

HP Network Node Manager iSPI Performance for Traffic Software

for the Windows® and Linux operating systems

Software Version: 9.21

Deployment Guide



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2009-2013 Hewlett-Packard Development Company, L.P.

Trademark Notices

Acrobat® is a trademark of Adobe Systems Incorporated.

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

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

UNIX® is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

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

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

Acknowledgements

This product includes software developed by the Apache Software Foundation.

(<http://www.apache.org>)

Documentation Updates

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

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

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

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

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

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

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

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

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

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

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

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

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

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

To find more information about access levels, go to:

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

Contents

| | | |
|---|---|----|
| 1 | About This Guide | 7 |
| | Documentation Conventions | 8 |
| | Setting Environment Variables | 9 |
| 2 | Introduction to the NNM iSPI Performance for Traffic | 11 |
| | IP Flow Data and NNM iSPI Performance for Traffic | 11 |
| | Architecture | 11 |
| | Workflow of the NNM iSPI Performance for Traffic | 12 |
| 3 | Deploying the NNM iSPI Performance for Traffic | 13 |
| | Deploying in an Entry-Level Environment | 13 |
| | Deploying in a Small or Medium-Sized Environment | 14 |
| | Deploying in a Large Environment | 14 |
| 4 | Preparation | 17 |
| 5 | Managing Securities | 19 |
| | Enabling Single Sign-On for the NNM iSPI Performance for Traffic | 19 |
| | Configuring Access with Public Key Infrastructure Authentication | 22 |
| | Enabling Security | 25 |
| | Enabling Secure Communication between NNMi and the NNM iSPI Performance for Traffic | 25 |
| | Enabling Secure Communication between NPS and the NNM iSPI Performance for Traffic | 29 |
| 6 | Deploying the NNM iSPI Performance for Traffic in a High-Availability Cluster | 31 |
| | Supported HA Products | 31 |
| | Prerequisites to Configuring the NNM iSPI Performance for Traffic for HA | 31 |
| | HA Installation Environments | 32 |
| | Option 1: NNMi and the Master Collector in the Same HA Cluster | 32 |
| | Configuring an HA Cluster on a Set of Systems with NNMi and the Master Collector | 32 |
| | Installing the Master Collector in an Existing NNMi HA Cluster Environment | 36 |
| | Option 2: the Master Collector in a Standalone HA Cluster | 39 |
| | Unconfiguring NNM iSPI Performance for Traffic from an HA Cluster | 43 |
| | Patching NNM iSPI Performance for Traffic Master Collector in HA | 46 |
| | Prerequisites to Apply Master Collector Patch in HA | 46 |
| | Applying Master Collector Patch in HA | 46 |
| | Install Master Collector Patch on Passive Master Collector | 46 |
| | Install Master Collector Patch on Active Master Collector | 47 |
| | Reconfigure Passive Master Collectors in HA | 48 |
| | Uninstalling Master Collector Patch in HA | 50 |
| | Uninstall Master Collector Patch from Passive Master Collector | 50 |

| | |
|--|-----------|
| Uninstall Master Collector Patch from Active Master Collector | 51 |
| Reconfigure Passive Master Collectors in HA | 52 |
| Upgrading the NNM iSPI Performance for Traffic in an HA Cluster | 54 |
| Master Collector and NNMi in the Same HA Cluster | 54 |
| Master Collector in a Standalone HA Cluster | 56 |
| 7 Deploying NNM iSPI for Traffic in an Application Failover Environment | 59 |
| Licensing | 59 |
| Configuring the NNM iSPI Performance for Traffic in Application Failover | 60 |
| 8 Tuning the NNM iSPI Performance for Traffic | 63 |
| Tuning the Master Collector and Leaf Collector | 63 |
| Additional Tuning Parameters | 66 |
| Disabling Data Generation for the Interface Traffic Reports | 67 |
| Enabling Subnet Details on Traffic Reports | 69 |
| Data Collection for Reports for Top Destination Ports | 70 |
| Tuning the Retention Period | 72 |
| Enhancing NPS Performance | 73 |
| Tuning the ETL for NPS | 73 |
| Disk Usage Recommendations | 74 |
| 9 Maintaining the NNM iSPI Performance for Traffic | 75 |
| Backup and Restore Commands | 75 |
| Backing up Master Collector | 75 |
| Resetting Master Collector Database | 76 |
| Restoring Master Collector | 77 |
| Backing up Leaf Collector | 78 |
| Resetting Leaf Collector Database | 78 |
| Restoring Leaf Collector | 79 |
| Changing the Hostnames | 80 |
| Changing the NNMi Hostname | 80 |
| Changing the Master Collector Hostname | 83 |
| Changing the NPS Hostname | 86 |
| 10 NNM iSPI Performance for Traffic Logging | 89 |
| 11 Deploying NNM iSPI Performance for Traffic in Global Network Management Environment .. | 91 |
| Licensing | 91 |
| We appreciate your feedback! | 93 |

1 About This Guide

This guide contains a collection of information and best practices for deploying HP Network Node Manager i Software Smart Plug-in Performance for Traffic (NNM iSPI Performance for Traffic in the rest of the document). This guide is targeted to:

- NNM iSPI Performance for Traffic and Network Performance Server (NPS) system administrator
- Network engineer
- HP support
- Engineer with experience in deploying and managing traffic deployments in large installations

Documentation Conventions

The NNM iSPI Performance for Traffic documentation uses the following conventions:

Table 1 NNM iSPI Performance for Traffic Documentation Conventions

| Symbol | Description |
|---|---|
| <p><i>%TrafficInstallDir%</i> (For Windows)</p> <p><i>\$TrafficInstallDir</i> (For Linux)</p> | <p>The NNM iSPI Performance for Traffic install directory when Master Collector or Leaf Collector is not installed on the same system as NNMi.</p> <p><i>For Windows</i></p> <p><drive>\Program Files\HP\HP BTO Software</p> <p><i>For Linux</i></p> <p>/opt/OV</p> |
| <p><i>%TrafficDataDir%</i> (For Windows)</p> <p><i>\$TrafficDataDir</i> (For Linux)</p> | <p>The NNM iSPI Performance for Traffic data directory when Master Collector or Leaf Collector is not installed on the same system as NNMi.</p> <p><i>For Windows</i></p> <p><drive>\ProgramData\HP\HP BTO Software</p> <p><i>For Linux</i></p> <p>/var/opt/OV/</p> |
| <p><i>%NnmInstallDir%</i> (For Windows)</p> <p><i>\$NnmInstallDir</i> (For Linux)</p> | <p>The environment variable for the NNMi application directory. The NNM iSPI Performance for Traffic is installed in this directory when Master Collector or Leaf Collector is installed on the same system as NNMi. This variable is automatically created by the NNMi installer for Windows.</p> <p><i>For Windows</i></p> <p><drive>\Program Files\HP\HP BTO Software</p> <p><i>For Linux</i></p> <p>/opt/OV</p> |
| <p><i>%NnmDataDir%</i> (For Windows)</p> <p><i>\$NnmDataDir</i> (For Linux)</p> | <p>The environment variable for the NNMi data directory. The NNM iSPI Performance for Traffic is installed in this directory when Master Collector or Leaf Collector is installed on the same system as NNMi. This variable is automatically created by the NNMi installer for Windows.</p> <p><i>For Windows</i></p> <p><drive>\ProgramData\HP\HP BTO Software</p> <p><i>For Linux</i></p> <p>/var/opt/OV/</p> |

Setting Environment Variables

NNM iSPI Performance for Traffic administrators can run a script that sets up many environment variables for navigating to commonly accessed locations.

To set up available environment variables on the NNMi server, use a command similar to the following examples:

Windows: C:\Program Files\HP\HP BTO Software\bin\nnm.envvars.bat

UNIX/Linux: /opt/OV/bin/nnm.envvars.sh

To set up environment variables on the NNM iSPI Performance for Traffic Master Collector, use a command similar to the following examples:

Windows: C:\Program Files\HP\HP BTO
Software\traffic-master\bin\traffic-master.envvars.bat

UNIX/Linux: /opt/OV/traffic-master/bin/traffic-master.envvars.sh

To set up environment variables on the NNM iSPI Performance for Traffic Leaf Collector, use a command similar to the following examples:

Windows: C:\Program Files\HP\HP BTO
Software\traffic-leaf\bin\traffic-leaf.envvars.bat

UNIX/Linux: /opt/OV/traffic-leaf/bin/traffic-leaf.envvars.sh

2 Introduction to the NNM iSPI Performance for Traffic

The NNM iSPI Performance for Traffic enriches the data obtained from the IP flow records that are exported by the routers on the network. You can use the enriched data to understand and analyze network traffic patterns and trends in your environment.

You can use the IP flow data, which is processed and enriched by the NNM iSPI Performance for Traffic, to generate reports with the help of the Network Performance Server (NPS). The NNM iSPI Performance for Traffic enables you to export the data into the CSV format for use with other data analysis tools.

IP Flow Data and NNM iSPI Performance for Traffic

Network routers are capable of exporting IP flow data records. An IP flow record includes details like IP addresses of the source and destination devices/systems, port of the source and destination devices/systems, number of bytes of data transmitted, and so on.

The NNM iSPI Performance for Traffic collects and processes these IP flow records and presents you with an enriched set of details where the flow information is enhanced with the network topology information present in NNMi. In addition, you can filter the collected data with user-defined filters or you can associate the flow with user-defined applications.

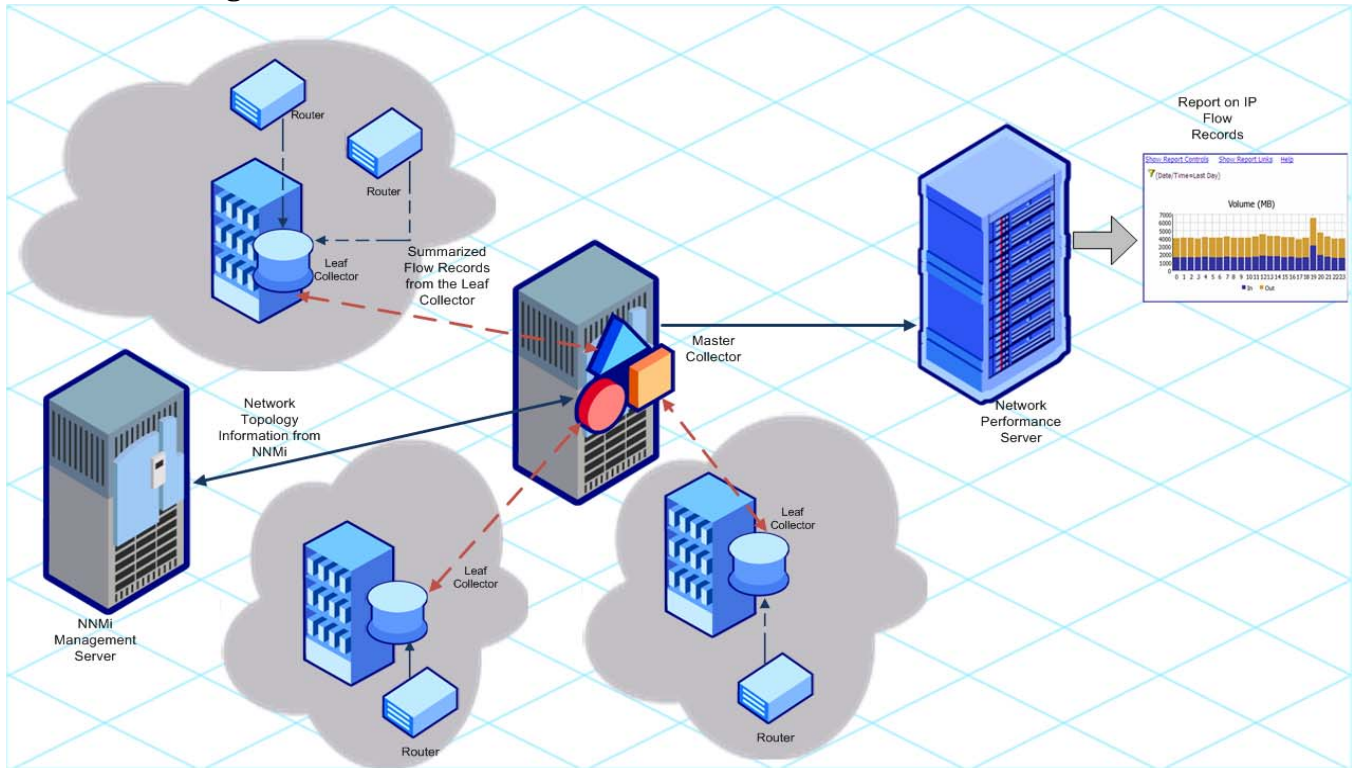
The NNM iSPI Performance for Traffic supports the following types of IP flows:

- NetFlow
 - NetFlow v5
 - NetFlow v9
- JFlow
- SFlow v5
- Internet Protocol Flow Information eXport (IPFIX)

Architecture

The NNM iSPI Performance for Traffic consists of two major components—the **Leaf Collector** and **Master Collector**. Leaf Collectors collect the IP flow records from different routers and forward the summarized data to the Master Collector. Master Collector processes the summarized data received from the Leaf Collectors and adds the topology context to the IP Flow records. The **HP NNMi Extension for iSPI Performance for Traffic**, which is installed on the NNMi management server, rules and definitions to generate reports from the data processed by the Master Collector.

Figure 1 Architecture of the NNM iSPI Performance for Traffic



Workflow of the NNM iSPI Performance for Traffic

- 1 The Leaf Collector collects the IP flow data from routers that are configured to export IP flow records.
- 2 The Leaf Collector forwards the collected data to the Master Collector.
- 3 The HP NNMi Extension for iSPI Performance for Traffic sends the network topology information to the Master Collector.
- 4 The Master Collector processes the data received from Leaf Collectors and adds the topology context to the collected data.
- 5 The Master Collector sends the processed data to NPS.
- 6 With the help of NPS, you can generate reports to analyze the network traffic.

3 Deploying the NNM iSPI Performance for Traffic

The *NNM iSPI Performance for Traffic Support Matrix* defines the following deployment environments for the NNM iSPI Performance for Traffic:

- Entry
- Small
- Medium
- Large

See the *NNM iSPI Performance for Traffic Support Matrix* to know more about the size of these environments. See the *NNM iSPI Performance for Traffic Installation Guide* for the installation information.

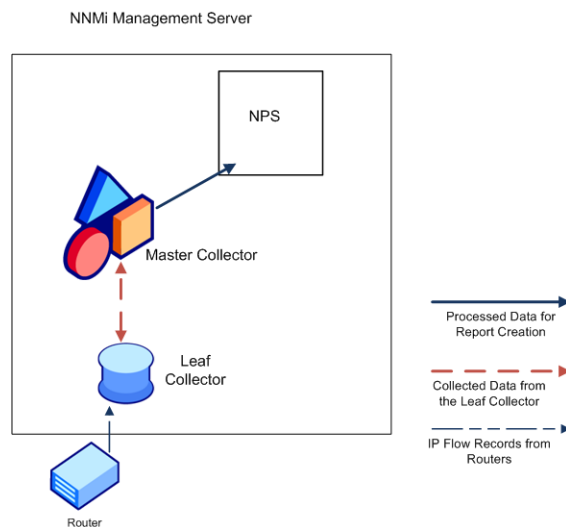
Deploying in an Entry-Level Environment

An entry-level environment is suitable for the evaluation purpose. If you want to create an environment to test and demonstrate different features of the iSPI, choose this type of deployment. Do not create a production setup in this environment.

In this deployment, you can install the Master Collector and Leaf Collector, along with the HP NNMi Extension for iSPI Performance for Traffic, on the NNMi management server. Only one Leaf Collector is used in this deployment.

In this environment, you can install NPS on the NNMi management server.

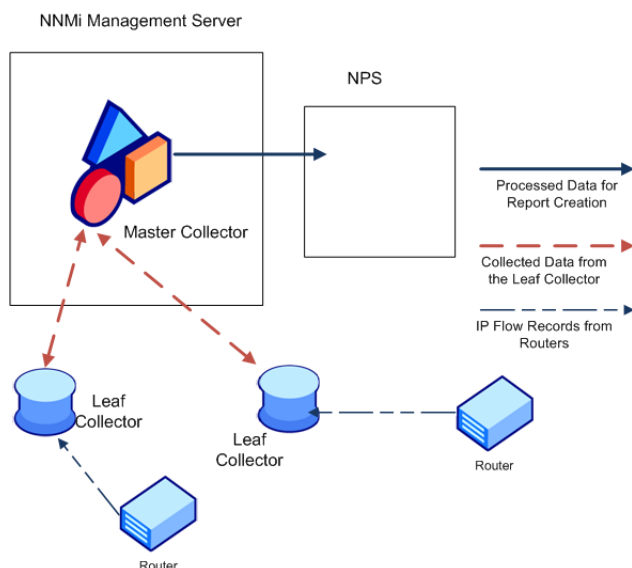
Figure 2 Entry-Level Deployment



Deploying in a Small or Medium-Sized Environment

In this deployment, you must install the Master and Leaf Collectors on different systems. You can choose to install the Master Collector on the NNMi management server and the Leaf Collector on the NPS system. See the *NNM iSPI Performance for Traffic Support Matrix* to determine the number of Leaf Collectors required for your environment.

