Task	Reference Document/Topic	Complete (Y/N)
Select an installation option: on the management server or a dedicated server	*Network Performance Server Support Matrix*	
Verify that versions 8.01, 8.10, and 8.11 of the iSPI for Performance are not installed on the system where you want to install NPS.		
Verify that the NNMi version is 9.20.		
Verify that NNMi is not configured with an instance of the iSPI for Performance. For example, look for menu items on the NNMi interface.		
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 a dedicated server installation: Verify that you selected a supported platform combination.	Platform Combination on page 15	
Only for a dedicated server installation: Verify that the management server and dedicated server belong to the same DNS domain. Note the fully qualified domain name of the dedicated server.	Domain Names on page 15	
Only for a dedicated server installation: To use security-enabled Linux as an NNMi management server, you must configure the security policies to make exceptions for NFS traffic on the SELinux management server.	Platform Combination on page 15	
Only for a dedicated server installation: To use a Linux management server, and firewalls are configured on either server or the network, you must modify the firewall settings to make exceptions for NFS traffic.		

Single Sign-On

Installing NPS enables a security mechanism known as Single Sign-on (SSO). SSO allows NPS to recognize the same user names and passwords 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 logging on a second time. By default, SSO is not configured.

For SSO to work, NPS and NNMi must share the same domain name. 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.

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

If NNMi and 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 NPS on a Dedicated Server

To install NPS on a dedicated server, you must run the enablement script on the NNMi management server and the installer program on the dedicated server.

Global Network Management

If NNMi is deployed in a Global Network Management (GNM) environment, you must do the following:

- Deploy one instance of NPS for each NNMi management server. Every regional manager and the global manager must have separate instances of NPS installed and deployed.
- Run the enablement script once on every regional manager and on the global manager.

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

If you are installing NPS or NNM iSPI Performance using terminal server session or remote desktop connection, do **not** download the ISO image to any of the following drive types:

- Network drive
- Detachable media

Enabling NPS on the NNMi Management Server

Make sure that the NNMi version is 9.20. The NNMi installer places the enablement script on the management server.

The script does the following when it runs on the NNMi management server:

- Depending on your selection, enables the Instant-On license for NNM iSPI Performance.
- Adds an HP NNM iSPI Performance > 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 Single Sign-On security for NPS.

To enable NPS, follow these steps:

1. Log on to the NNMi management server with root privileges.
2. Go to /opt/OV/bin
3. Run the nnmenableperfspi.ovpl script. The script starts operating in interactive mode and displays the following message:

   ```
   Do you want to also enable the iSPI Performance for Metrics evaluation license?
   ```

4. Type **Y** and press **Enter**.

   Selecting N causes the Extension Packs for NNM iSPI Performance to remain disabled (even during an upgrade).

The script displays the following message:

```
Would you like to begin?
```

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

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

7 Type the FQDN and press **Enter**.

Use only the FQDN. Do not use the IP address.

To install and configure NPS in an HA cluster, you must specify the virtual hostname of the cluster and run this script after the NPS HA resource group is configured and started. The script displays the following message:

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

8 Type **N**.

Or

To enable SSL for NPS (see Enabling Secured Transmission for NPS on page 45), type **Y**.

The script displays the following message:

```
The default port for the iSPI is 9300.
Press [return] to use this port.
```

9 Press **Enter**. The script prompts you to share drive space from the management server.

10 Choose the following file sharing option:

NFS share: Choose this option because you are using the Linux NPS installation media.

The script creates a share in the following location:

```
/var/opt/OV/shared/perfSpi/datafiles
```

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

11 The enablement script enables Single Sign-On security for NPS.

Note: The **`nnmenableperfspi.ovpl`** script does not ask you to provide the user name of a new user.

The enablement script stops. The Next Steps section displays the shared path (to be accessed by NPS).

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

Installing NPS

Follow these steps:

1 Log on with root privileges.

2 Insert the NPS installation media into the DVD drive.

3 Make sure the DVD-ROM drive is mounted. Use the cd command to change to the `/cdrom` directory.

4 From the media root, run the following command:

```
./setup.bin
```

The installation wizard opens.

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

5 Select **I accept the terms** and click **Next**. The Select Features page opens. This page offers you the option to install NPS without enabling NNM iSPI Performance.

6 To use NNM iSPI Performance, select the NNM iSPI Performance for Metrics–ExtensionPacks checkbox. Otherwise, clear the checkbox so the installer does not enable it.

Click **Next**.

The installer program initiates the system-checking process and verifies that system requirements are met.

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

8 Click **Install**. The installation process begins.

9 Toward the end of the installation process, the Configuration Utility opens.

Follow these steps:

a 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.

b Specify the detailed data archive retention period. Depending on the system resource, choose a value for this parameter.

The default retention periods are the following:

— Daily Data = 800 days

— Hourly Data = 70 days

— Raw/Detailed Data = 14 days

c Click **Apply**.

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

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

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=/disk/packages/
appRevision=9.20.000
tempDir=/tmp/
tempDir=/var/tmp/
customFeatureSelected=NNMPerfSPI MetricsExtensionPacks
installDir=/opt/OV/
customLangSelected= en
dataDir=/var/opt/OV/
systemDir=/usr/local/bin
appDescription=HP NNM iSPI for Performance
systemLocale=English
```

To install only NPS without enabling NNM iSPI Performance, 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 NPS.

To run a silent install, follow these steps:

1. Create and use the ini file you created with the template as follows:
   a. Using the template, create your own ini file and give it the following name:

      `ovinstallparams.ini`

   b. Copy the file to the `/var/tmp` folder on the target system.
2. Use the ini file created by another NPS installation as follows:
   a. Collect the ini file (`ovinstallparams<time_stamp>.ini`) from the source system (the system where NPS is already installed).)

      The path to the ini file is:

      `/tmp/HPOvInstaller/HPNNMPerformanceSPI_9.20.000`

   b. Make any necessary modifications to the file. To install only NPS without enabling NNM iSPI Performance, 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 and change the file name to:

      `ovinstallparams.ini`

   d. Copy the file to the `/var/tmp` folder on the target system.
3. Log on to the target system as root.
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.bin -i silent`

   The silent install begins. There is no progress indicator.
5. Confirm a successful install by checking the latest installation log file as follows:
   a. Navigate to:

      `/tmp/HPOvInstaller/HPNNMPerformanceSPI_9.20.000`

b Open the following file:

`HPNNMPerformanceSPI_9.20.000_<timestamp>_HPOvInstallerLog.html`

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

Verifying Error-Free Installation

Perform the following to verify that NPS was installed without errors.

Locate Application Files and Runtime Files

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

- `bin`
- `config`
- `Docs`
- `extensionpacks`
- `Installation`
- `java`
- `lib`
- `L10N`
- `PATCHES`
- `build.info` (a text file that contains the date of the NPS software build)
- `patch.info` (text file)

The default path to the dynamic runtime files is `opt/OV/NNMPerformanceSPI`.

The `/var/opt/OV/NNMPerformanceSPI` directory in the default path to the dynamic runtime files contains the following folders:

- `contentstore`
- `database`
- `logs`
- `nnmappfailover`
- `rconfig`
- `PerfSPI_Diagnostics`
- `AtmPvc_Health`
- `Component_Health`
- `FrameRelayPvc_Health`
- `Interface_Health`
- `temp`

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

Validate the Configuration File

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

To launch the configuration checker, follow these steps:

1 Go to the following directory:

```
/opt/OV/NNMPerformanceSPI/bin
```

2 Type the following command:

```
./checkConfig.ovpl
```

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

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

Time Zone

You must set the time zone to UTC or to a geographic time zone using /usr/bin/system-config-date.

Configuring NPS with the Configuration Utility

You can change the following parameters:

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

Follow these steps:

1 Launch the Configuration Utility:

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

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

3 Make any of the following changes:

- 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 data files directory.
- Modify the default retention period for archive table data. The default retention periods are the following:
  - Daily Data = 800 days
  - Hourly Data = 70 days
  - Raw/Detailed Data = 14 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 might be required to delay restarting.

Upgrading NPS on the Dedicated Server

You can upgrade NPS from versions 9.00 and greater to 9.20. To upgrade from versions prior to 9.00, you must first upgrade to version 9.00.

NPS 9.20 is supported with NNMi 9.20. Before upgrading, make sure that NNMi is upgraded to 9.20.

Before starting the upgrade, back up all NPS data using the following command:

```
/opt/OV/NNMPerformanceSPI/bin/backup.ovpl -b <dir>
```

If you created Report Views for scheduled reports, the views will be saved during the upgrade. Schedules, jobs, and queries made using Query Studio will also be saved. Shortcuts and other object types, however, will not be saved. Check the log entries in the `Migration.log` file, which can be found in the log directory, to see the results of the upgrade.

To upgrade NPS on the dedicated server, follow these steps:

1 Make sure that the NNMi version is 9.20.

2 Make sure that all scheduled reports are stopped from running during the upgrade (see The content store can hang during upgrade when the database is in use for scheduled jobs or reports. on page 54).

3 Log on to the NNMi management server with root privileges.

4 Run the enablement script by following the instructions in Enabling NPS on the NNMi Management Server on page 18.

5 Log on to the NNM iSPI Performance server with root privileges.

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

7 Follow the instructions in Installing NPS on page 19.

Upgrading the Database Indexes

NPS 9.20 provides a new database column index scheme that can improve report query performance when the report has a topology attribute filter applied and that attribute has more than 65,535 unique values.

To upgrade your database to use the new indexing scheme, run the following command:

```
dbCheckIndexes.ovpl -r
```

Be aware that, if you have a large database, the script could take several hours to run.

Disabling NPS on the NNMi Management Server

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

To disable NPS on the NNMi management server, follow these steps:

1. Make sure NNMi is running.
2. Log on to the NNMi management server with root privileges.
3. Go to /opt/ov/bin.
4. Run the nnmdisableperfspi.ovpl script.
5. Log on to the dedicated server with root 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 click **Continue**.
7. A welcome page opens. Click **OK**.
8. On the Application Maintenance page, select **Uninstall**, and click **Next**. The Pre-Uninstallation Summary page opens.
9. Click **Uninstall**. The program starts uninstalling NPS from the system.
10. When the program completely removes NPS, click **Done**. The removal process removes all the components of NPS from the system.

Uninstalling NPS from the Dedicated Server

To continue to use the reports created by different iSPI Performance products, you should not remove NPS. You cannot use reports if NPS is not available.

To remove NPS, follow these steps:

1. Log on to the NNMi management server with root privileges.
2. Go to /opt/OV/bin.
3. Run the nnmdisableperfspi.ovpl script.
4. Log on to the dedicated server with root privileges.
5. From the command prompt, run the following command:

   `/opt/OV/Uninstall/HPNNMPerformanceSPI/setup.bin`

   The wizard opens.

   If the Application requirement check warnings dialog box opens, review the warning messages, take appropriate actions, and click **Continue**.
6. A welcome page opens. Click **OK**.
7. On the Application Maintenance page, select **Uninstall**, and click **Next**. The Pre-Uninstallation Summary page opens.
8. Click **Uninstall**. The program starts uninstalling NPS from the system.

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

Reinstalling NPS after Uninstalling

To avoid problems with subsequent reinstallations, follow these steps:

1 Restart the server.

2 Verify that the /opt/ov/NNMPerformanceSPI folder is removed.

Installing NNM iSPI Performance

Skip this section if you installed NNM iSPI Performance when you installed NPS.

If NNMi and NPS are installed in an HA cluster, perform the following steps only on the active node:

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

2 Run the nnmenableperfspi.ovpl enablement script from the `/opt/OV/bin` directory. Answer **Y** to the following question:

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

3 Log on to the NPS system with root privileges.

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

5 On the Maintenance Selection page, select **Modify.**

6 Follow the on-screen instructions.

On the Select Features page, select the NNM iSPI Performance for Metrics–ExtensionPacks checkbox. The installer installs NNM iSPI Performance on the system.

Alternatively, run the following command from the `/opt/OV/NNMPerformanceSPI/bin` directory on the NPS system:

```
./metricsExtensionPacks.ovpl install
```

On each passive node, follow these steps:

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

2 Run the enablement script from the `/opt/OV/bin` directory. Answer **Y** to the following:

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

From the active node, copy all the properties files (with the .properties extension) from the following directory and transfer those files to the same directory on the passive node:

```
/opt/OV/nonOV/cognos/bi/webapps/PerfSpi/WEB-INF/classes/com/hp/ov/perfspi
```

Disabling NNM iSPI Performance

You can use NPS with other iSPI Performance products without using NNM iSPI Performance. To disable NNM iSPI Performance without uninstalling NPS, follow these steps:

1. Log in to the NNMi management server with root privileges.
2. From the NPS media, run the `setup.bin` file.
3. On the Maintenance Selection page, select **Modify**.
4. Follow the on-screen instructions.
5. On the Select Features page, clear the NNM iSPI Performance for Metrics–ExtensionPacks checkbox and wait for the process to complete.

Alternatively, you can run the following command from the `/opt/OV/NNMPerformanceSPI/bin` directory:

```
metricsExtensionPacks.ovpl uninstall
```

4 Installing NPS on the NNMi Management Server

Before you begin the installation process, make sure that NNMi is running on the server. the NNMi version must be 9.20.

If NNMi is deployed in a Global Network Management (GNM) environment, you must do the following:

- Deploy one instance of NPS for each NNMi management server. Every regional manager and the global manager must have separate instances of NPS installed and deployed.
- Run the enablement script once on every regional manager and on the global manager.

If you do not have the NPS software 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 DVD, you need to install a software application designed to burn ISO image files.

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

- Network drive
- Detachable media

Installing NPS

Follow these steps:

1. Log on to the management server with root privileges.
2. Insert the NPS installation media into the DVD drive.
3. Make sure the DVD-ROM drive is mounted, and use the cd command to change to the mounted media directory.
4. From the media root, run the following command:

   ```
   ./setup.bin
   ```

   The installation wizard opens.

   If the application requirement check warnings dialog box opens, review the warning messages, take appropriate action, and click **Continue**.
5. On the Introduction page, click **Next**. The Product Agreement page opens.
6. Select **I accept the terms** and click **Next**. The Select Features page opens. This page offers you the option to install NPS without enabling NNM iSPI Performance.
7. Select the NNM iSPI Performance for Metrics–ExtensionPacks check box. Or, clear the check box so the installer does not install NNM iSPI Performance.
8. Click **Next**. The installer program initiates the system-checking process and verifies that system requirements are met.
9. When the installation check succeeds, click **Next**. The Pre-Install Summary page opens.

10 Click **Install**. The installation process begins.

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

Custom Collection Extension Pack

If you created a custom collection Extension Pack, follow these steps:

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

```
/opt/OV/nonOV/cognos/bi/webapps/PerfSpi/WEB-INF/classes/com/hp/ov/perfspi
```

2 Copy all the files with the .properties extension in the directory, and transfer them 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 configuration for secured transmission, port number, and digital certificates.

Time Zone

You must set the time zone to UTC or to a geographic time zone using /usr/bin/system-config-date.

Configuring NPS with the Configuration Utility

See the instructions in Configuring NPS with the Configuration Utility on page 23.

Upgrading NPS on the NNMi Management Server

Before starting the upgrade, back up all NPS data using the following command:

```
/opt/OV/NNMPerformanceSPI/bin/backup.ovpl -b <dir>
```

If you created Report Views for scheduled reports, the views will be saved during the upgrade. Schedules, jobs, and queries made using Query Studio will also be saved. Shortcuts and other object types, however, will not be saved. Check the log entries in the `Migration.log` file, which can be found in the log directory, to see the results of the upgrade.

To upgrade NPS on the NNMi management server, follow these steps:

1 Make sure that the NNMi version is 9.20.

2 Make sure that all scheduled reports are stopped from running during the upgrade (The content store can hang during upgrade when the database is in use for scheduled jobs or reports. on page 54).

3 Log on to the management server with root privileges.

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

5 Follow the instructions in Installing NPS on page 28.

Upgrading the Database Indexes

NPS 9.20 provides a new database column index scheme that can improve report query performance when the report has a topology attribute filter applied and that attribute has more than 65,535 unique values.

To upgrade your database to use the new indexing scheme, run the following command:

```
dbCheckIndexes.ovpl -r
```

Be aware that, if you have a large database, the script could take several hours to run.

Uninstalling NPS from the NNMi Management Server

To continue to use the reports created by different iSPI Performance products, you should not remove NPS. You cannot use reports if NPS is not available.

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

1. Log on to the management server with root privileges.
2. Make sure NNMi is running.
3. From the command prompt, run the following command:

   ```
   /opt/OV/Uninstall/HPNNMPerformanceSPI/setup.bin
   ```

   The wizard opens.

   If the "Application requirement check warnings" dialog box opens, review the warning messages, take the appropriate action, and click **Continue**. A welcome page opens.
4. Click **OK**.
5. On the Application Maintenance page, select **Uninstall** and click **Next**. The Pre-Uninstallation Summary page opens.
6. Click **Uninstall**. The program starts uninstalling NPS from the system.
7. When the program completely removes NPS, click **Done**.

Reinstalling NPS after Uninstalling

To avoid problems with subsequent reinstallations, follow these steps:

1. Restart the Linux server.
2. Verify that the `opt/ov/NNMPerformanceSPI` folder is removed.

Installing NNM iSPI Performance

Skip this task if you installed NNM iSPI Performance when you installed NPS.

1. Log on to the NNMi management server with root privileges.
2. From the NPS media, run the `setup.bin` file.
3. Select **Modify** on the Maintenance Selection page.

4 Follow the on-screen instructions.

On the Select Features page, select the NNM iSPI Performance for Metrics–ExtensionPacks checkbox and wait for the installer to finish.

Alternatively, run the following command from the `/opt/OV/NNMPerformanceSPI/bin` directory on the NPS system:

```
metricsExtensionPacks.ovpl install
```

Disabling NNM iSPI Performance

You can use NPS with other iSPI Performance products without using NNM iSPI Performance. You can disable it without uninstalling NPS.

1 Log in to the NNMi management server with root privileges.

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

3 On the Maintenance Selection page, select **Modify**.

4 Follow the on-screen instructions.

5 On the Select Features page, clear the NNM iSPI Performance for Metrics–ExtensionPacks checkbox. The installer disables the HP NNM NNM iSPI Performance on the system.

Alternatively, you can run the following command from the /opt/OV/NNMPerformanceSPI/bin directory:

```
metricsExtensionPacks.ovpl uninstall
```

5 Installing NPS on a Dedicated Server in a High Availability Environment

Before you can install NPS in an HA environment, you must complete the following additional steps on NNMi:

1. Log on to the management servers with root privileges.
2. Open the `/etc/exports` file with a text editor.
3. Add the physical nodes of the NPS cluster in the following format:

   ```
   /var/opt/OV/shared/perfSpi/datafiles
   <node1>.domain.com(rw,sync,no_root_squash)
   /var/opt/OV/shared/perfSpi/datafiles
   <node2>.domain.com(rw,sync,no_root_squash)
   ```

   You can introduce a physical node using a line break.
4. Save the file.
5. Run the following command:

   ```
   exportfs -a
   ```

You can choose one of the following deployment options to install NPS:

- Option A: Install Only NPS in an HA Cluster
- Option B: Only the NNMi Management Server is in an HA Cluster

Option A: Install Only NPS in an HA Cluster

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

1. Configure the HA cluster on the system where you want to install 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. You can select any name; for example, NPSLinuxHA.
   - File system type, disk group, and volume group for the shared file system
   - Mount point of the NPS shared disk

   For more information about the NMS High Availability package used by NPS, see "Configuring NNMi in a High Availability Cluster" in the *Network Node Manager i Software Deployment Reference*.
3. Without running the enablement script on the NNMi management server, install NPS on the primary node in the cluster according starting on page 18, but do not start the ETL service.
4. On the primary node, follow these steps:

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

   `/opt/OV/NNMPerformanceSPI/bin/stopALL.ovpl`

b. Make sure the shared disk is mounted.

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

   `/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl PerfSPIHA`

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

d. Verify the configuration by running the following command:

   `/opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl -group <resource_group> -nodes`

   The local node should be listed.

   `/opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl -config PerfSPIHA -get PerfSPI_HA_CONFIGURED`

   The command should display `YES`.

   Make sure that the following folders were created:

   – `$OVDataDir/NNMPerofrmanceSPI_HA_Backupdir`, including all subfolders

   – `$MountPoint/NNMPerformanceSPI/dataDir/NNMPerformanceSPI`

e. Unmount the mount point.

Note: On a Veritas Linux, cluster, NNMPerformanceSPI_HA_Backupdir will still exist in the NPS data directory even after NPS is unconfigured.

5. Bring the NPS HA resource group online by running the following command:

   `/opt/OV/misc/nnm/ha/nnmhastartrg.ovpl PerfSPIHA <resource_group>`

6. Run the enablement script on the NNMi management server (see Enabling NPS on the NNMi Management Server on page 18 and pay special attention to the instructions for HA configuration). While running the enablement script, provide the virtual hostname of the NPS cluster. Write down the NNMi data path printed out at the end of running the enablement script.

7. Modify the NNMi data path using the output from step 6 by running /opt/OV/NNMPerformanceSPI/bin/runConfigurationGUI.ovpl.

8. Restart the HA group by running the following command:

   `/opt/OV/misc/nnm/ha/nnmhastoprg.ovpl PerfSPIHA <resource_group>` and `/opt/OV/misc/nnm/ha/nnmhastartrg.ovpl PerfSPIHA <resource_group>`

9. Install NPS on each passive node in the cluster according to the instructions beginning on page 18, but do not start the NPS service.

   If NPS is already installed on the passive node, stop the NPS service.

10. On each passive node, run the following command:

    `/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl PerfSPIHA`

    Note the following exceptions for the previous steps:

    — The data does not need to be copied to the shared disk because this was already done when the first node was configured. The service is already started.

    — Connect to the cluster will be lost when the primary node stops. It will reconnect.

— The following services will start running again. During this time, you can access the node through the virtual interface.
  – HP NNM iSPI Performance BI service
  – HP NNM iSPI Performance Database or DB SQL Rewrite Proxy process
  – HP NNM iSPI Performance ETL service

If you created a custom collection Extension Pack, do the following:

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

`/opt/OV/nonOV/cognos/bi/webapps/PerfSpi/WEB-INF/classes/com/hp/ov/perfspi`

2 From the active node, copy all of the properties files that are in the directory and transfer them to the same directory on each passive NPS system.

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

In this scenario, you must run the enablement script (Enabling NPS on the NNMi Management Server on page 18) once on the active NNMi management server, and once on every passive NNMi management server. Then install NPS.

Configuring HA

The following instructions explain how to configure HA when NNMi is not installed.

To configure the first node, follow these steps:

1 Run the following command:

`/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl PerfSPIHA`

2 When prompted, enter the following names:
  — Valid virtual host
  — Disk type
  — Disk group
  — Volume group
  — Directory where the disk will be mounted

3 Run the nnmmount command.

The resource group is created.

4 Stop all resources by running the stopALL.ovpl command.

5 Once everything stops, run the following command to unconfigure NPS:

`/opt/OV/misc/nnm/ha/nnmhaunconfigure.ovpl PerfSPIHA`

6 Rerun `/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl PerfSPIHA`.

7 Answer the questions posed by the script.

8 At the question, “Is this a distributed installation? (Y/N),” answer **N**.

It could take some time to copy the local NPS directories to the shared directories.

You will see information about the mount point, a symbolic link created for PerfSPI_DataDir, unmounting shared disk ready for starting resource group.

9 Start using the resource group using the following command:

```
/opt/OV/misc/nnm/ha/nnmhastartrg.ovpl PerfSPIHA
```

You will be able to see the progress of the resource groups as they come online.

10 Once everything is on line, run the statusALL.ovpl command to find which processes and services are running. This can take some time.

To configure the second node:

1 Follow the previous steps, and be aware of the following differences:

- This time, the data does not need to be copied to the shared disk because this was already done when the first node was configured. The product is already started.
- Connection will be lost to the cluster when the primary node stops. It will, however, reconnect.
- The following services will start running again:
  - HP NNM iSPI Performance BI service
  - HP NNM iSPI Performance Database and/or DB SQL Rewrite Proxy process
  - HP NNM iSPI Performance ETL Service
- During this time, you can access the node through the virtual interface.
- There will be a gap while the switch occurs, but the underlying service will be available.

Uninstalling NPS from an HA Cluster

First remove NPS from all passive nodes and then from the active node.

Follow these steps:

1 On each passive node:

a Log on to the node with root privileges.

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

```
/opt/OV/misc/nnm/ha/nnmhaunconfigure.ovpl PerfSPIHA <resource_group>
```

c Run the following command to stop all NPS processes:

```
/opt/OV/NNMPerformanceSPI/bin/stopALL.ovpl
```

d Follow the instructions in Uninstalling NPS from the Dedicated Server on page 25.

e Repeat for each passive node.

2 On the active node:

a Log on to the node with root privileges.

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

```
/opt/OV/misc/nnm/ha/nnmhastoprg.ovpl PerfSPIHA <resource_group>
```

c Run the following command to stop all NPS processes:

```
/opt/OV/NNMPerformanceSPI/bin/stopALL.ovpl
```

d Follow the instructions in Uninstalling NPS from the Dedicated Server on page 25.

Installing NNM iSPI Performance

Skip this task if you installed NNM iSPI Performance when you installed NPS.

On the active node only, follow these steps:

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

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

3 Select **Modify** on the Maintenance Selection page.

4 Follow the on-screen instructions.

Select the NNM iSPI Performance for Metrics–ExtensionPacks checkbox on the Select Features page. The installer installs NNM iSPI Performance on the system.

Alternatively, you can run the following command from the `/opt/OV/NNMPerformanceSPI/bin` directory:

```
metricsExtensionPacks.ovpl install
```

On each passive node, follow these steps:

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

2 Run the nnmenableperfspi.ovpl enablement script from the `/opt/OV/bin` directory.

Answer **Y** to the following question:

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

3 From the active node, copy all the files with the .properties extension from the following directory and transfer them to the same directory on the passive node:

```
/opt/OV/nonOV/cognos/bi/webapps/PerfSpi/WEB-INF/classes/com/hp/ov/perfspi
```

Disabling NNM iSPI Performance

You can use NPS with other iSPI Performance products without using NNM iSPI Performance. You can disable NNM iSPI Performance without uninstalling NPS.

On the active node only, follow these steps:

1 Log in to the NNMi management server with root privileges.

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

3 On the Maintenance Selection page, select **Modify**.

4 Follow the on-screen instructions.

5 On the Select Features page, clear the NNM iSPI Performance for Metrics–ExtensionPacks checkbox. The installer disables NNM iSPI Performance on the system.

   Alternatively, run the following command from the `/opt/OV/NNMPerformanceSPI/bin` directory:

   ```
   metricsExtensionPacks.ovpl uninstall
   ```

On each passive node, follow these steps:

1 Log in to the NNMi management server with root privileges.

2 Run the enablement script from the `/opt/OV/bin` directory.

3 Answer **N** to the following question:

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

6 Installing NPS on the NNMi Management Server in a High Availability Environment (HA "Add On")

Installing NPS

When NNMi is installed in an HA environment, you can install and configure NPS as an add-on product on the NNMi management server.

Follow these steps:

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

   ```
   ovstatus -c
   ```

2. On an active node, install NPS according to the instructions in Installing NPS on page 28.

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

4. Run the following command on the active node:

   ```
   /opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon PerfSPIHA
   ```

   The nnmhaconfigure.ovpl command is interactive and requires you to specify details related to the HA environment. For more information about this command, see "Configuring NNMi in a High Availability Cluster" in the *Network Node Manager i Software Deployment Reference*.

5. Verify the configuration by running the following command:

   ```
   /opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -get
   NNM_ADD_ON_PRODUCTS
   ```

   You should see `PerfSPIHA`.

6. On each passive node, install NPS according to the instructions in Installing NPS on page 28.

7. Stop NPS by running the stopALL.ovpl command.

8. Run the following command on each passive node:

   ```
   /opt/OV/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. For more information on this command, see the *Network Node Manager i Software Deployment Reference*.

9. Verify the configuration by running the following command on each passive node:

   ```
   /opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -get
   NNM_ADD_ON_PRODUCTS
   ```

   You should see `PerfSPIHA`.

Uninstalling NPS from an HA Cluster

First remove NPS from all passive nodes, and then from the active node.

On each passive node, follow these steps:

1. Log on with root privileges.
2. Run the following command to disable the HA configuration for NPS on the passive NNMi management server:

   ```
   /opt/OV/misc/nnm/ha/nnmhaunconfigure.ovpl NNM -addon PerfSPIHA
   ```

3. Run the following command to stop all NPS processes:

   ```
   /opt/OV/NNMPerformanceSPI/bin/stopALL.ovpl
   ```

4. Follow the instructions in Uninstalling NPS from the NNMi Management Server on page 30.

On the active node, follow these steps:

1. Log on with root privileges.
2. Run the following command to disable the HA configuration for NPS on the active NNMi management server:

   ```
   /opt/OV/misc/nnm/ha/nnmhaunconfigure.ovpl NNM -addon PerfSPIHA
   ```

3. Run the following command to stop all NPS processes:

   ```
   /opt/OV/NNMPerformanceSPI/bin/stopALL.ovpl
   ```

4. Follow the instructions in Uninstalling NPS from the NNMi Management Server on page 30 to remove NPS.

Installing NNM iSPI Performance

Skip this task if you installed NNM iSPI Performance when you installed NPS.

On the active node only, follow these steps:

1. Log on to the NNMi management server with root privileges.
2. From the NPS media, run the `setup.bin` file.
3. Select **Modify** on the Maintenance Selection page.
4. Follow the on-screen instructions.
5. Select the NNM iSPI Performance for Metrics–ExtensionPacks checkbox on the Select Features page. The installer installs NNM iSPI Performance on the system.

   Alternatively, you can run the following command from the `/opt/OV/NNMPerformanceSPI/bin` directory:

   ```
   metricsExtensionPacks.ovpl install
   ```

On each passive node, follow these steps:

1. Log on to the NNMi management server with root privileges.
2. Run the nnmenableperfspi.ovpl enablement script from the `/opt/OV/bin` directory.

3 Answer **Y** to the following question:

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

4 From the active node, copy all the files with the .properties extension from the following directory and transfer them to the same directory on the passive node:

```
/opt/OV/nonOV/cognos/bi/webapps/PerfSpi/WEB-INF/classes/com/hp/ov/perfspi
```

Disabling NNM iSPI Performance

You can use NPS with other iSPI Performance products without using NNM iSPI Performance. You can disable NNM iSPI Performance without uninstalling NPS.

On the active node only, follow these steps:

1 Log in to the NNMi management server with root privileges.

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

3 On the Maintenance Selection page, select **Modify**.

4 Follow the on-screen instructions.

5 On the Select Features page, clear the NNM iSPI Performance for Metrics–ExtensionPacks checkbox. The installer disables NNM iSPI Performance on the system.

Alternatively, you can run the following command from the `/opt/OV/NNMPerformanceSPI/bin` directory:

```
metricsExtensionPacks.ovpl uninstall
```

On each passive node, follow these steps:

1 Log in to the NNMi management server with root privileges.

2 Run the enablement script from the `/opt/OV/bin` directory.

3 Answer **N** to the following question:

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

7 Upgrading in a High Availability Environment

Before starting the upgrade, back up all NPS data using the backup.ovpl script:

```
%NNMInstallDir%/NNMPerformanceSPI/bin/backup.ovpl -b <backupdir>
```

All metrics data are preserved during the upgrade. ReportViews for scheduled reports, and schedules, jobs, and reports made using Query Studio are also saved. Shortcuts and other object types, however, are not saved.

To see which objects are migrated, check the log entries in the `Migration.log` file, which can be found in the `NNMPerformancelogs` directory after upgrading.

Make sure that the NNMi version is 9.20.

Make sure that all scheduled reports are stopped from running during the upgrade (The content store can hang during upgrade when the database is in use for scheduled jobs or reports. on page 54).

Note: There is an absolute limit on the amount of time a node takes to start the applications configured within the resource group. The default setting in NNMi and NPS version 9.0 was 15 minutes, but the default setting in NNMi and NPS version 9.20 has changed. You might, therefore, have to increase the timeout value, especially in an “add-on” environment where both NNMi and NPS have to be started.

To increase the timeout limit, run the following commands:

```
/opt/VRTSvcs/bin/haconf -makerw
/opt/VRTSvcs/bin/hares -modify <resource_group>-app OnlineTimeout 1800
/opt/VRTSvcs/bin/haconf -dump -makero
```

Scenario 1: NNMi and NPS on Same Server in Cluster

In this scenario, both NNMi and NPS are installed on the same server in a shared cluster (also known as co-located or “add-on”).

The following procedure is similar, but not identical, to the procedure for upgrading NNM in an HA environment.

Follow these steps:

1. Log in to a cluster node as a user with administrative privileges.
2. Identify the active server by running the following command:

   ```
   %NNMInstallDir%/misc/nnm/ha/nnmhaclusterinfo.ovpl -group
   <resourcegroupname> -activeNode
   ```
3. Log in to the active node.
4. Enable maintenance mode on the active node.
5. Upgrade NNM.
6. Upgrade NPS while it is still configured as part of the HA cluster.

Do not clear maintenance mode on the active node until inactive nodes are completed.

Upgrade NNM and NPS on all inactive nodes as follows:

7 Enter maintenance mode.

8 Upgrade NNM.

9 Make sure that all NPS processes are stopped.

On an inactive node, stopALL.ovpl will not work. Use the service control panel to make sure that all NNM iSPI Performance services are stopped.

10 Unconfigure HA by running the following command:

```
%NNMInstallDir%/misc/nnm/ha/nnmhaunconfigure.ovpl NNM –addon PerfSPIHA
```

11 Upgrade NPS while it is NOT configured as part of the HA cluster.

Repeat steps 7-11 for each inactive node.

After upgrading all inactive nodes, return to the active node.

Make sure that the active node's HA configuration is updated by unconfiguring and then reconfiguring HA.

12 Unconfigure HA by running the following command:

```
%NNMInstallDir%/misc/nnm/ha/nnmhaunconfigure.ovpl NNM –addon PerfSPIHA
```

13 Reconfigure HA with the following command:

```
%NNMInstallDir%/misc/nnm/ha/nnmhaconfigure.ovpl NNM –addon PerfSPIHA
```

14 Remove maintenance mode.

Proceed to reconfigure HA on all inactive nodes:

15 Reconfigure HA with the following command:

```
%NNMInstallDir%/misc/nnm/ha/nnmhaconfigure.ovpl NNM –addon PerfSPIHA
```

16 Remove maintenance mode.

All nodes should now have both NNM and NPS version 9.20

Scenario 2: On a Dedicated Server (or "Standalone")

Follow these steps:

1 Log in to a cluster node as a user with administrative privileges.

2 Identify the active server by running the following command:

```
%NNMInstallDir%/misc/nnm/ha/nnmhaclusterinfo.ovpl -group
<resourcegroupname> -activeNode
```

3 Log in to the active node.

4 Enable maintenance mode on the active node.

5 Upgrade NPS while it is still configured as part of the HA cluster.

Proceed to upgrade NPS on all inactive nodes, as follows:

6 Enter maintenance mode.

7 Make sure that all NPS processes are stopped.

On an inactive node, stopALL.ovpl will not work. Use the service control panel to make sure that all NNM iSPI Performance services are stopped.

8 Unconfigure HA with the following command:

```
%NNMInstallDir%/misc/nnm/ha/nnmhaunconfigure.ovpl PerfSPIHA
<resourcegroupname>
```

9 Upgrade NPS while it is NOT configured as part of the HA cluster.

Repeat steps 6-8 for each inactive node.

After upgrading all inactive nodes, return to the active node.

Make sure that the active node's HA configuration is updated by unconfiguring then reconfiguring HA.

10 Unconfigure HA with the following command:

```
%NNMInstallDir%/misc/nnm/ha/nnmhaunconfigure.ovpl NNM -addon PerfSPIHA
```

11 Reconfigure HA with the following command:

```
%NNMInstallDir%/misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon PerfSPIHA
```

12 Remove maintenance mode.

Proceed to reconfigure HA on all inactive nodes:

13 Reconfigure HA with the following command:

```
%NNMInstallDir%/misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon PerfSPIHA
```

14 Remove maintenance mode.

All nodes should now have NPS version 9.20

Upgrading the Database Indexes

NPS 9.20 provides a new database column index scheme that can improve report query performance when the report has a topology attribute filter applied and that attribute has more than 65,535 unique values.

To upgrade your database to use the new indexing scheme, run the following command:

```
dbCheckIndexes.ovpl -r
```

Be aware that, if you have a large database, the script could take several hours to run.

8 Using the Configuration Utility

You can change the following parameters:

- Path to the NNM data files folder
- Data retention

Follow these steps:

1. Launch the Configuration Utility:

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

2. Click **Stop**. (Stops data processing and table creation.)
3. Make any of the following changes:
   - 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 data files directory.
   - Modify the default retention period for archive table data. The default retention periods are the following:
     - Daily Data = 800 days
     - Hourly Data = 70 days
     - Raw/Detailed Data = 14 days
4. Click **Apply**.
5. Click **Start**.
6. Click **Exit**.

You must restart the service to have your changes take effect.

9 Enabling Secured Transmission for NPS

This is an optional procedure.

After installing NPS, you can specify whether it should use HTTPS (secured transmission) rather than HTTP, which is the default mode. NPS and NNMi can use different modes of transmission. By default, NNMi enables secured transmission during installation, but you can also use HTTP.

To enable HTTPS on NPS, you must run a script after installation. NPS uses HTTP over an SSL (Secure Sockets Layer) connection. This provides additional security between the NNM iSPI Performance server and the client web browser.

You can run the following command to enable, disable, or configure secured transmission for NPS:

```
configureWebAccess.ovpl
```

The command stops the BI Server. Any reports that are running will fail.

A number of information messages are displayed. This is normal.

The command uses the following port numbers:

- HTTP: 9300
- HTTPS: 9305

To enable, disable, or configure the HTTP and HTTPS ports, follow these steps:

1. Run the following command from the following location:

   ```
   /opt/OV/NNMPerformanceSPI/bin/configureWebAccess.ovpl
   ```

2. Respond to the messages displayed by the utility.

   If the utility fails, check the log files at `/var/opt/OV/NNMPerformanceSPI/logs/`.

Check that HTTPS is Enabled

Run the following command:

```
configureWebAccess.ovpl -h
```

The utility displays the mode of transmission, either HTTP or HTTPS.

Do not use any of the NPS ports reserved for non-HTTP/HTTPS traffic:

- 9301
- 9302
- 9303
- 9304
- 9306
- 9307

Do not use the default port for HTTP traffic (9300) for HTTPS.

The BI Server uses a built-in Certificate Authority (CA) for secured transmission.

Secured Transmission in an HA Environment

Secured transmission must be enabled on all the nodes in the cluster. But before you can configure a node, you must set maintenance mode for it. When you finish configuring the node, unset maintenance mode. Make sure all hosts in the same HA group have the same configuration. They must use the same protocol, port number, and certificate.

To set maintenance mode in NPS, follow these steps:

1. Go to the online node in the cluster.
2. Run the following command to set maintenance mode:

   ```
   /opt/ov/bin/haMaintenance.ovpl 1
   ```

3. Configure SSL.
4. Run the following command to unset maintenance mode:

   ```
   /opt/ov/bin/haMaintenance.ovpl 0
   ```

10 Troubleshooting

Troubleshooting NPS

The following diagnostic tools are provided to ensure trouble-free operation of NPS.

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 file contains every message generated since the previous night at midnight. The path to the file is:

```
/var/opt/OV/NNMPerformanceSPI/logs/prspi.log
```

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

1. Open the Log File Monitor.
   a. cd to the following directory: `/opt/OV/NNMPerformanceSPI/bin`
   b. Type the following command: `./runChainsaw.ovpl`
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 – Left of the Event pane

   You can use the tree logger pane to filter 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 might stop scrolling messages. If this happens, restart Chainsaw.

Log File Analyzer

The Log File Analyzer provides the following:

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

Follow these steps:

1. Open the Log File Analyzer:
   a. Go to the following directory: `/opt/OV/NNMPerformanceSPI/bin`
   b. Type the following command: `./log_analyzer.ovpl`
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 might want to examine it in more detail by viewing the associated log file 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 Chart
- Top N
- Top 10 Task Duration

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

2 Start the diagnostic collector:

a Go to the following directory: `/opt/OV/NNMPerformanceSPI/bin`

b Type the following command: `./collectDiagnostics.ovpl`

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

`/var/opt/OV/NNMPerformanceSPI/collectDiag`

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

Changing the Defaults for Performance Polling

When you install 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, see the online help for 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, see the online help for NPS ("Setting Thresholds in NNMi").

NPS provides the baseline metrics to define the normal (expected) range of values for any given metric. The baseline 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 you enter in the Threshold Configuration form. You can disable the upper normal value if you do not need to set the upper threshold for the metric. For more information about the Threshold Configuration form, see the online help for Administrators.

Setting Baselines

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

If NNMi is not configured for baseline metrics, some of the charts that are based on the baseline metrics will be empty in standard reports. This could be confusing to users.

More information about baseline metrics and how to configure them can be found in the "Baseline Metrics Glossary" topic in the NNM iSPI Performance online help and in the "Configure Baseline Settings for Interfaces" topic of the HP Network Node Manager iSPI Performance for Metrics online help.

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 as follows:

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 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.

HP recommends changing the default password (ErsAdmin) promptly after installation. Follow these steps:

1. Navigate to /opt/OV/NNMPerfornanceSPI/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.`

BI Server Does Not Start after Backup

When the content store database does not start in a timely fashion, the BI Server can time out.

Follow these steps:

1. Stop all services by running the stopALL.ovpl command.
2. Restart the BI Server by running the startBI.ovpl command.

Restrictions on BI Server Software

- You cannot have more than one Administrator at one time.
- You cannot have more than five 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 license.

Error message: “the dispatcher is still initializing”

In an HA environment, it is possible that resource groups will show when the BI service has not yet started. This just means that the resource group is online, but the BI service has not started yet. If you try to access the cluster via the web, the resource group will either be unavailable or, more likely, the navigation panel will load but you will see an error message similar to the following: “The dispatcher is still initializing, try again.”

Troubleshooting the Installation

The installer program does not start on Linux.

```
#./HPNMS_9.00_setup.bin
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...
awk: cmd. line:6: warning: escape sequence `\.' treated as plain `.'
 (i) Checking display ...
 (-) Display may not be properly configured
Please make sure the display is set properly...
```

Solution:

X-Windows display is not configured; therefore, the installer GUI cannot start. If you have a remote terminal session to the system on which you are installing the NPS software, set the DISPLAY environment variable to the hostname:port of a local X-Windows display server. You might have to use 'xhost +' to grant the remote machine display access.

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

Although you can continue with the installation despite warning messages, HP strongly recommends that you correct the problems before proceeding. Warnings are displayed if system recommendations are not met. Clicking on the name of the individual installation check reveals more details. For more information, see Prerequisites and Planning on page 13.

Solution:

Depends on warnings found.

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

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 reveals more details. For more information, see Prerequisites and Planning on page 13.

Solution:

Depends on errors found.

NNMi is not installed, yet the installer displays an ERROR message for NNMi Version check, indicating that the NNMi version is incorrect.

```
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
```

Solution:

Check to see if the `/opt/ov/NNMVersionInfo` file exists. 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.

Installation takes a long time.

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

Solution:

Allow the installer to proceed to completion.

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

The enablement script was not run.

Solution:

Run the nnmenableperfspi.ovpl script. See Enabling NPS on the NNMi Management Server on page 18.

Installer fails at AppCheckReqdLibs.

Installer fails at AppCheckReqdLibs with messages similar to the following:

```
rpmdb: Lock table is out of available locker entries
rpmdb: Unknown locker ID: 994
error: db4 error(22) from db->close: Invalid argument
error: cannot open Packages index using db3 - Cannot allocate memory (12)
error: cannot open Packages database in /var/lib/rpm
package compat-libstdc++-296.i386 is not installed
INFO: Required library not installed: compat-libstdc++-296.i386
rpmdb: Lock table is out of available locker entries
rpmdb: Unknown locker ID: 995
error: db4 error(22) from db->close: Invalid argument
error: cannot open Packages index using db3 - Cannot allocate memory (12)
error: cannot open Packages database in /var/lib/rpm
package compat-libstdc++-33-3.2.3.i386 is not installed
INFO: Required library not installed: compat-libstdc++-33-3.2.3.i386
```

```
rpmdb: Lock table is out of available locker entries
rpmdb: Unknown locker ID: 996
```

The RPM database is corrupt.

To solve the problem, you must rebuild the RPM database. First, back up the existing copy by running the following command:

```
tar cvzf rpmdb.backup.tar.gz /var/lib/rpm
rm /var/lib/rpm/__db.*
rpm --rebuilddb
```

To test, run the following command

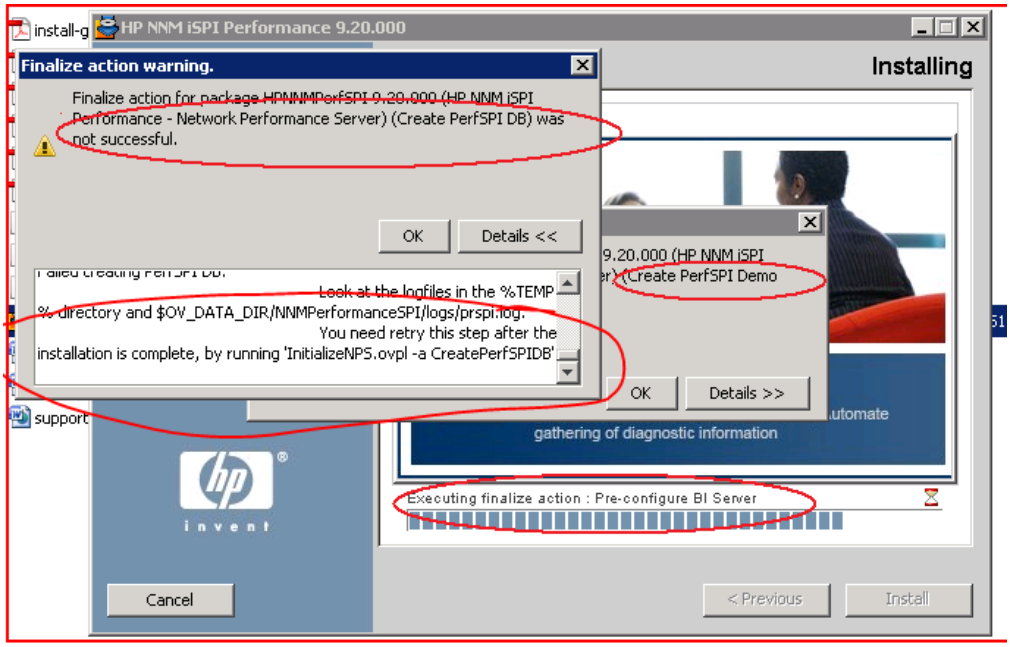
```
rpm -q -a
```

It should return a list of all installed RPMs.

The initializeNPS application returned an error.

The installer calls the initializeNPS.ovpl routine automatically. If any of the steps fail, the installer warns you but does not abort. You can correct any issues and rerun the failed steps from the command line to finish the initialization.

An error message will inform you to rerun the initializeNPS.ovpl script along with a specific action. The following is an example error message.



A menu will show the status of each Failed or Success action. You must run the Failed actions again. You might also have to rerun other actions if they have a dependency on the Failed actions. For best results, rerun all the actions after the Failed action listed in the menu, except for any help and quit actions.

You can either select an action number n, a range of actions n1-n2, or multiple actions separated by a comma.

The `PerfSPI_InitializeNPS.ovsh` and `prspi.log` files are created in the `%TEMP%` folder.

The content store can hang during upgrade when the database is in use for scheduled jobs or reports.

If the content store database is in use for writing by schedules or jobs, the export can fail.

The solution is to go to the BI Server portal prior to upgrade and disable the schedules and stop some of the services the dispatcher runs.

Follow these steps:

1. Log in to the BI Portal and launch BI Administration.
2. Open the Status tab.
3. Click **Schedules** in the list on the left.
4. Click the check box at the top of the list.
5. Click the **Disable** icon in the top right.
6. Select the **Configuration** tab.
7. Select **Dispatchers and Services** from the list on the left.
8. Click the dispatcher in the displayed list. You will see a list of services. Be aware that, by default, there is more than one page to this list.
9. Click **More** for each of the following services, and then immediately click **Stop**.
   - BatchReportService
   - JobService
   - ReportService
10. When the upgrade is complete, re-enable the schedules by logging in to the BI Portal and launching BI Administration.

Installer advises installation of some pre-requisite packages.

The recommended installation command might look like this:

```
yum install unixODBC.i386 unixODBC.x86_64 unixODBC-devel.i386
unixODBC-devel.x86_64
```

The solution is to run the commands in the following order:

- yum install unixODBC-libs
- yum install unixODBC.i386 unixODBC.x86_64
- yum install unixODBC.i386 unixODBC.x86_64 unixODBC-devel.i386 unixODBC-devel.x86_64

Troubleshooting the Configuration Utility

Configuration Utility shows a failure message.

```
FATAL: Service configuration test failed
```

The shared path is incorrectly formatted.

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

1. Go to the NNMi management server.
2. Collect the `nnmenableperfspi_log.txt` file for the enablement script from the following location: `/opt/ov/log` or `/var/opt/OV/log`.
3. At the end of the file, look for the shared location details in the Summary or Next Steps section.
4. Copy the location from the log file and paste in the Path field in the Configuration Utility.

Configuration Utility shows that the shared drive is not accessible.

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

Use the appropriate tools to make exceptions for the NFS traffic.

11 Licensing for NNM iSPI Performance

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

If you acquired a license for an iSPI other than NNM iSPI Performance, you will not be able to use the features of NNM iSPI Performance after the 30-day evaluation period is over. You must acquire a permanent license for NNM iSPI Performance.

Do not modify any of the report templates provided with the iSPI products. Modified report templates are not supported.

Permanent License

To obtain a permanent license for NNM iSPI Performance, follow these steps:

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:

   ```
   /opt/OV/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, type the license password in the text file, and save the text file.
3. On the NNMi management server, run the following command:

   ```
   /opt/OV/bin/nnmlicense.ovpl PerfSPI -f <license_text_file>
   ```

Additional License Passwords

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 for NNM iSPI Performance, go to the HP password delivery service at **https://webware.hp.com/welcome.asp**.

12 Installing NPS in an NNMi Application Failover Environment

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 NPS on a dedicated server and not on the NNMi management server. If you want to configure a redundant solution for NPS, you must install 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 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. There are no special tasks for the NPS administrator to perform.

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

- 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 are able to link from NPS to NNMi views on the new primary server, just like before the failover took place.

Application Failover Cluster

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 NNM iSPI Performance, install identical licenses on every server in the cluster.

Copying the Keystore File from NNMi to NPS

To copy the cluster.keystore certificate from NNMi to NPS, follow these steps:

1. Go to following directory on the NNMi management server:

   ```
   /var/opt/ov/shared/nnm/conf/nnmcluster/cluster.keystore
   ```

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

```
/var/opt/OV/NNMPerformanceSPI/nnmappfailover/keystore
```

The keystore enables access to the NNMi cluster. HP recommends using a secure copy mechanism, such as SCP or USB key.

13 Upgrading the Content Store

If you are upgrading from a previous version of NNM iSPI Performance, the content store will be upgraded automatically. The contents of the existing content store will be migrated to the new content store.

If you have a large amount of data stored, it can take some time (about 15 minutes per Gigabyte or more depending on your system) to export the data from the previous to the new database.

14 Getting Started with Reports

Once the installation is complete, you can begin launching reports. Detailed instructions for using, creating, and saving reports can be found in the *HP NNM iSPI Performance for Metrics Online Help*.

Launching Reports 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 click **Sign In**.

3. When the NNMi console opens, select **Actions** > **HP NNM iSPI Performance** > **Reporting–Report Menu**. The NPS report window opens.

Launching Reports from the Report Menu

1. Point your browser to the following URL:

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

   Or, if HTTPS was configured:

   `https://<fully-qualified-domain-name>:9305`

   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 click **Sign In**.

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

15 Ports Information

The following information on ports applies to both NNM iSPI Performance and NPS.

Port	Type	Name	Purpose	Config
Ports used over network				
9300	TCP	NPS UI	Default HTTP port – used for Web UI and BI Web Services	Change using `configureWebAccess.ovpl`
9305	TCP	NPS UI – SSL	Default Secure HTTPS port (SSL) – used for Web UI and BI Web Services	Change using `configureWebAccess.ovpl`
If NNM and NPS do not co-exist, the network ports used for the OS network file sharing are also required (NFS services on Linux, Windows File Sharing on Windows)				
Ports used by processes running on the same server (not used for communication between servers over the network)				
9301	TCP	Sybase ASE	Sybase ASE (BI Content Manager Database)	Change not supported
9302	TCP	Sybase IQ Agent	Sybase IQ Agent service	Change not supported
9303	TCP	Sybase IQ – PerfSPI DB	Sybase IQ database used to store all NPS Extension Pack data	Change not supported
9304	TCP	Sybase IQ – PerfSPI DEMO DB	Sybase IQ database used to store Extension Pack DEMO data	Change not supported
9306	TCP	Database SQL Rewrite Proxy – PerfSPI DB	SQL Rewrite proxy for the Perfspi database – used by the BI Server	Change not supported
9307	TCP	Database SQL Rewrite Proxy – PerfSPI DEMO DB	SQL Rewrite proxy for the Perfspi DEMO database – used by the BI Server	Change not supported
9308	TCP	Sybase ASE Backup Server	Sybase ASE backup server for the BI content manager database	Change not supported