Hewlett Packard Enterprise

HPE Network Node Manager i Software

Software Version: 10.21
for the Windows® and Linux® operating systems

Hardening Guide

Document Release Date: May 2017
Software Release Date: November 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.

Oracle Technology — Notice of Restricted Rights

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

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

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Apple is a trademark of Apple Computer, Inc., registered in the U.S. and other countries.

AMD is a trademark of Advanced Micro Devices, Inc.

Google™ is a registered trademark of Google Inc.

Intel®, Intel® Itanium®, Intel® Xeon®, and Itanium® are trademarks of Intel Corporation in the U.S. and other countries.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Internet Explorer, Lync, Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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

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

sFlow is a registered trademark of InMon Corp.

UNIX® is a registered trademark of The Open Group.

Acknowledgements

This product includes software developed by the Apache Software Foundation. (http://www.apache.org).

This product includes software developed by the Visigoth Software Society (http://www.visigoths.org/).

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics

from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

Using this Guide

This document provides information for increasing the security of the following products:

- NNMi
- NNM iSPIs
- Network Performance Server (NPS)

The information in this document applies to NNMi 10.21. For security configuration for another version of the product, see the appropriate documentation for that version.

Unless otherwise specified within a procedure, the expected use model for the content in this document is as follows:

1. Stop all NNMi services (see "Start, Stop, or Restart All NNMi Services" on page 25).
2. Apply the desired configurations as described in this document.

   Note: Remember to back up each configuration file to a location outside the NNMi directory structure before making any changes.

3. Start all NNMi services (see "Start, Stop, or Restart All NNMi Services" on page 25).

Note: In an NNMi global network management (GNM), application failover, or high availability environment, work on one NNMi management server at a time. That is, on one NNMi management server, stop the NNMi services, apply changes, and then start the NNMi services on that NNMi management server. Exceptions to this approach are noted where applicable.

Note the following conventions used in this document:

- Some file paths include a <*PRODUCT*> directory. Replace <*PRODUCT*> with the value for the specific product you are configuring. Possible values are:
  - `nnm`
  - `qa`
  - `traffic-master`
  - `traffic-leaf`
  - `ipt`
  - `mcast`
  - `mpls`

- For NNMi and the HPE Network Node Manager i Software Smart Plug-ins (iSPIs), any configuration specified in the `server.properties` file overrides the default configuration. This file is located as follows:
  - *Windows*:

    `%NnmDataDir%\nmsas\<PRODUCT>\server.properties`

  - *Linux*:

    `/var/opt/OV/nmsas/<PRODUCT>/server.properties`

- For the Network Performance Server (NPS), any configuration specified in the `NNMPerformanceSPI.cfg` file overrides the default configuration. This file is located as follows:
  - *Windows*:

    `%NnmDataDir%\NNMPerformanceSPI\rconfig\NNMPerformanceSPI.cfg`

  - *Linux*:

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

HTTPS Communication Configuration

This topic describes the default security configurations for HTTPS communication within NNMi.

- By default, NNMi and the HPE Network Node Manager i Software Smart Plug-ins (iSPIs) support HTTPS with a self-signed certificate generated at the time of installation.

  Note: It is strongly recommended that a CA-signed certificate be installed to replace the default certificate. See the "Managing Certificates" chapter in the *HPE Network Node Manager i Software Deployment Reference* for more information.

- The default cryptographic protocol for HTTPS communication with the NNMi web server is TLSv1.2.

See "Enable HTTPS-Only Communication" on page 22 to configure NNMi to allow only HTTPS communication.

Configure Cryptographic Protocols for HTTPS Communication

By default, NNMi supports the TLSv1.2 protocol for HTTPS communication.

It is recommended that NNMi use only TLSv1.2 unless older, less secure, protocols are necessary for supporting legacy clients.

To configure NNMi to use protocols other than TLSv1.2, follow these steps:

1. Log on to the NNMi management server.
2. Open the following file with a text editor:
   - *Windows*:

     `%NnmDataDir%\nmsas\NNM\server.properties`

   - *Linux*:

     `/var/opt/OV/nmsas/NNM/server.properties`

3. Adding or updating the `com.hp.ov.nms.ssl.PROTOCOLS` property with a comma-separated list of the protocols that you want to use.

   For example, if you want to use the TLSv1, TLSv1.1, and TLSv1.2 protocols, make sure the following line exists in the `server.properties` file:

   ```
   com.hp.ov.nms.ssl.PROTOCOLS=TLSv1.0,TLSv1.1,TLSv1.2
   ```

4. Restart the NNMi processes by running the following commands:
   - *On Windows:*
     i. **%nnminstalldir%\bin\ovstop -c**
     ii. **%nnminstalldir%\bin\ovstart -c**
   - *On Linux:*
     i. **/opt/OV/bin/ovstop -c**
     ii. **/opt/OV/bin/ovstart -c**

Application Failover

In an application failover environment, NNMi always uses TLSv1.2 for communication between the NNMi management servers. This setting is not configurable.

Configuring SSL Communications for Web Access and RMI Communications

NNMi includes a suite of default ciphers that are used in configuring Secure Sockets Layer (SSL) in Web access and Java Remote Method Invocation (RMI) communications. The ciphers are listed in the `nms-jboss.properties` file.

Caution: Adding or removing ciphers from the cipher list without the approval of HPE is not supported; doing so may cause damage to the product or cause the product to become inoperable.

Requirement for New NNMi 10.2x Installations

New installations of NNMi support only TLS v1.2 protocol by default. However, to be able to discover and monitor ESXi 5.1 hypervisors, NNMi is required to use the TLSv1 cryptographic protocol.

To configure NNMi to support the TLSv1 cryptographic protocol for device communication:

Note: This procedure enables NNMi to use less secure cryptographic protocols that are not FIPS 140-2-certified. This is a global change and may reduce the security of the product.

1. Log on to the NNMi management server.
2. Open the following file with a text editor:
   - *Windows:* `%NnmDataDir%\nmsas\NNM\server.properties`
   - *Linux:* `/var/opt/OV/nmsas/NNM/server.properties`

3. Update the `com.hp.ov.nms.ssl.PROTOCOLS` property to include the value `TLSv1`.
   If the property does not exist, add the following line:
   `com.hp.ov.nms.ssl.PROTOCOLS=TLSv1.2,TLSv1.1,TLSv1`
4. Configure NNMi to allow protocols and algorithms that are not FIPS-certified:
   a. On the NNMi management server, go to the following directory:
      - *On Windows:* `%nnminstalldir%\newconfig\HPNmsServStgs\Windows`
      - *On Linux:* `/opt/OV/newconfig/HPNmsServStgs/Linux`
   b. Copy the `java.security` file, and then place the copied file in the following directory:
      - *On Windows:* `%nnmdatadir%\conf\nnm`
      - *On Linux:* `/var/opt/OV/conf/nnm`
5. Restart the NNMi processes by running the following commands:
   - *On Windows:*
     i. **%nnminstalldir%\bin\ovstop -c**
     ii. **%nnminstalldir%\bin\ovstart -c**
   - *On Linux:*
     i. **/opt/OV/bin/ovstop -c**
     ii. **/opt/OV/bin/ovstart -c**

Configuring NNMi to Enable or Disable SSLv3 Ciphers

You can modify the NNMi list of ciphers. However, ensure that the original information is preserved by copying the properties file discussed in this section to a different directory. NNMi disables SSLv3 ciphers by default. You might need to enable SSLv3 ciphers to resolve web browser communication issues. For example, you might receive a connection error similar to one of the following:

- Secure Connection Failed
- This page can't be displayed

If you are also using NNM iSPI software that resides on the NNMi management server and you enable SSLv3 ciphers for NNMi, you must also enable SSLv3 for each iSPI . See the Deployment Reference for each corresponding NNM iSPI for information about enabling and disabling SSLv3.

When making file changes under High Availability (HA), the location of the server.properties file that you need to update is: <*Shared_Disk*>`/NNM/dataDir/nmsas/NNM/server.properties`.

To configure NNMi to enable SSLv3 ciphers:

1. Open the following file:
   Windows: `%NnmDataDir%\nmsas\NNM\server.properties`
   Linux: `$NnmDataDir/nmsas/NNM/server.properties`
2. Edit the following line:
   `com.hp.ov.nms.ssl.PROTOCOLS = SSLv2Hello,TLSv1,TLSv1.1,TLSv1.2`
   to include SSLv3. For example:
   `com.hp.ov.nms.ssl.PROTOCOLS = SSLv2Hello,TLSv1,TLSv1.1,TLSv1.2,SSLv3`

Note: You can remove any protocols contained in this line.

3. Save the file.

Note: If you are also enabling SSLv3 for one or more iSPIs, make those changes before stopping and starting the NNMi management server as described in the next steps.

4. Stop the NNMi management server:

   Run the `ovstop` command on the NNMi management server.
5. Re-start the NNMi management server:

   Run the `ovstart` command on the NNMi management server.

To disable the SSLv3 ciphers after they have been enabled:

1. Open the following file:

   Windows: `%NnmDataDir%\nmsas\NNM\server.properties`

   Linux: `$NnmDataDir/nmsas/NNM/server.properties`
2. Edit the following line:

   ```
   com.hp.ov.nms.ssl.PROTOCOLS = SSLv2Hello,TLSv1,TLSv1.1,TLSv1.2,SSLv3
   ```

   to remove SSLv3. For example:

   ```
   com.hp.ov.nms.ssl.PROTOCOLS = SSLv2Hello,TLSv1,TLSv1.1,TLSv1.2
   ```
3. Save the file.

Note: If you are also disabling SSLv3 for one or more iSPIs after it has been enabled, make those changes before stopping and starting the NNMi management server as described in the next steps.

4. Stop the NNMi management server:

   Run the `ovstop` command on the NNMi management server.
5. Re-start the NNMi management server:

   Run the `ovstart` command on the NNMi management server.

Configuring NNMi Ciphers

For information about the ciphers that NNMi uses, see "Configure the Ciphers Used by the NNMi Web Server" in the *NNMi Hardening Guide*.

NNMi Data Encryption

NNMi incorporates data encryption in many areas of the product. For example:

- Application failover encrypts messages sent between cluster nodes.
- NNMi stores passwords for user accounts in the NNMi database in encrypted form.

- Global Network Management (GNM) encrypts messages sent between regional managers and the global manager.

NNMi uses a method of data encryption that spans several NNMi components. NNMi data encryption supports the following encryption types:

- symmetric encryption—both parties share the same secret key
- asymmetric—public and private key encryption where each side has the other side's public key, but they keep their own private key
- MessageDigest (hash)—one-way encryption (cannot decrypt) where arbitrarily long strings are reduced to fixed size strings

This topic describes the default security configurations for encryption and hashing within NNMi.

- A new installation of NNMi10.21 uses Federal Information Processing Standards (FIPS) 140-2-validated cryptographic module (RSA BSAFE) for encryption and key management.

  In an upgraded NNMi environment, FIPS-compliant ciphers and algorithms are automatically used for most password encryption and network communication procedures. However, some legacy ciphers and algorithms do exist in the upgraded environment that do not meet FIPS guidelines.
- During installation, NNMi generates a self-signed certificate using a 2048-bit encryption key, SHA 256, and RSA.

  Note: HPE recommends using a CA-signed certificate instead of the self-signed certificate provided by NNMi.
- For local authentication into NNMi, NNMi uses a salted SHA-256 password hash for storing NNMi user passwords.
- For encryption of device passwords stored in the NNMi database, NNMi uses the AES 128 algorithm.

Encryption Configuration Files

The NNMi encryption framework includes a set of files that can be edited to configure encryption settings for your organization. The files are in the following folder:

- Windows: `%NnmDataDir%\shared\nnm\conf\crypto`
- Linux: `$NnmDataDir/shared/nnm/conf/crypto`

Caution: The crypto configuration files are intended for advanced users. Use extreme caution when editing the crypto configuration files. Improper editing of these files cause serious issues. For example, any changes to the encryption parameters for application failover causes application failover to no longer function. Likewise, changes to system and database password encryption settings causes NNMi to no longer start. See the following sections for procedures to follow when changing crypto configurations for different NNMi subsystems.

Text Blocks in the Crypto Configuration Files

The crypto configuration files include the following text blocks:

`<allowed>`

The <allowed> block defines the types of providers, algorithms, and minimum key lengths that are allowed to be used elsewhere in the crypto configuration files.

Note: If you attempt to use an algorithm or key length that is not allowed, NNMi generates an encryption error.

Tip: A provider is a vendor (or entity) that provides implementations of cryptographic algorithms.

The algorithms listed in the crypto configuration files are associated with the providers listed in those files.

<default>

The <default> block lists default settings used for all supported components. For example, the <default> block lists a one symmetric algorithm, one asymmetric algorithm, and one digest. If a there is a component block defined for a given component, that component uses the algorithm specified in its component block (in other words, the component block definition overrides the <default> block). Otherwise, a component will request the default algorithm (from the <default> block) for the specific type of encryption used by that component.

Each component uses only one type of encryption (symmetric, asymmetric, or digest). For example, application failover uses only symmetric encryption, so specifying an asymmetric or digest algorithm in an application failover component block would be ineffective and unnecessary.

Note: A key size listed in a default block or component block must be at least the size listed in the <allowed> block (but it can be greater, if desired). For example, if the <allowed> block includes AES-128, then AES-192 is also valid. However, if the <allowed> block specifies AES-192, AES-128 is not valid.

Encryption and Application Failover

To make encryption configuration changes for application failover (for example, changing an encryption algorithm or key length) do the following:

1. Stop NNMi and nnmcluster processes by running the ovstop command on both nodes. Note that when you use the ovstop command on an NNMi management server configured for application failover, NNMi automatically runs the following command:

   ```
   nnmcluster -disable -shutdown
   ```

2. Edit the nnmcluster-crypto-config.xml file as desired.

   Note: Application failover uses only symmetric encryption, so adding asymmetric or digest does not have any effect, and removing symmetric causes a failure.

3. Save your changes to the nnmcluster-crypto-config.xml file.
4. Remove the old key file.

   Tip: The file location is defined in the nnmcluster-crypto-config.xml file.

5. Generate a new key file by running the following command:

   `nnmcluster -genkey`

6. Copy the edited `nnmcluster-crypto-config.xml` file and the new key file to the other node in the cluster (in the same folders).

   Now the `nnmcluster-crypto-config.xml` file, which defines the encryption algorithms and keys, is the same on both nodes. Also, the key itself is the same on both nodes.

7. Start the cluster again by running `nnmcluster` on the active and standby nodes:

   Run `nnmcluster -daemon` on the active node

   > **Note:** Wait until the node becomes active

   Run `nnmcluster -daemon` on the standby node

Note: If you do not remove the old key file, you might receive an error similar to the following:

```
Warning: Generating a new encryption key will require the NNMi Cluster to be
shutdown.

Do you wish to continue (y/n)?

y

Error: The attempt to generate a new encryption key failed.

The most likely cause is that the keysize was increased
and the current key is invalid.

Please remove the existing key and try again.
```

Encryption and User Account Passwords

Note: This information does not apply to Lightweight Directory Access Protocol (LDAP) or Common Access Card (CAC) accounts.

NNMi user accounts created using the NNMi console are stored in the NNMi database. The passwords for these users are hashed and stored in the database.

When users sign into the NNMi console, or use a command line interface (CLI) tool, the password that they provide is hashed and compared to the hashed value stored in the database. If the user provides the correct password, these two hashed strings match, and the user is authenticated.

Earlier versions of NNMi (9.x) used encryption algorithms for hashing user passwords, which are now considered outdated. NNMi uses a stronger algorithm for user account passwords. However, since hashes are one-way encryption, it is not possible to decrypt and then re-encrypt the user passwords during and upgrade from NNMi 9.x to 10.x.

On upgrade, all existing users still have their passwords stored in the database using the legacy encryption algorithm. However, when a user whose password has been hashed using the legacy algorithm successfully logs on, the password they provided is automatically re-encrypted using the new hash algorithm specified in the crypto configuration files.

This means all passwords are updated to the new algorithm slowly over time, as each user logs in for the first time after upgrade. The same is true if the crypto configuration is changed in the future. User passwords are upgraded to the new hash algorithm on the next successful logon.

- Upgrading user passwords depends on the presence of the earlier legacy algorithm (for example, MD5) listed in the `<allowed>` block. Therefore, keep the earlier legacy algorithm listed in the `<allowed>` block until all passwords have been migrated.
- Without the presence of the earlier legacy algorithm in the `<allowed>` block, the existing passwords hashed in the database are not able to be re-hashed. Therefore, associated users are not be able to log on, and NNMi is not able to re-encrypt passwords using the new algorithm.
- If the earlier legacy algorithm has been removed from the `<allowed>` block, the administrator must either delete and recreate the users affected, or reset the respective passwords for users whose passwords were encrypted with earlier legacy algorithms.

Use the following command to determine whether a user's password is using the algorithm listed in the crypto configuration file, or the user's password is encrypted with earlier legacy algorithms no longer specified in the crypto configuration file:

```
nnmsecurity.ovpl -listUserAccounts legacy
```

See the `nnmsecurity.ovpl` reference page, or the Linux manpage, for more information.

Providing a Password for Embedded Database Tools

To run embedded database tools (such as psql), NNMi requires a password. NNMi provides a default password, which the user should change using the `nnmchangeembdbpw.ovpl` script.

Note: You must be logged in as administrator on Windows systems or root on Linux systems to run the `nnmchangeembdbpw.ovpl` script. For more information, see the `nnmchangeembdbpw.ovpl` reference page, or the Linux manpage

If you have configured NNMi in an High Availability (HA) environment, run the `nnmchangeembdbpw.ovpl` script on the Primary Cluster Node only.

On the Primary Cluster Node only:

1. Place the Primary Cluster Node into maintenance mode.

   See "Maintenance Mode" on page 1 for more information about placing nodes in maintenance mode.
2. Stop all NNMi processes:

   Windows: `%NNM_BIN%\ovstop -c`

   Linux: `$NNM_BIN/ovstop -c`
3. Restart `nnmsdbmgr`:

   Windows: `%NNM_BIN%\ovstart nnmsdbmgr`

   Linux: `$NNM_BIN/ovstart nnmsdbmgr`
4. To change the embedded database password, run the `nnmchangeembdbpw.ovpl` script.

   Windows: `%NNM_BIN%\nnmchangeembdbpw.ovpl`

   Linux: `$NNM_BIN/nnmchangeembdbpw.ovpl`

5. To ensure the change is copied to the replication directory, so it can be copied to the Secondary Cluster Note, run the `nnmdatareplication.ovpl` script:

   Windows: %NNM_DATA%\misc\nnm\ha\nnmdatareplication.ovpl NNM

   Linux: $NNM_DATA/misc/nnm/ha/nnmdatareplication.ovpl NNM
6. Restart all NNMi processes:

   Windows: `%NNM_BIN%\ovstart`

   Linux: `$NNM_BIN/ovstart`
7. Take the Primary Cluster Node out of Maintenance Mode.
8. Fail over to the Secondary Cluster Node.

   Note: The Secondary Cluster Node must NOT be in Maintenance Mode in order to have the Postgres password replicated.

The application automatically copies the password to the Secondary Cluster Node when the NNMi Resource Group is started on this node.

Allowing Non-Root Linux Users to Start and Stop NNMi

Note: If the `/opt/OV` directory is on a partition with the `nosuid` option set, the non-root user feature is not available. See `/etc/fstab` to determine if the partition is configured with the `nosuid` option set.

NNMi provides a way to allow non-root Linux users to start and stop NNMi. Do the following:

1. As root, edit the following file:

   `$NnmDataDir/shared/nnm/conf/ovstart.allow`
2. Include the non-root users (one per line) that you want to be able to start and stop NNMi.
3. Save your changes.

Note: When making file changes under High Availability (HA), you need to make the changes on both nodes in the cluster. For NNMi using HA configurations, if the change requires you to stop and restart the NNMi management server, you must put the nodes in maintenance mode before running the `ovstop` and `ovstart` commands. See "Maintenance Mode" on page 1 for more information.

Hardening Device Communication

NNMi uses SNMP (v1, v2c, and v3) to communicates with many devices. This section guides you to configure NNMi to use only secure SNMPv3 for all SNMP communication.

Configure NNMi to Use SNMPv3

Discovery and communication using SNMPv3 is more secure since SNMPv3 requires user-based security model (USM) user names instead of SNMPv1/SNMPv2c community strings to authenticate messages that are sent between NNMi and SNMP agents. Follow the *Configuring Communication Protocol* section in *NNMi Help for Administrators* to configure NNMi to use only the SNMPv3 protocol to discover and communicate with devices.

Block SNMPv1 or SNMPv2c Traps

Despite configuring device discovery to use only SNMPv3, some managed nodes may still try to send SNMPv1 or SNMPv2c traps to the NNMi management server. To prevent any SNMPv1 or SNMPv2c traps from reaching the NNMi management server, it is recommended that you configure NNMi to accept only SNMPv3 traps and block all SNMPv1 and SNMPv2c traps.

Note: Before completing this configuration procedure, make sure that NNMi is configured to discover your network with the SNMPv3 protocol.

1. Log on to the NNMi management server.
2. Run the following command:
   On Windows: **"%nnminstalldir%\bin\nnmtrapconfig.ovpl -setProp disallowV1V2 -persist"**
   On Linux: **/opt/OV/bin/nnmtrapconfig.ovpl -setProp disallowV1V2 -persist**
3. Do one of the following:
   - *On Windows:* Restart the `NNM TrapReceiver` service from the Services window.
   - *On Linux:* Run the following commands:
     /etc/init.d/nettrap stop
     /etc/init.d/nettrap start

Configure Secure SNMPv3 Communication

If you plan to discover devices by using the SNMPv3 protocol, you must perform this additional procedure to achieve the FIPS-compliant mode of secure SNMPv3 communication.

1. Log on to the NNMi management server.
2. Take a backup of the following file:
   - *Windows:* `%nnmdatadir%\shared\nnm\conf\crypto\nms-snmpv3-crypto-config.xml`
   - *Linux:* `/var/opt/OV/shared/nnm/conf/crypto/nms-snmpv3-crypto-config.xml`
3. Go to the following directory:
   - *Windows:* `%nnminstalldir%\newconfig\HPOvNmsSnmpCo`
   - *Linux:* `/opt/OV/newconfig/HPOvNmsSnmpCo`
4. Save the `nms-snmpv3-crypto-config-fips.xml` file as `nms-snmpv3-crypto-config.xml` on the

system by following these steps:

- *Windows:*
  i. Open the `nms-snmpv3-crypto-config-fips.xml` file with a text editor.
  ii. Copy the content of the file.
  iii. Create a new `nms-snmpv3-crypto-config.xml` file.
  iv. Paste the copied content into the `nms-snmpv3-crypto-config.xml` file.
  v. Save the `nms-snmpv3-crypto-config.xml` file in the `%nnmdatadir%\shared\nnm\conf\crypto` directory.
- *Linux:*
  Run the following command:
  cp /opt/OV/newconfig/HPOvNmsSnmpCo/nms-snmpv3-crypto-config-fips.xml /var/opt/OV/shared/nnm/conf/crypto/nms-snmpv3-crypto-config.xml
- `/var/opt/OV/shared/nnm/conf/crypto`

Note: The older version of the `nms-snmpv3-crypto-config.xml` file gets overwritten at this step.

5. Restart NNMi.

Select a FIPS-Compliant Algorithm for SNMPv3 Communication

If you configured NNMi to discover devices by using the SNMPv3 protocol, make sure NNMi is configured to use one of the following FIPS-compliant algorithms for discovering SNMPv3 information:

- Authentication protocol:
  - SHA-1
- Privacy protocol:
  - Triple-DES
  - AES-128
  - AES-192
  - AES-256

If you use weaker algorithms after following the instructions in "Configure Secure SNMPv3 Communication" on the previous page, NNMi's communication with devices will fail.

If you did not select one of the algorithms listed above while configuring discovery and communication, do the following:

1. Log on to the NNMi console as an administrator.
2. From the Configuration workspace, launch the Communication Configuration form.

Note: See the *Configuring Communication Protocol* section in *NNMi Help for Administrators*.

3. Launch the SNMPv3 Settings form from the Communication Configuration form.
4. Set Authentication Protocol to SHA-1.
5. Set Privacy Protocol to Triple-DES, AES-128, AES-192, or AES-256.
6. Save the configuration.

Alternatively, you can use the `nnmcommunication.ovpl` command to select these protocols. The `-authProtocol` and `-privProtocol` parameters help you select the authentication and privacy protocols. For more information, see the reference page (from the NNMi help menu, click **Help > NNMi Documentation Library > Reference Pages**) or Linux man page of `nnmcommunication.ovpl`.

User Authentication

Users can authenticate into the NNMi console by using a local user account or by using one of several external authentication components. Each approach requires administrative setup.

Local user accounts

Local user accounts are specific to the NNMi installation only. NNMi does not support password policy configuration for local user accounts.

Note: If the security standards of your environment require a specific password policy (for example, minimum password length or password expiration), it is recommended to use an external mechanism for user authentication. See "External authentication" below.

For information about creating local NNMi user accounts, see "Configure User Accounts" in the NNMi help.

External authentication

The administrator of the external authentication component determines the security behaviors for all users and all applications that use that component.

See "Configure NNMi to Use LDAP or PKI User Authentication" on the next page to use an external authentication technique.

NNMi console session timeout

By default, the NNMi console session timeout is 18 hours. The NNMi administrator can change this value for all NNMi console users in the **Console Timeout** field on the User Interface Configuration form (**Configuration > User Interface > User Interface Configuration**).

Note: It is recommended to configure the session timeout in accordance with the policy for your environment.

Passwords

For information about changing the password of the embedded database, see "Providing a Password for Embedded Database Tools" in the HPE Network Node Manager i Software Deployment Reference.

Configure NNMi to Use LDAP or PKI User Authentication

It is recommended that NNMi be integrated with a directory service through Lightweight Directory Access Protocol (LDAP) or configured to use Public Key Infrastructure (PKI) user authentication.

Follow the instructions in the one of the following sections in the *NNMi Deployment Reference*:

- *Integrating NNMi with a Directory Service through LDAP*
- *Configuring NNMi to Support Public Key Infrastructure User Authentication*

Change Default NPS Passwords

The NNM iSPI Performance for Metrics installer installs NPS with the following three applications with preset passwords:

- NPS database
- NPS BI Server
- NPS Software Development Kit (SDK)

To enhance the security of your monitoring environment, change all the three preset passwords.

Change the NPS Database Password

To change the NPS database password, run the following command:

changeDBpwd.ovpl <*password*>

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

Change the NPS BI Server Password

To change the NPS BI Server password, run the following command:

changeBIpwd.ovpl <*password*>

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

Change the NPS SDK Password

To change the NPS SDK password, run the following command:

changesdkUserPwd.ovpl-u<*username*>**-p**<*password*>

In this instance, <*username*> is the user name and <*password*> is a password of your choice.

Note: The `changesdkUserPwd.ovpl` command always requires you to provide a value for the user name. If you want to change only the password of the NPS SDK password, specify the old user name with the command.

Change the NNMi Embedded Database Password

NNMi provides a default password, which can be changed using the `nnmchangeembdbpw.ovpl` script.

For more information, see the *Providing a Password for Embedded Database Tools* section in the *NNMi Deployment Reference*.

Clickjacking Protection

NNMi is configured for linked pages to open in new frames when the links are from the SAMEORIGIN as the NNMi management server. This configuration is not changeable.

Configuring NNMi to Use FIPS 140-2-Validated Cryptographic Modules

This section explains how to configure NNMi to use Federal Information Processing Standards (FIPS) 140-2-validated cryptographic modules. FIPS guidelines provide a standard for security requirements for cryptographic modules defined by the National Institute of Standards Technology (NIST). This section explains how to configure NNMi to use cryptographic modules that are compliant with FIPS requirements.

Note: You can configure only NNMi Premium (that is NNMi, NNM iSPI Performance for Metrics, and NNM iSPI Performance for QA) to be FIPS-compliant.

To be able to meet the requirements of the FIPS 140-2 standards, NPS and NNMi must be installed on the same server.

A new installation of NNMi 10.21 uses FIPS 140-2-validated cryptographic module (RSA BSAFE) for encryption and key management and supports Public Key Cryptography Standards #12 (PKCS #12) certificates. A new command—`nnmkeytool.ovpl`—helps in managing this PKCS #12 certificates. For more information about managing new PKCS #12 certificates, see the *Managing Certificates* section in the *NNMi Deployment Reference*.

In an upgraded NNMi environment, FIPS-compliant ciphers and algorithms are automatically used for most password encryption and network communication procedures. However, some legacy ciphers and algorithms do exist in the upgraded environment that do not meet FIPS guidelines.

To achieve the highest level of FIPS 140-2-validated cryptography, do the following:

- Use a new installation of NNMi 10.21
- By default, NNMi installs a self-signed certificate. HPE recommends that you use CA-signed certificates and not the self-signed certificate. For more information about using the CA-signed certificates, see the *Advanced Configuration* section in the *NNMi Deployment Reference*.
- Follow configuration steps to disable some weaker SNMPv3 ciphers that are not FIPS-certified.
- Use only NNMi Premium.
- Install NNMi and NPS on the same system.

Note: Despite meeting the requirements listed above, the following components of NNMi and NPS do not use the FIPS 140-2-validated cryptography: remote access to the NPS Console, Performance Troubleshooting window, and Performance tab of the Analysis pane in the NNMi Console

This section provides you with the steps to configure NNMi to use the highest level of FIPS 140-2-validated cryptography.

Prerequisite

Make sure to disable the HTTP mode of communication. See "Enable HTTPS-Only Communication" on page 22 for more information.

Configure NNMi

Perform the following tasks to configure NNMi to use FIPS 140-2-validated cryptographic modules:

1. Task 1: Post-Upgrade Procedure: Encryption of Passwords

   This procedure is relevant only if you upgraded to NNMi10.21 from an older version of NNMi.

   If you did not use the `nnmsetcmduserpw.ovpl` command before upgrading NNMi to 10.21, skip this procedure.

   > **Tip:** Read the reference page of the `nnmsetcmduserpw.ovpl` command for more information.

   If you used the `nnmsetcmduserpw.ovpl` command to configure a valid NNMi User Name attribute value and NNMi Password attribute value to seamlessly run command line tools, you must follow these steps:

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

   b. Run the `nnmsetcmduserpw.ovpl` command again to configure all the NNMi credentials that were set before the upgrading NNMi to the version 10.21.

      > **Tip:** To find out all the users whose passwords were encrypted by using the `nnmsetcmduserpw.ovpl` command prior to upgrading NNMi to 10.21, find the `nms-users.properties` file, and then check the content of the file. Multiple copies of the `nms-users.properties` file may exist on the server.

2. "Configure Secure SNMPv3 Communication" on page 15
3. "Select a FIPS-Compliant Algorithm for SNMPv3 Communication" on page 16

Restrict Remote Access to the NPS Databases

> **Note:** Follow the instructions in this section only if NNMi and NPS are installed on the same server.

NPS uses an embedded database to store the performance data collected by NNMi and iSPIs for building reports. NPS uses another database, known as the Content Store, to store and maintain all the details of Extension Packs and reports. This procedure enables you to prevent remote systems to access these two databases.

The NPS databases use the following ports:

- 9301
- 9303
- 9306

This procedure helps you configure the firewall running on the NNMi management server to block communication through these ports.

To restrict remote access to the embedded NPS data store:

On Windows:

Use the Windows Firewall program to block remote communication though the 9303 and 9306 ports. For more information, see the Microsoft Windows documentation.

On Linux:

1. Log on to the NNMi management server as root.
2. Run the following commands:
   a. **service iptables start**
   b. **iptables -A INPUT -p tcp -i eth+ --dport 9303 -j REJECT**
   c. **iptables -A INPUT -p tcp -i eth+ --dport 9306 -j REJECT**
   d. **service iptables save**

To restrict remote access to the Content Store:

1. Log on to the NNMi management server as root or administrator.
2. Open the following file with a text editor:
   - *On Windows:* `%nnminstalldir%\nonOV\sybasease\interface`
   - *On Linux:* `/opt/OV/nonOV/sybasease/interfaces`
   - Make sure the following lines do not contain any external IP address or hostnames:

```
ASECONTENTSERVER
                    master tcp ether 127.0.0.1 9301
                    query tcp ether 127.0.0.1 9301
ASECONTENTSERVER_BS
                    master tcp ether localhost 9308
                    query tcp ether localhost 9308
```

Configure the NPS Console

Note: Follow the instructions in this section only if NNMi and NPS are installed on the same server.

In addition to disabling remote access to NPS databases, you can configure the NPS console to restrict users from launching the BI Server portal from remote systems by following these steps:

1. Log on to the NNMi management server.
2. Open the following file with a text editor:
   a. *Windows:* `%ovdatadir%\NNMPerformanceSPI/rconfig/NNMPerformanceSPI.cfg`
   b. *Linux:* `/var/opt/OV/NNMPerformanceSPI/rconfig/NNMPerformanceSPI.cfg`
3. To prevent users from launching the BI Server portal from remote systems, set the `CC_DISABLE_REMOTE_COGNOS_ADMINISTRATION` to `true`.
4. Save the file.
5. Restart the BI Server by running the following commands:

a. **stopBI.ovpl**
b. **startBI.ovpl**

You are now no longer able to use the menu items under the BI Server workspace in the NPS console.

Note: You can still log on to the NPS system, launch the NPS console with a local browser, and then use the BI Server workspace.

Auditing

Auditing of user actions is enabled by default for NNMi, NPS, and the NNM iSPI Performance for QA.

For more information about audit log files of NNMi, see the *NNMi Online Help*.

For more information about audit log files of NPS and the NNM iSPI Performance for Metrics, see the NNM iSPI Performance for Metrics *Online Help*.

For more information about audit log files of the NNM iSPI Performance for QA, see the *NNM iSPI Performance for QA Online Help*.

Strengthen Security

You can strengthen the security of NNMi by applying any or all of the following changes:

- "Enable HTTPS-Only Communication" below
- "Configure the Ciphers Used by the NNMi Web Server" on the next page
- "Application Failover: Configure the Ciphers Used by the NNMi Web Server" on page 24
- "Limit User Access to the NNMi Web Server" on page 25
- Strengthen Security of NPS

Enable HTTPS-Only Communication

Enable HTTPS-Only Communication for NNMi

The HTTP mode of communication can still be used even after installing and configuring NNMi to use HTTPS communication. To be able to restrict remote access to NNMi via HTTP, completely disable NNMi's HTTP mode of communication by following the instructions in the *Configuring NNMi to Require Encryption for Remote Access* section in the *NNMi Deployment Reference*.

Note: In a Global Network Management environment, perform this task on each regional manager and the global manager.

Enable HTTPS-Only Communication for NPS

Make sure that NPS is installed and configured to use only the HTTPS protocol.
To switch to HTTPS from HTTP communication:

1. Log on to the NPS system as root or administrator.
2. Run the following command:
   configureWebAccess.ovpl -ssl

Enable HTTPS-Only Communication for the NNM iSPI Performance for QA

1. Edit the following file (create the file if it does not exist) on the NNMi management server:
   - *Windows:* `%NnmDataDir%\nmsas\qa\server.properties`
   - *Linux:* `/var/opt/OV/nmsas/qa/server.properties`
2. Add the following four lines to the `server.properties` file:

   ```
   nmsas.server.net.bind.address = 127.0.0.1
   nmsas.server.net.bind.address.ssl = 0.0.0.0
   nmsas.server.net.hostname = localhost
   nmsas.server.net.hostname.ssl = ${com.hp.ov.nms.fqdn}
   ```
3. Restart NNMi and the NNM iSPI Performance for QA by running the following commands:
   - *Windows*
     i. **%nnminstalldir%\bin\ovstop**
     ii. **%nnminstalldir%\bin/ovstart**
   - *Linux*
     i. **/opt/OV/bin/ovstop**
     ii. **/opt/OV/bin/ovstart**

Configure the Ciphers Used by the NNMi Web Server

NNMi supports the following ciphers for secure communications with the NNMi web server.

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

To change the list of protocols that NNMi can use, uncomment and configure the `com.hp.ov.nms.ssl.CIPHERS` parameter in the following file:

- *Windows*:

  `%NnmDataDir%\shared\<PRODUCT>\conf\props\nms-jboss.properties`

- *Linux*:

  `var/opt/OV/shared/<PRODUCT>/conf/props/nms-jboss.properties`

This parameter contains an ordered list of one or more ciphers. If NNMi is unable to use the first cipher in the list to establish a connection between the NNMi web server and the user's web browser, NNMi tries to use the next cipher, and so forth. (The preceding list shows the default cipher ordering.)

You can edit the value of the `com.hp.ov.nms.ssl.CIPHERS` parameter to delete ciphers that NNMi should not use and to change the order in which NNMi attempts to use the available ciphers.

If you change the list of supported ciphers, HPE recommends ordering the ciphers list in order of strength. That is, place 256-bit encryption above 128-bit encryption.

Note:

- The value of the `com.hp.ov.nms.ssl.CIPHERS` parameter must be a comma-separated list that contains no white space and is one contiguous line.
- Save the cipher list before changing it. Removing ciphers from the `com.hp.ov.nms.ssl.CIPHERS` list can prevent NNMi from starting.
- The web browser must support at least one of the configured ciphers.
- In a GNM environment, modify the file on one NNMi management server, and then copy the revised file to the other NNMi management servers in the GNM environment. After the file is in place on all NNMi management servers, restart all NNMi management servers.

  In a high availability environment, modify the file on the active NNMi management server only.

Application Failover: Configure the Ciphers Used by the NNMi Web Server

In an application failover environment, cipher configuration of the application failover fileIO port uses the `com.hp.ov.nms.cluster.ssl.CIPHERS` parameter in the following file:

- *Windows*:

  `%NnmInstallDir%\misc\<PRODUCT>\props\shared\nms-cluster.properties`

- *Linux*:

  `/opt/OV/misc/<PRODUCT>/props/shared/nms-cluster.properties`

Modify the file on one NNMi management server, and then copy the revised file to the other NNMi management server in the application failover cluster.

The supported ciphers and the configuration considerations are the same as described in "Configure the Ciphers Used by the NNMi Web Server" on the previous page.

Limit User Access to the NNMi Web Server

It is recommended to limit traffic to the NNMi web server to only those users who should have access. Possible ways to limit this traffic include:

- Configure a firewall in front of the NNMi management server.

  For information about the ports that NNMi uses, see "NNMi and NNM iSPI Default Ports" in the *NNMi Deployment Guide*.
- Isolate user access to the NNMi management server on specific network interfaces only.

Start, Stop, or Restart All NNMi Services

Stopping the NNMi services before changing the NNMi configuration prevents conflicting data from being stored in the NNMi database. Some procedures call for restarting the NNMi services to read the updated configuration.

Tip: The `ovstart` and `ovstop` commands apply to all of the following products (if installed in your environment):

- NNMi
- NNM iSPI for IP Telephony
- NNM iSPI for MPLS
- NNM iSPI for IP Multicast
- NNM iSPI Performance for QA

For information about NNM iSPI Performance for Traffic, see "Start, Stop, or Restart All NNM iSPI Performance for Traffic Services" on page 27.

Follow the instructions specific to your environment:

- "One NNMi management server or GNM" below
- "Application failover" on the next page
- "High availability" on page 27

One NNMi management server or GNM

To start all NNMi services

- *Windows*: Do one of the following:
  - From the Windows Start menu, run **All Programs > HP > Network Node Manager > ovstart**.
  - Run the following command:

    `%NnmInstallDir%\bin\ovstart`
- *Linux*: Run the following command:

  `/opt/OV/bin/ovstart`

To stop all NNMi services

- *Windows*: Do one of the following:
  - From the Windows Start menu, run **All Programs > HP > Network Node Manager > ovstop**.
  - Run the following command:

    %NnmInstallDir%\bin\ovstop
- *Linux*: Run the following command:

  /opt/OV/bin/ovstop

To restart all NNMi services

- *Windows*: Do one of the following:
  - From the Windows Start menu, run **All Programs > HP > Network Node Manager > ovstop**, and then run **All Programs > HP > Network Node Manager > ovstart**.
  - Run the following commands:

    %NnmInstallDir%\bin\ovstop

    %NnmInstallDir%\bin\ovstart
- *Linux*: Run the following commands:

  /opt/OV/bin/ovstop

  /opt/OV/bin/ovstart

Application failover

To start all NNMi services

- *Windows*: Run the following command:

  %NnmInstallDir%\bin\ovstart
- *Linux*: Run the following command:

  /opt/OV/bin/ovstart

To stop all NNMi services

- *Windows*: Run the following command:

  %NnmInstallDir%\bin\ovstop
- *Linux*: Run the following command:

  /opt/OV/bin/ovstop -nofailover

To restart all NNMi services

- *Windows*: Run the following commands:

  %NnmInstallDir%\bin\ovstop -nofailover

  %NnmInstallDir%\bin\ovstart
- *Linux*: Run the following commands:

  /opt/OV/bin/ovstop -nofailover

  /opt/OV/bin/ovstart

High availability

See "Maintaining the High Availability Configuration" in the *NNMi Deployment Reference*.

Start, Stop, or Restart All NNM iSPI Performance for Traffic Services

Stopping the NNM iSPI Performance for Traffic services before changing the NNM iSPI Performance for Traffic configuration prevents conflicting data from being stored in the NNM iSPI Performance for Traffic database. Some procedures call for restarting the NNM iSPI Performance for Traffic services to read the updated configuration. Follow the instructions specific to your environment:

- "Master collector on a standalone server (but not in a high availability cluster)" below
- "Master collector on the NNMi management server (but not in a high availability cluster)" below
- "Master collector in a high availability cluster" on the next page
- "Leaf collector on another server" on the next page
- "Leaf collector on the NNMi management server" on page 29

Master collector on a standalone server (but not in a high availability cluster)

To start an NNM iSPI Performance for Traffic master collector

- *Windows*: Verify that the NNMi services are running, and then run the following command:

  `%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl`
- *Linux*: Verify that the NNMi services are running, and then run the following command:

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

To stop an NNM iSPI Performance for Traffic master collector

- *Windows*: Run the following command:

  `%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl`
- *Linux*: Run the following command:

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

To restart an NNM iSPI Performance for Traffic master collector

- *Windows*: Verify that the NNMi services are running, and then run the following commands:

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

  `%TrafficInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl`
- *Linux*: Verify that the NNMi services are running, and then run the following commands:

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

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

Master collector on the NNMi management server (but not in a high availability cluster)

To start an NNM iSPI Performance for Traffic master collector

- *Windows*: Verify that the NNMi services are running, and then run the following command:

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

- *Linux*: Verify that the NNMi services are running, and then run the following command:

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

To stop an NNM iSPI Performance for Traffic master collector

- *Windows*: Run the following command:

  %NnmInstallDir%\traffic-master\bin\nmstrafficmasterstop.ovpl
- *Linux*: Run the following command:

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

To restart an NNM iSPI Performance for Traffic master collector

- *Windows*: Verify that the NNMi services are running, and then run the following commands:

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

  %NnmInstallDir%\traffic-master\bin\nmstrafficmasterstart.ovpl
- *Linux*: Verify that the NNMi services are running, and then run the following commands:

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

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

Master collector in a high availability cluster

Before stopping the traffic master services, disable high availability resource group monitoring by creating the required maintenance file. See "Deploying the NNM iSPI Performance for Traffic in a High-Availability Cluster" in the *NNM iSPI Performance for Traffic Deployment Reference*.

Leaf collector on another server

To start an NNM iSPI Performance for Traffic leaf collector

- *Windows*: Verify that the NNMi services are running, and then run the following command:

  %TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
- *Linux*: Verify that the NNMi services are running, and then run the following command:

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

To stop an NNM iSPI Performance for Traffic leaf collector

- *Windows*: Run the following command:

  %TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
- *Linux*: Run the following command:

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

To restart an NNM iSPI Performance for Traffic leaf collector

- *Windows*: Verify that the NNMi services are running, and then run the following commands:

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

  %TrafficInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
- *Linux*: Verify that the NNMi services are running, and then run the following commands:

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

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

Leaf collector on the NNMi management server

To start an NNM iSPI Performance for Traffic leaf collector

- *Windows*: Verify that the NNMi services are running, and then run the following command:
  %NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
- *Linux*: Verify that the NNMi services are running, and then run the following command:
  /opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl

To stop an NNM iSPI Performance for Traffic leaf collector

- *Windows*: Run the following command:
  %NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
- *Linux*: Run the following command:
  /opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl

To restart an NNM iSPI Performance for Traffic leaf collector

- *Windows*: Verify that the NNMi services are running, and then run the following commands:
  %NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstop.ovpl
  %NnmInstallDir%\traffic-leaf\bin\nmstrafficleafstart.ovpl
- *Linux*: Verify that the NNMi services are running, and then run the following commands:
  /opt/OV/traffic-leaf/bin/nmstrafficleafstop.ovpl
  /opt/OV/traffic-leaf/bin/nmstrafficleafstart.ovpl

Send Documentation Feedback

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

Feedback on Hardening Guide (Network Node Manager i Software 10.21)

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!