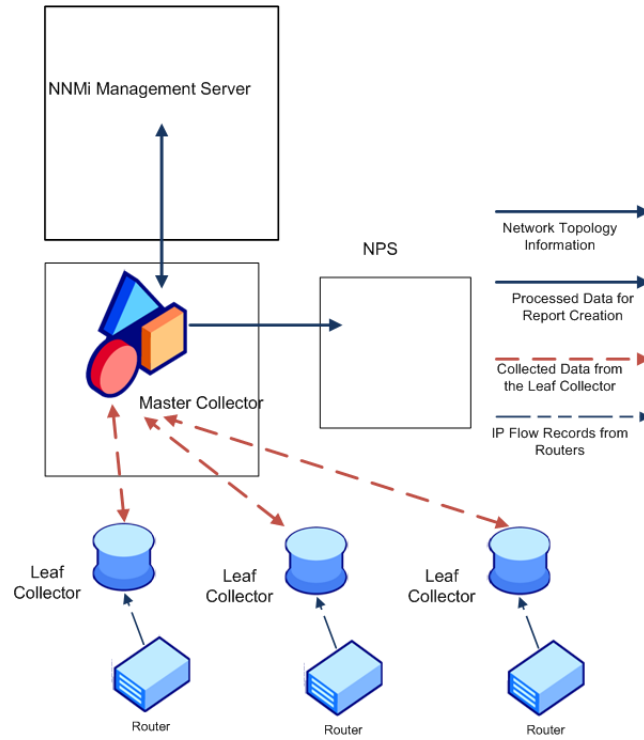
Figure 3 Small or Medium-Sized Deployment



Deploying in a Large Environment

This deployment type is suitable for large-scale production environments. This environment requires multiple instances of the Leaf Collectors. See the *NNM iSPI Performance for Traffic Support Matrix* to determine the number of Leaf Collectors required for your environment.

Figure 4 Large Deployment



4 Preparation

Before installing the NNM iSPI Performance for Traffic, read the information about system hardware and software requirements described in the following table:

Table 2 Software and hardware pre-installation checklist

| Document Type | Document Path |
|--|---|
| <i>HP Network Node Manager i Software Smart Plug-in Performance for Traffic Installation Guide</i> | Windows Media: DVD main drive (root) |
| | Linux Media: Root directory |
| | NNM iSPI Performance for Traffic console: Help > NNM iSPI Documentation Library > iSPI Performance for Traffic Install Guide |
| <i>HP Network Node Manager i Software Smart Plug-in Performance for Traffic Release Notes</i> | Windows Media: DVD main drive (root) |
| | Linux Media: Root directory |
| | NNM iSPI Performance for Traffic console: Help > NNM iSPI Documentation Library > iSPI Performance for Traffic Release Notes |
| <i>HP Network Node Manager i Software Smart Plug-in Performance for Traffic System and Device Support Matrix</i> | Windows Media: DVD main drive (root) |
| | UNIX Media: Root directory |
| | NNM iSPI Performance for Traffic console: Help > NNM iSPI Documentation Library > iSPI Performance for Traffic System and Device Support Matrix |

For current versions of all documents listed here, go to:

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

5 Managing Securities

The NNM iSPI Performance for Traffic enables you to configure single sign-on (SSO) to provide access to NNM iSPI Performance for Traffic Configuration form from the NNMi console while maintaining secured level of access as described in the [Enabling Single Sign-On for the NNM iSPI Performance for Traffic](#) on page 19.

You can also configure NNMi to map Public Key Infrastructure (PKI) certificates to NNMi user accounts. As a result, you can log on to the NNMi console without having to type in the NNMi user name and password on the Login page. However, you will be prompted to provide NNMi user name and password again when you try to launch the NNM iSPI Performance for Traffic Configuration form, unless you perform additional steps to reconcile the mapping with the iSPI as described in the [Configuring Access with Public Key Infrastructure Authentication](#) on page 22.



Do not enable the Single Sign-On feature when NNMi and the NNM iSPI Performance for Traffic are configured to use the Public Key Infrastructure (PKI) authentication.

You can configure the NNM iSPI Performance for Traffic to communicate securely with the NNMi management server and NPS. For more information, see [Enabling Security](#) on page 25.

Enabling Single Sign-On for the NNM iSPI Performance for Traffic

This section describes the steps required to enable single sign-on (SSO) for the NNM iSPI Performance for Traffic. With SSO, when you log on to the NNMi console, you can access the NNM iSPI Performance for Traffic Configuration form without providing the logon credentials again.

[Master Collector and NNMi Installed on the Same System](#)

If you have installed the Master Collector on the NNMi management server, follow these steps:

- 1 Log on to the Master Collector system as an administrator on Windows and as root on Linux.
- 2 Navigate to the following directory:
On Windows
`%NnmDataDir%\shared\nnm\conf\props`
On Linux
`/var/opt/OV/shared/nnm/conf/props`
- 3 Open the `nms-ui.properties` file with a text editor.
- 4 Specify the value of the following entry as `true` in the `nms-ui.properties` file:

```
com.hp.nms.ui.sso.isEnabled = true
```

- 5 Run the following command:

On Windows

```
%NnmInstallDir%\bin\nmssso.ovpl -reload
```

On Linux

```
/opt/OV/bin/nmssso.ovpl -reload
```

- 6 Run the following command:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterssoreload.ovpl
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterssoreload.ovpl
```

Master Collector and NNMi Installed on Separate Systems

If you have installed the Master Collector on a separate system (and not on the NNMi management server), follow these steps:

- 1 Log on to the NNMi management server as an administrator on Windows and as root on Linux.

- 2 Navigate to the following directory:

On Windows

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

On Linux

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

- 3 Open the `nms-ui.properties` file with a text editor.
- 4 Specify the value of the following entry as `true` in the `nms-ui.properties` file:

```
com.hp.nms.ui.sso.isEnabled = true
```

- 5 Run the following command:

On Windows

```
%NnmInstallDir%\bin\nmssso.ovpl -reload
```

On Linux

```
/opt/OV/bin/nmssso.ovpl -reload
```

- 6 *Windows Only:* Follow these steps:

- Make sure that the `com.hp.nms.ui.sso.initString` property in the `%NnmDataDir%\shared\nnm\conf\props\nms-ui.properties` file and the `initString` property in the `%NnmDataDir%\shared\nnm\conf\lwssofmconf.xml` file are set to the same value.
- Make sure that the `com.hp.nms.ui.sso.protectedDomains` property in the `%NnmDataDir%\shared\nnm\conf\props\nms-ui.properties` file and the `domain` element in the `%NnmDataDir%\shared\nnm\conf\lwssofmconf.xml` file are set to the same value.

- 7 *Linux Only:* Follow these steps:

- Make sure that the `com.hp.nms.ui.sso.initString` property in the `/var/opt/OV/shared/nnm/conf/props/nms-ui.properties` file and the `initString` property in the `/var/opt/OV/shared/nnm/conf/lwssofmconf.xml` file are set to the same value.
 - Make sure that the `com.hp.nms.ui.sso.protectedDomains` property in the `/var/opt/OV/shared/nnm/conf/props/nms-ui.properties` file and the domain element in the `/var/opt/OV/shared/nnm/conf/lwssofmconf.xml` file are set to the same value.
- 8 Log on to the Master Collector system as an administrator on Windows and as root on Linux.
 - 9 Stop the Master Collector by running the following command:
 - On Windows*
 - `%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl` or `%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl`
 - On Linux*
 - `/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl`
 - 10 Create the following directory structure on the Master Collector system:
 - On Windows*
 - `%TrafficDataDir%\shared\nnm\conf\props`
 - On Linux*
 - `/var/opt/OV/shared/nnm/conf/props`
 - 11 *Windows Only:* Follow these steps:
 - a Copy the following file from the `%NnmDataDir%\shared\nnm\conf` directory on the NNMi management server to the `%TrafficDataDir%\shared\nnm\conf` directory on the Master Collector system:
 - `lwssofmconf.xml`
 - b Copy the following file from the `%NnmDataDir%\shared\nnm\conf\props` directory on the NNMi management server to the `%TrafficDataDir%\shared\nnm\conf\props` directory on the Master Collector system:
 - `nms-ui.properties`
 - 12 *Linux Only:* Follow these steps:
 - a Copy the following file from the `/var/opt/OV/shared/nnm/conf` directory on the NNMi management server to the `/var/opt/OV/shared/nnm/conf` directory on the Master Collector system:
 - `lwssofmconf.xml`
 - b Copy the following file from the `/var/opt/OV/shared/nnm/conf/props` directory on the NNMi management server to the `/var/opt/OV/shared/nnm/conf/props` directory on the Master Collector system:
 - `nms-ui.properties`
 - 13 Navigate to the following directory:
 - On Windows*
 - `%TrafficDataDir%\shared\nnm\conf\props`

On Linux

`/var/opt/OV/shared/nm/conf/props`

- 14 Open the `nms-ui.properties` file with a text editor.
- 15 Specify the value of the following entry as `true` in the `nms-ui.properties` file on the Master Collector:

`com.hp.nms.ui.sso.isEnabled = true`

- 16 Start the Master Collector by running the following command:

On Windows

`%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl` or
`%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl`

On Linux

`/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl`

- 17 Run the following command on the Master Collector system:

On Windows

`%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterssoreload.ovpl`

On Linux

`/opt/OV/traffic-master/bin/nmstrafficmasterssoreload.ovpl`

- 18 Clear the browser cookies and log on to the NNMi console again with a new browser session and as a non-system user.
- 19 Launch the NNM iSPI Performance for Traffic Configuration form. With SSO enabled, you must be able to access the NNM iSPI Performance for Traffic Configuration form without providing logon credentials.

Configuring Access with Public Key Infrastructure Authentication

This section describes the steps required to configure the NNM iSPI Performance for Traffic to use the PKI authentication. With PKI authentication, you can access the NNM iSPI Performance for Traffic console without providing the logon credentials.



When NNMi is configured to use the PKI authentication, it is mandatory for the iSPI to use the PKI authentication. You must not configure only the iSPI to use the PKI authentication when NNMi continues to use the credentials-based authentication.

Configuring the iSPI to use the PKI authentication involves the following tasks:

- [Configuring NNMi](#) on page 23
- [Configuring a Certificate Validation Method](#) on page 23
- [Configuring the NNM iSPI Performance for Traffic](#) on page 23



If you configure the NNM iSPI Performance for Traffic to use the PKI authentication when the Master Collector is in HA cluster, you must perform the required configuration tasks on both, primary (active) and secondary (passive) servers. For more information, see [Deploying the NNM iSPI Performance for Traffic in a High-Availability Cluster](#).

Task 1: Configuring NNMi

To configure NNMi to use the PKI authentication, follow the steps in the *Configuring NNMi to Support Public Key Infrastructure Authentication* section in the *HP Network Node Manager Deployment Reference*.

After configuring NNMi to use the PKI authentication, if you do not perform [Task 3](#) on page 23, you will be prompted to provide NNMi user name and password when you try to launch the NNM iSPI Performance for Traffic Configuration form.

Task 2: Configuring a Certificate Validation Method

When NNMi is configured to use the PKI authentication, unauthorized access using invalid certificates must be prevented. You must perform additional steps to configure NNMi to use a certificate validation method—Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP).

Follow the steps in the *Certificate Validation (CRL and OCSP)* section in the *HP Network Node Manager Deployment Reference*.


Task 3: Configuring the NNM iSPI Performance for Traffic

Configuring NNMi to use the PKI authentication essentially requires updating the `nms-auth-config.xml` file, which is available in NNMi's configuration data directory (`%nnmdatadir%\nmsas\NNM\conf` on Windows; `/var/opt/OV/nmsas/NNM/conf` on UNIX/Linux). You must modify the `nms-auth-config.xml` file in the iSPI configuration data directory based on the updated `nms-auth-config.xml` file to enable the iSPI to use the PKI authentication.

Master Collector and NNMi Installed on the Same System

To configure the NNM iSPI Performance for Traffic to use the PKI authentication, follow these steps:

- 1 Make sure that [Task 1](#) and [Task 2](#) are complete.
- 2 Log on to the Master Collector system.
- 3 Navigate to the following directory:
On Windows
`%nnmdatadir%\nmsas\traffic-master\conf`
On Linux
`/var/opt/OV/nmsas/traffic-master/conf`
- 4 Open the `nms-auth-config.xml` file using a text editor.
- 5 Modify the `nms-auth-config.xml` file on the Master Collector to enable PKI authentication. For information on the required changes, see the *Configuring NNMi for PKI (X.509 Certificate Authentication)* section in the *HP Network Node Manager Deployment Reference*.

 Make sure that you modify the iSPI `nms-auth-config.xml` file to match the changes done to the `nms-auth-config.xml` file on the NNMi management server.

- 6 Save and close the file.
- 7 Run the following command on the Master Collector system:

On Windows

```
%NNMInstallDir%\traffic-master\bin\nmstrafficauthreload.ovpl
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficauthreload.ovpl
```

Master Collector and NNMi Installed on Separate Systems

To configure the NNM iSPI Performance for Traffic to use the PKI authentication, follow these steps:

- 1 Log on to the Master Collector system.
- 2 Navigate to the directory that contains the `nnm.truststore` files:

On Windows

```
%TrafficDataDir%\shared\nnm\certificates
```

On Linux

```
/var/opt/OV/shared/nnm/certificates
```

- 3 You must import your trusted CA certificate (entire chain if required) into the `nnm.truststore` file.

For example, the `mycompany_ca.cer` file contains the certificate you must use. Run the following command to import the CA certificate into the NNMi `nnm.truststore` file:

On Windows

```
%TrafficInstallDir%\nonOV\jdk\nnm\bin\keytool -importcert -noprompt  
-keystore "%TrafficDataDir%\shared\nnm\certificates\nnm.truststore"  
-file mycompany_ca.cer -storepass <password> -alias <aliasname>
```

On Linux

```
/opt/OV/nonOV/jdk/nnm/bin/keytool -importcert -noprompt -keystore "  
var/opt/OV/shared/nnm/certificates/nnm.truststore" -file  
mycompany_ca.cer -storepass <password> -alias <aliasname>
```

- 4 Make sure that [Task 1](#) and [Task 2](#) are complete.
- 5 Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-master\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-master/conf
```

- 6 Open the `nms-auth-config.xml` file using a text editor.
- 7 Modify the `nms-auth-config.xml` file on the Master Collector to enable PKI authentication. For information on the required changes, see the *Configuring NNMi for PKI (X.509 Certificate Authentication)* section in the *HP Network Node Manager Deployment Reference*.



Make sure that you modify the iSPI `nms-auth-config.xml` file to match the changes done to the `nms-auth-config.xml` file on the NNMi management server.

- 8 Save and close the file.
- 9 Run the following command on the Master Collector system:

On Windows

```
%TrafficInstallDir%\traffic-master\bin\nmstrafficauthreload.ovpl
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficauthreload.ovpl
```

Enabling Security

This section describes the steps required to enable security on the NNM iSPI Performance for Traffic. You can enable secure communication between the following:

- NNMi management server and the NNM iSPI Performance for Traffic
- NPS and the NNM iSPI Performance for Traffic

Enabling Secure Communication between NNMi and the NNM iSPI Performance for Traffic

Master Collector and NNMi Installed on the Same System

To enable secure communication between NNMi and the NNM iSPI Performance for Traffic when Master Collector is installed on the NNMi management server, follow these steps:

- 1 Log on to the Master Collector system.
- 2 Stop the Master Collector processes using the following command:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl
```

- 3 Navigate to the following directory:

On Windows

```
%NnmDataDir%\nmsas\traffic-master\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-master/conf
```


- 4 Open the `nnm.extended.properties` file with a text editor.
- 5 Set the value of the following properties to **true**:


- `com.hp.ov.nms.spi.traffic-master.spi.isSecure`
- `com.hp.ov.nms.spi.traffic-master.Nnm.isSecure`

➤ If you have enabled the `Is Secure` option when installing the NNM iSPI Performance for Traffic, you do not have to set the above properties.

➤ If the NNMi management server is configured for application failover, set the `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.isSecure` property to **true**.

- 6 Set the value of the following properties to **HTTPS**:
 - `com.hp.ov.nms.spi.traffic-master.spi.secureprotocol`
 - `com.hp.ov.nms.spi.traffic-master.Nnm.secureprotocol`

 If the NNMi management server is configured for application failover, set `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.secureprotocol` to **HTTPS**.
- 7 Set the value of the following properties to the HTTPS port number of the NNMi management server:
 - `com.hp.ov.nms.spi.traffic-master.Nnm.secureport`
 - `com.hp.ov.nms.spi.traffic-master.Nnm.https.port`

 If the NNMi management server is configured for application failover, set the value of the following properties to the HTTPS port number of the NNMi management server:

 - `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.secureport`
 - `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.https.port`
- 8 Navigate to the following directory:

On Windows

```
%NnmInstallDir%\traffic-master\server\conf
```

On Linux

```
/opt/OV/traffic-master/server/conf
```
- 9 Open the `login-config.xml` file using a text editor.
- 10 Search for the following string:


```
<application-policy name="nnm">
```
- 11 Locate the `<module-option name="nnmAuthUrl">http://<nnmhost>:<nnmport>/spilogin/auth</module-option>` property and change the following:
 - `http` to **https**
 - HTTP port number of the NNMi management server to the HTTPS port number of the NNMi management server
- 12 Save and close the file.
- 13 Restart the Master Collector processes using the following command:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

Master Collector and NNMi Installed on Separate Systems

To enable secure communication between NNMi and the NNM iSPI Performance for Traffic when Master Collector is not installed on the NNMi management server, follow these steps:

- 1 Log on to the Master Collector system.
- 2 Stop the Master Collector processes using the following command:

On Windows

```
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl
```

- 3 Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-master\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-master/conf
```

- 4 Open the `nmm.extended.properties` file with a text editor.

- 5 Set the value of the following properties to **true**:

- `com.hp.ov.nms.spi.traffic-master.spi.isSecure`
- `com.hp.ov.nms.spi.traffic-master.Nnm.isSecure`

➤ If you have enabled the **Is Secure** option when installing the NNM iSPI Performance for Traffic, you do not have to set the above properties.

➤ If the NNMi management server is configured for application failover, set the `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.isSecure` property to **true**.

- 6 Set the value of the following properties to **HTTPS**:

- `com.hp.ov.nms.spi.traffic-master.spi.secureprotocol`
- `com.hp.ov.nms.spi.traffic-master.Nnm.secureprotocol`

➤ If the NNMi management server is configured for application failover, set the `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.secureprotocol` to **HTTPS**.

- 7 Set the value of the following properties to HTTPS port number of the NNMi management server:

- `com.hp.ov.nms.spi.traffic-master.Nnm.secureport`
- `com.hp.ov.nms.spi.traffic-master.Nnm.https.port`

➤ If the NNMi management server is configured for application failover, set the value of the following properties to HTTPS port number of the NNMi management server:

- `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.secureport`
- `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.https.port`

- 8 Navigate to the following directory:

On Windows

```
%TrafficInstallDir%\traffic-master\server\conf
```

On Linux

```
/opt/OV/traffic-master/server/conf
```

- 9 Open the `login-config.xml` file using a text editor.

- 10 Search for the following string:

```
<application-policy name="nnm">
```

- 11 Locate the `<module-option name="nnmAuthUrl">http://<nnmhost>:<nnmport>/spillogin/auth</module-option>` property and change the following:

- `http` to `https`
- HTTP port number of the NNMi management server to the HTTPS port number of the NNMi management server

- 12 Save and close the file.

- 13 Log on to the NNMi management server.

- 14 Navigate to the following directory:

On Windows

```
%NNMDataDir%\shared\nnm\certificates
```

On Linux

```
/var/opt/OV/shared/nnm/certificates
```

- 15 Copy the `nnm.cert` file to a temporary directory on the Master Collector system.

► If `nnm.cert` file is not available in the `%NnmDataDir%\shared\nnm\certificates\` or `/var/opt/OV/shared/nnm/certificates` directory, follow these steps:

- 1 Run the following command to generate the `nnm.cert` file:

On Windows

```
%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool -export -file  
c:\temp\nnm.cert -keystore c:  
%NnmDataDir%\shared\nnm\certificates\nnm.keystore  
-alias<nnm FQDN>.selfsigned -storepass nnmkeypass
```

On Linux

```
/opt/OV/nonOV/jdk/nnm/bin/keytool -export -file c:/temp/  
nnm.cert - keystore c: /var/opt/OV/shared/nnm/certificates/  
nnm.keystore - alias<nnm_FQDN>.selfsigned -storepass  
nnmkeypass
```

For example,

```
C:\Program Files (x86)\HP\HP BTO Software\nonOV\jdk\b\bin>keytool  
- export -file c:\depot\nnm.cert -keystore c:\depot\nnm.keystore  
-alias 192.168.10.0.selfsigned -storepass nnmkeypass
```

- 2 Copy the `nnm.cert` file to a temporary directory on the Master Collector system.

- 16 Run the following command to add the certificate to the truststore:

On Windows

```
%TrafficInstallDir%\nonOV\jdk\nnm\bin\keytool -importcert -file  
"<tmp>/nnm.cert" -keystore "%TrafficDataDir%\shared\nnm/certificates/  
nnm.truststore" -storepass ovpass - noprompt -alias nnm
```

On Linux

```
/opt/OV/nonOV/jdk/nm/bin/keytool -importcert -file "<tmp>/nm.cert"
- keystore "/var/opt/OV/shared/nm/certificates/nm.truststore"
-storepass ovpass -noprompt -alias nm
```

- 17 Run the following command to verify that the certificates are added to the truststore:

On Windows

```
%TrafficInstallDir%\nonOV\jdk\nm\bin\keytool -list -keystore
"%TrafficDataDir%\shared\nm\certificates\nm.truststore"
```

On Linux

```
/opt/OV/nonOV/jdk/nm/bin/keytool -list -keystore "/var/opt/OV/
shared/nm/certificates/nm.truststore"
```

- 18 Restart the Master Collector processes using the following command:

On Windows

```
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficmasterstart.ovpl
```

Enabling Secure Communication between NPS and the NNM iSPI Performance for Traffic

To enable secure communication between the NPS and the NNM iSPI Performance for Traffic when NPS is running in secure mode, follow these steps:

- 1 Export the third-party Cognos certificate


To export the Cognos certificate using the browser keystore, follow these steps:

- a Log on to NPS directly, by pointing your browser at the following URL:

```
https://<fully_qualified_domain_name>:<nps_https_port>
```

In this instance, *<fully_qualified_domain_name>* is the fully qualified domain name of the NPS system and *<nps_https_port>* is the HTTPS port that NPS uses for secure communication. The default port that NPS uses for secure communication is 9305.

- b View the certificate and export it as a DER-encoded binary file. Name the file as **trafficcet.cer**.

 Ignore any warning message that you may see.

- c Copy the exported certificate to a temporary location on the Master Collector.

- 2 Import the third-party Cognos certificate to nm.truststore.

To import the certificate to the nm.truststore, follow these steps:

- a Stop the Master Collector processes using the following command:

On Windows

```
%NmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl
```

or

```
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl
```

If you have installed the Master Collector on the NNMi management server, you must stop the NNMi processes before importing the certificate into the `nnm.truststore` by running the `ovstop -c ovjboss` command.

- b Import the Cognos certificate into the `nnm.truststore` file.

For example, the `trafficcet.cer` file contains the certificate you must use. Run the following command to import the CA certificate into the `nnm.truststore` file:

On Windows


```
%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool -importcert -noprompt -  
keystore "%NnmDataDir%\shared\nnm\certificates\nnm.truststore"  
-file trafficcet.cer -storepass ovpass -alias cognos
```

or

```
%TrafficInstallDir%\nonOV\jdk\nnm\bin\keytool -importcert  
-noprompt - keystore  
"%TrafficDataDir%\shared\nnm\certificates\nnm.truststore" -file  
trafficcet.cer -storepass ovpass -alias cognos
```

On Linux

```
/opt/OV/nonOV/jdk/nnm/bin/keytool - importcert -noprompt -keystore  
"/var/opt/OV/shared/nnm/certificates/nnm.truststore" -file  
trafficcet.cer -storepass ovpass -alias cognos
```

-  Ignore any warning message that you may see.

The keytool used should be the Oracle implementation and not the GNU implementation.

If you have stopped NNMi processes in step a, you must start the NNMi processes after importing the certificate into the `nnm.truststore` by running the `ovstart -c ovjboss` command.

- c Start the Master Collector processes using the following command:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl
```

or

```
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl
```

6 Deploying the NNM iSPI Performance for Traffic in a High-Availability Cluster

You can install the NNM iSPI Performance for Traffic in a high availability (HA) environment to achieve redundancy in your monitoring setup. Since the NNM iSPI Performance for Traffic consists of multiple components that can be installed on different systems, you can choose the HA implementation of the NNM iSPI Performance for Traffic from multiple deployment scenarios.

Supported HA Products

The HP Network Node Manager iSPI Performance for Traffic Software-provided commands for configuring and running NNM iSPI Performance for Traffic under HA work with the following HA products for the designated operating systems:

- Veritas Cluster Server (VCS) version 5.0
- Veritas Cluster Server (VCS) version 5.1
- Microsoft Cluster Service for Windows 2008 and 2008 R2

While you can follow the procedures in this chapter to configure NNM iSPI Performance for Traffic to run under other HA products, HP does not provide support for cluster configuration issues for other configurations.

Prerequisites to Configuring the NNM iSPI Performance for Traffic for HA

Any system that you want to include as a node in an NNM iSPI Performance for Traffic HA cluster must meet the following requirements:

- Supports the use of a virtual IP address.
- Supports the use of a shared disk.
- Meets all requirements for NNM iSPI Performance for Traffic as described in the *HP Network Node Manager iSPI Performance for Traffic Software System and Device Support Matrix*.
- Meets all requirements described in the documentation for the HA product on which you plan to run NNM iSPI Performance for Traffic.
- Before you begin to configure the NNM iSPI Performance for Traffic for HA, use the commands for your HA product to configure and test an HA cluster. The HA cluster provides such functionality as checking the application heartbeat and initiating failover.

The HA cluster configuration must, at a minimum, include the following items:

- (Linux only) ssh
- (Linux only) remsh
- Virtual IP address for the HA cluster that is DNS-resolvable
- Virtual hostname for the HA cluster that is DNS-resolvable

HA Installation Environments

Among the three components of the NNM iSPI Performance for Traffic, you can install only the Master Collector under an HA cluster. In an environment where NNMi is installed in an HA cluster, you may choose to install the Master Collector in the same cluster or in a different cluster.

To install the Master Collector in an HA cluster, you can choose one of the following options:

- NNMi and the Master Collector in the same cluster
- Only the Master Collector in an HA cluster

If NNMi is installed in an HA cluster, you must install the HP NNMi Extension for iSPI Performance for Traffic on all NNMi management servers in the cluster.

Option 1: NNMi and the Master Collector in the Same HA Cluster

In this scenario, you can choose to install the Master Collector on the NNMi management server as an add-on product.



NPS may or may not be installed in an HA. However, make sure that NPS is not installed on the NNMi management server. NPS and the Master Collector cannot both exist as HA products in the same HA cluster at the same time.

Configuring an HA Cluster on a Set of Systems with NNMi and the Master Collector

If you have NNMi and the Master Collector installed on at least two systems, you can create an HA cluster and configure NNMi and the Master Collector to run under HA.

You can configure NNMi and Master Collector on the primary node and secondary node in an HA environment. For more information on how to install NNMi in an HA environment, see *NNMi Deployment Reference*.

Configuring the Master Collector on the primary node involves the following tasks:

Task 1: Installing NNMi and Master Collector


Install NNMi and Master Collector on each system. For more information, see the *NNMi Installation Guide* and the *NNM iSPI Performance for Traffic Installation* guide.

Task 2: Configuring NNMi to Run under HA

Configure the HA software on the systems and configure NNMi to run under HA. See the *NNMi Deployment Reference* for information on configuring NNMi to run under HA.

Task 3: Configuring the Master Collector on the Primary (active) node

Configure the Master Collector on the primary (active) node, follow these steps:

- 1 Run the following command to find the virtual hostname:
nnmofficialfqdn.ovpl
- 2 Modify the login-config.xml file from the %NnmInstallDir%\traffic-master\server\conf or /opt/OV/traffic-master/server/conf directory to reflect the virtual FQDN of the NNMi management server:
 - Open the login-config.xml file with a text editor.
 - Look for the element <module-option name="nnmAuthUrl">.
 - Modify the string contained within the element to reflect the virtual FQDN of the NNMi management server.
 - Save the file.
- 3 Go to the following directory:
On Windows
%NnmDataDir%\nmsas\traffic-master\conf
On Linux
/var/opt/OV/nmsas/traffic-master/conf
- 4 In the nnm.extended.properties file, set the com.hp.ov.nms.spi.traffic-master.Nnm.perfspidatapath property to the value that was displayed by the nnmenableperfspi.ovpl script.
 The nnmenableperfspi.ovpl script records all the details in the nnmenableperfspi_log.txt file (available in the %NnmDataDir%\log or /var/opt/OV/log directory) on the NNMi system, which you can use for your reference.


Default values are:

On Windows

%HA_MOUNT_POINT%\NNM\dataDir\shared\perfSpi\datafiles

On Linux

\$HA_MOUNT_POINT/NNM/dataDir/shared/perfSpi/datafiles

 Mount Point is the directory location for mounting the NNMi shared disk. This mount point must be consistent between systems. (That is, each node must use the same name for the mount point.) For example:

Windows: S:\

Make sure that you specify the drive completely. S and S: are unacceptable formats and do not provide access to the shared disk.

Linux: /nnmmount

- 5 Go to [step 9](#) on page 34 if you do not want to configure the NNM iSPI Performance for Traffic to use PKI authentication when Master Collector is in an HA cluster.

If you configure the NNM iSPI Performance for Traffic to use the PKI authentication when Master Collector is in an HA cluster, you must perform the required configuration changes on primary (active) server.

- For the Master Collector using HA configurations, if the change requires you to stop and restart the Master Collector system, you must put the active node in maintenance mode before running the `nmstrafficmasterstop.ovpl` and `nmstrafficmasterstart.ovpl` commands.

- 6 Navigate to the following directory:

On Windows

```
%nnmdatadir%\nmsas\traffic-master\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-master/conf
```

- 7 Open the `nms-auth-config.xml` file using a text editor.
- 8 Modify the `nms-auth-config.xml` file on the Master Collector to enable PKI authentication. For information on the required changes, see the *Configuring NNMi for PKI (X.509 Certificate Authentication)* section in the *HP Network Node Manager Deployment Reference*.

- Make sure that you modify the iSPI `nms-auth-config.xml` file to match the changes done to the `nms-auth-config.xml` file on the NNMi management server.

- 9 Run the following command to configure the Master Collector to run under the HA cluster:

For Windows

```
%NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon TRAFFIC
```

For Linux

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

Task 4: [Configuring the Master Collector on the Secondary \(passive\) node](#)

To configure the Master Collector on the secondary (passive) node, follow these steps:

- 1 Install NNMi with Master Collector on the secondary node. Make sure the secondary node has a separate Fully Qualified Domain Names (FQDN) during the installation. See the *NNMi Installation Guide* and the *HP Network Node Manager iSPI Performance for Traffic Software Installation* guide for more information.
- 2 Run the following command to find the virtual hostname:

```
nnmofficialfqdn.ovpl
```
- 3 Modify the `login-config.xml` file from the `%NnmInstallDir%\traffic-master\server\conf` or `/opt/OV/traffic-master/server/conf` directory to reflect the virtual FQDN of the NNMi management server:
 - Open the `login-config.xml` file with a text editor.
 - Look for the element `<module-option name="nnmAuthUrl">`.


- Modify the string contained within the element to reflect the virtual FQDN of the NNMi management server.
 - Save the file.
- 4 Go to the following directory:

On Windows

```
%NnmDataDir%\nmsas\traffic-master\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-master/conf
```
 - 5 In the `nnm.extended.properties` file, set the `com.hp.ov.nms.spi.traffic-master.Nnm.perfspidatapath` property to the value that was displayed by the `nnmenableperfspi.ovpl` script.


 The `nnmenableperfspi.ovpl` script records all the details in the `nnmenableperfspi_log.txt` file (available in the `%NnmDataDir%\log` or `/var/opt/OV/log` directory) on the NNMi system, which you can use for your reference.

Default values are:

On Windows: `%HA_MOUNT_POINT%\NNM\dataDir\shared\perfSpi\datafiles`

On Linux: `$HA_MOUNT_POINT/NNM/dataDir/shared/perfSpi/datafiles`
 - 6 Go to [step 10](#) on page 35 if you do not want to configure the NNM iSPI Performance for Traffic to use PKI authentication when Master Collector is in an HA cluster.

If you configure the NNM iSPI Performance for Traffic to use the PKI authentication when Master Collector is in an HA cluster, you must perform the required configuration changes on secondary (passive) server.


 For the Master Collector using HA configurations, if the change requires you to stop and restart the Master Collector system, you must put the passive node in maintenance mode before running the `nmstrafficmasterstop.ovpl` and `nmstrafficmasterstart.ovpl` commands.
 - 7 Navigate to the following directory:

On Windows

```
%nnmdatadir%\nmsas\traffic-master\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-master/conf
```
 - 8 Open the `nms-auth-config.xml` file using a text editor.
 - 9 Modify the `nms-auth-config.xml` file on the Master Collector to enable PKI authentication. For information on the required changes, see the *Configuring NNMi for PKI (X.509 Certificate Authentication)* section in the *HP Network Node Manager Deployment Reference*.

 Make sure that you modify the iSPI `nms-auth-config.xml` file to match the changes done to the `nms-auth-config.xml` file on the NNMi management server.
 - 10 Run the following commands to configure the Master Collector on the secondary node to run under the HA cluster:

For Windows

```
%NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon TRAFFIC
```

For Linux

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

Task 5: Configuring Each Passive Node in the HA Cluster

Repeat [Task 4](#) on each passive node in the HA cluster.

Installing the Master Collector in an Existing NNMi HA Cluster Environment

You can configure the Master Collector on the primary node and secondary node in an existing NNMi HA cluster environment. For more information on how to install NNMi in an HA environment, see *NNMi Deployment Reference* guide.

- 1 Install the HP NNMi Extension for iSPI Performance for Traffic on each server in the HA cluster. While installing the HP NNMi Extension for iSPI Performance for Traffic, specify the virtual FQDN of the NNMi server as the FQDN of the Master Collector system
- 2 Make sure that NNMi is running on the primary server.
- 3 Put the NNMi resource group to the HA maintenance mode by placing the maintenance file under the following directory:

On Windows

```
%NnmDataDir%\hacluster\<resource_group_name>
```

On UNIX/Linux

```
/var/opt/OV/hacluster/<resource_group_name>
```

- 4 Install the Master Collector on the primary (active) node in the cluster, but do *not* start the collector.
 - a Modify the login-config.xml file from the %NnmInstallDir%\traffic-master\server\conf or /opt/OV/traffic-master/server/conf directory to reflect the virtual FQDN of the NNMi management server:
 - Open the login-config.xml file with a text editor.
 - Look for the element <module-option name="nnmAuthUrl">.
 - Modify the string contained within the element to reflect the virtual FQDN of the NNMi management server.
 - Save the file.
 - b Go to the following directory:


On Windows

```
%NnmDataDir%\nmsas\traffic-master\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-master/conf
```

- c In the `nmn.extended.properties` file, set the `com.hp.ov.nms.spi.traffic-master.Nnm.perfspidatapath` property to the value that was displayed by the `nmnableperfspi.ovpl` script.


 The `nmnableperfspi.ovpl` script records all the details in the `nmnableperfspi_log.txt` file (available in the `%NnmDataDir%\log` or `/var/opt/OV/log` directory) on the NNMi system, which you can use for your reference.

Default values are:

- On Windows: `%HA_MOUNT_POINT%\NNM\dataDir\shared\perfSpi\datafiles`
- On Linux: `$HA_MOUNT_POINT/NNM/dataDir/shared/perfSpi/datafiles`

- d Go to [step 5](#) on page 37 if you do not want to configure the NNM iSPI Performance for Traffic to use PKI authentication when Master Collector is in an HA cluster.

If you configure the NNM iSPI Performance for Traffic to use the PKI authentication when Master Collector is in an HA cluster, you must perform the required configuration changes on primary (active) server.

 For the Master Collector using HA configurations, if the change requires you to stop and restart the Master Collector system, you must put the active node in maintenance mode before running the `nmstrafficmasterstop.ovpl` and `nmstrafficmasterstart.ovpl` commands.

- e Navigate to the following directory:


On Windows

`%nmmdatadir%\nmsas\traffic-master\conf`

On Linux

`/var/opt/OV/nmsas/traffic-master/conf`

- f Open the `nms-auth-config.xml` file using a text editor.
- g Modify the `nms-auth-config.xml` file on the Master Collector to enable PKI authentication. For information on the required changes, see the *Configuring NNMi for PKI (X.509 Certificate Authentication)* section in the *HP Network Node Manager Deployment Reference*.

 Make sure that you modify the iSPI `nms-auth-config.xml` file to match the changes done to the `nms-auth-config.xml` file on the NNMi management server.

- 5 Remove the maintenance file that you added in [step 3](#) on page 36.
- 6 Initiate a failover to a secondary (passive) node in the cluster where you want to install the Master Collector. Make sure that NNMi fails over and runs on the secondary server successfully.
- 7 On this system, follow these steps:
 - a Put the NNMi resource group to the HA maintenance mode by placing the maintenance file under the following directory:
`%NnmDataDir%\hacluster\<resource_group_name>`
`/var/opt/OV/hacluster/<resource_group_name>`
 - b Run `ovstatus -c` to make sure that `ovjboss` is running.


- c Install the Master Collector on this server, but do *not* start the collector.
- d Modify the `login-config.xml` file from the `%NnmInstallDir%\traffic-master\server\conf` or `/opt/OV/traffic-master/server/conf` directory to reflect the virtual FQDN of the NNMi management server:
 - Open the `login-config.xml` file with a text editor.
 - Look for the element `<module-option name="nnmAuthUrl">`.
 - Modify the string contained within the element to reflect the virtual FQDN of the NNMi management server.
 - Save the file.
- e Go to the following directory:

On Windows

```
%NnmDataDir%\nmsas\traffic-master\conf
```

On Linux


```
/var/opt/OV/nmsas/traffic-master/conf
```
- f In the `nnm.extended.properties` file, set the `com.hp.ov.nms.spi.traffic-master.Nnm.perfspidatapath` property to the value that was displayed by the `nnmenableperfspi.ovpl` script.

 The `nnmenableperfspi.ovpl` script records all the details in the `nnmenableperfspi_log.txt` file (available in the `%NnmDataDir%\log` or `/var/opt/OV/log` directory) on the NNMi system, which you can use for your reference.

Default values are:

 - On Windows: `%HA_MOUNT_POINT%\NNM\dataDir\shared\perfSpi\datafiles`
 - On Linux: `$HA_MOUNT_POINT/NNM/dataDir/shared/perfSpi/datafiles`
- g Go to [step k](#) on page 39 if you do not want to configure the NNM iSPI Performance for Traffic to use PKI authentication when Master Collector is in an HA cluster.

If you configure the NNM iSPI Performance for Traffic to use the PKI authentication when Master Collector is in an HA cluster, you must perform the required configuration changes on secondary (passive) server.

 For the Master Collector using HA configurations, if the change requires you to stop and restart the Master Collector system, you must put the passive node in maintenance mode before running the `nmstrafficmasterstop.ovpl` and `nmstrafficmasterstart.ovpl` commands.
- h Navigate to the following directory:

On Windows

```
%nnmdatadir%\nmsas\traffic-master\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-master/conf
```
- i Open the `nms-auth-config.xml` file using a text editor.

- j Modify the `nms-auth-config.xml` file on the Master Collector to enable PKI authentication. For information on the required changes, see the *Configuring NNMi for PKI (X.509 Certificate Authentication)* section in the *HP Network Node Manager Deployment Reference*.
- Make sure that you modify the iSPI `nms-auth-config.xml` file to match the changes done to the `nms-auth-config.xml` file on the NNMi management server.
- k Remove the maintenance file that you added in [step a](#) on page 37.
- 8 If you have multiple nodes in the cluster, fail over to another passive server, and then repeat [step a](#) on page 37 through [step k](#) on page 39.
- 9 Fail over to the server that was active when you started this procedure.
- 10 Run the following command on the active server first, and then on all passive servers:
For Windows

```
%NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon TRAFFIC
```

For Linux

```
/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon TRAFFIC
```
- 11 Verify that the Master Collector is successfully registered by running the following command:
On Windows

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

On Linux

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

Option 2: the Master Collector in a Standalone HA Cluster

In this scenario, NNMi may exist in an HA cluster, but not in the same cluster where the Master Collector is installed. NPS may or may not be installed in an HA. However, NPS and Master Collector cannot both exist as HA products in the same HA cluster at the same time.

- If you want to configure the NNM iSPI Performance for Traffic Master Collector to use PKI authentication when NNMi and the Master Collector already exist in two different HA clusters, you must follow [step 7](#) on page 40 to [step 14](#) on page 41 on both, primary (active) and secondary (passive) Master Collector servers. For more information to use PKI authentication, see [Configuring Access with Public Key Infrastructure Authentication](#) on page 22.

Installing the NNM iSPI Performance for Traffic in this environment involves the following tasks:

Task 1: Installing the HP NNMi Extension for iSPI Performance for Traffic

Install the HP NNMi Extension for iSPI Performance for Traffic on the NNMi management server. Make sure to specify the virtual FQDN of the Master Collector system during installation.

Task 2: Configuring the Primary (active) server

To configure the primary (active) server, follow these steps:

- 1 Make sure that requirements in [Prerequisites to Configuring the NNM iSPI Performance for Traffic for HA](#) on page 31 are met.
- 2 Note down the disk group and logical volume group name of the cluster.
- 3 Install NNM iSPI Performance for Traffic Master Collector, and then verify that the Master Collector is working correctly.
- 4 Stop the Master Collector:

```
nmstrafficmasterstop.ovpl
```

If NNM iSPI Performance for Traffic Master Collector is already installed on a node that you will include in this HA resource group, also run `nmstrafficmasterstop.ovpl` on that node at this time

- 5 Copy the NNM iSPI Performance for Traffic data disk to the shared disk:

On Windows, run the following command:

```
%TrafficInstallDir%\traffic-master\misc\nnm\ha\nnmhadisk.ovpl TRAFFIC  
-to <HA_mount_point>
```

On Linux, run the following command:

```
/opt/OV/misc/nnm/ha/nnmhadisk.ovpl TRAFFIC -to <HA_mount_point>
```

► To prevent database corruption, run this command (with the `-to` option) only one time.

- 6 Run the following command to configure the NNM iSPI Performance for Traffic HA resource group:

On Windows

```
%TrafficInstallDir%\traffic-master\misc\nnm\ha\nnmhaconfigure.ovpl  
TRAFFIC
```

On Linux

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

Specify the details specific to this cluster (and *not* the cluster where NNMi may exist) while answering the questions asked by the script (see *Table: NNMi HA Primary Node Configuration Information* in the *NNMi Deployment Reference*).

- 7 Go to [step 15](#) on page 41 if you do not want to configure the NNM iSPI Performance for Traffic to use PKI authentication when Master Collector is in a standalone HA cluster.

If you configure the NNM iSPI Performance for Traffic to use the PKI authentication when Master Collector is in a standalone HA cluster, you must perform the required configuration changes on both, primary (active) and secondary (passive) servers.

► When making file changes under HA, you must make the changes on both nodes in the cluster. For the Master Collector using HA configurations, if the change requires you to stop and restart the Master Collector system, you must put the active and passive nodes in maintenance mode before running the `nmstrafficmasterstop.ovpl` and `nmstrafficmasterstart.ovpl` commands.

- 8 Navigate to the directory that contains the `nnm.truststore` files:

On Windows

```
%TrafficDataDir%\shared\nnm\certificates
```

On Linux

```
/var/opt/OV/shared/nnm/certificates
```

- 9 You must import your trusted CA certificate (entire chain if required) into the `nnm.truststore` file.

For example, the `mycompany_ca.cer` file contains the certificate you must use. Run the following command to import the CA certificate into the NNMi `nnm.truststore` file:

On Windows

```
%TrafficInstallDir%\nonOV\jdk\nnm\bin\keytool -importcert -noprompt  
-keystore "%TrafficDataDir%\shared\nnm\certificates\nnm.truststore"  
-file mycompany_ca.cer -storepass <password> -alias <aliasname>
```

On Linux

```
/opt/OV/nonOV/jdk/nnm/bin/keytool -importcert -noprompt -keystore "  
var/opt/OV/shared/nnm/certificates/nnm.truststore" -file  
mycompany_ca.cer -storepass <password> -alias <aliasname>
```

- 10 Make sure that [Task 1](#) and [Task 2](#) listed under [Configuring Access with Public Key Infrastructure Authentication](#) on page 22 are complete.
- 11 Navigate to the following directory:

On Windows

```
%TrafficDataDir%\nmsas\traffic-master\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-master/conf
```

- 12 Open the `nms-auth-config.xml` file using a text editor.
- 13 Modify the `nms-auth-config.xml` file on the Master Collector to enable PKI authentication. For information on the required changes, see the *Configuring NNMi for PKI (X.509 Certificate Authentication)* section in the *HP Network Node Manager Deployment Reference*.



Make sure that you modify the `iSPI nms-auth-config.xml` file to match the changes done to the `nms-auth-config.xml` file on the NNMi management server.

- 14 Save and close the file.
- 15 Run the following command to start the NNM iSPI Performance for Traffic HA resource group.

On Windows

```
%TrafficInstallDir%\traffic-master\misc\nnm\ha\nnmhastartrg.ovpl  
TRAFFIC <resource_group>
```

On Linux:

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



Now that NNM iSPI Performance for Traffic is running under HA, do not use the `nmstrafficmasterstart.ovpl` and `nmstrafficmasterstart.ovpl` commands for the normal operation. Use these commands only for HA maintenance purposes.

Task 3: Configuring the Secondary (passive) server

To configure the secondary (passive) server, follow these steps:

- 1 Install the NNM iSPI Performance for Traffic Master Collector, and then verify that the NNM iSPI Performance for Traffic Master Collector is working correctly.

- 2 Stop the Master Collector:

```
nmstrafficmasterstop.ovpl
```

- 3 Run the following command to configure the NNM iSPI Performance for Traffic HA resource group:

On Windows

```
%TrafficInstallDir%\traffic-master\misc\nnm\ha\nnmhaconfigure.ovpl  
TRAFFIC
```

On Linux

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

- 4 Provide the same details that were provided during active node configuration.



When making file changes under HA, you must make the changes on both nodes in the cluster. For the Master Collector using HA configurations, if the change requires you to stop and restart the Master Collector system, you must put the passive node in maintenance mode before running the `nmstrafficmasterstop.ovpl` and `nmstrafficmasterstart.ovpl` commands.

- 5 Go to [step 13](#) on page 43 if you do not want to configure the NNM iSPI Performance for Traffic to use PKI authentication when Master Collector is in a standalone HA cluster.

If you configure the NNM iSPI Performance for Traffic to use the PKI authentication when Master Collector is in a standalone HA cluster, you must perform the required configuration changes on both, primary (active) and secondary (passive) servers.

- 6 Navigate to the directory that contains the `nnm.truststore` files:

On Windows

```
%TrafficDataDir%\shared\nnm\certificates
```

On Linux

```
/var/opt/OV/shared/nnm/certificates
```

- 7 You must import your trusted CA certificate (entire chain if required) into the `nnm.truststore` file.


For example, the `mycompany_ca.cer` file contains the certificate you must use. Run the following command to import the CA certificate into the NNMi `nnm.truststore` file:

On Windows

```
%TrafficInstallDir%\nonOV\jdk\nnm\bin\keytool -importcert -noprompt  
-keystore "%TrafficDataDir%\shared\nnm\certificates\nnm.truststore"  
-file mycompany_ca.cer -storepass <password> -alias <aliasname>
```

On Linux

```
/opt/OV/nonOV/jdk/nnm/bin/keytool -importcert -noprompt -keystore "  
var/opt/OV/shared/nnm/certificates/nnm.truststore" -file  
mycompany_ca.cer -storepass <password> -alias <aliasname>
```

- 8 Make sure that [Task 1](#) and [Task 2](#) listed under [Configuring Access with Public Key Infrastructure Authentication](#) on page 22 are complete.
- 9 Navigate to the following directory:
On Windows
`%TrafficDataDir%\nmsas\traffic-master\conf`
On Linux
`/var/opt/OV/nmsas/traffic-master/conf`
- 10 Open the `nms-auth-config.xml` file using a text editor.
- 11 Modify the `nms-auth-config.xml` file on the Master Collector to enable PKI authentication. For information on the required changes, see the *Configuring NNMi for PKI (X.509 Certificate Authentication)* section in the *HP Network Node Manager Deployment Reference*.
 Make sure that you modify the iSPI `nms-auth-config.xml` file to match the changes done to the `nms-auth-config.xml` file on the NNMi management server.
- 12 Save and close the file.
- 13 Run the following command to verify that the configuration was successful.
On Windows
`%TrafficInstallDir%\traffic-master\misc\nnm\ha\nnmhaclusterinfo.ovpl -group <resource_group> -nodes`
On UNIX/Linux
`/opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl -group <resource_group> -nodes`
The command output lists all configured nodes for the specified HA resource group.
- 14 Optionally, test the configuration by failing over to a passive node and failing back to the original node.

Unconfiguring NNM iSPI Performance for Traffic from an HA Cluster

The process of removing an NNM iSPI Performance for Traffic node from an HA cluster involves undoing the HA configuration for that instance of NNM iSPI Performance for Traffic Master Collector. You can then run that instance of NNM iSPI Performance for Traffic Master Collector as a standalone system or you can uninstall NNM iSPI Performance for Traffic Master Collector from that node.

If you want to keep NNM iSPI Performance for Traffic configured for high availability, the HA cluster must contain one node that is actively running NNM iSPI Performance for Traffic Master Collector and at least one passive NNM iSPI Performance for Traffic Master Collector node.

If you want to completely remove NNM iSPI Performance for Traffic Master Collector from the HA cluster, unconfigure the HA functionality on all nodes in the cluster.

To completely unconfigure NNM iSPI Performance for Traffic from an HA cluster, follow these steps:

- 1 Determine which node in the HA cluster is active. On any node, run the following command:

```
%NnmInstallDir%\traffic-master\misc\nnm\ha\nnmhaclusterinfo.ovpl
-group <resource_group> -activeNode or
%TrafficInstallDir%\traffic-master\misc\nnm\ha\nnmhaclusterinfo.ovpl
-group <resource_group> -activeNode

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

- 2 On each passive node, unconfigure NNMi from the HA cluster:

```
%NnmInstallDir%\traffic-master\misc\nnm\ha\nnmhaunconfigure.ovpl
TRAFFIC <resource_group> or
%TrafficInstallDir%\traffic-master\misc\nnm\ha\nnmhaunconfigure.ovpl
TRAFFIC <resource_group>

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

This command removes access to the shared disk but does not unconfigure the disk group or the volume group.

- 3 On each passive node, remove the resource group-specific files:

Delete all files in the following directory:

```
%NnmInstallDir%\traffic-master\hacluster\<resource_group>\ or
%TrafficInstallDir%\traffic-master\hacluster\<resource_group>\

/opt/OV/traffic-master/hacluster/<resource_group>
```

- 4 On the active node, disable HA resource group monitoring by creating the following maintenance file:

```
%NnmInstallDir%\traffic-master\hacluster\<resource-group>\maintenance
or
%TrafficInstallDir%\traffic-master\hacluster\<resource-group>\mainten
ance

/opt/OV/hacluster/<resource-group>/maintenance
```

The file can be empty.

- 5 Stop traffic Master Collector using the following command:

```
nmstrafficmasterstop.ovpl --HA
```

To prevent data corruption, make sure no instance of traffic Master Collector is running and accessing the shared disk.

- 6 Run the following command on the active node:

```
nnmhadisk.ovpl TRAFFIC -from <mount-point>
```

- 7 Remove all files from shared disk.

- 8 Delete the maintenance file.

```
del %NnmDataDir%\hacluster\<resource-group>\maintenance or del
%TrafficDataDir%\hacluster\<resource-group>\maintenance

rm -rf /opt/OV/hacluster/<resource-group>/maintenance
```

- 9 On the active node, stop the NNM iSPI Performance for Traffic Master Collector HA resource group:

```
%NnmInstallDir%\traffic-master\misc\nnm\ha\nnmhastoprg.ovpl TRAFFIC
<resource_group> or
%TrafficInstallDir%\traffic-master\misc\nnm\ha\nnmhastoprg.ovpl
TRAFFIC <resource_group>

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

This command does not remove access to the shared disk. Nor does it unconfigure the disk group or the volume group.

