Hewlett Packard
Enterprise

HPE Network Node Manager iSPI Performance for Traffic Software

Software Version: 10.20
for the Windows® and Linux® operating systems

Deployment Reference

Document Release Date: March 2017
Software Release Date: July 2016

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. HPE 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 HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

Documentation Updates

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

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

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

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

Support

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

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

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

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

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to **https://softwaresupport.hpe.com** and click **Register**.

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

Contents

Chapter 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
- 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:

NNM iSPI Performance for Traffic Documentation Conventions

Symbol	Description
%TrafficInstallDir% (For Windows) $*TrafficInstallDir (For Linux)*	The NNM iSPI Performance for Traffic install directory when Master Collector or Leaf Collector is not installed on the same system as NNMi. *For Windows* *<drive>*`\Program Files\HP\HP BTO Software` *For Linux* `/opt/OV`
%TrafficDataDir% (For Windows) $*TrafficDataDir (For Linux)*	The NNM iSPI Performance for Traffic data directory when Master Collector or Leaf Collector is not installed on the same system as NNMi. *For Windows* *<drive>*`\ProgramData\HP\HP BTO Software` *For Linux* `/var/opt/OV/`
%NnmInstallDir% (For Windows) $*NnmInstallDir (For Linux)*	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. *For Windows* *<drive>*`\Program Files\HP\HP BTO Software` *For Linux* `/opt/OV`

NNM iSPI Performance for Traffic Documentation Conventions, continued

Symbol	Description
%*NnmDataDir%* *(For Windows)* $*NnmDataDir (For Linux)*	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. *For Windows* <*drive*>`\ProgramData\HP\HP BTO Software` *For Linux* `/var/opt/OV/`

Other Available 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 the extended list of the available environment variables, 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`

Chapter 2: Introduction to the NNM iSPI Performance for Traffic

The NNM iSPI Performance for Traffic enriches the data obtained from the IP flow data 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 record, 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

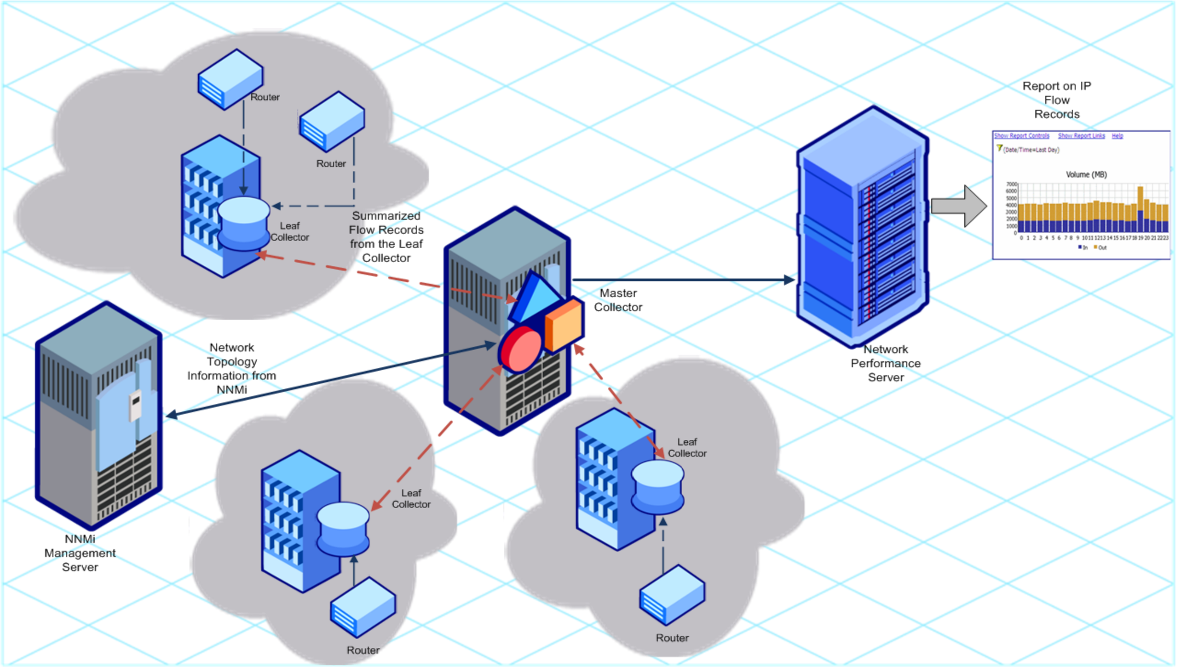
Network routers are capable of exporting IP flow data records. An IP flow data record includes details like IP addresses of the source and destination devices or systems, port of the source and destination devices or systems, number of bytes of data transmitted, and so on.

The NNM iSPI Performance for Traffic identifies, collects, and processes the ingress and egress IP flow data records on a specific interface. It can also identify the flow direction when both the ingress and egress flows are enabled on the interface. The NNM iSPI Performance for Traffic provides you with an enriched set of details in which the flow information is enhanced with the network topology information present in NNMi. You can also filter the collected data with user-defined filters or associate the flow with user-defined applications.

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.

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 processes the collected data.
   - The Leaf Collector aggregates and enriches the collected data with the help of in-built rules of aggregation, and then forwards the aggregated data to the Master Collector. The Leaf Collector can aggregate the raw data at every 5 minutes.
   - The Leaf Collector forwards all the **raw data**[1] too, without any modification, to the Master Collector.

     Note: You can configure the NNM iSPI Performance for Traffic to stop forwarding the raw data to the Master Collector.
3. NNMi 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 data that it collected from the Leaf Collector. In addition, the Master Collector also performs DNS resolution, applies ToS Group configuration, applies thresholds, and so on.

[1] The raw data is the set of IP flow records that are exported by traffic flow-exporting routers on the network and collected by the NNM iSPI Performance for Traffic Leaf Collectors. By default, the NNM iSPI Performance for Traffic logs the raw data into the NPS database. In a medium or large-scale environment, it is recommended that you disable the logging of the raw data into the NPS database.

5. The Master Collector logs the processed data to the NPS database. Depending on the configuration, the Master Collector can log two different types of data samples into the NPS database: raw data and data aggregated at every five minutes.
6. With the help of NPS, you can generate reports to analyze the network traffic. Also, with the data collected by Leaf Collector and stored into the NPS database, the NNM iSPI Performance for Traffic shows different dashboards and graphs in the NNMi console.

Chapter 3: Deploying the NNM iSPI Performance for Traffic

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

- Entry
- Small
- Medium
- Large

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

Chapter 4: Preparation

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

Software and Hardware Pre-installation Checklist

Document Type	Document Path
HP Network Node Manager iSPI Performance for Traffic Interactive Installation Guide	• Media root • Manuals web site
NNMi Ultimate Release Notes	Manuals web site
NNMi Ultimate Support Matrix	Manuals web site

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

https://softwaresupport.hpe.com

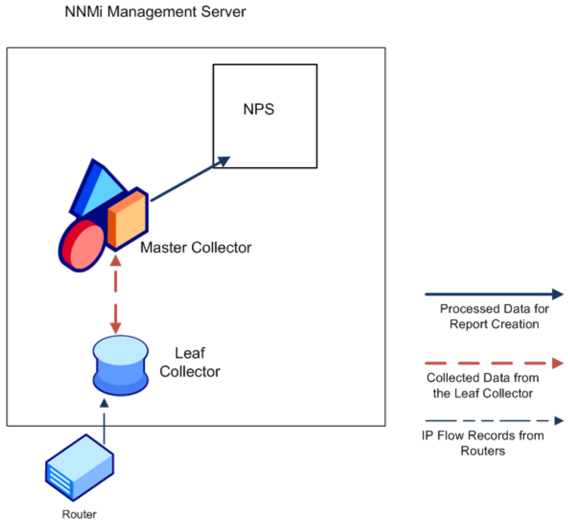
Deploying in an Entry-Level Environment

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.

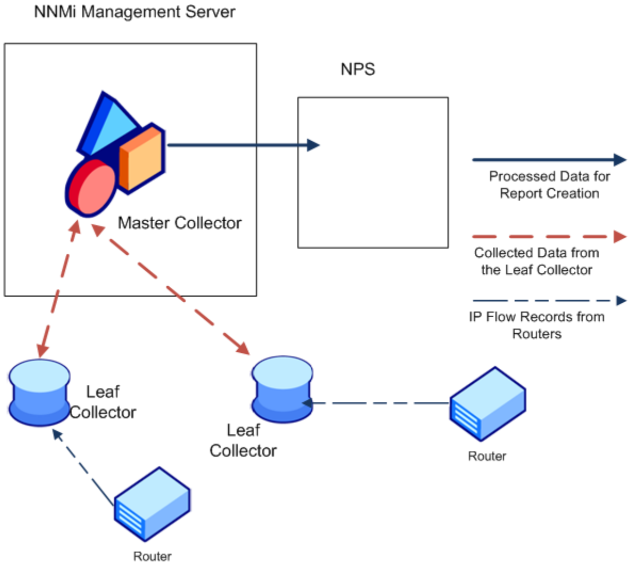
Entry-Level Deployment



Deploying in a Small or Medium-Sized Environment

In this deployment, you must install the Master Collectors 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 *NNMi Ultimate Support Matrix* to determine the number of Leaf Collectors required for your environment.

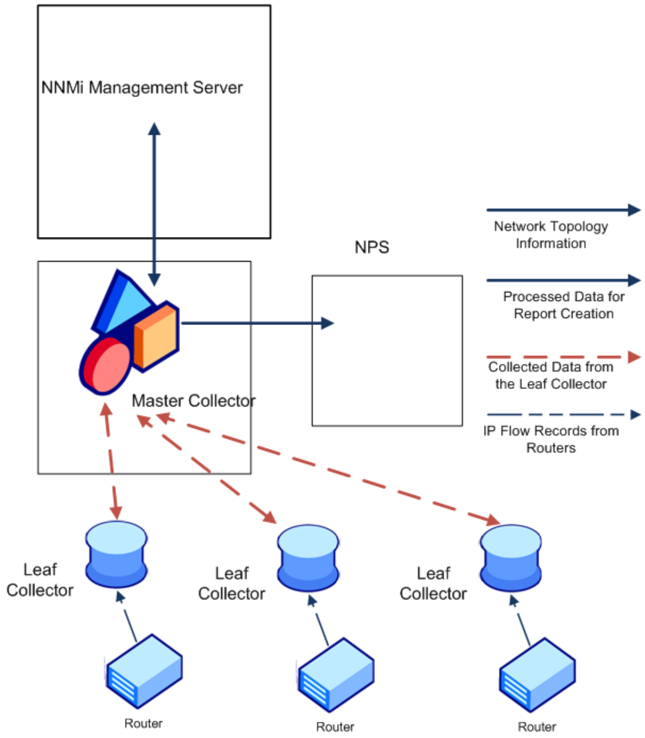
Small or Medium-Sized Deployment


NNMi Management Server
NPS
Master Collector
Processed Data for Report Creation
Collected Data from the Leaf Collector
IP Flow Records from Routers
Leaf Collector
Leaf Collector
Router
Router

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 *NNMi Ultimate Support Matrix* to determine the number of Leaf Collectors required for your environment.

Large Deployment


NNMi Management Server
NPS
Network Topology Information
Processed Data for Report Creation
Collected Data from the Leaf Collector
IP Flow Records from Routers
Master Collector
Leaf Collector
Leaf Collector
Leaf Collector
Router
Router
Router

Disable Raw Data Logging

The raw data is the set of IP flow records that are exported by the traffic flow-exporting routers on the network and collected by the NNM iSPI Performance for Traffic Leaf Collectors. By default, the NNM iSPI Performance for Traffic logs the raw data into the NPS database. In a medium or large-scale environment, it is recommended that you disable logging of the raw data into the NPS database.

The Interface Traffic Extension Pack, provided with the NNM iSPI Performance for Traffic, consumes the raw data while generating reports. You cannot use Interface Traffic reports if you disable logging of the raw data.

Note:

- Logging of the raw data is supported for up to 480k unique flow records per minute at the Master Collector.
- The Master Collector in the medium tier cannot process more than 600K flow records per minute when the raw data continues to be logged into the NPS database.
- See the *NNMi Ultimate Support Matrix* for more information about system requirements when the logging of raw data is enabled.

To disable raw data logging, 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. Restart the Leaf Collectors by running the following commands on each Leaf Collector system:
   On Windows
   a. `%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl` or `%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl`
   b. `%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl` or `%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl`

   On Linux
   a. `/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl`
   b. `/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl`

After you complete the procedure, the NNM iSPI Performance for Traffic stops logging the raw data to the NPS database.

Enable Raw Data

Enable the NNM iSPI Performance for Traffic to again log raw data to the NPS database by following 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 `Enable Flush`.
5. Click `Save`.
6. Restart the Leaf Collectors by running the following commands on each Leaf Collector system:
   On Windows
   a. `%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl` or `%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl`
   b. `%NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl` or `%TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl`

   On Linux
   a. `/opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl`
   b. `/opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl`

After you complete the procedure, the NNM iSPI Performance for Traffic again starts logging the raw data to the NPS database.

Chapter 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" below.

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 19.

> **Note:** 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.

The NNM iSPI Performance for Traffic enables you to communicate securely with the NNMi management server and NPS. You can also configure the NNM iSPI Performance for Traffic to ensure secure communication between the Master Collector and Leaf Collectors. For more information, see "Enabling Security" on page 21.

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\nnmsso.ovpl -reload
   ```

On Linux

```
/opt/OV/bin/nnmsso.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\nnmsso.ovpl -reload
   ```

   On Linux

   ```
   /opt/OV/bin/nnmsso.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:
    - 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`
    - 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:
    - 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`
    - 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/nnm/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.

> **Note:** 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 steps:

1. Configuring NNMi
2. Configuring a Certificate Validation Method
3. Configuring the NNM iSPI Performance for Traffic

> **Note:** 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.

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 *HPE Network Node Manager Deployment Reference Guide*.

   After configuring NNMi to use the PKI authentication, if you do not perform Step 3, you will be prompted to provide NNMi user name and password when you try to launch the NNM iSPI Performance for Traffic Configuration form.
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 *HPE Network Node Manager Deployment Reference Guide*.
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:

a. Make sure that Step 1 and Step 2 are complete.

b. Log on to the Master Collector system.

c. Navigate to the following directory:
On Windows

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

On Linux

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

d. Open the `nms-auth-config.xml` file using a text editor.

e. 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 *HPE Network Node Manager Deployment Reference*.

> **Note:** 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.

f. Save and close the file.

g. Run the following command at the command prompt:
On Windows

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

On Linux

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

Master Collector and NNMi Installed on Separate Systems

> **Note:** 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 nodes in maintenance mode before running the `nmstrafficmasterstop.ovpl` and `nmstrafficmasterstart.ovpl` commands.

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

a. Log on to the Master Collector system.

b. Navigate to the directory that contains the `nnm.truststore` files:
On Windows

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

On Linux

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

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

d. 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\hpsw\bin\keytool -importcert -noprompt -keystore
“%TrafficDataDir%\shared\nnm\certificates\nnm.truststore” -file mycompany_ca.cer
-storepass ovpass -alias <aliasname>
```

On Linux

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

e. Make sure that Step 1 and Step 2 are complete.

f. Navigate to the following directory:
On Windows

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

On Linux

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

g. Open the `nms-auth-config.xml` file using a text editor.

h. 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 *HPE Network Node Manager Deployment Reference*.

> **Note:** 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.

i. Save and close the file.

j. Run the following command on the Master Collector system:
On Windows

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

On Linux

```
/opt/OV/traffic-master/bin/nmstrafficmasterauthreload.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
- NNM iSPI Performance for Traffic and NPS
- Master Collector and Leaf Collectors

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`

   Note: 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.

   Note: 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`

   Note: 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`

   Note: 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 `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`

   Note: 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.

   Note: 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`

   > **Note:** 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 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`

   > **Note:** 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>/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. 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.

    > **Note:** If `nnm.cert` file is not available in the `%NnmDataDir%\shared\nnm\certificates\` folder,

follow these steps:

a. Run the following command to generate the `nnm.cert` file:
On Windows
```
%NnmInstallDir%\bin\nnmkeytool.ovpl -export -file c:\nnm.cert -keystore
nnm-key.p12 -storetype PKCS12 -storepass nnmkeypass -alias <nnmi_
FQDN>.selfsigned
```
On Linux
```
$NnmInstallDir/bin/nnmkeytool.ovpl -export -file /tmp/nnm.cert -keystore
nnm-key.p12 -storetype PKCS12 -storepass nnmkeypass -alias <nnmi_
FQDN>.selfsigned
```
In this instance, <nnmi_FQDN> is the FQDN of the NNMi management server.

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

16. Run the following command on the Master Collector to add the certificate to the truststore:
On Windows
```
%TrafficInstallDir%\nonOV\jdk\hpsw\bin\keytool -importcert -file "<tmp>/nnm.cert" -
keystore "%TrafficDataDir%/shared/nnm/certificates/nnm.truststore" -storepass ovpass
-noprompt -alias <nnmi_FQDN>
```
On Linux
```
/opt/OV/nonOV/jdk/hpsw/bin/keytool -importcert -file "<tmp>/nnm.cert" -keystore
"/var/opt/OV/shared/nnm/certificates/nnm.truststore" -storepass ovpass -noprompt -
alias <nnmi_FQDN>
```
In this instance, <nnmi_FQDN> is the FQDN of the NNMi management server.

17. Run the following command on the Master Collector to verify that the certificates are added to the truststore:
On Windows
```
%TrafficInstallDir%\nonOV\jdk\hpsw\bin\keytool -list -keystore
"%TrafficDataDir%\shared\nnm\certificates\nnm.truststore" -storepass ovpass
```
On Linux
```
/opt/OV/nonOV/jdk/hpsw/bin/keytool -list -keystore
"/var/opt/OV/shared/nnm/certificates/nnm.truststore" -storepass ovpass
```

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 Master Collector and NPS

To enable secure communication between the Master Collector and NPS 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 `trafficcert.cer`.

Note: 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 `nnm.truststore`.

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

a. Stop the Master Collector processes using 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
```

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 `trafficcert.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\hpsw\bin\keytool -importcert -noprompt -keystore
“%NnmDataDir%\shared\nnm\certificates\nnm.truststore” -file trafficcert.cer -
storepass ovpass -alias cognos
```

or

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

On Linux

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

Note: 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
```

Enabling Secure Communication between the Master and the Leaf Collector

During the Leaf Collector installation, the installation script creates a self-signed certificate for the Leaf Collector system. This certificate contains an alias that includes the fully-qualified domain name of the node. The installation script adds this self-signed certificate to the `nnm.keystore`, `nnm.truststore`, and `nnm.cert` files on the Leaf Collector system.

After installing the Master Collector and the Leaf Collector, you can use the Leaf Collector system's self-signed certificate to enable the Master Collector to use HTTPS protocol to communicate with Leaf Collector systems.

To enable secure communication between the Master and the Leaf Collectors, follow these steps:

1. Add the Leaf Collector Certificate to the Trusted Certificates on the Master Collector.
   When Master Collector and Leaf Collector are installed on the same system, no additional steps are required to add Leaf Collector certificates to the trusted certificates.

   When Master Collector and Leaf Collector are installed on separate systems, follow these steps for each Leaf Collector system:

   a. Log on to the Leaf Collector system.
   b. Navigate to the directory that contains the Leaf Collector certificate file, `nnm.cert`:
      On Windows

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

      or

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

      On Linux

      ```
      /var/opt/OV/shared/nnm/certificates
      ```
   c. Copy the Leaf Collector certificate to the Master Collector system.

      > **Note:** 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 nodes in maintenance mode before running the `nmstrafficmasterstop.ovpl` and `nmstrafficmasterstart.ovpl` commands.

   d. 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
      ```

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.

e. Import the Leaf Collector certificate into the `nnm.truststore` file.
For example, the `leaf.cert` file contains the certificate from the Leaf Collector that you must use. The `leaf.cert` file can be the self-signed certificate or a signed certificate from the Certificate Authority that you need to import.
Run the following command to import the CA certificate into the `nnm.truststore` file:
On Windows

```
%NnmInstallDir%\nonOV\jdk\hpsw\bin\keytool -importcert -noprompt -keystore
“%NnmDataDir%\shared\nnm\certificates\nnm.truststore” -file leaf.cert -storepass
ovpass -alias <Leaf_FQDN>
```

or

```
%TrafficInstallDir%\nonOV\jdk\hpsw\bin\keytool -importcert -noprompt -keystore
“%TrafficDataDir%\shared\nnm\certificates\nnm.truststore” -file leaf.cert -
storepass ovpass -alias <Leaf_FQDN>
```

On Linux

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

If you have stopped NNMi processes in *step d*, you must start the NNMi processes after importing the certificate into the `nnm.truststore`.

f. 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
```

2. Log on to the NNM iSPI Performance for Traffic Configuration UI with the `system` user account to enable secure communication between the Master Collector and the Leaf Collector. Follow the steps listed in the *Configuring Leaf Collector Systems* section in the *HP Network Node Manager iSPI Performance for Traffic Software Online Help*.

Using a Signed Certificate from a Certificate Authority

To use a signed certificate from a Certificate Authority instead of self-signed certificate on the Master Collector, follow these steps:

1. Log on to the Master Collector system.
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. Follow steps similar to the steps listed in the *Generating a Certificate Authority Certificate* section in the *HPE Network Node Manager i Software Deployment Reference*.
4. Navigate to the following directory on the Master Collector:
   On Windows

   `%NnmDataDir%\nmsas\traffic-master`

   or

   `%TrafficDataDir%\nmsas\traffic-master`

   On Linux

   `/var/opt/OV/nmsas/traffic-master`
5. Open the `server.properties` file using a text editor.
6. Add the following property :
   `nmsas.server.security.keystore.alias=`<*new alias name*>

   In this instance, <*new alias name*> is the alias name that you provide when importing the signed certificate.
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 use a signed certificate from a Certificate Authority instead of self-signed certificate on the Leaf Collector, follow these steps:

1. Log on to the Leaf Collector system.
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. Follow steps similar to the steps listed in the *Generating a Certificate Authority Certificate* section in the *HPE Network Node Manager i Software Deployment Reference*.
4. Navigate to the following directory on the Leaf Collector:
   On Windows

   `%NnmDataDir%\nmsas\traffic-leaf`

   or

   `%TrafficDataDir%\nmsas\traffic-leaf`

   On Linux

   `/var/opt/OV/nmsas/traffic-leaf`
5. Open the `server.properties` file using a text editor.

6. Add the following property :
   `nmsas.server.security.keystore.alias=<`*new alias name*`>`

   In this instance, <*new alias name*> is the alias name that you provide when importing the signed certificate.
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
   ```

Chapter 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, HPE 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 *NNMi Ultimate 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 NNMi Extension for iSPI Performance for Traffic on all NNMi management servers in the cluster.

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.

> **Note:** 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 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 Guide*.

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

1. Installing NNMi and Master Collector

Install NNMi and Master Collector on each system. For more information, see the *NNMi Interactive Installation Guide* and the *HP Network Node Manager iSPI Performance for Traffic Interactive Installation Guide*.

2. Install the HPE NNMi Extension for iSPI Performance for Traffic on each server in the HA cluster. When installing the HPE NNMi Extension for iSPI Performance for Traffic, specify the virtual FQDN of the NNMi server as the FQDN of the Master Collector system.
3. 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 Guide* for information on configuring NNMi to run under HA.
4. Configuring the Master Collector on the Primary (active) node
   To configure the Master Collector on the primary (active) node, follow these steps:
   a. Run the following command to find the virtual hostname:
      `nnmofficialfqdn.ovpl`
   b. Modify the `login-config.xml` file from the `%NnmInstallDir%\traffic-master\server\conf%NnmInstallDir%\conf\traffic-master` or `/opt/OV/traffic-master/server/conf/opt/OV/conf/traffic-master` directory to reflect the virtual FQDN of the NNMi management server:
   c. Open the `login-config.xml` file with a text editor.
   d. Look for the element `<module-option name=”nnmAuthUrl”>`.
   e. Modify the string contained within the element to reflect the virtual FQDN of the NNMi management server.
   f. Save the file.
   g. Go to the following directory:
      On Windows

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

      On Linux

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

      > **Note:** 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.

   i. Default values are:
      On Windows

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

      On Linux

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

      > **Note:** 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`

j. *Go to Step n 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.

> **Note:** 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.

k. Navigate to the following directory:
On Windows

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

On Linux

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

l. Open the `nms-auth-config.xml` file using a text editor.

m. 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 *HPE Network Node Manager Deployment Reference Guide*.

> **Note:** 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.

n. 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
```

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

a. 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 Interactive Installation Guide* and the *HP Network Node Manager iSPI Performance for Traffic Interactive Installation Guide* for more information.

b. Run the following command to find the virtual hostname:
`nnmofficialfqdn.ovpl`

c. Modify the `login-config.xml` file from the `%NnmInstallDir%\traffic-master\server\conf%NnmInstallDir%\conf\traffic-master` or `/opt/OV/traffic-master/server/conf/opt/OV/conf/traffic-master` directory to reflect the virtual FQDN of the NNMi management server:

d. Open the `login-config.xml` file with a text editor.

e. Look for the element `<module-option name=”nnmAuthUrl”>`.

f. Modify the string contained within the element to reflect the virtual FQDN of the NNMi management server.

g. Save the file.

h. Go to the following directory:
On Windows

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

On Linux

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

i. 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

j. *Go to Step p 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.*

k. 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.

l. 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.

m. Navigate to the following directory:
On Windows

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

On Linux

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

n. Open the `nms-auth-config.xml` file using a text editor.

o. 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 *HPE Network Node Manager Deployment Reference*.

> **Note:** 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.

p. 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
```

6. Configuring Each Passive Node in the HA Cluster
   Repeat Step 4 on each passive node in the HA cluster.

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:

   On Windows

   `%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`

   On Linux

   `/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:

   On Windows

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

   On Linux

   `/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>`*`\maintenance`

   `/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.

   On Windows

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

   On Linux

   `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:

   On Windows

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

   On Linux

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

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

    On Windows

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

    On Linux

    `/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:

    On Windows

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

    On Linux

    `/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 Collector host name from virtual IP to actual host name of the node:

    On Windows

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

    On Linux

    `/var/opt/OV/shared/traffic-master/conf/nnm.extended.properties`
14. For the 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 the Master Collector using the following command:
    `nmstrafficmasterstart.ovpl`

Unconfiguring NNM iSPI Performance for Traffic from an NNMi HA Cluster

To completely unconfigure NNM iSPI Performance for Traffic from an HA cluster in a co-located setup, follow these steps:

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

   On Windows:

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

   On Linux:

   ```
   $NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl -group <resource_group> -activeNode
   ```
2. On each passive node, unconfigure the NNM iSPI Performance for Traffic add-on from the HA cluster. To unconfigure, run the following command:

   On Windows:

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

   On Linux:

```
$NnmInstallDir/misc/nnm/ha/nnmhaunconfigure.ovpl NNM -addon TRAFFIC
```

3. Verify that theNNM iSPI Performance for Traffic add-on is unconfigured on all the cluster passive nodes. To verify, run the following command:

   On Windows:

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

   On Linux:

   ```
   $NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS
   ```

   If any passive cluster node with the NNM iSPI Performance for Traffic add-on appears in the output, repeat step 2 on that node.

4. You can now unconfigure the NNM iSPI Performance for Traffic from the HA cluster on the active node. To unconfigure, run the following command:

   On Windows:

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

   On Linux:

   ```
   $NnmInstallDir/misc/nnm/ha/nnmhaunconfigure.ovpl NNM -addon TRAFFIC
   ```

5. Make sure that NNMi is running on the active node.

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" below
2. "Install Master Collector Patch on Active Master Collector" on the next page
3. "Reconfigure Passive Master Collectors in HA" on page 42

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`

     > **Note:** 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>`

     > **Note:** 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`

     > **Note:** 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>`

  > **Note:** 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.

   > **Note:** 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

1. To install Master Collector Patch on active Master Collector in HA, follow these steps:
2. Move the HA cluster in maintenance mode by creating the following files on active Master Collector:
   On Windows

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

   `%NmmDataDir%\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`
3. 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`

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

   On Linux

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

   `/opt/OV/nonOV/traffic-master/bin/nmstrafficmasterstop.ovpl --HA`
4. Install the Master Collector Patch as described in the patch text.

   > **Note:** Do NOT unconfigure HA on the active Master Collector.

5. 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`

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

On Linux

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

```
/opt/OV/nonOV/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`

     > **Note:** 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`

     > **Note:** 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`

     > **Note:** 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`

     > **Note:** 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>\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`

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

Uninstalling Master Collector Patch in HA

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

1. "Uninstall Master Collector Patch from Passive Master Collector" below
2. "Uninstall Master Collector Patch from Active Master Collector" on the next page
3. "Reconfigure Passive Master Collectors in HA" on page 45

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>\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
  ```

  > **Note:** 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>
  ```

  > **Note:** 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
  ```

  > **Note:** 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>
  ```

  > **Note:** 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.

   > **Note:** 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>\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`

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

   On Linux

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

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

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

   > **Note:** 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`

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

   On Linux

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

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

Reconfigure Passive Master Collectors in HA

1. To reconfigure passive Master Collector in HA, follow these steps:
2. 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`

     > **Note:** 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`

> **Note:** 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`

  > **Note:** 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`

  > **Note:** 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`

3. Delete the following files to remove the passive Master Collector (s) from the maintenance mode:
   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`

4. Delete the following files to remove the active Master Collector from the maintenance mode:
   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`

Chapter 7: Deploying the NNM iSPI Performance 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 NNM iSPI Performance for Traffic 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 Collector and Leaf Collectors are installed on separate non-co-located systems.
- The NNMi Extension for iSPI Performance for Traffic must be installed on both the primary and secondary NNMi management servers.
- The Master Collector must be configured on both primary and secondary NNMi management servers to point to the following:
  - The NNMi instance (provide the physical FQDN)
  - The network share drive where the NNM iSPI Performance for Metrics data files folder on the HA system is shared.

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.

> **Note:** If you want to enable secure communication (HTTPS) between the Master Collector and the NNMi management server, see "Enabling Security" on page 21

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 `nnm.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.

     > **Note:** If you want to enable secure communication (HTTPS) between the Master Collector and the NNMi management server, see "Enabling Security" on page 21.

   - 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.traffic-master.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`
12. Navigate to the following directory:
    On Windows
    `%NnmInstallDir%\traffic-master\server\conf\`

    On Linux
    `/opt/OV/traffic-master/server/conf/`
13. Open the `login-config.xml` file with a text editor.
14. Search for the following string:
    `<application-policy name="nnm">`
15. Modify the host name of the NNM secondary management server in the following properties:

    ```
    login-module code="com.hp.ov.nms.as.server.security.NmsSPILoginModule"
    flag="sufficient"> <module-option
    name="nnmAuthUrl">http://<secondarynnmhostname>:<nnmport>/spilogin/auth</moduleoptio
    n><module-option name="password-stacking">useFirstPass</moduleoption></login-module>
    ```
16. Save and close the file.

Chapter 8: Tuning the NNM iSPI Performance for Traffic

HPE 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. HPE also recommends that you configure the report data retention period for the flow data generated by Master Collector.

Enhancing the Performance of the Master Collector and the 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\%NnmDataDir%\shared\traffic-master\conf\nms-traffic-master.address.properties` or `%TrafficDataDir%\nmsas\traffic-master\conf\%TrafficDataDir%\shared\traffic-master\conf\nms-traffic-master.address.properties`

  On Linux

  `/var/opt/OV/nmsas/traffic-master/conf//var/opt/OV/shared/traffic-master/conf/nms-traffic-master.address.properties`
- On the Leaf Collector system
  On Windows

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

  On Linux

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

The *NNMi Ultimate Support Matrix* defines the following types of environments:

- Entry
- Small
- Medium
- Large

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

Note: 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.

   Note: HPE 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 `flowrecord.pool.size` property to the value recommended for FlowRecord for your environment in *Table 4* in *NNM iSPI Performance for Traffic Support Matrix*. HPE recommends that you set this property to the recommended value *only* once.

   Note:

   - If you have multiple Leaf Collector instances on the same Leaf Collector system, you must divide the required pool size among the Leaf Collector instances. You can then set the flowrecord.pool.size and topn.flowrecord.pool.size properties for each Leaf Collector instance in the nms-traffic-leaf.address.properties file accordingly. For example, if the object pool size required for FlowRecord of a Leaf Collector system is 100K and you have two Leaf Collector instances, you must set the flowrecord.pool.size property to 50K.
   - 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 400MB to the Xmx value for Leaf Collector. For information on how to change the Xmx value, see "Modifying the JVM Parameters" on page 54.

   d. 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*. HPE recommends that you set this property to the recommended value *only* once.

   Note: 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 1GB to the Xmx value for Leaf Collector. For information on how to change the Xmx value, see

> "Modifying the JVM Parameters" on page 54.

e. In a large tier environment, if the NNM iSPI Performance for Traffic monitors at least 4000 interfaces with at least 20 thresholds, you must set the `thresold.objectpool.size` property to at least `1000000`.

f. Save the file.

g. Restart the Leaf Collector by running the following command:
On Windows

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

   On Linux

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

> **Note:** 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 the file.

e. Restart the Master Collector by running the following command:
On Windows

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

   On Linux

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

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.

> **Note:** The 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 the NNM iSPI Performance for Traffic writes files successfully to the NNMi system, the 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, the 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 the 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 the NNM iSPI Performance for Traffic, 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. `nnm.shared.drive.size`: Defines the minimum amount of disk space required on the NNMi system for the 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 Object Pool Tuning

The NNM iSPI Performance for Traffic automatically tunes the pool size of the Leaf Collector based on the values that you set for pool sizes in your environment. You can disable this feature if you do not want variable memory usage.

To disable the automatic tuning of the pool size for a Leaf Collector instance, follow these steps:

1. Log on to the Leaf Collector system.
2. Stop the Leaf Collector processes by running the following commands:
   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\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`
4. Open the `nms-traffic-leaf.address.properties` file with a text editor.
5. Add the following property:
`leaf.collector.object.pool.tuner.disable=true`
Adding the above property disables automatic tuning of pool sizes for all instances.
6. Save and close the file.
7. Start the Leaf Collector processes by running the following commands:
On Windows

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

   On Linux

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

Modifying the JVM Parameters

You can modify the JVM parameters for the Master Collector 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 the *Master Collector Size* table in *NNMi Ultimate 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 the *Master Collector Size* table in *NNMi Ultimate 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 the *Leaf Collector Size* table in *NNMi Ultimate 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 the *Leaf Collector Size* table in *NNMi Ultimate 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
```

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 *HPE Network Node Manager iSPI Performance for Metrics Installation Guide*.

Each extension pack provided by the 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:

  Retention Period Default Values

Extension Pack	Default Value
Interface_Traffic	3
Interface_Traffic_1_minute	30
Interface_Traffic _Aggregated	400

  Note: The Interface Traffic_1_min reports are disabled by default. For information on how to enable these reports, see the *Configuring Master Collectors* section in the *HP Network Node Manager iSPI Performance for Traffic Software Online Help*.

- `PRSPI_DataRetention_Hour`: Number of days for which the data summarized every hour is stored.

  Note: 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.

  Note: 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. HPE 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. Transfer the contents of the `customConfig.cfg` file into a new `userConfig.cfg` file and save the new file in the same location.
5. In the new `userConfig.cfg` file, set the parameter `PRSPI_DataRetention_Raw` to modify the number of days for which the detailed data is stored.

   > **Note:** Modifying the retention period can have significant impact on the disk usage.
6. Save and close `customConfig.cfg` file.
7. 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" below.

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 the next page.

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. Create a new `userConfig.cfg` file in the same location and transfer the contents of the `customConfig.cfg` file into the new `userConfig.cfg` file.

5. In the new `userConfig.cfg` file, set the following parameters for each extension pack to tune the ETL for NPS:

   > **Note:** Increasing the tuning parameters for ETL process of NPS to values listed in tables below will result in significant increase in CPU utilization. Make sure that there is sufficient CPU bandwidth available before increasing these parameters.

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

   The number of child processes for the ETL process of NPS for medium and large tiers of traffic data based on different extension packs (`ETL_MaxChildProcs`):

Approximate managed environment tier	Interface_ Traffic	Interface_Traffic_1_ Minute	Interface_Traffic_ Aggregated
Medium	5	10	10
Large	10	50	20

   The maximum number of records per child process for the ETL process of NPS for medium and large tiers of traffic data based on different Extension Packs (`ETL_MaxRecordsPerChild`):

Approximate managed environment tier	Interface_ Traffic	Interface_Traffic_1_ Minute	Interface_Traffic_ Aggregated
Medium	100k	100k	100k
Large	100k	200k	200k

   The number of files per batch for the ETL process of NPS for medium and large tiers of traffic data based on different Extension Packs (`ETL_MaxMetricsFilesPerBatch`):

Approximate managed environment tier	Interface_ Traffic	Interface_Traffic_1_ Minute	Interface_Traffic_ Aggregated
Medium	20	25	20
Large	30	50	30

6. Save and close `userConfig.cfg` file.
7. 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.

Chapter 9: Maintaining Reports

The NNM iSPI Performance for Traffic enables you to view reports that provide you an insight into the network traffic and helps you monitor network performance by analyzing the traffic flow. All the reports are not available by default as enabling few of them may increase the load on the NNM iSPI Performance for Traffic and NPS. This section describes how to enable or disable these reports based on your requirements to enhance the performance of the NNM iSPI Performance for Traffic.

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

> **Note:** The Interface Traffic_1_min reports are disabled by default. For information on how to enable these reports, see the *Configuring Master Collectors* section in the *HP Network Node Manager iSPI Performance for Traffic Software Online Help*.

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. Open the `nms-traffic-leaf.address.properties` file with a text editor.
3. Add the `enable.subnet.report` property and set it to `true`.
4. Save and close the file.
5. 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 Data Collection for Reports for Top Destination Ports

Data collection for the following reports is disabled by default:

- Interface Traffic Aggregated Top Sources for Destination Port
- Interface Traffic Aggregated Top Destinations for Destination Port
- Interface Traffic Aggregated 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

> **Note:** 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.

> **Note:** The Interface Traffic_1_min reports are disabled by default. For information on how to enable these reports, see the *Configuring Master Collectors* section in the *HP Network Node Manager iSPI Performance for Traffic Software Software Online Help*.

To enable data collection for Top Destination Ports reports, 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

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

   OR

   ```
   %NNMDataDir%\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:
   ```
   topn.subtypes.dstport=true
   ```
   Addition of this line enables data collection for the `Top Conversations for Destination Port` reports.
6. Add the following line:
   ```
   enable.srcordst.dstport=true
   ```

Addition of this line enables data collection for the `Top Sources for Destination Port` and `Top Destinations for Destination Port reports`.

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

To disable data collection for Top Destination Ports reports, 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

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

   OR

   `%NNMDataDir%\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`

Chapter 10: 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.

Upgrading the Operating System of the Collector Systems

Before you perform an in-place operating system upgrade of Leaf Collector and Master Collector systems, stop the collector processes.

On the Master Collector system:

1. Log on as root or administrator.
2. Run the following command to stop the collector:

   On Windows

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

   On Linux

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

On the Leaf Collector system:

1. Log on as root or administrator.
2. Run the following command to stop the collector:

   On Windows

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

   On Linux

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

After the operating system upgrade is complete, run the following command to start the collectors:

- To start the Master Collector:

  On Windows

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

  On Linux

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

- To start the Leaf Collector:

On Windows

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

On Linux

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

Changing 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\traffic-master\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.nnm.host` property to the hostname of the NNMi management server.
5. Save and close the file.
6. Open the `nnm.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.

> **Note:** 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%\traffic-master\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</module-option><module-option name="password-stacking">useFirstPass</module-option> </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="password-stacking">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
```

> **Note:** If the Master Collector is configured for secure communication, 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 21.

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
```

> **Note:** If the Master Collector is configured for secure communication, 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 21.

16. Restart the Master Collector system.

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

> **Note:** 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
   `%NnmDataDir%\nmsas\traffic-leaf\` or `%TrafficInstallDir%\nmsas\traffic-leaf\`

On Linux
`/var/opt/OV/nmsas/traffic-leaf`

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` *`<nnm hostname>`* `-port 80 -u system -p` *`<passwd>`* `invoke com.hp.ov.nms.topo:service=NetworkApplication removeApplication traffic`
   b. `nnmtwiddle.ovpl -host` *`<nnm hostname>`* `-port 80 -u system -p` *`<NNMi system user passwd>`* `invoke com.hp.ov.nms.topo:service=NetworkApplication setApplicationService traffic` *`<master hostname - new one>`* `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
   `%NnmDataDir%\nmsas\traffic-master` or `%TrafficDataDir%\nmsas\traffic-master`

   On Linux
   `/var/opt/OV/nmsas/traffic-master`
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
   `%trafficinstalldir%\traffic-master\server` or `%nnminstalldir%\traffic-master\server`

On Linux

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

7. Open the `server.properties` file with a text editor.
8. Modify the value of `java.rmi.server.hostname` property to the hostname of the Master Collector.
9. Save and close the file.
10. 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`
11. Open the `nnm.extended.properties` file with a text editor.
12. Modify the value of the `com.hp.ov.nms.spi.traffic-master.spi.hostname` property to the hostname of the Master Collector.
13. Save and close the file.
14. Move the content of the `<NmmDataDir>\shared\nnm\certificates` to a different directory path if the Master Collector is not installed on the same system as NNMi.
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`

    > **Note:** 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 21.

    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`

> **Note:** 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 21.

16. 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\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 Leaf Collector.
5. Save and close the file.
6. Navigate to the following directory:
   On Windows
   `%NnmInstallDir%\nmsas\traffic-leaf\conf` or `%TrafficInstallDir%\nmsas\traffic-leaf\conf`

   On Linux
   `/opt/OV/traffic-leaf\conf`
7. Open the `nms-traffic-leaf.address.properties` file with a text editor.
8. Modify the value of `leaf.host` property to the hostname of the Leaf Collector.
9. Save and close the file.
10. Navigate to the following directory:
    On Windows
    `%NnmDataDir%\nmsas\traffic-leaf` or `%TrafficDataDir%\nmsas\traffic-leaf`

    On Linux
    `/var/opt/OV/nmsas/traffic-leaf`
11. Open the `server.properties` file with a text editor.
12. Modify the value of the `java.rmi.server.hostname` property to the hostname of the NNMi management server.
13. Save and close the file.
14. Move the content of the following directory to a different directory path if the Leaf Collector is configured for secure communication with the Master Collector:
    On Windows
    `%NnmDataDir%\shared\nnm\certificates`

    On Linux
    /var/opt/OVshared/nnm/certificates

15. Generate new certificates again using the following commands if the Leaf Collector is configured for secure communication with the Master Collector:
    On Windows
    a.
    ```
    “%NmInstallDir%>\nonOV\jdk\nnm\bin\keytool" -genkey -alias <Leaf
    FQDN>.selfsigned -keyalg rsa -sigalg SHA1withRSA -keysize 2048 -dname cn=<Leaf
    FQDN> -keypass nnmkeypass -validity 36500 -keystore
    “%NmnDataDir%\shared\nnm\certificates\nnm.keystore" -storepass nnmkeypass
    ```
    b.
    ```
    “%NmInstallDir%\nonOV\jdk\nnm\bin\keytool" -export -file
    “%NmnDataDir%\shared\nnm\certificates\nnm.cert" -keystore
    “%NmnDataDir%\shared\nnm\certificates\nnm.keystore" -alias <Leaf FQDN>.selfsigned
    -storepass nnmkeypass
    ```
    c.
    ```
    “%NmInstallDir%\nonOV\jdk\nnm\bin\keytool" -importcert -file
    “%NmnDataDir%\shared\nnm\certificates\nnm.cert" -keystore
    “%NmnDataDir%\shared\nnm\certificates\nnm.truststore" -storepass ovpass -noprompt
    ```

    > **Note:** If the Leaf Collector is configured for secure communication, you must import the certificates from the Leaf Collector to the `nnm.truststore` again. For more information, see "Enabling Secure Communication between the Master and the Leaf Collector" on page 27.

    On Linux
    a.
    ```
    “/opt/OV/nonOV/jdk/nnm/bin/keytool" -genkey -alias <Leaf FQDN>.selfsigned -keyalg
    rsa -sigalg SHA1withRSA -keysize 2048 -dname cn=<Leaf 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 <Leaf 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
    ```

    > **Note:** If the Leaf Collector is configured for secure communication, you must import the certificates from the Leaf Collector to the `nnm.truststore` again. For more information, see "Enabling Secure Communication between the Master and the Leaf Collector" on page 27.

16. Restart the Leaf Collector system.
17. Log on to the NNMi console with the administrator privileges.
18. Go to the **Configuration** workspace.
19. Double-click **NNM iSPI Performance for Traffic Configuration**. The NNM iSPI Performance for Traffic form opens.
20. Log on to the NNM iSPI Performance for Traffic form with the system user account created during the installation of the Master Collector.
21. 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*.

22. 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

For changes required on the NPS system, see the *Maintaining NPS* section in the *NNM iSPI Performance for Metrics Deployment Reference*.

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 *Preinstallation Tasks* in the *Installing the Master Collector* section in the *HP Network Node Manager iSPI Performance for Traffic Software Interactive 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
   `%NnmDataDir%\nmsas\traffic-master\conf` or `%TrafficDataDir%\nmsas\traffic-master\conf`

   On Linux
   `/var/opt/OV/nmsas/traffic-master/conf`
3. Open the `nps.extended.properties` with a text editor.
4. Modify the value of the following property:
   `com.hp.ov.nms.spi.traffic-master.nps.hostname`
5. Save and close the file.

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.

> **Note:** 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 *HPE 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 the Master Collector

Note: Before you restore the Master Collector database, you must reset the Master Collector database as described in "Resetting Master Collector Database" above.

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:

   On Windows

   *<Install_Dir>***\traffic-master\bin\nmstrafficmasterresetdb.ovpl**

   On Linux

   /opt/OV/traffic-master/bin/nmstrafficmasterresetdb.ovpl
4. 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 in "Backing up Master Collector" on page 72.

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 in "Backing up Master Collector" on page 72.

5. If the FQDN of the new system is different from the original Master Collector system (where you took the backup), follow the steps in "Changing the Master Collector Hostname" on page 67.
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`

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

Note: Before you restore the Leaf Collector database, you must reset the Leaf Collector database as described in "Resetting Leaf Collector Database" above.

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 in "Backing up Leaf Collector" on the previous page.

   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 in "Backing up Leaf Collector" on the previous page.

4. If the FQDN of the new system is different from the original Leaf Collector system (where you took the backup), follow the steps in "Changing the Leaf Collector Hostname" on page 69.
5. 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`

Chapter 11: 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.

Chapter 12: 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 Master Collector in the Global Manager can be configured to receive data from the Regional Master Collectors in the following ways:

- The Master Collector in the Global Manager can receive data from the Master Collector in the Regional Manager. In this case, you must add the regional Master Collector as a remote Master source in the global Master Collector. This ensures that the complete set of data received by the regional Master Collector is forwarded to the global Master Collector. In the above scenario the global Master Collector receives data processed by both Leaf Collector 1 and Leaf Collector 2.
- The Master Collector in the Global Manager can receive data directly from a regional Leaf Collector system, bypassing the regional Master Collector. In this case the regional Leaf Collector (Leaf Collector 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 Master Collector as well as the global Master Collector.

The regional Master Collector or the regional Leaf Collector) can only be configured to send data to the global 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.

Glossary

A

aggregated data

The Leaf Collector can aggregate raw data samples at every 5 minutes by applying the in-built aggregation rule. Raw data samples are collected from the flow records forwarded by different flow-exporting routers to the Leaf Collector. This data is used to build reports from the Interface_Traffic_Aggregated Extension Pack.

application

The NNM iSPI Performance for Traffic enables you to correlate traffic flows to applications that are running in your network environment. With the help of the NNM iSPI Performance for Traffic Configuration form, you can map each flow to an application.On Top Applications reports, the NNM iSPI Performance for Traffic provides a list of the applications that are associated with high volume of traffic flow.

C

conversation

A conversation is the process of transfer of data packets between two devices. The NNM iSPI Performance for Traffic can calculate the volume of data packet exchanged between two devices (that is, the volume of conversation) from the data available in IP flow records and highlights the node pairs with high volume of conversation on Top Conversations reports.

D

destination

A destination is a device or a system on the network that is capable of receiving data packets from other devices or systems.

F

flow

A flow or a 'traffic flow' is a sequence of data packets from one device or system to another device or system.

N

node pair

A 'node pair' is a pair of devices or systems that exchange data packets. The NNM iSPI Performance for Traffic can identify node pairs from the IP flow records collected by Leaf Collectors.

R

raw data

The raw data is the set of IP flow records that are exported by traffic flow-exporting routers on the network and collected by the NNM iSPI Performance for Traffic Leaf Collectors. By default, the NNM iSPI Performance for Traffic logs the raw data into the NPS database. In a medium or large-scale environment, it is recommended that you disable the logging of the raw data into the NPS database.

S

site

A logical organization of networking devices. On an enterprise network, a site can be a logical grouping of networking devices generally situated in similar geographic location. The location can include a floor, a building, or an entire branch office or several branch offices connected to another branch office via WAN/MAN. Each site is uniquely identified by its name. In case of the service provider networks, the Virtual Routing and Forwarding (VRF) on a Provider Edge (PE) router or a Customer Edge (CE) router can be defined as a site. Logically grouping networking devices into sites enables you to get an overview of your network performance.

site priority

An interface can be associated with only one site. While creating the site, you need to specify an ordering number for the site to resolve conflicts in case an interface matches multiple sites. The NNM iSPI Performance for Traffic associates the interfaces with a site that has the lowest ordering number. If you do not provide an ordering number for the site, the NNM iSPI Performance for Traffic assigns default ordering. Default ordering for a site is given the lowest priority. If an interface matches multiple sites, the site with the lower ordering gains priority to associate with the interface.

source

A source is a device or a system on the network that is capable of sending data packets to other devices or systems. From IP flow records, the NNM iSPI Performance for Traffic can identify the device or system from which each traffic flow originates.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Deployment Reference (Network Node Manager iSPI Performance for Traffic Software 10.20)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to network-management-doc-feedback@hpe.com.

We appreciate your feedback!