HP Network Node Manager i Software

Software Version: 10.10
Windows® and Linux® operating systems

Hardening Guide

Document Release Date: November 2015
Software Release Date: November 2015

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

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/).

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.hp.com

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:
https://hpp12.passport.hp.com/hppcf/createuser.do

Or click the **Register** link at the top of the HP Software Support page.

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

Support

Visit the HP Software Support Online web site at: **https://softwaresupport.hp.com**

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

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

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

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

https://hpp12.passport.hp.com/hppcf/createuser.do

To find more information about access levels, go to:

https://softwaresupport.hp.com/web/softwaresupport/access-levels

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Using this Guide

This document provides information for increasing the security of your NNMi installation. The information in this document applies to NNMi 10.10. 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 16).
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 16).

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 HP 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`

Communication Configuration

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

- By default, NNMi and the HP Network Node Manager i Software Smart Plug-ins (iSPIs) use HTTP for communication with the web browser.

  Note: It is recommend to enable HTTPS communication for each product as described in the product documentation.

- The default SSL protocols for HTTPS communication with the NNMi web server are TLSv1.0, TSLv1.1 and TLSv1.2.

  Note: It is recommended to disable TLSv1.0 and TLSv1.1 unless they are needed for communicating with applications that do not support TLSv1.2. For instructions, see "Configure TLS Protocols" below.

Configure TLS Protocols

By default, NNMi supports the follow protocols:

- SSLv2Hello
- TLSv1.0
- TLSv1.1
- TLSv1.2

It is recommended to disable TLSv1.0 and TLSv1.1 unless they are needed for communicating with applications that do not support TLSv1.2.

Configure the protocols to use with the `com.hp.ov.nms.ssl.PROTOCOLS` parameter in the following file:

- *Windows*:

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

- *Linux*:

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

Application Failover

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

Encryption

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

- During installation, NNMi generates a self-signed certificate using a 2048-bit encryption key, SHA 256, and RSA.

  Note: HP 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.

For more information, see "NNMi Data Encryption" in the *HP Network Node Manager i Software Deployment Reference*.

Passwords

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

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.

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.

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.

Strengthen Security

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

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_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_HA384
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256

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, HP 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 an 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.

Disable the JMX Console

It is recommended to disable the JMX console until it is needed for troubleshooting purposes.

Note: For the NNM iSPI Performance for Traffic, you must perform this task on the Master Collector system and each Leaf Collector system.

The NNM iSPI Performance for Metrics does not provide a JMX console, and, therefore, you need not perform this task for the NNM iSPI Performance for Metrics.

To disable access to the JMX console, add the following content:

```
<!-- disable the jmx-console -->
<realm name="jmx-console">
    <mode>NO_ACCESS</mode>
</realm>
```

inside the `realms` block of the following file:

- *Windows*:

  `%NnmDataDir%\nmsas\<PRODUCT>\conf\nms-auth-config.xml`
- *Linux*:

  `var/opt/OV/nmsas/<PRODUCT>/conf/nms-auth-config.xml`

For example:

```
<!-- realms describes the configuration of specific services or applications -->
<realms>
    <!-- valid modes are X509 or FORM -->
    <realm name="console">
        <mode>FORM</mode>
    </realm>
    <!-- disable the jmx-console -->
    <realm name="jmx-console">
        <mode>NO_ACCESS</mode>
    </realm>
</realms>
```

Then, run the appropriate command to re-read the `nms-auth-config.xml` file:

- NNMi: **`nnmsecurity.ovpl -reloadAuthConfig`**
- NNM iSPI Performance for QA: **`nmsqaauthconfigreload.ovpl -reloadAuthConfig`**
- NNM iSPI Performance for Traffic Master Collector: **`nmsmasterauthconfigreload.ovpl -reloadAuthConfig`**
- NNM iSPI Performance for Traffic Leaf Collector: **`nmsleafauthconfigreload.ovpl -reloadAuthConfig`**
- NNM iSPI for IP Telephony: **`nmsiptauthconfigreload.ovpl -reloadAuthConfig`**
- NNM iSPI for MPLS: **`nmsmplsauthconfigreload.ovpl -reloadAuthConfig`**
- NNM iSPI for IP Multicast: **`nmsmcastauthconfigreload.ovpl -reloadAuthConfig`**

To re-enable the JMX console for troubleshooting, comment out the preceding configuration, and the re-run reload command.

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 Quality Assurance

For information about NNM iSPI Performance for Traffic, see "Start, Stop, or Restart All NNM iSPI Performance for Traffic Services" on page 18.

Follow the instructions specific to your environment:

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

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 availabililty

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 20

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 10.10)

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!