- 10 On the active node, unconfigure NNM iSPI Performance for Traffic from the HA cluster:

```
%NnmInstallDir%\traffic-master\misc\nnm\ha\nnmhaunconfigure.ovpl
TRAFFIC <resource_group> or
%TrafficInstallDir%\traffic-master\misc\nnm\ha\nnmhaunconfigure.ovpl
TRAFFIC <resource_group>

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

This command removes access to the shared disk but does not unconfigure the disk group or the volume group.

- 11 On the active node, remove the resource group-specific files:

Delete all files in the following directory:

```
%NnmDataDir%\nmsas\traffic-master\hacluster\<resource_group>\ or
%TrafficDataDir%\nmsas\traffic-master\hacluster\<resource_group>\

/var/opt/OV/hacluster/<resource_group>/
```

- 12 Unmount the shared disk.

- If you want to reconfigure the NNM iSPI Performance for Traffic HA cluster at some point, you can keep the disk in its current state.
- If you want to use the shared disk for another purpose, copy all data that you want to keep (as described in the next procedure), and then use the HA product commands to unconfigure the disk group and volume group.

- 13 After all the nodes are unconfigured from HA. Modify the following file and change the master host name from virtual IP to actual host name of the node:

```
%NnmDataDir%\shared\traffic-master\conf\nnm.extended.properties or
%TrafficDataDir%\shared\traffic-master\conf\nnm.extended.properties

/var/opt/OV/shared/traffic-master/conf/nnm.extended.properties
```

- 14 For add-on Master Collector change these two parameters:

- com.hp.ov.nms.spi.traffic-master.spi.hostname=<FQDN of the localhost>
- com.hp.ov.nms.spi.traffic-master.Nnm.hostname=<FQDN of the NNM server>

For standalone Master Collector change the following parameter:

- com.hp.ov.nms.spi.traffic-master.spi.hostname=<FQDN of the localhost>
- com.hp.ov.nms.spi.traffic-master.Nnm.hostname=<FQDN of the NNM server>

- 15 Start traffic Master Collector using the following command:

```
nmstrafficmasterstart.ovpl
```

Patching NNM iSPI Performance for Traffic Master Collector in HA

This section describes the steps required to install and uninstall NNM iSPI Performance for Traffic Master Collector Patch when Master Collector is configured in HA. The steps provided in this section are applicable to both options described in [HA Installation Environments](#) on page 32.

Prerequisites to Apply Master Collector Patch in HA

Make sure that the following prerequisites are met before you begin the Master Collector Patch installation process:

- You must upgrade NNMi, NNM iSPI Performance for Metrics, NNMi Extension for iSPI Performance for Traffic, and NNM iSPI Performance for Traffic Leaf Collector to latest available patch.
- Make sure that your primary Master Collector node is configured as the active node.
- You must install patch on each passive Master Collector (s) before installing the patch on active Master Collector.

Applying Master Collector Patch in HA

To install Master Collector Patch, follow the steps listed below in the same order:

- 1 [Install Master Collector Patch on Passive Master Collector](#) on page 46
- 2 [Install Master Collector Patch on Active Master Collector](#) on page 47
- 3 [Reconfigure Passive Master Collectors in HA](#) on page 48

Install Master Collector Patch on Passive Master Collector

To install Master Collector Patch on passive Master Collectors in HA, follow these steps:

- 1 Move the HA cluster in maintenance mode by creating the following files on each passive Master Collector:

On Windows

```
%NnmDataDir%\nmsas\traffic-master\hacluster\<resource_group>\maintenance or  
%TrafficDataDir%\nmsas\traffic-master\hacluster\<resource_group>\maintenance
```

```
%NnmDataDir%\nmsas\traffic-master\hacluster\<resource_group>\maint_NNM or  
%TrafficDataDir%\nmsas\traffic-master\hacluster\<resource_group>\maint_NNM
```

On Linux

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

- 2 Log on to each passive Master Collector as an administrator on Windows and as root on Linux.
- 3 Run the following command to remove the Master Collector temporarily from HA cluster:

On Windows

- NNMi and the Master Collector in the same cluster

```
%NnmInstallDir%\misc\nnm\ha\nnmhaunconfigure.ovpl NNM -addon
TRAFFIC
```

- ▶ When NNMi and the Master Collector are in the same cluster, make sure that the following command does not show a passive Master Collector in the list:

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

- Master Collector in a Standalone HA Cluster

```
%TrafficInstallDir%\misc\nnm\ha\nnmhaunconfigure.ovpl TRAFFIC
<resource_group>
```

- ▶ When Master Collector is installed in a standalone HA Cluster, make sure that the following command does not show a passive Master Collector in the list:

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

On Linux

- NNMi and the Master Collector in the same cluster

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

- ▶ When NNMi and the Master Collector are in the same cluster, make sure that the following command does not show passive Master Collector in the list:

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

- Master Collector in a Standalone HA Cluster

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

- ▶ When Master Collector is installed in a standalone HA Cluster, make sure that the following command does not show a passive Master Collector in the list:

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

- 4 Apply the Master Collector Patch as described in the patch text.



Do NOT reconfigure HA again on this passive Master Collector until the patch is installed on active Master Collector.

Install Master Collector Patch on Active Master Collector

To install Master Collector Patch on active Master Collector in HA, follow these steps:

- 1 Move the HA cluster in maintenance mode by creating the following files on active Master Collector:

On Windows

```
%NnmDataDir%\nmsas\traffic-master\hacluster\<resource_group>\maintenance or
%TrafficDataDir%\nmsas\traffic-master\hacluster\<resource_group>\maintenance

%NnmDataDir%\nmsas\traffic-master\hacluster\<resource_group>\maint_NNM or
%TrafficDataDir%\nmsas\traffic-master\hacluster\<resource_group>\maint_NNM
```

On Linux

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

- 2 Run the following command to stop the Master Collector process on active Master Collector:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl --HA or
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl --HA
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl --HA
```

- 3 Install the Master Collector Patch as described in the patch text.



Do NOT unconfigure HA on the active Master Collector.

- 4 Run the following command to start the Master Collector process on active Master Collector:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl --HA or
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl
--HA
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl --HA
```

Reconfigure Passive Master Collectors in HA

To reconfigure passive Master Collector in HA, follow these steps:

- 1 On each passive Master Collector, run the following command to reconfigure HA.

On Windows

- NNMi and the Master Collector in the same cluster

```
%NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon TRAFFIC
```



When NNMi and the Master Collector are in the same cluster, make sure that the following command shows a passive Master Collector in the list:

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

- Master Collector in a Standalone HA Cluster


```
%TrafficInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl TRAFFIC
```

- ▶ When Master Collector is installed in a standalone HA Cluster, make sure that the following command shows a passive Master Collector in the list:

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

For Linux

- NNMi and the Master Collector in the same cluster

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

- ▶ When NNMi and the Master Collector are in the same cluster, make sure that the following command shows passive Master Collector in the list:

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

- Master Collector in a Standalone HA Cluster

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

- ▶ When Master Collector is installed in a standalone HA Cluster, make sure that the following command shows a passive Master Collector in the list:

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

- 2 Delete the following files to remove the passive Master Collector (s) from the maintenance mode:

On Windows

```
%NnmDataDir%\nmsas\traffic-master\hacluster\<resource_group>\maintena  
nce or  
%TrafficDataDir%\nmsas\traffic-master\hacluster\<resource_group>\main  
tenance
```

```
%NnmDataDir%\nmsas\traffic-master\hacluster\<resource_group>\maint_NN  
M or  
%TrafficDataDir%\nmsas\traffic-master\hacluster\<resource_group>\main  
t_NNM
```

On Linux

```
/var/opt/OV/hacluster/<resource_group>/maintenance
```

```
/var/opt/OV/hacluster/<resource_group>/maint_NNM
```

- 3 Delete the following files to remove the active Master Collector from the maintenance mode:

On Windows

```
%NnmDataDir%\nmsas\traffic-master\hacluster\<resource_group>\maintena  
nce or  
%TrafficDataDir%\nmsas\traffic-master\hacluster\<resource_group>\main  
tenance
```

```
%NnmDataDir%\nmsas\traffic-master\hacluster\<resource_group>\maint_NN  
M or  
%TrafficDataDir%\nmsas\traffic-master\hacluster\<resource_group>\main  
t_NNM
```

On Linux

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

Uninstalling Master Collector Patch in HA

To uninstall Master Collector Patch, follow the steps listed below in the same order:

- [Uninstall Master Collector Patch from Passive Master Collector](#) on page 50
- [Uninstall Master Collector Patch from Active Master Collector](#) on page 51
- [Reconfigure Passive Master Collectors in HA](#) on page 52

Uninstall Master Collector Patch from Passive Master Collector

To uninstall Master Collector Patch from passive Master Collectors in HA, follow these steps:

- 1 Move the HA cluster in maintenance mode by creating the following files on each passive Master Collector:

On Windows

```
%NnmDataDir%\nmsas\traffic-master\hacluster\<resource_group>\mainten  
ance or  
%TrafficDataDir%\nmsas\traffic-master\hacluster\<resource_group>\main  
tenance  
  
%NnmDataDir%\nmsas\traffic-master\hacluster\<resource_group>\maint_NN  
M or  
%TrafficDataDir%\nmsas\traffic-master\hacluster\<resource_group>\main  
t_NNM
```

On Linux

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

- 2 Log on to each passive Master Collector as an administrator on Windows and as root on Linux.
- 3 Run the following command to remove the Master Collector temporarily from HA cluster:

On Windows

- NNMi and the Master Collector in the same cluster

```
%NnmInstallDir%\misc\nnm\ha\nnmhaunconfigure.ovpl NNM -addon  
TRAFFIC
```



When NNMi and the Master Collector are in the same cluster, make sure that the following command does not show a passive Master Collector in the list:

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

- Master Collector in a Standalone HA Cluster

```
%TrafficInstallDir%\misc\nnm\ha\nnmhaunconfigure.ovpl TRAFFIC  
<resource_group>
```

- When Master Collector is installed in a standalone HA Cluster, make sure that the following command does not show a passive Master Collector in the list:

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

On Linux

- NNMi and the Master Collector in the same cluster

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

- When NNMi and the Master Collector are in the same cluster, make sure that the following command does not show passive Master Collector in the list:

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

- Master Collector in a Standalone HA Cluster

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

- When Master Collector is installed in a standalone HA Cluster, make sure that the following command does not show a passive Master Collector in the list:

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

- 4 Uninstall the Master Collector Patch as described in the patch text.



Do NOT reconfigure HA again on this passive Master Collector until the patch is uninstalled successfully.

Uninstall Master Collector Patch from Active Master Collector

To uninstall Master Collector Patch from active Master Collector in HA, follow these steps:

- 1 Move the HA cluster in maintenance mode by creating the following files on active Master Collector:

On Windows

```
%NnmDataDir%\nmsas\traffic-master\hacluster\<resource_group>\mainten  
ance or  
%TrafficDataDir%\nmsas\traffic-master\hacluster\<resource_group>\main  
tenance  
  
%NnmDataDir%\nmsas\traffic-master\hacluster\<resource_group>\maint_NN  
M or  
%TrafficDataDir%\nmsas\traffic-master\hacluster\<resource_group>\main  
t_NNM
```

On Linux

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

- 2 Run the following command to stop the Master Collector process on active Master Collector:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl --HA or  
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl --HA
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl --HA
```

- 3 Uninstall the Master Collector Patch as described in the patch text.



Do NOT unconfigure HA on the active Master Collector.

- 4 Run the following command to start the Master Collector process on active Master Collector:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl --HA or  
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl  
--HA
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl --HA
```

Reconfigure Passive Master Collectors in HA

To reconfigure passive Master Collector in HA, follow these steps:

- 1 On each passive Master Collector, run the following command to reconfigure HA.

On Windows

- NNMi and the Master Collector in the same cluster

```
%NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon TRAFFIC
```



When NNMi and the Master Collector are in the same cluster, make sure that the following command shows a passive Master Collector in the list:

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

- Master Collector in a Standalone HA Cluster

```
%TrafficInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl TRAFFIC
```



When Master Collector is installed in a standalone HA Cluster, make sure that the following command shows a passive Master Collector in the list:

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

For Linux

- NNMi and the Master Collector in the same cluster

```
/opt/OV/misc/nnm/ha/nmhaconfigure.ovpl NNM -addon TRAFFIC
```



When NNMi and the Master Collector are in the same cluster, make sure that the following command shows passive Master Collector in the list:

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

— Master Collector in a Standalone HA Cluster

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



When Master Collector is installed in a standalone HA Cluster, make sure that the following command shows a passive Master Collector in the list:

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

- 2 Delete the following files to remove the passive Master Collector (s) from the maintenance mode:

On Windows

```
%NnmDataDir%\nmsas\traffic-master\hacluster\<resource_group>\mainten  
ance or  
%TrafficDataDir%\nmsas\traffic-master\hacluster\<resource_group>\main  
tenance  
  
%NnmDataDir%\nmsas\traffic-master\hacluster\<resource_group>\maint_NN  
M or  
%TrafficDataDir%\nmsas\traffic-master\hacluster\<resource_group>\main  
t_NNM
```

On Linux

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

- 3 Delete the following files to remove the active Master Collector from the maintenance mode:

On Windows

```
%NnmDataDir%\nmsas\traffic-master\hacluster\<resource_group>\mainten  
ance or  
%TrafficDataDir%\nmsas\traffic-master\hacluster\<resource_group>\main  
tenance  
  
%NnmDataDir%\nmsas\traffic-master\hacluster\<resource_group>\maint_NN  
M or  
%TrafficDataDir%\nmsas\traffic-master\hacluster\<resource_group>\main  
t_NNM
```


On Linux

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

Upgrading the NNM iSPI Performance for Traffic in an HA Cluster

Master Collector and NNMi in the Same HA Cluster

To upgrade the NNM iSPI Performance for Traffic in an environment where the Master Collector and NNMi exist in the same HA cluster, follow these steps:

- 1 On the primary (active) node, follow these steps:
 - a Put the NNMi resource group to the HA maintenance mode by placing the maintenance file under the following directory:
On Windows
`%NnmDataDir%\hacluster\<resource_group_name>`
On Linux
`/var/opt/OV/hacluster/<resource_group_name>`
 - b Make sure all processes are running.
 - c Upgrade NNMi to the version 9.21 or higher.
 - d Start NNMi by running the following command:
`ovstart -c ovjboss`
 - e Make sure NPS is already upgraded to the version 9.21 (Patch 1) at this time.
 - f Stop the ETL processes on the NPS system. To stop the ETL processes, run the following command:
On Windows
`%NnmInstallDir%\NNMPerformanceSPI\bin\stopETL.ovpl`
On Linux
`/opt/OV/NNMPerformanceSPI/bin/stopETL.ovpl`
 - g Back up the `perfspi.pm` file. The `perfspi.pm` file is available at the following location:
On Windows
`%NnmInstallDir%\nonOV\perl\bin\lib\5.8.8`
On Linux
`/opt/OV/nonOV/perl/bin/lib/5.8.8`
 - h Apply the QCCR1B109116 hotfix on the NPS system. Contact HP Support to obtain this hotfix.
 - i Stop the Master Collector:
`nmstrafficmasterstop.ovpl --HA`
 - j Upgrade the HP NNMi Extension for iSPI Performance for Traffic to the version 9.21.
 Make sure that the ETL processes on the NPS system are stopped.
 - k Restart the `ovjboss` process:

- **ovstop -c ovjboss**
 - **ovstart -c ovjboss**
- l Upgrade the Master Collector to the version 9.21.
- m Start the Master Collector:
 - nmstrafficmasterstart.ovpl --HA**
- 2 On the secondary (passive) node, follow these steps:
 - a Put the NNMi resource group to the HA maintenance mode by placing the maintenance file under the following directory:
 - On Windows*
 - `%NnmDataDir%\hacluster\<resource_group_name>`
 - On Linux*
 - `/var/opt/OV/hacluster/<resource_group_name>`
 - b Make sure all NNMi processes are running.
 - c Upgrade NNMi to the version 9.21.
 - d Upgrade the HP NNMi Extension for iSPI Performance for Traffic and Master Collector to the version 9.21.
- 3 Repeat [step 2](#) on all other passive nodes in the cluster.
- 4 Remove the maintenance file from all passive nodes in the cluster.
- 5 Remove the maintenance file from the active node.
- 6 Fail over to a passive node.
- 7 Run the following command on the node that is currently active:
 - On Windows*
 - `%NnmInstallDir%\support\nnmtwiddle.ovpl -host <NNMi hostname> -port 80 -u system -p <password> invoke com.hp.ov.nms.topo ervice=NetworkApplication setApplicationService traffic <master hostname> http 12080`
 - On Linux*
 - `/opt/OV/support/nnmtwiddle.ovpl -host <NNMi hostname> -port 80 -u system -p <password> invoke com.hp.ov.nms.topo ervice=NetworkApplication setApplicationService traffic <master hostname> http 12080`

In this instance, <NNMi hostname> is the physical hostname of NNMi and <master hostname> is the virtual hostname of the Master Collector; <password> is the password for the NNMi system user.
- 8 Repeat [step 6](#) and [step 7](#) for each passive node.
- 9 Failback to the node that was active in the beginning of this procedure.
- 10 Start the ETL processes on the NPS system. To start the ETL processes, run the following command:
 - On Windows*
 - `%NnmInstallDir%\NNMPerformanceSPI\bin\startETL.ovpl`
 - On Linux*

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

Master Collector in a Standalone HA Cluster

To upgrade the NNM iSPI Performance for Traffic in an environment where the Master Collector exists in an HA cluster, follow these steps:

- 1 Upgrade NNMi and NPS to the version 9.21.
- 2 *Only when the Master Collector is on Windows.* Follow these steps:
 - a Go to the following directory on the NNMi management server:
`%NnmInstallDir%\misc\nnm\ha`
 - b Copy the `nnmhamscs.vbs` file.
 - c Place the `nnmhamscs.vbs` file into the `%NnmInstallDir%\misc\nnm\ha` directory on all Master Collector systems in the HA cluster.
 - d Stop the resource group on the primary (active) node:

```
%TrafficInstallDir%\traffic-master\misc\nnm\ha\nnmhastoprg.ovpl  
TRAFFIC <resource_group>
```
 - e Copy the `nnmhamscs.vbs` file from the `%NnmInstallDir%\misc\nnm\ha` directory and place the copied file in the `%TrafficInstallDir%\traffic-master\hacluster\<resource_group>` directory as `hamscs.vbs`. on the active Master Collector system in the HA cluster.
 - f Open the `hamscs.vbs` file with a text editor.
 - g Search for the string "product_name" (include the " " characters) and replace it with the string TRAFFIC.
 - h Save the file.
 - i Copy the modified `hamscs.vbs` file into the `%TrafficInstallDir%\traffic-master\hacluster\<resource_group>` directory on all secondary (passive) Master Collector systems in the cluster.
 - j Start the resource group on the primary (active) node:

```
%TrafficInstallDir%\traffic-master\misc\nnm\ha\nnmhastartrg.ovpl  
TRAFFIC <resource_group>
```
- 3 On the primary (active) node, follow these steps:
 - a Put the Master Collector resource group to the HA maintenance mode by placing the maintenance file under the following directory:
On Windows
`%TrafficDataDir%\nmsas\traffic-master\hacluster\<resource_group_name>`
On Linux
`/var/opt/OV/hacluster/<resource_group_name>`
 - b Stop the Master Collector:

```
nmstrafficmasterstop.ovpl --HA
```
 - c Run the following command:

```
encrypttrafficpasswd.ovpl --nnmEncrypt=<web_service_password>
```


In this instance, *<web_service_password>* is the password of the web service user that you used while installing the HP NNMi Extension for iSPI Performance for Traffic.

- d Open `nnm.extended.properties` file with a text editor from the following location:

On Windows

`%NnmDataDir%\shared\traffic-master\conf`

On Linux

`/var/opt/OV/shared/traffic-master/conf`

- e Copy the value of the property
`com.hp.ov.nms.spi.traffic-master.Nnm.password`.

- f Paste this value against the property
`com.hp.ov.nms.spi.traffic-master.Nnm.password` in the
`nnm.extended.properties` file that is available in the following location:

On Windows

`%HA_MOUNT_POINT%\NNM\dataDir\shared\traffic-master\conf`

On Linux

`$HA_MOUNT_POINT/NNM/dataDir/shared/traffic-master/conf`

- g Upgrade the Master Collector to the version 9.21.

- h *Only on Windows.* Run the following command:

```
nmstrafficmastersetuser.ovpl [--domain=<domainname>]--username  
<username> --password <password>
```

In this instance, *<domainname>* is the Fully Qualified Domain Name of the Windows and *<username>* is the user that has the read/write access rights to the shared network directory.



Domain is a mandatory parameter if you are using a Windows domain account.

For more information, see the *Configuring a User for the Master Collector System* section in the *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*.

- i Start the Master Collector:

```
nmstrafficmasterstart.ovpl --HA
```

- 4 On the secondary (passive) node, follow these steps:

- a Put the Master Collector resource group to the HA maintenance mode by placing the maintenance file under the following directory:

On Windows

`%TrafficDataDir%\nmsas\traffic-master\hacluster\<resource_group_name>`

On Linux

`/var/opt/OV/hacluster/<resource_group_name>`

- b Upgrade the Master Collector to the version 9.21.

- c *Only on Windows.* Run the following command:

```
nmstrafficmaster setuser.ovpl [--domain=<domainname>] --username  
<username> --password <password>
```

In this instance, <domainname> is the Fully Qualified Domain Name of the Windows and <username> is the user that has the read/write access rights to the shared network directory.

► Domain is a mandatory parameter if you are using a Windows domain account.

For more information, see the *Configuring a User for the Master Collector System* section in the *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*.

- 5 Repeat [step 4](#) on all other passive nodes.
- 6 Delete the maintenance file from all passive nodes in the cluster.
- 7 Delete the maintenance file from the active node.
- 8 Optionally, test the configuration by failing over to a passive node and failing back to the original node.

7 Deploying NNM iSPI for Traffic in an Application Failover Environment

The NNM iSPI Performance for Traffic cannot be configured to support application failover. However, it can exist in an environment where NNMi is installed in an application failover environment. When NNMi is configured for application failover, the Master Collector tries to establish connection with the primary NNMi management server. When Master Collector is not able to connect to the primary NNMi management server, it tries to connect to the secondary NNMi management server using the credentials provided in the `nnm.extended.properties` file.

The following deployment configuration is supported:

- NNMi is installed in an application failover environment, as primary and secondary instances on two separate systems.
- The NNM iSPI Performance for Traffic Master and Leaf Collectors are installed on separate non-co-located systems.
- The HP NNMi Extension for iSPI Performance for Traffic must be installed on both the primary and secondary systems.
- The NNM iSPI Performance for Traffic licenses must be installed on both primary and secondary systems.
- The Master Collector must be configured on both primary and secondary systems to point to the following:
 - The NNMi instance (provide the physical hostname)
 - The network share drive where the NNM iSPI Performance for Metrics data files folder on the HA system is shared.

Licensing

When NNMi is in an Application Failover, you require one NNM iSPI Performance for Traffic production license (iSPI Points license) on the primary (active) NNMi management server and one NNM iSPI Performance for Traffic non-production license on the secondary (passive) NNMi management server.

If Master Collector and Leaf Collector are not located on the same system, you must also enable the Collector Connection Software LTU on the primary (production) and secondary (non-production) NNMi management servers. For more information, see the *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*.

Configuring the NNM iSPI Performance for Traffic in Application Failover

You can configure the NNMi for failover before installing the NNM iSPI Performance for Traffic or after installing the NNM iSPI Performance for Traffic by providing the details of primary and secondary NNMi management servers on the Master Collector system.

Scenario 1: The NNM iSPI Performance for Traffic is installed after the NNMi is configured for application failover

If you install the NNM iSPI Performance for Traffic after NNMi is configured for application failover, follow these steps:

- 1 Install the NNMi Extension for iSPI Performance for Traffic on both primary and secondary NNMi management server.

To install the NNMi Extension for iSPI Performance for Traffic on the secondary NNMi management server, you must use the Master Collector FQDN provided on the primary NNMi management server.
- 2 Install the Master Collector and provide the details for both the primary and secondary NNMi management servers.

► If you want to enable secure communication (HTTPS) between the Master Collector and the NNMi management server, see [Enabling Security](#) on page 25.

Scenario 2: The NNMi is configured for application failover after the NNMi and the NNM iSPI Performance for Traffic are installed

If you install the NNM iSPI Performance for Traffic before NNMi is configured for application failover, follow these steps after you configure the NNMi for application failover:

- 1 Install the NNMi Extension for iSPI Performance for Traffic on secondary NNMi management server.

To install the NNMi Extension for iSPI Performance for Traffic on the secondary NNMi management server, you must use the Master Collector FQDN provided on the primary NNMi management server.
- 2 Log on to the Master Collector system.
- 3 Run the following command to stop the Master Collector processes:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl or  
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl
```

- 4 Navigate to the following directory:

On Windows

```
%NnmDataDir%\nmsas\traffic-master\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-master/conf
```

- 5 Open the `nmn.extended.properties` file using a text editor.
- 6 Set the `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.hostname` property to the FQDN of the secondary NNMI management server.
- 7 Modify the following properties:
 - Set the `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.port` property to the HTTP port number of the Master Collector. The default HTTP port number is 12080.
 - Set the value of the `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.isSecure` property to value set in the `com.hp.ov.nms.spi.traffic-master.spi.isSecure` property.
 - Set the `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.present` property to **true**. Setting this property to true indicates that the NNMI management server is configured for application failover.
 - Set the value of the `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.protocol` property to the value set in the `com.hp.ov.nms.spi.traffic-master.Nnm.protocol` property.
- If you want to enable secure communication (HTTPS) between the Master Collector and the NNMI management server, see [Enabling Security](#) on page 25.
- Set the `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.username` property to the WS client username provided in the `com.hp.ov.nms.spi.traffic-master.Nnm.username` property. Make sure that you create a user (with same username and password) on secondary NNMI management server as created on primary NNMI management server.
- Set the `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.https.port` property to the HTTPS port number of the NNMI management server set in the `com.hp.ov.nms.spi.traffic-master.Nnm.https.port` property. The default HTTPS port number is 443.
- Set the `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.perfspidatapath` property to the data path shared folder on the secondary NNMI management server.
- Set the `com.hp.ov.nms.spi.traffic-master.Nnm.secondary.jndi.port` property to the JNDI port number of the NNMI management server set in the `com.hp.ov.nms.spi.traffic-master.Nnm.jndi.port` property. The default JNDI port number is 1099.
- 8 Save and close the file.
- 9 Run the following command to set the `com.hp.ov.nms.spi.trafficmaster.Nnm.secondary.password` property to the encrypted password that you entered in the `com.hp.ov.nms.spi.traffic-master.Nnm.password` property:

On Windows

```
%NnmInstallDir%\traffic-master\bin\encrypttrafficpassword.ovpl --
nnmEncrypt=<password string for ws user on secondary> --secondary or
%TrafficInstallDir%\traffic-master\bin\encrypttrafficpassword.ovpl --
nnmEncrypt=<password string for ws user on secondary> --secondary
```

On Linux

```
/opt/OV/traffic-master/bin/encrypttrafficpassword.ovpl
--nnmEncrypt=<password string for ws user on secondary> --secondary
```

- 10 Save and close the file.

- 11 Run the following command to start the Master Collector processes:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl or  
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl
```

8 Tuning the NNM iSPI Performance for Traffic

HP recommends that after installation, you configure the NNM iSPI Performance for Traffic to optimize its performance in small, medium, and large tier environment by tuning a set of parameters. HP also recommends that you configure the report data retention period for the flow data generated by Master Collector.

Tuning the Master Collector and Leaf Collector

The NNM iSPI Performance for Traffic provides you with a set of parameters that you can configure for the optimum performance of the iSPI in a large-scale environment. These tuning parameters are available in the following files:

- On the Master Collector system

On Windows

`%NnmDataDir%\nmsas\traffic-master\conf\nms-traffic-master.address.properties` or
`%TrafficDataDir%\nmsas\traffic-master\conf\nms-traffic-master.address.properties`

On Linux

`/var/opt/OV/nmsas/traffic-master/conf/
nms-traffic-master.address.properties`

- On the Leaf Collector system

On Windows

`%NnmDataDir%\nmsas\traffic-leaf\conf\nms-traffic-leaf.address.properties` or
`%TrafficDataDir%\nmsas\traffic-leaf\conf\nms-traffic-leaf.address.properties`

On Linux

`/var/opt/OV/nmsas/traffic-leaf/conf/
nms-traffic-leaf.address.properties`

The *NNM iSPI Performance for Traffic Support Matrix* defines the following types of environments:

- Entry
- Small
- Medium
- Large

The *NNM iSPI Performance for Traffic Support Matrix* also provides ideal values of tuning parameters for each type of environment. It is recommended that you tune those parameters according to the values provided in *Table 4* in *NNM iSPI Performance for Traffic Support Matrix*.

To configure the tuning parameters of the NNM iSPI Performance for Traffic after installation, follow these steps:



After installation, you must perform these steps.

- 1 Identify the type of your environment—entry, small, medium, or large (see *NNM iSPI Performance for Traffic Support Matrix*). To determine the rate of flow records in your network, run the `nmstrafficflowanalysistool.ovpl` command. For more information, see *Reference pages* for this tool.
- 2 Note down the recommended values for the tuning parameters from *Table 4* in *NNM iSPI Performance for Traffic Support Matrix*.
- 3 Follow these steps on each Leaf Collector system:

- a Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
- b Open the `nms-traffic-leaf.address.properties` file with a text editor.



HP recommends that you do not modify the following properties in the `nms-traffic-leaf.address.properties` file available on the Leaf Collector system:

- `Collector Name.flowrecord.pool.size`
- `Collector Name.topn.flowrecord.pool.size`

In this instance, *Collector Name* is the name of the Leaf Collector instance. The properties `Collector Name.flowrecord.pool.size` and `Collector Name.topn.flowrecord.pool.size` may be added after you install NNM iSPI Performance for Traffic 9.20 Patch 1 and the Leaf Collector starts receiving IP flow data from different routers.

- c Set the `datagram.pool.size` property to the value recommended for Datagram for your environment in *Table 4* in *NNM iSPI Performance for Traffic Support Matrix*.
- d Set the `flowrecord.pool.size` property to the value recommended for FlowRecord for your environment in *Table 4* in *NNM iSPI Performance for Traffic Support Matrix*. HP recommends that you set this property to the recommended value *only once*.



Increase in FlowRecord pool size requires additional memory. For every 100K increase in FlowRecord pool size, you must provide additional 200 MB memory. For example, if you increase FlowRecord pool size by 200K, you must add additional 400 MB to the Xmx value for Leaf Collector. For information on how to change the Xmx value, see [Modifying the JVM Parameters](#) on page 68.

- e Set the `topn.flowrecord.pool.size` property to the value recommended for TopN Flowrecord for your environment in *Table 4* in *NNM iSPI Performance for Traffic Support Matrix*. HP recommends that you set this property to the recommended value *only once*.



Increase in TopN FlowRecord pool size requires additional memory. For every 100K increase in TopN FlowRecord pool size, you must provide additional 200 MB memory. For example, if you increase TopN FlowRecord pool size by 500K, you must add additional 1 GB to the Xmx value for Leaf Collector. For information on how to change the Xmx value, see [Modifying the JVM Parameters](#) on page 68.

f Save and close the file.

g Restart the Leaf Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl or  
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

► During the operation, the NNM iSPI Performance for Traffic automatically updates the values of these parameters. With every automatic update of tuning parameters, the NNM iSPI Performance for Traffic creates a new entry in the Flow Processing Status view in the NNMi console.

4 Follow these steps on the Master Collector system:

a Log on to the Master Collector system as an administrator on Windows and as root on Linux.

b Open the `nms-traffic-master.address.properties` file with a text editor.

c Set the `nms.traffic-master.maxflowrecord.inqueue` property to the value recommended for Master Queue Size for your environment in *Table 4* in *NNM iSPI Performance for Traffic Support Matrix*.

d Save and close the file.

e Restart the Master Collector by running the following command:

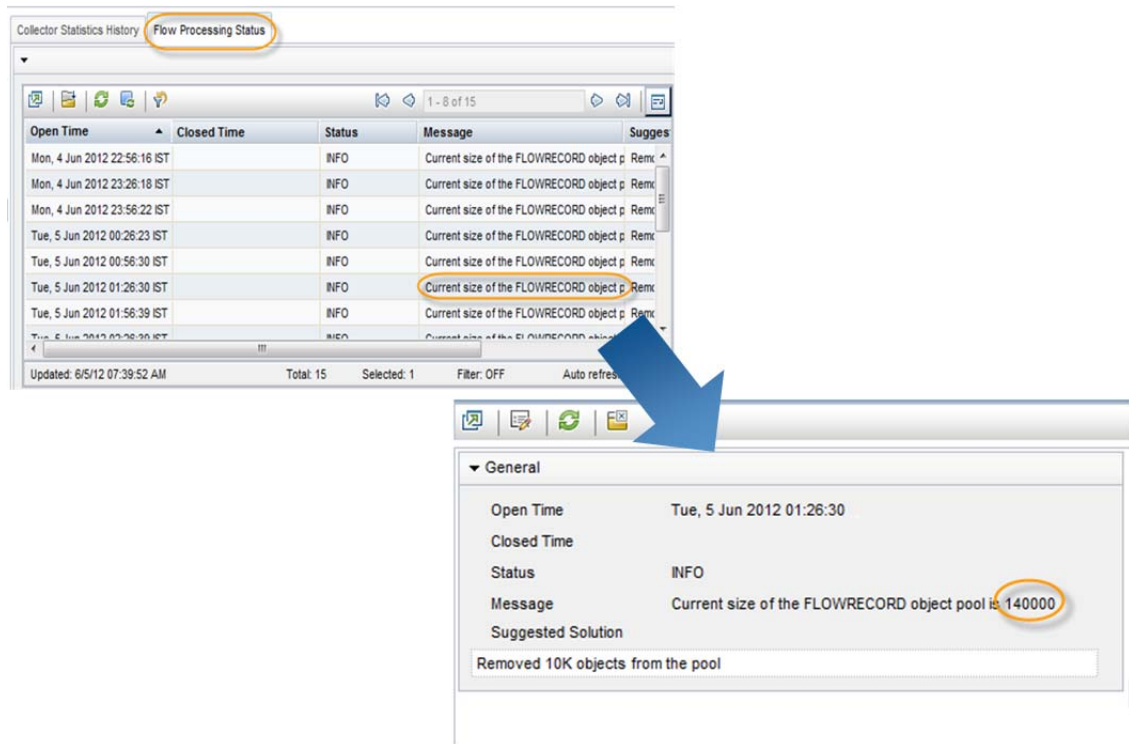
On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl or  
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl
```

Figure 5 Flow Processing Status View Showing Automatic Update of Tuning Parameters



Additional Tuning Parameters

The NNM iSPI Performance for Traffic is unable to write files on the NNMi system when sufficient disk space is not available or there are large number of pending files for each type of report to be written to the NNMi system.



NNM iSPI Performance for Traffic writes files to the NNMi system in the `%NnmDataDir%\shared\perfSpi\datafiles` directory on Windows and `/var/opt/OV/shared/perfSpi/datafiles` directory on Linux.

To ensure that NNM iSPI Performance for Traffic writes files successfully to the NNMi system, NNM iSPI Performance for Traffic detects the amount of disk space available on the NNMi system and number of pending files of each type to be written to the NNMi system. Before writing files to the NNMi system, NNM iSPI Performance for Traffic reads these values from the Master Collector configuration. By default, minimum amount of disk space required on the NNMi system for Master Collector to write files to the NNMi system is 1 GB and maximum number of pending files of each type that can be queued when writing files to the NNMi system is 100.

To modify the default values set in NNM iSPI Performance for Traffic to detect these values, follow these steps on the Master Collector system:

- 1 Log on to the Master Collector system as an administrator on Windows and as root on Linux.
- 2 Stop the Master Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl or  
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl
```

- 3 Open the `nms-traffic-master.address.properties` file with a text editor.
- 4 Set the following properties depending on your requirements:
 - a `nmm.shared.drive.size`: Defines the minimum amount of disk space required on the NNMi system for Master Collector to write files to the NNMi system.
 - b `nps.max.pending.files`: Defines the maximum number of pending files of each type that can be queued when writing files to the NNMi system.

- 5 Save the file.

- 6 Start the Master Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl or  
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl
```



On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl
```

Disabling Data Generation for the Interface Traffic Reports

When the NNM iSPI Performance for Traffic is configured in large-scale environment, you must disable the data generation for the Interface Traffic reports for optimum performance.

To disable the data generation for the Interface Traffic reports, follow these steps:

- 1 Log on to the NNM iSPI Performance for Traffic Configuration form.
- 2 Click **Master Collector**. The Master Collector Details page opens.
- 3 Locate the Interface Traffic Data Flush parameter and click  **Edit**.
- 4 Set the Value field for the Interface Traffic Data Flush parameter to Disable Flush.
- 5 Click  **Save**.
- 6 Start the Leaf Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl or  
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

- 7 Start the Master Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl or  
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl
```

8 Modifying the JVM Parameters

You can modify the JVM parameters for the Master and Leaf Collector to change the Initial Java Heap size (`-Xms`) and the Maximum Java Heap size (`-Xmx`).

To change the Initial Java Heap size (`-Xms`) and the Maximum Java Heap size (`-Xmx`) for Master Collector, follow these steps:

- 1 Log on to the Master Collector system as an administrator on Windows and as root on Linux.
- 2 Stop the Master Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl or  
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl
```

- 3 Navigate to the following directory:

On Windows

```
%NnmDataDir%\nmsas\traffic-master\conf
```

or

```
%TrafficDataDir%\nmsas\traffic-master\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-master/conf
```

- 4 Open the `nms-traffic-master.jvm.properties` file using a text editor.
- 5 Set the `-Xms` property to the value recommended for the Initial Java Heap size (`-Xms`) for your environment in *Table 1* in *NNM iSPI Performance for Traffic Support Matrix*. By default, Initial Java Heap size is set to 128 MB.
- 6 Set the `-Xmx` property to the value recommended for the Maximum Java Heap size (`-Xmx`) for your environment in *Table 1* in *NNM iSPI Performance for Traffic Support Matrix*. By default, Maximum Java Heap size is set to 4096 MB.
- 7 Save and close the file.
- 8 Start the Master Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl or  
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl
```

To change the Initial Java Heap size (`-Xms`) and the Maximum Java Heap size (`-Xmx`) for Leaf Collector, follow these steps:

- 1 Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
- 2 Stop the Leaf Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl or  
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

- 3 Navigate to the following directory:

On Windows

```
%NnmDataDir%\nmsas\traffic-leaf\conf
```

or

```
%TrafficDataDir%\nmsas\traffic-leaf\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-leaf/conf
```

- 4 Open the `nms-traffic-leaf.jvm.properties` file using a text editor.
- 5 Set the `-Xms` property to the recommended value for the Initial Java Heap size (`-Xms`) for your environment in *Table 2* in *NNM iSPI Performance for Traffic Support Matrix*. By default, Initial Java Heap size is set to 128 MB.
- 6 Set the `-Xmx` property to the recommended value for the Maximum Java Heap size (`-Xmx`) for your environment in *Table 2* in *NNM iSPI Performance for Traffic Support Matrix*. By default, Maximum Java Heap size is set to 4096 MB.
- 7 Save and close the file.
- 8 Start the Leaf Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl or  
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

Enabling Subnet Details on Traffic Reports

The NNM iSPI Performance for Traffic enables you to view Source Subnet Address and Destination Subnet Address in the Traffic reports. However, these subnet details are not visible on the Traffic reports by default. You must perform additional configuration steps to be able to view subnet details on the NNM iSPI Performance for Traffic reports. Enabling the subnet details may increase the load on the NNM iSPI Performance for Traffic and NPS. Therefore, you may require additional system resources, such as CPU, memory, and disk space.

Subnet details are available in the Report Options in the **Grouping By** list on the following reports:

- Interface Traffic reports: Most Changed, Top N, Top N Chart, and Top N Table
- Interface Traffic 15-minute and Interface Traffic 1-minute reports: Top Interfaces reports for Top N Analysis, Top N Chart Analysis, and Top N Table Analysis

When the subnet details are disabled, the Source Subnet Address and Destination Subnet Address options are available in the **Grouping By** list. However, the subnet address is shown on the report as 0.0.0.0/0.

To view subnet details in the Traffic reports, follow these steps on Leaf Collector system:

- 1 Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
- 2 Stop the Leaf Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl or  
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

- 3 Open the `nms-traffic-leaf.address.properties` file with a text editor.
- 4 Add the `enable.subnet.report` property and set it to `true`.
- 5 Save and close the file.
- 6 Start the Leaf Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl or  
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

Data Collection for Reports for Top Destination Ports

Data collection for the following 15-min and 1-min reports is disabled by default:

- Interface Traffic_15_min Top Sources for Destination Port
- Interface Traffic_15_min Top Destinations for Destination Port
- Interface Traffic_15_min Top Conversations for Destination Port
- Interface Traffic_1_min Top Sources for Destination Port
- Interface Traffic_1_min Top Destinations for Destination Port
- Interface Traffic_1_min Top Conversations for Destination Port



Enabling these reports may increase the load on the NNM iSPI Performance for Traffic and NPS. Therefore, you may require additional system resources, such as CPU, memory, and disk space.

To enable data collection for these reports:

- 1 Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
- 2 Stop the Leaf Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl or  
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

`/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl`

- 3 Navigate to the following directory:

On Windows

`%NNMDataDir%\nmsas\traffic-leaf\conf` or

`%TrafficDataDir%\nmsas\traffic-leaf\conf`

On Linux

`/var/opt/OV/nmsas/traffic-leaf/conf`

- 4 Open the `nms-traffic-leaf.address.properties` file with a text editor.
- 5 Add the following line of code:

`topn.subtypes.dstport=true`

- 6 Save and close the `nms-traffic-leaf.address.properties` file.
- 7 Start the Leaf Collector by running the following command:

On Windows

`%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl` or

`%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl`

On Linux

`/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl`

To disable data collection for these reports:

- 1 Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
- 2 Stop the Leaf Collector by running the following command:

On Windows

`%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl` or

`%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl`

On Linux

`/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl`

- 3 Navigate to the following directory:

On Windows

`%NNMDataDir%\nmsas\traffic-leaf\conf` or

`%TrafficDataDir%\nmsas\traffic-leaf\conf`

On Linux

`/var/opt/OV/nmsas/traffic-leaf/conf`

- 4 Open the `nms-traffic-leaf.address.properties` file with a text editor.
- 5 Do one of the following:

— Remove the following line of code:

`topn.subtypes.dstport=true`

— Set the property `topn.subtypes.dstport` to **false**.

- 6 Save and close the `nms-traffic-leaf.address.properties` file.

- 7 Start the Leaf Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl or  
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

Tuning the Retention Period

The retention period is the time for which the detailed and summarized data generated by the Master Collector is stored on the NPS system for reporting purposes. The stored data contributes to the NPS system disk usage. On the NPS system, after the database occupies a portion of the disk, you cannot reduce the database (*.db) files and reuse that disk space for operating system. To reduce the disk usage you can modify the retention periods for the extension pack provided by NPS or individual extension packs provided by NNM iSPI Performance for Traffic. The retention period value set for the extension packs provided by NNM iSPI Performance for Traffic overrides the retention period value set for the extension pack provided by NPS. For information on changing retention periods for NPS, see the *HP Network Node Manager iSPI Performance for Metrics Installation Guide*.

Each extension pack provided by NNM iSPI Performance for Traffic is installed with different retention periods for the detailed and summarized data. Following parameters define these retention periods:

- PRSPI_DataRetention_Raw: Number of days for which the detailed data is stored. The detailed data for NNM iSPI Performance for Traffic is stored in raw tables only. Therefore, to change the retention period, you must modify PRSPI_DataRetention_Raw parameter. The NNM iSPI Performance for Traffic extension packs provide the default retention periods listed in the following table:

Table 3 Retention Period Default Values

| Extension Pack | Default Value |
|------------------------------|---------------|
| Interface Traffic | 3 |
| Interface Traffic 1 Minute | 30 |
| Interface Traffic 15 minutes | 400 |

- PRSPI_DataRetention_Hour: Number of days for which the data summarized every hour is stored.
 - NNM iSPI Performance for Traffic does not store data in summary tables. Modifying this parameter will not change the retention period.
- PRSPI_DataRetention_Day: Number of days for which the data summarized every day is stored.
 - NNM iSPI Performance for Traffic does not store data in summary tables. Modifying this parameter will not change the retention period.

- `PRSPI_SUMMARY_Policy`: Summarization policy for the extension pack. HP recommends that you do not set this parameter for any extension pack of NNM iSPI Performance for Traffic.

To change the default retention period for individual extension pack, follow these steps:

- 1 Log on to the NPS system.
- 2 Stop the ETL process.
- 3 Open `customConfig.cfg` file with a text editor:

On Windows

```
<NPS_Data_Dir>\NNMPerformanceSPI\rconfig\<extensionpack_name>\customConfig.cfg
```

In this instance, `<NPS_Data_Dir>` is the directory where NPS configuration and data files are stored after you install NPS.

On Linux

```
/var/opt/OV/NNMPerformanceSPI/rconfig/<extensionpack_name>/customConfig.cfg
```

- 4 Set the parameter `PRSPI_DataRetention_Raw` to modify the number of days for which the detailed data is stored.



Modifying the retention period can have significant impact on the disk usage.

- 5 Save and close `customConfig.cfg` file.
- 6 Restart the ETL process.

Enhancing NPS Performance

NPS processes the NNM iSPI Performance for Traffic files slowly that results in increasing the number of pending files for each type of report to be written to the NNMi system. You can increase the performance of the NPS system by tuning the ETL. For more information, see [Tuning the ETL for NPS](#) on page 73.

You can also enhance the performance of NPS by tuning the hardware. Optimize the disk and file system when large amount of data processing is required to reduce the disk latency and I/O wait for optimized record processing and reporting. For more information, see [Disk Usage Recommendations](#) on page 74.

Tuning the ETL for NPS

To tune the ETL for NPS, follow these steps:

- 1 Log on to the NPS system.
- 2 Stop the ETL process.
- 3 Open `customConfig.cfg` file with a text editor:

On Windows

```
<NPS_Data_Dir>\NNMPerformanceSPI\rconfig\<extensionpack_name>\customConfig.cfg
```

In this instance, *<NPS_Data_Dir>* is the directory where NPS configuration and data files are stored after you install NPS.

On Linux

```
/var/opt/OV/NNMPerformanceSPI/rconfig/<extensionpack_name>/  
customConfig.cfg
```

- 4 Set the following parameters for each extension pack to tune the ETL for NPS:

► Increasing the tuning parameters for ETL process of NPS to values listed in Table 6, Table 7, and Table 8 result in significant increase in CPU utilization. Make sure that there is sufficient CPU bandwidth available before increasing these parameters.

- Set the `ETL_MaxChildProcs` parameter to the value recommended for number of child processes for your environment in Table 6 in *NNM iSPI Performance for Traffic Support Matrix*.
 - Set the `ETL_MaxRecordsPerChild` parameter to the value recommended for maximum number of records per child process for your environment in Table 7 in *NNM iSPI Performance for Traffic Support Matrix*.
 - Set the `ETL_MaxMetricsFilesPerBatch` parameter to the value recommended for number of files per batch for your environment in Table 8 in *NNM iSPI Performance for Traffic Support Matrix*.
- 5 Save and close `customConfig.cfg` file.
 - 6 Restart the ETL process.

Disk Usage Recommendations

To reduce the disk latency and I/O wait, follow these recommendations:

- Create the storage locations `/var/opt/OV`, `IQ_SYSTEM_TEMP`, and `USER_MAIN` on different disks on SAN. Run the following command to set the location and size of these storage locations:

For Windows

```
<NPS_Install_Dir>\NNMPerformanceSPI\bin\dbsize.ovpl
```

For Linux

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

- Set `IQ_SYSTEM_TEMP` to a minimum value of 100 GB.
- Set the disk cache ratios to 50/50 read/write
- Use raw disks for storage locations

For more information, contact your Storage Area Network administrator.

9 Maintaining the NNM iSPI Performance for Traffic

The NNM iSPI Performance for Traffic enables you to back up and restore the configuration files and the embedded database on the Master Collector and Leaf Collector. This chapter explains the scripts that the NNM iSPI Performance for Traffic provides to back up and restore Master Collector and Leaf Collector database and configuration files.

This chapter also describes the changes that are required when you change the hostname of the NNMi management server, Master Collector, Leaf Collector, or NPS.

Backup and Restore Commands

The NNM iSPI Performance for Traffic provides you with the following scripts to back up and restore database and configuration files:

- `nmstrafficmasterbackup.ovpl`: Creates a complete backup of all the Master Collector database and configuration files.
- `nmstrafficmasterresetdb.ovpl`: Deletes the existing Master Collector database and recreates the Master Collector database and tables.
- `nmstrafficmasterrestore.ovpl`: Restores the backup that was created by using the `nmstrafficmasterbackup.ovpl` script.
- `nmstrafficleafbackup.ovpl`: Creates a complete backup of all the Leaf Collector database and configuration files.
- `nmstrafficleafresetdb.ovpl`: Deletes the existing Leaf Collector database and recreates the Leaf Collector database and tables.
- `nmstrafficleafrestore.ovpl`: Restores the backup that was created by using the `nmstrafficleafbackup.ovpl` script.

For more information, see the appropriate reference page.



The scripts provided by the NNM iSPI Performance for Traffic enable you to back up and restore files when NNMi and Master Collector or Leaf Collector are not installed on the same system. To back up and restore files when NNMi and Master Collector or Leaf Collector are installed on the same system, see the *HP Network Node Manager i Software Deployment Reference Guide*.

Backing up Master Collector

To back up the Master Collector, follow these steps:

- 1 Log on to the Master Collector system as an administrator on Windows and as root on Linux.

- 2 Stop the Master Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl or  
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl
```

- 3 Run the following command to start the back up of Master Collector database and configuration files:

```
nmstrafficmasterbackup.ovpl -target <Full path of the target archived  
file> -scope [all|db]
```

In this instance, *<Full path of the target archived file>* is the directory where you want to store the backup file.

The option `all` enables you to back up the database and configuration files.

The option `db` enables you to back up the database only.

The backup script creates a tar file of the backup data.

- 4 Start the Master Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl or  
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl
```

Resetting Master Collector Database

To reset the Master Collector database, follow these steps:

- 1 Log on to the Master Collector system as an administrator on Windows and as root on Linux.

- 2 Stop the Master Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl or  
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl
```

- 3 Run the following command to reset the Master Collector database:

```
nmstrafficmasterresetdb.ovpl -start
```

- 4 Start the Master Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl or  
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl
```

Restoring Master Collector



Before you restore the Master Collector database, you must reset the Master Collector database as described in [Resetting Master Collector Database](#) on page 76.

To restore the Master Collector database, follow these steps:

- 1 Log on to the Master Collector system as an administrator on Windows and as root on Linux.

- 2 Stop the Master Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl or  
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstop.ovpl
```

- 3 Run the following command to restore the Master Collector configuration files and database:

```
nmstrafficmasterrestore.ovpl -source <Full path of the archived file  
to restore> -scope [all|db]
```

In this instance, *<Full path of the archived file to restore>* is the full path of the backup file that you want to restore.

Option `all` restores the backup of the database and configuration files. You can restore the backup using the option `all` only if you have previously backed up the database and configuration files using the option `all` in [step 3](#) on page 76.

Option `db` restores the backup of the database only. You can restore the backup using the option `db` only if you have previously backed up the database using the option `db` in [step 3](#) on page 76.

- 4 Start the Master Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl or  
%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl
```

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterstart.ovpl
```

Backing up Leaf Collector

To back up the Leaf Collector, follow these steps:

- 1 Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
- 2 Stop the Leaf Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl or  
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

- 3 Run the following command to start the back up of Leaf Collector database and configuration files:

```
nmstrafficleafbackup.ovpl -target <Full path of the target archived  
file> -scope [all|db]
```

In this instance, *<Full path of the target archived file>* is the directory where you want to store the backup file.

The option `all` enables you to back up the database and configuration files.

The option `db` enables you to back up the database only.

The backup script creates a tar file of the backup data.

- 4 Start the Leaf Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl or  
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

Resetting Leaf Collector Database

To reset the Leaf Collector database, follow these steps:

- 1 Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
- 2 Stop the Leaf Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl or  
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

- 3 Run the following command to reset the Leaf Collector database:

```
nmstrafficleafresetdb.ovpl -start
```

- 4 Start the Leaf Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl or  
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

Restoring Leaf Collector



Before you restore the Leaf Collector database, you must reset the Leaf Collector database as described in [Resetting Leaf Collector Database](#) on page 78.

To restore the Leaf Collector database, follow these steps:

- 1 Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
- 2 Stop the Leaf Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl or  
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
```

- 3 Run the following command to restore the Leaf Collector configuration files and database:

```
nmstrafficleafrestore.ovpl -source <Full path of the archived file to  
restore> -scope [all|db]
```

In this instance, *<Full path of the archived file to restore>* is the full path of the backup file that you want to restore.

Option `all` restores the backup of the configuration files and database. You can restore the backup using the option `all` only if you have previously backed up the configuration files and database using the option `all` in [step 3](#) on page 78.

Option `db` restores the backup of the database only. You can restore the backup using the option `db` only if you have previously backed up the database using the option `db` in [step 3](#) on page 78.

- 4 Start the Leaf Collector by running the following command:

On Windows

```
%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl or  
%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
```

On Linux

```
/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl
```

Changing the Hostnames

You can change the hostname of the NNMi management server, Master Collector, Leaf Collector, and NPS. Whenever you change hostname for one of the servers, the dependent server must be made aware of the change. For example, if the hostname of the NNMi management server changes, you must update the Master Collector and NPS with the new hostname. The following sections describe the changes required when one of the hostname changes.

Changing the NNMi Hostname

If you change the NNMi hostname, you must update the following NNM iSPI Performance for Traffic components:

- NNMi Extension for iSPI Performance for Traffic
- Master Collector
- Leaf Collector

On the NNMi Extension for iSPI Performance for Traffic system, follow these steps:

- 1 Log on to the NNMi management server as an administrator on Windows and as root on Linux.
- 2 Run the following command:

On Windows

```
%NnmInstallDir%\bin\nnmsetofficialfqdn.ovpl
```

On Linux

```
/opt/OV/bin/nnmsetofficialfqdn.ovpl
```

On the Master Collector system, follow these steps:

- 1 Log on to the Master Collector system as an administrator on Windows and as root on Linux.
- 2 Navigate to the following directory:

On Windows

```
%NnmDataDir%\nmsas\traffic-master\conf or  
%TrafficDataDir%\nmsas\trafficmaster\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-master/conf
```

- 3 Open the `nms-traffic-master.address.properties` file with a text editor.
- 4 Modify the value of `jboss.nm.host` property to the hostname of the NNMi management server.
- 5 Save and close the file.
- 6 Open the `nm.extended.properties` file with a text editor.

- 7 Modify the value of the `com.hp.ov.nms.spi.traffic-master.nnm.hostname` property to the hostname of the NNMi management server.

► If the NNMi management server is configured for application failover, modify the value of the `com.hp.ov.nms.spi.traffic-master.nnm.secondary.hostname` property to the hostname of the NNMi management server and restart the Master Collector.

- 8 Save and close the file.
- 9 Navigate to the following directory:

On Windows

```
%NnmInstallDir%\traffic-master\server\conf\ or  
%TrafficDataDir%\trafficmaster\server\conf\
```

On Linux

```
/opt/OV/traffic-master/server/conf/
```

- 10 Open the `login-config.xml` file with a text editor.
- 11 Search for the following string:

```
<application-policy name="nnm">
```

- 12 Modify the hostname of the NNMi management server in the following properties:

- ```
<login-module
code="com.hp.ov.nms.as.server.security.NmsSPILoginModule"
flag="sufficient"> <module-option name="nnmAuthUrl">http://
<nnmhostname>:<nnmport>/spilogin/auth</moduleoption>< module-option
name="password-stacking">useFirstPass</moduleoption> </login-module>
```
- ```
<login-module  
code="com.hp.ov.nms.as.server.security.NmsSPILoginModule"  
flag="sufficient"><module-option name="nnmAuthUrl">https://  
<nnmsecurehostname>:<nnmsecureport>/spilogin/auth</  
module-option><module-option name="passwordstacking"> useFirstPass</  
module-option></login-module>
```

- 13 Save and close the file.
- 14 Move the content of the following directory to a different directory path if the Master Collector is not installed on the same system as NNMi:

On Windows

```
%NnmDataDir%\shared\nnm\certificates
```

On Linux

```
/var/opt/OV/shared/nnm/certificates
```

- 15 Generate new certificates again using the following commands if the Master Collector is not installed on the same system as NNMi:

On Windows

```
a "%TrafficInstallDir%\nonOV\jdk\nnm\bin\keytool" -genkey -alias  
<Master FQDN>.selfsigned -keyalg rsa -sigalg SHA1withRSA -keysize  
2048 -dname cn=<Master FQDN> -keypass nnmkeypass -validity 36500  
-keystore "%TrafficDataDir%\shared\nnm\certificates\nnm.keystore"  
-storepass nnmkeypass
```

- b `"%TrafficInstallDir%\nonOV\jdk\nnm\bin\keytool" -export -file "%TrafficDataDir%\shared\nnm\certificates\nnm.cert" -keystore "%TrafficDataDir%\shared\nnm\certificates\nnm.keystore" -alias <Master FQDN>.selfsigned -storepass nnmkeypass`
- c `"%TrafficInstallDir%\nonOV\jdk\nnm\bin\keytool" -importcert -file "%TrafficDataDir%\shared\nnm\certificates\nnm.cert" -keystore "%TrafficDataDir%\shared\nnm\certificates\nnm.truststore" -storepass ovpass - noprompt`

➤ If the Master Collector is configured for secure communication with the NNMi management server, you must add the certificates from the NNMi management server to the `nnm.truststore` again. For more information, see [Enabling Secure Communication between NNMi and the NNM iSPI Performance for Traffic](#) on page 25.

On Linux

- a `"/opt/OV/nonOV/jdk/nnm/bin/keytool" -genkey -alias <Master FQDN>.selfsigned -keyalg rsa -sigalg SHA1withRSA -keysize 2048 -dname cn=<Master FQDN> -keypass nnmkeypass -validity 36500 -keystore "/var/opt/OV/shared/nnm/certificates/nnm.keystore" -storepass nnmkeypass`
- b `"/opt/OV/nonOV/jdk/nnm/bin/keytool" -export -file "/var/opt/OV/shared/nnm/certificates/nnm.cert" -keystore "/var/opt/OV/shared/nnm/certificates/nnm.keystore" -alias <Master FQDN>.selfsigned -storepass nnmkeypass`
- c `"/opt/OV/nonOV/jdk/nnm/bin/keytool" -importcert -file "/var/opt/OV/shared/nnm/certificates/nnm.cert" -keystore "/var/opt/OV/shared/nnm/certificates/nnm.truststore" -storepass ovpass - noprompt`

➤ If the Master Collector is configured for secure communication with the NNMi management server, you must add the certificates from the NNMi management server to the `nnm.truststore` again. For more information, see [Enabling Secure Communication between NNMi and the NNM iSPI Performance for Traffic](#) on page 25.

16 Restart the Master Collector system.

On the Leaf Collector system that is installed on the NNMi management server, follow these steps:

➤ No changes are required on the Leaf Collector system when Leaf Collector is not installed on the NNMi management server.

- 1 Log on to the Leaf Collector system as an administrator on Windows and as root on Linux.
- 2 Navigate to the following directory:

On Windows

`%NnmDataDir%\nmsas\traffic-leaf\conf`

On Linux

`/var/opt/OV/nmsas/traffic-leaf/conf`

- 3 Open the `nms-traffic-leaf.address.properties` file with a text editor.

- 4 Modify the value of `leaf.host` property to the hostname of the NNMi management server.
- 5 Save and close the file.
- 6 Navigate to the following file:
On Windows
`%NnmInstallDir%\traffic-leaf\server\ or
%TrafficInstallDir%\trafficleaf\server\`
On Linux
`/opt/OV/traffic-leaf/server`
- 7 Open the `server.properties` file.
- 8 Modify the value of `java.rmi.server.hostname` property to the hostname of the NNMi management server.
- 9 Save and close the file.
- 10 Restart the Leaf Collector system.

Changing the Master Collector Hostname

If you change the Master Collector hostname, you must update the following NNM iSPI Performance for Traffic components:

- NNMi Extension for iSPI Performance for Traffic
- Master Collector

On the NNMi Extension for iSPI Performance for Traffic system, follow these steps:

- 1 Log on to the NNMi management server.
- 2 Navigate to the following directory:
On Windows
`%NnmInstallDir%\support`
On Linux
`/opt/OV/support`
- 3 Run the following commands:
 - a `nnmtwiddle.ovpl -host <nnmhostname> -port 80 -u system -p <NNMi system user passwd> invoke
com.hp.ov.nms.topo:service=NetworkApplication removeApplication traffic`
 - b `nnmtwiddle.ovpl -host <nnmhostname> -port 80 -u system -p <NNMi system user passwd> invoke
com.hp.ov.nms.topo:service=NetworkApplication setApplicationService traffic <masterhostname> http 12080`
 - c `nnmtwiddle.ovpl -u system -p <nnm system passwd> invoke
com.hp.ov.nms.topo:service=NetworkApplication printConfiguration`
- 4 Restart the NNMi management server.

On the Master Collector system, follow these steps:

- 1 Log on to the Master Collector system.
- 2 Navigate to the following directory:

On Windows

```
%NnmInstallDir%\traffic-master\server or %TrafficInstallDir%\trafficmaster\server
```

On Linux

```
/opt/OV/traffic-master/server
```

- 3 Open the `server.properties` file with a text editor.
- 4 Modify the value of `java.rmi.server.hostname` property to the hostname of the Master Collector.
- 5 Save and close the file.
- 6 Navigate to the following directory:

On Windows

```
%NnmDataDir%\nmsas\traffic-master\conf or  
%TrafficDataDir%\nmsas\trafficmaster\conf
```

On Linux

```
/var/opt/OV/nmsas/traffic-master/conf
```

- 7 Open the `nnm.extended.properties` file with a text editor.
- 8 Modify the value of the `com.hp.ov.nms.spi.traffic-master.spi.hostname` property to the hostname of the Master Collector.
- 9 Save and close the file.
- 10 Move the content of the following directory to a different directory path if the Master Collector is not installed on the same system as NNMi:

On Windows

```
%NnmDataDir%\shared\nnm\certificates
```

On Linux

```
/var/opt/OV/shared/nnm/certificates
```

- 11 Generate new certificates again using the following commands if the Master Collector is not installed on the same system as NNMi:

On Windows

- a `"%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool" -genkey -alias <Master FQDN>.selfsigned -keyalg rsa -sigalg SHA1withRSA -keysize 2048 -dname cn=<Master FQDN> -keypass nnmkeypass -validity 36500 -keystore "%NnmDataDir%\shared\nnm\certificates\nnm.keystore" -storepass nnmkeypass`
- b `"%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool" -export -file "%NnmDataDir%\shared\nnm\certificates\nnm.cert" -keystore "%NnmDataDir%\shared\nnm\certificates\nnm.keystore" -alias <Master FQDN>.selfsigned -storepass nnmkeypass`

- c `"%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool" -importcert -file
"%NnmDataDir%\shared\nnm\certificates\nnm.cert" -keystore
"%NnmDataDir%\shared\nnm\certificates\nnm.truststore" -storepass
ovpass - noprompt`

➤ If you have enabled secure communication (HTTPS) between the Master Collector and the NNMi management server, see [Enabling Secure Communication between NNMi and the NNM iSPI Performance for Traffic](#) on page 25.

On Linux

- a `"/opt/OV/nonOV/jdk/nnm/bin/keytool" -genkey -alias <Master
FQDN>.selfsigned -keyalg rsa -sigalg SHA1withRSA -keysize 2048
-dname cn=<Master FQDN> -keypass nnmkeypass -validity 36500
-keystore "/var/opt/OV/shared/nnm/certificates/nnm.keystore"
-storepass nnmkeypass`
- b `"/opt/OV/nonOV/jdk/nnm/bin/keytool" -export -file "/var/opt/OV/
shared/nnm/certificates/nnm.cert" -keystore "/var/opt/OV/shared/
nnm/certificates/nnm.keystore" -alias <Master FQDN>.selfsigned
-storepass nnmkeypass`
- c `"/opt/OV/nonOV/jdk/nnm/bin/keytool" -importcert -file "/var/opt/
OV/shared/nnm/certificates/nnm.cert" -keystore "/var/opt/OV/
shared/nnm/certificates/nnm.truststore" -storepass ovpass -
noprompt`

➤ If you have enabled secure communication (HTTPS) between the Master Collector and the NNMi management server, see [Enabling Secure Communication between NNMi and the NNM iSPI Performance for Traffic](#) on page 25.

12 Restart the Master Collector.

Changing the Leaf Collector Hostname

If you change the Leaf Collector hostname, follow these steps on the Leaf Collector system:

- 1 Log on to the Leaf Collector system.
- 2 Navigate to the following directory:

On Windows

`%NnmDataDir%\nmsas\traffic-leaf\conf` or
`%TrafficDataDir%\nmsas\trafficleaf\conf`

On Linux

`/var/opt/OV/nmsas/traffic-leaf/conf`

- 3 Open the `nms-traffic-leaf.address.properties` file with a text editor.
- 4 Modify the value of `leaf.host` property to the hostname of the Leaf Collector.
- 5 Save and close the file.
- 6 Navigate to the following directory:

On Windows

`%NnmInstallDir%\traffic-leaf\server` or
`%TrafficInstallDir%\traffic-leaf\server`

On Linux

/opt/OV/traffic-master/leaf

- 7 Open the `server.properties` file with a text editor.
- 8 Modify the value of the `java.rmi.server.hostname` property to the hostname of the NNMi management server.
- 9 Save and close the file.
- 10 Restart the Leaf Collector system.
- 11 Log on to the NNMi console with the administrator privileges.
- 12 Go to the **Configuration** workspace.
- 13 Double-click **NNM iSPI Performance for Traffic Configuration**. The NNM iSPI Performance for Traffic form opens.
- 14 Log on to the NNM iSPI Performance for Traffic form with the system user account created during the installation of the Master Collector.
- 15 Delete the Leaf Collector instances and the Leaf Collector Systems. For more information, see the *Configuring Leaf Collector Instances and the Configuring Leaf Collector Systems* sections in the *HP Network Node Manager iSPI Performance for Traffic Software Online Help*.
- 16 Add the Leaf Collector instances and the Leaf Collector Systems. For more information, see the *Configuring Leaf Collector Instances and the Configuring Leaf Collector Systems* sections in the *HP Network Node Manager iSPI Performance for Traffic Software Online Help*.

Changing the NPS Hostname

If you change the NPS hostname, you must update the following:

- NNMi management server
- Master Collector

On the NNMi management server, follow these steps:

- 1 Log on to the NNMi management server.
- 2 Navigate to the following directory:
On Windows
`%NnmInstallDir%\bin`
On Linux
`/opt/OV/bin`
- 3 Run the `nnmenableperfspi.ovpl -disable` command at the command prompt.
- 4 Run the `nnmenableperfspi.ovpl` command and provide the hostname when prompted.
- 5 Share the `%NnmDataDir%\shared\perfSpi\datafiles` directory again on the network for the user with the web server client role. Make sure that the user has the read/write access to this directory. For more information, see *Enable the Read/Write Access to the Data Files on the NNMi Management Server* section in the *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*.

On the Master Collector system, follow these steps:

- 1 Log on to the Master Collector system.
- 2 Navigate to the following directory:

On Windows

%NmDataDir%\nmsas\traffic-master\conf or
%TrafficDataDir%\nmsas\trafficmaster\conf

On Linux

/var/opt/OV/nmsas/traffic-master/conf

- 3 Open the `nps.extended.properties` file with a text editor.
- 4 Modify the value of the following property to provide the hostname of NPS:
`com.hp.ov.nms.spi.traffic-master.nps.hostname`
- 5 Save and close the file.

10 NNM iSPI Performance for Traffic Logging

To monitor the performance of the Master Collector or Leaf Collector, or to observe how NNM iSPI Performance for Traffic processes and services are behaving, you can view log files that display a history of process and service activity of the NNM iSPI Performance for Traffic. These files are available in the following directory:

- Master Collector

- *Windows*

- `%NnmDataDir%\log\traffic-master` or
`%TrafficDataDir%\log\traffic-master`

- *Linux*

- `/var/opt/OV/log/traffic-master`

- Leaf Collector

- *Windows*

- `%NnmDataDir%\log\traffic-leaf` or `%TrafficDataDir%\log\traffic-leaf`

- *Linux*

- `/var/opt/OV/log/traffic-leaf`

The NNM iSPI Performance for Traffic stores the log messages in the following log files:

- For the Leaf Collector: `traffic_spi_leaf.log`
- For the Master Collector: `traffic_spi_master.log`

The NNM iSPI Performance for Traffic logs messages at the following logging levels:

- SEVERE: Events that relate to abnormal Master Collector or Leaf Collector behavior.
- WARNING: Events that indicate potential problems.
- INFO: Messages written to the NNMi console (or its equivalent) and all messages included in the WARNING logging level.

11 Deploying NNM iSPI Performance for Traffic in Global Network Management Environment

NNM iSPI Performance for Traffic offers full support for deployment in a Global Network Management environment. Each instance has the following components:

- NNMi
- NNM iSPI Performance for Metrics and Network Performance Server
- The NNM iSPI Performance for Traffic Master Collector
- The NNM iSPI Performance for Traffic Leaf Collectors

The NNMi in the Global Manager receives data from the Regional Managers. The Traffic Master Collector in the Global Manager can be configured to receive data from the Regional Traffic Master Collectors in the following ways:

- The Traffic Master Collector in the Global Manager can receive data from the Traffic Master Collector in the Regional Manager. In this case, you must add the regional Traffic Master Collector as a remote Master source in the global Traffic Master Collector. This ensures that the complete set of data received by the regional Master Collector is forwarded to the global Traffic Master Collector. In the above scenario the global Traffic Master Collector receives data processed by both Traffic Leaf 1 and Traffic Leaf 2.
- The Traffic Master Collector in the Global Manager can receive data directly from a regional Leaf Collector system, bypassing the regional Traffic Master Collector. In this case the regional Traffic Leaf Collector (Traffic Leaf 3 in the above scenario) can be added as a leaf remote source to the global Master collector. This will ensure that the data received by all the Leaf Collectors on the remote Leaf Collector system is sent to the regional Traffic Master Collector as well as the global Traffic Master Collector.

The regional Traffic Master Collector or the regional Traffic Leaf Collector) can only be configured to send data to the global Traffic Master Collector. The global Master Collector cannot administer and manage these components.

Add all the regional Master Collectors as remote Master sources to the global Master Collector.

Licensing

In a Global Network Management environment, you can monitor data from remote Leaf Collectors that belong to different regions. This configuration requires you to use iSPI point licenses for remote Master Collector as well as global Master Collector. This configuration also requires you to enable the Collector Connection Software LTU (see the *HP Network Node Manager iSPI Performance for Traffic Software Installation Guide*).

We appreciate your feedback!

If an email client is configured on this system, click

[Send Email](#)

If no email client is available, copy the following information to a new message in a web mail client and send the message to **docfeedback@hp.com**.

Product name and version: NNM iSPI Performance for Traffic, 9.21

Document title: Deployment Guide

Feedback:

