Hewlett Packard
Enterprise

HPE Network Node Manager iSPI Performance for Metrics Software

Software Version: 10.30
for the Windows® and Linux® operating systems

Deployment Reference

Document Release Date: June 2017
Software Release Date: June 2017

Legal Notices

Warranty

Restricted Rights Legend

Oracle Technology — Notice of Restricted Rights

Copyright Notice

Trademark Notices

Acknowledgements

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

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

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

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

Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/group/softwaresupport/search-result?keyword=.

This site requires an HP Passport account. If you do not have one, click the **Create an account** button on the HP Passport Sign in page.

Support

Visit the HPE Software Support web site at: **https://softwaresupport.hpe.com**

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

HPE Software 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 HPE 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 **https://softwaresupport.hpe.com** and click **Register**.

To find more information about access levels, go to:
https://softwaresupport.hpe.com/web/softwaresupport/access-levels

Contents

Overview

This document describes the system design considerations involved in building and maintaining the Network Performance Server (NPS) component of your network monitoring solution. This document provides detailed guidelines on how to set up a distributed deployment of NPS, how to configure different components of NPS for optimal performance, and how to maintain the environment. This document supplements the Interactive Installation Guide and the Support Matrix.

The latest version of this document is available here.

This document includes the following information:

- "Introduction to Different Installation Models" on page 10. Provides an introduction to the concept of distributed NPS deployment.
- "Creating a Distributed Environment" on page 16. Provides instructions to create a new distributed deployment of NPS.
- "Switching from a Standalone Environment" on page 50. Describes how to migrate a standalone NPS system to a distributed environment.
- "Maintaining the NPS Database" on page 108. Describes how to back up, restore, and recreate the NPS database.
- "Tuning the Business Intelligence Server" on page 117. Describes how to fine-tune different settings of the Business Intelligence Server for optimal performance.

System Configuration

This section lists important system configuration requirements for the NPS system.

Configure the Open Files Limit (Linux Only)

NPS requires that the open files limit of the NPS system (Linux) be set to at least 8192.

To set this limit, follow these steps:

Log on to the system as root.

1. Open the following file with a text editor:

   ```
   /etc/security/limits.conf
   ```

2. Check that the value of the `nofile` parameter (against both the hard and soft types) is higher than 8192.
   If a lower value is set, change the value to at least 8192.
   For example:

   ```
   * soft nofile 8192
   ```

   ```
   * hard nofile 8192
   ```

3. Save the file.
4. Restart NPS by running the following commands:
   a. **stopALL.ovpl**
   b. **startALL.ovpl**

Part I: Installation Models

While deploying NPS, you can use one of the three available deployment architecture. The size of your monitoring environment is an important factor in deciding the right deployment architecture. This section of the document provides information about each deployment architecture.

Introduction to Different Installation Models

Single-Server Model

You can install NPS on the NNMi management server when you plan to monitor a small or medium-sized environment. The procedure to install NPS (and the NNM iSPI Performance for Metrics) on the NNMi management server involves running the NNM iSPI Performance for Metrics on the NNMi management server. See the *NNM iSPI Performance for Metrics Support Matrix* for information about the sizes of environments that are supported by this *same-server* installation model where NPS co-exists with NNMi on the same server.

Dedicated Server Model

To achieve greater performance and scale, you can install NPS (and the NNM iSPI Performance for Metrics) on a standalone, dedicated server. Installing NPS in this model involves running the nnmenableperfspi.ovpl script on the NNMi management server and running the NNM iSPI Performance for Metrics installer on a dedicated server. You can opt for this installation model when you want to monitor a large or very large environment.

Distributed Deployment of NPS

You can deploy NPS across a number of systems to take advantage of more computing resources and achieve greater scale. The **distributed deployment of NPS** enables you to distribute the computing load across multiple systems and designate each system to perform a specific operation determined by the **role** assigned to the system and provides a way to get past resource constraints on a single server. Distributed environments are best-suited to large scale network monitoring with high scale needs in the area of scheduled report generation, real-time analytics, or custom collection reporting.

Support for NNMi Application Failover

Application Failover for NNMi ensures redundancy. Failover allows a secondary NNMi server to take over immediately after the failure of a primary NNMi server. Failover relies on jboss clustering technology, ongoing file system synchronization, and a Java keystore file that must be copied from NNM to NPS. For details, see the *HPE Network Node Manager iSPI Performance for Metrics Installation Guide*.

NPS supports NNMi Application Failover, which is transparent to users. Aside from an interruption in service lasting about 15 minutes while failover is in progress, users are not aware that a failover took place, and the administrator is not required to perform any special tasks related to failover.

The ability of NPS to support Application Failover depends on files it retrieves from the primary server in the cluster. NPS retrieves these files during startup. As soon as NPS has the files, it begins monitoring the status of the primary server by checking for status changes every 5 minutes. If NPS detects a status change, the following events take place automatically:

- NPS determines which server is the new primary server.
- NPS redirects data collection to a shared directory on the new primary server.
- NPS begins collecting data (metrics and topology files) from the new primary server in the cluster.

> **Note:** After failing over to the standby server, all reportlet dashboards and bookmark links will stop working. You must regenerate all reportlet dashboards and bookmark links after failover.

Immediately after failover, NPS users are able to link from NPS to NNMi views on the new primary server, just as they could before failover.

Achieving Scale Through Distribution

Server resources include CPU, memory, and disk I/O. When any one of these resources is fully consumed, you experience performance limitations that can prevent NPS from processing and loading the incoming data fast enough. The following behaviors indicate that NPS is unable to process the data optimally with the available resources:

You can address these problems, to a point, by adjusting how the server memory and CPU resources are allocated with the help of different tuning parameters provided by NPS. See "Tuning the Business Intelligence Server" on page 117 and "Tuning the NPS Database" on page 121 for more information. If you continue to experience resource bottleneck after tuning NPS, consider spreading NPS processes across multiple servers by creating a distributed deployment of NPS.

You can plan to create a distributed deployment of NPS if you observe the following:

- One or more Extension Packs routinely fail to complete loading within its polling interval (usually 5 minutes). To assess this, launch the ETL Performance by ExtPk Report View (from the **Self Monitoring > Quicklaunch Diagnostic Reports** menu in the navigation pane in the NPS console). Monitor the value of the `Process Time (secs) (avg)` metric for each Extension Packs. If the value exceeds 300 seconds for an Extension Pack, you can consider creating a distributed deployment with a dedicated server with the Extract, Transform, and Load Server (ETL Server) role.
- After launching the NPS console, the navigation pane appears empty for several seconds. In this case, you can consider creating a distributed deployment with a dedicated server with the User Interface and Business Intelligence Server (UiBi Server).
- If scheduled reports often fail to complete, consider configuring a separate server with the UiBi Server role.

Roles

You can assign one, two, or all three of the following roles to an NPS system in a distributed deployment:

- **Database Server:** The Database Server (DB Server) role is responsible for creating and hosting the NPS database and running database queries. The NNM iSPI Performance for Metrics installs Sybase IQ on each NPS system. When you assign the DB Server role to a system, NPS starts the Sybase IQ database on the system and creates a shared directory.

  In a distributed deployment, you can assign the DB Server role to one or more systems.

  > **Note:** You can plan to configure multiple DB Servers if you have a very large environment with high usage of interactive (not scheduled) reports.
  >
  > Multiple DB Servers are supported only in a Linux environment. Also, you must configure a shared storage system with raw disks with the help of the Storage Area Network (SAN) infrastructure while creating multiple DB Servers.
  >
  > As a best practice, if you need to configure multiple DB Servers, always start with two servers. Later, based on the performance of the solution, you can add more DB Servers to the environment.

- **User Interface and Business Intelligence Server:** The User Interface and Business Intelligence Server

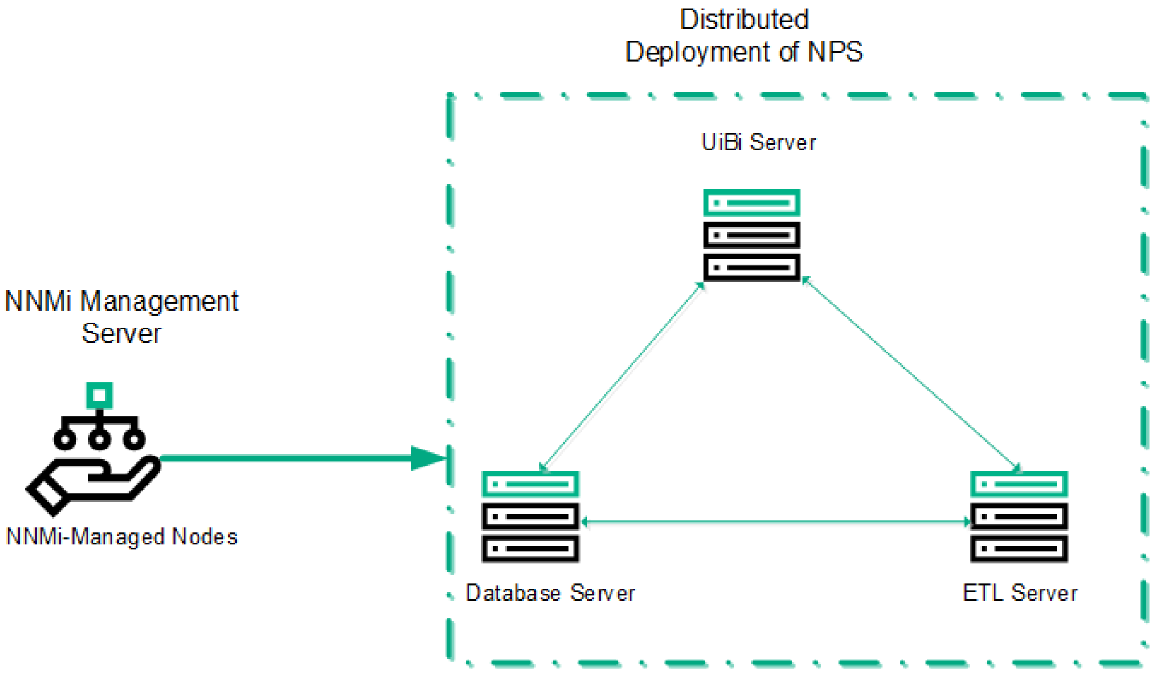
(UiBi Server) role is responsible for rendering the available data into reports with the help of templates provided with Extension Packs. When you assign the UiBi Server role to a system, NPS starts the BI server and creates a shared directory.

You can assign the UiBi Server role to *only one* system.

- **Extract, Transform, and Load Server:** The Extract, Transform, and Load Server (ETL Server role) is responsible for performing Extract, Transform, and Load (ETL) operations for the collected metrics.

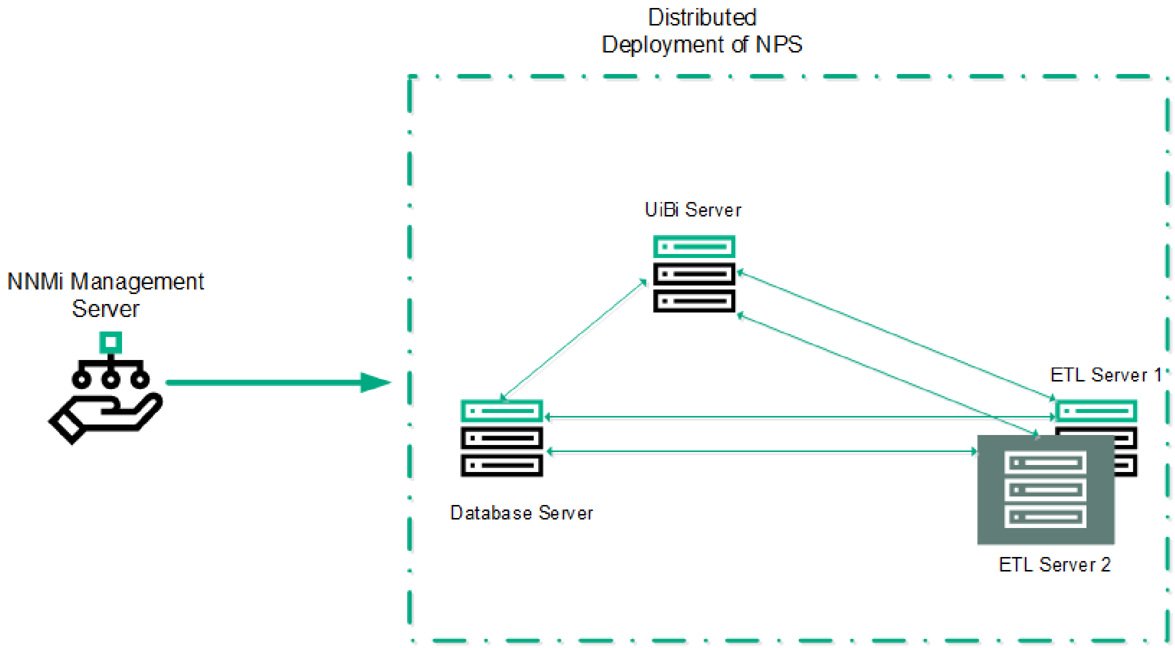
  You can assign the ETL Server role to as many systems as you like. However, each Extension Pack must be enabled on only one ETL Server.

  Distributed Deployment of NPS with a Single ETL Server

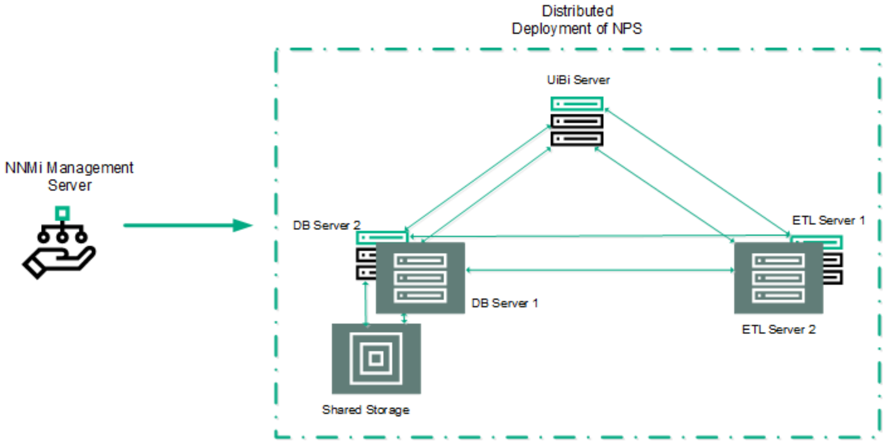


When you configure multiple ETL Servers, you must allocate specific Extension Packs to be processed by each ETL Server. In other words, you must identify which Extension Packs are going to be processed by which ETL Server.

Distributed Deployment of NPS with Two ETL Servers



Distributed Deployment of NPS with Two DB Servers with Shared Storage



Guidelines for Deploying NPS in a Distributed Environment

You can configure NPS in a distributed environment from day one of your operation by installing NPS on multiple systems and assigning specific roles to each NPS system. This configuration is recommended for very large scale environment. For more information about the scale of the environment where the distributed deployment of NPS could be an ideal solution, see the *Support Matrix*.

To create a distributed environment in phases, follow these guidelines:

- All NPS systems in the distributed deployment must run on the same operating system.
- All NPS systems in the distributed deployment must have the same time zone configuration.
- While creating a distributed deployment, use the following sequence while configuring server roles:

a. Configure the DB Server role.
b. Configure the UiBi Server role.
c. Configure the ETL Server role.

Part II: Preinstallation Planning and Creating a Distributed Deployment

This section of the document provides step-by-step instructions to plan and create a distributed deployment of NPS. You can also migrate your standalone NPS installation to a distributed environment by following the instructions provided in this section.

> **Note:** The information in the *Preinstallation Planning and Creating a Distributed Deployment* section provides instructions to create a distributed environment with NPS 10.30. You can apply the NPS 10.30 patch after the procedure is complete. For patch installation instructions, see "Installing Patches in a Distributed Deployment of NPS" on page 82.

Creating a Distributed Environment

> **Note:** The information in the *Creating a Distributed Deployment* section provides instructions to create a distributed environment with NPS 10.30. You can apply the NPS 10.30 patch after the procedure is complete. For patch installation instructions, see "Installing Patches in a Distributed Deployment of NPS" on page 82.

At the time of installation, the NNM iSPI Performance for Metrics installer automatically assigns all three roles to the NPS system. If you want to deploy NPS in a distributed environment, you must install NPS on each system in the distributed environment, and then run the `configureNpsServer.ovpl` script on each system to assign roles.

To create a distributed environment, follow these steps:

1. "Identify Systems".
2. "Installing NPS".
3. "Assign Roles" on page 30

Identify Systems

Identify the systems on which you want to install NPS. Make sure all systems meet the hardware and software requirements listed in the *HPE Network Node Manager iSPI Performance for Metrics Software Support Matrix* and the Prerequisites section in the *HPE Network Node Manager iSPI Performance for Metrics Software Installation Guide*.

> **Note:** All systems must run with the same operating system.

Installing NPS

With the help of the *HPE Network Node Manager iSPI Performance for Metrics Software* 10.30 media, install NPS on each system. Follow the instructions in this section.

After the installation of the version 10.30 is complete, apply the NNM iSPI Performance for Metrics 10.30 patch.

Prerequisites

Before you begin, make sure that the following prerequisites are met:

General Prerequisites

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).

The NNMi management server and the NPS systems must have the same domain name.

Verify that the NPS systems 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 systems:

- `nnm.mycompany.com`
- `nps.reporting.mycompany.com`

Automatic operating system updates

Disable the automatic update feature of the operating system to prevent automatic installation of operating system fixes and enhancements while you install NPS. You can enable the feature after successful installation of NPS.

Network

It is recommended that you install NPS on a system with Gigabit Ethernet LAN interfaces.

The network interface card (NIC) on each system should have at least 1 Gbps link speed.

> **Tip:** If you plan to store large volumes of data in the NPS database, you can choose SAN disks for the NPS system. However, if you plan to use a single SAN disk for NPS and a few other applications, you might observe poor NPS performance due to inference from other applications.
>
> Use a benchmark tool to assess the performance of the disk prior to installing NPS.
>
> On Linux, use a benchmark tool (like bonnie++) to assess the performance of the disk prior to installing NPS. On high-performing I/O systems, bonnie++ should have a total run time of 1 minute 10 seconds or less.

Port Availability

The following ports must be available on each system in the distributed deployment of NPS:

Port	Type	Purpose	Configuration
9300	TCP	Default HTTP port – used for Web UI and BI Web Services	After installation, you can change this port by using `configureWebAccess.ovpl`.
9305	TCP	Default Secure HTTPS port (SSL) – used for Web UI and BI Web Services	After installation, you can change this port by using `configureWebAccess.ovpl`.
9301	TCP	Sybase ASE	Change not supported
9302	TCP	Sybase IQ Agent service	Change not supported
9303	TCP	Sybase IQ–the NPS database	Change not supported
9306	TCP	Database SQL Rewrite Proxy–the NPS database	Change not supported

Port	Type	Purpose	Configuration
9308	TCP	Sybase ASE backup server for the BI content manager database	Change not supported

For NNMi on Linux. Make sure that the Samba software is installed on the management server. Configure the security policies or firewall settings to make exceptions for the SMB traffic.

Firewall

Make sure that firewall rules do not block traffic through the following ports:

- 9303
- 9306
- HTTP port if you have configured NPS to use HTTP (default: 9300; after installation, you can change this port by using `configureWebAccess.ovpl`)
- HTTPS port if you have configured NPS to use HTTPS (default: 9305; after installation, you can change this port by using `configureWebAccess.ovpl`)

Requirements on Linux

Required libraries

The NPS installer requires a set of libraries to be present on the system. The installer performs a prerequisite check and, if any prerequisite libraries are missing, shows a list of missing libraries. You can then install the missing libraries manually or by using the `yum` command, and then start the installer again.

List of Prerequisite Libraries

- libstdc++.i686
- compat-libstdc++-296.i686
- compat-libstdc++-33.i686
- compat-libstdc++-33.x86_64
- libpng.i686
- libpng.x86_64
- libXp.i686
- libXp.x86_64
- ncurses
- openmotif.i686
- openmotif.x86_64
- tcsh
- unixODBC.i686
- unixODBC.x86_64
- unixODBC-devel.i686
- unixODBC-devel.x86_64
- libXtst.i686
- libXtst

- libXi.i686
- libXi
- libaio
- nspr.i686
- nspr.x86_64
- nss.i686
- nss.x86_64

You can install NNM iSPI Performance for Metrics10.30 on Red Hat Enterprise Linux 7.x. However, you must install the NNM iSPI Performance for Metrics 10.21 patch after installing the NNM iSPI Performance for Metrics10.30 on Red Hat Enterprise Linux 7.x and creating the distributed deployment of NPS (see "Installing Patches in a Distributed Deployment of NPS" on page 82). The NNM iSPI Performance for Metrics10.30 cannot function on Red Hat Enterprise Linux 7.x without the 10.21 patch.

Installing the NNM iSPI Performance for Metrics10.30 on Red Hat Enterprise Linux 7.x requires the following additional libraries:

- compat-libstdc++-296.i686
- motif
- motif.i686
- openmotif.i686
- openmotif.x86_64

Tip: Install the motif libraries before installing the openmotif libraries.

If the `yum` commands for installing the compat-libstdc++-296.i686, openmotif.i686, and openmotif.x86_64 library fail, download the library files on the NPS system, and then install by running the `rpm -i` commands with the `--nodeps --force` options.

For example:

```
rpm -i compat-libstdc++-296-2.96-146.1.i686.rpm --nodeps --force

rpm -i openmotif-2.3.3-8.el6.x86_64.rpm --nodeps –force

rpm -i openmotif-2.3.3-8.el6.i686.rpm --nodeps --force
```

IPv4 address in the hosts file

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

Time zone

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

All systems in the distributed deployment of NPS must be in the same time zone.

Set the Maximum Number of Open Files

You must set the maximum number of open files to at least 8192.

To set this limit, follow these steps:

1. Log on to the system as root.
2. Open the following file with a text editor:

```
/etc/security/limits.conf
```

3. Check that the value of the `nofile` parameter (against both the `hard` and `soft` types) is higher than 8192.

   If a lower value is set, change the value to at least 8192.

   For example:

   ```
   * soft nofile 8192
   ```

   ```
   * hard nofile 8192
   ```

4. Save the file.

Installing on ext4 File Systems

If you plan to install NPS on an ext4 file system, disable the journaling feature to enhance performance. To check that journaling is enabled, run the following command:

tune2fs -l /<*device*> **| grep "Filesystem features"**

In this instance, <*device*> is the name of the file system on which you plan to install NPS.

If the output of the command shows `has_journal`, the journaling feature is enabled.

To disable journaling, follow these steps:

1. Make sure that the file system is unmounted or mounted as read only.
2. Run the following command:

   tune2fs -O ^has_journal /<*device*>

Enable Access Control List on Systems with Mounted File Systems (Only on Linux)

You must perform this additional step if the `/var/opt` directory exists on a mounted file system on one of these systems:

- NNMi management server
- The system where you want to configure the DB Server
- The system where you want to configure the UiBi Server

Follow these steps on each of the above systems if the `/var/opt` directory exists on a mounted drive:

1. Open the `/etc/fstab` file with a text editor.
2. Find the line that starts with the following:

   <file_system> <mount_point>

   <file_system> is the `/var/opt` directory (either `/var` or `/var/opt`)
3. In the line, add `acl` to the list of options.
4. Save the file.
5. Run the following command to remount `/var/opt`:

   mount -o remount /var/opt

   Or

   mount -o remount /var

Prerequisites for Installing on Multi-homed Systems

While installing NPS on a system with multiple IP addresses, make sure that one of the IP addresses is present in the hosts file. Follow these steps:

1. Log on to the system where you are going to install NPS.
2. Go to the following directory:

   On Windows

   ```
   C:\Windows\System32\drivers\etc
   ```

   On Linux

   ```
   /etc
   ```

3. Open the `hosts` file with a text editor.
4. Add one of the IP addresses and the FQDN of the system in a new line.
5. Save the file.

Prerequisites for Configuring Multiple DB Servers

> **Note:** You can plan to configure multiple DB Servers if you have a very large environment with high usage of interactive (not scheduled) reports.
>
> Multiple DB Servers are supported only in a Linux environment. Also, you must configure a shared storage system with raw disks with the help of the Storage Area Network (SAN) infrastructure while creating multiple DB Servers.
>
> As a best practice, if you need to configure multiple DB Servers, always start with two servers. Later, based on the performance of the solution, you can add more DB Servers to the environment.

Modify the perfspi.cfg File

1. Log on to one of the DB Servers in the deployment.
2. Open the following file with a text editor:

   ```
   /var/opt/OV/database/perfspi.cfg
   ```

3. Change the line `-n perfspi` to `-n` <*hostname*>`perfspi`.

   In this instance, <*hostname*> is the hostname of the local system.
4. Save the file.
5. Repeat these steps on all the DB Servers in the environment.

Configure Storage Resources

A distributed deployment of NPS with multiple DB Servers require a raw storage system. Before configuring the DB Server roles, make sure to complete the storage configuration.

To configure the storage resources:

1. Make sure that all the servers used in this distributed deployment of NPS use the multipath I/O configuration.
2. Create at least the following VDisks for the deployment:
   - One VDisk for the entire distributed environment (you can label it as SYSTEM).
   - One VDisk for each DB Server in the distributed environment to host temporary data (you can label them as TEMP1, TEMP2, and so on).
   - At least one VDisk to store the tables and columns of the NPS database (you can label it as USER_MAIN1)
3. Note down the WWID of each VDisk.

Enabling NNMi to Work with NPS

You must run a set of scripts on the NNMi management server to enable NNMi to work with the distributed deployment of NPS.

These scripts perform the following tasks:

- Adding a new menu item (NNM iSPI Performance) in the Actions menu of the NNMi console
- Enabling the evaluation license of the NNM iSPI Performance for Metrics on the NNMi management server
- Creating a shared directory on the NNMi management server where NNMi can store the performance data collected from the managed network (NPS collects the data from this shared directory)
- Creating a user on the NNMi management server with write privilege to the newly created shared directory

To enable NNMi to work with NPS, follow these steps:

> **Note:** If NNMi is installed in a high-availability or Application Failover cluster, follow these steps on each node in the cluster.

When NNMi is installed on Linux

1. Log on to the NNMi management server as root.
2. If the `/var/opt` directory on the NNMi management server is on a mounted file system, you must perform the following additional steps:
   a. Open the `/etc/fstab` file with a text editor.
   b. Find the line that starts with the following:

      <file_system> <*mount_point*>

      <file_system> is the `/var/opt` directory (either `/var` or `/var/opt`)
   c. In the line, add `acl` to the list of options.
   d. Save the file.
   e. Run the following command to remount `/var/opt`:

      mount -o remount /var/opt

      Or

      mount -o remount /var
3. Go to the following directory:

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

4. To run the script in the interactive mode:

   a. Run the following command:

      ./nnmenableperfspi.ovpl

      The script prompts you for the fully qualified domain name of the NPS system.

   b. Type the fully qualified domain name of the system on which you want to assign the UiBi Server role, and then press **Enter**.

      The script verifies the availability of the NPS system with a ping command.

      After successful verification, the script prompts you to specify the port that will be used by the NPS system.

   c. Type a port number that is available for use, and then press **Enter**.

      The script prompts you to specify the communication protocol for NPS.

   d. Type HTTPS if want to use the secure communication mode, and then press **Enter**.

      If you want to use the non-secure HTTP mode of communication, press **Enter** without specifying anything.

      The script prompts you to choose the type of file-sharing technique to exchange data between the NNMi management server and the NPS system. Available options are **CIFS**[1] and **NFS**[2].

   e. Type **CIFS** or **NFS**, and then press **Enter**.

      > **Note:** While creating a distributed deployment of NPS, choose NFS only if NNMi and all NPS system are on Linux. If you select NFS, make sure to apply the NNM iSPI Performance for Metrics 10.30 patch after completing the procedure of creating the distributed deployment of NPS. For instructions to install the 10.30 patch, see "Installing Patches in a Distributed Deployment of NPS" on page 82.

      The script enables the evaluation license of the NNM iSPI Performance for Metrics on the NNMi management server, adds new items under the **Actions** menu, and enables file sharing between the NNMi management server and the NPS system.

      Follow these steps:

      i. The script prompts you to specify a user name that will be assigned as the owner of the shared file system.

         Type a user name of your choice, and then press **Enter**. You need not type a pre-existing user name.

         The script prompts you to type a password for the user that it is going to create.

      ii. Type a password that meets the operating system's password policy requirements, and then press **Enter**.

         The script prompts you to specify the directory that will be used as the shared file system.

      iii. Type the complete path to the directory that you want to use as the shared file system between the NNMi management server and the NPS system, and then press **Enter**

         The script performs the following tasks:

[1] Common Internet File System (CIFS) is an application-layer file sharing protocol.

[2] Network File Share (NFS) is a file sharing protocol between systems running on UNIX/Linux.

- Enables the evaluation license of the NNM iSPI Performance for Metrics on the NNMi management server
- Adds menu items under the Actions menu in the NNMi console to launch the NPS console
- Creates the shared file system
- Creates a user (if necessary) that can access the newly created shared file system

5. To run the script in the non-interactive (silent) mode:

   a. In a text editor, add the following content:

```
spiHost=

spiPort=

spiProtocol=

shareType=

userName=

password=

shareName=

sharedDir=
```

   b. Specify a value for each parameter:

Parameter	Description
spiHost	Type the fully qualified domain name of the system on which you want to assign the UiBi Server role.
spiPort	Type the port that will be used by the NPS system. Type a port number that is available for use.
spiProtocol	Type HTTPS if want to use the secure communication mode. Type HTTP if you want to use the non-secure mode of communication.
shareType	Type CIFS.
userName	Type a user name of your choice. You need not type a pre-existing user name. This user name that will be assigned as the owner of the shared file system.
password	Type the password of the above user. The password must meet the operating system's password policy requirements.
shareName	Type a name of your choice for the shared file system.
sharedDir	Specify the directory that will be used as the shared file system. Type the complete path to the directory that you want to use as the shared file system between the NNMi management server and the NPS system.

   c. Save the file on the NNMi management server.

   d. Run the following command:

   ./nnmenableperfspi.ovpl -f *<configFile>*

In this instance, <*configFile*> is the name of the configuration file (with complete path to the file).

The script performs the following tasks:

- Enables the evaluation license of the NNM iSPI Performance for Metrics on the NNMi management server
- Adds menu items under the Actions menu in the NNMi console to launch the NPS console
- Creates the shared file system
- Creates a user (if necessary) that can access the newly created shared file system

When NNMi is Installed on Windows

1. Log on to the NNMi management server as Administrator.
2. Go to the following directory:

   ```
   %nnminstalldir%\bin
   ```

3. To run the script in the interactive mode:

   a. Run the following command:

      nnmenableperfspi.ovpl

      The script prompts you for the fully qualified domain name of the NPS system.

   b. Type the fully qualified domain name of the system on which you want to assign the UiBi Server role, and then press **Enter**.

      The script verifies the availability of the NPS system with a ping command.

      After successful verification, the script prompts you to specify the port that will be used by the NPS system.

   c. Type a port number that is available for use, and then press **Enter**.

      The script prompts you to specify the communication protocol for NPS.

   d. Type HTTPS if want to use the secure communication mode, and then press **Enter**.

      If you want to use the non-secure HTTP mode of communication, press **Enter** without specifying anything.

      The script prompts you to choose the type of file-sharing technique to exchange data between the NNMi management server and the NPS system.

   e. When you use a Windows NNMi management server, you must choose only the **CIFS**[1] protocol for file sharing.

      Type CIFS, and then press **Enter**.

      The script prompts you to specify a user name that will be assigned as the owner of the shared file system.

   f. Type a user name of your choice, and then press **Enter**. You need not type a pre-existing user name.

      > **Tip:** If you specify a user name that does not already exists, the script creates a new local user (and not a Windows domain user).
      >
      > You can specify a pre-existing Windows domain user.

[1] Common Internet File System (CIFS) is an application-layer file sharing protocol.

> Always use the following format while specifying a pre-existing domain user name:
>
> *<domain>****<user_name>*
>
> In this instance, *<domain>*is the domain name and *<user_name>* is the user name.

The script prompts you to specify a password of the user that it is going to create.

g. Type a password that meets the operating system's password policy requirements, and then press **Enter**.

   The script prompts you to specify the directory that will be used as the shared file system.

h. Type the complete path to the directory that you want to use as the shared file system between the NNMi management server and the NPS system, and then press **Enter**.

   The script performs the following tasks:

   - Enables the evaluation license of the NNM iSPI Performance for Metrics on the NNMi management server
   - Adds menu items under the Actions menu in the NNMi console to launch the NPS console
   - Creates the shared file system
   - Creates a user (if necessary) that can access the newly created shared file system

4. To run the script in the non-interactive (silent) mode:

   a. In a text editor, add the following content:

```
spiHost=

spiPort=

spiProtocol=

shareType=

userName=

password=

shareName=

sharedDir=
```

   b. Specify a value for each parameter:

Parameter	Description
spiHost	Type the fully qualified domain name of the system on which you want to assign the UiBi Server role.
spiPort	Type the port that will be used by the NPS system. Type a port number that is available for use.
spiProtocol	Type the communication protocol for NPS. Type HTTPS if want to use the secure communication mode. Type HTTP if you want to use the non-secure mode of communication.
shareType	Type CIFS.

Parameter	Description
	When NNMi is installed on Windows, you can use only the **CIFS**[1] protocol.
userName	Type a user name of your choice, and then press **Enter**. You need not type a pre-existing user name. **Tip:** If you specify a user name that does not already exists, the script creates a new local user (and not a Windows domain user). You can specify a pre-existing Windows domain user. Always use the following format while specifying a pre-existing domain user name: *<domain>**<user_name>* In this instance, <*domain*>is the domain name and <*user_name*> is the user name.
password	Type the password of the above user.
shareName	Type a name of your choice for the shared file system.
sharedDir	Specify the directory that will be used as the shared file system. Type the complete path to the directory that you want to use as the shared file system between the NNMi management server and the NPS system.

c. Save the file on the NNMi management server.

d. Run the following command:

nnmenableperfspi.ovpl -f <*configFile*>

In this instance, <*configFile*> is the name of the configuration file (with complete path to the file).

Installing NPS on Each System in the Environment

To install NPS on each system., follow these steps:

1. Insert the NNM iSPI Performance for Metrics installation media into the DVD drive.
2. Use the cd command to change to the media directory.
3. From the media root, run the setup file:

   On Windows, double-click the **setup.exe** file.

   On Linux, run the following command:

   ./setup.bin

   The installation wizard opens.

   Select the language of the wizard, and then click **OK**.

   If the application requirement check warnings dialog box opens, review the warning messages, take appropriate action, and the click Continue.

[1] Common Internet File System (CIFS) is an application-layer file sharing protocol.

4. On the Introduction page, click Next. The License Agreement page opens.
5. Select I accept the terms, and click Next. The Select Features page opens.
6. Clear the NNM iSPI Performance for Metrics–ExtensionPacks check box.

    Note: You must clear the check box at this step. After installation and configuration, you can activate the NNM iSPI Performance for Metrics Extension Packs with the help of the `metricsExtensionPacks.ovpl` script.

7. Click **Next**.

    On Windows only. The Choose the Installation Directory page opens. If you want to install NPS in a non-default directory (or drive), make appropriate selections, and then click **Next**.

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

8. When the installation check succeeds, click **Next**.

    If the installation check shows warnings and errors, review the messages, take appropriate action, and then click **Next**.

    If the installer check shows necessary libraries are missing, follow these steps:

    a. Note down the names of missing libraries indicated by the installation wizard.
    b. Make sure the system is connected to the Internet and set up to work with Red Hat Network updates.
    c. To install each missing library, run the following command:

        yum install<*library*>

        In this instance, <*library*> is the name of the missing library as indicated by the installation wizard.

        You can specify multiple libraries in the command—each separated by a space. (For example, **yum install openmotif.x86_64 libXp.x86_64 libpng.x86_64**.)

    d. Type **Y** to install the libraries.

    While installing these libraries, you may see the following error message:

    ```
    Error: Multilib version problems found.
    ```

    To resolve this issue, run the following command:

    yum update<*library_name*>

    In this instance, <*library_name*> is the library name without the architecture field (i686 or x86_64).

    For example, if you see the error while installing `libXp.i686`, run the following command:

    yum update libXp

    After successfully running the **yum update** command, run the command to install the missing library (step c).

    The Pre-Install Summary page opens.

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

The Choose Java JDK dialog box opens.

NNM iSPI Performance for Metrics requires that Java Development Kit (JDK) 1.8 be available on the system. This version of the NNM iSPI Performance for Metrics installer contains OpenJDK 1.8. You can select the **Install bundled OpenJDK** option to install OpenJDK 1.8 that is embedded with the NNM iSPI Performance for Metrics media.

Alternatively, if another version of JDK 1.8 is already available on the system, you can select the Use Already-Installed JDK option, and then click **Browse** to select the path to the JDK.

On Linux, it is recommended that you use the JDK 1.8.x provided by your operating system vendor (Red Hat or SUSE).

> For example:
>
> To install Red Hat OpenJDK 1.8.x on Red Hat Enterprise Linux, run the following command:
>
> **yum install java-1.8.0-openjdk-devel.x86_64**
>
> To install SUSE OpenJDK 1.8.x on SUSE Linux, run the following command:
>
> **zypper install java-1_8_0-openjdk**

To find out the directory where JDK is installed, run one of the following commands:

whereis java

which java

On Windows, it is recommended that you install the Oracle JDK 1.8.x.

> **Tip:** Click **Validate** to check that the specified path is valid.

After making a selection, click **Continue**.

Toward the end of the installation process, the HPE NNM iSPI Performance Configuration window opens.

Do the following:

a. Select the Remote CIFS Share Access option, and then specify the share name, account name, and password. Use the same details that you provided while running the `nnmenableperfspi.ovpl` script.

   > **Tip:** You can find the network share and user account details specified during the last run of the `nnmenableperfspi.ovpl` file in the following file on the NNMi management server:
   >
   > (The file does not store the password.)
   >
   > *On Linux:*
   >
   > `/var/opt/OV/log/nnmenableperfspi.txt`
   >
   > *On Windows:*
   >
   > `%nnmdatadir%\log\nnmenableperfspi.txt`

   Do not modify the data retention period values. Do not click **Start** under Service Status.

b. Click **Apply**.

c. Click **Exit**.

Additional Configuration for NNMi in Application Failover

If NNMi is installed in an application failover cluster, place the `cluster.keystore` file on each role by following these steps:

1. On the NNMi management server, copy the `cluster.keystore` file from the following directory:
   - For NNMi on Windows:
     `%NnmDataDir%\shared\nnm\conf\nnmcluster`
   - For NNMi on Linux:
     `/var/opt/OV/shared/nnm/conf/nnmcluster`
2. On each server in the distributed deployment, place the `cluster.keystore` file in the following directory:
   - On Windows: `%npsdatadir%\nnmappfailover\keystore`
   - On Linux: `/var/opt/OV/NNMPerformanceSPI/nnmappfailover/keystore`

Also, update the `nms-cluster.properties` file by following these steps:

1. Log on to the active NNMi management server.
2. Go to the following directory:
   - *Windows:* `%NnmDataDir%\shared\nnm\conf\props`
   - *Linux:* `/var/opt/OV/shared/nnm/conf/props`
3. Set the `com.hp.ov.nms.cluster.getActiveMethod` property to **https** if you want to configure NNMi and NPS to use only HTTPS; set the property to **http** if you want to configure NNMi and NPS to use HTTP.
4. Save the file.
5. Restart NNMi by running the following commands:
   - *On Windows:*
     i. **%nnminstalldir%\bin\ovstop -c**
     ii. **%nnminstalldir%\bin\ovstart -c**
   - *On Linux:*
     i. **/opt/OV/bin/ovstop -c**
     ii. **/opt/OV/bin/ovstart -c**

Assign Roles

You can assign roles to an NPS system by configuring the `serverRoleConfig.cfg` file first, and then running the `configureNpsServer.ovpl` command.

Note: Once role assignment is complete, you cannot configure an NPS system in a distributed deployment to assume a different role.

In this configuration step, you need to specify the details of the network share and user account specified while running the `nnmenableperfspi.ovpl` script. As a best practice, you must always securely note down share and user account details that are specified while running the `nnmenableperfspi.ovpl` script.

You can find the network share and user account details specified during the last run of the `nnmenableperfspi.ovpl` file in the following file on the NNMi management server:

(The file does not store the password.)

On Linux:

`/var/opt/OV/log/nnmenableperfspi.txt`

On Windows:

`%nnmdatadir%\log\nnmenableperfspi.txt`

The NPS installer places the `serverRoleConfig.cfg` file in the following directory:

- *On Windows:* `%NPSInstallDir%\config`
- *On Linux:* `$NPSInstallDir/config`

To configure the `serverRoleConfig.cfg` file, follow these steps:

1. Log on to the NPS system.
2. Open the `serverRoleConfig.cfg` file with a text editor.
3. Make only the following changes to the file:
   - To configure only the DB Server role, set the following properties to the values shown here:

Property	Value
Role.Etl	0
Role.UiBi	0
Role.DB	1

   - To configure only the UiBi Server role, set the following properties to the values shown here:

Property	Value
Role.Etl	0
Role.Db	0
Role.UiBi	1
UiBi.DbServer.Hostname	Type the FQDN of the DB Server. If you want to configure multiple DB Servers, specify the FQDN of the Controller.
UiBi.NnmServer.Hostname	Type the FQDN of the NNMi management server.
UiBi.NnmServer.Share.Name	Type the name of the network share created on the NNMi

Property	Value
	management server while running the `nnmenableperfspi.ovpl` script.
UiBi.NnmServer.Share.User	Type the name of the user account specified while running the `nnmenableperfspi.ovpl` script.
UiBi.NnmServer.Share.Pass	Type the password of the above user account.

- To configure only the ETL Server role, set the following properties to the values shown here:

Property	Value
Role.ETL	1
Role.Db	0
Role.UiBi	0
Etl.DbServer.Hostname	Type the FQDN of the DB Server. If you want to configure multiple DB Servers, specify the FQDN of the Controller.
Etl.UiBiServer.Hostname	Type the FQDN of the UiBi Server.
Etl.NnmServer.Hostname	Type the FQDN of the NNMi management server.
Etl.RuntimeConfig.PRSPI_ DISABLE_ EXTENSIONPACK_ AUTOINSTALL	0 **Note:** If you want to configure multiple ETL Servers, make sure, at a given point, this value is set to 0 only on one ETL Server.
Etl.RuntimeConfig.PRSPI_ DISABLE_ CUSTOMCOLLECTION_ AUTOINSTALL	0 **Note:** If you want to configure multiple ETL Servers, make sure, at a given point, this value is set to 0 only on one ETL Server.

- To configure the DB Server and ETL Server roles, set the following properties to the values shown here:

Property	Value
Role.ETL	1
Role.UiBi	0

Property	Value
Role.Db	1
Etl.DbServer.Hostname	Type the FQDN of the DB Server. If you want to configure multiple DB Servers, specify the FQDN of the Controller.
Etl.UiBiServer.Hostname	Type the FQDN of the UiBi Server.
Etl.NnmServer.Hostname	Type the FQDN of the NNMi management server.
Etl.RuntimeConfig.PRSPI_ DISABLE_ EXTENSIONPACK_ AUTOINSTALL	0 **Note:** If you want to configure multiple ETL Servers, make sure, at a given point, this value is set to 0 only on one ETL Server.
Etl.RuntimeConfig.PRSPI_ DISABLE_ CUSTOMCOLLECTION_ AUTOINSTALL	0 **Note:** If you want to configure multiple ETL Servers, make sure, at a given point, this value is set to 0 only on one ETL Server.

- To configure the UiBi Server and ETL Server roles, set the following properties to the values shown here:

Property	Value
Role.ETL	1
Role.UiBi	1
Role.Db	0
Etl.DbServer.Hostname	Type the FQDN of the DB Server. If you want to configure multiple DB Servers, specify the FQDN of the Controller.
Etl.NnmServer.Hostname	Type the FQDN of the NNMi management server.
Etl.NnmServer.Share.Name	Type the name of the network share created on the NNMi management server while running the `nnmenableperfspi.ovpl` script.
Etl.NnmServer.Share.User	Type the name of the user account specified while running the `nnmenableperfspi.ovpl` script.
Etl.NnmServer.Share.Pass	Type the password of the above user account.

Property	Value
UiBi.DbServer.Hostname	Type the FQDN of the DB Server. If you want to configure multiple DB Servers, specify the FQDN of the Controller.
UiBi.NnmServer.Hostname	Type the FQDN of the NNMi management server.
UiBi.NnmServer.Share.Name	Type the name of the network share created on the NNMi management server while running the `nnmenableperfspi.ovpl` script.
UiBi.NnmServer.Share.User	Type the name of the user account specified while running the `nnmenableperfspi.ovpl` script.
UiBi.NnmServer.Share.Pass	Type the password of the above user account.
Etl.RuntimeConfig.PRSPI_ DISABLE_ EXTENSIONPACK_ AUTOINSTALL	0 **Note:** If you want to configure multiple ETL Servers, make sure, at a given point, this value is set to 0 only on one ETL Server.
Etl.RuntimeConfig.PRSPI_ DISABLE_ CUSTOMCOLLECTION_ AUTOINSTALL	0 **Note:** If you want to configure multiple ETL Servers, make sure, at a given point, this value is set to 0 only on one ETL Server.

- To configure only the DB Server and UiBi Server roles, set the following properties to the values shown here:

Property	Value
Role.ETL	0
Role.UiBi	1
Role.Db	1
Etl.DbServer.Hostname	Type the FQDN of the DB Server. If you want to configure multiple DB Servers, specify the FQDN of the Controller.
Etl.UiBiServer.Hostname	Type the FQDN of the UiBi Server.
UiBi.DbServer.Hostname	Type the FQDN of the DB Server.
UiBi.NnmServer.Hostname	Type the FQDN of the NNMi management server.

Property	Value
UiBi.NnmServer.Share.Name	Type the name of the network share created on the NNMi management server while running the `nnmenableperfspi.ovpl` script.
UiBi.NnmServer.Share.User	Type the name of the user account specified while running the `nnmenableperfspi.ovpl` script.
UiBi.NnmServer.Share.Pass	Type the password of the above user account.

4. Save the file.

   > **Tip:** Always retain a backup of this file.

5. Drop the database from NPS systems where the DB Server role will not be present.

   a. Identify the systems where you are not going to enable the DB Server role. You can do this by inspecting the contents of the `serverRoleConfig.cfg` file that you have modified on each system.

      If the `Role.Db` parameter is set to 0 in the `serverRoleConfig.cfg` file, the system will not have the DB Server role activated after this procedure is complete.

   b. Log on as `root` or `administrator` to the systems where the DB Server role will not be present, and then run the following command:

      initializeNPS.ovpl -a DropPerfSPIDB

      > **Caution:** Running this command on an incorrect NPS system (that is, the system where the DB Server role. is going to remain active) will lead to data loss.

6. Log on as `root` or `administrator` to each NPS system, and then run the following command:

   > **Note:** Run this command on NPS system in the following order:
   >
   > a. The DB Server
   >
   > b. The UiBi Server
   >
   > c. The ETL Servers

   configureNpsServer.ovpl -f <*config_file*>

   In this instance, <*config_file*> is the name (with the full path) of the configuration file.

   > **Tip:** As a best practice, take a backup of the `serverRoleConfig.cfg` file that you configured for use with the `configureNpsServer.ovpl` script.

Additional Configuration for Multiple DB Servers

> **Note:** You can plan to configure multiple DB Servers if you have a very large environment with high

usage of interactive (not scheduled) reports.

Multiple DB Servers are supported only in a Linux environment. Also, you must configure a shared storage system with raw disks with the help of the Storage Area Network (SAN) infrastructure while creating multiple DB Servers.

As a best practice, if you need to configure multiple DB Servers, always start with two servers. Later, based on the performance of the solution, you can add more DB Servers to the environment.

The multiple DB Server configuration requires creating a Controller node and at least one Secondary node. Make sure that all the requirements listed in "Prerequisites for Configuring Multiple DB Servers" on page 21 are met.

HPE recommends that you create only one Secondary node in the beginning. If you continue to see performance problems, you can create additional Secondary nodes.

Create the Controller Node

To create a Controller node:

Note: Do not create more than one Controller node.

1. Log on to a DB Server as root.
2. Create a new directory by running the following command:

   mkdir /opt/OV/db_setup
3. Copy setup scripts from the NNM iSPI Performance for Metrics media to the newly created directory:

   cd /opt/OV/db_setup

   cp <*NPS_Installer_Root*>**/packages/misc/multiplex/* . dos2unix *.sh**

   chmod a+r *.sh
4. Create initial devices:

   a. Open the `makeInitialRawDevices.sh` script with a text editor.

   b. Replace the WWID values of `SYSTEM_TEMP_WWID`, `SYSTEM_MAIN_WWID`, and `USER_MAIN_WWID` with the correct WWID values from the details that you noted down in step 3.

      Example:

      ```
      # SYSTEM_TEMP must be a unique WWID for each node in the multiplex
      SYSTEM_TEMP_WWID=36001438005dea10300008000002e0000

      # SYSTEM_MAIN and USER_MAIN must be shared WWIDs, presented by SAN to all
      nodes in MPLEX
      SYSTEM_MAIN_WWID=36001438005dea10300008000000b0000
      USER_MAIN_WWID=36001438005dea1030000800000050000
      ```

      Note: `SYSTEM_TEMP_WWID` must be unique on each DB Server. `SYSTEM_MAIN_WWID` and `USER_MAIN_WWID` are common across all servers.

   c. Save the file.

   d. Run the following command:

      ./makeInitialRawDevices.sh

      Type **yes** when you are prompted to confirm if you want to replace the existing database.

5. Create the database on the Controller node by running the following command:

   ./createControllerDB.sh

   The command creates a database by using the raw devices and scripts configured in the previous step.

   If the command fails, see the log messages in the `/var/opt/OV/logs/createControllerDB.sh.log` file.

6. Add additional DB Servers.

   a. Open the `addMultiplexServers.sh` script with a text editor.

   b. Replace the hostnames with the hostnames of each of the remaining DB Servers in your deployment. Add or remove lines as needed; end each line with a backslash.

      ```
      REMOTE_HOSTNAMES="\

        nnmsaw2-cronus \

        nnmsaw2-hyperion \

        nnmsaw1-zeta \

        nnmsaw2-eos \
      "
      ```

   c. Save the file.

   d. Run the following command:

      ./addMultiplexServers.sh

      The command performs the following tasks:

      - Initializes this server as the Controller node
      - Authorizes each additional server as the Secondary node

7. Run the following command:

   resetSPI.ovpl

8. Make sure that the database is up and running. Check the status of the database by running the following command:

   statusDB.ovpl

Create a Secondary Node

To create a Secondary node:

1. Open the `setupSecondaryNode.sh` script with a text editor.
2. Set the `CONTROLLER_HOSTNAME` property to the hostname of this Controller node.

   For example, if the hostname of the Controller node configured in the above procedure is `nnmsaw2-lapetos`, set the property to:

```
CONTROLLER_HOSTNAME=nnmsaw2-lapetos
```

3. Save the file.

> **Note:** Do not run the `setupSecondaryNode.sh` script on the Controller node. This script will be copied over to the Secondary nodes.

4. Log on as root to the node that was identified as the Secondary node.
5. Create a new directory by running the following command:

   mkdir /opt/OV/db_setup
6. Copy the following setup scripts from the `/opt/OV/db_setup` directory on the Controller node to the newly created directory on this Secondary node:

   ```
   makeInitialRawDevices.sh
   ```

   ```
   setupSecondaryNode.sh
   ```
7. Create initial devices:
   1. Open the `makeInitialRawDevices.sh` script with a text editor.
   2. Replace the SYSTEM_TEMP WWID values with the correct WWID values from the details that you noted down in step 3.

      The content of the file may look like this:

      ```
      # SYSTEM_TEMP must be a unique WWID for each node in the multiplex
      SYSTEM_TEMP_WWID=36001438005dea10300008000002e0000
      ```

      ```
      # SYSTEM_MAIN and USER_MAIN must be shared WWIDs, presented by SAN to all nodes
      in MPLEX
      SYSTEM_MAIN_WWID=36001438005dea10300008000000b0000
      USER_MAIN_WWID=36001438005dea1030000800000050000
      ```

      > **Note:** `SYSTEM_TEMP_WWID` must be unique on each DB Server. `SYSTEM_MAIN_WWID` is common across all servers.
   3. Save the file.
   4. Run the following command:

      ./makeInitialRawDevices.sh

      Type **yes** when you are prompted to confirm if you want to replace the existing database.
8. Create the Secondary database by running the following command:

   ./setupSecondaryNode.sh
9. Verify that the Secondary server is created successfully.
   - Run the following command to check the status of the database:

     statusDB
   - Run the following command:

     dbisql -c "DSN=PerfspiDSN" "sp_iqmpxvalidate"

The output should list:

```
No errors detected
```

Configure the UiBi Server

Configure the UiBi Server to connect to the Secondary node:

1. Log on to the UiBi Server.
2. Run the following command:

   iqdsn -y -w <*secondary_hostname*>**DSN -c "UID=DBA;PWD= HP_IQ; AutoPreCommit=N;CommLinks=tcpip{port=9306;host=**<*secondary_hostname*>**;DOBROADCAST=NONE;VERIFY=NO}"**

   In this instance, <*secondary_hostname*> is the host name of the Secondary node (only host name, not FQDN).

   For example:

   iqdsn -y -w NPSDBServer2DSN -c "UID=DBA;PWD= HP_IQ; AutoPreCommit=N;CommLinks=tcpip {port=9306;host=NPSDBServer2;DOBROADCAST=NONE;VERIFY=NO}"

   where the host name of the Secondary node is `NPSDBServer2`.

   > **Note:** If the host name of the Secondary node contains the hyphen (-) characters, follow these steps:
   >
   > a. Open the following file on the UiBi Server:
   >
   > ```
   > /var/opt/OV/NNMPerformanceSPI/database/perfspi.cfg
   > ```
   >
   > b. Go below the following line:
   >
   > ```
   > #startup parameters for PerfSPIDB database
   > ```
   >
   > c. In the line underneath, replace the hyphen (-) character in the Secondary host name with the underscore (_) character.
   >
   > d. Save the file.

3. Run the following command:

   dbping –d –c “DSN=<*seondary_hostname*>**DSN”**

   In this instance, <*secondary_hostname*> is the host name of the Secondary node (only host name, not FQDN).

   For example:

   dbping –d –c “DSN=NPSDVServer2DSN”

   where the host name of the Secondary node is `NPSDBServer2`.

   The output of the command should display the following message:

   ```
   Ping database successful.
   ```

   If the command fails, check that the Linux firewall is not blocking communication.
4. Open the following file with a text editor:

`/var/opt/OV/NNMPerformanceSPI/rconfig/NNMPerformanceSPI.cfg`

5. Set the `PRSPI_DB_DSN` parameter to <*seondary_hostname*>`DSN`.

   In this instance, <*secondary_hostname*> is the host name of the Secondary node (only host name, not FQDN).
6. Save the file.

Install iSPIs and Extension Packs

Install iSPIs and custom poller Extension Packs only after assigning roles to all systems in the distributed deployment of NPS. If you install iSPIs and custom poller Extension Packs before configuring roles for NPS systems, duplicate instances of Extension Packs will be installed in your environment.

Install iSPIs and Custom Poller Extension Packs in an Environment with a Single ETL Server

Before you install any iSPIs, follow these steps:

1. Make sure that the `Etl.RuntimeConfig.PRSPI_DISABLE_EXTENSIONPACK_AUTOINSTALL` property is set to 0 in the `serverRoleConfig.cfg` file on the ETL Server.
2. Make sure that the `Etl.RuntimeConfig.PRSPI_DISABLE_CUSTOMCOLLECTION_AUTOINSTALL` property is set to 0 in the `serverRoleConfig.cfg` file on the ETL Server.

   > **Tip:** Changes in the `serverRoleConfig.cfg` file take effect only after you run the **configureNpsServer.ovpl -f** <*config_file*> command on the system.

3. If you want to use the NNM iSPI Performance for Metrics Extension Packs, you must install the NNM iSPI Performance for Metrics on the ETL Server by running the following command:

   On Windows:

   %npsinstalldir%\bin\metricsExtensionPacks.ovpl install

   On Linux:

   /opt/OV/NNMPerformanceSPI/bin/metricsExtensionPacks.ovpl install

   Additionally, log on to the UiBi Server, and then run the following command to install the Path Health Extension Pack:

   On Windows:

   %npsinstalldir%\bin\installPathHealth.ovpl

   On Linux:

   /opt/OV/NNMPerformanceSPI/bin/installPathHealth.ovpl
4. Install the iSPI by following the instructions in the iSPI documentation.
5. Install the custom poller Extension Packs by following the instructions in the NPS Online Help.
6. After installation, restart the NPS processes by running the following commands on each NPS system in the environment:

   stopALL.ovpl

   startALL.ovpl

Install iSPIs and Custom Poller Extension Packs in an Environment with Multiple ETL Servers

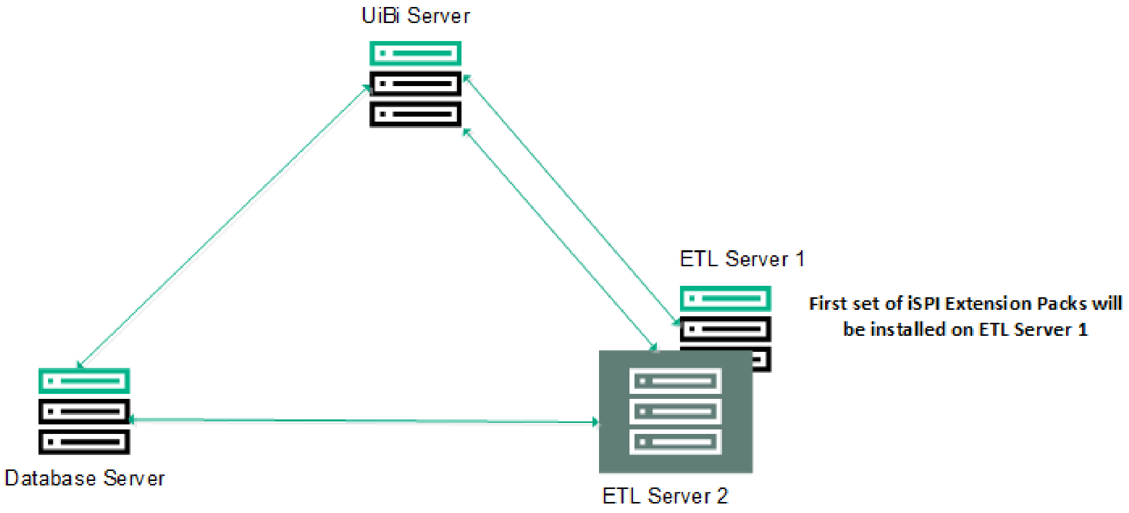
The benefit of assigning the ETL Server role on multiple systems is you can distribute the load of processing multiple Extension Packs across a series of servers. The `Etl.RuntimeConfig.PRSPI_DISABLE_EXTENSIONPACK_AUTOINSTALL` and `Etl.RuntimeConfig.PRSPI_DISABLE_CUSTOMCOLLECTION_AUTOINSTALL` properties help you distribute this load.

The iSPI Extension Packs are automatically transferred to the ETL Server where `Etl.RuntimeConfig.PRSPI_DISABLE_EXTENSIONPACK_AUTOINSTALL` is set to 0. Similarly, the custom poller Extension Packs are automatically transferred to the ETL Server where `Etl.RuntimeConfig.PRSPI_DISABLE_CUSTOMCOLLECTION_AUTOINSTALL` is set to 0.

To distribute the load across multiple ETL Servers, follow this work-flow:

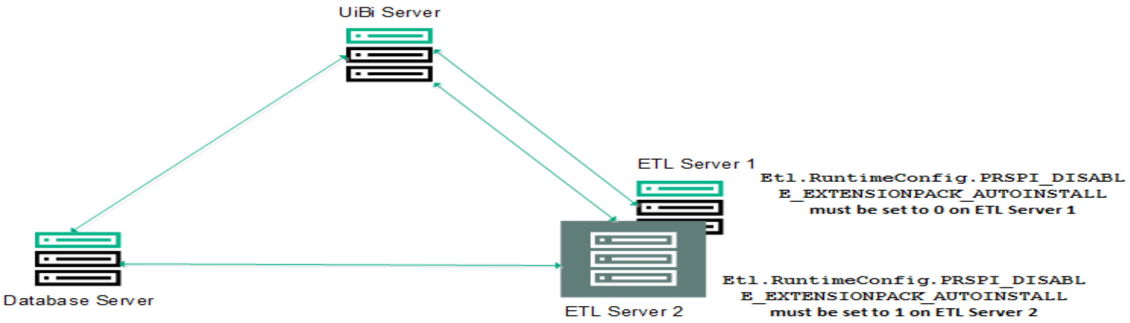
For iSPI Extension Packs

1. Identify the ETL Server on which you want to install first set of iSPI Extension Packs.


UiBi Server
ETL Server 1
First set of iSPI Extension Packs will be installed on ETL Server 1
Database Server
ETL Server 2

2. Make sure that `Etl.RuntimeConfig.PRSPI_DISABLE_EXTENSIONPACK_AUTOINSTALL` is set to 0 in the `serverRoleConfig.cfg` file on the identified ETL Server.

   `Etl.RuntimeConfig.PRSPI_DISABLE_EXTENSIONPACK_AUTOINSTALL` must be set to 1 in the `serverRoleConfig.cfg` file on all other ETL Servers.


UiBi Server
ETL Server 1
Etl.RuntimeConfig.PRSPI_DISABL
E_EXTENSIONPACK_AUTOINSTALL
must be set to 0 on ETL Server 1
Database Server
ETL Server 2
Etl.RuntimeConfig.PRSPI_DISABL
E_EXTENSIONPACK_AUTOINSTALL
must be set to 1 on ETL Server 2

3. Install the first set of iSPIs by following the iSPI documentation. After the iSPI installation is complete, the Extension Packs are automatically transferred and installed on the identified ETL Server.
4. Run the **about.ovpl** command on the ETL Server to verify that Extension Packs are installed correctly.

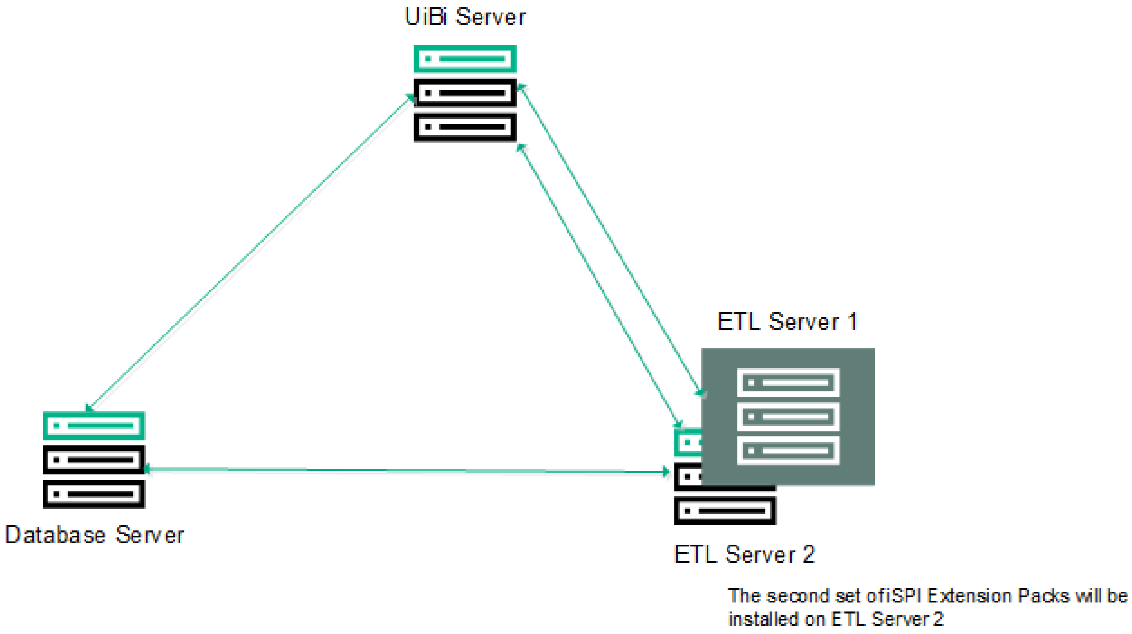
   If you see that an Extension Pack, which you did not originally plan to install on this server, has been installed inadvertently, you can disable that Extension Pack on this server by running the following command:

   disableExtensionPackEtl.ovpl -p <*Extension_Pack*>

   In this instance, <*Extension_Pack*> is the name of the Extension Pack displayed by the `about.ovpl` command.

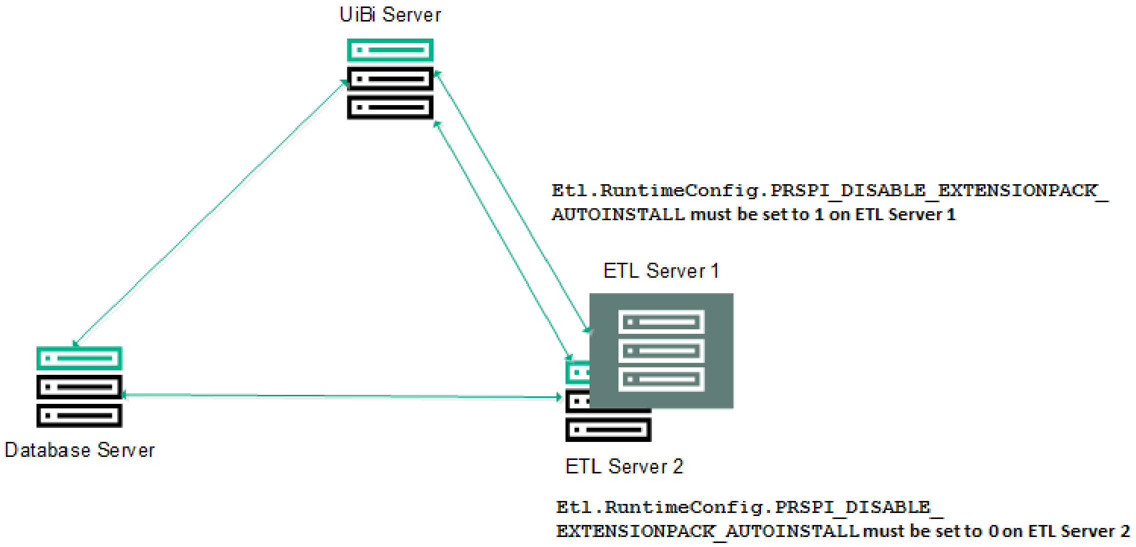
   > **Note:** You can enable an Extension Pack by running the following command:
   >
   > **enableExtensionPackEtl.ovpl -p** <*Extension_Pack*>

5. Identify the ETL Server on which you want to install the second set of iSPI Extension Packs.


UiBi Server
ETL Server 1
Database Server
ETL Server 2
The second set of iSPI Extension Packs will be installed on ETL Server 2

6. Make sure that `Etl.RuntimeConfig.PRSPI_DISABLE_EXTENSIONPACK_AUTOINSTALL` is set to 0 in the `serverRoleConfig.cfg` file on the identified ETL Server.

   `Etl.RuntimeConfig.PRSPI_DISABLE_EXTENSIONPACK_AUTOINSTALL` must be set to 1 in the `serverRoleConfig.cfg` file on all other ETL Servers.


UiBi Server
Etl.RuntimeConfig.PRSPI_DISABLE_EXTENSIONPACK_AUTOINSTALL must be set to 1 on ETL Server 1
ETL Server 1
Database Server
ETL Server 2
Etl.RuntimeConfig.PRSPI_DISABLE_EXTENSIONPACK_AUTOINSTALL must be set to 0 on ETL Server 2

7. Install the second set of iSPIs by following the iSPI documentation. After the iSPI installation is complete, the Extension Packs are automatically transferred and installed on the identified ETL Server.
8. Run the **about.ovpl** command on the ETL Server to verify that Extension Packs are installed correctly.

   If you see that an Extension Pack, which you did not originally plan to install on this server, has been installed inadvertently, you can disable that Extension Pack on this server by running the following command:

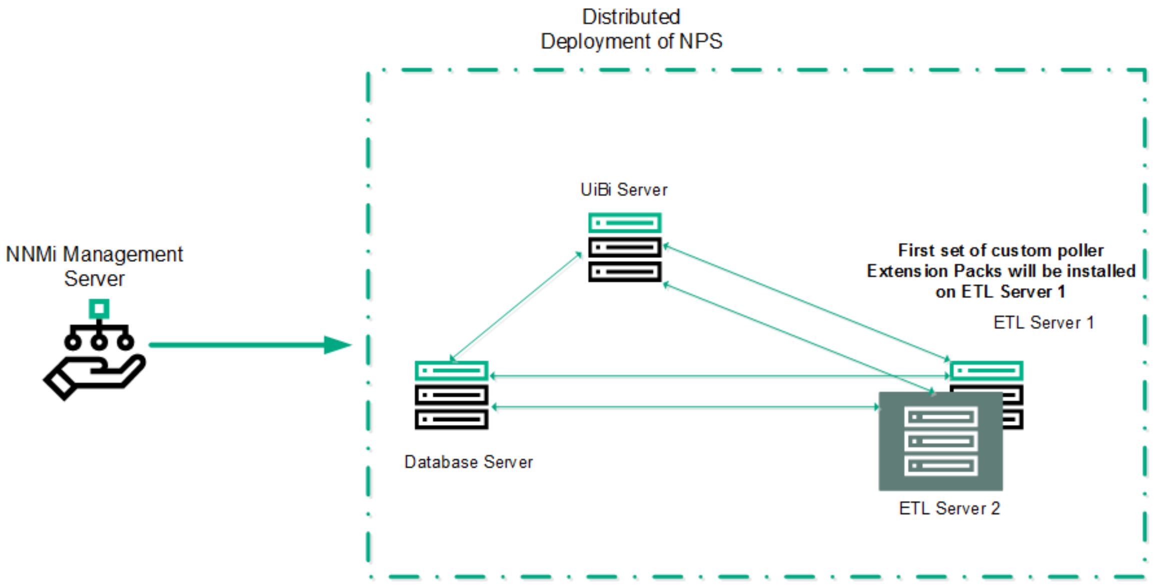
   disableExtensionPackEtl.ovpl -p <*Extension_Pack*>

In this instance, <*Extension_Pack*> is the name of the Extension Pack displayed by the `about.ovpl` command.

> **Note:** You can enable an Extension Pack by running the following command:
>
> **enableExtensionPackEtl.ovpl -p** <*Extension_Pack*>

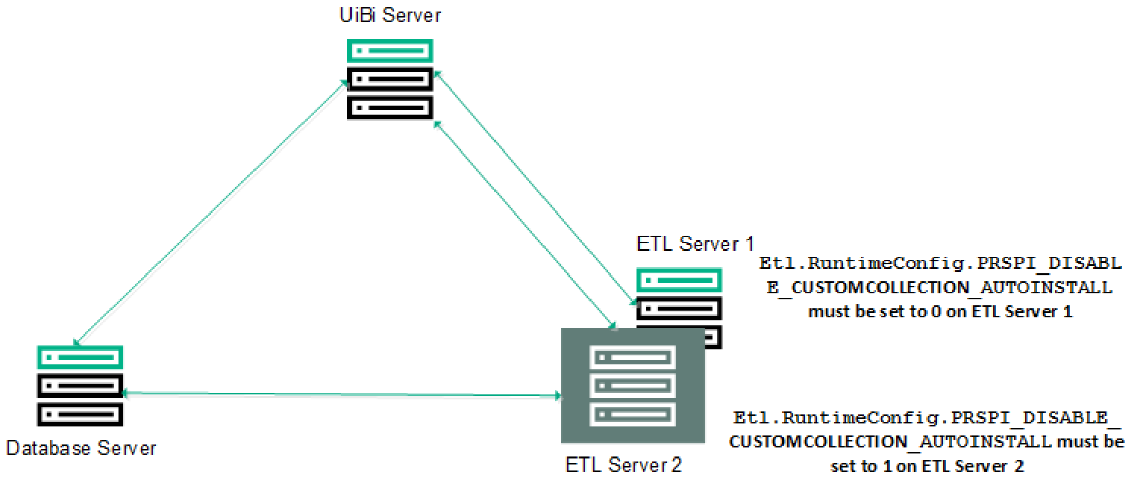
For Custom Poller Extension Packs

1. Identify the ETL Server on which you want to install first set of custom poller Extension Packs.



2. Make sure that `Etl.RuntimeConfig.PRSPI_DISABLE_CUSTOMCOLLECTION_AUTOINSTALL` is set to 0 in the `serverRoleConfig.cfg` file on the identified ETL Server.

   `Etl.RuntimeConfig.PRSPI_DISABLE_CUSTOMCOLLECTION_AUTOINSTALL` must be set to 1 in the `serverRoleConfig.cfg` file on all other ETL Servers.


UiBi Server
ETL Server 1
Etl.RuntimeConfig.PRSPI_DISABL
E_CUSTOMCOLLECTION_AUTOINSTALL
must be set to 0 on ETL Server 1
Database Server
ETL Server 2
Etl.RuntimeConfig.PRSPI_DISABLE_
CUSTOMCOLLECTION_AUTOINSTALL must be
set to 1 on ETL Server 2

3. Install the first set of custom poller Extension Packs by following the NPS Online Help.
4. Run the **about.ovpl** command on the ETL Server to verify that Extension Packs are installed correctly.

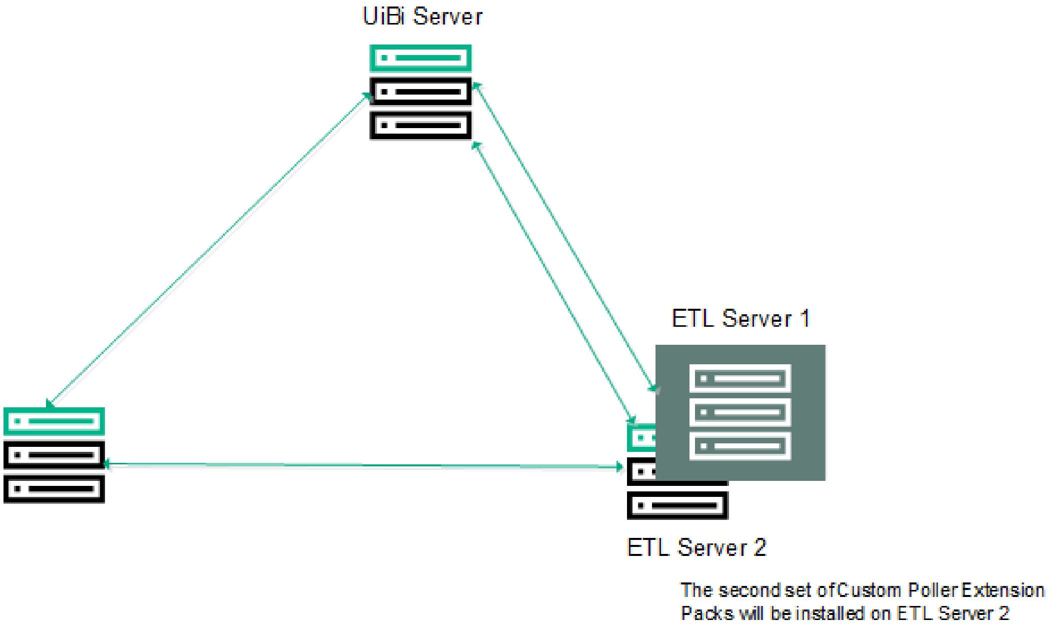
If you see that an Extension Pack, which you did not originally plan to install on this server, has been installed inadvertently, you can disable that Extension Pack on this server by running the following command:

disableExtensionPackEtl.ovpl -p <*Extension_Pack*>

In this instance, <*Extension_Pack*> is the name of the Extension Pack displayed by the `about.ovpl` command.

> **Note:** You can enable an Extension Pack by running the following command:
>
> **enableExtensionPackEtl.ovpl -p** <*Extension_Pack*>

5. Identify the ETL Server on which you want to install the second set of custom poller Extension Packs.


UiBi Server
ETL Server 1
ETL Server 2
The second set of Custom Poller Extension Packs will be installed on ETL Server 2

6. Make sure that `Etl.RuntimeConfig.PRSPI_DISABLE_CUSTOMCOLLECTION_AUTOINSTALL` is set to 0 in the `serverRoleConfig.cfg` file on the identified ETL Server.

   `Etl.RuntimeConfig.PRSPI_DISABLE_CUSTOMCOLLECTION_AUTOINSTALL` must be set to 1 in the `serverRoleConfig.cfg` file on all other ETL Servers.
7. Install the second set of custom poller Extension Packs by following the NPS Online Help.
8. Run the **about.ovpl** command on the ETL Server to verify that Extension Packs are installed correctly.

   If you see that an Extension Pack, which you did not originally plan to install on this server, has been installed inadvertently, you can disable that Extension Pack on this server by running the following command:

   disableExtensionPackEtl.ovpl -p <*Extension_Pack*>

   In this instance, <*Extension_Pack*> is the name of the Extension Pack displayed by the `about.ovpl` command.

> **Note:** You can enable an Extension Pack by running the following command:
>
> **enableExtensionPackEtl.ovpl -p** <*Extension_Pack*>

9. After installation, restart the NPS processes by running the following commands on each NPS system in the environment:

   stopALL.ovpl

   startALL.ovpl

Configuring Additional DB Servers

This section provides instructions to introduce additional DB Servers to a distributed deployment of NPS with multiple DB Servers. After creating a distributed deployment of NPS with two DB Servers, if you continue to see performance problems, plan to add another DB Server to the environment and configure the new DB Server to operate as a Secondary node. You can distribute the processing load of Extension Packs between the two Secondary nodes.

> **Note:** Follow the steps in this section only if you have created a distributed deployment of NPS with a Controller DB Server and at least one Secondary DB Server. Do not follow the steps if you have not already created a distributed deployment of NPS with at least two DB Servers.

Create a New Secondary DB Server

1. Install NPS on a new system and configure the DB Server role.
2. Follow the instructions in the "Assign Roles" on page 30 to configure the DB Server role.
3. Log on to the new DB Server, and then configure the DB Server to operate as a Secondary node.

   To create a Secondary node:

   a. Open the `setupSecondaryNode.sh` script with a text editor.

   b. Set the `CONTROLLER_HOSTNAME` property to the hostname of this Controller node.

      For example, if the hostname of the Controller node configured in the above procedure is `nnmsaw2-lapetos`, set the property to:

      ```
      CONTROLLER_HOSTNAME=nnmsaw2-lapetos
      ```

   c. Save the file.

      > **Note:** Do not run the `setupSecondaryNode.sh` script on the Controller node. This script will be copied over to the Secondary nodes.

   d. Log on as root to the node that was identified as the Secondary node.

   e. Create a new directory by running the following command:

      mkdir /opt/OV/db_setup

   f. Copy the following setup scripts from the `/opt/OV/db_setup` directory on the Controller node to the newly created directory on this Secondary node:

      ```
      makeInitialRawDevices.sh
      ```

      ```
      setupSecondaryNode.sh
      ```

   g. Create initial devices:

   i. Open the `makeInitialRawDevices.sh` script with a text editor.
   ii. Replace the SYSTEM_TEMP WWID values with the correct WWID values from the details that you noted down in step 3.

       The content of the file may look like this:

```
# SYSTEM_TEMP must be a unique WWID for each node in the multiplex
SYSTEM_TEMP_WWID=36001438005dea10300008000002e0000

# SYSTEM_MAIN and USER_MAIN must be shared WWIDs, presented by SAN to all
nodes in MPLEX
SYSTEM_MAIN_WWID=36001438005dea10300008000000b0000
USER_MAIN_WWID=36001438005dea1030000800000050000
```

> **Note:** `SYSTEM_TEMP_WWID` must be unique on each DB Server. `SYSTEM_MAIN_WWID` is common across all servers.

   iii. Save the file.
   iv. Run the following command:

       ./makeInitialRawDevices.sh

       Type **yes** when you are prompted to confirm if you want to replace the existing database.

h. Create the Secondary database by running the following command:

   ./setupSecondaryNode.sh

i. Verify that the Secondary server is created successfully.

   - Run the following command to check the status of the database:

     statusDB

   - Run the following command:

     dbisql -c "DSN=PerfspiDSN" "sp_iqmpxvalidate"

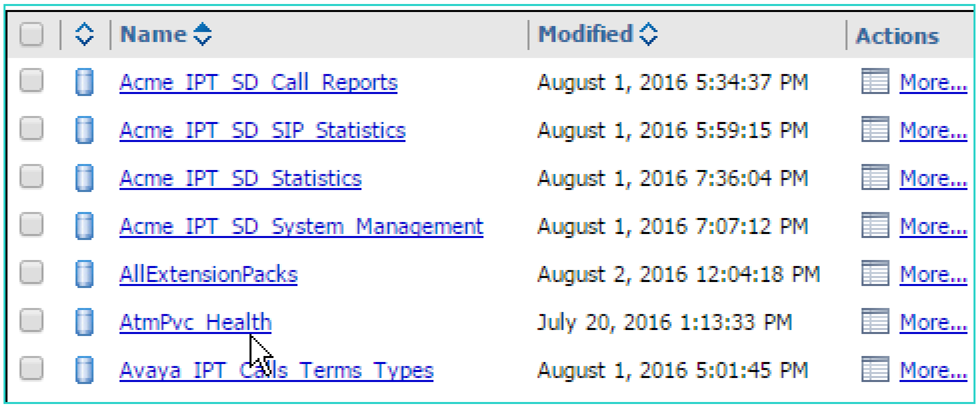
     The output should list:

```
No errors detected
```

Configure Extension Packs to Connect to the New Secondary Node

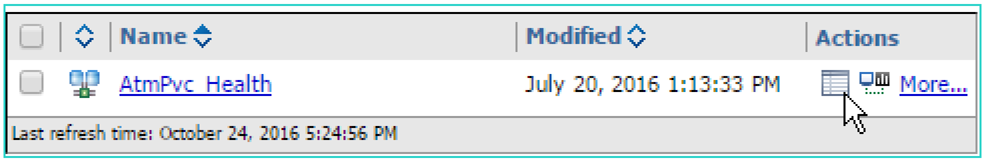
This procedure enables you to transfer the processing loads of a subset of Extension Packs to the new Secondary node.

1. Open the NPS console.
2. Click **BI Server > Administrator Log On**. The HPE NNM iSPI Performance BI Server Administration page opens.
3. Go to the Configuration tab.



□	◇	Name	Modified	Actions
□		Acme_IPT_SD_Call_Reports	August 1, 2016 5:34:37 PM	More...
□		Acme_IPT_SD_SIP_Statistics	August 1, 2016 5:59:15 PM	More...
□		Acme_IPT_SD_Statistics	August 1, 2016 7:36:04 PM	More...
□		Acme_IPT_SD_System_Management	August 1, 2016 7:07:12 PM	More...
□		AllExtensionPacks	August 2, 2016 12:04:18 PM	More...
□		AtmPvc_Health	July 20, 2016 1:13:33 PM	More...
□		Avaya_IPT_Calls_Terms_Types	August 1, 2016 5:01:45 PM	More...

4. Click an Extension Pack.

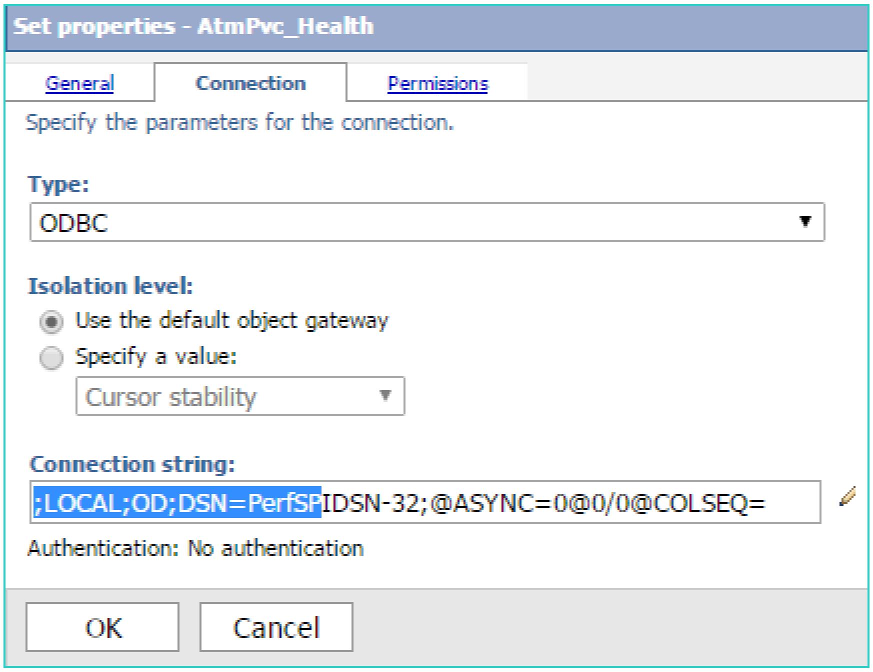


□	◇	Name	Modified	Actions
□		AtmPvc_Health	July 20, 2016 1:13:33 PM	More...

Last refresh time: October 24, 2016 5:24:56 PM

5. Click the **Set Properties** action.

6. Go to the Connections tab.



Set properties - AtmPvc_Health

General | Connection | Permissions

Specify the parameters for the connection.

Type:

ODBC ▼

Isolation level:

● Use the default object gateway

○ Specify a value:

Cursor stability ▼

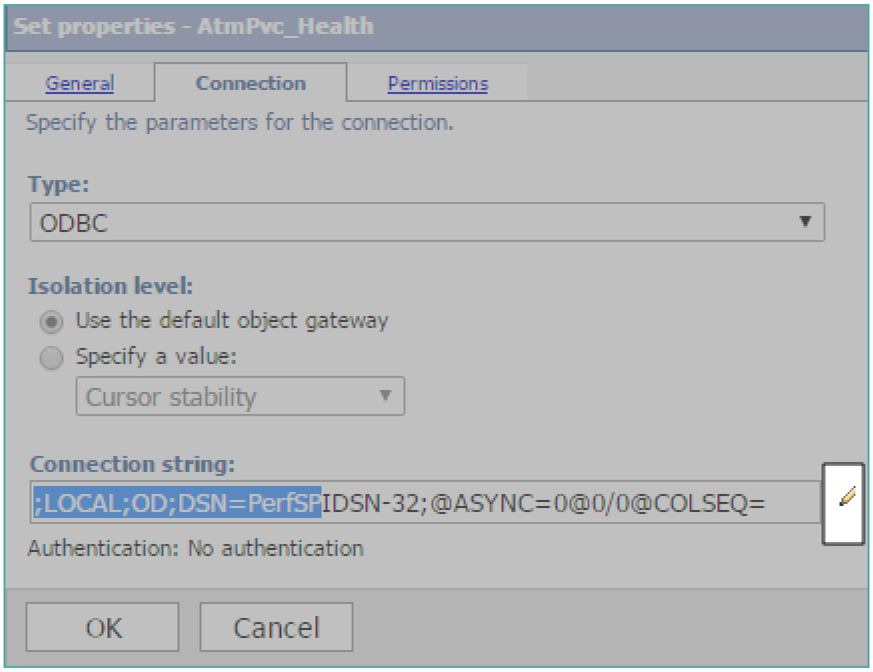
Connection string:

;LOCAL;OD;DSN=PerfSPIDSN-32;@ASYNC=0@0/0@COLSEQ=

Authentication: No authentication

OK | Cancel

7. Click the **Edit** button.



Set properties - AtmPvc_Health

Specify the parameters for the connection.

Type: ODBC

Isolation level:

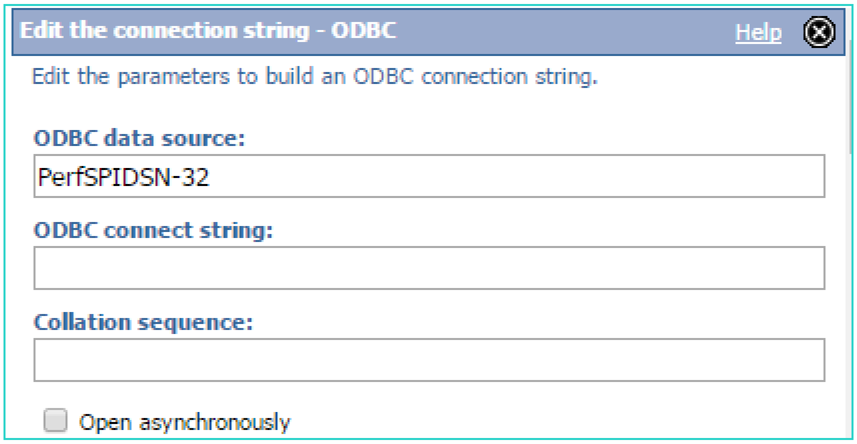
● Use the default object gateway

○ Specify a value: Cursor stability

Connection string: ;LOCAL;OD;DSN=PerfSPIDSN-32;@ASYNC=0@0/0@COLSEQ=

Authentication: No authentication

The Edit the Connection String page opens.



Edit the connection string - ODBC

Edit the parameters to build an ODBC connection string.

ODBC data source: PerfSPIDSN-32

ODBC connect string:

Collation sequence:

□ Open asynchronously

8. Type the DSN of the newly configured SecondaryDB Server in the ODBC Data Source box.

> **Tip:** The DSN of the SecondaryDB Server is of the following format:
>
> <*hostname*>`DSN`
>
> In this instance, <*hostname*> is the host name of the new Secondary node (only host name, not FQDN).

9. Click **OK**.
10. Repeat step 4 through step 9 for all the Extension Packs that you want to configure with the new Secondary node.

Switching from a Standalone Environment

Note: You cannot directly upgrade an NPS 9.20 or 9.10 standalone environment to an NPS 10.30 distributed deployment. You must first upgrade to NPS 10.30, and then follow the steps in this chapter to switch to a distributed environment. For instructions to upgrade NPS 9.10 or 9.20 to 10.30, see the *NNM iSPI Performance for Metrics Interactive Installation Guide*.

You can also start your operation with only one NPS system, and gradually expand into a distributed deployment by installing additional servers and spreading the load across them. If you observe performance degradation in your single-NPS environment due to resource bottleneck (CPU, memory, or disk I/O), you can consider building a distributed NPS environment. To create a distributed environment in phases, follow these guidelines:

1. **Split out the ETL Server to a separate server.**

   Install NPS on a new, dedicated system, and then assign the ETL Server role to the new system. On the original NPS system, configure only the DB Server and UiBi Server roles.
2. **Split out the UiBi Server or DB Server to a separate server.**

   If you continue to experience resource bottleneck on the original NPS system, disable one of the existing roles (the UiBi Server or DB Server role) on the original system, install NPS on a third system, and then assign the UiBi Server or DB Server role to the new system.
3. **Split out the ETL Server role to multiple servers.**

   If you experience resource bottleneck on the new NPS system where you configured the ETL Server role,install NPS on yet another new system, and then assign the ETL Server role to the new system. This configuration helps you distribute the ETL processing load across two different servers.

   Note: While using multiple systems with the ETL Server role, you must enable a unique set of Extension Packs on each ETL server.

- If you continue to experience performance issues on systems with the ETL Server role, install NPS on additional systems and assign only the ETL Server role to those systems. You cannot configure the UiBi Server or DB Server on multiple systems.
- Before you start migrating to a distributed deployment, always take complete backup of the existing NPS installation.

  Note: This is a precautionary step. Although you need to back up the content store and database separately, taking a complete backup will help prevent loss of data in the event of disruptive system failure during the process of migration.

  Run the following command to take a complete backup of NPS:

  backup.ovpl -b *<dir>*

  In this instance, *<dir>* is the local directory where you want to store the backup file.

  The command creates a single `.tar.gz` file.

Creating a Separate ETL Server

You can segregate out the ETL Server role by installing NPS onto a separate system and configuring the ETL Server role on that system.

To create a separate ETL Server, follow these steps:

1. "Record the Details of Your Existing NPS Environment" below
2. "Disable the ETL Server Role on the Original NPS System" on the next page
3. "Install a New instance of NPS" on page 53\
4. " Enable the ETL Server Role on the New NPS System" on page 53
5. "Run the nnmenableperspi.ovpl Script" on page 55

Record the Details of Your Existing NPS Environment

It is important to note down the details of your current NPS setup. You may migrate the ETL Server from a standalone, single-server NPS, or from an already created distributed deployment with the ETL Server co-existing with another server role on a single system.

Fill out the following table with the details of your existing environment.

Details of your existing NPS environment			
Standalone		**Distributed deployment**	
FQDN of the NPS system		FQDN of DB Server	
		FQDN of UiBi Server	
FQDN of the NNMi management server		FQDNof existing ETL Server	
		FQDN of the NNMi management server	

Also, correctly note down the share and user details that were specified while running the `nnmenableperfspi.ovpl` script. you can find these details specified during the last run of the `nnmenableperfspi.ovpl` file in the following directory on the NNMi management server:

(The file does not store the password.)

On Linux:

```
/var/opt/OV/log/nnmenableperfspi.txt
```

On Windows:

```
%nnmdatadir%\log\nnmenableperfspi.txt
```

Fill out the following table with the details:

NNMi details	
NNMi share name	

NNMi share user name	
NNMi share user password	

Disable the ETL Server Role on the Original NPS System

1. Run the following command on the original NPS system to take a backup of archived files:

   > **Note:** Since you are going to migrate the ETL Server role onto a different system, you must take a backup of all files. This backup will later be restored on the new system.

   > **Tip:** Before you begin, make sure sufficient disk space exists on the NPS system to run the backup procedure and store the backed-up data. Determine the size of the configuration and archived data files by measuring size of the following directory:
   >
   > *On Windows*
   >
   > `%npsdatadir%\NNMPerformance`
   >
   > *On Linux*
   >
   > `/var/opt/OV/NNMPerformance`

   backup.ovpl -b <*dir_file*> **-f**

   In this instance, <*dir_file*> is the local directory where you want to store the backup file. The command creates a backup file in the <*dir_file*> directory, which is a `.tar.gz` file.
2. Stop all NPS processes on the original NPS server:

   stopALL.ovpl
3. Configure the `serverRoleConfig.cfg` file to disable the ETL Server role on the original NPS system. The following table lists the parameters that must be modified to disable the ETL Server role:

   > **Tip:** The `serverRoleConfig.cfg` file is located in the following directory:
   >
   > - *On Windows:*`%NPSInstallDir%\config`
   > - *On Linux:*`$NPSInstallDir/config`
   >
   > Take a copy of the default `serverRoleConfig.cfg` file to a different directory and modify the copied file.

Property	Value	Description
Role.ETL	0	Make sure this value is set to 0.

4. Run the following command to check that the configuration file is correctly updated:

   configureNpsServer.ovpl –f <*config_file*> **-m validate –o** <*outputFile*>

   Check that the contents of <*outputFile*> is error free.

> **Note:** If you see any errors, review the contents of the serverRoleConfig.cfg file, and then run the command again.

5. Run the following command on the NPS system to disable the ETL Server role:

   configureNpsServer.ovpl -f <*config_file*>

   The ETL Server role is now disabled on this system.
6. Check that only the DB Server and UiBi Server roles are enabled by running the `about.ovpl` command.
7. Restart all processes by running the following command:

   startALL.ovpl

Install a New instance of NPS

Install a new instance of NPS on a new system. While installing, choose to install the NNM iSPI Performance for Metrics Extension Packs. Do not start the ETL process on this system at the end of the installation.

As a result of the installation, a new NPS system is created where all roles are enabled.

Enable the ETL Server Role on the New NPS System

1. Log on to the newly created NPS system.
2. Run the following command on this new NPS system to restore all backed-up files (that were backed up in step 2):

   restore.ovpl -b <*backup_file*>
3. Drop all database tables on this system by running the following command:

   > **Caution:** Make sure you run this command on the right system (that is, the new system where you installed NPS). Running this command on an incorrect NPS system will lead to data loss.

   initializeNPS.ovpl -a DropPerfSPIDB
4. Configure the `serverRoleConfig.cfg` file to assign the ETL Server role to this NPS system:

   > **Tip:** The `serverRoleConfig.cfg` file is located in the following directory:
   >
   > - *On Windows:*`%NPSInstallDir%\config`
   > - *On Linux:*`$NPSInstallDir/config`
   >
   > Take a copy of the default `serverRoleConfig.cfg` file to a different directory and modify the copied file.

Property	Value	Description
Role.ETL	1	Make sure this property is set to 1.

Property	Value	Description
Role.Db	0	Make sure this property is set to 0.
Role.UiBi	0	Make sure this property is set to 0.
Etl.DbServer.Hostname	Type the FQDN of the system with the DB Server role.	This could be the original server from which you are migrating the ETL Server. Refer to the table where you noted down the details.
Etl.UiBiServer.Hostname	Type the FQDN of the system with the UiBi Server role.	This could be the original server from which you are migrating the ETL Server. Refer to the table where you noted down the details.
Etl.RuntimeConfig.PRSPI_DISABLE_EXTENSIONPACK_AUTOINSTALL	0	Make sure this property is set to 0.
Etl.RuntimeConfig.PRSPI_DISABLE_CUSTOMCOLLECTION_AUTOINSTALL	0	Make sure this property is set to 0.
Etl.NnmServer.Hostname	Type the FQDN of the NNMi server.	Refer to the table where you noted down the details.
Etl.NnmServer.Share.Name	Type the name of the share created by nnmenableperfspi.ovpl.	Refer to the table where you noted down the details.
Etl.NnmServer.Share.User	Type the name of the user created by nnmenableperfspi.ovpl	Refer to the table where you noted down the details.
Etl.NnmServer.Share.Pass	Type the password of the above user.	Refer to the table where you noted down the details.

5. Run the following command to check that the configuration file is correctly updated:

   configureNpsServer.ovpl –f *<config_file>* **-m validate –o** *<outputFile>*

   Check that the contents of <*outputFile*> is error free.

   > **Note:** If you see any errors, review the contents of the serverRoleConfig.cfg file, and then run the command again.

6. Run the following command on this new NPS system:

configureNpsServer.ovpl -f <*config_file*>

The ETL Server role is now enabled on this system.

7. Check that only the ETL Server is enabled by running the `about.ovpl` command.
8. Start all processes by running the following command:

   startALL.ovpl

Run the nnmenableperspi.ovpl Script

> **Note:** If the original NPS system was configured to use the CIFS share (and *not* the NFS share), skip this section.

After moving the ETL Server role to a new system, you must run the `nnmenableperfspi.ovpl` script once again on the NNMi management server and you must select the CIFS share this time. Using an NFS share with the distributed deployment of NPS is not supported.

Creating a Separate DB Server

You can segregate out the DB Server role by installing NPS onto a separate system and configuring the DB Server role on that system.

To create this setup, follow these steps:

1. "Record the details of your existing NPS environment" below
2. "Take a Backup of the Database " on the next page
3. "Install a New Instance of NPS" on page 57
4. "Enable Only the DB Server Role on the New System" on page 57
5. "Disable the DB Server Role on the Original System" on page 58
6. " Reconcile the DB Server FQDN on Other Servers" on page 58

Record the details of your existing NPS environment

It is important to note down the details of your current NPS setup. You may migrate the DB Server from a standalone, single-server NPS, or from an already created distributed deployment with the DB Server co-existing with another server role on a single system.

Fill out the following table with the details of your existing environment.

Details of your existing NPS environment			
Standalone		**Distributed deployment**	
FQDN of the NPS system		FQDN of DB Server	
		FQDN of UiBi Server	
FQDN of the NNMi management server		FQDN of existing ETL Server	

		FQDN of the NNMi management server	

In this configuration step, you need to specify the details of the network share and user account specified while running the `nnmenableperfspi.ovpl` script. As a best practice, you must always securely note down share and user account details that are specified while running the `nnmenableperfspi.ovpl` script.

You can find the network share and user account details specified during the last run of the `nnmenableperfspi.ovpl` file in the following file on the NNMi management server:

(The file does not store the password.)

On Linux:

```
/var/opt/OV/log/nnmenableperfspi.txt
```

On Windows:

```
%nnmdatadir%\log\nnmenableperfspi.txt
```

Fill out the following table with the details:

NNMi details	
NNMi share name	
NNMi share user name	
NNMi share user password	

Take a Backup of the Database

1. Run the following command on the original NPS system to take a database backup:

   > **Note:** Since you are going to migrate the DB Server role onto a different system, you must take a backup of the entire database. This backup will later be restored on the new system.

   > **Tip:** Before you begin, make sure sufficient disk space exists on the NPS system to run the backup procedure and store the backed-up data. Determine the size of the NPS database by running the following command:
   >
   > **dbsize.ovpl -q**

   backup.ovpl -b<*dir_db*> **-d**

   In this instance, <*dir_db*> is the local directory where you want to store the backup file. The command creates a backup file (with the `.tar.gz` extension) in the <*dir_db*> directory.

2. Stop all NPS processes on the original NPS server where the DB Server role is currently enabled:

   stopALL.ovpl

Install a New Instance of NPS

Install a new instance of NPS on a new system. While installing, *do not* choose to install the NNM iSPI Performance for Metrics Extension Packs. Do not start the ETL process on this system at the end of the installation.

As a result of the installation, a new NPS system is created where all roles are enabled.

Restore the Database on the New System

Run the following command on this new NPS system to restore all backed-up database files (that were backed up in step 1):

restore.ovpl -b <*backup_db*>

In this instance, <*backup_db*> is the backed-up database file.

Enable Only the DB Server Role on the New System

1. Log on to the newly created NPS system.
2. Configure the `serverRoleConfig.cfg` file to enable the DB Server role to this NPS system. The following table lists the properties that must be modified to enable the DB Server role:

   > **Tip:** The `serverRoleConfig.cfg` file is located in the following directory:
   >
   > - *On Windows:*`%NPSInstallDir%\config`
   > - *On Linux:*`$NPSInstallDir/config`
   >
   > Take a copy of the default `serverRoleConfig.cfg` file to a different directory and modify the copied file.

Property	Value
Role.ETL	0
Role.Db	1
Role.UiBi	0

3. Run the following command to check that the configuration file is correctly updated:

   configureNpsServer.ovpl –f <*config_file*> **-m validate –o** <*outputFile*>

   Check that the contents of <*outputFile*> is error free.

   > **Note:** If you see any errors, review the contents of the serverRoleConfig.cfg file, and then run the command again.

4. Run the following command on this new NPS system:

   configureNpsServer.ovpl -f <*config_file*>

The DB Server role is now enabled on this system.

5. Check that only the DB Server role is enabled by running the `about.ovpl` command.

Disable the DB Server Role on the Original System

1. Drop all databases on the original NPS system by running the following command:

   initializeNPS.ovpl -a DropPerfSPIDB

2. Configure the `serverRoleConfig.cfg` file to disable the DB Server role on the original NPS system. The following table lists the properties that must be modified to disable the DB Server role:

   > **Tip:** The `serverRoleConfig.cfg` file is located in the following directory:
   >
   > - *On Windows:*`%NPSInstallDir%\config`
   > - *On Linux:*`$NPSInstallDir/config`
   >
   > Take a copy of the default `serverRoleConfig.cfg` file to a different directory and modify the copied file.

Property	Value	Description
Role.Db	0	Make sure this property is set to 0.
All properties that end with `DbServer.Hostname`	FQDN of the new DB Server.	Type the FQDN of the new NPS system where you will be configuring the DB Server role.

3. Run the following command to check that the configuration file is correctly updated:

   configureNpsServer.ovpl –f <*config_file*> **-m validate –o** <*outputFile*>

   In this instance, <*config_file*> is the complete path (including the file name) to the `serverRoleConfig.cfg` file that you edited.

   Check that the contents of <*outputFile*> is error free.

   > **Note:** If you see any errors, review the contents of the serverRoleConfig.cfg file, and then run the command again.

4. Run the following command on the NPS system to disable the DB Server role:

   configureNpsServer.ovpl -f <*config_file*>

   The DB Server role is now disabled on this system.

5. Check that only the DB Server role is completely disabled by running the `about.ovpl` command.

6. Restart all processes by running the following command:

   startALL.ovpl

Reconcile the DB Server FQDN on Other Servers

Only if you started off with an existing distributed deployment.

If you performed this procedure in an existing distributed deployment, you must configure all other servers in the deployment to communicate with the new DB Server.

For example, if your original setup consisted of a single system with the DB Server and UiBi Server roles and a single system for the UiBi Server, you must configure the ETL Server now to communicate with the new DB Server.

Follow these steps:

1. Log on to the system as root or administrator.
2. Configure the `serverRoleConfig.cfg` file to specify the FQDN of the new DB Server.

> **Tip:** The `serverRoleConfig.cfg` file is located in the following directory:
>
> - *On Windows:*`%NPSInstallDir%\config`
> - *On Linux:*`$NPSInstallDir/config`
>
> Take a copy of the default `serverRoleConfig.cfg` file to a different directory and modify the copied file.

Property	Value	Description
Role.Db	0	Make sure this property is set to 0. This setting ensures the DB Server is not enabled on this system.
Role.UiBi and Role.ETL	1 or 0	Make sure to correctly set these properties depending on the role of the system.
All properties that end with `DbServer.Hostname`	FQDN of the new DB Server.	Type the FQDN of the new NPS system where you will be configuring the DB Server role.
All properties that end with `nnmserver.hostname`	FQDN of the NNMi management server	Type the FQDN of the NNMi management server.
All properties that end with `NnmServer.Share.Name`	The NNMi share name	Type the NNMi share name that was configured while running the `nnmenableperfspi.ovpl` script. Follow the details noted down in the worksheet.
All properties that end with `NnmServer.Share.User`	The NNMi share user name	Type the NNMi share user name that was configured while running the `nnmenableperfspi.ovpl` script. Follow the details noted down in the worksheet.
All properties that end with	The NNMi share user	Type the NNMi share user password that was configured while running the

Property	Value	Description
`NnmServer.Share.Pass`	password	`nnmenableperfspi.ovpl` script. Follow the details noted down in the worksheet.

Look for the properties that end with `Dbserver.hostname` and set those properties to the new FQDN of the DB Server.

3. Run the following command to check that the configuration file is correctly updated:

   configureNpsServer.ovpl –f *<config_file>* **-m validate –o** *<outputFile>*

   In this instance, is the complete path (including the file name) to the `serverRoleConfig.cfg` file that you edited.

   Check that the contents of *<outputFile>* is error free.

   > **Note:** If you see any errors, review the contents of the serverRoleConfig.cfg file, and then run the command again.

4. Run the following command:

   configureNpsServer.ovpl -f *<config_file>*.

5. Restart all processes by running the following command:

   startALL.ovpl

Creating a Separate UiBi Server

You can segregate out the UiBi Server role by installing NPS onto a separate system and configuring the UiBi Server role on that system.

To create this setup, follow these steps:

1. "Record the Details of Your Existing NPS Environment" below
2. "Take a Backup of Files and the Content Store" on the next page
3. "Install a New Instance of NPS." on page 62
4. "Enable Only the UiBi Server Role on the New NPS System" on page 62
5. " Disable the UiBi Server Role on the Original NPS System" on page 65
6. "Reconcile the UiBi Server FQDN on Other Servers" on page 66
7. "Run the nnmenableperfspi.ovpl Script" on page 67

Record the Details of Your Existing NPS Environment

It is important to note down the details of your current NPS setup. You may migrate the DB Server from a standalone, single-server NPS, or from an already created distributed deployment with the DB Server co-existing with another server role on a single system.

Fill out the following table with the details of your existing environment.

Details of your existing NPS environment

Standalone		Distributed deployment	
FQDN of the NPS system		FQDN of DB Server	
		FQDN of UiBi Server	
FQDN of the NNMi management server		FQDN of existing ETL Server	
		FQDN of the NNMi management server	

Tip: In this configuration step, you need to specify the details of the network share and user account specified while running the `nnmenableperfspi.ovpl` script. As a best practice, you must always securely note down share and user account details that are specified while running the `nnmenableperfspi.ovpl` script.

You can find the network share and user account details specified during the last run of the `nnmenableperfspi.ovpl` file in the following file on the NNMi management server:

(The file does not store the password.)

On Linux:

```
/var/opt/OV/log/nnmenableperfspi.txt
```

On Windows:

```
%nnmdatadir%\log\nnmenableperfspi.txt
```

Fill out the following table with the details:

NNMi details	
NNMi share name	
NNMi share user name	
NNMi share user password	

Take a Backup of Files and the Content Store

Creating a new UiBi Server server requires you to transfer all the necessary data from the old system to the new system. This is achieved by taking a backup of all files and the content store on the original NPS system and restoring the backed-up data to the newly configured UiBi Server server. Therefore, before you begin the migration of the UiBi Server role, you must take a backup.

1. Run the following command on the original NPS system to take a backup of archived data files:

   Note: Since you are going to migrate the UiBi Server role onto a different system, you must take a backup of all files. This backup will later be restored on the new system.

> **Tip:** Before you begin, make sure sufficient disk space exists on the NPS system to run the backup procedure and store the backed-up data. Determine the size of the configuration and archived data files by measuring size of the following directory:
>
> *On Windows*
>
> `%npsdatadir%\NNMPerformance`
>
> *On Linux*
>
> `/var/opt/OV/NNMPerformance`

backup.ovpl -b <*dir_file*> **-f**

In this instance, <*dir_file*> is the local directory where you want to store the backup file.

2. Run the following command on the original NPS system to take a content store backup:

> **Note:** Since you are going to migrate the UiBi Server role onto a different system, you must take a backup of the content store. This backup will later be restored on the new system.

> **Tip:** Before you begin, make sure sufficient disk space exists on the NPS system to run the backup procedure and store the backed-up data. Determine the size of the NPS content store by running the following command:
>
> **cssize.ovpl -q**

backup.ovpl -b <*dir_cs*>**-c**

In this instance, <*dir_cs*> is the local directory where you want to store the backup file.

Install a New Instance of NPS.

Install a new instance of NPS on a new system. While installing, *do not* choose to install the NNM iSPI Performance for Metrics Extension Packs. Do not start the ETL process on this system at the end of the installation.

Enable Only the UiBi Server Role on the New NPS System

1. Log on to the newly created NPS system.
2. Run the following command on this new NPS system to restore all backed-up files (that were backed up in step 1):

   restore.ovpl -b <*backup_file*>

   In this instance, <*backup_file*> is the backed-up NPS files.
3. Run the following command on this new NPS system to restore the content store (that were backed up in step 2):

   restore.ovpl-b<*backup_cs*>

   In this instance, <*backup_cs*> is the backed-up NPS content store.
4. Drop all database tables on this system by running the following command:

> **Caution:** Make sure you run this command on the right system (that is, the new system where you installed NPS). Running this command on an incorrect NPS system will lead to data loss.

initializeNPS.ovpl -a DropPerfSPIDB

5. Configure the `serverRoleConfig.cfg` file to enable the UiBi Server role to this NPS system. The following table lists the properties that must be modified to enable the UiBi Server role:

> **Tip:** The `serverRoleConfig.cfg` file is located in the following directory:
>
> - *On Windows:*`%NPSInstallDir%\config`
> - *On Linux:*`$NPSInstallDir/config`
>
> Take a copy of the default `serverRoleConfig.cfg` file to a different directory and modify the copied file.

Property	Value	Description
Role.ETL	0	Make sure this property is set to 0. This setting ensures the ETL Server is not enabled on this system.
Role.Db	0	Make sure this property is set to 0. This setting ensures the DB Server is not enabled on this system.
Role.UiBi	1	Make sure this property is set to 1.
UiBi.Share.User	The share user name.	NNMi share user name that was configured while running the `nnmenableperfspi.ovpl` script. Follow the details noted down in the worksheet. Do not modify if you are using the default share user.
UiBi.Share.Pass	The share user password	NNMi share user password that was configured while running the `nnmenableperfspi.ovpl` script. Follow the details noted down in the worksheet. Do not modify if you are using the default share user.

Property	Value	Description
UiBi.DbServer.Hostname	The FQDN of the DB Server.	The FQDN of the system that is configured as the DB Server.
UiBi.DbServer.User	The share user name.	NNMi share user name that was configured while running the `nnmenableperfspi.ovpl` script. Follow the details noted down in the worksheet. Do not modify if you are using the default share user.
UiBi.DbServer.Pass	The share user password	NNMi share user password that was configured while running the `nnmenableperfspi.ovpl` script. Follow the details noted down in the worksheet. Do not modify if you are using the default share user.
UiBi.NnmServer.Hostname	The FQDN of the NNMi management server.	Type the FQDN of the NNMi management server.
UiBi.NnmServer.Share.Name	NNMi network share	Type the name of the network share created on the NNMi management server while running the `nnmenableperfspi.ovpl` script.
UiBi.NnmServer.Share.User	Type the name of the user account specified while running the `nnmenableperfspi.ovpl` script.	Type the name of the user account specified while running the `nnmenableperfspi.ovpl` script.
UiBi.NnmServer.Share.Pass	Type the password of the above user account.	Type the password of the above user account.

6. Run the following command to check that the configuration file is correctly updated:

   configureNpsServer.ovpl –f *<config_file>* **-m validate –o** *<outputFile>*

   Check that the contents of <*outputFile*> is error free.

   Note: If you see any errors, review the contents of the serverRoleConfig.cfg file, and then run the command again.

7. Run the following command on this new NPS system:

configureNpsServer.ovpl -f <*config_file*>

The UiBi Server role is now enabled on this system.

8. Check that only the UiBi Server role is enabled by running the `about.ovpl` command.

   > **Tip:** You can delete the edited serverRoleConfig.cfg file at this point.

9. Restart all processes by running the following command:

   startALL.ovpl

Disable the UiBi Server Role on the Original NPS System

At this point, you must go back to the original NPS system and disable the UiBi Server role.

1. Stop all NPS processes on the original NPS system:

   stopALL.ovpl

2. Configure the `serverRoleConfig.cfg` file to disable the UiBi Server role on the original NPS system. The following table lists the properties that must be modified to disable the UiBi Server role:

   > **Tip:** The `serverRoleConfig.cfg` file is located in the following directory:
   >
   > - *On Windows:*`%NPSInstallDir%\config`
   > - *On Linux:*`$NPSInstallDir/config`
   >
   > Take a copy of the default `serverRoleConfig.cfg` file to a different directory and modify the copied file.

Property	Value	Description
Role.UiBi	0	Make sure this property is set to 0.
All properties that end with `UiBiServer.Hostname`	FQDN of the new UiBi Server.	Type the FQDN of the new NPS system where you have configured the UiBi Server role.
All properties that end with `nnmserver.hostname`	FQDN of the NNMi management server	Type the FQDN of the NNMi management server.
All properties that end with `NnmServer.Share.Name`	The NNMi share name	Type the NNMi share name that was configured while running the `nnmenableperfspi.ovpl` script. Follow the details noted down in the worksheet.
All properties that end with `NnmServer.Share.User`	The NNMi share user name	Type the NNMi share user name that was configured while running the `nnmenableperfspi.ovpl` script. Follow the details noted down in the worksheet.
All properties that end	The NNMi	Type the NNMi share user password that was configured

Property	Value	Description
with `NnmServer.Share.Pass`	share user password	while running the `nnmenableperfspi.ovpl` script. Follow the details noted down in the worksheet.

3. Run the following command to check that the configuration file is correctly updated:

   configureNpsServer.ovpl –f *<config_file>* **-m validate –o** *<outputFile>*

   In this instance, is the complete path (including the file name) to the `serverRoleConfig.cfg` file that you edited.

   Check that the contents of <*outputFile*> is error free.

   > **Note:** If you see any errors, review the contents of the serverRoleConfig.cfg file, and then run the command again.

4. Run the following command on the original NPS system to disable the UiBi Server role:

   configureNpsServer.ovpl -f *<config_file>*

   The UiBi Server role is now disabled on this system.

5. Check that only the UiBi Serverrole is completely disabled by running the `about.ovpl` command.

   > **Tip:** You can delete the edited serverRoleConfig.cfg file at this point.

6. Restart all processes by running the following command:

   startALL.ovpl

Reconcile the UiBi Server FQDN on Other Servers

Only if you started off with an existing distributed deployment.

If you performed this procedure in an existing distributed deployment, you must configure all other servers in the deployment to communicate with the new UiBi Server. For example, if your original setup consisted of a single system with the DB Server and UiBi Server roles and a single system for the ETL Server, you must configure the ETL Server now to communicate with the new UiBi Server.

Follow these steps:

1. Log on to the system as root or administrator.
2. Configure the `serverRoleConfig.cfg` file to specify the FQDN of the new DB Server.

   > **Tip:** The `serverRoleConfig.cfg` file is located in the following directory:
   >
   > - *On Windows:*`%NPSInstallDir%\config`
   > - *On Linux:*`$NPSInstallDir/config`
   >
   > Take a copy of the default `serverRoleConfig.cfg` file to a different directory and modify the copied file.

Look for the properties that end with `UiBiserver.hostname` and set those properties to the new FQDN of the DB Server.

3. Run the following command to check that the configuration file is correctly updated:

   configureNpsServer.ovpl –f *<config_file>* **-m validate –o** *<outputFile>*

   In this instance, is the complete path (including the file name) to the `serverRoleConfig.cfg` file that you edited.

   Check that the contents of <*outputFile*> is error free.

   > **Note:** If you see any errors, review the contents of the serverRoleConfig.cfg file, and then run the command again.

4. Run the following command:

   configureNpsServer.ovpl -f <*config_file*>.

5. Restart all processes by running the following command:

   startALL.ovpl

Run the nnmenableperfspi.ovpl Script

After moving the UiBi Server role to a new system, you must run the `nnmenableperfspi.ovpl` script once again on the NNMi management server and you must provide the FQDN of the new UiBi Server this time.

Modifying Data Retention Settings

By default, NPS is installed with the following settings:

- Daily data retention period: 800 days
- Hourly data retention period: 70 days
- Raw/detailed data retention period: 14 days

If you want to modify the data retention settings in a distributed deployment of NPS, follow these steps:

1. Decide the new retention periods. The retention period of the raw data must be smaller than the retention period of the hourly data; the retention period of the hourly data again must be smaller than that of the daily data.
2. Decide if the modified retention periods will apply to all Extension Packs or just to a subset of Extension Packs installed in the environment.
3. To modify the retention periods of all Extension Packs on a system with the ETL Server role:
   1. Log on to the ETL Server as administrator or root.
   2. Launch the NNM iSPI Performance Configuration window.

      On Windows

      Click **Start > All Programs > HP > NNM iSPI Performance > Configuration Utility**.

      On Linux

      Run the following command:

      /opt/OV/NNMPerformanceSPI/bin/runConfigurationGUI.ovpl
   3. Specify the changes in data retention settings, and then click **Apply**. The change is applied to all the Extension Packs that are installed (and enabled) on the system.
   4. If you have created an environment with multiple ETL Servers and want to change the data retention settings on the other ETL Servers, perform similar steps (step a through step c) on them.
4. To configure different retention periods for different Extension Packs on an ETL Server:
   1. Log on to the ETL Server as administrator or root.
   2. Go to the following directory:

      On Windows

      `%npsdatadir%\NNMPerformanceSPI\rconfig\`<*Extension_Pack_Name*>

      On Linux

      `/var/opt/OV/NNMPerformanceSPI/rconfig/`<*Extension_Pack_Name*>

      > **Tip:** To find out the names of installed Extension Packs, run the following command:
      >
      > **about.ovpl**
   3. Locate the `customConfig.cfg` file in this directory.
   4. Create an empty `userConfig.cfg` file, and then transfer all the parameters that are available in the `customConfig.cfg` file to the `userConfig.cfg` file.
   5. In the `userConfig.cfg`file, change the values of the following properties to modify the data retention periods:

   - `PRSPI_DataRetention_Raw` (for raw data)
   - `PRSPI_DataRetention_Hour` (for hourly data)
   - `PRSPI_DataRetention_Day` (for daily data)

f. Save the `userConfig.cfg` file.

g. Restart the ETL process for the changes to take effect by running the following commands:

   - **stopETL.ovpl**
   - **startETL.ovpl**

Part III: Upgrading an Existing Distributed Deployment of NPS

Note: The information in the *Upgrading an Existing Distributed Deployment of NPS* section provides instructions to upgrade NPS from an older version (10.10 or 10.20) to the version 10.30. You can apply the NPS 10.30 patch after the upgrade procedure is complete. For patch installation instructions, see "Installing Patches in a Distributed Deployment of NPS" on page 82.

You can upgrade an existing distributed deployment of NPS to the current version.

Tip: If possible, take a backup of all the copies of the `serverRoleConfig.cfg` files that you used while assigning server roles.

To upgrade a distributed deployment of NPS, perform these tasks:

1. **Task 1:** "Upgrade NPS" below
2. **Task 2:** "Reconfigure the DB Server Role" on page 73
3. **Task 3:** "Reconfigure the UiBi Server Role" on page 73
4. **Task 3:** "Upgrade All iSPIs" on page 74
5. **Task 4:** "Post-Upgrade Steps" on page 75

Upgrade NPS

1. Stop NPS services on the UiBi Server by running the following command:

   stopALL.ovpl
2. Stop NPS services on the ETL Servers by running the following command:

   stopALL.ovpl
3. Stop NPS services on the DB Server by running the following command:

   stopALL.ovpl
4. Upgrade NPS to the current version on each system by following these steps:

   Note: While upgrading NPS, follow this sequence:

   a. Upgrade the DB Server.
   b. Upgrade the UiBi Server.
   c. Upgrade the ETL Server.

   Do not start upgrading the UiBi Server until the DB Server is completely upgraded; do not start upgrading the ETL Servers until the UiBi Server is completely upgraded.

a. Extract the contents of the NNM iSPI Performance for Metrics media.
b. Use the cd command to change to the media directory.
c. From the media root, run the `setup` file (`setup.exe` for Windows; `setup.bin` for Linux).

   The installation wizard opens.

   > **Note:** *For Linux Only.* If you are performing these steps from a remote server by using an XServer, and if the `DISPLAY` variable is not set correctly, the following message may appear:
   >
   > ```
   > Choose locale....
   >
   > -----------------------
   >
   > 1- Deutsch
   >
   > ->2- English
   >
   > 3- Espanol
   >
   > 4- Francais
   >
   > CHOOSE LOCALE BY NUMBER:
   > ```
   >
   > If you see this message, do not continue with the installation. Stop the installation by pressing **Ctrl+C**, make sure that the `DISPLAY` variable is set correctly, and then run the `setup` file again.

   Select the language of the wizard, and then click **OK**.

   If the application requirement check warnings dialog box opens, review the warning messages, take appropriate action, and then click **Continue**.
d. On the Introduction page, click **Next**. The License Agreement page opens.
e. Select **I accept the terms**, and click **Next**.
f. When the upgrade check succeeds, click **Next**.

   If the upgrade check shows warnings and errors, review the messages, take appropriate actions, and then click **Next**.

   > **Tip:** *For Linux only.* If the installer check shows necessary libraries are missing, click here.
   >
   > To install missing libraries on the system, follow these steps:
   >
   > i. Note down the names of missing libraries indicated by the installation wizard.
   > ii. Make sure the system is connected to the Internet and set up to work with Red Hat or SUSE package repositories.
   > iii. To install each missing library, run the following command:
   >
   >   *On Red Hat Enterprise Linux*
   >
   >   **yum install**<*library*>
   >
   >   > **Tip:** You can specify multiple libraries in the command—each separated by a space. (For example, **yum install openmotif.x86_64 libXp.x86_64 libpng.x86_64**.)
   >
   >   *On SUSE Linux Enterprise Server*
   >
   >   **zypper install** <*library*>

In this instance, <*library*> is the name of the missing library as indicated by the installation wizard.

iv. Type **Y** to install the libraries.

The Pre-Upgrade Summary page opens.

g. Make sure that the NNM iSPI Performance for Metrics–ExtensionPacks check box is not selected.

h. Click **Upgrade**. The upgrade process begins.

The Choose Java JDK dialog box opens.

The NNM iSPI Performance for Metrics10.30 installer removes the JDK that was installed on the system by the previous version of the installer provides an option to install OpenJDK 1.8. You can select the **Install bundled OpenJDK** option to install OpenJDK 1.8 that is embedded with the NNM iSPI Performance for Metrics media.

Alternatively, if another version of JDK 1.8 is already available on the system, you can select the **Use Already-Installed JDK** option, and then click **Browse** to select the path to the JDK.

On Linux, it is recommended that you use the JDK 1.8.x provided by your operating system vendor (Red Hat or SUSE).

For example:

To install Red Hat OpenJDK 1.8.x on Red Hat Enterprise Linux, run the following command:

yum install java-1.8.0-openjdk-devel.x86_64

To install SUSE OpenJDK 1.8.x on SUSE Linux, run the following command:

zypper install java-1_8_0-openjdk

To find out the directory where JDK is installed, run one of the following commands:

whereis java

which java

On Windows, it is recommended that you install the Oracle JDK 1.8.x.

Tip: Click **Validate** to check that the specified path is valid.

After making a selection, click **Continue**.

Toward the end of the upgrade process, the HPE NNM iSPI Performance Configuration window opens.

On the DB Server and UiBi Server, click **Exit**.

Note: On the DB Server and UiBi Server, do not change any settings. Do not click **Start**.

After the upgrade procedure is complete, you cannot configure an NPS system in a distributed deployment to assume a different role.

On the ETL Server, make sure that the correct share path is specified, make sure that CIFS is selected as the sharing mode, and then click **Apply** if you had to make any changes; otherwise, click **Exit**.

Reconfigure the DB Server Role

1. Log on to the DB Server as root or administrator.
2. Do one of the following:
   - Retrieve the copy of the `serverRoleConfig.cfg` file that was used to configure the server role on this system.

     > **Tip:** If you are unable to retrieve the copy of the `serverRoleConfig.cfg` file that was used before, follow the alternative procedure.

   - Alternatively, create a new copy of the `serverRoleConfig.cfg` file:

     Create a new `serverRoleConfig.cfg` file by following the instructions in the "Assign Roles" on page 30 section.
3. Configure the DB Server role again by running the following command:

   configureNpsServer.ovpl -f<*config_file*>

   In this instance, <*config_file*> is the name (with the full path) of the configuration file.

Reconfigure the UiBi Server Role

1. Log on to the UiBi Server as root or administrator.
2. Do one of the following:
   - Reconfigure the `serverRoleConfig.cfg` file:
     1. Retrieve the copy of the `serverRoleConfig.cfg` file that was used to configure the server role on this system.

        > **Tip:** If you are unable to retrieve the copy of the `serverRoleConfig.cfg` file that was used before, follow the alternative procedure.

     2. Save the file.
   - Alternatively, create a new copy of the `serverRoleConfig.cfg` file:

     Create a new `serverRoleConfig.cfg` file by following the instructions in the "Assign Roles" on page 30 section.
3. Configure the UiBi Server role again by running the following command:

   configureNpsServer.ovpl -f <*config_file*>

   In this instance, <*config_file*> is the name (with the full path) of the configuration file.

Re-configure the ETL Server Role

1. Log on to the ETL Server as root or administrator.
2. Do one of the following:
   - Retrieve the copy of the `serverRoleConfig.cfg` file that was used to configure the server role on this system.

     > **Tip:** If you are unable to retrieve the copy of the `serverRoleConfig.cfg` file that was used before, follow the alternative procedure.

   - Alternatively, create a new copy of the `serverRoleConfig.cfg` file:

     Create a new `serverRoleConfig.cfg` file by following the instructions in the "Assign Roles" on page 30 section.

3. Configure the ETL Server role again by running the following command:

   configureNpsServer.ovpl -f <*config_file*>

   In this instance, <*config_file*> is the name (with the full path) of the configuration file.

Upgrade All iSPIs

Upgrade all other iSPIs to 10.30. Follow the information in the iSPI documentation.

If you are using the NNM iSPI Performance for Metrics Extension Packs, do one of the following:

- In a single-ETL Server deployment, log on to the ETL Server as root or administrator, and then run the following commands:

  On Windows:

  a. **%npsinstalldir%\bin\metricsExtensionPacks.ovpl install**

  b. **%npsinstalldir%\bin\installPathHealth.ovpl**

  On Linux:

  a. **/opt/OV/NNMPerformanceSPI/bin/metricsExtensionPacks.ovpl install**

  b. **/opt/OV/NNMPerformanceSPI/bin/installPathHealth.ovpl**

- In a multi-ETL Server deployment, log on (as root or administrator) to the ETL Server where the NNM iSPI Performance for Metrics Extension Packs were originally installed, and then run the following command:

  On Windows:

  a. **%npsinstalldir%\bin\metricsExtensionPacks.ovpl install**

  b. **%npsinstalldir%\bin\installPathHealth.ovpl**

  On Linux:

  a. **/opt/OV/NNMPerformanceSPI/bin/metricsExtensionPacks.ovpl install**

  b. **/opt/OV/NNMPerformanceSPI/bin/installPathHealth.ovpl**

Post-Upgrade Steps

1. Run the `nnmenableperfspi.ovpl` script on the NNMi management server.

   > **Tip:** To provide the same configuration details that existed prior to upgrading NPS to the current version, see the contents of the following file:
   >
   > (The file does not store the password.)
   >
   > *On Linux:*
   >
   > `/var/opt/OV/log/nnmenableperfspi.txt`
   >
   > *On Windows:*
   >
   > `%nnmdatadir%\log\nnmenableperfspi.txt`

   When NNMi is installed on Linux

   a. Log on to the NNMi management server as root.

   b. If the `/var/opt` directory on the NNMi management server is on a mounted file system, you must perform the following additional steps:

      i. Open the `/etc/fstab` file with a text editor.

      ii. Find the line that starts with the following:

      <file_system> *<mount_point>*

      <file_system> is the `/var/opt` directory (either `/var` or `/var/opt`)

      iii. In the line, add `acl` to the list of options.

      iv. Save the file.

      v. Run the following command to remount `/var/opt`:

      mount -o remount /var/opt

      Or

      mount -o remount /var

   c. Go to the following directory:

      `/opt/OV/bin`

   d. To run the script in the interactive mode:

      i. Run the following command:

      ./nnmenableperfspi.ovpl

      The script prompts you for the fully qualified domain name of the NPS system.

      ii. Type the fully qualified domain name of the system on which you want to assign the UiBi Server role, and then press **Enter**.

      The script verifies the availability of the NPS system with a ping command.

      After successful verification, the script prompts you to specify the port that will be used by the NPS system.

      iii. Type a port number that is available for use, and then press **Enter**.

The script prompts you to specify the communication protocol for NPS.

iv. Type HTTPS if want to use the secure communication mode, and then press **Enter**.

If you want to use the non-secure HTTP mode of communication, press **Enter** without specifying anything.

The script prompts you to choose the type of file-sharing technique to exchange data between the NNMi management server and the NPS system. Available options are **CIFS**[1] and **NFS**[2].

v. Type **CIFS** or **NFS**, and then press **Enter**.

> **Note:** While creating a distributed deployment of NPS, choose NFS only if NNMi and all NPS system are on Linux. If you select NFS, make sure to apply the NNM iSPI Performance for Metrics 10.30 patch after completing the procedure of creating the distributed deployment of NPS. For instructions to install the 10.30 patch, see "Installing Patches in a Distributed Deployment of NPS" on page 82.

The script enables the evaluation license of the NNM iSPI Performance for Metrics on the NNMi management server, adds new items under the **Actions** menu, and enables file sharing between the NNMi management server and the NPS system.

Follow these steps:

A. The script prompts you to specify a user name that will be assigned as the owner of the shared file system.

Type a user name of your choice, and then press **Enter**. You need not type a pre-existing user name.

The script prompts you to type a password for the user that it is going to create.

B. Type a password that meets the operating system's password policy requirements, and then press **Enter**.

The script prompts you to specify the directory that will be used as the shared file system.

C. Type the complete path to the directory that you want to use as the shared file system between the NNMi management server and the NPS system, and then press **Enter**

The script performs the following tasks:

- Enables the evaluation license of the NNM iSPI Performance for Metrics on the NNMi management server
- Adds menu items under the Actions menu in the NNMi console to launch the NPS console
- Creates the shared file system
- Creates a user (if necessary) that can access the newly created shared file system

e. To run the script in the non-interactive (silent) mode:

i. In a text editor, add the following content:

```
spiHost=

spiPort=
```

[1] Common Internet File System (CIFS) is an application-layer file sharing protocol.
[2] Network File Share (NFS) is a file sharing protocol between systems running on UNIX/Linux.

```
spiProtocol=

shareType=

userName=

password=

shareName=

sharedDir=
```

ii. Specify a value for each parameter:

Parameter	Description
spiHost	Type the fully qualified domain name of the system on which you want to assign the UiBi Server role.
spiPort	Type the port that will be used by the NPS system. Type a port number that is available for use.
spiProtocol	Type HTTPS if want to use the secure communication mode. Type HTTP if you want to use the non-secure mode of communication.
shareType	Type CIFS.
userName	Type a user name of your choice. You need not type a pre-existing user name. This user name that will be assigned as the owner of the shared file system.
password	Type the password of the above user. The password must meet the operating system's password policy requirements.
shareName	Type a name of your choice for the shared file system.
sharedDir	Specify the directory that will be used as the shared file system. Type the complete path to the directory that you want to use as the shared file system between the NNMi management server and the NPS system.

iii. Save the file on the NNMi management server.

iv. Run the following command:

./nnmenableperfspi.ovpl -f <*configFile*>

In this instance, <*configFile*> is the name of the configuration file (with complete path to the file).

The script performs the following tasks:

- Enables the evaluation license of the NNM iSPI Performance for Metrics on the NNMi management server
- Adds menu items under the Actions menu in the NNMi console to launch the NPS console
- Creates the shared file system
- Creates a user (if necessary) that can access the newly created shared file system

When NNMi is Installed on Windows

a. Log on to the NNMi management server as Administrator.

b. Go to the following directory:

```
%nnminstalldir%\bin
```

c. To run the script in the interactive mode:

   i. Run the following command:

      nnmenableperfspi.ovpl

      The script prompts you for the fully qualified domain name of the NPS system.

   ii. Type the fully qualified domain name of the system on which you want to assign the UiBi Server role, and then press **Enter**.

      The script verifies the availability of the NPS system with a ping command.

      After successful verification, the script prompts you to specify the port that will be used by the NPS system.

   iii. Type a port number that is available for use, and then press **Enter**.

      The script prompts you to specify the communication protocol for NPS.

   iv. Type HTTPS if want to use the secure communication mode, and then press **Enter**.

      If you want to use the non-secure HTTP mode of communication, press **Enter** without specifying anything.

      The script prompts you to choose the type of file-sharing technique to exchange data between the NNMi management server and the NPS system.

   v. When you use a Windows NNMi management server, you must choose only the **CIFS**[1] protocol for file sharing.

      Type CIFS, and then press **Enter**.

      The script prompts you to specify a user name that will be assigned as the owner of the shared file system.

   vi. Type a user name of your choice, and then press **Enter**. You need not type a pre-existing user name.

      > **Tip:** If you specify a user name that does not already exists, the script creates a new local user (and not a Windows domain user).
      >
      > You can specify a pre-existing Windows domain user.
      >
      > Always use the following format while specifying a pre-existing domain user name:
      >
      > *<domain>******<user_name>*
      >
      > In this instance, <*domain*>is the domain name and <*user_name*> is the user name.

      The script prompts you to specify a password of the user that it is going to create.

   vii. Type a password that meets the operating system's password policy requirements, and then press **Enter**.

      The script prompts you to specify the directory that will be used as the shared file system.

   viii. Type the complete path to the directory that you want to use as the shared file system between the NNMi management server and the NPS system, and then press **Enter**.

[1] Common Internet File System (CIFS) is an application-layer file sharing protocol.

The script performs the following tasks:

- Enables the evaluation license of the NNM iSPI Performance for Metrics on the NNMi management server
- Adds menu items under the Actions menu in the NNMi console to launch the NPS console
- Creates the shared file system
- Creates a user (if necessary) that can access the newly created shared file system

d. To run the script in the non-interactive (silent) mode:

i. In a text editor, add the following content:

```
spiHost=

spiPort=

spiProtocol=

shareType=

userName=

password=

shareName=

sharedDir=
```

ii. Specify a value for each parameter:

Parameter	Description
spiHost	Type the fully qualified domain name of the system on which you want to assign the UiBi Server role.
spiPort	Type the port that will be used by the NPS system. Type a port number that is available for use.
spiProtocol	Type the communication protocol for NPS. Type HTTPS if want to use the secure communication mode. Type HTTP if you want to use the non-secure mode of communication.
shareType	Type CIFS. When NNMi is installed on Windows, you can use only the **CIFS**[1] protocol.
userName	Type a user name of your choice, and then press **Enter**. You need not type a pre-existing user name. **Tip:** If you specify a user name that does not already exists, the script creates a new local user (and not a Windows domain user). You can specify a pre-existing Windows domain user.

[1] Common Internet File System (CIFS) is an application-layer file sharing protocol.

Parameter	Description
	Always use the following format while specifying a pre-existing domain user name: <*domain*>****<*user_name*> In this instance, <*domain*>is the domain name and <*user_name*> is the user name.
password	Type the password of the above user.
shareName	Type a name of your choice for the shared file system.
sharedDir	Specify the directory that will be used as the shared file system. Type the complete path to the directory that you want to use as the shared file system between the NNMi management server and the NPS system.

iii. Save the file on the NNMi management server.

iv. Run the following command:

nnmenableperfspi.ovpl -f <*configFile*>

In this instance, <*configFile*> is the name of the configuration file (with complete path to the file).

2. Log on to the DB Server, and then run the following commands:
   a. **stopALL.ovpl**
   b. **startALL.ovpl**
3. Log on to the UiBi Server, and then run the following commands:
   a. **stopALL.ovpl**
   b. **startALL.ovpl**
4. Log on to each ETL Server, and then follow these steps:

Note: In an environment with multiple ETL Servers, perform this step on each system where the ETL Server role is enabled.

a. Run the following command to change the default SDK password:

On Windows: **%ovinstalldir%\NNMPerformanceSPI\bin\changeSdkUserPwd.ovpl -u npssdkuser -p** <*password*>

On Linux: **/opt/OV/NNMPerformanceSPI/bin/changeSdkUserPwd.ovpl -u npssdkuser -p** <*password*>

In this instance, <*password*> is a password of your choice.

Note: In an environment with multiple ETL Servers, you must set the identical password on each ETL Server.

b. Run the following commands to restart NPS:

i. **stopALL.ovpl**

ii. **startALL.ovpl**

Part IV: Installing Patches in a Distributed Deployment of NPS

This section of the document provides step-by-step instructions to apply a patch on NPS in a distributed environment.

Installing a Patch to a Distributed Deployment of NPS

> **Tip:** As a precaution, take a backup of NPS data on all the servers and all the copies of the `serverRoleConfig.cfg` files that you used while assigning server roles.

1. Stop NPS services on the UiBi Server by running the following command:

   stopALL.ovpl
2. Stop NPS services on the ETL Servers by running the following command:

   stopALL.ovpl
3. Stop NPS services on the DB Server by running the following command:

   stopALL.ovpl
4. Apply the patch to NPS using the instructions provided with the patch. Follow the patch installation steps given in the patch document, and ensure that the patch is installed successfully.

   > **Note:** Apply the patch in the following sequence:
   >
   > a. DB Server
   >
   > b. UiBi Server
   >
   > c. ETL Server
   >
   > Do not apply patch to the UiBi Server until the patch is applied to DB Server; do not apply patch to the ETL Servers until the patch is applied to the UiBi Server.

Configuration Task on the ETL Server

1. Log on to the ETL Server as root or administrator.
2. Do one of the following:
   - Retrieve the copy of the `serverRoleConfig.cfg` file that was used to configure the server role on this system.

> **Tip:** If you are unable to retrieve the copy of the `serverRoleConfig.cfg` file that was used before, follow the alternative procedure.

- Alternatively, create a new copy of the `serverRoleConfig.cfg` file by following the instructions in the "Assign Roles" on page 30 section.

3. Configure the ETL Server role again by running the following command:

   configureNpsServer.ovpl -f <*config_file*>

   In this instance, <*config_file*> is the name (with the full path) of the configuration file.

Additional Configuration Steps

1. Run the `nnmenableperfspi.ovpl` script on the NNMi management server by following the instructions in the "Enabling NNMi to Work with NPS" on page 22 section.

   > **Tip:** To provide the same configuration details that existed prior to applying the patch, see the contents of the following file:
   >
   > (The file does not store the password.)
   >
   > *On Linux:*
   >
   > `/var/opt/OV/log/nnmenableperfspi.txt`
   >
   > *On Windows:*
   >
   > `%nnmdatadir%\log\nnmenableperfspi.txt`

2. Log on to the DB Server, and then run the following commands:
   a. **stopALL.ovpl**
   b. **startALL.ovpl**
3. Log on to the UiBi Server, and then run the following commands:
   a. **stopALL.ovpl**
   b. **startALL.ovpl**
4. Log on to each ETL Server, and then run the following commands:

   > **Note:** In an environment with multiple ETL Servers, perform this step on each system where the ETL Server role is enabled.

   a. **stopALL.ovpl**
   b. **startALL.ovpl**

Uninstalling a Patch from a Distributed Deployment of NPS

> **Note:** Read the patch *readme* file to determine if the patch can be uninstalled.

To uninstall a patch from a distributed deployment of NPS, follow these steps:

1. Stop NPS services on the UiBi Server by running the following command:

   stopALL.ovpl
2. Stop NPS services on the ETL Servers by running the following command:

   stopALL.ovpl
3. Stop NPS services on the DB Server by running the following command:

   stopALL.ovpl
4. Uninstall the patch on NPS using the instructions provided with the patch. Follow the patch uninstallation steps given in the patch *readme* and ensure that the patch is uninstalled successfully.

   > **Note:** Uninstall the patch in the following sequence:
   >
   > a. ETL Server
   > b. UiBi Server
   > c. DB Server

Part V: Additional Configuration for Using NFS

> **Note:** This section is relevant only if you plan to use Linux and had chosen the NFS share when you ran the `nnmenableperfspi.ovpl` script. Skip this section if you use Windows.

If you chose to use the NFS share while running the `nnmenableperfspi.ovpl` script, you must perform additional tasks listed in this section to manually export the data share.

1. Log on to the NNMi management server.
2. Open the `/etc/exports` file with a text editor.
3. Locate the following line:

   `/var/opt/OV/shared/perfSpi/datafiles` *<UiBi Server FQDN>* `(rw,sync,no_root_squash)`

   In this instance, *<UiBi Server FQDN>* is the FQDN of the UiBi Server.
4. You must create a similar statement for each ETL Server in the environment. That is, you must add the following statement for each ETL Server:

   `/var/opt/OV/shared/perfSpi/datafiles` *<ETL Server FQDN>* `(rw,sync,no_root_squash)`

   In this instance, *<ETL Server FQDN>* is the FQDN of an ETL Server.

   In a multi-ETL environment, you must add a statement for each ETL Server. For example, in an environment with three ETL Servers, you must add three such statements in the `exports` file.
5. Save the file.
6. Run the following command:

   /usr/sbin/exportfs –a
7. Follow these steps on the DB Server:
   1. Open the `$NPSInstallDir/config/serverRoleConfig.cfg` file.
   2. Locate the following section:

      ```
      #Db config section
      ```
   3. Add the following lines in the section:

      `Db.Share.Protocol = NFS`

      `Db.Share.Etls =`*<etlserver>*

      In this instance, *<etlserver>* is the FQDN of the ETL Server. In a multi-ETL environment, provide a comma-separated list of FQDNs of all ETL Servers.
   4. Save the file.
8. Follow these steps on the UiBi Server:
   1. Open the `$NPSInstallDir/config/serverRoleConfig.cfg` file.
   2. Locate the following section:

      ```
      #UiBi config section
      ```

c. Add the following lines in the section:

   ```
   UiBi.Share.Protocol = NFS
   UiBi.Share.Etls =<etlserver>
   ```

   In this instance, <*etlserver*> is the FQDN of the ETL Server. In a multi-ETL environment, provide a comma-separated list of FQDNs of all ETL Servers.

d. Save the file.

9. Follow these steps on the ETL Server:

   a. Open the `$NPSInstallDir/config/serverRoleConfig.cfg` file.

   b. Locate the following section:

   ```
   #Db config section
   ```

   c. Add the following line in this section:

   ```
   Etl.Share.Protocol = NFS
   ```

   d. Save the file.

10. Log on as `root` to each NPS system, and then run the following command:

    Note: Run this command on NPS system in the following order:

    a. The DB Server

    b. The UiBi Server

    c. The ETL Servers

    ./configureNpsServer.ovpl -f `$NPSInstallDir/config/serverRoleConfig.cfg`

    Tip: As a best practice, take a backup of the `serverRoleConfig.cfg` file that you configured for use with the `configureNpsServer.ovpl` script.

Part VI: NPS in a Global Network Management Environment

This section covers the steps to allow a configuration with NNMi in a Global Network Management (GNM) environment along with a single instance of NPS attached to the Global NNMi management server (Global Manager). With this setup, NPS is not required at the regional NNMi management servers (Regional Managers). Instead, you need to do the following after installing NPS:

1. Install an NNMi Premiun or Ultimate license on each Regional Manager.
2. Install an NNMi Premiun or Ultimate license on the Global Manager.

A limitation of using this solution is that you cannot launch the NPS console (**Actions > Reporting - Report Menu**) and the Performance Troubleshooting console from Regional Managers.

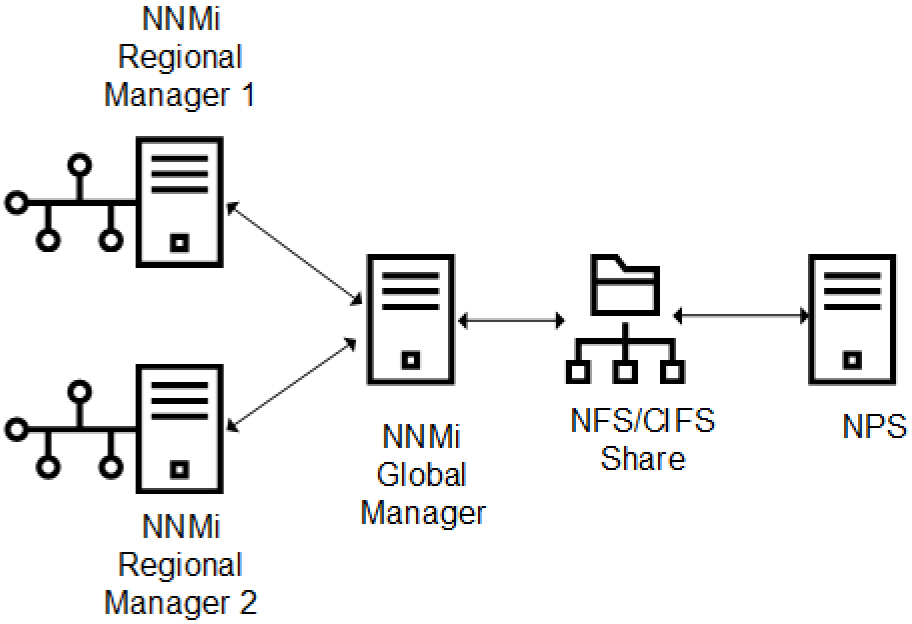
This section assumes a working knowledge of the basic architecture of NNMi and the NNM iSPI Performance for Metrics/NPS solution.

Note: You cannot use baseline reports in this deployment.

Architecture

Here is a simplistic picture of the architecture that will be covered in this document. This can be expanded to more than two Regional Managers.

GNM Deployment with NPS



In this document, we only use two Regional Managers, one Global Manager, and one NPS system, but you can expand this deployment to multiple Regional Managers.

Licensing Requirement

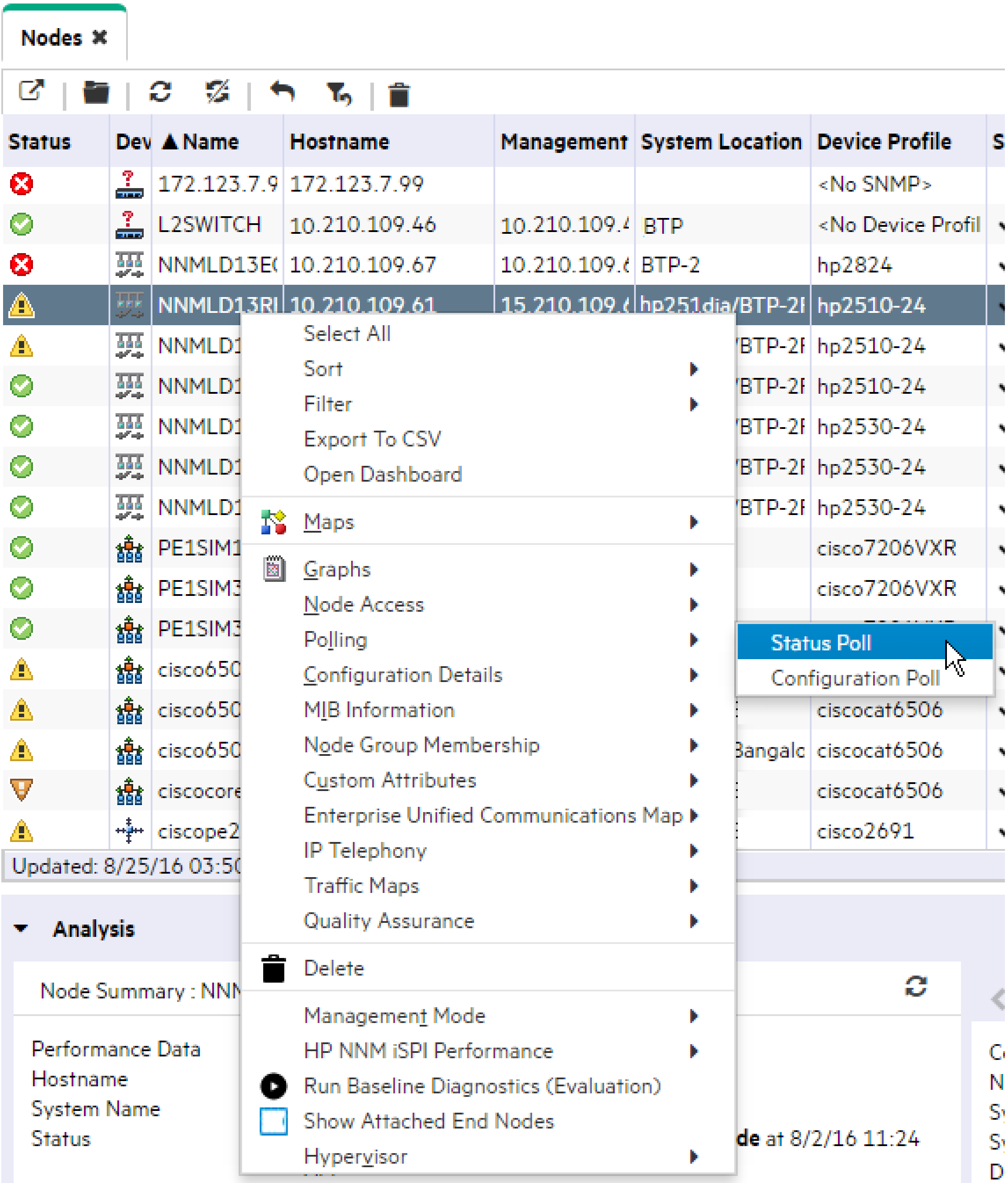
You must install the Premium or Ultimate licenses on the regional and Global Managers. The installation of licenses enables Performance polling on the Regional Manager.

For example, if you have three Regional Managers, you must obtain four Premium or Ultimate license keys (three for Regional Managers; one for the Global Manager).

GNM with NPS in a Linux Environment

To install NPS in a GNM environment, follow these steps:

1. Complete the GNM configuration between two NNMi servers. The details of this process are described in the *HPE Network Node Manager i Software Deployment Reference*.
2. Go to the Global Manager and run the `nnmenableperfspi.ovpl` script. Select NFS and complete all configuration steps. This script, at the end of its run, shows a path in the command line console. Note down this path.
3. Install the NNM iSPI Performance for Metrics on a separate, dedicated system. Near the end of the installation, the installer opens the HPE NNMi iSPI Performance Configuration window and you are prompted to specify the shared path to the Global Manager.
4. In the HPE NNMi iSPI Performance Configuration window, type the shared path in the Path box as displayed by the `nnmenableperfspi.ovpl` script (that is, the path that you noted down in a previous step).
5. Click **Start** to start the services.
6. *Optional.* You can perform a status poll of a router from the Global Manager. You will notice that the Global Manager does not do any performance polling yet because performance polling is not enabled on Regional Managers. Performance polling is enabled and licensed on the Global Manager.



Status	Dev	▲ Name	Hostname	Management	System Location	Device Profile	S
✖		172.123.7.9	172.123.7.99			<No SNMP>	
✓		L2SWITCH	10.210.109.46	10.210.109.4	BTP	<No Device Profil	
✖		NNMLD13E(	10.210.109.67	10.210.109.6	BTP-2	hp2824	
⚠		NNMLD13RI	10.210.109.61	15.210.109.(	hp251dia/BTP-2I	hp2510-24	
⚠		NNMLD1			BTP-2I	hp2510-24	
✓		NNMLD1			BTP-2I	hp2510-24	
✓		NNMLD1			BTP-2I	hp2530-24	
✓		NNMLD1			BTP-2I	hp2530-24	
✓		NNMLD1			BTP-2I	hp2530-24	
✓		PE1SIM1				cisco7206VXR	
✓		PE1SIM3				cisco7206VXR	
✓		PE1SIM3					
⚠		cisco650					
⚠		cisco650				ciscocat6506	
⚠		cisco650			Bangalc	ciscocat6506	
▼		ciscocore				ciscocat6506	
⚠		ciscope2				cisco2691	

Updated: 8/25/16 03:5(

7. Install the NNMi Ultimate or Premium license on each Regional Manager by using the `nnmlicense.ovpl` command, but do not run the `nnmenableperfspi.ovpl` script.
8. On the Global Manager, install an NNMi Ultimate or Premium license.
9. *Optional.* Now if you run the status poll of an object from the Global Manager, you will see that the object is polled for performance data.

Note: After some time, you will see several .csv.gz files accumulating in the

`/var/opt/OV/shared/perfSpi/datafiles/metric/final` directory on each Regional Manager. These files are generated by the Regional Manager's state poller. You can delete these files at any time.
This buildup of files will cause a warning eventually on the Reional Manager. Note that NNMi will not put more than 1 GB (by default) of files into this directory.
However, NNMi may show the following error messages in the System Information window:

```
The Performance SPI Custom Poller Bus Adapter has status Minor because the file space limit (10 megabytes) has been reached and no additional data can be written.
```

```
The Performance SPI Bus Adapter has status Minor because the file space limit (10 megabytes) has been reached and no additional data can be written.
```

You can control the accumulation of the `.csv.gz` files by reducing the maximum size of the storage of these files. You can also configure NNMi to suppress alerting of this issue (that is, the buildup of the `.csv.gz` files into the `nps_baselinestate` directory).

To control the buildup of the `.csv.gz` files, edit the `/var/opt/OV/shared/perfSpi/conf/nmsAdapter.conf` file on each Regional Manager by changing the `maxFileSpaceMB` property to a smaller number like 10.
For example:

```
maxFileSpaceMB:10
```

Restart NNMi (by running **ovstop** and **ovstart**) after making this change.

To suppress alerting of the buildup of the `.csv.gz` files, edit the `/var/opt/OV/shared/nnm/conf/props/nms-topology.properties` file on each Regional Manager by adding the following lines:

```
#Suppress warnings about Max Space on regional NNMi
```

```
com.hp.ov.nms.health.SUPPRESSED_CONCLUSIONS=PerformanceSpiBusAdapterIsMaxFileSpace
```

Restart NNMi (by running **ovstop** and **ovstart**) after making this change.

GNM with NPS in a Windows Environment

Note: For this setup, use only Windows NNMi management server.

To install NPS in a GNM environment, follow these steps:

1. Complete the GNM configuration between two NNMi management servers. The details of this process are described in the *HPE Network Node Manager i Software Deployment Reference*.
2. Go to the Global Manager and run the `nnmenableperfspi.ovpl` script. The script shows the following question:

   ```
   What username would you like for the new local account ? Or press [return] if you want to use an existing local or domain account.
   ```

3. Type a user name of your choice (for example, `localact`), and then press **Enter**. The following question appears:

   ```
   Type a password for the user:
   ```

4. Type a password of your choice, and then press **Enter**. The following question appears:

```
Retype the password to confirm:
```

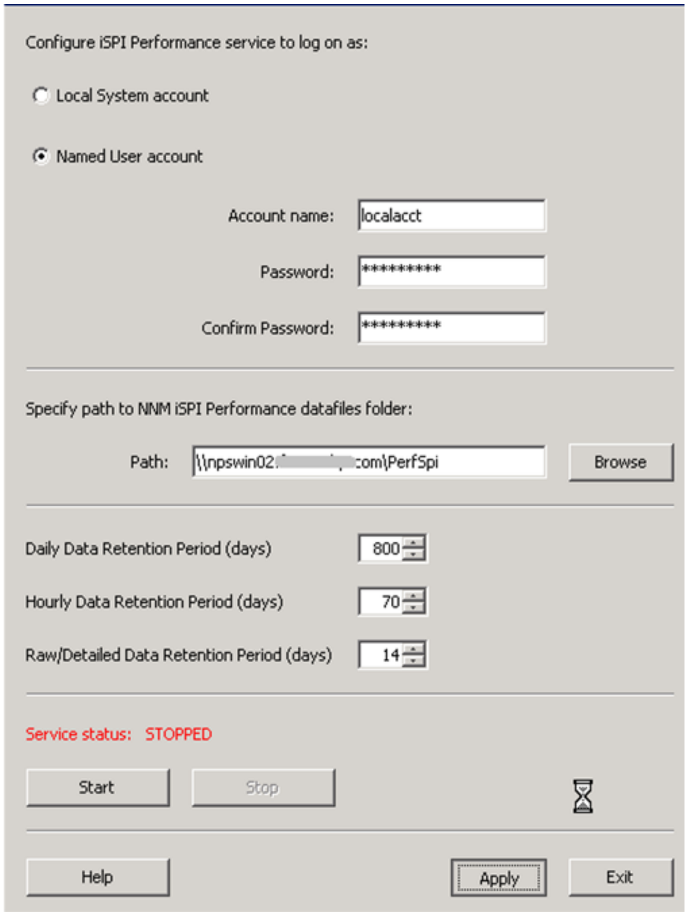
5. Type the password again, and then press **Enter**. The string of messages appears in the console, which includes the following message:

```
set <Path to iSPI Performance datafile folder> to: \\<NPS_FQDN>\PerfSpi
```

   In this instance, *<NPS_FQDN>* is the FQDN of the NPS system. Note down the user name and password provided in this step.

6. Install the NNM iSPI Performance for Metrics on a separate, dedicated system.

   Near the end of the installation, the installer opens the HPE NNMi iSPI Performance Configuration window and you are prompted to enter the shared path to the Global Manager.



Configure iSPI Performance service to log on as:

○ Local System account

● Named User account

Account name: localacct

Password: **********

Confirm Password: **********

Specify path to NNM iSPI Performance datafiles folder:

Path: \\npswin02.[redacted]com\PerfSpi

Daily Data Retention Period (days): 800

Hourly Data Retention Period (days): 70

Raw/Detailed Data Retention Period (days): 14

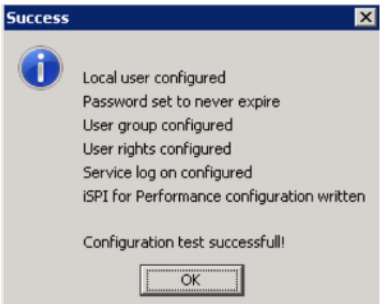
Service status: STOPPED

7. Type the following path in the Path box:

   \\<NPS_FQDN>\PerfSpi

8. Type the account name and password that you noted down above"GNM with NPS in a Windows Environment" on the previous page.

9. Then click Apply. It will run a configuration test at this point. You should see a success window as shown below.

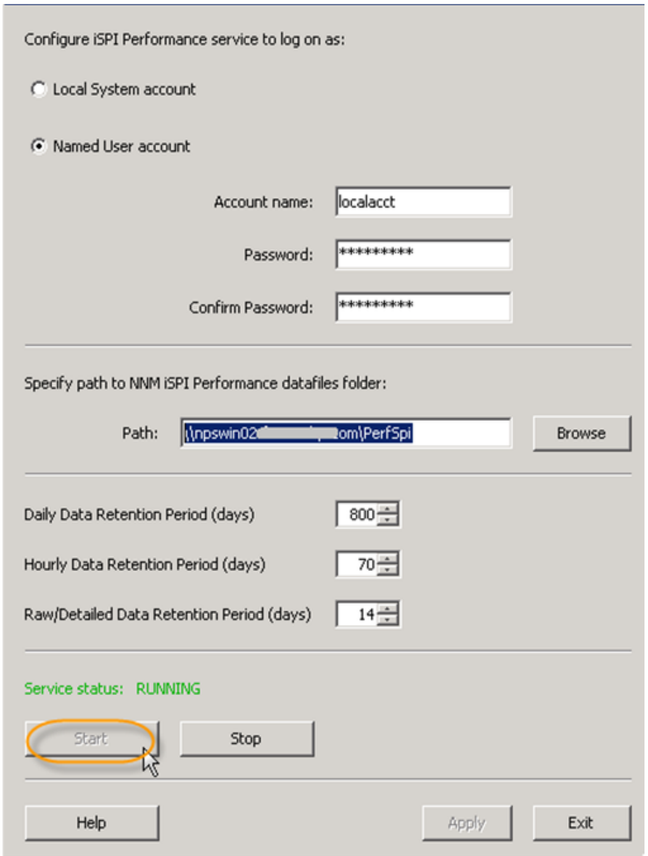


Success

Local user configured
Password set to never expire
User group configured
User rights configured
Service log on configured
iSPI for Performance configuration written

Configuration test successfull!

10. Now click **Start** to start the services.



Configure iSPI Performance service to log on as:

○ Local System account

● Named User account

Account name: localacct

Password: **********

Confirm Password: **********

Specify path to NNM iSPI Performance datafiles folder:

Path: \\npswin02[redacted]om\PerfSpi

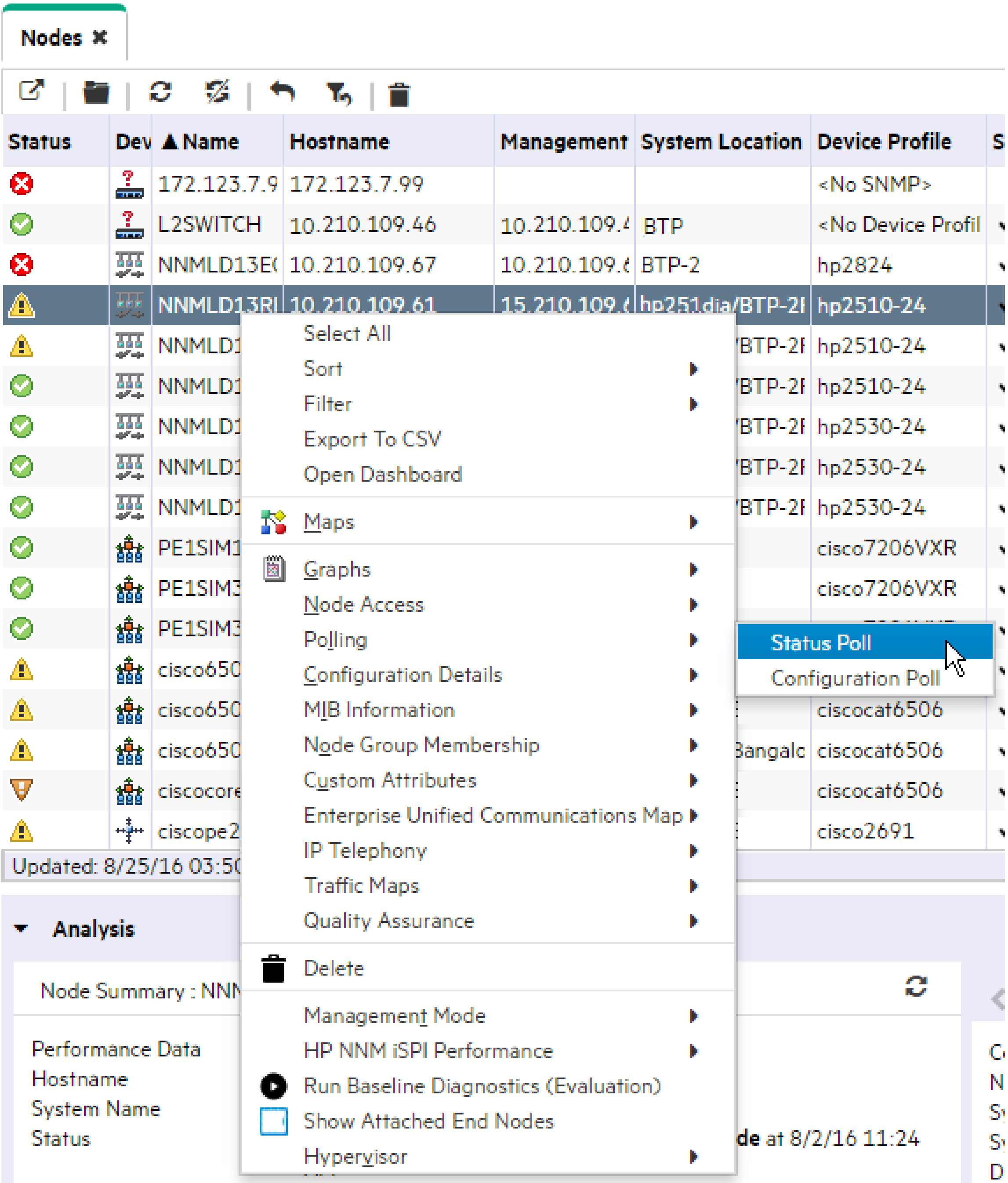
Daily Data Retention Period (days) 800

Hourly Data Retention Period (days) 70

Raw/Detailed Data Retention Period (days) 14

Service status: RUNNING

11. *Optional.* You can perform a status poll of a router from the Global Manager. You will notice that the Global Manager does not do any performance polling yet because performance polling is not enabled on Regional Managers. Performance polling is enabled and licensed on the Global Manager.



Status	Dev	▲Name	Hostname	Management	System Location	Device Profile	S
✗		172.123.7.9	172.123.7.99			<No SNMP>	
✓		L2SWITCH	10.210.109.46	10.210.109.4	BTP	<No Device Profil	
✗		NNMLD13E(	10.210.109.67	10.210.109.(	BTP-2	hp2824	
⚠		NNMLD13RI	10.210.109.61	15.210.109.(	hp251dia/BTP-2I	hp2510-24	
⚠		NNMLD1			BTP-2I	hp2510-24	
✓		NNMLD1			BTP-2I	hp2510-24	
✓		NNMLD1			BTP-2I	hp2530-24	
✓		NNMLD1			BTP-2I	hp2530-24	
✓		NNMLD1			BTP-2I	hp2530-24	
✓		PE1SIM1				cisco7206VXR	
✓		PE1SIM3				cisco7206VXR	
✓		PE1SIM3					
⚠		cisco650					
⚠		cisco650				ciscocat6506	
⚠		cisco650			Bangalc	ciscocat6506	
▽		ciscocore				ciscocat6506	
⚠		ciscope2				cisco2691	

Updated: 8/25/16 03:5(

Node Summary : NNN

Performance Data
Hostname
System Name
Status

de at 8/2/16 11:24

12. Install the NNMi Ultimate or Premium license on each Regional Manager by using the `nnmlicense.ovpl` command, but do not run the `nnmenableperfspi.ovpl` script.
13. On the Global Manager, install an NNMi Ultimate or Premium license.
14. *Optional.* Now if you run the status poll of an object from the Global Manager, you will see that the object is polled for performance data.

Note: After some time, you will see several `.csv.gz` files accumulating in the `%NNMDataDir%\shared\perfSpi\datafiles\metric\final` directory on each Regional Manager.

These files are generated by the Regional Manager's state poller. You can delete these files at any time. This buildup of files will cause a warning eventually on the Regional Manager. Note that NNMi will not place more than 1 GB (by default) of files into this directory.

NNMi may show the following error messages in the System Information window:

```
The Performance SPI Custom Poller Bus Adapter has status Minor because the file space
limit (10 megabytes) has been reached and no additional data can be written.
```

```
The Performance SPI Bus Adapter has status Minor because the file space limit (10
megabytes) has been reached and no additional data can be written.
```

You can control the accumulation of `.csv.gz` files by reducing the maximum size of the storage of these files. You can also configure NNMi to suppress alerting of this issue (that is, buildup of `.csv.gz` files in the `nps_baselinestate` directory.

To control the buildup of `.csv.gz` files, edit the `%NNMDataDir%\shared\perfSpi\conf\nmsAdapter.conf` file on each Regional Manager by changing the maxFileSpaceMB property to a smaller number like 10.

For example:

```
maxFileSpaceMB:10Restart NNMi (by running ovstop and ovstart) after making this
change.
```

To suppress alerting of the buildup of `.csv.gz` files, edit the `%NNMDataDir%\shared\nnm\conf\props\nms-topology.properties` file on each Regional Manager by adding the following lines:

```
#Suppress warnings about Max Space on regional NNMicom.hp.ov.nms.health.SUPPRESSED_
CONCLUSIONS=PerformanceSpiBusAdapterIsMaxFileSpace
```

Restart NNMi (by running **ovstop** and **ovstart**) after making this change.

Notes and Limitations

- With the installation of the Premium or Ultimate licenses, the **HPE NNM iSPI Performance** menu items appear on both regional and Global Managers. The menu items on Regional Managers are unresponsive and can be masked since no corresponding NPS systems are attached to them.
- The QA Performance dashboard menu does not show any data on the Regional Manager.
- All tabs related to the performance metrics in the analysis panes of nodes and interfaces are available only on the Global Manager. These tabs are not available on the Regional Manager.
- The **Open Dashboard** context menu item on node and interface objects on the Regional Manager cannot show panels that display performance data.
- The Performance Analysis workspace with inventories of Node Performance Metrics and Interface Performance Metrics are available only on the Global Manager.
- The performance tab in the analysis pane for the performance category of incidents shows performance data only on the Global Manager.

- Real-time performance data is unavailable when the connectivity between regional and Global Managers is disrupted. However, with the restoration of the connectivity, the performance data becomes available for monitoring.

Part VII: Installing NPS Patches in High-Availability Clusters

This section of the document provides step-by-step instructions to install a patch on NPS in a high-availability (HA) cluster. This chapter also provides you with steps to uninstall a patch on NPS in a HA cluster.

Installing a Patch on NPS in HA Cluster

> **Note:** Patch must be first applied on all the passive nodes.

Installing a Patch on the Passive Node

1. Before applying the patch on each passive node, temporarily move the HA cluster to maintenance mode. To move a node in a HA cluster to maintenance mode, create the following files on each passive NPS server:

   On Linux:

   - `/var/opt/OV/hacluster/<resource_group>/maintenance`
   - `/var/opt/OV/hacluster/<rsource_group>/maint_NNM`

   On Windows:

   - `%NPSDataDir%/../hacluster/<resource_group>/maintenance`
   - `%NPSDataDir%/../hacluster/<rsource_group>/maint_NNM`

2. On each passive node in the cluster, log on with the administrative privileges and temporarily remove the node from the HA cluster.

   On Linux:

   Before unconfiguring, check the following:

   a. Go to the following directory:
      `/var/opt/OV`

   b. Check if `NNMPerformanceSPI_HA_Backupdir` is a link.

      If it is a link, remove it and move `NNMPerformanceSPI_HA_Backupdir.<timestamp>`, which is a physical directory, to `NNMPerformanceSPI_HA_Backupdir`.

      If it is not a link, do not change anything.

   To unconfigure, run the following command:

   On Linux:

   /opt/OV/misc/nnm/ha/nnmhaunconfigure.ovpl PerfSPIHA <resource_group> (for a dedicated NPS setup)

/opt/OV/misc/nnm/ha/nnmhaunconfigure.ovpl NNM –addon PerfSPIHA (for a co-located NPS setup)

> **Note:** For a co-located setup, make sure that the **/opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS** command does not list a passive node.

On Windows:

- **%NPSInstallDir%/../misc/nnm/ha/nnmhaunconfigure.ovpl PerfSPIHA <resource_group>** (for a dedicated NPS setup)
- **%NnmInstallDir%/misc/nnm/ha/nnmhaunconfigure.ovpl NNM –addon PerfSPIHA** (for a co-located NPS setup)

> **Note:** For a co-located setup, make sure that the **%NnmInstallDir%/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS** command does not list a passive node.

3. Install the NPS Patch. Follow the patch installation steps given in the patch document, and ensure that the patch is installed successfully.

   > **Caution:** Do not configure HA back on this node until the patch is applied on the active node.

4. Run the following command to stop the processes that were started during the patch install (in a new shell):

   On Linux:

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

   On Windows:

   %NPSInstallDir%/bin/stopALL.ovpl

Installing a Patch on the Active Node

1. Before applying the patch on the active node, temporarily move the HA cluster to maintenance mode. HA cluster on a node can be moved to maintenance mode by creating the following files on the active NPS server:

   On Linux:

   - `/var/opt/OV/hacluster/<resource_group>/maintenance`
   - `/var/opt/OV/hacluster/<rsource_group>/maint_NNM`

   On Windows:

   - `%NPSDataDir%/../hacluster/<resource_group>/maintenance`
   - `%NPSDataDir%/../hacluster/<rsource_group>/maint_NNM`

2. Install the NPS Patch. Follow the patch installation steps given in the patch document, and ensure that the patch is installed successfully.

Caution: Do not unconfigure HA on the active node at this point.

3. After the installation is done, stop all the NPS processes by running the following command:

   On Linux:

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

   On Windows:

   %NPSInstallDir%/bin/stopALL.ovpl

4. Open a new shell and run the following command to start all the processes:

   On Linux:

   /opt/OV/NNMPerformanceSPI/bin/startALL.ovpl

   On Windows:

   %NPSInstallDir%/bin/startALL.ovpl

5. *On Linux only*. Set the mount point using the following command in the active node:

   /opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl -config PerfSPIHA –set <mount-point>

6. Re-enable perfspi integration by running the following script on the NNMi system:

   On Linux:

   $NnmInstallDir/bin/nnmenableperfspi.ovpl

   On Windows:

   %NnmInstallDir%/bin/nnmenableperfspi.ovpl

   Note: For more information, see the “*"Enabling NNMi to Work with NPS" on page 22*” topic. Provide the virtual FQDN of the NPS HA setup when prompted for the NPS host name.

Reconfiguring the Passive Nodes Back in HA Cluster

1. On each passive node, run the following command to reconfigure HA:

   On Linux:

   - `/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl PerfSPIHA (for dedicated setup)`

   - `/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl NNM –addon PerfSPIHA (for co-located setup)`

   Note: For a co-located setup, make sure that the **/opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS** command does not list a passive node.

   On Windows:

   - **%NPSInstallDir%/../misc/nnm/ha/nnmhaconfigure.ovpl PerfSPIHA** (for dedicated setup)

   - **%NnmInstallDir%/misc/nnm/ha/nnmhaconfigure.ovpl NNM –addon PerfSPIHA** (for co-located setup)

> **Note:** For a co-located setup, make sure that the **%NnmInstallDir%/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS** command does not list a passive node.

2. Remove the passive nodes out of maintenance mode. HA cluster node can be moved out of maintenance mode by deleting the following files on all the passive NPS nodes:

   On Linux:

   - `/var/opt/OV/hacluster/<resource_group>/maintenance`
   - `/var/opt/OV/hacluster/<rsource_group>/maint_NNM`

   On Windows:

   - `%NPSDataDir%/../hacluster/<resource_group>/maintenance`
   - `%NPSDataDir%/../hacluster/<rsource_group>/maint_NNM`

3. Remove the active node out of maintenance mode. HA cluster node can be moved out of maintenance mode by deleting the following files on the active NPS system:

   On Linux:

   - `/var/opt/OV/hacluster/<resource_group>/maintenance`
   - `/var/opt/OV/hacluster/<rsource_group>/maint_NNM`

   On Windows:

   - `%NPSDataDir%/../hacluster/<resource_group>/maintenance`
   - `%NPSDataDir%/../hacluster/<rsource_group>/maint_NNM`

Uninstalling an NPS Patch from HA Clusters

> **Note:** Patch must be first uninstalled on all the passive nodes. Read the patch *readme* file to determine if the patch can be uninstalled.

Uninstalling a Patch on the Passive Node

1. Before uninstalling the patch on each passive node, temporarily move the HA cluster to maintenance mode. HA cluster on a node can be moved to maintenance mode by creating the following files on each passive NPS server:

   On Linux:

   - `/var/opt/OV/hacluster/<resource_group>/maintenance`
   - `/var/opt/OV/hacluster/<rsource_group>/maint_NNM`

   On Windows:

- `%NPSDataDir%/../hacluster/<resource_group>/maintenance`
- `%NPSDataDir%/../hacluster/<rsource_group>/maint_NNM`

2. On each passive node in the cluster, log on with the administrative privileges and temporarily remove the node from the HA cluster by running the following command:

   On Linux:

   - **/opt/OV/misc/nnm/ha/nnmhaunconfigure.ovpl PerfSPIHA <resource_group>**(for a dedicated NPS setup)
   - **/opt/OV/misc/nnm/ha/nnmhaunconfigure.ovpl NNM –addon PerfSPIHA** (for a co-located NPS setup)

   Note: For a co-located setup, make sure that the **/opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS** command does not list a passive node.

   On Windows:

   - **%NPSInstallDir%/../misc/nnm/ha/nnmhaunconfigure.ovpl PerfSPIHA <resource_group>** (for a dedicated NPS setup)
   - **%NnmInstallDir%/misc/nnm/ha/nnmhaunconfigure.ovpl NNM –addon PerfSPIHA** (for a co-located NPS setup)

   Note: For a co-located setup, make sure that the **%NnmInstallDir%/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS** command does not list a passive node.

3. Uninstall the NPS patch. Follow the patch uninstallation steps given in the patch document, and ensure that the patch is uninstalled successfully.

   Caution: Do not reconfigure HA back on this node until the patch on the active node is uninstalled.

4. Run the following command to stop the processes that were started during the patch uninstall (in a new shell):

   On Linux:

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

   On Windows:

   %NPSInstallDir%/bin/stopALL.ovpl

Uninstalling a Patch on the Active Node

1. Before uninstalling the patch on the active node, temporarily move the HA cluster to maintenance mode. HA cluster on a node can be moved to maintenance mode by creating the following files on active NPS server:

   On Linux:

- `/var/opt/OV/hacluster/<resource_group>/maintenance`
- `/var/opt/OV/hacluster/<rsource_group>/maint_NNM`

On Windows:

- `%NPSDataDir%/../hacluster/<resource_group>/maintenance`
- `%NPSDataDir%/../hacluster/<rsource_group>/maint_NNM`

2. Uninstall the NPS Patch. Follow the patch uninstallation steps given in the patch document file, and ensure that the patch is uninstalled successfully.

   > **Caution:** Do not unconfigure HA on the active node at this point.

3. After the patch is uninstalled, stop all the NPS processes by running the following command:

   On Linux:

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

   On Windows:

   %NPSInstallDir%/bin/stopALL.ovpl

4. Open a new shell and run the following command to start all the processes:

   On Linux:

   /opt/OV/NNMPerformanceSPI/bin/startALL.ovpl

   On Windows:

   %NPSInstallDir%/bin/startALL.ovpl

5. Re-enable perfspi integration by running the following script on the NNMi system:

   On Linux:

   $NnmInstallDir/bin/nnmenableperfspi.ovpl

   On Windows:

   %NnmInstallDir%/bin/nnmenableperfspi.ovpl

   > **Note:** For more information, see the "*"Enabling NNMi to Work with NPS" on page 22*" topic. Provide the virtual FQDN of the NPS HA setup when prompted for the NPS host name.

Reconfiguring the Passive Nodes Back in HA Cluster

1. On each passive node, run the following command to reconfigure HA:

   On Linux:

   - `/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl PerfSPIHA` (for dedicated setup)
   - `/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl NNM –addon PerfSPIHA` (for co-located setup)

   > **Note:** For a co-located setup, make sure that the **/opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS** command does not list a passive node.

   On Windows:

- `%NPSInstallDir%/../misc/nnm/ha/nnmhaconfigure.ovpl PerfSPIHA` (for dedicated setup)
- `%NnmInstallDir%/misc/nnm/ha/nnmhaconfigure.ovpl NNM –addon PerfSPIHA` (for co-located setup)

> **Note:** For a co-located setup, make sure that the **%NnmInstallDir%/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS** command does not show a passive node in this list.

2. Remove the passive nodes out of maintenance mode. HA cluster node can be moved out of maintenance mode by deleting the following files on all the passive NPS nodes:

   On Linux:

   - `/var/opt/OV/hacluster/<resource_group>/maintenance`
   - `/var/opt/OV/hacluster/<rsource_group>/maint_NNM`

   On Windows:

   - `%NPSDataDir%/../hacluster/<resource_group>/maintenance`
   - `%NPSDataDir%/../hacluster/<rsource_group>/maint_NNM`

3. Remove the active node out of maintenance mode. HA cluster node can be moved out of maintenance mode by deleting the following files on the active NPS server:

   On Linux:

   - `/var/opt/OV/hacluster/<resource_group>/maintenance`
   - `/var/opt/OV/hacluster/<rsource_group>/maint_NNM`

   On Windows:

   - `%NPSDataDir%/../hacluster/<resource_group>/maintenance`
   - `%NPSDataDir%/../hacluster/<rsource_group>/maint_NNM`

Part VIII: Maintaining NPS

After installing and configuring NPS, you might want to make changes to your environment like changing the IP address or hostname of the NPS system or the NNMi management server. You might want to free up ports used by NPS and configure non-default ports for NPS. This chapter provides you with steps to make these changes after NPS is completely installed and configured.

Modifying the FQDN of the NPS System

If you change the FQDN of the NPS system, you must perform the following steps before using NPS:W

1. Log on to the NNMi management server as root or administrator.
2. *In a co-located setup.*

   If NPS co-exists with NNMi, you must run the `nnmsetofficialfqdn.ovpl` command.

   a. Go to `%nnminstalldir%\bin` on Windows and `/opt/OV/bin` on Linux.

   b. Run the `nnmsetofficialfqdn.ovpl` script.

   c. Go to `%nnminstalldir%\NNMPerformanceSPI\bin` on Windows and `/opt/OV/NNMPerformanceSPI/bin` on Linux.

   d. Run the `configureServerID.ovpl` script.

   e. Go to `%nnminstalldir%\bin` on Windows and `/opt/OV/bin` on Linux.

   f. Run the `nnmenableperfspi.ovpl` script.

   The following prompt appears:

   ```
   Do you wish to use the prior selections as defaults? (Y/N):
   ```

   i. Type **Y**, and then press **Enter**.

   ii. Press **Enter** for all prompts.
3. *In a dedicated NPS setup.*

   If NPS is installed on a dedicated server, follow these steps:

   a. On the NNMi management server, run the `nnmdisableperfspi.ovpl` script.

   The `nnmdisableperfspi.ovpl` script is available in the *%nnminstalldir%*`\bin` directory on Windows and `/opt/OV/bin` directory on Linux.

   b. *Linux only.* If NPS is installed on Linux, run the following command on the NPS system to unmount the shared drive that was created to facilitate data exchange between NPS and NNMi.

   umount /<*share_name*>

   In this instance, <*share_name*> is the name of the share created while installing NPS.

   c. On the NPS system, run the `configureServerID.ovpl` script.

   The `configureServerID.ovpl` script is available in the *%npsinstalldir%*`\bin` directory on Windows and `/opt/OV/NNMPerformanceSPI/bin` directory on Linux.

   d. On the NNMi management server, run the `nnmenableperfspi.ovpl` script.

   The `nnmenableperfspi.ovpl` script is available in the *%nnminstalldir%*`\bin` directory on Windows and `/opt/OV/bin` directory on Linux.

Modifying the Default Communication Port

By default, NPS uses the port 9300 (for HTTP) or 9305 (for HTTPS) for communication via a web browser. After NPS is installed and configured, you can modify the NPS configuration to change the NPS communication port.

To change the communication port:

Note: When NPS is installed in a high availability cluster, perform this task on the active server first, fail over to the other server, and then perform the task again on the server that is currently active.

In a distributed deployment of NPS, perform this task on the UiBi Server.

1. Log on to the NPS system as root or administrator.
2. If NPS is configured for HTTP communication, run the following command:

   configureWebAccess.ovpl -newport <*port_number*>

   If NPS is configured for HTTPS communication, run the following command:

   configureWebAccess.ovpl -newport <*port_number*> **-ssl**

   In this instance, <*port_number*> is the new communication port number.

Maintaining the NPS Database

The NPS database store a large amount of data that is gathered from different sources (like NNMi and iSPIs) and enables NPS to compute aggregates from a large number of data points. The database can keep 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.

With scripts and utilities available with NPS, you can monitor the health and performance of the database and perform maintenance tasks like checking the health of the database, deleting and recreating the database, and so on.

Changing the Default Database Password

The NPS installer installs the NPS database with a default password.

To change the default database password, log on to the NPS system as root or administrator, and then run the following command:

changeDBpwd.ovpl <*new_password*>

In this instance, <*new_password*> is the password of your choice.

> **Note:** In a distributed deployment of NPS, you must run the above command on each NPS system in the following order:
>
> 1. DB Server
> 2. UiBi Server
> 3. ETL Server

Checking the Database Health

The `dbsize.ovpl` utility enables you to check the health of the NPS database.

To use the `dbsize.ovpl` utility to check the health of the NPS database, follow these steps:

1. Log on to the NPS system as root or administrator. In a distributed deployment of NPS, log on to the DB Server as root or administrator.
2. Open a command line console, and then run one of the following commands:

Command	Description
dbsize.ovpl -q	The command output displays the usage summary of different dbspaces within the database. (NPS creates the following dbspaces within the database: `IQ_SYSTEM_MAIN`, `IQ_SYSTEM_TEMP`, and `USER_MAIN`).
dbsize.ovpl -s	The command output displays the size of different fact tables

Command	Description
	for each Extension Pack.
statusDB.ovpl	The command output displays the status of the NPS database.

Back Up and Restore

NPS provides command-line tools that back up and restore all NPS data.

To back up the NPS data:

> **Tip:** Before you begin, make sure sufficient disk space exists on the NPS system to run the backup procedure and store the backed-up data. Determine the size of the NPS database, content store, and configuration and archived data files.
>
> To determine the size of the NPS database, run the following command:
>
> **dbsize.ovpl -q**
>
> To determine the size of the content store, run the following command:
>
> **cssize.ovpl -q**
>
> To determine the total size of all configuration and archived data files, measure the size of the following directory:
>
> *On Windows*
>
> `%npsdatadir%`
>
> *On Linux*
>
> `/var/opt/OV/NNMPerformanceSPI`

1. Log on to the NPS system with the same account used to install NPS.
2. Run the following command:

   ```
   backup.ovpl -b <dir> [-c] [-d] [-f]
   ```

In this instance, *<dir>* is the location where you want to place the backed-up data. Do not use environment variables with this option.

Options

- Use the `-c` option to back up the content store.
- Use the `-d` option to back up the database.
- Use the `-f` option to back up all NPS configuration and archived data files.
- Use the `-t` option to suppress creating a single compressed archive (tar.gz) file. This option leaves the directory as is on the file system, and greatly speeds up the backup process.

You must specify a valid directory location as an argument of the `-b` option. If you do not specify any other options, the backup script will back up the content store and the database.

The duration of the backup process depends on the size of the database. Before you start the backup process, verify the amount of disk space used by the data you want to back up, and make sure the system has enough free disk space. Although the script produces compressed output, the backup process requires sufficient temporary disk space.

For command details, see backup.ovpl

To restore NPS data:

1. Log in to the NPS system with the same account used to install NPS.
2. Run the following command:

   ```
   restore.ovpl [-h] [-b <file>] [-l] [-r DBFILE=>NEW_PATH_TO_DBFILE.iq[,DBFILE=>NEW_
   PATH_TO_DBFILE.iq]]
   ```

In this instance:

`-h`	displays this text
`-b <file>`	specifies backup file
`-l`	lists file content without restoring
`-r DBFILE=>NEW_PATH_TO_DBFILE.iq [,DBFILE=>NEW_PATH_TO_DBFILE.iq]`	allows one or more database file to be restored to the specified (non-default) location

The restore operation overwrites all preceding NPS data.

When the restore is complete, the ETL service will not be running. You must restart the service to resume the processing of new data. To start ETL, run the startETL.ovpl, startALL.ovpl command, or use the Start button on the Configuration Utility.

If you change the password of the database after a backup operation, you must change it again after restoring the backed-up database.

Incremental Backup

A comprehensive backup strategy is essential for disaster recovery. Although full backups are simple to implement and easy to execute when restoration is required, they can slow down processes that are running, take a long time to complete, and require large (sometimes excessively large) amounts of storage.

Incremental backups, however, can balance speed, resource conflicts, and required storage against ease of restoration.

The purpose of a backup is to provide a recovery point. Different systems have different requirements for recovery points. A backup strategy that offers daily recovery points can be implemented through a weekly schedule of full backups combined with incremental daily backups on all other days.

For additional security, each backup should be stored on removable media and made secure. This should also include creating several generations of media.

To implement a backup strategy that incorporates four generational copies:

1. Run a full backup.ovpl backup on a weekly basis.

   Use no backup flags (that is, c, d, or f) so that the database, the content store, and the file system are backed up.

   Here is an example:

- Linux:

  ```
  $NPSInstallDir/bin/backup.ovpl -b /var/backup/full
  ```

- Windows:

  ```
  %NPSInstallDir%\bin\backup.ovpl -b E:\backup\full
  ```

2. Copy the backed up data to one of four versions of backup tapes.

   Backup tapes should be kept off site. Alternatively, they can be created directly using WAN links to copy data.
3. Run an incremental backup on a daily basis.

   Use no backup flags (c, d, or f) , so that the database, the content store, and the file system are backed up.

   Use the optional –i flag to perform an incremental backup.

   Here is an example:

   - Linux

     ```
     $NPSInstallDir/bin/backup.ovpl -b /var/backup/incremental -i
     ```

   - Windows

     ```
     %NPSInstallDir%\bin\backup.ovpl -b E:\backup\incremental -i
     ```

   Only changes since the last backup (full or incremental) are saved.
4. Copy the backed up data to one of four backup tapes.

   Append the data. Do not overwrite existing backed up data.

If restoration is required:

- Restore from the desired full backup. See the reference page or man page for restore.ovpl.
- Restore (in sequential order) each incremental backup from oldest to most recent.

> **Note:** When restoring an incremental backup that includes the content store, you must restore each backup in turn without starting the BI Server. If you start the BI Server, it will write to the content store database and prohibit restoring from any further incremental backups.
>
> If you do write to the content store database before restoring an incremental backup, you must return to the full backup and start the restoration process again.

Backing Up and Restoring on the Same System

If the backup is restored on the same system with the same installation directories and product version as the backup, the entire contents of data directory will be restored, including all configuration files, archived data files, the database, and the content store.

Restoring a Backup Made on a Previous Product Version

Backups made on earlier product versions can be restored with some limitations.

- User configurable settings (retention and installed Extension Pack list) are merged into the current settings.
- The database and content store are restored.
- Other (internal) configuration files are not restored. The restore command
- Archived data files are not restored.
- All Extension Packs must be installed again to ensure that the reports and database structures are upgraded to the latest version.

Prerequisite for Restoring a Backup Made on NPS 10.00 or Lower

Skip this procedure if you want to restore a backup made on 10.10 (or higher).

To restore the data backed up on NPS 10.00 or lower, make sure that the source NPS database password match the target NPS 10.30 database password.

> **Note:** As a best practice, you must always change the default NPS database password after installation by running the following command:
>
> **changeDBpwd.ovpl** <*password*>
>
> In this instance, <*password*> is the non-default NPS database password.

To restore the data backed up on NPS 10.00 or lower, make sure that the source NPS database password matches the target NPS 10.30 database password.

If the source NPS system had a different database password, run the following command on the target NPS 10.30 system before beginning the restore procedure:

changeDBpwd.ovpl <*old_password*>

In this instance, <*old_password*> is the non-default NPS database password that was configured with the source NPS system.

Restoring Data

To restore the data that was backed up on a previous version of NPS, follow these steps:

> **Note:** In a distributed deployment of NPS, you must perform these steps on the DB Server.

1. Transfer the backup file to the NPS system
2. Log in to the NPS system as root or administrator.
3. Run the following command:

   restore.ovpl -b <*backup_file*>

   In this instance, <*backup_file*> is the backup file.

   > **Note:** If the command fails to work and shows an error message (`C API (dbcapi) could not be loaded`), open a new command prompt and run the command again.

4. After running the `restore.ovpl` command, follow these steps:
   a. Run the Configuration Utility again and check that all the settings (share name, user name, data

retention periods, and so on) are correct.

To open the Configuration Utility, run the following command:

runConfigurationGUI.ovpl

b. Run the following command to configure the communication protocol and port:

   configureWebAccess.ovpl -newport <*port_number*> **[-ssl]**

   In this instance, <*port_number*> is the communication port that you have chosen while running the nnmenableperfspi.ovpl command. Use the `-ssl` parameter only if you want to use the HTTPS communication.

c. Run the following commands:

   i. **initializeNPS.ovpl -a StartBIServer**
   ii. **initializeNPS.ovpl -a SetupCSRolesAndSecurity**
   iii. **initializeNPS.ovpl -a ConfigBIAccess**
   iv. **initializeNPS.ovpl -a RestartBIServer**
   v. **startDB.ovpl**
   vi. **addSdkUser.ovpl -u npssdkuser**
   vii. **changeSdkUserPwd.ovpl -u npssdkuser -p HP_NPS**

d. Run the following command to complete the upgrade of each Extension Pack:

   installExtensionPack.ovpl -x -e <*Extension_Pack*>**.tar.gz**

   In this instance, <*Extension_Pack*> is the name of the Extension Pack bundle.

   > **Note:** To view the names of Extension Pack bundles, run the following command:
   >
   > **about.ovpl**

e. Run the following command if the Path Health Extension Pack was in use with the previous version of NPS:

   installPathHealth.ovpl -e Path_Health.tar.gz

f. Run the following command if you created security groups in NNMi:

   installUgSg.ovpl -e ugsg.tar.gz

g. Run the following command if Custom Poller Extension Packs were in use with the previous version of NPS:

   initializeNPS.ovpl -a InitializeCustomCollections

Restoring a Backup Made on a Different System with Different Installation Directories

Backups made on a different system with different installation directories can be restored with some limitations.

- User configurable settings (retention and installed Extension Pack list) are merged into the current settings.
- Other (internal) configuration files are not restored.
- Archived data files are not restored.

- The database and content store are restored.
- All Extension Packs must be installed again to ensure that the reports and database structures are upgraded to the latest version.
- You might have to rerun the nnmenableperfspi.ovpl script and Configuration Utility.

Restoring a Backup When Additional Files Were Added to Extend the Database

If the `dbsize.ovpl` utility was used to extend a database by adding additional files to the DBSPACE, the backup will attempt to restore these files to the same directory as the standard database files.

To relocate database files during a restore:

The `-r` option enables you to identify one or more DBFile names and corresponding OS path or file name locations where each should be restored.

When dbsize.ovpl is used to add files, the DBFile names used will look like `perfspi_USER_MAIN_<timestamp>`. You can use the `-l` option to determine the files to be included in your backup (for backups made on 9.20 and later).

You can specify a different OS path or file name when restoring by using the `-r` option; for example, `restore.ovpl -b backup.20111027135608.tar.gz -r "perfspi_USER_MAIN_3466235673656=>C:/new location/perfspi_USER_MAIN_3466235673656.iq"`.

If you backed up the content store using the standard backup utility provided in earlier releases, you will not be able to restore them in the current release. The current database backup format is incompatible with earlier releases.

Post-Restore Steps on Windows

Skip this section if NPS is installed on Linux.

After restoring the NPS data on a new system, you must run the following commands on the NPS system:

> **Note:** Run the commands by logging in as the user that was configured while running the `nnmenableperfspi.ovpl` command.

- **addSdkUser.ovpl -u** <*user_name*>
- **changeSdkUserPwd.ovpl -u** <*user_name*> **-p** <*password*>

In this instance, <*user_name*> is a user name of your choice and <*password*> is a password that you need to choose for <*user_name*>.

If you do not run the above commands, you will not be able to use the Performance Analysis inventory view and the Interface Health and Component Health dashboards in the NNMi console.

Recreating the NPS Database

You can recreate your Sybase IQ database and start over with the installation default size of 2.5 GB. This feature can be useful if your existing database has grown too large, or if you want to lower your retention settings. Lowering the retention settings will maintain the smaller size of the database for a longer period of time. The `resetNPS.ovpl` utility enables you to delete and recreate the NPS database.When the NPS database becomes irrecoverably corrupt, you can delete and recreate the database.

Modifying Default Settings

> **Note:** If you do not want to modify any settings of the NPS database, skip this section and go to Recreate the Database.

1. Open the `databaseSetup.cfg` file from the following directory:
   - *On Windows:*`%NPSInstallDir%\config`
   - *On Linux:*`$NPSInstallDir/config`
2. Make the following changes:
   - **Cache settings:**
     - To allocate a specific volume to the main cache, specify a value in MB for the `Db.Cfg.Iqmc` property.

       For example, to allocate 12 GB for the main cache, specify `Db.Cfg.Iqmc=12288`.
     - To allocate a specific volume to the temporary cache, specify a value in MB for the `Db.Cfg.Iqtc` property.

       For example, to allocate 12 GB for the temporary cache, specify `Db.Cfg.Iqtc=12288`.
   - **Dbspace settings:**
     - Number of Dbspace files:

       By default, NPS creates 20 Dbspace files. You can configure NPS to create more Dbspace files by appending additional `Db.DbFile` lines under the line `Db.DbFile.020`.

       For example:

       `Db.DbFile.021=default`

       `Db.DbFile.022=default`.
     - Dbspace location:

       If you want to store the Dbspace files in a non-default location in a non-default file, you can specify the location by replacing `default` with the complete path to the file.

       For example:

       `Db.DbFile.021=C:\Data\user_main_021.iq`

       > **Note:** File name must have the extension `iq`.
3. Save the file.

Recreate the Database

1. Log on to the NPS system as root or administrator. In a distributed deployment of NPS, log on to the DB Server as root or administrator.
2. Take a backup of the NPS database. For more information, see "To back up the NPS data:" on page 109
3. Open a command line console, and then run the following command:

   resetSPI.ovpl

4. Select the option 2.

   This option deletes the database, creates a new database, and then restores the archived data.

   After processing, deleting, and recreating the database, the command shows the following message:

   ```
   Do you want to start the ETL service now? (Y/N)
   ```

5. Type **N**,and then press Enter. The following message appears:

   ```
   Hit Enter key to exit...
   ```

6. Press **Enter**.
7. Run the **resetSPI.ovpl** command again.
8. Select the option 5.

   This option deletes the database (along with the archived data), and then creates a new database.

   After processing, deleting, and recreating the database, the command shows the following message:

   ```
   Hit Enter key to exit...
   ```

9. Press **Enter**.
10. Start the ETL process:

    startETL.ovpl

Tuning NPS

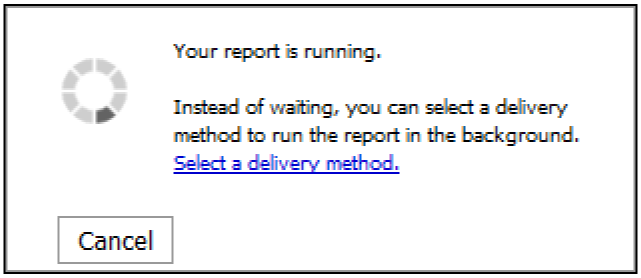
This chapter describes how to fine-tune different settings for an optimal performance of NPS in a large environment.

Tuning the Business Intelligence Server

The Business Intelligence Server enables you to generate insightful, web-based reports from the data in the database. The performance of the Business Intelligence Server depends on the number of scheduled reports and jobs, number of users trying to launch reports concurrently, and the underlying hardware. You can adjust the values of certain configuration parameters to resolve degrading performance of the Business Intelligence Server (or problems with launching reports) in a very large scale environment. This chapter provides guidelines for adjusting the configuration parameters to address performance issues.

Common symptoms of performance problems with the Business Intelligence Server are:

- Report takes a very long time to appear; the *Select a delivery method* prompt remains visible for a very long time.



Your report is running.

Instead of waiting, you can select a delivery method to run the report in the background. Select a delivery method.

- The NPS console shows a blank page instead of the report
- Error messages appear in the `Cognos.log` file (available in `%npsdatadir%\logs` on Windows, in `/var/opt/NNMPerformanceSPI/logs` on Linux)

Tip: In a distributed deployment of NPS, the UiBi Server hosts the Business Intelligence Server component.

Monitoring the Performance of the Business Intelligence Server

You can monitor the performance of the Business Intelligence Server with the help of performance monitoring tools provided by the operating system.

On Windows, you can use the Windows task manager and any Windows I/O benchmarking tools.

On Linux, you can use the `iostat` and `top` commands.

You can also detect performance problems with the help of the BI Portal. Follow these steps:

1. Log on to the NNMi console as administrator.
2. Click **Actions > NNM iSPI Performance > Reporting - Report Menu**. The NPS console opens.

3. In the NPS console, click the **BI Server** workspace in the navigation pane.
4. Click **Administration**. The BI Server Administration page opens.
5. In the BI Server Administration page, select **Interactive activities** in the Filter section, and then click **Apply**.The right pane displays the number of reports that are currently running.
6. Select **Background activities** in the Filter section, and then click **Apply**.The right pane displays the following details:
   - Number of reports that are running in the background (Executing)
   - Number of reports that are waiting to be run (Waiting)
   - Number of pending reports (Pending)
   - Number of suspended reports (Suspended)

   Too many pending and waiting reports lead to poor performance of the Business Intelligence Server.

You can also check the `Cognos.log` file (available in `%npsdatadir%\logs` on Windows, in `/var/opt/NNMPerformanceSPI/logs` on Linux) for errors. The following error messages in the `Cognos.log` file indicate performance problems:

- `http-9300-55 caf 2047 1 Audit.dispatcher.caf Request Failure SecureErrorId:` *<date>*-*<time>*`.646-#44 Original Error: DPR-ERR-2002 Unable to execute the request because there were no connections to the process available within the configured time limit`

  This error indicates that the system has too many reports currently in progress.

  To avoid this error, follow the steps in the Configuring Business Intelligence Server Settings section.
- `-567911568 QOS 5000 1 Audit.RTUsage.QOS <message code="-232" severity="error" title="QE-DEF-0459 CCLException" type="general">RQP-DEF-0177 An error occurred while performing operation &apos;sqlScrollBulkFetch&apos; status=&apos;-232&apos;. UDA-SQL-0107`

  This error indicates that NPS received an error from the underlying database.

  To avoid this error, limit the number of very large-scale reports over long time periods with very fine granularity.

Best Practices

- For frequently used reports, use Report Views. See the *Using Report Views* section in *Online Help*.
- You can also schedule frequently used reports. Do not schedule high-frequency schedules for reports that are viewed rarely.
- Reports that run with very long time ranges tend to be slow and put greater load onto the database. Consider using reports with short time ranges whenever possible.
- Reports that run with very fine time grains require excess resources from NPS while creating chart images or HTML table structures with drillthrough links. Consider using fewer reports that run with very fine time grains to speed up report runs and reduce the load.

Configuring Business Intelligence Server Settings

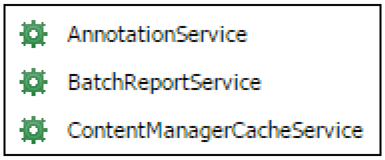
You can adjust the values of certain configuration parameters to resolve some performance problems. The changes outlined below enable the Business Intelligence Server to process more interactive report requests in parallel. This will place a larger load on the database server, but may be appropriate for a distributed deployment of NPS with multiple users all requesting reports simultaneously.

1. Log on to the NNMi console as administrator.
2. Click **Actions > NNM iSPI Performance > Reporting - Report Menu**. The NPS console opens.
3. In the NPS console, click the **BI Server** workspace in the navigation pane.
4. Click **Administration**. The BI Server Administration page opens.
5. In the BI Server Administration page, go to the Configuration tab.
6. In the left pane, click **Dispatchers and Services**.
7. Click the dispatcher on the Configuration page.

> **Tip:** You may see multiple dispatchers on this page if you used the `configureWebAccess.ovpl` command to change the default communication port of NPS. On the Configuration page, each dispatcher appears in the following format:
>
> *<hostname>*`:`*<port>*`/p2pd`
>
> In this instance, *<hostname>* is the hostname of the NPS system; *<port>* is the communication port for NPS.
>
> When you see multiple dispatchers, choose the active dispatcher that runs with the current NPS port.

8. Modify the `BatchReportService` parameters by following these steps:

   a. In the list of services, locate BatchReportService.

   AnnotationService
   BatchReportService
   ContentManagerCacheService

   b. Against BatchReportService, click ▤.

   c. Go to the Settings tab.

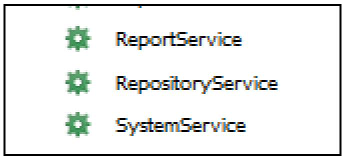
   d. You can modify the following properties:

Property	Default	Suggested Maximum Value
Number of high affinity connections for the batch report service during non-peak period	2	2
Number of low affinity connections for the batch report service during non-peak period	4	10
Maximum number of processes for the batch report service during non-peak period	2	10
Number of high affinity connections for the batch report service during peak period	2	2
Number of low affinity connections for the batch service during	4	10

Property	Default	Suggested Maximum Value
peak period		
Maximum number of processes for the batch report service during peak period	2	10

9. Modify the `ReportService` parameters by following these steps:

   a. In the list of services, locate ReportService.



ReportService
RepositoryService
SystemService

Tip: If you are unable to locate ReportService, click ⏩ **Next Page**.

   b. Against ReportService, click ▤.

   c. Go to the Settings tab.

   d. You can modify the following properties:

Property	Default	Suggested Maximum Value
Number of high affinity connections for the report service during non-peak period	2	10
Number of low affinity connections for the report service during non-peak period	8	10
Maximum number of processes for the report service during non-peak period	2	10
Number of high affinity connections for the report service during peak period	2	10
Number of low affinity connections for the report service during peak period	8	10
Maximum number of processes for the report service during peak period	2	10

10. Click **OK**. Changes take effect immediately.

Resolving Problems with Jobs and Report Scheduling

To resolve problems with jobs and report scheduling, modify the `max online engines` parameter. I f you see problems like scheduled reports failing to run or configured jobs not appearing in the navigation panel, follow these steps:

1. Log on to the NPS system (the UiBi Server in case of a distributed deployment of NPS).
2. Open the following file with a text editor:

   On Windows:

   ```
   %npsinstalldir%\nonOV\sybasease\ASE-15_0\ASECONTENTSERVER.cfg
   ```

   On Linux:

   ```
   /opt/OV/nonOV/sybasease/ASE-15_0/ASECONTENTSERVER.cfg
   ```

3. Set the value of the `max online engines` property to an integer (recommended value is 2 for a standalone NPS; set it to a value higher than 2 in a distributed deployment of NPS).
4. If you see the error message `CM-SYS-5025 Content Manager cannot update an object` in the `Cognos.log` file (available in `%npsdatadir%\logs` on Windows, in `/var/opt/NNMPerformanceSPI/logs` on Linux), set the `procedure cache size` property to a higher value.
5. Run the following commands:

   stopCS.ovpl

   startCS.ovpl

Tuning the NPS Database

The NPS database stores the data used for building reports. The performance of the database depends on the database configuration, volume of data stored in the database, the number of scheduled reports and jobs, number of users trying to launch reports concurrently, and the underlying hardware.

In a very large scale environment, you can adjust the values of certain configuration parameters to resolve degrading performance. This chapter provides guidelines for adjusting the configuration parameters to address performance issues.

You can configure the `perfspi.cfg` file to modify the NPS database to use non-default values for the main and temporary cache of the database.

To change the default cache size, follow these steps:

1. Log on to the NPS system as root or administrator. In a distributed deployment of NPS, log on to the DB Server as root or administrator.
2. Go to the following directory:

   On Windows:

   ```
   %npsdatadir%\database
   ```

   On Linux:

   ```
   $NPSDataDir/database
   ```

3. Open the `perfspi.cfg` file with a text editor.
4. Specify the temporary cache size (in MB) against the `-iqtc` property.
5. Specify the main cache size (in MB) against the `-iqmc` property.
6. Save the file.
7. Run the following commands to restart the database:

a. **stopDB.ovpl**
b. **startDB.ovpl**

Log Files

NPS creates the following log files in the `logs` directory:

> **Note:** The `log` directory is located in:
>
> *On Windows*
>
> `%npsdatadir%\NNMPerformanceSPI`
>
> *On Linux*
>
> `/var/opt/OV/NNMPerformanceSPI/`

Log Files

File Name	Description
prspi.log	Contains all operational details of NPS.
perfspi.srv.log	Contains all operational details of the Sybase IQ database used by NPS. This file can grow up to 512 MB.
perfspi.iqmsg	Sybase IQ messages file. This file can grow up to 512 MB.
dbproxy.log	Records all database queries triggered by NPS.
perfspiUI.log	Log file created and updated by the Business Intelligence Server and content store.

Part IX: Using Certificate Authority

NPS 10.30 enables you to use certificates signed by a third-party certificate authority (CA). By using a third-party certificate authority, you can ensure secure communication between the NPS system and the browser used to access different parts of the NPS console.

To configure NPS to use a third-party CA:

1. Enable the HTTPS Mode
2. Generate the Third-Party CA Certificate
3. Import the Third-Party CA Certificate

Task 1: Enable the HTTPS Mode

If you select the HTTPS mode of communication while running the `nnmenableperfspi.ovpl` script on the NNMi management server, NPS starts running in the HTTPS mode after the installation is complete. In that case, you need not perform this task.

If did not select the HTTPS mode of communication while running the `nnmenableperfspi.ovpl` script, follow these steps:

> **Note:** In a distributed deployment of NPS, perform this task on the UiBi Server.

1. Log on to the NPS system as administrator or root.
2. Run the following command:
   - *On Windows:* **%ovinstalldir%\NNMPerformanceSPI\bin\configureWebAccess.ovpl -newport** *<port_number>* **-ssl**
   - *On Linux:* **/opt/OV/NNMPerformanceSPI/bin/configureWebAccess.ovpl -newport** *<port_number>* **-ssl**

   In this instance, *<port_number>* is the port on which you want to run the NPS Business Intelligence Server.
3. Restart the Business Intelligence Server by running the following commands:

   On Windows:

   a. **%ovinstalldir%\NNMPerformanceSPI\bin\stopBI.ovpl**
   b. **%ovinstalldir%\NNMPerformanceSPI\bin\startBI.ovpl**

   On Linux:

   a. **/opt/OV/NNMPerformanceSPI/bin/stopBI.ovpl**
   b. **/opt/OV/NNMPerformanceSPI/bin/startBI.ovpl**

Task 2: Generate the Third-Party CA Certificate

To generate the third-party CA certificate, follow these steps:

Note: In a distributed deployment of NPS, perform this task on the UiBi Server.

1. Log on to the NPS system as administrator or root.
2. Run the following command:
   - *On Windows:***%ovinstalldir%\NNMPerformanceSPI\bin\runBIConfigGUI.ovpl**
   - *On Linux:***/opt/OV/NNMPerformanceSPI/bin/runBIConfigGUI.ovpl**

   The HPE NNM iSPI Performance BI Configuration window opens.
3. In the Explorer pane, click **Security > Cryptography > Cognos**.
4. In the right pane, under the Signing Key Settings section, change the Signing key store password. Note down this new password.
5. In the right pane, under the Encryption Key Settings section, change the Encryption key store password. Note down this new password.
6. Close the HPE NNM iSPI Performance BI Configuration window.
7. Go to the following directory:
   - *On Windows:* **%ovinstalldir%\nonOV\conos\bi\configuration**
   - *On Linux:* **/opt/OV/nonOV/cognos/bi/configuration**
8. Take a backup of the following files and directories:
   - `cogstartup.xml`
   - `encryptkeypair/`
   - `signkeypair/`
9. Set the `JAVA_HOME` environment variable to the following directory:
   - *On Windows:* `%ovinstalldir%\nonOV\jdk\hpsw`
   - *On Linux:* `/opt/OV/nonOV/jdk/hpsw`
10. Go to the following directory:
    - *On Windows:* **%ovinstalldir%\nonOV\conos\bi\bin**
    - *On Linux:* **/opt/OV/nonOV/cognos/bi/bin**
11. Run the following commands:
    - *On Windows:*
      - **ThirdPartyCertificateTool.bat -c -s -d "CN=**<*NPS_FQDN*>**,O=**<*org name*>**,C=**<*Country*>**" -r signRequest.csr -D ../configuration/signkeypair -p** <*password_sign*>
      - **ThirdPartyCertificateTool.bat -c -e -d "CN=**<*NPS_FQDN*>**,O=**<*org name*>**,C=**<*Country*>**" -r encryptRequest.csr -D ../configuration/encryptkeypair -p** <*password_encrypt*>

- *On Linux:*
  - **./ThirdPartyCertificateTool.sh -c -s -d "CN=**<*NPS_FQDN*>**,O=**<*org name*>**,C=**<*Country*>**" -r signRequest.csr -D ../configuration/signkeypair -p** <*password_sign*>
  - **./ThirdPartyCertificateTool.sh -c -e -d "CN=**<*NPS_FQDN*>**,O=**<*org name*>**,C=**<*Country*>**" -r encryptRequest.csr -D ../configuration/encryptkeypair -p** <*password_encrypt*>

In this instance, <*password_sign*> is the password that you assigned in step 4; <*password_encrypt*> is the password that you assigned in step 5; <*NPS_FQDN*> is the fully qualified domain name of the NPS system.

The above commands create the `signRequest.csr` and `encryptRequest.csr` files. Use these `.csr` files to obtain corresponding `signRequest.cer` and `encryptRequest.cer` files and the root certificate (`ca.cer`) from the third-party signing authority.

Task 3: Import the Third-Party CA Certificate

To import the third-party CA certificate into the Business Intelligence Server of NPS, follow these steps:

Note: In a distributed deployment of NPS, perform this task on the UiBi Server.

1. Log on to the NPS system as administrator or root.
2. Go to the following directory:
   - *On Windows:***%ovinstalldir%\nonOV\conos\bi\bin**
   - *On Linux:***/opt/OV/nonOV/cognos/bi/bin**
3. Place the `signRequest.cer`, `encryptRequest.cer`, and `ca.cer` files (created in the previous task) in this directory.
4. Rename the `signRequest.cer`and `encryptRequest.cer` files to `signCertificate.cer` and `encryptCertificate.cer`.
5. Run the following commands:
   - *On Windows:*
     - **ThirdPartyCertificateTool.bat -i -s -r signCertificate.cer -D ../configuration/signkeypair -p** <*password_sign*> **-t ca.cer**
     - **ThirdPartyCertificateTool.bat -i -e -r encryptCertificate.cer -D ../configuration/encryptkeypair -p** <*password_encrypt*> **-t ca.cer**
     - **ThirdPartyCertificateTool.bat -i -T -r ca.cer -D ../configuration/signkeypair -p** <*password_ca*>
   - *On Linux:*
     - **./ThirdPartyCertificateTool.sh -i -s -r signCertificate.cer -D ../configuration/signkeypair -p** <*password_sign*> **-t ca.cer**
     - **./ThirdPartyCertificateTool.sh -i -e -r encryptCertificate.cer -D ../configuration/encryptkeypair -p** <*password_encrypt*> **-t ca.cer**
     - **./ThirdPartyCertificateTool.sh -i -T -r ca.cer -D ../configuration/signkeypair -p NoPassWordSet**

In this instance, <*password_sign*> is the password that you assigned in step 4; <*password_encrypt*> is the password that you assigned in step 5.

6. Go to the following directory:
   - *On Windows:* **%ovinstalldir%\nonOV\conos\bi\configuration**
   - *On Linux:* **/opt/OV/nonOV/cognos/bi/configuration**
7. Undo the `JAVA_HOME` variable configuration that was set in step 9.
8. Open the `cogstartup.xml` file with a text editor and make sure that the `crn:parameter` element contains the following content:

```
<crn:parameter name="thirdPartyCA">

 <crn:value xsi:type="xsd:boolean">true</crn:value>

</crn:parameter>
```

9. Restart the Business Intelligence Server by running the following commands:

   On Windows:

   a. **%ovinstalldir%\NNMPerformanceSPI\bin\stopBI.ovpl**
   b. **%ovinstalldir%\NNMPerformanceSPI\bin\startBI.ovpl**

   On Linux:

   a. **/opt/OV/NNMPerformanceSPI/bin/stopBI.ovpl**
   b. **/opt/OV/NNMPerformanceSPI/bin/startBI.ovpl**

Part X: Troubleshooting

- *Problem:* Installation of the Cross Domain Extension Pack fails in a distributed deployment of NPS. The following error message appears in the installation log file:

  ```
  WARN: Failed command system("<Install_Dir>/nonOV/perl/a/bin/perl" -I"<Install_
  Dir>/NNMPerformanceSPI/lib/perllibs/lib" "<Install_
  Dir>/NNMPerformanceSPI/bin/mkCrossDomainExtensionPack.ovpl"): 3
  ```

  *Solution:*Install the Cross Domain Extension Pack manually with the help of the following command:

  mkCrossDomainExtensionPack.ovpl.

  To double the temporary dbspace, follow these steps:

  a. Log on to the NPS system that has the DB Server role assigned.
  b. Run the following command:

     dbsize.ovpl -d IQ_SYSTEM_TEMP

- *Problem:* When you try to launch a report,the following error message appears in the reports pane of the NPS console:

  ```
  An error occurred while performing operation 'sqlScrollBulkFetch' status = '232'.
  ```

  Cause: If the temporary dbspace of the Sybase IQ database runs out of space, this error message appears.

  Solution: Increase the temporary dbspace.

  To double the temporary dbspace, follow these steps:

  a. Log on to the NPS system that has the DB Server role assigned.
  b. Run the following command:

     dbsize.ovpl -d IQ_SYSTEM_TEMP

- *Problem:* When you try to launch a report,the following error message appears in the reports pane of the NPS console:

  ```
  Unable to execute the request because there were no connections to the process
  available within the configured time limit.
  ```

  Cause: If the actual number of concurrent users exceeds the maximum number of users specified in the `perfspi.cfg` file, this error appears.

  Solution: Increase the maximum number of users in the `perfspi.cfg` file.

  Follow these steps:

  a. Log on to the NPS system that has the DB Server role assigned.
  b. Go to the following directory:

     On Windows

     ```
     %NPSDataDir%\NNMPerformanceSPI/database
     ```

     On Linux

     ```
     /var/opt/OV/NNMPerformanceSPI/database
     ```

c. Open the `perfspi.cfg` file with a text editor.

d. Change the value of the `-gm` parameter from 100 to 200.

e. Restart the database processes:

   i. **stopDB.ovpl**

   ii. **startDB.ovpl**

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Deployment Reference (Network Node Manager iSPI Performance for Metrics Software 10.30)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to network-management-doc-feedback@hpe.com.

We appreciate your feedback!