HP Network Node Manager i Software

For the Windows®, HP-UX, Linux, and Solaris operating systems

Software Version: NNMi 9.20

HP Network Node Manager i Software—HP Network Automation Integration Guide

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2008–2012 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

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

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

UNIX® is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

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

Acknowledgements

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

This product includes software developed by the Indiana University Extreme! Lab. (http://www.extreme.indiana.edu)

Available Product Documentation

In addition to this guide, the following documentation is available for NNMi:

- *HP Network Node Manager i Software Documentation List*—Available on the HP manuals web site. Use this file to track additions to and revisions within the NNMi documentation set for this version of NNMi. Click a link to access a document on the HP manuals web site.

- *NNMi Installation Guide*—This is an interactive document, and is available on the NNMI 9.20 product media.
  See the nnmi_interactive_installation_en_README.txt file, located on the product media, for more information.

- *HP Network Node Manager i Software Upgrade Reference*—Available on the HP manuals web site.

- *HP Network Node Manager i Software Release Notes*—Available on the product media and the NNMi management server.

- *HP Network Node Manager i Software System and Device Support Matrix*—Available on the product media and the NNMi management server.

- *HP Network Node Manager iSPI Network Engineering Toolset Planning and Installation Guide*— Available on the NNM iSPI NET diagnostics server product media.

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

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

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

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

Or click the **New users - please register** link on the HP Passport sign-in 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.

Contents

HP Network Automation

HP Network Automation software (HP NA) tracks, regulates, and automates configuration and software changes across globally distributed, multi-vendor networks through process-powered automation.

For information about purchasing HP NA, contact your HP sales representative.

This document contains the following topics:

- HP NNMi–HP NA Integration
- Enabling the HP NNMi–HP NA Integration
- Configuring Single Sign-On Between NNMi and HP NA
- Using the HP NNMi–HP NA Integration
- Changing the HP NNMi–HP NA Integration
- Disabling the HP NNMi–HP NA Integration
- Troubleshooting the HP NNMi–HP NA Integration
- Application Failover and the HP NNMi–HP NA Integration
- HP NNMi–HP NA Integration Configuration Form Reference
- HP NNMi Integration Configuration in HP NA Reference

HP NNMi–HP NA Integration

The HP NNMi–HP NA integration combines the HP NA configuration change detection capabilities with the HP NNMi network monitoring capabilities, placing more information at your fingertips when problems occur.

▶ The HP NNMi integration with Cisco Systems Network Compliance Manager (NCM) works in the same way as the HP NNMi–HP NA integration. The information in this document also applies to the HP NNMi–Cisco Systems NCM integration.

The integration provides the following functionality:

- Synchronizes the HP NNMi and HP NA topologies for lower ownership cost and better management coverage of provisioned devices.

- Automatically runs HP NA device diagnostics when certain NNMi incidents occur.

- Prevents unnecessary alarming in HP NNMi while devices are out of service as HP NA applies device configuration updates.

- Updates the NNMi configuration with information for accessing managed devices.

- The NNMi Analysis Pane shows NA node and interface information.

Additionally, without exiting the NNMi console, you can connect to HP NA to view information about NA-managed devices and configuration change events. While in HP NA, you can perform any NA functions for which you have the necessary credentials.

The HP NNMi–HP NA integration adds menu items to the NNMi console for opening connections to HP NA and for viewing configuration information on devices managed by HP NA. These tools provide the following functionality:

- View detailed device information, including vendor, model, modules, operating system version, and recent diagnostic results.

- View device configuration changes and configuration history.

- Compare configurations (typically the most recent and last previous configurations) to see what changed, why, and who made the changes.

- View device compliance information.

- Run NA diagnostics and command scripts from NNMi nodes.

- Detect connections with mismatched speed or duplex configurations.

▶ The HP NNMi–HP NA integration does not support devices using IPv6 addresses as management addresses or dual-stacked devices with the SNMP management address preference set to IPv6.

▶ These features are not available for network devices that are not configured in HP NA or for NA devices for which change detection is disabled.

▶ The HP NNMi–HP NA integration cannot distinguish among duplicate IP addresses. For this reason, the integration is not supported in overlapping address domain (OAD) environments.

Value

The HP NNMi–HP NA integration provides the following features and benefits in an environment already running both HP NNMi and HP NA:

- Alarm integration—The HP NNMi–HP NA integration communicates HP NA configuration change information to the NNMi console, enabling you to quickly identify whether configuration changes might have caused network problems. From within HP NNMi, you can quickly access HP NA functionality to view specific configuration changes and device information, identify who made the change, and roll back to the previous configuration to restore network operation. Because a majority of network outages are caused by device configuration errors, this feature can enhance both problem identification and response time in resolving network downtime.

- Access to HP NA configuration history from HP NNMi—In the NNMi console, a device-level menu provides access to HP NA features for reviewing configuration changes. For any device in the HP NA database, this feature displays configuration changes side-by-side so that you can easily view changes. You can also view configuration history.

- Operations efficiency—Network operations personnel can monitor and investigate information from two data sources within a single screen.

Integrated Products

The information in this document applies to the following products:

- HP NA

For the list of supported versions, see the *NNMi System and Device Support Matrix*.

- NNMi 9.20

The NNM iSPI NET license is no longer required for this integration.

Integration Configuration Details

The integration is limited to one HP NA server connected with one NNMi management server. HP NNMi and HP NA must be in the same network segment (also called an NA realm).

HP NNMi and HP NA can be installed on the same computer or on different computers.

For HP NNMi and HP NA to run correctly on the same computer, you must install HP NNMi before installing HP NA. If you install HP NA before installing HP NNMi, the HP NNMi installation reports a port conflict with HP NA and does not complete.

.The two products can be installed on different computers in either of the following configurations:

- Different operating systems. For example, the NNMi management server is a Linux system, and the HP NA server is a Windows system.

- The same operating system. For example, the NNMi management server is a Windows system, and the HP NA server is a second Windows system.

For the most recent information about supported hardware platforms and operating systems, see the support matrices for both products.

Documentation

This document describes how to configure and use the integration.

Enabling the HP NNMi–HP NA Integration

Enabling the HP NNMi–HP NA integration sets the NNMi management server as the definitive topology master in the managed environment. In HP NNMi, create one node group containing the nodes to synchronize with the NA inventory. The integration synchronizes the contents of this node group with the appropriate NA Security partition as described in Topology Synchronization Between HP NNMi and HP NA on page 21.

This section describes the following procedures:

- Integration Configuration Upgraded from NNMi 9.1x to NNMi 9.20 on page 10
- Integration Configuration Upgraded from NNMi 9.0x to NNMi 9.1x or NNMi 9.20 on page 11
- New Integration Configuration on page 13

Integration Configuration Upgraded from NNMi 9.1x to NNMi 9.20

If you plan to upgrade either HP NNMi or HP NA 9.1x to version 9.20, you must upgrade both applications to version 9.20 for the integration to work correctly. To upgrade and enable the HP NNMi–HP NA integration to use NNMi 9.20 and NA 9.20, follow these steps:

1 *Important*: If you have the HP NNMi–HP NA integration enabled, disable the integration. See Disabling the HP NNMi–HP NA Integration on page 33.

2 Upgrade both HP NNMi and HP NA to version 9.20. Upgrade these applications in any order, as the upgrade sequence does not matter.

➤ If you have HP NNMi and HP NA installed on the same server, you might see a port conflict warning from the NA installer when upgrading NA to version 9.20. Assuming that HP NNMi is using the ports shown in the warning, ignore these warnings. See NNMi's *nnm.ports* reference page, or the UNIX manpage, for more information.

➤ Do not attempt to enable the HP NNMi–HP NA integration until you finish upgrading both HP NNMi and HP NA to version 9.20.

3 In the NNMi console, configure the connection from HP NNMi to HP NA:

   a Open the **HP NNMi–HP NA Integration Configuration** form (**Integration Module Configuration > HP NA**).

   b Select the **Enable Integration** check box to make the remaining fields on the form available.

   The **HP NNMi–HP NA Integration Configuration** form contain the values from the NNMi 9.1x configuration. The new fields on this form are set to their default values.

   c Enter values for the new integration configuration fields (**Topology Filter Node Group**, **Topology Synchronization Interval**, and **Discover Device Drivers in NA**).

   For information about these fields, see Integration Behavior on page 37.

   d Click **Submit** at the bottom of the form.

   A new window opens a status message. If the message indicates a problem with connecting to the NA server, click **Return,** and then adjust the values for connecting to the NA server as suggested by the text of the error message.

4   *Optional*. Configure single sign-on between HP NNMi and HP NA as described in
Configuring Single Sign-On Between NNMi and HP NA on page 17.

If the NA menu items are not available on the NNMi console **Actions** menu, log out of
the NNMi console, then log back in.

Integration Configuration Upgraded from NNMi 9.0x to NNMi 9.1x or NNMi 9.20

Prior to NNMi 9.1x, HP NA provided the NNMi connector tool that established
communication between HP NNMi and HP NA. HP NNMi now provides this
functionality; the HP NA-provided NNMi connector is no longer used.

If the HP NNMi–HP NA integration was configured on an NNMi 9.0x management
server, the process of upgrading to NNMi 9.20 disables the integration (but retains
the configuration values). Objects in the NA database still contain the NNMi UUID
and will be synchronized with the current NNMi topology when you enable the
integration from the upgraded NNMi management server.

The integration now provides for single sign-on between the NNMi console and the
NA user interface. See Configuring Single Sign-On Between NNMi and HP NA on
page 17 for more information.

Beginning with NNMi 9.1x Patch 1, you can configure HP NNMi to map NNMi
security groups to NA partitions. That means that, after you select the `Map NNMi
security groups to NA partitions` check box and submit the change, a node
synchronized to NA will always be added or updated to be in a security partition
having the same name as that node's NNMi security group.

If a partition does not exist, HP NNMi creates one having the same name as the
NNMi security group, associates it with the NA `Site` view with an *NNMi Security
Group* description. NNMi's `Default Security Group` maps to NA's `Default Site`
partition.

In this document, the term NA partition refers to the specific NA partition HP NNMi
creates for each node. This NA partition has the same name as the NNMi security
group.

The NA administrator should promptly configure security for NA users mapped to the
newly created partitions. These security configurations should be based on the
corresponding security constraints for the associated security groups in HP NNMi.

If you plan to upgrade HP NNMi from NNMi 9.0 to NNMi 9.10 or from NNMi 9.0x
patch 5 or newer to NNMi 9.20, you must first uninstall the NNMi connector as shown
in the following steps. To upgrade and enable the HP NNMi–HP NA integration for
the NNMi 9.1x or NNMi 9.20 management server, follow these steps:

1   Disable the HP NNMi–HP NA integration.

2   Uninstall the NNMi connector from the NNMi management server:

- *Windows*: Open the Control Panel, click **Add or Remove Programs**, then remove
HP NA - HP Network Node Manager connector.

- *Linux or Solaris*: Run the following command:

    HP NA and HP NNMi installed on the same server:
    $NAINSTALLDIR/UninstallConnector/Uninstall\ NA

    HP NA and HP NNMi installed on separate servers:
    $NAINSTALLDIR/UninstallerData/Uninstall\ NA

> The default value of `$NAINSTALLDIR`:
> *HP NA and HP NNMi installed on the same server: /opt/NA*
> *HP NA and HP NNMi installed on separate servers (Windows):*
> C:\NA
> *HP NA and HP NNMi installed on separate servers (Linux): /*
> root/NA

3 Upgrade from NNMi 9.0x to NNMi 9.1x or NNMi 9.20.

4 Verify that HP NA has been upgraded to a supported version, as listed in the "Integrations" section of the *NNMi System and Device Support Matrix*.

5 Delete the remnant `integration.jar` file from the system:

   a Stop the NA ManagementEngine service:

      — *Windows*: Open the **Services** control panel (**Start > Settings > Control Panel > Administrative Tools > Services**). In the list of services, right-click **TrueControl ManagementEngine**, and then click **Stop**.

      — *Linux or Solaris*: Run the following command:

         /etc/init.d/truecontrol stop

   b Manually remove the `integration.jar` file from the following location:

      — *Windows*: %NAINSTALLDIR%\server\ext\jboss\server\default\lib\
         `integration.jar`

      — *Linux or Solaris*:
         $NAINSTALLDIR/server/ext/jboss/server/default/lib/
         `integration.jar`

   c Restart the NA ManagementEngine service:

      — *Windows*: Open the **Services** control panel (**Start > Control Panel > Administrative Tools > Services**). In the list of services, right-click **TrueControl ManagementEngine**, and then click **Start**.

      — *Linux or Solaris*: Run the following command:

         /etc/init.d/truecontrol restart

6 *Optional*. Configure single sign-on between HP NNMi and HP NA as described in Configuring Single Sign-On Between NNMi and HP NA on page 17.

7 In the NNMi console, configure the connection from HP NNMi to HP NA:

   a Open the **HP NNMi–HP NA Integration Configuration** form (**Integration Module Configuration > HP NA**).

   b Select the **Enable Integration** check box to make the remaining fields on the form available.

      The **HP NNMi–HP NA Integration Configuration** form contain the values from the NNMi 9.1x configuration. The new fields on this form are set to their default values.

   c Enter values for the new integration configuration fields (**Topology Filter Node Group**, **Topology Synchronization Interval**, and **Discover Device Drivers in NA**).

      For information about these fields, see Integration Behavior on page 37.

   d Click **Submit** at the bottom of the form.

A new window opens a status message. If the message indicates a problem with connecting to the NA server, click **Return**, and then adjust the values for connecting to the NA server as suggested by the text of the error message.

If the NA menu items are not available on the NNMi console **Actions** menu, log out of the NNMi console, then log back in.

New Integration Configuration

To enable the HP NNMi–HP NA integration, follow these steps:

1   *Optional*. If you want the integration to discover the drivers on devices in the synchronized topology, specify the SNMP configuration for the nodes in the NNMi topology. In the NA user interface, follow these steps:

   a   Open the **Device Password Rule** page (**Devices > Device Tools > Device Password Rules**).

   b   Create one or more password rules that specify how to communicate with the nodes in the NNMi topology.

2   In the NNMi console, configure the connection from HP NNMi to HP NA:

   a   Open the **HP NNMi–HP NA Integration Configuration** form (**Integration Module Configuration > HP NA**).

   b   Select the **Enable Integration** check box to make the remaining fields on the form available.

   c   *Optional*. Select **NNMi SSL**, **NA SSL**, or both. If you select any of these check boxes, complete the steps shown in step 4 on page 14.

   d   Enter the information for connecting to the NNMi management server. For information about these fields, see NNMi Management Server Connection on page 36.

   e   Enter the information for connecting to the NA server. For information about these fields, see NA Server Connection on page 37.

   f   Enter values for the remaining fields:

       For information about these fields, see Integration Behavior on page 37.

   g   Click **Submit** at the bottom of the form.

       A new window displays a status message. If the message indicates a problem with connecting to the NA server, click **Return**, and then adjust the values for connecting to the NA server as suggested by the text of the error message.

3 *Optional*. In the NA user interface, alter the default settings of the NA functionality provided by the integration:

a Open the **Administrative Settings - 3rd Party Integrations** page (**Admin > Administrative Settings > 3rd Party Integrations**).

b Verify that **Enabled** is selected for **3rd Party Integrations**.

c Change the selections for any of the following fields:

— **Rediscover Hosts After Tasks**

— **Out of Service Events**

— **If the device task fails**

— **If device compliance check fails after the task completed**

— **Propagate SNMP Community Strings**

For information about these fields, see HP NNMi Integration Configuration in HP NA Reference on page 38.

d Click **Save** at the bottom of the page.

4 *Optional*. If you selected any of the check boxes in step c on page 13, complete the following steps to configure an SSL connection between HP NNMi and HP NA.

a Export the NA certificates from the `truecontrol.keystore` file using the following command:

Windows:
```
<NAInstallDir>\jre\bin\keytool.exe -export -alias sentinel
-file C:\temp\na.cer -keystore
<NAInstallDir>\server\ext\jboss\server\default\conf\
truecontrol.keystore -storepass sentinel
```

UNIX:
```
<NAInstallDir>/jre/bin/keytool -export -alias sentinel -file
na.cer -keystore <NAInstallDir>/server/ext/jboss/server/
default/conf/truecontrol.keystore -storepass sentinel
```

b Verify that you see the `Certificate stored in file <directory>:\cert` message.

c Copy the certificate from the cert file you created in step a on page 14 to the NNMi management server.

d Open a command window on the NNMi management server.

e To import the NA certificate into the NNMi `nnm.truststore` file, run the following command:

Windows:
```
%NnmInstallDir%\nonOV\jdk\b\bin\keytool.exe -import -alias
sentinel -file "<certificate file directory>\na.cer"
-keystore
%NnmDataDir%\shared\nnm\certificates\nnm.truststore"
-storepass ovpass
```

UNIX:
```
$NnmInstallDir/nonOV/jdk/b/bin/keytool -import -alias
sentinel -file <certificate file directory>/na.cer -keystore
$NnmDataDir/shared/nnm/certificates/nnm.truststore"
-storepass ovpass
```

Make sure you answer **yes** when asked whether to `Trust this certificate?`. The following program listing is an example of what happens after you run this command.

```
Owner: CN=localhost, OU=Hewlett Packard Company, O=Hewlett
Packard Company, L=Palo Alto, ST=CA, C=US

Issuer: CN=localhost, OU=Hewlett Packard Company, O=Hewlett
Packard Company, L=Palo Alto, ST=CA, C=US

Serial number: 484e9d84

Valid from: Tue Jun 10 09:28:04 MDT 2008 until: Fri Jun 08
09:28:04 MDT 2018

Certificate fingerprints:

        MD5:  65:94:D1:A0:44:84:E2:69:A4:23:DC:B9:5E:EB:91:A8

        SHA1:
05:DE:DC:68:58:45:CA:EA:88:FF:16:05:E7:65:A9:5B:23:29:D7:65

Trust this certificate? [no]:  yes

Certificate was added to keystore
```

f   Obtain the NNMi certificate alias name using the following command.

Windows:

** %NnmInstallDir%\nonOV\jdk\b\bin>keytool.exe -v -list
-keystore %NnmDataDir%\shared\nnm\certificates\nnm.keystore"
-storepass nnmkeypass**

Unix:

**<NnmInstallDir>/nonOV/jdk/b/bin/keytool -v -list -keystore
<NnmDataDir>/OV/shared/nnm/certificates/nnm.keystore
-storepass nnmkeypass**

g   Export the NNMi certificate to a file using the following command.

Windows:

**%NnmInstallDir%\nonOV\b\bin\keytool -export -alias <alias>
-file <directory>\nnm.cer -keystore
%NNMDataDir%\shared\nnm\certificates\nnm.keystore -storepass
nnmkeypass**

Unix:

**<NnmInstallDir>/nonOV/jdk/b/bin/keytool -export -alias
<alias> -file <Directory>/nnm.cer -keystore <NnmDataDir>/
shared/nnm/certificates/nnm.keystore -storepass nnmkeypass**

h   Copy the NNMi certificate file to a directory on the NA server.

i   Import the NNMi certificate to the NA `truecontrol.truststore` file using the following command.

Windows:

**<NAInstallDir>\jre\bin\keytool.exe -import -alias <alias>
-file <Directory>\nnm.cer -keystore
<NAInstallDir>\server\ext\jboss\server\default\conf\truecont
rol.truststore -storepass sentinel**

Unix:

```
<NAInstallDir>/jre/bin/keytool -import -alias <alias> -file
<Directory>/nnm.cer -keystore <NAInstallDir>/server/ext/
jboss/server/default/conf/truecontrol.truststore -storepass
sentinel
```

Make sure you answer **yes** when asked whether to `Trust this certificate?`. The following program listing is an example of what happens after you run this command.

```
Owner: CN=naqa-e01-vm59.fc.usa.hp.com
Issuer: CN=naqa-e01-vm59.fc.usa.hp.com
Serial number: 4e81ef8f
Valid from: Tue Sep 27 09:45:19 MDT 2011 until: Thu Sep 03
09:45:19 MDT 2111
Certificate fingerprints:
        MD5:  E4:26:B2:0C:C5:A5:FE:46:F2:0E:2A:C3:5E:83:18:AE
        SHA1:
EB:E9:A3:F0:6B:C7:45:E9:4B:16:00:52:1C:B4:9F:75:B6:DF:3F:DC
Signature algorithm name: SHA1withRSA
        Version: 1
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

j   Restart the NA server:

Windows:

Restart the following services:

— TrueControl FTP Server

— TrueControl Management Engine

— TrueControl SWIM Server

— TrueControl Syslog Server

— TrueControl TFTP Server

Unix:

Restart the NS servers using the following command:
/etc/init.d/truecontrol restart

k   Run the following command sequence on the NNMi management server:

–   **ovstop**

–   **ovstart**

l   *Optional*: Run the following commands on both the NNMi management server and the NA server. Compare the outputs to make sure the keystore certificates reside on both servers' truststore files:

NNMi management server (Windows):
**keytool.exe -v -list -keystore
%NnmDataDir%\shared\nnm\certificates\nnm.truststore
-storepass ovpass**

NNMi management server (UNIX):
**keytool -v -list -keystore $NnmDataDir/shared/nnm/
certificates/nnm.truststore -storepass ovpass**

NA server (Windows):
```
<NAInstallDir>\jre\bin\keytool.exe -v -list -keystore
<NAInstallDir>\server\ext\jboss\server\default\conf\truecont
rol.truststore -storepass sentinel
```

NA server (UNIX):
```
<NAInstallDir>/jre/bin/keytool -v -list -keystore /opt/NA/
server/ext/jboss/server/default/conf/truecontrol.truststore
-storepass sentinel
```

5   *Optional*. If you want the integration to detect connections with mismatched speed or duplex configurations, populate the MAC addresses for the interfaces of the NNMi devices in the NA topology. In the NA user interface, follow these steps:

a   For each node in the NNMi topology, verify that the NNMUuid property is set on the corresponding device in the NA inventory.

The integration topology synchronization process sets the NNMUuid property. This property is listed in the **Device Details** section of the device page in NA.

b   On the **Device Password Rule** page (**Devices > Device Tools > Device Password Rules**), create one or more password rules that specify how to communicate with the nodes in the NNMi topology.

If you created password rules in step 1 on page 13, you do not need to do so again.

c   On the **New Task - Discover Driver** page (**Devices > Device Tasks > Discover Driver**), discover the drivers for the devices imported from the NNMi topology.

If you configured the integration to discover drivers, the integration has already completed this step.

d   Create a snapshot of the devices imported from the NNMi topology (**Devices > Device Tasks > Take Snapshot**).

If you configured the integration to discover drivers, the integration has already completed this step.

e   Run the **NA Topology Data Gathering** diagnostic (**Devices > Device Tasks > Run Diagnostics**) for the devices imported from the NNMi topology.

f   Verify that each device synchronized with the NNMi topology has a MAC address for each of its interfaces.

On a device page, click **View > Device Detail > MAC Addresses** to display the MAC addresses for that device.

6   If the NA menu items are not available on the NNMi console **Actions** menu, log out of the NNMi console, then log back in.

Configuring Single Sign-On Between NNMi and HP NA

Single sign-on is available for all HP enterprise applications that use identical initialization string values and also share a common network domain name.

If the HP NNMi and HP NA user names are exactly the same for a particular individual, that person can log on to NNMi and view NA pages without logging on to NA. This single sign-on feature maps user names, but not passwords, between the two

products. The passwords for logging on to HP NNMi and HP NA can be different. Single sign-on does not map user roles, so the user can have different privileges in each application. For example, a user might have operator level 1 privileges in HP NNMi and administrator privileges in HP NA.

To configure single sign-on access from HP NNMi to HP NA, make sure that both applications use the same initialization string. You can copy the string from either application to the other. Consider all applications that interact when choosing which initialization string value to use. If necessary, also update the initialization string configuration for other applications.

On the NNMi management server, locate the NNMi initialization string as follows:

1   Open the following file in a text editor:

   - *Windows*: `%NNM_PROPS%\nms-ui.properties`

   - *UNIX*: `$NNM_PROPS/nms-ui.properties`

Enable SSO   2   Look for a section in the file that resembles the following:

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

```
Change this as follows:
```

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

NNMi initialization string   3   Search for the string `initString`.

The initialization string is the value of the `initString` parameter without the quotation marks.

For example, if the `nms-ui.properties` file contains the following text:

```
initString=E091F3BA8AE47032B3B35F1D40F704B4
```

the initialization string is:

```
E091F3BA8AE47032B3B35F1D40F704B4
```

4   If you change the value of the `initString` parameter, run the following command to commit the changes:

   nnmsso.ovpl -reload

See the *nnmsso.ovpl* reference page, or the UNIX manpage, for more information.

NA initialization string   On the NA server, locate the NA initialization string as follows:

1   Open the following file in a text editor:

   - *Windows*:
     `%NA_HOME%\server\ext\jboss\server\default\conf\lwssofmconf.xml`

   - *UNIX*:
     `$NA_HOME/server/ext/jboss/server/default/conf/lwssofmconf.xml`

   The default value of the `NA_HOME` environment variable is as follows:

   - *Windows*: `C:\na`

   - *UNIX*: `/opt/NA`

2   In the `enableLWSSO` tag, set the enableLWSSOFramework attribute to true:

   `enableLWSSOFramework="true"`

3   In the `lwssoValidation` block, do the following:

- Set the value of the `domain` tag to the full domain name of the NA server. For example, if the hostname of the NA server is na.location.example.com, set `<domain>location.example.com</domain>`.

  ➤ This step assumes that the NNMi management server is in the same domain as the NA server. If it is not, you must add a `DNSDomain` element for the NNMi management server's domain to the `trustedHosts` block.

4 In the `crypto` tag, set the `initString` attribute to the value of the `initString` property in the NNMi `nms-ui.properties` file.

  ➤ The settings in the `crypto` block must be identical for all applications participating in SSO.

5 In the `trustedHosts` block, set the DNSDomain tag to the value of the domain tag in the `lwssoValidation` block, for example:

  `<DNSDomain>location.example.com</DNSDomain>`

  ➤ This step assumes that the NNMi management server is in the same domain as the NA server. If the NA server is in a different domain than the NNMi management server, add `DNSDomain` entries for both domains.

6 Make sure all of the applications participating in SSO have a GMT (Greenwich Mean Time) time difference of less than 15 minutes. Although they can be in different time zones, the time difference, after conversion to GMT, should be the same.

7 Restart the NA jboss server:

  - *Windows*: In the NA user interface, on the **Admin > Start/Stop Services** page, restart the Management Engine.

  - *UNIX*: Run the following command:

    /etc/init.d/truecontrol restart

8 In the NNMi console, configure the connection from NNMi to NA:

  a Open the **HP NNMi–HP NA Integration Configuration** form (**Integration Module Configuration > HP NA**).

  b Select the **Enable Integration** check box to make the remaining fields on the form available.

  c Enter values for the integration configuration fields (**Topology Filter Node Group**, **Topology Synchronization Interval**, and **Discover Device Drivers in NA**).

    For information about these fields, see Integration Behavior on page 37.

  d Click **Submit** at the bottom of the form.

    A new window displays a status message. If the message indicates a problem with connecting to the NA server, click **Return**, and then adjust the values for connecting to the NA server as suggested by the text of the error message.

9 If the NA menu items are not available on the NNMi console **Actions** menu, log out of the NNMi console, then log back in.

10 Both HP NNMi and HP NA automatically log users out of their user interfaces after some period of time. When configuring SSO for the HP NNMi–HP NA integration, *set the NNMi and NA timeout values to be identical*. Do the following to set identical NNMi and NA timeout values:

a   Select one timeout value, in minutes, to use as NNMi and NA user interface timeout values. HP recommends using a value of 30 minutes. If your HP NNMi–HP NA integration does not require a high level of security, use a value of 60 minutes or longer.

b   On the NA server, open the following file in a text editor:

— *Windows*:
`%NA_HOME%\server\ext\jboss\server\default\conf\lwssofmconf.xml`

— *UNIX*:

`$NA_HOME/server/ext/jboss/server/default/conf/lwssofmconf.xml`

The default value of the NA_HOME environment variable is as follows:

— *Windows*: `C:\na`

— *UNIX*: `/opt/NA`

c   Find the `<expirationPeriod>1440</expirationPeriod>` tag.

d   Replace the existing value with the value you selected in step a.

e   Save your changes. This change takes effect the next time you restart NA.

f   On the NNMi management server, open the following file in a text editor:

— *Windows*: `%NNM_PROPS%\nms-ui.properties`

— *UNIX*: `$NNM_PROPS/nms-ui.properties`

g   Find the `#!com.hp.nms.ui.sso.expirationPeriod=1440` string.

h   Remove the remove the **#!** characters located at the beginning of the string, then replace the existing value with the value you selected in step a.

i   Save your changes.

j   Run the following command to commit the changes:

nnmsso.ovpl -reload

See the *nnmsso.ovpl* reference page, or the UNIX manpage, for more information.

Using the HP NNMi–HP NA Integration

The HP NNMi–HP NA integration adds functionality to both HP NNMi and HP NA. This section contains the following topics:

Topology Synchronization Between HP NNMi and HP NA

The HP NNMi–HP NA integration dynamically synchronizes the topology for the nodes in the specified NNMi synchronization node group with the devices in the appropriate NA security partition. The integration matches NNMi nodes with NA devices by comparing hostnames and IP addresses (if necessary). The integration adds the NA ID to each synchronized NNMi node and the NNMi UUID to each synchronized NA device.

The **Topology Filter Node Group** parameter on the **HP NNMi–HP NA Integration Configuration** form specifies the NNMi synchronization node group.

This synchronization occurs as follows:

- When the integration is first enabled on the **HP NNMi–HP NA Integration Configuration** form, the integration performs a complete topology synchronization between the NNMi synchronization node group and the appropriate NA security partition.

  — If any NNMi nodes in the synchronization node group do not exist in HP NA, the integration adds these nodes to the appropriate NA security partition.

  — If any NNMi nodes in the synchronization node group already exist in HP NA, the integration moves these devices to the NA Default Site partition or into the appropriate NA security partition if NNMi Security Group to NA Partition mapping is enabled.

  — If any devices in the NA inventory are not in the NNMi synchronization node group, the integration sends discovery hints to HP NNMi for these devices. The NNMi auto-discovery rule configuration determines whether these nodes are discovered. The NNMi node group configuration determines which node groups include the devices hinted by NA.
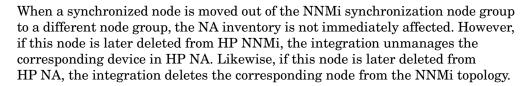
  It is possible for the NA inventory to contain nodes that are not in the NNMi synchronization node group. All nodes in the NNMi synchronization node group are in the appropriate NA security partition after synchronization completes.

- After initial synchronization, the integration maintains the topology synchronization as follows:

  — When a new node is added to the NNMi synchronization node group, the integration creates this device in the appropriate NA security partition.

  — When a new device is added to the NA inventory, the integration sends a discovery hint to HP NNMi as long as the device meets the following criteria:

    – The NA devices are part of the appropriate NA Security partition established when you enabled the HP HP NNMi–HP NA integration.

- The NA devices can be identified by an IP address.

- The NA devices do not have an associated NNMi UUID.

- The NA devices are not members of the NNMi node group that contains the nodes to synchronize with the NA inventory.

— When a synchronized node is deleted from HP NNMi, the integration unmanages the corresponding device in HP NA. The device history is still available for unmanaged devices in HP NA.

— When a synchronized device is deleted from HP NA, the integration deletes the corresponding node from the NNMi topology

If you have an auto-discovery rule defined in HP NNMi that prevents HP NNMi from acting on the hints from HP NA, do the following:

1   Modify the auto-discovery rule to include those devices that are in the appropriate NA Security partition, but not in the NNMi node group containing the nodes to synchronize with the NA inventory.

2   Repeat the steps to enable the HP NNMi–HP NA integration so HP NNMi can act on the NA hints sent to HP NNMi.

When a synchronized node is moved out of the NNMi synchronization node group to a different node group, the NA inventory is not immediately affected. However, if this node is later deleted from HP NNMi, the integration unmanages the corresponding device in HP NA. Likewise, if this node is later deleted from HP NA, the integration deletes the corresponding node from the NNMi topology.

Periodic Synchronization Considerations

Periodically, the HP NNMi–HP NA integration performs a complete topology synchronization from HP NNMi to HP NA. The HP NNMi–HP NA integration does not perform a complete topology synchronization from HP NA to HP NNMi. If the HP NNMi–HP NA integration remains enabled, this periodic synchronization follows the same process as the synchronization that occurs when the integration is first enabled.

The **Topology Synchronization Interval** parameter on the **HP NNMi–HP NA Integration Configuration** form specifies the frequency of periodic topology synchronization.

Consider the following guidelines when choosing the topology synchronization interval:

• Topology synchronization is a fail-safe mechanism. If the connection between the NNMi management server and the NA server is highly reliable, the topology synchronization interval can be large.

• The recommended minimum topology synchronization interval for 500 or fewer synchronized nodes is 24 hours. For each additional 500 synchronized nodes, consider adding another 24 (or more) hours.

Periodic topology synchronization is load balanced with NNMi Spiral Discovery and paced to avoid overloading the NNMi management server. During periods of high discovery activity, topology synchronization remains quiet.

Support for HP Blade System Virtual Connect Devices

HP Blade System Virtual Connect devices can federate to form a Virtual Connect domain consisting of a primary device and one or more standby and slave devices. The integration should pass to the NA inventory information about only those Virtual Connect devices that are acting as a domain primary or as standalone devices.

To limit which Virtual Connect devices are synchronized with the NA inventory, follow these steps:

1 Create one or more NNMi node groups based on an additional filter that uses any of the following capabilities:

   • com.hp.nnm.capability.node.hpvcStandalone

   • com.hp.nnm.capability.node.hpvcPrimary

   • com.hp.nnm.capability.node.hpvcStandby

   • com.hp.nnm.capability.node.hpvcSlave

2 Create one parent node group for all node groups created in step 1.

   In this parent node group, also include any other devices that should be synchronized with the NA inventory.

3 Update the **Topology Filter Node Group** parameter on the **HP NNMi–HP NA Integration Configuration** form with the name of the parent node group. For more information, see Integration Behavior on page 37.

HP NNMi Functionality Provided by the Integration

The HP NNMi–HP NA integration provides communication from HP NNMi to HP NA for the following functionality:

• Launching NA Views from the NNMi Console on page 23

• Configuring NA Diagnostics and Command Scripts as Incident Actions on page 24

• Viewing the Results of Incident Actions that Access NA on page 25

• Identifying Layer 2 Connections with Mismatched States on page 25

Launching NA Views from the NNMi Console

The HP NNMi–HP NA integration provides links to HP NA from the NNMi console.

Enabling the HP NNMi–HP NA integration adds the following items to the **Actions** menu in the NNMi console:

• **Show HP NA Diagnostic Results**—Displays a list of the NA tasks that have been scheduled for the device in an NNMi incident. Select a task to view the task results. For more information, see Viewing the Results of Incident Actions that Access NA on page 25.

• **Rerun HP NA Diagnostics**—Runs any NA actions that are configured for the device in an NNMi incident. For more information, see Viewing the Results of Incident Actions that Access NA on page 25.

• **Show mismatched connections**—Displays a table of all layer 2 connections with possible speed or duplex configuration differences. For more information, see Identifying Layer 2 Connections with Mismatched States on page 25.

- **View HP NA Device Information**—Opens the current NA **Device Details** page for the device selected in HP NNMi.

- **View HP NA Device Configuration**—Opens the NA **Current Configuration** page for the device selected in HP NNMi.

➤ If real-time change detection is disabled for a device, the information shown is the configuration HP NA captured at the last device polling interval. If configuration changes were made following that capture, the information on the **Current Configuration** page might not be the actual current configuration.

- **View HP NA Device Configuration Diffs**—Opens the NA **Compare Device Configuration** page for the device selected in HP NNMi.

- **View HP NA Device Configuration History**—Opens the **NA Device Configurations History** page for the device selected in HP NNMi.

- **View HP NA Policy Compliance Report**—Opens the NA **Policy, Rule and Compliance Search Results** page for the device selected in HP NNMi.

- **Telnet to HP NA Device**—Opens a **Telnet** window for connecting to the device selected in HP NNMi.

- **SSH to HP NA Device**—Opens an **SSH** window for connecting to the device selected in HP NNMi.

- **Launch HP NA**—Opens the NA user interface.

- **Launch HP NA Command Scripts**—Opens the **New Task—Run Command Script** page in HP NA. The page is pre-filled for the node or incident selected in the NNMi console.

- **Launch HP NA Diagnostics**—Opens the **New Task—Run Diagnostics** page in HP NA. The page is pre-filled for the node or incident selected in the NNMi console.

For information about using the NA functionality, see the *HP Network Automation User's Guide*.

Configuring NA Diagnostics and Command Scripts as Incident Actions

Enabling the HP NNMi–HP NA integration modifies some out-of-the-box NNMi incidents to include incident actions that access NA diagnostics each time the associated incident type occurs. Table 1 lists the modified incidents.

Table 1   NNMi Incidents Configured with NA Diagnostics

NNMi Incident	NA Diagnostic
OSPFNbrStateChange	Show Neighbor
OSPFVirtIfStateChange	Show Neighbor
OSPFIfStateChange	Show Neighbor Show Interfaces
InterfaceDown	Show Interfaces
CiscoChassisChangeNotification	Show Module

You can add an action that accesses HP NA to any other NNMi incident, and you can modify the default incident actions. On the **Actions** tab for an incident, add a new lifecycle transition action with **Command Type** of ScriptOrExecutable. In the

Command text box, enter either `naruncmdscript.ovpl` or `narundiagnostic.ovpl` with the appropriate arguments. For examples, see the action configurations of the incidents listed in Table 1.

Viewing the Results of Incident Actions that Access NA

When an incident of a type that has been configured with an NA action arrives, HP NNMi initiates the configured action and stores the task ID of the diagnostic or command script as an attribute of that incident. The presence of the task ID enables the **Show HP NA Diagnostic Results** and **Rerun HP NA Diagnostics** items on the **Actions** menu.

To view the outcome of the action at the time the incident occurred, in an NNMi incident view, select the incident, and then select **Actions > Show HP NA Diagnostic Results**.

To view current results of the configured action, in an NNMi incident view, select the incident, and then select **Actions > Rerun HP NA Diagnostics**.

If you run the task multiple times, HP NNMi lists the most recent task ID on the **Custom Attributes** tab of the **Incident** form. The **Show HP NA Diagnostic Results** action displays all of the tasks that have been run for the incident so that you can compare the results from different runs.

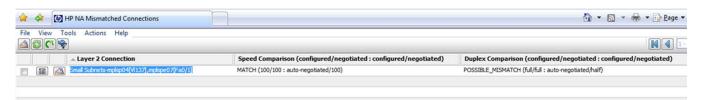## Identifying Layer 2 Connections with Mismatched States

When the HP NNMi–HP NA integration is enabled, HP NNMi periodically queries HP NA for the speed and duplex settings of the two interfaces on either end of each layer 2 connection in the NNMi topology. Additionally, HP NNMi queries HP NA for the speed and duplex settings of the interfaces for any new connection added to the NNMi topology and, when the NNM iSPI Performance for Metrics is running, for any connection with performance threshold exceptions that might indicate a mismatched connection. HP NNMi uses a mismatch detection algorithm to determine whether the values might result in a mismatched connection.

▶ HP NNMi can perform the mismatch analysis only when the NA inventory includes the MAC addresses for both interfaces that form a layer 2 connection. If the NA interface records do not include valid MAC addresses, run the NA **Topology Data Gathering** diagnostic to update the MAC address fields. For more information, see step 5 on page 17.

The **Actions > Show mismatched connections** command displays a table, shown in Figure 1, of layer 2 connections that HP NNMi suspects might contain speed mismatches, duplex mismatches, or both speed and duplex mismatches.

Figure 1   Example Mismatched Connections Table

For each suspect connection, the table lists the speed and duplex values for the interfaces on either side of the connection and an interpretation of the data. The possible interpretations are as follows:

- `MATCH` indicates that the speed values and duplex values most likely result in a properly functioning layer 2 connection.

- `POSSIBLE_MISMATCH` indicates that the speed values, the duplex values, or both speed and duplex values might conflict, resulting in a poor or non-performing connection.

- `MISMATCH` indicates that the speed values, the duplex values, or both speed and duplex values most likely conflict, resulting in a poor or non-performing connection.

The **HP NA Connection Check Interval** parameter on the **HP NNMi–HP NA Integration Configuration** form specifies the frequency of the connection queries.

HP NA Functionality Provided by the Integration

The HP NNMi–HP NAintegration provides communication from HP NA to HP NNMi for the following functionality:

- Sending Device Configuration Change Notifications on page 26
- Maintaining Accurate Device Information on page 26
- NA Node and Interface Information Displayed in NNMi Analysis Panes on page 27
- Disabling Network Management During Device Configuration on page 30
- Propagating Device Community String Changes on page 31
- NA Event Rules on page 31

Sending Device Configuration Change Notifications

HP NA sends SNMP traps to HP NNMi when a device is added to the NA inventory and when the configuration changes on a device in the NA inventory. The NNMi operator can see these traps in the incident views and investigate the changes if necessary.

The integration adds the NASnmpTrapv1 and NASnmpTrapv2 SNMP trap incident configurations to HP NNMi.

Maintaining Accurate Device Information

For certain device configuration tasks, after the task completes, HP NA triggers HP NNMi to rediscover the device.

The **Rediscover Host After Tasks** field on the NA **Administrative Settings - 3rd Party Integrations** page specifies the device configuration tasks that trigger HP NNMi to rediscover a device. The default selections are:

- Update Device Software
- Deploy Passwords
- Reboot Device
- Discover Driver

You can select any or all of the following additional tasks:

- Run Command Script

- Run Diagnostics
- Delete ACLs
- Configure Syslog
- Run ICMP Test
- Take Snapshot
- Synchronize Startup and Running
- OS Analysis

To disable this feature, clear all selections from the task list.

NA Node and Interface Information Displayed in NNMi Analysis Panes

If an incident's source node has both an NA ID and an NNMi UUID, HP NNMi shows additional NA information in **Node Configuration**, **History of Node Configuration**, and **Interface Configuration** tabs. To view this NA information, you must log on to HP NNMi with a user account that is assigned one of the roles shown for the *Minimum NNMi Role for Analysis Pane Data*. See Table 4 on page 37 for more information.

HP NNMi displays port information from HP NA if an interface managed by HP NNMi matches a port name from HP NA. HP NNMi uses the following steps to perform this matching:

1   HP NNMi matches an interface IP address from HP NNMi to a port IP address from HP NA.

2   HP NNMi matches a port name from HP NA to any of the following interface attributes from HP NNMi: `ifName`, `ifAlias`, `ifDescr`, or `sourceObjectName`.

3   HP NNMi matches a MAC layer address from HP NA to a physical address from HP NNMi.

If multiple port configurations from HP NA match a single interface managed by HP NNMi, HP NNMi does not show any configuration information for this match.

If multiple interfaces managed by HP NNMi match a single port configuration from HP NA, HP NNMi shows port information from HP NA for this match in the NNMi **Interface Configuration** tab.

HP NNMi shows information from HP NA in the following NNMi locations:

- Node Inventory Analysis Pane
    - Node Configuration
    - History of Node Configuration
- Interface Inventory Analysis Pane
    - Interface Configuration
- Incident Browsing Analysis Pane (Node Incidents)
    - Node Configuration
    - History of Node Configuration
- Incident Browsing Analysis Pane (Interface Incidents)
    - Interface Configuration

After selecting any of the following incidents in the **Incident Browsing** workspace, you can use HP NNMi to show additional interface information, as shown in Figure 2, in the NNMi analysis pane:

- InterfaceDown

- InterfaceFCSLANErrorRateHigh

- InterfaceFCSWLANErrorRateHigh

- InterfaceInputDiscardRateHigh

- InterfaceInputErrorRateHigh

- InterfaceInputUtilizationHigh

- InterfaceOutputDiscardRateHigh

- InterfaceOutputErrorRateHigh

- InterfaceOutputUtilizationHigh

- InterfaceTraffic

You can also see this same information from NNMi's interface inventory. Figure 2 shows the NNMi analysis pane after opening an interface from the interface inventory.

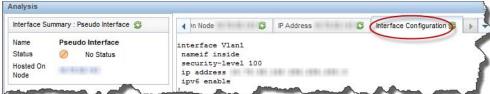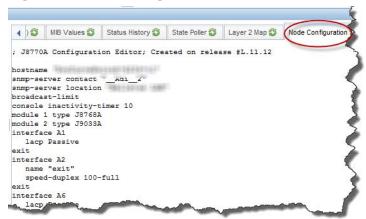**Figure 2   Interface Configuration Tab**

Figure 3 shows the NNMi analysis pane after opening a node from the device inventory, then selecting the **Node Configuration** tab.
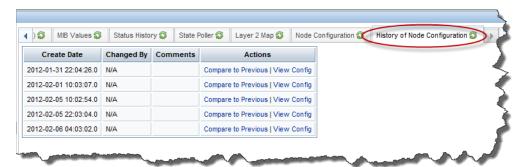
Figure 3   Node Configuration Tab

You can also view this configuration information by using HP NNMi's **Action** > **HP Network Automation** > **View HP NA Device Configuration** menu.

Figure 4 shows the NNMi analysis pane after opening a node from the device inventory, then selecting the **History of Node Configuration** tab.

Figure 4   History of Node Configuration Tab

You can also view this device configuration history by using HP NNMi's **Action** > **HP Network Automation** > **View HP NA Device Configuration History** menu.

After selecting the following incidents in the **Incident Browsing** workspace, HP NNMi shows additional node information in the analysis pane:

- AddressNotResponding
- NodeDown
- NodeOrConnectionDown
- SNMPv1 NA Config trap
- SNMPv2 NA Config trap
- BackplaneOutOfRangeOrMalfunctioning
- BufferOutOfRangeOrMalfunctioning
- CpuOutOfRangeOrMalfunctioning
- DiskOutOfRangeOrMalfunctioning
- MemoryOutOfRangeOrMalfunctioning
- NodeTraffic
- RoundTripTimeHigh
- TestFailed

You can also view **Node Configuration** and **History of Node Configuration** information from an incident. Figure 5 shows the NNMi analysis pane after opening a Node Down Incident, then selecting the **Node Configuration** tab.

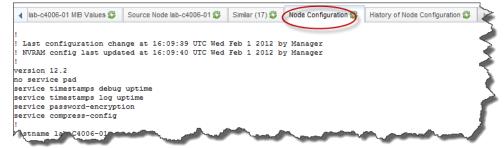**Figure 5   Node Configuration Tab**

Figure 6 shows the NNMi analysis pane after opening a Node down Incident, then selecting the **History of Node Configuration** tab.

Figure 6   History of Node Configuration Tab

To view additional node configuration information from the HP NA application, click **History of Node Configuration** or **Compare to Previous**.

Disabling Network Management During Device Configuration

For certain device configuration tasks, HP NA triggers HP NNMi to set the device to the DISABLED status during the configuration process. This administrative status suppresses NNMi monitoring of the device to prevent unnecessary incidents. Before configuring a device, HP NA sends an out-of-service event to HP NNMi. After device configuration succeeds, HP NA sends an in-service event to HP NNMi that removes the DISABLED status from the device and resumes regular state polling.

The **Out of Service Events** field on the NA **Administrative Settings - 3rd Party Integrations** page specifies the device configuration tasks that trigger HP NNMi to set a device to the DISABLED status during the task. The default selections are:

- Update Device Software

- Deploy Passwords

- Reboot Device

You can select any or all of the following additional tasks:

- Run Command Script

- Run Diagnostics

- Delete ACLs

- Configure Syslog

- Discover Driver

- Run ICMP Test

- Take Snapshot

- Synchronize Startup and Running

- OS Analysis

To disable this feature, clear all selections from the task list.

If device configuration does not complete satisfactorily, the behavior depends on the integration configuration.

- The **If the device task fails** setting on the NA **Administrative Settings - 3rd Party Integrations** page specifies whether the integration should remove or retain the DISABLED status in HP NNMi if device configuration is not successful.

- The **If device compliance check fails after the task completed** setting on the NA **Administrative Settings - 3rd Party Integrations** page specifies whether the integration should remove or retain the DISABLED status in HP NNMi if the device configuration is not compliant.

These settings apply to all device tasks selected in the **Out of Service Events** field. You cannot set the recovery behavior per task.

Propagating Device Community String Changes

When SNMP community string propagation is enabled, the integration behaves as follows:

- If the SNMPv1 or SNMPv2c community string that HP NA uses for accessing a synchronized device changes, HP NA informs HP NNMi of the change. HP NNMi then updates its settings for communicating with that device.

  HP NNMi immediately starts using the new community string for the device.

  HP NA sends updates to HP NNMi only when the community string for managing a device changes. HP NNMi does not receive updates when HP NA deploys a new community string to a device.

- If a new device is added to the NA inventory, HP NA informs HP NNMi of the SNMPv1 and SNMP v2c community strings that HP NA uses for managing the device.

The integration does not propagate SNMPv3 users from HP NA to HP NNMi.

The **Propagate SNMP Community Strings** setting on the NA **Administrative Settings - 3rd Party Integrations** page specifies whether the integration should forward SNMP community strings from HP NA to HP NNMi. By default, community string propagation does not occur.

NA Event Rules

NA event rules define how HP NA communicates with the NNMi management server.

Do not modify or delete these event rules in HP NA.

The integration defines the following event rules in HP NA:

- HP NNMi–HP NA Integration using SNMP Traps

  When a new device is added to the NA inventory or a device configuration is changed, this NA event sends an SNMP trap to HP NNMi. For more information, see Sending Device Configuration Change Notifications on page 26.

- NA/NNMi Topology Synchronization for Device Addition

  When a new device is added to the NA inventory, this NA event sends a device hint to HP NNMi. For more information, see Topology Synchronization Between HP NNMi and HP NA on page 21.

- NA/NNMi Topology Synchronization for Device Deletion

  When a device is deleted from the NA inventory, this NA event sends a request to delete the device from the NNMi topology. For more information, see Topology Synchronization Between HP NNMi and HP NA on page 21.

- NA/NNMi Integration Rediscover Host

  When the configuration for a device in the NA inventory changes, this NA event requests the latest NNMi status for the device. For more information, see Maintaining Accurate Device Information on page 26.

- NA/NNMi Integration Out Of Service

  When a task is started, this NA event sets the device to the OUT OF SERVICE state in HP NNMi. After the task completes, this event sets the device back to the IN SERVICE state in HP NNMi. For more information, see Disabling Network Management During Device Configuration on page 30.

- HP NNMi–HP NA Integration SNMP Community String Propagate

  When the Last Used Device Password Changed is changed for a device in the NA inventory, this NA event sends the community string that NA is using to manage the device to HP NNMi. For more information, see Propagating Device Community String Changes on page 31.

Changing the HP NNMi–HP NA Integration

1 In the NA user interface, open the **Administrative Settings - 3rd Party Integrations** page (**Admin > Administrative Settings > 3rd Party Integrations**).

   a Modify the values as appropriate. For information about the fields on this form, see the following references:

      — Maintaining Accurate Device Information on page 26

      — Disabling Network Management During Device Configuration on page 30

      — Propagating Device Community String Changes on page 31

   b Click **Save** at the bottom of the page.

2 In the NNMi console, open the **HP NNMi–HP NA Integration Configuration** form (**Integration Module Configuration > HP NA**).

   a Modify the values as appropriate. For information about the fields on this form, see HP NNMi–HP NA Integration Configuration Form Reference on page 36.

   b Verify that the **Enable Integration** check box at the top of the form is selected, and then click **Submit** at the bottom of the form.

➤ The changes take effect immediately. You do not need to restart ovjboss.

Disabling the HP NNMi–HP NA Integration

1   In the NNMi console, open the **HP NNMi–HP NA Integration Configuration** form (**Integration Module Configuration >** HP NA).

2   Clear the **Enable Integration** check box at the top of the form, and then click **Submit** at the bottom of the form. The integration actions are no longer available.

➤   The changes take effect immediately. You do not need to restart ovjboss.

Troubleshooting the HP NNMi–HP NA Integration

This section contains the following topics:

- Test the Integration on page 33
- NA Devices are Missing from the NNMi Topology on page 35

Test the Integration

➤   If the integration has worked successfully in the past, it is possible that some aspect of the configuration, for example, the NNMi or NA user password, has changed recently. Try updating the integration configuration as described in HP NNMi–HP NA Integration Configuration Form Reference on page 36, before walking through this entire procedure.

1   In the NNMi console, open the **HP NNMi–HP NA Integration Configuration** form (**Integration Module Configuration >** HP NA).

For information about the fields on this form, see HP NNMi–HP NA Integration Configuration Form Reference on page 36.

2   To check the status of the integration, in the **HP NNMi–HP NA Integration Configuration** form, click **Submit** at the bottom of the form (without making any configuration changes).

🚩   When successful, this step initiates a complete topology synchronization between HP NNMi and HP NA.

A new window displays a status message.

If the message indicates a problem with connecting to the NA server, HP NNMi and HP NA are not able to communicate. Continue with step 3 of this procedure.

3   To verify the accuracy and access level of the NA credentials, log on to the NA user interface with the credentials for the **NA User** from the **HP NNMi–HP NA Integration Configuration** form.

If you cannot log on to the NA user interface, contact the NA administrator to verify your logon credentials.

4   To verify that the connection to the NA server is configured correctly, in a web browser on the NNMi management server, enter the following URL:

http://<*naserver*>:<*naport*>/soap
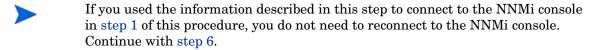
Where the variables are related to values on the **HP NNMi–HP NA Integration Configuration** form as follows:

-   <*naserver*> is the value of **NA Host**.

-   <*naport*> is the value of **NA Port**.

If the NA web service is running on the specified server and port, the NA server responds with a message similar to:

     NAS SOAP API: Only handles HTTP POST requests

-   If the expected message appears, continue with step 5.

-   If you see an error message, the connection to the NA server is not configured correctly. Contact the NA administrator to verify the information you are using to connect to the NA web services. Continue to troubleshoot the connection to HP NA until you see the expected message.

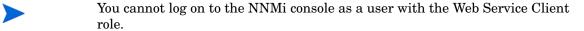5   Verify that the connection to HP NNMi is configured correctly:

➤   If you used the information described in this step to connect to the NNMi console in step 1 of this procedure, you do not need to reconnect to the NNMi console. Continue with step 6.

   a   In a web browser on the NA server, enter the following URL:

     http://<*NNMiserver*>:<*port*>/nnm/

   Where the variables are related to values on the **HP NNMi–HP NA Integration Configuration** form as follows:

   —   <NNMiserver> is the value of **NNMi Host**.

   —   <port> is the value of **NNMi Port**.

   b   When prompted, enter the credentials for an NNMi user with the Administrator role.

   You should see the NNMi console. If the NNMi console does not appear, contact the NNMi administrator to verify the information you are using to connect to HP NNMi. Continue to troubleshoot the connection to HP NNMi until the NNMi console appears.

➤   You cannot log on to the NNMi console as a user with the Web Service Client role.

6   Contact the NNMi administrator to verify the values of the **NNMi User** with the Web Service Client role and the corresponding **NNMi Password**.

7   Update the **HP NNMi–HP NA Integration Configuration** form with the values that you used for successful connections in step 4 and step 5 of this procedure. Also, re-enter the NNMi user and password from step 6 on this form.

For more information, see HP NNMi–HP NA Integration Configuration Form Reference on page 36.

8   Click **Submit** at the bottom of the form.

9 If the status message still indicates a problem with connecting to the NA server, do the following:

    a Clear the web browser cache.

    b Clear all saved form or password data from the web browser.

    c Close the web browser window completely, and then re-open it.

    d Repeat step 7 and step 8 of this procedure.

10 Test the configuration by launching one of the actions listed in Using the HP NNMi–HP NA Integration on page 21.

NA Devices are Missing from the NNMi Topology

If a device in the NA inventory does not appear in the NNMi synchronization node group, follow these steps:

1 Examine the NNMi node inventory to determine whether the device is in the topology but in a different node group.

    If this is the case, update the definition of the NNMi synchronization node group to include the device.

2 Examine the NNMi IP address inventory to determine whether the IP address used in NA is listed in HP NNMi.

    If the IP address is included in HP NNMi, determine which node hosts the IP address. This node should be synchronized with the NA device. HP NNMi might be using a different management address for this node than the IP address that HP NA sent as a discovery hint.

3 Optionally re-enable the integration.

    HP NA only sends discovery hints when the integration is enabled and when a new device is added to the NA inventory. If the device was added to HP NA during a network outage or before the NNMi synchronization node group and auto-discovery rules were correctly included, re-enable the integration to cause HP NA to re-send the discovery hint.

Application Failover and the HP NNMi–HP NA Integration

If the NNMi management server participates in NNMi application failover, the HP NNMi–HP NA integration reconfigures the NA server with the new NNMi management server hostname after failover occurs. Failover should be transparent to users of the integration.

The integration does not support failover of the NA server.

HP NNMi–HP NA Integration Configuration Form Reference

In the NNMi console, the **HP NNMi–HP NA Integration Configuration** form contains the parameters for configuring communications from HP NNMi to HP NA. This form is available from the **Integration Module Configuration** workspace.

➤ Only NNMi users with the Administrator role can access the **HP NNMi–HP NA Integration Configuration** form.

The **HP NNMi–HP NA Integration Configuration** form collects information for the following general areas:

- NNMi Management Server Connection
- NA Server Connection
- Integration Behavior

To apply changes to the integration configuration, update the values on the **HP NNMi–HP NA Integration Configuration** form, and then click **Submit**.

NNMi Management Server Connection

Table 2 lists the parameters for connecting to the NNMi management server from HP NA. You can determine many of these values by examining the URL that invokes an NNMi console session. Coordinate with the NNMi administrator to determine the appropriate values for this section of the configuration form.

Table 2   NNMi Management Server Information in the NNMi Console

Field	Description
NNMi SSL NA SSL	If you selected either of these check boxes, complete the actions shown on step 4 on page 14 to configure an SSL connection between HP NNMi and HP NA.
NNMi Host	The official fully-qualified domain name of the NNMi management server. This field is read-only. **NOTE**: The integration selects the port for connecting to the NNMi console by determining the value of `nmsas.server.port.web.http` in the following file: • *Windows*: `%NnmDataDir%\conf\nnm\props\nms-local.properties` • *UNIX*: `$NnmDataDir/conf/nnm/props/nms-local.properties`
NNMi User	The user name for connecting to the NNMi console. This user must have the NNMi Web Service Client role. Best practice: Create and use an `NNMiIntegration` user account with the Web Service Client role.
NNMi Password	The password for the specified NNMi user.

NA Server Connection

Table 3 lists the parameters for connecting to the web services on the NA server. Coordinate with the NA administrator to determine the appropriate values for this section of the configuration form.

Table 3   NA Server Information in the NNMi Console

HP NA Server Parameter	Description
NNMi SSL NA SSL	If you selected either of these check boxes, complete the actions shown on step 4 on page 14 to configure an SSL connection between HP NNMi and HP NA.
NA Host	The fully-qualified domain name or the IP address of the NA server.
NA Port	The port for connecting to the NA web services. The default NA ports are as follows: • 80—for connections to NA on a separate computer from NNMi • 8080—for connections to NA on the same computer as NNMi **TIP:** The NA URL displays the SSL port. If you selected **NNMi SSL**, **NA SSL**, or both during the integration configuration, SSL will work for integration communications. If you did not select an SSL option during the integration configuration, enter the correct non-SSL port.
NA User	A valid NA user account name with the NA Administrator role. **NOTE:** The password for this user name is passed in cleartext. Best practice: Create and use an `NAIntegration` user account.
NA Password	The password for the specified NA user.

Integration Behavior

Table 4 lists the NNMi console parameters for configuring the behavior of the HP NNMi–HP NA integration.

Table 4   Integration Behavior Information in the NNMi Console

Parameter	Description
Topology Filter Node Group	The NNMi node group containing the set of nodes to synchronize with the NA topology. The integration populates the NA inventory with information about every node in this node group. Select the node group from the list of node groups on this NNMi management server. If no node group is specified, the integration synchronizes the entire NNMi topology into the NA inventory.
Topology Synchronization Interval (hrs)	The frequency with which HP NNMi performs a complete topology synchronization with HP NA as described in Topology Synchronization Between HP NNMi and HP NA on page 21. The default interval for the connection check is 24 hours. To disable periodic topology synchronization, set this value to `0`.

Table 4   Integration Behavior Information in the NNMi Console (cont'd)

Parameter	Description
Discover Device Drivers in HP NA	The NA configuration specification. If the **Discover Device Drivers in NA** check box is selected, HP NA automatically discovers the device drivers for the devices added to NA as a result of topology synchronization with HP NNMi. The default setting is cleared. In this case, you can initiate device driver discovery manually.
NA Connection Check Interval (hrs)	The frequency with which HP NNMi verifies with HP NA the interface data for all layer 2 connections in the NNMi topology as described in Identifying Layer 2 Connections with Mismatched States on page 25. The default interval for the connection check is 24 hours. To disable the periodic connection check, set this value to 0.
Minimum NNMi Role for Analysis Pane Data	To view NA information in an NNMi analysis pane, you must log on to HP NNMi with a user account that is assigned one of the roles shown below. The selections for the Minimum NNMi Role for Analysis Pane Data are as follows: • Disable Feature: Disables HP NNMi from showing NA data in the NNMi analysis pane. • NNMi Administrators: Shows NA data in the NNMi analysis pane to NNMi users having the Administrator role. • NNMi Level 2 Operators: Shows NA data in the NNMi analysis pane to NNMi users having the Operator Level 2 or Administrator role. • NNMi Level 1 Operators: Shows NA data in the NNMi analysis pane to NNMi users having the Operator Level 1, Operator Level 2, and Administrator role. • NNMi Guest Users: HP NNMi shows NA data in the NNMi analysis pane to all NNMi users.
Map NNMi Security Groups to NA Partitions	After you select the Map NNMi security groups to NA partitions check box and submit the change, a node synchronized to NA will always be added or updated to be in a security partition having the same name as that node's NNMi security group.

HP NNMi Integration Configuration in HP NA Reference

In the NA user interface, the **NNMi Integration** section of the **Administrative Settings - 3rd Party Integrations** page contains the parameters for configuring communications from HP NA to HP NNMi. Enabling the integration on the **HP NNMi–HP NA Integration Configuration** form sets the fields on the **Administrative Settings - 3rd Party Integrations** page. Access the **Administrative Settings - 3rd Party Integrations** page to change the integration behavior for NNMi device rediscovery triggers, out-of-service triggers, and SNMP community string propagation.

The **Administrative Settings - 3rd Party Integrations** page is available from **Admin > Administrative Settings > 3rd Party Integrations**. To apply changes to the integration configuration, update the values on this page, and then click **Save**.

▶ Only NA users with the Administrator role can access the **Administrative Settings - 3rd Party Integrations** page.

Integration Communication

Table 5 lists the parameters for connecting to the NNMi web services from the NA server. The integration configures these parameters with the information on the **HP NNMi–HP NA Integration Configuration** form in the NNMi console.

Table 5   Integration Connection Information in the NA User Interface

Field	Description
NA User	The NA user account name specified on the **HP NNMi–HP NA Integration Configuration** form.
NA Partition	The NA partition specified on the **HP NNMi–HP NA Integration Configuration** form.
NNMi Host	The NNMi management server name specified on the **HP NNMi–HP NA Integration Configuration** form.
NNMi HTTP Port	The NNMi console port determined by the integration.
NNMi User	The NNMi user name specified on the **HP NNMi–HP NA Integration Configuration** form.
NNMi Password	The NNMi user password specified on the **HP NNMi–HP NA Integration Configuration** form.

Additional Integration Behavior

Table 6 lists the NA user interface parameters for configuring the behavior of the HP NNMi–HP NA integration.

Table 6   Integration Behavior Information in the NA User Interface

Field	Description
Rediscover Hosts After Tasks	The NA tasks for which the integration triggers an NNMi device discovery on task completion. The default selections are: • Update Device Software • Deploy Passwords • Reboot Device • Discover Driver For more information, see Maintaining Accurate Device Information on page 26.
Out of Service Events	The NA tasks for which the integration sets a device to the DISABLED state while the task occurs. The default selections are: • Update Device Software • Deploy Passwords • Reboot Device For more information, see Disabling Network Management During Device Configuration on page 30.
If the device task fails	The device task failure recovery specification for out-of-service events. The default setting is to return the device to service in HP NNMi. For more information, see Disabling Network Management During Device Configuration on page 30.
If device compliance check fails after the task completed	The device compliance check failure recovery specification for out-of-service events. The default setting is to return the device to service in HP NNMi. For more information, see Disabling Network Management During Device Configuration on page 30.
Propagate SNMP Community Strings	The community string propagation specification. The default setting is disabled. For more information, see Propagating Device Community String Changes on page 31.

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click *here*.

If no email client is available, copy the information below to a new message in a web mail client, and then send this message to **ovdoc-nsm@hp.com**.

Product name and version: NNMi 9.20

Document title: *HP Network Node Manager i Software - HP Network Automation Integration Guide*

Feedback: